(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2005-514720
(P2005-514720A)
(43)公表日　平成17年5月19日(2005.5.19)

(51)Int.Cl.[7]	F I			テーマコード（参考）
G11B 20/10	G11B 20/10	H		5B035
G06K 17/00	G06K 17/00	V		5B058
G06K 19/08	G11B 7/24	572E		5D029
G06K 19/10	G11B 7/24	572L		5D044
G11B 7/24	G11B 7/24	572M		5J104

審査請求 未請求　予備審査請求 有　（全 36 頁）　最終頁に続く

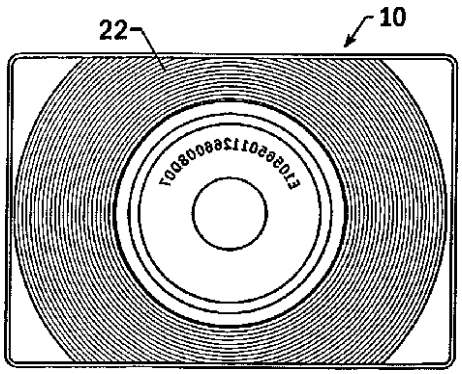
(21)出願番号　特願2003-558786 (P2003-558786)
(86)(22)出願日　平成14年12月20日 (2002.12.20)
(85)翻訳文提出日　平成16年8月30日 (2004.8.30)
(86)国際出願番号　PCT/US2002/041123
(87)国際公開番号　WO2003/058548
(87)国際公開日　平成15年7月17日 (2003.7.17)
(31)優先権主張番号　60/344,658
(32)優先日　平成13年12月31日 (2001.12.31)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　60/361,458
(32)優先日　平成14年3月4日 (2002.3.4)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　60/365,068
(32)優先日　平成14年3月14日 (2002.3.14)
(33)優先権主張国　米国 (US)

(71)出願人　504252743
ディジタル・データ・リサーチ・カンパニー
アメリカ合衆国フロリダ州３２７０１，アルタモンテ・スプリングス，シャディ・コート　６９４
(74)代理人　100099623
弁理士　奥山　尚一
(74)代理人　100096769
弁理士　有原　幸一
(74)代理人　100107319
弁理士　松島　鉄男

最終頁に続く

(54)【発明の名称】セキュリティ・クリアランス・カードおよび該カードを読取るシステムおよび方法

(57)【要約】
本発明のセキュリティ・クリアランス・カードのシステムおよび方法には、カード所有者の身元を証明するためのデータを格納するカードを含む。別の種類の情報に加えて、カードは所有者のバイオメトリック・データおよび他の識別データを格納する。データのそれぞれの部分は、格納データの各部分に指定されたセキュリティの所定レベルに基づいて、さまざまな暗号化方法を用いて暗号化できる。このとき、読取素子は、セキュリティ・クリアランス・カード暗号化データの少なくとも一部を読取りでき、個人からの少なくとも１つのバイオメトリック・データを受け取ることができる。次に、カードに格納されたバイオメトリック・データは、セキュリティ・クリアランス・カードに表された個人のバイオメトリック・データと比較され、カードの保有者がそのカードの所有者であることが証明される。



【特許請求の範囲】
【請求項１】
データを格納できるＣＤ－ＲＯＭにより形成される基板と、
カード保有者の身元を証明するためのデータを少なくとも含む、前記基板の表面に置かれたデータ記憶媒体と
を有してなる、カード保有者の身元を証明するためのセキュリティ・クリアランス・カード。
【請求項２】
前記データ記憶媒体が、符号化されたカード保有者の身元を証明するデータを含むバーコードである、請求項１に記載のセキュリティ・クリアランス・カード。
【請求項３】
前記カードが少なくとも３種類のデータ、すなわち身元データ、フィールド・データ、および他のデータを含み、身元データは前記カード所有者を証明するのに用いられ、フィールド・データは前記カード所有者に関連するデータであり、他のデータは前記カードに格納される関連事項のデータであり、
前記ＣＤ－ＲＯＭは３種類のデータすべてを格納して有することができ、
前記データ記憶媒体は、身元データおよびフィールド・データだけを格納して有する、請求項１に記載のセキュリティ・クリアランス・カード。
【請求項４】
セキュリティ・クリアランス・カードに格納された複数のデータ部分と、
複数のセキュリティ・レベルと
をさらに有し、
前記複数のデータ部分の少なくとも１つが、セキュリティ・クリアランス・カードの所有者の少なくとも１つのバイオメトリック識別子を含み、
前記複数のデータ部分の各々が前記複数のセキュリティ・レベルのいずれかに関連付けされている、請求項１に記載のセキュリティ・クリアランス・カード。
【請求項５】
セキュリティ・クリアランス・カードの作成と、前記セキュリティ・クリアランス・カードのデータの修正とに関連する少なくとも１つのイベントのレコードを含むログをさらに有する、請求項４に記載のセキュリティ・クリアランス・カード。
【請求項６】
カードの使用が有効になる日に対応する発効期日をさらに備える、請求項４に記載のセキュリティ・クリアランス・カード。
【請求項７】
セキュリティ・クリアランス・カードの所有者の身元を証明するためのセキュリティ・クリアランス・カードであって、
セキュリティ・クリアランス・カードに格納された複数のデータ部分と、
複数のセキュリティ・レベルと
を備え、
前記複数のデータ部分の少なくとも１つが、セキュリティ・クリアランス・カードの所有者の少なくとも１つのバイオメトリック識別子を含み
前記複数のデータ部分が前記複数のセキュリティ・レベルに関連付けされている、セキュリティ・クリアランス・カード。
【請求項８】
セキュリティ・クリアランス・カード上に置かれたデータ記憶媒体をさらに備え、前記複数のデータ部分の少なくとも１つが前記データ記憶媒体内に格納される、請求項７に記載のセキュリティ・クリアランス・カード。
【請求項９】
前記データ記憶媒体が符号化されたデータ部分を含むバーコードである、請求項８に記載のセキュリティ・クリアランス・カード。

【請求項１０】
ＣＤ－ＲＯＭをさらに備え、前記複数のデータ部分の少なくとも１つが前記ＣＤ－ＲＯＭに格納される、請求項７に記載のセキュリティ・クリアランス・カード。
【請求項１１】
前記カードが、データ部分を格納して有するＣＤ－ＲＯＭと、前記ＣＤ－ＲＯＭの表面に置かれるデータ記憶媒体とを備える、請求項７に記載のセキュリティ・クリアランス・カード。
【請求項１２】
前記複数のデータ部分の個々のデータを身元データ、フィールド・データ、および他のデータのいずれかとして分類し、
身元データは前記カード所有者を証明するのに用いられ、フィールド・データは前記カード所有者に関連するデータであり、他のデータは前記カードに格納される関連事項のデータである、請求項７に記載のセキュリティ・クリアランス・カード。
【請求項１３】
前記カードが、データ部分を格納して有するＣＤ－ＲＯＭと、前記ＣＤ－ＲＯＭの表面に置かれるデータ記憶媒体とを備え、
前記データ記憶媒体が身元データおよびフィールド・データの少なくとも１つを格納しており、
前記ＣＤ－ＲＯＭが身元データ、フィールド・データ、および他のデータの少なくとも１つを格納している、請求項７に記載のセキュリティ・クリアランス・カード。
【請求項１４】
前記複数のデータ部分の少なくともいずれかが、少なくとも１つの所有者に関連するデータと、所有者に関連する対象とを有する、請求項７に記載のセキュリティ・クリアランス・カード。
【請求項１５】
前記複数のデータ部分の少なくともいずれかが、選択された暗号化方法を用いて暗号化されている、請求項７に記載のセキュリティ・クリアランス・カード。
【請求項１６】
データを暗号化するのに用いる暗号化方法が、データに関連するセキュリティ・レベルに基づいている、請求項１５に記載のセキュリティ・クリアランス・カード。
【請求項１７】
複数の前記データ部分のそれぞれが、対応する異なるセキュリティ・レベルに関連付けされ、各データ部分がデータに関連するセキュリティ・レベルに基づく暗号化方法で暗号化されている、請求項１６に記載のセキュリティ・クリアランス・カード。
【請求項１８】
複数の暗号化方法が、動的に生成されるブロック暗号アルゴリズムである複数のアルゴリズムを含む、請求項１５に記載のセキュリティ・クリアランス・カード。
【請求項１９】
複数の暗号化方法が、所有者のバイオメトリック識別子に基づく暗号化方法を含む、請求項１５に記載のセキュリティ・クリアランス・カード。
【請求項２０】
複数の暗号化方法が、セキュリティ・クリアランス・カードの作成日に基づく暗号化方法を含む、請求項１５に記載のセキュリティ・クリアランス・カード。
【請求項２１】
前記複数のデータ部分の少なくともいずれかが、セキュリティ・クリアランス・カードに関連するイベントのレコードを含むデータログを備える、請求項７に記載のセキュリティ・クリアランス・カード。
【請求項２２】
前記データログが、前記カードに格納されたデータ部分になされる修正のレコードを含む、請求項２１に記載のセキュリティ・クリアランス・カード。

【請求項２３】
前記データログがカードの作成に関連するレコードを含む、請求項２１に記載のセキュリティ・クリアランス・カード。
【請求項２４】
前記データログが、カードが作成された日と、カードが作成された場所と、カードを作成した個人に関連するバイオメトリック・データとの少なくとも１つを含む、請求項２３に記載のセキュリティ・クリアランス・カード。
【請求項２５】
セキュリティ・クリアランス・カードの保有者の身元を証明するためのセキュリティ・システムであって、
カード所有者のバイオメトリック識別子を格納して有するセキュリティ・クリアランス・カードと、
前記セキュリティ・クリアランス・カードの格納されるバイオメトリック識別子を読取りできる少なくとも１つのカード読取素子と、
セキュリティ・クリアランス・カードの保有者のバイオメトリック・データを取り込むための少なくとも１つのバイオメトリック・データ読取素子と、
前記カード読取素子と前記バイオメトリック・データ読取素子と通信する処理素子と
を含み、
前記処理素子が、前記カード読取素子により読取られたセキュリティ・クリアランス・カードに格納されたバイオメトリック識別子と、前記バイオメトリック・データ読取素子により読取られたセキュリティ・クリアランス・カードの保有者のバイオメトリック・データとを比較し、それにより、カードの保有者がカード所有者であることを証明するものである、セキュリティ・システム。
【請求項２６】
前記セキュリティ・クリアランス・カードが、
ＣＤ－ＲＯＭから形成される基板と、
前記ＣＤ－ＲＯＭの表面に置かれたデータ記憶媒体と
を備えている、請求項２５に記載のセキュリティ・システム。
【請求項２７】
前記ＣＤ－ＲＯＭの表面上の前記データ記憶媒体がバーコードであり、
前記少なくとも１つのカード読取素子は、ＣＤ－ＲＯＭ読取器およびバーコード読取器の少なくともいずれかを備えて、前記ＣＤ－ＲＯＭおよび前記データ記憶媒体の少なくともいずれかに格納されたデータを読取るものである、請求項２６に記載のセキュリティ・システム。
【請求項２８】
前記ＣＤ－ＲＯＭおよび前記データ記憶媒体が複数のデータ部分を備えることができ、そのデータ部分が身元データ、フィールド・データ、および他のデータのいずれかとして分類され、
身元データは前記カード所有者を証明するのに用いられ、フィールド・データは前記カード所有者に関連するデータであり、他のデータは前記カードに格納される関連事項のデータであり、
前記ＣＤ－ＲＯＭは３種類のデータすべてを格納して含むことができ、
前記データ記憶媒体は身元データおよびフィールド・データだけを格納して含むものである、請求項２７に記載のセキュリティ・システム。
【請求項２９】
複数のデータ部分を格納して有し、各データ部分がデータのセキュリティ・レベルを定義しており、データに関連付けされたセキュリティ・レベル値を有するセキュリティ・クリアランス・カードと、
前記セキュリティ・クリアランス・カードからデータを読取りできる少なくとも１つのカード読取素子と、

前記セキュリティ・クリアランス・カードからデータ部分にアクセスするために、前記カード読取器と通信する少なくとも１つのコンピュータ・システムと
を備え
前記少なくとも１つのカード読取素子と前記少なくとも１つのコンピュータ・システムとは、それらに関連付けされており、前記カード読取素子と前記コンピュータ・システムとが前記カードからアクセスできるデータのセキュリティ・レベルを規定するセキュリティ・クリアランス値を有している、セキュリティ・システム。
【請求項３０】
前記セキュリティ・クリアランス・カードは前記カード読取素子に提供され、
前記カード読取素子は、前記カードに格納されている全てのデータ部分を読取るが、前記カード読取素子に関連するセキュリティ・クリアランス値によるアクセスのために指定される、関連付けられたセキュリティ・レベルを有するデータ部分だけにアクセスするものである、請求項２９に記載のセキュリティ・システム。
【請求項３１】
前記コンピュータ・システムは、前記セキュリティ・クリアランス・カードから前記カード読取素子により読取られる全データ部分を受け取り、前記コンピュータ・システムに関連するセキュリティ・クリアランス値によるアクセスのために指定される関連付けされたセキュリティ・レベルを有するデータ部分にアクセスするものである、請求項３０に記載のセキュリティ・システム。
【請求項３２】
複数のデータ部分を格納して有する少なくとも１つのセキュリティ・クリアランス・カードと、ここで、前記セキュリティ・クリアランス・カードの各データ部分は、データのセキュリティ・レベルを定義する、データに関連付けされたセキュリティ・レベル値を有しており、
前記セキュリティ・クリアランス・カードからデータを読取りできる少なくとも１つのカード読取素子と、
前記カード読取器と通信する複数のコンピュータ・システムと
を備え
前記複数のコンピュータ・システムのそれぞれは、それに関連付けされており、当該コンピュータ・システムが前記カードからアクセスできるデータのセキュリティ・レベルを規定するセキュリティ・クリアランス値を有しており、
前記カード読取素子が前記セキュリティ・クリアランス・カードのデータ部分を読取るときに、該データ部分が前記コンピュータ・システムのそれぞれに提供され、前記コンピュータ・システムのそれぞれは、前記コンピュータ・システムに関連するセキュリティ・クリアランス値に対応するデータ部分だけにアクセスする、セキュリティ・システム。
【請求項３３】
前記カード読取素子は、関連付けられたセキュリティ・クリアランス値を有し、前記セキュリティ・クリアランス・カードに格納された全データ部分を読取りでき、前記カード読取素子に関連するセキュリティ・クリアランス値に対応するデータ部分にアクセスできるものである、請求項３２に記載のセキュリティ・システム。
【請求項３４】
前記セキュリティ・クリアランス・カードは、それぞれ第１および第２セキュリティ・レベルを関連付けて有する少なくとも第１および第２データ部分を有し、
前記カード読取素子は、前記カード読取素子が第１セキュリティ・レベルを有するデータにアクセスできることを規定するセキュリティ・クリアランス値を有し、
前記コンピュータ・システムの少なくともいずれかは、前記コンピュータ・システムが第１セキュリティ・レベルを有するデータと第２セキュリティ・レベルを有するデータとの両方にアクセスできることを示すセキュリティ・クリアランス値を有し、
前記カード読取素子が前記セキュリティ・クリアランス・カードからデータを読取るときに、前記カード読取素子は、第１および第２データ部分の両方を読取り、かつ第１レベ

ルのセキュリティを有するデータ部分にアクセスし、
前記コンピュータ・システムは、前記カード読取素子から第１および第２データ部分の両方を受取り、両方のデータ部分にアクセスするものである、請求項３２に記載のセキュリティ・システム。
【請求項３５】
前記コンピュータ・システムの少なくともいずれかに関連するセキュリティ・クリアランス値は、変更可能であり、それにより前記コンピュータ・システムが前記カードからアクセスできるデータのセキュリティ・レベルを変化させるものである、請求項３２に記載のセキュリティ・システム。
【請求項３６】
前記コンピュータ・システムを操作できる複数のオペレータをさらに備え、
前記オペレータのそれぞれが、それに関連付けされており、前記オペレータがアクセスできるデータのセキュリティ・レベルを規定するセキュリティ・クリアランス値を有している、請求項３２に記載のセキュリティ・システム。
【請求項３７】
複数の保護位置と前記保護位置のそれぞれに関連するカード読取器とをさらに備え、前記保護位置のそれぞれは、セキュリティ・レベル値を関連付けて有している、請求項３２に記載のセキュリティ・システム。
【請求項３８】
前記保護位置が、１つの設備、アイテムの位置、およびデータ・ファイルの位置である、請求項３７に記載のセキュリティ・システム。
【請求項３９】
各セキュリティ・クリアランス・カードが、前記セキュリティ・クリアランス・カードの所有者がアクセスできる保護位置のセキュリティ・レベルを規定する関連付けされたセキュリティ・クリアランス値を有するものであり、前記所有者が選択された保護位置だけにアクセスできる請求項３７に記載のセキュリティ・システム。
【請求項４０】
セキュリティ・クリアランス・カードに関連するセキュリティ・クリアランス値を変化させて、前記セキュリティ・クリアランス・カードの所有者によりアクセスできる特定の保護位置を変更できる、請求項３９に記載のセキュリティ・システム。
【請求項４１】
保護位置のそれぞれが関連するセキュリティ・レベル値を有する複数の保護位置と、
前記保護位置のそれぞれに関連するカード読取素子と、
前記カード読取器のそれぞれと通信するセンターのコンピュータ・システムと、
複数のセキュリティ・クリアランス・カードと
を備え、
各セキュリティ・クリアランス・カードは、それに関連付けられており、前記セキュリティ・クリアランス・カードの所有者がアクセスできるセキュリティ・レベルを示すセキュリティ・クリアランス値を有し、
前記センターのコンピュータ・システムは、保護位置のセキュリティ・レベル値を変更して、セキュリティ・クリアランス・カードの所有者が前記保護位置にアクセスできるのを変更できるものである、セキュリティ・システム。
【請求項４２】
複数の個人のだれが保護位置にアクセスするかを示すデータ・ファイルを保護位置のそれぞれが有している複数の保護位置と、
前記保護位置のそれぞれに関連するカード読取素子と、
前記カード読取器のそれぞれと通信するセンターのコンピュータ・システムと、
複数のセキュリティ・クリアランス・カードと
を備え、
各セキュリティ・クリアランス・カードが、前記セキュリティ・クリアランス・カード

の所有者に対応する身元値を有し、
前記センターのコンピュータ・システムが保護位置に関連するデータ・ファイルを変更して、セキュリティ・クリアランス・カードのどの所有者が前記保護位置にアクセスできるかを変更できる、セキュリティ・システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は一般に、セキュリティ・システムに関し、さらに詳細には、大きい格納空間と格納した情報のセキュリティを向上させたセキュリティ・クリアランス・カードを使用するセキュリティ・システムであって、様々なカード読取器およびオペレータによるカード上のデータへのアクセスを選択的に制御し、およびカード保有者による設備のさまざまな部分へのアクセスを選択的に制御するセキュリティ・システムに関する。
【背景技術】
【０００２】
多くの企業および行政機関はセキュリティ・システムを利用して、設備、データなどへのアクセスを制御している。アクセスは一般に、セキュリティ・クリアランス・カードおよび／またはパスワード・アクセスを用いて制御される。多くの従来のセキュリティ・システムは、カード読取器、バイオメトリック・スキャナなどを使用して制御される。さらに、多くの従来のセキュリティ・システムはネットワークをベースにしている。詳細には、これらのシステムは、個人に関連するセキュリティ識別番号および／または個人に関連する格納されたバイオメトリック・データなど、設備、データなどへのアクセスを許可された個人に関するセキュリティ・アクセス・コードおよびデータを含む集中型データ・サーバを使用する。一般に、これらの従来のセキュリティ・システムは集中型ネットワーク方式で作動するため、アクセスの意思決定を遅らせる可能性がある。さらに、これらのシステムで使用されるセキュリティ・クリアランス・カードは、基本的に、サーバ内にあるユーザに関連するデータを認識するのに用いられるトークンを単に含むだけのカードであるか、またはカードが簡単に損傷を受ける可能性があるプロセッサおよびメモリを含む。また、従来のセキュリティ・システムは一般に、設備および場所へのアクセスに関する複雑な意思決定を含まない。特に、大部分のシステムは、標準的なエントリ／ノー・エントリの意思決定を使用するだけで、アクセス条件の動的な変更を許可しない。最終的に、多くの従来のセキュリティ・システムは、さまざまなセキュリティ読取器およびセキュリティ要員によるセキュリティ・クリアランス・カードに格納されているさまざまなレベルの情報へのアクセスを制限する能力を持たない。これらの問題点は、以下の詳細に議論される。
【０００３】
セキュリティ・クリアランス・カードは、通常、特定の場所、対象(object)、情報、電子メディア、および／またはアクセスが制限されているその他の有形または無形のアイテムへのアクセスの承認を受けている個人に対して発行される。例えば、アクセスを制限するアイテムを含む組織は、通常、組織がアイテムにアクセスする権限を認可すると考えるこれらの個人にセキュリティ・クリアランス・カードを発行する。したがって、セキュリティ・クリアランス・カードは、カードを携帯する個人が１つまたは複数の制限されたアイテムにアクセスすることを許可するような、特定の種類の情報、表示／または方法を保有することができる。例えば、カードが画像情報を含むことにより、セキュリティ要員または他の要員がカードを視覚的に検査して、カードが有効であり、および／またはカードが制限されたアイテムへの自動的アクセスを可能にする情報を含んでいることを保証できる。
【０００４】
通常個人は、セキュリティ・クリアランス・カードを発行する前に、個人身元の証拠、すなわち、出生証明、住所証明、運転免許証、社会保障カード、ビザ、パスポート、および／または個人の身元を証明するその他の情報の提供に基づくような、いくつかの種類の

背景調査を受けなければならない。加えて、個人は、学歴、職歴、所属および／または特定の種類の背景調査に関連する個人の経歴に関するその他の情報など、背景に関する詳細な情報を提供しなければならない場合がある。個人に関する望ましい情報が累積されると、その情報は、情報が有効であることを保証するために、組織にとって許容できる何らかの方法で検証される。

【０００５】

いくつかの従来のセキュリティ・カードは、カードが発行される個人に関連するデータを符号化するための、バーコード、磁気ストライプおよび／または他の類似の種類のデータ記憶デバイスを含む。またカードは、前述のような、基本的な個人の身元およびアクセス・データに加えて、他の種類のデータを含む。

【０００６】

セキュリティ・システムによっては、カード保有者のバイオメトリック・データを用いて、検証を行う。これらのシステムにおいて、指紋、網膜スキャン、音声サンプル、ＤＮＡサンプルなど、カード所有者の１つまたは複数のバイオメトリック・データが、カード所有者から採取され、セキュリティ・システムの集中型データベースに格納される。次に、トークンまたは他の識別子が、バーコードまたは類似の符号化デバイスの形式でカード上に格納される。作動においては、保有者がカードをカード読取器に提示すると、バイオメトリック・データに関するトークンが読み込まれる。セキュリティ・システムはトークンを使用してネットワーク・データベースをポーリングし、保有者に関するトークンを取り出す。さらに、保有者はセキュリティ・システムに接続されているバイオメトリック・スキャナを用いて走査されたバイオメトリックを有する。セキュリティ・システムは、スキャナから取られた走査されたバイオメトリック・データと、カードから取られた保存されたバイオメトリックとを比較して、カードを提示している人物が登録されたカード保有者であるかどうかを証明する。

【０００７】

前述のとおり、バイオメトリック識別子は、通常、セキュリティ・カードに直接格納されない。その代わり、トークンはカードに格納され、このトークンは、カードの所有者に関連するバイオメトリック識別子が格納されているリモート・データベースに問合わせするのに必要な情報を提供する。したがって、カード読取器は、カードに格納されているトークンを読み込み、トークンにより提供される指示に基づいて適切なリモート・データベースに問合わせできる。この例においては、カード読取器は、カード保有者を確認するため、リモート・データベースとの連続的または半連続的な通信を行う。言い換えると、格納されたバイオメトリック・データと走査されたバイオメトリック・データの比較は、カード読取器の、リモート・データベースとの通信能力に依存する。加えて、格納されたバイオメトリック・データの完全性はリモート・データベースの完全性に依存している。バイオメトリック・データの比較は、カード読取器とリモート・データベース間の通信が妨げられリモート・データベースが妨害され、および／またはリモート・データベースが意図的にまたは偶然に破壊されるため、簡単に危険にさらされる。さらに、リモート・データベースのポーリングおよびそのデータベースからのバイオメトリック・データの取り出しに関連するその他の遅延が発生する場合がある。また、カード読取器に対してネットワーク接続できることを要求することは、セキュリティ・システムが遠隔に配置されたセキュリティ・チェックポイントで使用される事例については、現実的ではない。

【０００８】

多くの従来のセキュリティ・カード・システムの別の欠点は、格納容量である。これら従来のカードに格納できるデータ量は、バーコード、磁気ストライプおよび／またはカードの表面に印刷される類似の方式のデータ格納手段に符号化して格納するデータ量により制限される。

【０００９】

最近は、データ格納にＣＤ－ＲＯＭを使用する名刺が開発されている。これらの名刺は、カードに類似した形をしているＣＤ－ＲＯＭを含む。ＣＤ－ＲＯＭの表面には、名前、

役職、会社名、住所、電話番号その他など、カード所有者に関するビジネス・データが存在する。これらの名刺に利点は、ＣＤ－ＲＯＭ上に追加データを格納できることである。例えば、ＣＤ－ＲＯＭカードは、カード所有者に関連する会社関係のデータを格納するのに利用される。このデータは、名刺の受取人が従来のＣＤ－ＲＯＭプレイヤーを用いて見ることができる。

【００１０】

ＣＤ－ＲＯＭ名刺はカードに格納できるデータ量を増大させるが、これらの従来のカードは、セキュリティの設定に利用するのに適していない。詳細には、これらの従来の名刺は、名前・会社名・住所およびＣＤ－ＲＯＭ上に格納された会社に関するその他のマーケティング情報など、カードの前面に情報を含んでいるが、通常そのカードがカード所有者のものであることを受取人に証明する、カードに印刷されたまたは格納された情報はない。したがって、個人がＣＤ－ＲＯＭカードを提示する場合、ＣＤ－ＲＯＭカードがその個人のものであること、またはカードに格納されているデータがその個人に関連していることを保証する方法はない。

【００１１】

また、スマート・カードもセキュリティ・システムでの利用目的で開発されている。スマート・カードは、埋め込まれたメモリまたは埋め込まれたメモリおよびプロセッサ両方、のどちらかを含む。これらのカードは、セキュリティ・カード上に追加のデータ情報を格納するのを可能にする。さらに、プロセッサを利用してメモリに格納されたデータの処理を実行できる。ただし、これらのカードは、関連するセキュリティ問題を有する。特に、スマート・カードはハッキングを受けやすい。スマート・カードのメモリに対する読み取りおよび書き込みの手順が決定されると、カード上のセキュリティ・データは簡単にアクセスされ変更される可能性がある。その結果、カードは危険にさらされるか、または変更されて無許可の人物により使用される可能性がある。

【００１２】

従来のセキュリティ・クリアランス・カードに関連する欠点に加えて、セキュリティ・システム自体の欠点もいくつか存在する。問題の１つは、データのアクセスの制限である。詳細には、データによっては、セキュリティ・カード上にデータの他の部分のデータよりも機密度の高い広範囲のデータを含むのが望ましい。例えば、カード保有者を証明するためのデータに加えて、財産記録、医療記録および犯罪暦など、カード保有者に関する経歴に関するデータをカードが含む。この場合、カードの所有者を証明するためのデータへのアクセスを認めると同時に、個人の経歴に関するデータへのアクセスを制限することは重要である。残念ながら、多くの従来のセキュリティ・カードには、これは不可能である。通常、カード読取器を操作する要員が、カード上に格納されているすべてのデータにはアクセスできないことを保証する方法は無い。したがって、カードに搭載されているデータにアクセスする唯一の人物がカードの所有者でない限り、一般に、カードを読出しできるいずれの人物も、カード所有者がそのカードに格納しようとするデータ・タイプを限定できる全てのカード上に格納されたデータを見ることが許可される。

【００１３】

多くの従来のセキュリティ・システムに伴うその他の問題は、設備またはデータ、またはセキュリティが要求される他のものにアクセスを行うおよび行わない人物の決定の柔軟性である。詳細には、多くの従来のシステムは「合格／不合格」意思決定上で作動する。ある設備、データなどにアクセスを許可された人物のリストは、システムにおいてハードコードされ、動的には変更されない。例えば、個人が、本来は、設備の１つの部分にアクセスする許可を有しているが、設備の他の部分に対しては許可を有していない場合がある。多くの従来のセキュリティ・システムには、設備の第２の部分へのアクセスを提供された個人のリストは、個人情報を伴って、手動で更新され、その後、設備の入口の第２の部分におけるカード読取器またはセキュリティ・ゲートに提供される必要がある。これは、特に、設備へのアクセスを許可された個人のリストを通常ベースで変更される場合において、時間のかかる処理である。

【発明の開示】
【発明が解決しようとする課題】
【００１４】
従来技術におけるこれらの欠点の観点から、カード所有者の身元を立証する方法を提供すると同時に、大量のデータを搭載可能なセキュリティ・カードの必要性がある。またカードは、不正操作を減少し、追加のデータ・セキュリティを実現することが必要とされる。加えて、情報へのアクセスを取得しようとする個々の試みのセキュリティ・レベルに基づき、カード上に格納されたさまざまなレベルのデータへのアクセスを制限するようこのようなカードの必要性が存在する。また、セキュリティ情報を立証するのにネットワークへの常時接続を必要としないセキュリティ・システム、ならびに設備へのアクセスを許可された人物に関する情報の動的な更新を可能にするセキュリティ・システムの必要性が存在する。
【課題を解決するための手段】
【００１５】
本発明は、前述ならびに従来技術において指摘された多くの他の問題点を改良する。本発明のセキュリティ・システムの利点の多くは、以下に要約され、その後に詳細に説明される。
【００１６】
本発明は、大きいデータ記憶容量を有するセキュリティ・クリアランス・カードを使用するセキュリティ・システムを提供し、同時にまた、カード所有者の身元を証明するためのさまざまな機能を提供する。さらに、本発明のセキュリティ・クリアランス・カードは、カードを証明するのに用いるセキュリティ・システムのカード読取器にネットワークとの常時接続を必要としないような、自立型のセキュリティ・チェック・システムを提供する。
【００１７】
詳細には、本発明のセキュリティ・システムは、データの複数部分を格納できるセキュリティ・クリアランス・カードを提供する。カードの保有者の少なくとも１つのバイオメトリック識別子が少なくともいずれかのデータ部分に格納されている。他のデータ部分には、保有者の略歴、保有者の銀行の記録、犯罪暦などのカード保有者のさまざまな情報を含むことできる。加えて、各データ部分はセキュリティ・レベルに関連付けできるため、さまざまな種類のデータがさまざまなレベルのセキュリティを有することができる。
【００１８】
データ部分は、使用されるセキュリティ・カードの種類に依存して、さまざまな方法で格納できる。例えば、ＣＤ－ＲＯＭを備えるセキュリティ・カードを使用できるが、この場合には、データはＣＤ－ＲＯＭに格納される。カードは、追加してまたは代替的に、データを格納するバーコード、ホログラムなど、カードの表面に配置されたデータ記憶媒体を含むことができる。さらに、本発明のセキュリティ・クリアランス・カードはスマート・カードとして具体化できるが、この場合にはデータがカードのメモリ部分に格納される。
【００１９】
前述のとおり、本発明のセキュリティ・クリアランス・カードは、カード保有者の少なくとも１つの格納されたバイオメトリック・データを含む。これにより、カードに関連するセキュリティ・システムはネットワークから独立して作動できる。詳細には、この実施形態のセキュリティ・システムは、カードの読取りデバイスおよびユーザのバイオメトリック・データを走査するデバイスを含む。動作の際、ユーザのバイオメトリック・データが走査され、あらかじめ格納されたカード保有者のバイオメトリック・データは、ＣＤ－ＲＯＭまたはスマート・カードの場合、カードに格納されているデータから、あるいはカード表面に格納されているバーコードまたはホログラムの場合、カード表面上の記憶媒体のどちらかから取り出される。その後、格納されたおよび走査されたバイオメトリック・データを比較して、カードを提示している個人がカードの所有者であることを立証する。

セキュリティ・クリアランス・カード自体にバイオメトリック・データを置くことにより、セキュリティ・システムは、ネットワーク上に置かれた遠隔データベースをポーリングしてこのデータを取り出す必要が無くなる。

【００２０】

これによりいくつかの利点がもたらされる。第１に、すべてのカード保有者のデータが損なわれ、盗まれ、または別の方法で破壊される可能性がある場合、すべてのカード保有者のバイオメトリック・データのすべてを、同一のセンターのデータベースに必ずしも格納する必要はない。さらに、本発明のセキュリティ・クリアランス・カードは、データが傍受される可能性がある場合、ネットワークを介する安全保護データの伝送を必要としない。さらに、本発明のセキュリティ・クリアランス・カードにより、セキュリティ・チェックポイントをネットワーク接続から完全に解放または部分的に解放できるため、チェックポイントを自立型とし、また遠隔地に配置できるようになる。

【００２１】

前述の通り、本発明のセキュリティ・クリアランス・カードは、通常、カード保有者に関連する広範囲のデータを格納している。バイオメトリック・データなどカードの所有者を証明するのに用いるデータに加えて、セキュリティ・カードはカード保有者の情報データを含む。このデータは、ユーザに関する一般的データを含むが、財産データ、医療データ、犯罪暦など、セキュリティ上の機密度の高いデータを含む。広範囲のデータをカード上に置かくことができることから、データへのアクセスを制限することが重要になる。この点を考慮して、本発明のセキュリティ・カードの格納データはさまざまなレベルで格納されている。したがって、これらのレベルへのアクセスは、他人による観察から制限される。アクセスのさまざまなレベルを、本発明のセキュリティ・システムにおけるオペレータおよび／またはデバイスに割り当てることにより、指定された人物だけが、あるレベルにおいて現れるデータを見ることができる。

【００２２】

また本発明のセキュリティ・システムは、セキュリティ・クリアランス・カードから読取られるデータを、セキュリティ・システムの他のデバイスに渡すことを可能にする。詳細には、セキュリティ・クリアランス・カードは、アクセスに関して制限されるさまざまなレベルの下で格納されているデータを含む。カード読取器はカードからデータのすべてを走査するが、セキュリティ・アクセスを制限されるために、データの特定部分を読取ることができるだけである。しかしデータの他の部分は、他のレベルの制限されたデータを読取ることができる、セキュリティ・システム内の他のデバイスに渡すことができる。このように、カードからのデータは、カード読取器により取り出され、カード読取器が理解できなくても、データを読取る権利を有するセキュリティより高いレベルにある他のデバイスに渡すことができる。

【００２３】

例として、カード読取器は、カード保有者を確認し、設備へのアクセスを認可するのに必要なカード上のデータへのアクセスを有するだけである。ただし、保有者の前科に関するデータ部分はカード読取器により読取りできるが、カード読取器を復号可能にはしないで、読取器に接続されている他のデバイスに転送し、そこでデータを観察して、その人物がセキュリティのリスクを提示するかどうかを決定することができる。

【００２４】

カードに関するイベントの記録もカードに格納される。例えば、データ部分の修正および追加の記録、カード作成および／またはカード保有者から受け取ったバイオメトリック・データはカードに格納される。この監査の記録により、セキュリティ要員は、カードの使用ならびにカードのセキュリティを破ろうとする可能な違反または試みを追跡できる。

【００２５】

本発明のセキュリティ・クリアランス・カードは、また、開始日、確認日などに関する情報の格納を可能にできる。詳細には、カードはカード読取器により読取られる有効期限を含む。カードが選択された有効期限を超過している場合、保有者はアクセスを拒否され

る。これはカードの窃盗に対する保護のために重要である。カードが盗まれたとしても、カードは限定された期間に使用できるだけである。さらに、開始日がカード上に含まれる。開始は、カードが有効になる時を定義する。開始日より前の使用はセキュリティ・システムにより拒否される。作成日もまた、カード上に格納される。この作成日は、カード上のデータを暗号化するのに用いられる暗号化方法が時々変更されるような方式において使用される。詳細には、日付の範囲に対して、これらの日付の間に作成されたカードはある方法を使用して暗号化され、さらに別の方法が他の範囲の日に使用される。カードが読取られると作成日も読取られる。作成日に基づき、カード読取器は、カードから読取られたデータを利用するのに用いる暗号化方式を認識する。

【００２６】

データの完全性を保護するために、本発明のセキュリティ・システムは一般に、常時ではないが、「追記型」（write once/read many times）手順を用いて、カード上にデータを格納する。追記型手順は、カードを使用して不正なアクセスを取得しようとしている人物によって試みられるカード上のセキュリティ・データの上書きを防ぐ。

【００２７】

カード上のデータは、さまざまな暗号化方法のうちの少なくともいずれかを用いて暗号化される。具体的には、データのそれぞれの部分は格納されている各データ部分に割り当てられているセキュリティ・レベルに基づき、さまざまな暗号化方法を用いて暗号化される。暗号化方法は、カード上に格納されるデータの少なくとも一部分を暗号化するのに用いられるさまざまなアルゴリズムを含む。例えば、アルゴリズムはブロック暗号アルゴリズムであってもよい。

【００２８】

本発明のセキュリティ・システムはまた、特定場所の設備、データなどへのアクセスを許可されている人物のリストの動的な変更を可能にする。詳細には、ネットワークを介して、特定の位置へのアクセスが許可されている個人のリストを変更するか、または別に、カード読取器を用いて遠隔で更新および格納できる。カードが読取器により走査され保有者が立証されると、カード読取器はリストにアクセスしカードの保有者が設備へのアクセスを有する人物として指定されているかどうかを確認する。保有者がリスト上にない場合、設備へのアクセスは拒否される。

【００２９】

別の方法として、保護された位置のセキュリティ・レベルを変更し、それにより、アクセスが許可されたカード所有者のリストを変更する。例えば、保護された位置が小数のカード所有者へのアクセスが認められているだけの第１のセキュリティ・レベルを有する場合、保護された位置に関するセキュリティ・レベルはより低くすることができ、それにより、より多くのカード所有者のアクセスを許可する。

【００３０】

これまで、本発明を一般的事項で説明してきたが、以下、添付図面を参照する。図面は必ずしも縮尺通りではない。

【発明を実施するための最良の形態】

【００３１】

本発明を、添付図面を参照してさらに詳細に説明する。添付図面には、本発明の実施形態いくつかを示すが、全部は示していない。実際に、本発明は多くの異なる形態で実現化できる。本発明は本明細書に記載した実施形態に限定されるものではなく、これら実施形態を提供することにより、本開示内容が適用すべき法的要件を満足するようにするものである。同一符号は全体を通して同一素子を指す。

【００３２】

本発明は、従来技術に関する前述の問題点の多くを改良するセキュリティ・クリアランス・カードを提供する。詳細には、本発明は、大きいデータ記憶容量を可能にするセキュリティ・クリアランス・カードを使用するセキュリティ・システムを提供し、同時にまた、カード所有者の身元を証明するためのさまざまな機能を提供する。さらに、本発明のセ

キュリティ・クリアランス・カードは、カード読取器と組み合わされて、さまざまなセキュリティ・レベルでカードに格納されたデータの各部分を関連付けでき、カード読取器および／またはカード読取器のオペレータが観察および／またはアクセスできるデータ量を限定できる。

【００３３】

本発明は一般に、制限された情報、位置、または他の有形または無形アイテムにアクセスを希望する個人の身元を証明できるセキュリティ・システムに関する。図１には本発明のセキュリティ・システムの１つの実施形態を示すが、セキュリティ・システムの他の多くの実施形態および応用が実現可能であり、それらの多くは以下に詳細に説明される。例えば、個人１２はドア１４から入ることを望むことできる。個人１２はセキュリティ・クリアランス・カード１０を提示し、そのカードはカード読取器１６により読取りできる。カード読取器１６は個人１２からバイオメトリック・データを受け取り、そのデータをカードに格納された、カード保有者に関連付けされたバイオメトリック・データと比較することができる。次に、カード読取器のオペレータは、モニター１８によって、バイオメトリック・データ比較の結果と、オペレータがアクセスを許可されるカードに格納されたデータ部分とを見ることができる。個人１２のバイオメトリック・データがカード１０のバイオメトリック・データと一致し、オペレータ２０によりアクセスされたデータが、カード保有者がドア１４を入ることを許可するのに必要なデータに一致すると、個人１２はドア１４から入るのを許可される。一方、個人１２のバイオメトリック・データがカード１０のバイオメトリック・データと一致しない場合、および／またはオペレータ２０によりアクセスされたデータが、カード保有者がドア１４を入ることを許可するのに必要なデータに一致しない場合、個人１２はドア１４から入るのを拒否される。代替方法では、カード保有者の走査されたバイオメトリック・データとカードに格納されたバイオメトリック・データとの比較は、コンピュータまたは専用プロセッサにより電子的に実行できる。

【００３４】

カード１０は、身元データ、フィールド・データ、および関連事項の任意の追加データを含むことができる。身元データは、カード保有者が実際にカード所有者本人であることを証明するのに使用できるあらゆる種類のデータを含む。例えば、身元データはカード所有者の名前、住所、および誕生日を含むことができるが、これらに限定されない。身元データはまたカード所有者の少なくとも１つのバイオメトリック・データを含むことができる。

【００３５】

フィールド・データは、カード所有者に関するあらゆる種類の詳細データ、および／またはカード所有者が責任を有するアイテムとすることができる。例えば、フィールド・データはカード所有者の運転免許証番号、運転免許制約、有権者情報、および雇用情報、および／またはアイテムの履歴、アイテムを利用するための情報、またはカード所有者が責任を有するアイテムに関する任意の他の種類の情報を含むことができるが、これらに限定されない。フィールド・データは複数レベルを有することができ、各レベルはセキュリティの異なるレベルに関連付けできる。例えば、カード所有者の雇用者の名前および住所などの基本雇用情報は、フィールド・データの第１レベルに置かれ、一方、カード所有者の個人記録は基本雇用情報に関連付けできるが、第１レベルより高度に保護される、フィールド・データの１つまたはそれ以上の高いレベルに置かれる。さらに、フィールド・データは高レベルに分類されるデータを含むことができ、これらデータは最高レベルのセキュリティを有する。高レベルに分類されるデータには、カードの内部制御およびカード所有者の少なくとも１つのバイオメトリック・データを含むことができるが、これらに限定されない。

【００３６】

追加データは、カード所有者がカードに格納することを望むあらゆる他の種類のデータとすることができる。例えば、追加データは文書、ファイル、チャート、または他の形式のデータであってもよい。追加データはまた、希望する場合は、セキュリティの指定レベ

ルとすることができる。

【００３７】

データは一般に、当業者には公知のように、データの部分またはパケットに分割される。各データ部分はさまざまなセキュリティ・レベルの１つに関連付けでき、また、各データ部分は、以下の説明するように、圧縮、符号化、および／または暗号化できる。簡単化の目的で、データ部分はここでは「データ」と称する。

【００３８】

カード所有者は、身元データがカードに格納されている個人である。カード１０に格納されたフィールド・データおよび／または追加データは、カード所有者に関連付けできる。代替方法では、フィールド・データおよび／または追加データは、カード所有者が責任を有する何らかの有形または無形アイテムに関連付けできる。例えば、カードに格納されたフィールド・データおよび／または追加データは、船舶、コンテナ、組織、アイデア、電子媒体、または他の種類の、有形または無形の対象（object）に関連付けでき、また、カード所有者はその対象に責任を有する任意の人物であってもよい。さらに、カード１０の所有者の身元を証明するためのカードの特定の実施形態においては、カード１０の複数所有者を有することができる。この場合、カードに格納される身元データは各所有者に関連付けされる。

【００３９】

先に簡単に述べたように、カード１０に格納される身元データは、任意の形式を取ることができ、また、カードの所有者または複数所有者を識別するのに用いられる任意の選択されたデータとすることができる。例えば、カード所有者に関連するバイオメトリック・データをカードに格納できる。バイオメトリック・データは、当業者には公知の任意の種類のバイオメトリック識別子であってもよい。例えば、バイオメトリック識別子は１つまたは複数の指紋、網膜スキャン、音声サンプル、ＤＮＡサンプル、これらの２つまたはそれ以上の組合せ、または任意の他の種類のバイオメトリック・データであってもよい。バイオメトリック・データは、カード所有者の身元の証明のためにカードが提示された時にいつでも容易にアクセスできるカード内の位置に格納でき、それにより、格納されたバイオメトリック・データは、以下に詳細に説明するように、カードを提示する人物のバイオメトリック・データと比較できる。さらに、バイオメトリック・データは、カード内の、アクセスを厳重に制限される高レベルに分類された部分に格納することができ、それにより、バイオメトリック・データの完全性を保存できる。さらに、容易にアクセスできるバイオメトリック・データは、高レベルに分類されたバイオメトリック・データと比較することにより、容易にアクセスできるバイオメトリック・データを危険にさらさないことを保証できる。

【００４０】

カード１０を提示する人物（「カードの保有者」とも称する）のバイオメトリック・データがカード１０に格納されたバイオメトリック識別子に一致すると、カードを提示する人物は、アクション、すなわちある場所または物への許可されたアクセスを実行することが認められて、カードに格納された任意のデータ、および／またはカードに格納されたデータにより許可される他の任意の種類の機能も利用することができる。しかし、カードを提示する人物のバイオメトリック・データがカードに格納されたバイオメトリック識別子に一致しない場合、カードを提示する人物はカード所有者に認められるいずれの種類の機能も拒否される。

【００４１】

図２および３は、本発明の１つの実施形態によるセキュリティ・クリアランス・カード１０（以後「カード」）を示す。この実施形態のカードはカード所有者の身元を証明するためのいくつかの形態を含む。例えば、カード１０はＣＤ－ＲＯＭ２２から形成される。ＣＤ－ＲＯＭは一般フィールド・データおよび身元データを含むだけでなく、追加データを含むことができる。図３に示すように、カード１０はまた、カードの表面に置かれるデータ格納媒体２４を含むことができる。データ格納媒体２４は一般フィールド・データお

よび身元データの両方を含むことができる。

【００４２】

ＣＤ－ＲＯＭ２２は当業者には公知の任意のタイプのＣＤ記憶素子であってもよい。一般にＣＤ－ＲＯＭ２２は、カード１０の中心にＣＤ－ＲＯＭ２２の中心を有するカード１０の形体である。したがって、カード１０はＣＤ－ＲＯＭ読取器内に置くことができ、以下に詳細に説明されるように、その読取器でカードのＣＤ－ＲＯＭ部分を読取りできる。本発明の好ましい実施形態においては、ＣＤ－ＲＯＭに格納されたデータはＣＤ－ＲＯＭをアクセスするデバイスにより読取りされるだけであり、データは削除、変更または修正できない。ＣＤ－ＲＯＭに書き込まれるデータは永久にＣＤ－ＲＯＭ内に格納される。したがって、新しいデータはＣＤ－ＲＯＭに書き込みできるが、古いデータもＣＤ－ＲＯＭ内に残る。このタイプのＣＤ－ＲＯＭは一般にＣＤＲと呼ばれる。ＣＤＲは本発明のセキュリティ・クリアランス・カード１０において有利である。この理由は、カードに格納される全データの永久記録が将来の参照に備えて維持されるからである。ＣＤＲは「追記型」と呼ばれることもある。さらに、ＣＤ－ＲＯＭはまた、オリジナル・データを格納したオペレータ、ならびに後続データをＣＤ－ＲＯＭに格納したすべてのオペレータの位置および身元を含む監査のための形跡（trail）を含むことができる。したがって、カードに格納されたデータに関して疑問がある場合、データの起点およびデータが書き込まれた環境はカードから用意に得ることができる。したがって、この種類のデータ格納は、データ格納に対して、カードに格納されたデータの不正操作を防止する能力を持たないマイクロプロセッサ・ベースのスマート・カードなどの、従来技術方式に比べてより厳重に保護されおよび不正操作されない。

【００４３】

別のデータ書込み手順も使用できることは、理解されるべきである。カードに格納されたデータに厳重なセキュリティを保証しない実施形態のような、本発明の別の実施形態においては、書込みデータの削除、変更または修正、さらに読込みを可能にするＣＤ－ＲＯＭを使用できる。このタイプのＣＤ－ＲＯＭは一般にＣＤＲＷと称する。

【００４４】

図２に関しては、データ格納媒体２４は、それがカードのＣＤ－ＲＯＭ部分を妨害しない限り、カードのどの位置にでも配置できる。例えば、データ格納媒体２４は一般に、図３に示すとおり、カードの少なくとも片面上に符号化フォーマットでプリントされる。この用途の目的に対し、符号化データは、カード１０への格納のための一般的電子データ・フォーマットを適用する。したがって、符号化は暗号化と同一ではない。暗号化は、認定された関係者だけがデータにアクセスできるようにデータを変更することと定義される。以下に詳細を説明するように、データ格納媒体２４に含まれるデータは、当業者に公知の任意の方法を用いて符号化することにより、データを復号化できる読取器がそのデータを利用できるようにする。例えば、データ格納媒体はＰＤＦ－４１７などのバーコードの形体に符号化できる。代替方法では、データ格納媒体はホログラム、連続の符号化ドット、グラフィック・イメージ、磁気ストリップなどに格納できる。先のＣＤＲの説明と同様に、バーコードまたは簡単に変更できない別のタイプの表示は、データ格納の有利な方法である。なぜなら、データおよびデータの生成を取り巻く環境が、将来の参照に備えて、カード内に永久的に格納されるからである。

【００４５】

カードに格納されたバイオメトリック・データおよび任意の別のデータに加えて、ＣＤ－ＲＯＭ２２および／またはデータ格納媒体２４はカード所有者のディジタル写真を含むことができる。この写真を詳細な検査に利用して、カードを提示する人物がカード所有者であるかどうかをチェックできる。なぜなら、以下に詳細に説明するように、カードがカード読取器で読取られるとき、オペレータはカード所有者の写真にアクセスして、写真とカードを提示する人物とを目視で比較できるからである。代替方法では、カード読取器は、カメラなどを用いて、カードを提示する人物の画像を撮影後、その画像とカード所有者の写真を比較できる。このように、ディジタル写真は一般に、ＣＤ－ＲＯＭおよび／また

はカードのデータ格納媒体部分に、身元データとして格納されるが、フィールド・データの一部として格納することもできる。本発明のカード１０の別の実施形態においては、カード所有者の画像２６を、図３に示すように、カード１０の表面上に含むことができる。この画像２６は、ＣＤ－ＲＯＭおよび／またはカード１０のデータ格納媒体部分に格納された画像に、追加またはこれに代わることができる。

【００４６】

カード１０はまた、カードの表面に、図３のカードの片面の実施形態の領域２８内に示されるとおり、カード１０の満了日および／または発効期日に加えて、氏名、電話番号、および／またはカード所有者の肩書などの任意の別の種類のデータを含むことができる。

【００４７】

重要な点は、図２および３に示すように、本発明はセキュリティ・クリアランス・カードを提供し、そのカード内に、カード所有者を証明するためのいくつかの異なる種類の身元データを格納することである。カード所有者の証明プロセスは、カードを作成し、セキュリティおよびカードを介するアクセスを維持するための、全体セキュリティ・システム（本明細書では、「身元証明システム」とも呼ばれる）のさまざまな態様と共に、以下に詳細に述べる。

【００４８】

図２および３は、本発明のセキュリティ・クリアランス・カードを、カード表面にプリントした情報を有するＣＤ－ＲＯＭとして示す。これはセキュリティ・クリアランス・カードの１つの実施形態としてだけ理解されるべきである。詳細には、本発明のセキュリティ・クリアランス・カードは、カードにプリントされたバーコードなどのデータ記憶媒体を有する標準カードの形体に具体化できる。この実施形態においては、身元データ、フィールド・データ、および関連事項の任意の追加データは符号化され、カード表面にプリントされるデータ記憶媒体に格納される。この実施形態のカードは、セキュリティ・システムにおいて、カードの表面にプリントされるデータ記憶媒体のデータ格納容量に比べて大きいデータ格納容量の利点を有するＣＤ－ＲＯＭを備えたＣＤ－ＲＯＭカードと全く同一に作動する。代替方法では、本発明のセキュリティ・クリアランス・カードはスマート・カードの形体に具体化できる。データ格納および取出しはＣＤ－ＲＯＭカードと同様である。手短に言えば、本発明のさまざまな態様はＣＤ－ＲＯＭベースのカードの使用に限定されず、さまざまなデータ格納手段を有する多くの異なる種類のカードを使用できる。

【００４９】

第１の態様は、セキュリティ・クリアランス・カードの作成に使用する所有者に関するデータの収集および格納である。詳細には、ＣＤ－ＲＯＭおよび／またはカードのデータ格納部分などの、カードに所望のデータを格納するために、身元証明システムのオペレータはカードの予想所有者から身元データを受取り、そのデータをデータベースに格納する。当業者には公知の任意の種類のデータベースを利用でき、そのデータベースには任意の適正なプロトコルを介してアクセスできる。本発明の身元証明システムの１つの実施形態においては、データベースは関係型であり、ＯＤＢＣ（Ｏｐｅｎ　Ｄａｔａｂａｓｅ　Ｃｏｎｎｅｃｔｉｖｉｔｙ）標準プロトコルを介してアクセスされる。このデータベースはオペレータの位置に配置するか、または、遠隔に配置し、ＬＡＮ（ローカル・エリア・ネットワーク）、ＷＡＮ（広域ネットワーク）、イントラネットおよび／またはインターネットなどの従来または無線方式ネットワークを介してオペレータ位置と通信することができる。

【００５０】

図４は、カード読取器１６のさまざまな実施形態を示す。これら読取器の１つは従来コンピュータ３０であり、オペレータはこのコンピュータを用いて、コンピュータ３０の位置のデータベース、または制御センター５６に設置されたデータベースにアクセスできる。制御センター５６は、以下に詳細に述べるように、予想のカード所有者の身元証明が実行される任意の位置にあってもよい。制御センター５６はまた、カード所有者および予想のカード所有者のすべてまたは少なくとも一部に関連する身元確認データのセンタのリポ

ジトリーが維持される位置または素子であってもよい。以下に詳細に述べるとおり、カード読取器１６のデータ・アクセス能力および／またはカード読取器のオペレータは、必要に応じて、制御センター５６を介して制御および変更できる。

【００５１】

データは、当業者には公知の方法で、カードの予想所有者から得ることができる。例えば、カードの予想所有者は出生証明、住所証明、運転免許証、パスポート、ビザ、または他の公式文書などの文書をオペレータに提示する。オペレータが、アクセス可能であるとして確立されているいずれかの方法で、カードの予想所有者の提供した情報がその個人に属することを決定すると、オペレータは、カードの予想所有者に関連付けされた証明された身元データを含むデータベース内にファイルなどのレコードを作成できる。このレコードは、その日を過ぎると無効となるカードに関連した満了日、および／または、カードが有効になる将来の特定日を指定するカードの発効期日を含むことができる。満了日または数年先に満了日を持たない永久または長期間セキュリティ・クリアランス・カードは、さまざまな種類の長期間身元データおよびフィールド・データを格納するカードの所有者に対して作成できる。例えば、本発明のセキュリティ・クリアランス・カードの特定の実施形態においては、運転免許証情報、有権者登録情報、雇用情報、および他の種類の長期間情報を、カードに格納するフィールド・データ内に含むことができる。したがって、カードに含まれている全情報が証明されると、永久または長期間カードをカード所有者に発行できる。また別に、オフィス・ビルへの短期間の訪問者、地方への短期間の訪問などの短期間の利用に対し、および／または時間情報が永久または長期間カードについて証明されている間、一時的セキュリティ・クリアランス・カードを発行でき、そのカードには身元データおよび／またはカードの短期間利用に必要なフィールド・データだけを含む。

【００５２】

データベース内にレコードを作成するために、オペレータはインタフェースを介してデータベースに身元データを入力する。データベースは、図４に示すような、任意のタイプのコンピュータ３０、処理素子および／またはデータベースと通信するデータ・エントリ素子、および／または制御センター５６内に設置されたデータベースなどのデータベースと通信するネットワーク３２または類似装置であってもよい。例えば、本発明の身元証明システムの１つの実施形態においては、オペレータ・インタフェースは、Microsoft WindowsまたはUnixオペレーション・システムなどの任意の最新のオペレーション・システムを利用するコンピュータであってもよい。レコードには他の情報も含むことができるが、この情報はカードの将来の用途、特定の身元証明システムの必要事項、または他の理由に依存する。オペレータが、カードの予想所有者の提供した情報がその個人に属することを決定できない場合、この個人はセキュリティ・クリアランス・カードを拒否され、証明を実行でき、および／または詳細な情報を個人に要求できるまでだけ有効な一時的カードが発行される。

【００５３】

カードの予想所有者はまた、データベース・レコードに格納するための少なくとも１つのバイオメトリック・データも提出する。例えば、本発明の身元証明システムの１つの実施形態においては、カードの予想所有者は、オペレータ・インタフェースと通信する指紋スキャナを介して少なくとも１つの指紋をデータベースに提出できる。指紋スキャナは当業者には公知の任意のタイプのスキャナであってもよい。本発明の身元証明システムの１つの実施形態においては、指紋スキャナはBiometric Access Corporation(BAC)から市販されているSecure Touch ＰＣスキャナである。個人の指紋の画像のようなバイオメトリック・データは、スキャナからオペレータ・インタフェースに転送できる。バイオメトリック・データは分析および／または調製して、当業者には公知の任意の方法で、オペレータ・インタフェースを介して格納できる。例えば、バイオメトリック・データが指紋の画像である場合、ＢＡＣソフトウェアまたは当業者には公知の任意の他の種類のソフトウェアを利用して、画像から特徴テンプレートが抽出される。特徴テンプレートは画像から無関係なデータを削除して、バイオメトリック画像の比較を容易にする。

【００５４】
指紋以外またはこれに追加するバイオメトリック・データを使用できる。例えば、カード所有者の網膜または顔面スキャン、ＤＮＡまたは音声サンプル、心拍特徴などを採取して格納できる。次に、これらさまざまなバイオメトリック・データは独立または組み合わせて使用して、セキュリティ・クリアランス・カードの所有者を証明できる。
【００５５】
カードの予想所有者の１つまたは複数の画像をキャプチャーして、データベース・レコードに組み入れることができる。画像はディジタル写真または他の任意の種類の写真であってもよい。画像がディジタルである場合、オペレータ・インタフェースおよびデータベースに直接転送できる。ただし画像がディジタルでない場合、当業者には公知のように、走査してディジタル・フォーマットに変換するか、またはオペレータ・インタフェースおよびデータベースに転送できるフォーマットに変換する。予想のカード所有者の画像をキャプチャーするために、オペレータ・インタフェースは、当業者には公知の任意のタイプの画像キャプチャーデバイスと通信できるようにされる。
【００５６】
本発明の身元証明システムの１つの実施形態においては、予想カード所有者の画像はＴＷＡＩＮ準拠画像キャプチャーデバイスを用いてキャプチャーできる。ＴＷＡＩＮはコンピュータ・ハードウェアおよびソフトウェアの両方であり、ソフトウェア・アプリケーションと画像アプリケーション・デバイス間の通信用の標準プロトコルおよびＡＰＩ（アプリケーション・プログラム・インタフェース）を定義する。ＴＷＡＩＮはＴｗａｉｎ　Ｗｏｒｋｉｎｇ　Ｇｒｏｕｐから市販されている。予測カード所有者の画像をキャプチャーすると、この画像はＴＷＡＩＮまたは当業者には公知の任意の他の方式を介してオペレータ・インタフェースに転送できる。次に、画像を分析および／または調製して、当業者には公知の任意の方法で、オペレータ・インタフェースを介して格納できる。例えば、オペレータは、データベースおよび／またはカードに格納される画像をキャプチャーまたは調製できる。
【００５７】
さらに、個人からキャプチャーされるバイオメトリック、画像および／または他の身元データは調製して、格納されたバイオメトリック・画像および他の身元データの既存の捜査当局の（law enforcement）データベースに適合するフォーマットに変換される。このように、キャプチャーされたバイオメトリック・画像および他の身元データを該当する捜査当局データベースとの比較を実行し、存在する場合は捜査当局の情報を得る。さらに、個人からキャプチャーされるバイオメトリック、画像および／または他の身元データは該当する捜査当局データベースに転送して、必要に応じて、捜査当局データベースに追加または更新できる。本発明の身元証明システムのこれら実施形態においては、オペレータ・インタフェースおよび／またはデータベースは、広域ネットワークなどの従来または無線ネットワークを介して捜査当局データベースと通信する。
【００５８】
例えば、本発明の身元証明システムの１つの実施形態においては、オペレータ・インタフェースおよび／またはデータベースは、さまざまな州および／または連邦の捜査機関の属するＡＦＩＳ（Automatic Fingerprint Identification System：自動指紋認証システム）と通信する。したがって、セキュリティ・クリアランス・カードを得ようとする個人から１つまたは複数の指紋が得られると、指紋をＡＦＩＳに転送して、レコードの指紋と比較できる。この手順はまた、転送されたバイオメトリック・データおよび／または画像を、捜査当局データベース内の既存のバイオメトリック・データおよび／または画像にマッチングさせ、いずれかの一致に関連して、既存のバイオメトリック・データおよび／または画像が、既存のバイオメトリック・データおよび／または画像をオペレータに提出する個人とその個人が同一であるかどうかを決定することにより、予想カード所有者の身元を証明する別の方法を可能にする。
【００５９】

本発明のセキュリティ・クリアランス・カードの別の重要な態様は、カード自体の上における、カード所有者の身元に関連するデータを格納する能力である。詳細には、オペレータがレコードをデータベースに入力し終わるか、またはオペレータがレコードをデータベースに入力している間に、レコードに含まれるデータのすべてまたは一部をカードに格納でき、カード内の記憶媒体（例えば、ＣＤ－ＲＯＭ、スマート・カードなど）、および／またはセキュリティ・クリアランス・カード１０のデータ記憶媒体部分などに格納できる。

【００６０】

特定の実施形態において重要な点は、カードを自立型システムに形成するために、バイオメトリック・データを含むレコードの少なくとも一部をカードに格納できることである。これにより、セキュリティ・システムは、ネットワーク・データベースからデータを取り出すことなく、カード所有者を証明できる。

【００６１】

前述のように、データを受取り・証明・格納することに加えて、オペレータはまた、フィールド・データおよび追加データを受取・証明して、セキュリティ・クリアランス・カード内に格納することができる。前述のように、フィールド・データには、カードのさまざまな用途において必要となる任意の種類の情報を含めることができる。さらに、フィールド・データは、フィールド・データに含まれる各種類のデータに指定されるセキュリティ・レベルに基づいて分離できる。本発明のセキュリティ・クリアランス・カードのさまざまな実施形態はフィールド・データのさまざまな種類の組合せを含むことができる。例えば、個人に関連するフィールド・データは、運転免許証情報、有権者登録情報、雇用情報、銀行口座情報、および望まれる他の種類の情報を含むことができる。本発明のセキュリティ・クリアランス・カード１０の別の実施形態においては、フィールド・データを対象（有形または無形）に関連付けできる。例えば、フィールド・データが自動車に関連している場合、フィールド・データは、その自動車が何をおよび／または誰を運送するかに関する情報、自動車の移動履歴、および自動車または運転者に関連する他の情報を含むことができる。

【００６２】

フィールド・データのそれぞれの種類は、さまざまなセキュリティ・レベルに指定することができ、フィールド・データの各種類内のデータも、指定されるさまざまなセキュリティ・レベルを有している。以下に詳細に説明するように、フィールド・データの各種類およびフィールド・データの各種類内において指定されるセキュリティ・レベルのために、カードを読取りできる各要員は、特定の用途に直接該当するデータだけにアクセスできる。例えば、低レベルのデータはカード所有者の名前および場合により所有者のディジタル写真を含むことができる。高レベルのセキュリティ・データは、住所、口座番号などの所有者の個人情報を含むことができる。さらに高レベルのセキュリティ・データはさらに重要な機密情報を含むことができる。従来システムの限界は、このデータのすべてが一般に、データの機密度に関係なく、カードを走査する人物によりアクセス可能である点である。しかし、本発明は、特定のカード読取器および／またはカード読取器のオペレータがデータの一定レベルまたは複数レベルだけを読取りできるように保証することにより、この問題点を解決する。これに関しては以下に詳しく述べる。

【００６３】

カード１０内に身元データ、フィールド・データおよび／または他のデータが存在するだけでなく、カード作成およびデータ記憶体の環境（ここでは「作成データ」と称する）もカード内に格納される。例えば、オペレータがカードにデータを格納するとき、オペレータの身元情報をカードに格納できる。カードにカード所有者データを格納し、カードを作成するのに用いる装置の識別名もカードに格納できる。さらに、何らかのカード所有者データを得て処理または格納する、すべてのサーバまたはデータベースの識別名もカードに格納できる。カード内のカード作成およびデータ格納に関する作成日および任意の他の種類の情報も、カードに格納されるデータに含めることができる。したがって、カードに

関するカード作成およびデータ格納を追跡するのに必要な情報のすべてをカードに直接格納し、カードに関する問題が発生した場合、即座にアクセスできるようにすることができる。カードに直接格納される作成日を含むデータのすべてを有することは、データのどれかについて分離したデータベースにアクセスすることを必要としないため、本発明のセキュリティ・システムの速度およびセキュリティを、システムで利用するデータの多くを分離したデータベースに依存する従来のセキュリティ・システムに比べて大幅に向上させる。

【００６４】

さらに、本発明のセキュリティ・クリアランス・カード１０は、前述のように、ＣＤ－ＲＯＭ部分２２を含むだけでなく、データ記憶媒体部分２４も含むことができるため、特定データへのアクセスを、データの位置、カード読取器のタイプ、および／またはカード読取器のオペレータの身元に基づき、さらに制限することができる。例えば、本発明の１つの実施形態においては、低いセキュリティ・レベルのデータはカードの前面にプリントされたデータ記憶媒体部分２４内に置き、一方、高いセキュリティ・レベルのデータはＣＤ－ＲＯＭ部分２２内に置くことができる。特定のカード読取器は、バーコード読取器、磁気ストリップ読取器などのような、データ記憶媒体に対する読取器だけを備えることにより、そのカード読取器がアクセスできるデータだけを、カード表面に置かれたデータ記憶媒体内に格納されるデータとすることができる。さらに、上の例では、特定のオペレータを、低いセキュリティ・レベルのデータだけへのアクセスを許可するようにでき、したがって、オペレータはカードのデータ記憶部分だけに対して読取器を操作できるようになる。このように、カード内に異なる種類の記憶媒体を含むことにより、カードに、従来のセキュリティ・クリアランス・カードが保有しない別のセキュリティ機能を実現できる。

【００６５】

さらに、本発明のセキュリティ・クリアランス・カード１０はさまざまな種類の多量のデータを格納でき、また、身元証明に必要な全情報および他の適用可能データは本発明のセキュリティ・クリアランス・カードに含まれる。カードを提示する人物のバイオメトリック・データをそれと比較するバイオメトリック・データに対して、またはカード読取器が必要とする他のデータに対して、集中データベースにアクセスする必要がない。したがって、以下に詳細に述べるように、カード読取器に組み合わせるカードは低コストで、より効率的であり、従来の方法に比べてセキュリティ・クリアランス・カードの所有者の身元を証明する高信頼性方法を有する。

【００６６】

カード所有者に身元を証明するための、さまざまな機能を有するセキュリティ・クリアランス・カードを提供することに加えて、本発明のセキュリティ証明システムは、カードに格納されるデータのセキュリティを保証するのに用いるさまざまな機能を提供する。これら機能のそれぞれを個別の表題に分けて説明する。

【００６７】

［Ａ．圧縮］

ＣＤ－ＲＯＭ２２および／またはデータ記憶媒体２４などのカードに格納される、バイオメトリック・データ、任意選択では写真を含むデータを当業者には公知の任意の方法によって圧縮することができる。例えばデータは、Digital Data Research Companyから市販されているTexCopm圧縮などの構文圧縮、辞書ベース圧縮、および／または任意の種類の演算圧縮を用いてディジタル圧縮できる。圧縮方式を利用してカードに格納されるデータを圧縮することにより、最大量のデータをカードに格納できる。

【００６８】

前述のように、カード１０に格納されるデータは一般に、複数部分またはパケット内に格納され、カードに格納されるデータをさらに圧縮するのを容易にする。各データ部分は当業者には公知の方法で配置できる。例えば、各データ部分は固定フィールド位置に配置され、これにより、効率的な格納および処理態様を提供するが、データ部分の変更が発生する場合に困難性が増す。本発明の別の実施形態においては、データは、フィールド識別

子、レコード・マークの終端、および／または文脈的および意味的アーチファクトなどの、言語的アーチファクトを含めて配置される。この方法は、データ部分の変調における柔軟性を提供するために望ましい。カード１０の特定用途の要件に依存して、他の適正な配置方法も利用できる。

【００６９】

［Ｂ．暗号化］

ＣＤ－ＲＯＭ２２およびデータ記憶媒体２４などのカード１０に格納される、バイオメトリック・データ、任意選択では写真を含むデータは当業者には公知の任意の方法で暗号化できる。本発明のカード１０の１つの実施形態においては、暗号化に先立って、データを前述のように圧縮することができる。本発明のカードの別の実施形態においては、データは圧縮せずに暗号化できる。

【００７０】

当業者には公知の暗号化方法の任意の方式を利用して、カードに格納されるデータを暗号化できる。例えば、任意の方式の暗号化アルゴリズムを用いてデータを暗号化でき、この暗号化はキーを含む。暗号化がキーを含む場合、キー内容およびサイズが周期的に変化する。このように、利用される暗号化アルゴリズムの数と種類（キーがアルゴリズムにより使用されるかどうか、使用される場合はキーの内容とサイズがどうであるか）に依存して、さまざまな種類の暗号化方式を生成することができる。暗号化アルゴリズムは動的に生成されるブロック暗号化アルゴリズムであってもよい。

【００７１】

単一カードまたはカード・セットに利用される暗号化方式は暗号化カクテル（encryption cocktail）と呼ばれる。このように、さまざまな種類の暗号化カクテルを生成して、各カードまたは各カード・セットが異なる暗号化カクテルを有するようにできる。したがって、異なる暗号化カクテルは、カードまたはカード・セットに特定の固有の暗号化構造を有する。例えば、１つの企業のビルにアクセスするのに用いられるカードまたはカード・セットは、別の企業のビルにアクセスするのに用いるカードまたはカード・セットと異なる暗号化カクテルを利用する。この種類の暗号化割当ては極めて安全な環境を生成する。なぜなら、１つのカードまたはカード・セットの暗号化構造が決定されたとしても、別のカードまたはカード・セットのセキュリティは維持されるからであり、これは従来技術のセキュリティ・システムと異なり、特にマイクロプロセッサ・カードを利用するシステムとは異なる。

【００７２】

さらに、複数の種類の暗号化号式を用いて、カードに格納されるデータの異なる部分を暗号化できる。したがって、例えばデータに割当てられるセキュリティ・レベルおよび／またはデータの機密度に応じて、異なる暗号化方式をカードに格納されるさまざまな種類のデータに割当てできる。例えば、前述のように、カードに格納される身元データ、フィールド・データ、および／または追加データに割当てられる、さまざまなレベルのセキュリティのそれぞれには、異なる暗号化方式を指定できる。カードに格納されたデータの想定された読取器に対して、特定種類の暗号化または複数の暗号化データだけを読取る能力を割当てることと連携したこの構成によって、読取器に関連する利用に該当するカードに格納されたデータ部分だけをカードを読取る要員が読取りおよび／またはアクセスすること許することが保証される。

【００７３】

前述のように、セキュリティ・クリアランス・カードはさまざまなレベルのデータを含むことができる。例えば、低レベルのデータはカード所有者の名前および場合により所有者のディジタル写真を含むことができる。高レベルのセキュリティ・データは、住所、口座番号などの所有者の個人情報を含むことができる。さらに高レベルのセキュリティ・データはさらに重要な機密情報を含むことができる。従来システムの限界は、このデータのすべてが一般に、データの機密度に関係なく、カードを走査する人物によりアクセス可能である点にある。しかし、本発明はこの問題点を解決する。詳細には、本発明のシステム

は、カード所有者に関するデータを異なるセキュリティ・レベルに分類し、データに関連付けされた特定のセキュリティ・レベルにアクセスする権限を有するカード読取器のオペレータだけに、データへのアクセスを許可する。

【００７４】

例えば、特定のカード読取器およびカード読取器のオペレータまたはオペレータ・グループは、カードに格納されたデータの特定部分だけにアクセスできる。カード読取器は、特定種類または複数の特定種類の暗号化データだけを復号でき、別の種類の暗号化方式で暗号化されたデータへのカード読取器へのアクセスを制限している。さらに、各オペレータまたはオペレータ・グループを、各オペレータまたはオペレータ・グループがアクセスを許可されるデータの暗号化の種類だけを読取りする能力に関連付けることができる。カード読取器および／またはオペレータが特定種類の暗号化データを読取ることを許可されているかどうかに関係なく、図５に示すように、暗号化データは暗号読取器５８により読取りできる。

【００７５】

カードに格納される身元データ、フィールド・データ、および／または追加データは、データの特定種類に割当てられるセキュリティ・レベルに応じて、さまざまな暗号化方式を用いて暗号化できる。例えば、図１の例では、オペレータ２０をカードに格納された身元データ部分などの、第１レベルのデータの暗号化だけを読取る能力に対応でき、一方で、オペレータ・マネージャを、第１レベルのデータの暗号化だけでなく、高レベルのセキュリティを割当てられたデータの少なくとも一部の暗号化も読取る能力に関連付け、これにより、マネージャがカード所有者により組織に提示されるリスクを評価するのを支援する。本発明のセキュリティ・システムの別の実施形態においては、カード所有者の名前、住所およびバイオメトリック・データなどの基本の身元データは暗号化されず、一方で、他の身元データ、フィールド・データおよび／または追加データのすべては暗号化される。したがって、特定のカード読取器および／またはオペレータはすべての種類の暗号化を読取る能力には対応しておらず、その結果、基本の身元データだけに、すべての暗号化データへのアクセス能力を用いることなくアクセスできる。

【００７６】

さらに、暗号化方式をカード所有者のバイオメトリック・データに関連付けできる。したがって、以下に詳細に説明するように、カードを提示する人物のバイオメトリック・データが、カードの少なくともＣＤ－ＲＯＭ部分２２に格納されたカード所有者のバイオメトリック・データに一致する場合、カードに格納されているデータは、ある読取器によってだけ暗号化しないようにできる。さらに、カードに格納されたデータの暗号化方式をカード所有者のバイオメトリック・データに関連付けることにより、各カードに使用される各暗号化方式は異なり、その結果、カードに格納されたデータのセキュリティを向上させる。

【００７７】

本発明の別の実施形態においては、暗号化方式はカードに格納される作成データに関連付けできる。したがって、各カードに格納されるデータの暗号化は、各カードに関連する異なる作成環境に基づいて異なる。

【００７８】

前述のさまざまな暗号化方式は、機密度の高いセキュリティ・カード・データを格納するための、極めて安全な環境を提供する。さらに、１つのカードの暗号化カクテルが不正な方法で明らかになった場合でも、１つだけが危険にさらされるだけである。従来のセキュリティ・クリアランス・カードでは、全てのカードは、マイクロプロセッサ・カード、スマート・カードなどのように、カードまたはデータベース内で同一セキュリティ構造を有しており、状況が大きく異なっている。なぜなら、従来カードは、カードおよび／またはデータベースのセキュリティ構造が明らかになった場合、カードのすべておよび大部分のセキュリティが危険にさらされるためである。

【００７９】

各カードはデータの異なる配置（表題「圧縮」で述べたように）および異なるデータ暗号化方式を利用する可能性があるため、各カードに利用されるデータ配置および暗号化は特定の方法でカード読取器を通信して、カードに格納されたデータの該当部分を発見および読取りできるようにする必要がある。本発明のセキュリティ・システムの１つの実施形態においては、データベースおよび／またはテーブル方式を用いて、配置、暗号化およびそのデータ部分に関連する他の情報を記録する。データベースおよび／またはテーブルはカード１０に格納できる。さらに、カードに格納された各データ部分にはＩＤ番号を割当てでき、この番号を用いてデータベースおよび／またはテーブル内のデータ部分に関連する情報を検索できる。

【００８０】

カード読取器がカードに格納されたデータ部分を走査するとき、ＩＤ番号はそのデータ部分から抽出される。次に、カード読取器はデータベースおよび／またはテーブルにアクセスし、ＩＤ番号を利用して、そのデータ部分の配置、データ部分の暗号化、およびそのデータ部分に関連する任意の他の情報を検索する。カード読取器および／またはカード読取器を操作するオペレータは、そのデータ部分に割当てされた暗号化の種類を復号することを許可され、カード読取器はそのデータ部分を読取ることができる。カード読取器がデータ部分を読取るかどうかに関係なく、以下に述べるように、読取器はデータ部分を別の下流における用途に送出できる。

【００８１】

［Ｃ．カード読取器］

本発明のセキュリティ証明システムはさらにカード読取器１６を含むことができ、この読取器は本発明に従ってセキュリティ・クリアランス・カード１０を読取り、カード所有者の身元を証明し、特定の場合には、カードに格納された身元データ、フィールド・データ、および追加データの少なくとも一部にアクセスできる。図５には、カード読取器の機能のいくつかを示すカード読取器１６の１つの実施形態の図を示す。カード読取器は、カードのＣＤ－ＲＯＭ部分２２に格納されたデータの少なくとも一部を読取りできるＣＤ－ＲＯＭ読取器３４を含むことができる。詳細には、ＣＤ－ＲＯＭ読取器３４は、カードのＣＤ－ＲＯＭ部分２２に格納された、カード所有者のバイオメトリック・データを読取りできる。さらに、カード読取器１６はカードのデータ記憶媒体部分２４の少なくとも一部を読取りできる読取器３６を含むことができる。したがって、読取器３６はデータ記憶媒体に格納された符号化データの少なくとも一部を復号できる。例えば、カード上に現れるデータ記憶媒体はバーコードである場合、本発明のカード読取器１６は読取器としてバーコード・スキャナを含む。

【００８２】

本発明のカード読取器１６はさらに、カード所有者のバイオメトリック・データにアクセスするための、少なくとも１つのバイオメトリック・センサ４０を含む。バイオメトリック・センサの特性は、走査に対して選択されたバイオメトリック・データの種類に依存する。例えば、１つまたは複数のバイオメトリック・センサは指紋スキャナ、網膜スキャナ、音声認識デバイスなどにできる。

【００８３】

カード読取器１６はまた、ＣＤ－ＲＯＭ読取器３４、読取器３６、バイオメトリック・センサ４０からデータを受け取る処理素子３８、および／またはカード１０および／またはカードを提示する個人からのデータを受け取ることができる任意の他の素子を含む。処理素子３８は、カードに格納されたカード所有者のバイオメトリック・データと、該当する種類のバイオメトリック・センサ４０によりカード読取器で受け取られる、カードを提示する個人のバイオメトリック・データとの比較ができる。比較結果が所定の許容差内にある２つのバイオメトリック・データ間の差である場合、カードを提示する個人は、セキュリティ・システムによりカード所有者と見なされる。許容差レベルは任意の所望値に設定できる。例えば、許容差レベルは、完全一致を除いたあらゆる結果が、カード所有者と見なされるカードを提示する個人を示すことがない値に設定できる。あるいは、許容差レ

ベルは、２つのバイオメトリック・データ間に一定量の誤差を認める値に設定できる。

【００８４】

カード１０を提示する個人がカード所有者と見なされる場合、一致インジケータ４２は、送信器４４を介してカード読取器１６の外部に置かれた該当のインジケータに一致表示を伝送する。例えば、インジケータは特定の色で点灯して一致を示すＬＥＤ（発光ダイオード）であってもよく、またはディスプレイの表示であってもよい。

【００８５】

カード読取器１６はまた、アクセス使用と試みる個人により提示されたバイオメトリック・データを記録することにより、すべてのアクセスの試み、成功および不成功の経過記録（ログ）を維持できる。記憶素子またはログ４６は、カード読取器位置にあるデータベース内に格納でき、また永久または一時的記憶素子に周期的にダウンロードするか、またはカード読取器の特定用途に依存して消去できる。したがって、カード読取器はスタンド・アロン型にでき、または図４に示すように、ＬＡＮ（ローカル・エリア・ネットワーク）、ＷＡＮ（広域ネットワーク）、イントラネットおよび／またはインターネットなどの従来または無線式の任意の方式のネットワーク３２を介して、データベースなどの少なくとも１つの遠隔記憶素子４８と通信できる。本発明の別の実施形態においては、カード読取器はアクセス試みのログをローカルにも、一時的にも格納できないが、前記のネットワークを介してデータベースなどの遠隔記憶素子４８と通信できる。したがって、アクセス試みのデータは、試みの発生時に、遠隔記憶素子４８に直接送信できる。提示されたバイオメトリック・データを含むログ・データ４６を分析して、個人に属さないセキュリティ・クリアランス・カードを利用しようとするすべての個人を識別できる。次に、必要に応じて、これら個人に対し適正なアクションが取られる。

【００８６】

カード読取器１６は、カード読取器の設置位置に応じて、有人または無人で操作できる。例えば、カード読取器の実施形態は、図４のデバイス３０、５０、５２、および５４に示すような、従来のコンピュータまたは他の種類のデバイスであってもよい。デバイスは、カード読取器１６の特定用途に依存して、据置式または移動式にできる。

【００８７】

有人式カード読取器１６に対しては、カード読取器のオペレータはカード読取器にログ・オンして、オペレータの身元を記録することを要求できる。ログ・オンするために、カード読取器の可能なオペレータは、カード読取器により格納および／またはアクセス可能である、可能なオペレータのバイオメトリック・データに一致する、少なくとも１つのバイオメトリック・データを提示することを要求される。例えば、可能なオペレータのバイオメトリック・データは、カード読取器から分離しているが、カード読取器と通信する記憶素子４８内に格納できる。カード読取器１６の別の実施形態においては、可能なオペレータのバイオメトリック・データをカード読取器に含まれる記憶素子に格納することにより、カード読取器１６はいかなる種類の遠隔素子にもアクセスする必要がない、スタンド・アロン・デバイスとなる。オペレータがカード読取器にログ・オンするたびに、オペレータは、カード読取器により格納および／またはアクセス可能であるバイオメトリック・データと比較できる、少なくとも１つのバイオメトリック・データを提示することを要求される。オペレータにより提示されたバイオメトリック・データが、カード読取器により格納および／またはアクセス可能であるバイオメトリック・データに一致すると、そのオペレータはカード読取器を操作することを許可される。オペレータにより提示されたバイオメトリック・データが、カード読取器により格納および／またはアクセス可能であるバイオメトリック・データに一致しない場合、そのオペレータはカード読取器へのアクセスを拒否され、別のバイオメトリック・データの提示、および／または特定用途および／またはカード読取器の位置に基づく任意の他の機能の提示を要求される。先に述べたように、カード読取器はシステムの試みるユーザにより走査されるバイオメトリック・データのログを格納し、後の分析およびシステムに侵入を試みる人物の決定に備えることができる。

【００８８】
前述のように、セキュリティ・クリアランス・カードはさまざまなセキュリティ・レベルのデータを含むことができる。例えば、低レベルのデータはカード所有者の名前および場合により所有者のディジタル写真を含むことができる。高レベルのセキュリティ・データは、住所、口座番号などの所有者の個人情報を含むことができる。さらに高レベルのセキュリティ・データはさらに重要な機密情報を含むことができる。従来システムの限界は、このデータのすべてが一般に、データの機密度に関係なく、カードを走査する人物によりアクセス可能である点である。しかし、本発明はこの問題点を解決する。詳細には、本発明のシステムは、カード所有者に関するデータを異なるセキュリティ・レベルに分類し、情報に関連付けされた特定のセキュリティ・レベルにアクセスする権限を有する、カード読取器および／またはカード読取器のオペレータによってだけその情報へのアクセスを許可する。

【００８９】
したがって、カード読取器の可能なオペレータのバイオメトリック・データを格納することに加えて、カード読取器の可能なオペレータまたはオペレータ・グループに関連する他のデータもカード読取器にローカルに、または任意の方式のネットワーク３などを介して通信する遠隔記憶素子に格納できる。例えば、本発明の１つの実施形態においては、カードに格納されたデータへのアクセス・レベルに関する情報、すなわち前述の身元データ、フィールド・データ、および／または追加データは、特定のカード読取器の各可能なオペレータまたはオペレータ・グループに割当てられ、またこの情報はカード読取器によりアクセスできる位置に格納できる。このように、カード読取器にログ・オンするオペレータの身元および／またはタイプに応じて、およびオペレータに割当てられるアクセス・レベルに基づいて、カード読取器はカードに格納されたデータの特定の部分だけを読取りできる。

【００９０】
例えば、空港に設置される本発明の身元証明システムの１つの実施形態においては、空港入口の警備員または複数の警備員などのカード読取器のオペレータまたはオペレータ・グループが、オペレータがカードに格納されたデータから身元データの部分（すなわち、バイオメトリック・データ、氏名、住所、生年月日、および／または発効期日および満了日）だけをみることができるアクセス・レベルを許可される。したがって、前述のように、警備員はバイオメトリック・データ比較の結果だけを見ることができ、またカード所有者に関する他の身元データの少なくとも一部を見ることができる。この実施形態においては、空港管理者または複数の管理者などの、カード読取器の別の可能なオペレータまたはオペレータ・グループには、管理者がカードに格納された身元データ、フィールド・データ、および／または追加データの別の部分を見ることができるアクセス・レベルが許可される。例えば、本発明の身元証明システムの実施形態においては、身元データは、空港／航空機安全に対して発生する可能な脅威として識別されている各個人の身元データのリストと比較できる。カードを提示する個人がこのリストに一致すると、空港管理者はカード読取器にログ・オンでき、カード読取器が空港管理者のバイオメトリック・データをカードに格納された別のデータへのアクセス許可として認識し、空港管理者を、特定の個人により引き起こされる空港／航空機に対するリスクを評価するのを支援するデータ部分にアクセス可能にできる。

【００９１】
本発明の身元証明システムの１つの実施形態においては、図５に示すように、暗号読取器５８により、各オペレータまたはオペレータ・グループを、それらがアクセスを許可されたデータの暗号化の種類だけを読取る能力に関連付けることにより、カード読取器の特定のオペレータまたはオペレータ・グループは、カードに格納されたデータ特定部分だけにアクセス可能になる。前述のように、カードに格納された身元データ、フィールド・データ、および／または追加データは、特定の種類のデータに割当てられるセキュリティ・レベルに応じてさまざまな暗号化方式を用いて暗号化できる。例えば、前述の例において

は、警備員をカードに格納された身元データまたは身元データの一部の暗号化だけを読取る能力に対応付けでき、一方、空港管理者は、カードに格納された身元データの一部または全部の暗号化だけでなく、フィールド・データおよび／または追加データの少なくとも各部分の暗号化を読取る能力に対応付けされ、それにより、空港管理者がカード所有者により引き起こされる空港／航空機に対するリスクを評価するのを支援する。

【００９２】

本発明の身元証明システムの別の実施形態においては、カード読取器の特定のオペレータは、セキュリティ・クリアランス・カード１０に格納されたデータを変更、追加および／または削除などの修正する能力を有することができる。例えば、カード１０はＣＤＲＷなどのＣＤ－ＲＯＭ２２を含み、これに身元データ、フィールド・データ、および／または追加データを格納でき、またオペレータはＣＤ－ＲＯＭに格納されたデータを読取るだけでなく、データを変更、追加および／または削除することにより、データを修正することもできる。本発明の別の実施形態においては、カードは身元データ、フィールド・データ、および／または追加データを格納するための、ＣＤＲなどのＣＤ－ＲＯＭ２２を含み、またオペレータはデータだけを読取ることができる。オペレータがＣＤＲに格納されたデータの修正を許可される場合、修正は、カードに格納された既存データのいずれも変更または削除せずに、カードに格納されたデータに追加することを含むだけである。他のデータ書込み手順も使用できることは理解されるべきである。

【００９３】

カードに格納されたデータに厳重なセキュリティを保証しない実施形態のような、本発明の別の実施形態においては、書込みデータの削除、変更または修正、さらに読込みを可能にするＣＤ－ＲＯＭを使用できる。このタイプのＣＤ－ＲＯＭは一般にＣＤＲＷと称する。

【００９４】

したがって、このようなオペレータが利用するカード読取器１６はまた、キーボード６０または他の種類の情報受入れデバイスなどのデータ入力手段、および送信機４４を介してのように、修正データをカードの適正な部分に格納する能力を有する。カードに格納されたデータを修正する能力を、特定のオペレータのバイオメトリック・データに関連付けできるが、これには、オペレータがカード読取器にログ・オンするとき、オペレータは、前述のように、可能なオペレータの格納されたバイオメトリック・データに一致する、少なくとも１つのバイオメトリック・データを提示し、カード読取器が、オペレータがカードに格納されたデータを修正する能力を有することを認識するようにする。本発明の身元証明システムの１つの実施形態においては、オペレータは、オペレータ自身のセキュリティ・クリアランス・カードの変更が許可されない、この結果、セキュリティ・クリアランス・カードの変更は、カードへの格納に先立ち第３者により確認される必要がある。さらに、本発明の身元証明システムの実施形態においては、カードに格納されたデータの修正のすべてを追跡することにより、修正の細部は後日必要とされる場合に、正確な修正がなされ、修正を実行したオペレータがカード内および／または遠隔記憶素子内で識別および格納されるようにする。データがＣＤＲに格納されるカードに関して先に述べたように、カードに格納されたデータの変更を追跡するために、修正はカードに格納された以前のデータを完全に上書きできず、その結果、変更は以前のデータの上に追加データ層を生成し、以前のデータのいずれも削除しない。したがって、以前のデータは、そのデータが必要になる場合、後日アクセスできる。

【００９５】

別のセキュリティ手順として、カード読取器はまた、セキュリティ・クリアランス・カードを検査して、カードの完全性を証明後、位置または対象への個々のアクセスを可能にし、またさまざまな用途においてカードに格納されたデータに依存できる。したがって、カードはカード読取器により証明される、厳重に保護される内部制御データを含むことができる。さらに、カード読取器は修正データを検査して、格納されたデータの修正が前述の手順に従ってなされたことを保証できる。何らかの矛盾がデータ内またはカードの内部

制御データ内に存在する場合、カード読取器は所望の位置への個人アクセスを拒否し、有人読取器に対しては、矛盾をオペレータに表示する。例えば、カード読取器がデータ内またはカードの内部制御データ内の矛盾を削除する場合、カード読取器は特定の色および／または記号を表示して、矛盾の位置および／または特性を示すことができる。このような矛盾はまた、有人または無人カード読取器を起動して、以下に詳細に説明するように、１つまたは複数のアクションを開始する。

【００９６】

一般に無人カード読取器はカードに格納されたデータから身元データの少なくとも一部を読取りすることにより、カードに格納されたバイオメトリック・データと、カードを提示する個人からのカード読取器により受け取られたバイオメトリックでとの比較に基づいて、位置または対象（有形または無形）へのアクセスを許可または拒否できる。ただし、本発明の身元証明システムの別の実施形態においては、有人および／または無人カード読取器はまた、カードに格納された身元データのすべて、フィールド・データの少なくとも一部、および／または追加データを、カード読取器の特定用途に基づいて、読取りできる。前記と同様な方法で、各カード読取器を、各カード読取器がアクセスを許可されたデータの暗号化種類だけを読取りする能力に対応付けすることにより、各カード読取器は、カードに格納された身元データ、フィールド・データ、および／または追加データの特定部分だけにアクセスできる。

【００９７】

カード読取器がアクセスできるデータの種類および／または量を変更することにより、特定のカード所有者がアクセスできるアイテムを変更できる。本発明のセキュリティ・システムの１つの実施形態においては、制御センター５６などのセンターのノードは、セキュリティ・システム内の１つまたは複数のカード読取器１６と通信できる。特定のカード所有者に許可されるアクセスの種類の変更は、センターのノードでなされ、該当するカード読取器に伝送される。例えば、カード所有者Ａには、最初に、特定組織内の全アイテムへのアクセスが許可される。アイテムの変更および／またはカード所有者Ａの状態の変更により、カード所有者Ａのアクセス許可を変更して、カード所有者Ａが組織のドア５にアクセスできないようにすることができる。カード所有者Ａのアクセス許可の変更はセンターのノードでなされ、センターのノードは該当するカード読取器、この例ではドア５に関連付けカード読取器に伝送される。ここでドア５のカード読取器はドア５へのカード所有者Ａのアクセスには応じない。同様に、アクセスできるカード読取器のオペレータ・データの量および種類も変更できる。したがって、このセキュリティ・システムはカード所有者アクセスの変更を効率的に実行でき、同時に、アクセス決定が、決定を必要とするたびに、従来のセキュリティ・システムのように、カード読取器が遠隔データベースに照会をすることを要求する代わりに、カード読取器レベルで実施されることを保証する。

【００９８】

したがって、本発明のセキュリティ・クリアランス・カード１０は、カード読取器１６と組み合わさって、セキュリティ・クリアランス・カードを提示する個人が実際のカード所有者でるかどうかを決定する、安全で、信頼性の高い効率的な方法を提供するだけでなく、カード読取器および／またはカード読取器を操作する要員が、必要なデータだけにアクセスできることを保証する。したがって、カード所有者に関連する個人的情報は非公開のままであり、個人情報へのアクセスを許可された読取器および／または要員だけがその情報へのアクセスを許可される。さらに、カード読取器および／またはカード読取器オペレータがアクセスできるデータの種類および／または量の変更は、センターのノードでなされ、該当するカード読取器に伝送されて、変更が効率的に実施されるが、アクセス決定はカード読取器レベルで連続的に実行される。

【００９９】

有人および／または無人カード読取器１６は、図１に示すモニター１８などのディスプレイ６２も備えて、オペレータおよび／またはカードを提示する個人に情報を表示する。例えば、有人または無人カード読取器１６を含む、本発明の身元証明システムの実施形態

においては、オペレータおよび／またはカードを提示する個人は、カードに格納されたバイオメトリック・データがカードを提示する個人により提出されたバイオメトリック・データと一致するかどうかを少なくとも表示するディプレイを見ることができる。この表示は、バイオメトリック・データ比較結果に基づいて、特定の色に調整されたディスプレイ・スクリーンの少なくとも一部で構成されており、例えば、バイオメトリック・データが一致するときは緑色、一致しないときは赤色となる。ディスプレイ・スクリーンによりオペレータに提供できる色の代わりまたはこれに追加して、単語、記号および／またはオブジェクトをオペレータに示し、バイオメトリック・データ比較の結果を詳しく表示できる。例えば、バイオメトリック・データが一致したときは、「ｙｅｓ」、「ＯＫ」、サムアップリンク記号などをスクリーンに表示でき、一方、バイオメトリック・データが一致しないときは、「ｎｏ」、「ストップ」、ストップ記号などをスクリーンに表示できる。有人および／または無人カード読取器１６を含む、本発明の身元証明システムの実施形態においては、身元データの少なくとも一部、すなわち、カード所有者のバイオメトリック・データ、名前、住所、および／または生年月日、および／またはカードの発効期日および満了日を、カード読取器が身元データを読取るときに表示できる。セキュリティ／プライバシーの理由のために、無人および／または有人カード読取器１６は表示する身元データの量を限定できる。有人カード読取器にログ・オンしたオペレータが、カードに格納されたフィールド・データおよび／または追加データの少なくとも一部を読取りできるとき、そのデータはディスプレイ６２によりオペレータにも表示できる。

【０１００】

バイオメトリック・データ比較の結果に応じて、カード読取器は特定のアクションを開始できる。本発明の身元証明システムの１つの実施形態においては、有人および／または無人カード読取器１６は、バイオメトリック・データが一致しない場合、および／またはカードに格納された身元データが、特定の理由から識別された個人に関連する身元データに一致する場合、データアクション・イニシエータ６４により可聴または無音アラームなどのアクションを開始できる。例えば、カード読取器は、個人に関連する特定の問題または他の何らかの理由により、識別された個人に関連する身元データを格納またはアクセスできる。次に、バイオメトリック・データ比較の前または後のどちらかであるが、カードを提示する個人に所望の位置または対象にアクセスすることを許可する前で、かつカードに格納されたデータに依存する前に、カード読取器はカードに格納された身元データを、カード読取器内に格納された身元データと比較できる。したがって、無音または可聴アラームは、カード読取器のオペレータに、カード読取器の利用および／または位置に基づいて、カードを提示する個人をさらに調査すべきことを示す。本発明の身元証明システムの別の実施形態においては、バイオメトリック・データが一致しない場合、および／または特定の理由から識別された個人に関連する身元データにカードに格納された身元データが一致する場合には、カード読取器がアクション・イニシエータ６４により、例えば管理者および／または警察官の即座に連絡するなどの（すなわち、下流における用途（downstream application））、他のアクションを開始できる。この種類のアクションは、前述のアラーム・アクションおよび／または他の種類のアクションと共にまたはこれと別に開始できる。

【０１０１】

カード読取器はまた、カード読取器、個人のセキュリティ・クリアランス・カード、および／またはカード読取器がアクセスできる別の位置に格納された命令を読取りできる。この命令は、バイオメトリック・データ比較結果、身元データ分析、および／またはカードを提示する個人により提出された情報に基づいて開始するアクションの種類を含む。例えば、カード読取器は、カード所有者が提示するバイオメトリック・データのタイプに基づいて、読取器に異なるアクションを開始するように指示する命令を読取りできる。例えば、本発明の身元証明システムの１つの実施形態においては、カード読取器に通常動作を実行する命令を与えることができる。すなわち、カードを提示する個人が右手の人差し指の指紋をカード読取器に提出するとき、バイオメトリック・データ比較に基づいてカード

を提示する個人へのアクセスを許可または拒否する。ただし、個人が別の指からの指紋を提出する場合、カード読取器は、管理者および／または警察官などの、その状況に対処できる要員または組織に即座に通知するように命令を受ける。カード読取器１６の実施形態のこの機能は、カード読取器１６が高価な、機密度の高いデータおよび／または位置にアクセスできる状況において有利である。例えば、カード読取器１６が銀行口座へのカード所有者アクセスを許可する状況においては、カード所有者は通常状況では右手の人差し指の指紋を提出できるが、カード所有者が危険な場合、例えば別の人物がカード所有者に銀行口座へのアクセスを強制して、その別の人物が口座へのアクセスを得ようとする場合、カード所有者は別の指の指紋を提出でき、それにより、カード読取器を起動して、即座に警察官、すなわち下流における用途に連絡する。

【０１０２】

図６に示すように、本発明によるあらゆる所定のセキュリティ・システムも、特定のカード読取器、特定のカード読取器オペレータ、特定のカード所有者、および／または特定の下流における用途が、カード１０に格納されたデータの特定レベルおよび／またはサブレベルにアクセスタできる、ように構成できる。図６は、各カードが少なくとも１０レベルの格納データを有し、各レベルがレベル１および７に示すような複数のサブレベルを有する、セキュリティ・システムを示す。セキュリティ・システムのカードに格納されたデータの可能なユーザまたはサブクラスのユーザが、チャートの上部に記載されている。例えば、図６のセキュリティ・システムのカードに格納されたデータの可能なユーザとして、カード読取器の３つのサブクラス（ＣＲ１、ＣＲ２、ＣＲ３）、カード読取器のオペレータの３つのサブクラス（ＯＰ１、ＯＰ２、ＯＰ３）、カード所有者の３つのサブクラス（ＣＯ１、ＣＯ２、ＣＯ３）、下流における用途の３つのサブクラス（ＡＰ１、ＡＰ２、ＡＰ３）がある。本発明のセキュリティ・システムの別の実施形態は、存在する場合、異なる量のレベル、サブレベル、および／またはユーザのサブクラスを含む。別の実施形態では、ユーザのクラスはサブクラスに分割できないが、代わりに、各ユーザは個々にリストアップできる。

【０１０３】

ユーザの可能なサブクラスの直ぐ下のボックス内の「Ｘ」は、そのサブクラスが、Ｘが配置された行に関連するデータのレベルおよび／またはサブレベルと解釈できることを示す。例えば、図６に示すように、ＣＲ１はカード１０のレベル１～４に格納されるすべてのデータと解釈でき、一方、ＯＰ３はレベル８だけに格納されるデータと解釈できる。したがって、特定のレベルおよび／またはサブレベルの特定種類のデータだけを格納し、ユーザのどの可能なサブクラスが、どのレベルおよび／またはサブレベルと解釈できるかを効果的に割り当てることにより、本発明のセキュリティ・システムは、従来のセキュリティ・システムが実現できない、柔軟な、効率的なデータ保護を実現する。さらに、本発明のセキュリティ・システムは遠隔データベースまたはいずれかのタイプの記憶素子にアクセスすることなく、機能することが可能であるが、カードに格納されたデータを、遠隔にあってもよい、セキュリティ・システムの下流における用途などの他のユーザに伝送することもできる。例えば、図６に示すように、ＣＲ１はカードのレベル１０に格納されたデータを読取ることはできないが、ＣＲ１はレベル１０からＡＰ２にデータを伝送でき、そこでレベル１０データを読取りできる。

【０１０４】

さらに、本発明のセキュリティ・システムは、カードに格納されたデータの特定レベルおよび／またはサブレベルへの条件付アクセスを可能にする。例えば、オペレータまたはカード所有者を、１つまたは複数のデータ・レベルおよび／またはサブレベルの所有者として割当てできる。前述のように、バイオメトリック・データの一致により、最初にカード読取器がカードを走査し、オペレータおよび／またはカード所有者に身元証明を実行した後、カード読取器はデータのあるレベルおよび／またはサブレベルの所有者に、データのアクセスを許可または拒否するように促す。本発明のセキュリティ・システムの１つの実施形態においては、所有者に、所有者の許可を示す別のバイオメトリック・サンプルを

提出するように促すことができる。例えば、図６の例では、ＣＯ３は、別のユーザまたはユーザのサブクラスがカード所有者の社会保障番号を読取りできるかどうかを、ケースバイケースで、それらが許可できることを要求したカード所有者のサブクラスにできる。レベル９がカード所有者の社会保障番号を含むと仮定すると、ＯＰ２サブクラスのオペレータおよび／またはＡＰ２サブクラスの下流における用途のレベル９のデータへのアクセスを許可する前に、ＣＯ３サブクラスのカード所有者を許可する必要がある。

【０１０５】

したがって、カード読取器１６は、セキュリティ・システムのあらゆる可能なユーザが該当する種類のデータだけを読取り、観察および／またはアクセスすることを保証する。さらに、処理素子を含むカード読取器への命令をカード読取器内に置くことにより、カード読取器が命令またはデータについて遠隔デバイスにアクセスする必要がなくなる。さらに、カード読取器は、カード読取器に提出されたバイオメトリック・データを格納することにより、セキュリティ・クリアランス・カードを利用する試行の経過を記録でき、それにより、カードを利用しようとするあらゆる不正な試みを、格納されたバイオメトリック・データの分析により、容易に識別できる。このように、カード読取器は、本発明のセキュリティ・クリアランス・カードと組み合わさって、個人の身元を証明するだけでなく、許可された人物だけがカード所有者のデータを観察および／またはアクセスできることを保証する、安全で、柔軟性のある、低コスト方法を提供する。

【０１０６】

［Ｄ．用途例］

本発明の身元証明システムの特定の有利な実施形態を以下に説明する。身元証明システムの可能な用途は広範囲にわたり、これら特定の実施形態は例示目的だけに示すものである。例えば、身元証明システムは、少し名前を挙げるだけでも、海港、空港、外国人登録（学生および労働者の両方）、官庁および民間ビル、発電所、水力発電所、および刑務者で利用できる。これら実施形態の説明においては、上で説明した本発明の、セキュリティ・クリアランス・カードを含む身元証明システムの詳細が組み込まれる。

【０１０７】

本発明の身元証明システムの実施形態は、従業員または他の個人が「制限領域」にアクセスする前に背景検査を受けなければならないあらゆる用途に利用できる。このような状況においては、背景検査を実行後に、適正な該当手順が実行され終わると、従業員または他の個人には、本発明によるセキュリティ・クリアランス・カードが発行される。したがって、セキュリティ・クリアランス・カードがカード所有者のバイオメトリック・データを格納し、かつカードを提示する個人が、制限領域にアクセスする前に、一致するバイオメトリック・データを提供する必要があるため、適正な手順に従う背景検査の合格しない個人が制限領域にアクセスできるリスクはほとんど発生しない。この種類の用途は、海港、発電所、水力発電所、官庁および民間ビル、刑務者、および選択されたグループの人物だけがアクセスできる特定領域および／またはアイテムを含む他の場所で利用できる。

【０１０８】

別の実施形態においては、個人に対し、制限領域を出るときに、セキュリティ・クリアランス・カードを用いてカード読取器により検査することを要求できる。この実施形態では、身元証明システムは、特定個人が特定領域にアクセスする時間量および／または回数を追跡できる。この種類のデータは、会計用途、および／または個人が放射線に曝露される時間量の制限のような、特定領域に滞在する時間の制限を強制する用途などの、さまざまな他の下流における用途に利用できる。後者の例では、個人が制限値に達すると、カード読取器は、個人のバイオメトリック・データがカードに格納されたバイオメトリック・データに一致していても、個人が制限領域にそれ以上アクセスするのを認めない。個人が再度放射線に曝露されると、カード読取器は再度個人が制限領域にアクセス可能にする。さらに、特定の用途においては、少なくとも所定の時間期間、個人を特定領域にアクセス可能にするが、その領域から出ないようにすることが望ましい。したがって、本発明のセキュリティ・システムにおいては、この用途も具体化できる。

【０１０９】
本発明の身元証明システムの別の実施形態においては、セキュリティ・クリアランス・カードを、個人の代わりに、有形または無形の対象に関連付けできる。例えば、セキュリティ・クリアランス・カードは出荷に関連付けして、カードが出荷に関するデータ、例えば中身、出荷主、宛先、所有者、および出荷に関する他のデータなどを格納するようにできる。さらにカードは、出荷に責任を有する個人の身元データを格納することにより、個人のバイオメトリック・データをカードに格納し、個人が一致するバイオメトリック・データを提出して、出荷の有効性を保証するようにする。
【０１１０】
本発明の身元証明システムはまた、有権者証明および登録に使用できる。例えば、個人の有権者登録をカードに格納でき、また投票場所はカード読取器を有することができる。したがって、選挙作業担当者は、セキュリティ・クリアランス・カードに格納されたデータの有権者登録部分だけを読取る能力を有する、カード読取器のオペレータとしてみなすことができる。したがって、個人は自分のカードを選挙作業担当者に提示でき、この担当者は、カード読取器を操作して、カードに格納されたバイオメトリック・データと、個人により提出された少なくとも１つのバイオメトリック・データとを比較する。バイオメトリック・データが一致し、個人の有権者登録情報が証明されると、その個人はその場所での投票を許可される。したがって、本発明の身元証明システムは、投票する人物が投票を登録された人物であることを保証することにより、有権者の不正のリスクを大幅に低減する。
【０１１１】
本発明の身元証明システムの実施形態はまた、外国人（学生および労働者の両方）の登録および追跡にも利用できる。この用途においては、本発明のセキュリティ・クリアランス・カードは各外国人に発行でき、カードは少なくとも１つの格納されたバイオメトリック・データを含む、特定の外国人に関する身元データを含む。外国人には一定期間ごとに該当の公的機関に報告することを要求することにより、政府が外国人の状態に関する情報（外国人が学校に入学しおよび／またはその国で働き続けることを保証するなどの）を得ることができる。外国人が該当官庁に報告し、カードを提出すると、官庁の職員はカード読取器を操作して、カードに格納された身元データの少なくとも一部を読取り、個人より提示された少なくとも１つのバイオメトリック・データがカードに格納されたバイオメトリック・データに一致することを証明できる。次に、職員は外国人の活動を基にして彼らの状態を決定する。外国人の報告のログを作成して、外国人が彼らの義務を順守していることを文書化する。外国人が報告を提出しない場合、または外国人の状態が変化した場合、本発明の身元証明システムは、その情報を該当の職員に自動的に報告することにより、職員が適正なアクションを取れるようにすることができる。この実施形態においては、カード読取器は中央制御装置および／または外国人情報を管理する下流における用途と組み合わせることにより、カード読取器が外国人に関するデータを適正な場所に自動的に伝送するようにできる。
【０１１２】
前述のさまざまな例および全体の説明に述べたように、本発明のセキュリティ・クリアランス・カードおよび身元証明システムは、さまざまな可能な用途に利用できる。セキュリティ・クリアランス・カードは、カード読取器と組み合わせて、遠隔データベースにアクセスすることを必要とせずに、個人の身元を証明できるだけでなく、システムはカード読取器のオペレータが、彼らが許可を得ている、カードに格納されたデータの一部のみを観察および／またはアクセスできる。さらに本発明は、個人がカードを利用することを試みるときに提出するバイオメトリック・データのログを取ることにより、カードの用途を追跡し、カードの不正使用を容易に捕獲し、責任を持つ人物を識別できる。したがって、本発明のセキュリティ・クリアランス・カードおよび身元証明システムは、該当する個人が特定の位置、情報、対象、および／または保護を望む他のアイテムにだけアクセスできることを保障する、効率的で、安全かつ正確な方法を提供する。

【０１１３】
当業者には、本明細書で述べる、前述の説明および関連図面に提示された内容の利益を有する本発明の多くの変形形態および他の実施形態は、容易に明らかになるであろう。したがって、本発明はここで開示した特定の実施形態に限定されず、それの変形形態および他の実施形態も、添付の特許請求の範囲に含まれるものとする。本明細書では特定の用語を用いたが、これらは一般的および説明的意味で用いただけであり、限定を目的とするものではない。

【図面の簡単な説明】

【０１１４】
【図１】本発明の１つの実施形態によるセキュリティ・システムの用途を示す図である。
【図２】本発明の１つの実施形態によるセキュリティ・クリアランス・カードのＣＤ－ＲＯＭ部分の平面図である。
【図３】本発明の１つの実施形態によるセキュリティ・クリアランス・カードの表面上の置かれたデータ格納媒体の平面図である。
【図４】本発明の１つの実施形態による、制御センターおよび／または遠隔記憶素子と通信可能な複数のカード読取器の図である。
【図５】本発明の１つの実施形態によるカード読取器の機能を示す図である。
【図６】本発明の１つの実施形態による、セキュリティ・クリアランス・カードに格納されるデータのレベル、データのユーザの可能なクラスおよびサブクラスを示すチャートであり、このサブクラスはデータのそのレベルにアクセスすることを許可される。

【図１】

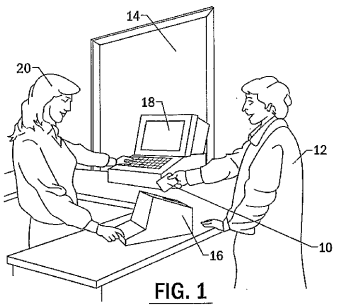


FIG. 1

【図３】

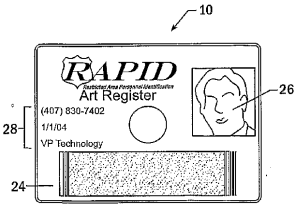


FIG. 3

【図２】

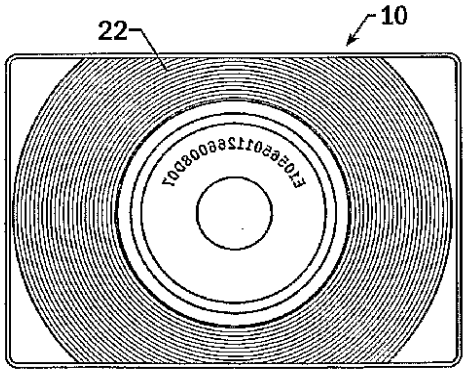


FIG. 2

【図４】

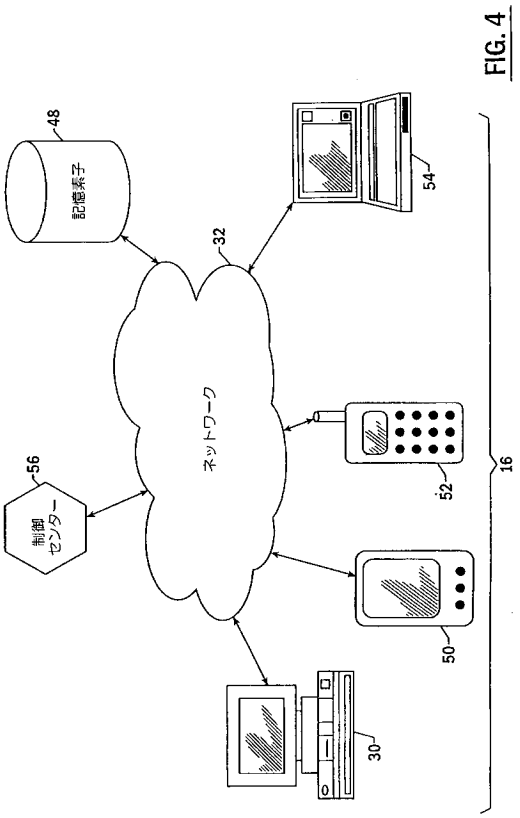


FIG. 4

【図５】

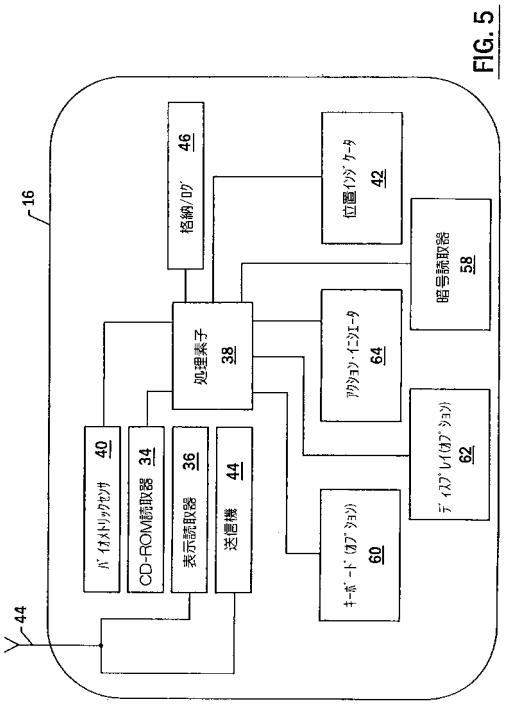


FIG. 5

【図６】

データ		ユーザ															
レベル	サブレベル	クラス	カード読取器			オペレータ			カード所有者			下流における用途		
		サブクラス	CR1	CR2	CR3	OP1	OP2	OP3	CO1	CO2	CO3	AP1	AP2	AP3
1	1		X			X	X		X		X	X	X	
	2		X			X	X		X	X	X	X	X	
2	3		X				X		X		X	X		X
	4		X		X				X				X	
3	5		X		X	X				X				
4	6				X	X				X				
5	7				X		X		X		X			X
6	8				X	X	X			X	X		X	X
7	9				X	X	X			X	X		X	X
8	10				X			X	X				X	X
9	11						X				X	X		X
10	12													

FIG. 6

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/US 02/41123

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06K19/04 G06K19/06

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)
IPC 7 G06K

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	FR 2 805 911 A (EUDELINE PATRICK) 7 September 2001 (2001-09-07) the whole document	1-4, 7-20, 25-42
A	WO 01 63611 A (CHIP ON MEDIA INC ;OGURI TETSUYA (JP); KUROSE TADAYUKI (JP); YAMAD) 30 August 2001 (2001-08-30) abstract; figure 2	1-42
A	EP 0 918 301 A (ORGA CONSULT GMBH) 26 May 1999 (1999-05-26) the whole document	1-24
A	EP 0 956 818 A (CITICORP DEV CENTER) 17 November 1999 (1999-11-17) the whole document	25-42

☐ Further documents are listed in the continuation of box C. ☒ Patent family members are listed in 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 document 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	Date of mailing of the international search report
22 April 2003	29/04/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Degraeve, A

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 02/41123

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FR 2805911 A	07-09-2001	FR 2805911 A1	07-09-2001
WO 0163611 A	30-08-2001	AU 6592300 A	03-09-2001
		WO 0163611 A1	30-08-2001
EP 0918301 A	26-05-1999	DE 19751868 C1	08-07-1999
		EP 0918301 A2	26-05-1999
EP 0956818 A	17-11-1999	EP 0956818 A1	17-11-1999
		US 2001048025 A1	06-12-2001

フロントページの続き

(51)Int.Cl.[7]	FI		テーマコード（参考）
Ｇ１１Ｂ 20/12	Ｇ１１Ｂ 20/12		
Ｈ０４Ｌ 9/32	Ｇ０６Ｋ 19/00	Ｓ	
	Ｇ０６Ｋ 19/00	Ｆ	
	Ｈ０４Ｌ 9/00	６７３Ｄ	
	Ｈ０４Ｌ 9/00	６７３Ｅ	

(31)優先権主張番号 10/272,464
(32)優先日 平成14年10月16日(2002.10.16)
(33)優先権主張国 米国(US)

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NO,NZ,OM,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VN,YU,ZA,ZM,ZW

（特許庁注：以下のものは登録商標）
ＵＮＩＸ
ＷＩＮＤＯＷＳ

(72)発明者 レジスター，アーサー・フレデリック，ジュニア
アメリカ合衆国フロリダ州３２７０１，アルタモンテ・スプリングス，シャディ・コート ６９４
(72)発明者 キャンパー，フランク・ジェイ
アメリカ合衆国アリゾナ州３５０２３，ヒューイタウン，オールド・ウォリアー・リヴァー・ロード ９１５

Ｆターム(参考) 5B035 AA14 BB01 BB03 BB11 BC01
5B058 CA40 KA02 KA31 KA37 KA38
5D029 TA02 TA21 TA23
5D044 BC03 CC04 CC08 DE50 GK17
5J104 AA07 AA16 EA03 EA22 KA01 KA04 KA16 NA05 NA35 NA38
NA41 PA14