(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7026701号
(P7026701)

(45)発行日　令和4年2月28日(2022.2.28)

(24)登録日　令和4年2月17日(2022.2.17)

(51)国際特許分類

		FI		
G06F 21/31 (2013.01)		G06F	21/31	360
G06K 19/07 (2006.01)		G06K	19/07	180
G06K 19/073 (2006.01)		G06K	19/073	054
G06K 19/08 (2006.01)		G06K	19/08	060
G06F 21/32 (2013.01)		G06F	21/32	

請求項の数　17　（全16頁）　最終頁に続く

(21)出願番号　特願2019-566318(P2019-566318)
(86)(22)出願日　平成29年9月1日(2017.9.1)
(65)公表番号　特表2020-528591(P2020-528591A)
(43)公表日　令和2年9月24日(2020.9.24)
(86)国際出願番号　PCT/EP2017/071972
(87)国際公開番号　WO2018/219481
(87)国際公開日　平成30年12月6日(2018.12.6)
審査請求日　令和2年7月15日(2020.7.15)
(31)優先権主張番号　1709738.7
(32)優先日　平成29年6月19日(2017.6.19)
(33)優先権主張国・地域又は機関
英国(GB)

(73)特許権者　517124778
ズワイプ アクティーゼルスカブ
ノルウェー王国 ０１５１ オスロ ロードゥースガータ ２４
(74)代理人　110000556
特許業務法人 有古特許事務所
(72)発明者　ドレイファス， ヘンリー ナーダス
アメリカ合衆国 ３２７７１ フロリダ サンフォード レイク マークハム プリザーブ トレイル １８９９
審査官　宮司 卓佳

最終頁に続く

(54)【発明の名称】　スマートカードおよびスマートカードの制御方法

(57)【特許請求の範囲】
【請求項１】
スマートカードの動作を制御するためのプロセッサと、
認証ユーザを識別するための生体認証センサと
を備えるスマートカードであって、
前記プロセッサが、
（ｉ）スマートカードの物理的に複製不可能な特性に基づくスマートカードの身元の確認と、
（ｉｉ）生体認証センサによるユーザの身元の認証と
の両方を必要とする多要素認証プロセスに基づいて、スマートカードの１以上の安全機構へのアクセスを許可するように構成され、
前記多要素認証プロセスが、前記物理的に複製不可能な特性および生体認証に適用される重み付けを含む、スマートカード。
【請求項２】
前記物理的に複製不可能な特性が、登録プロセス中に前記スマートカードにより記録される、請求項１に記載のスマートカード。
【請求項３】
前記物理的に複製不可能な特性を表すデータを保存するためのメモリを備え、スマートカードが、物理的に複製不可能な特性に対して元々記録されたデータを提供したものと同じスマートカードであることを確認するために、プロセッサが、物理的に複製不可能な特性

の保存データを、同じ物理的に複製不可能な特性を表すと称する新たに取得されたデータと比較するように構成される、請求項１または２に記載のスマートカード。
【請求項４】
前記スマートカードの前記物理的に複製不可能な特性が、前記スマートカードの物理的エンティティに基づいて測定できる特性である、請求項１、２または３に記載のスマートカード。
【請求項５】
前記物理的に複製不可能な特性が、外部刺激または内部刺激に対するスマートカードの物理的反応の形をとる、請求項１から４のいずれか一項に記載のスマートカード。
【請求項６】
前記物理的に複製不可能な特性が、入力信号に対する電気部品の反応として定義できる機能など、前記スマートカードの電気部品の物理的に複製不可能な特性である、請求項１から５のいずれか一項に記載のスマートカード。
【請求項７】
電気部品の前記物理的に複製不可能な特性が、半導体デバイスの物理的に複製不可能な特性および生体認証センサの物理的に複製不可能な特性の少なくとも１つを含む、請求項６に記載のスマートカード。
【請求項８】
前記物理的に複製不可能な特性が、前記スマートカード上の加速度計を介して測定される前記スマートカードの振動パターンに基づく、請求項１から５のいずれか一項に記載のスマートカード。
【請求項９】
前記多要素認証プロセスが、複数の異なる物理的に複製不可能な特性の組み合わせに基づく前記スマートカードの身元確認を含む、請求項１から８のいずれか一項に記載のスマートカード。
【請求項１０】
前記多要素認証プロセスが、前記スマートカードの身元の確認および／またはユーザの身元の認証のための精度閾値を含む、請求項１から９のいずれか一項に記載のスマートカード。
【請求項１１】
前記プロセッサが、前記センサからの生体認証データおよび／または物理的に複製不可能な特性に関する経時的な変化を説明するために、経時的に多要素認証プロセスを適応させるように構成される、請求項１から１０のいずれか一項に記載のスマートカード。
【請求項１２】
前記多要素認証プロセスが、設定回数の直近の認証、例えば少なくとも１０、少なくとも２０または少なくとも５０の最近の認証のすべてのデータを記録することにより、生体認証および／または物理的に複製不可能な特性を経時的に監視することを含む、請求項１から１１のいずれか一項に記載のスマートカード。
【請求項１３】
前記プロセッサが、過去の認証のために記録されたデータを使用して、経時的な変化を識別したり前記多要素認証プロセスの受入基準を更新したりするように構成される、請求項１２に記載のスマートカード。
【請求項１４】
前記プロセッサが、過去の認証から記録されたデータを使用して、前記生体認証センサからのデータおよび／または以前の認証から記録されたデータと同一である物理的に複製不可能な特性を確認し、前記生体認証センサからのデータおよび／または前記物理的に複製不可能な特性からのデータの一方または両方が以前の認証からのデータと同一である場合、認証の試みを拒否することにより、前記スマートカードの潜在的な不正使用を検出するように構成される、請求項１２または１３に記載のスマートカード。
【請求項１５】

スマートカードを制御する方法であって、前記スマートカードが、前記スマートカードの動作を制御するためのプロセッサと、認証ユーザを識別するための生体認証センサを備え、前記方法が、多要素認証プロセスに基づいて、前記スマートカードの動作を制御して前記スマートカードの１以上の安全機構へのアクセスを許可することを含み、
前記多要素認証プロセスが、
（ｉ）前記スマートカードの物理的に複製不可能な特性に基づく前記スマートカードの身元の確認と、
（ｉｉ）前記生体認証センサによるユーザの身元の認証と
の両方を必要とし、
前記多要素認証プロセスが、前記物理的に複製不可能な特性および生体認証に適用される重み付けを含む、方法。
【請求項１６】
請求項１から１４のいずれか一項に記載のスマートカードを使用することを含む、請求項１５に記載の方法。
【請求項１７】
請求項１から１４のいずれか一項に記載のスマートカード内のプロセッサ上で実行されると、前記プロセッサに前記スマートカードの動作を制御させて、多要素認証プロセスに基づいて前記スマートカードの１以上の安全機構へのアクセスを許可する命令を含むコンピュータプログラムであって、
前記多要素認証プロセスが、（ｉ）前記スマートカードの物理的に複製不可能な特性に基づく前記スマートカードの身元の確認と、（ｉｉ）前記生体認証センサによるユーザの身元の認証との両方を必要とし、
前記多要素認証プロセスが、前記物理的に複製不可能な特性および生体認証に適用される重み付けを含む、コンピュータプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、１以上の安全機構を有するスマートカード、このようなスマートカードを制御するための方法およびコンピュータプログラム製品、ならびにこのようなスマートカードの製造方法に関する。
【背景技術】
【０００２】
スマートカードは、ますます広く使用されるようになり、例えばアクセスカード、クレジットカード、デビットカード、支払カード、ポイントカード、ＩＤカードなどを含む。スマートカードは、ＲＦＩＤなどの非接触技術を介して、データを保存したり、ユーザや外部デバイスと通信したりできる電子カードである。これらのカードは、アクセスを可能にしたり、取引を認証したりするために、リーダと通信して情報を伝達できる。
【０００３】
指紋認証などの生体認証は、ますます広く使用されている。生体認証を伴うスマートカードは、スマートカードの安全機構へのアクセスを可能にしたり、例えば金融取引を認証したりするために、センサを介してユーザと通信する。
【０００４】
スマートカードのサイズ、使用可能な電源、および必要な機能からの制約に関して、生体認証されたスマートカードで課題が生ずる。
【０００５】
スマートカードのサイズは、支払カードとして使用可能なスマートカードの場合、クレジットカードについてのＩＳＯ規格により制限される場合がある。したがって、すべての部品は、理想的にはフレキシブルで軽量であるだけでなく、しっかりとパッケージ化された形態に収まる必要がある。
【０００６】

使用可能な電力は、スマートカードのサイズと選択される電源により制限される。「チップとピン」タイプのカードの接点との接続を介して引かれる電力など、外部電源への有線接続を含めることができる。しかし、このアプローチを介して引かれる電流に関して、スマートカード自体での大電力の処理の困難さだけでなく外部電源からの技術的な制約があり得る。無線接続は、スマートカードのアンテナと、スマートカードリーダのアンテナなどの外部アンテナとの非接触接続を用いて電力を収集しながら使用できる。これの可能な実施は、国際公開第２０１６／０５５６６３号および国際公開第２０１７／０２５４８１号に記載されている。このように取得できる電力量には制限があることが理解されよう。

【先行技術文献】

【特許文献】

【０００７】

【文献】国際公開第２０１６／０５５６６３号
国際公開第２０１７／０２５４８１号

【発明の概要】

【発明が解決しようとする課題】

【０００８】

使用可能な電力量は、スマートカードのプロセッサの潜在的なクロック速度にも影響を与える可能性があり、プロセッサのサイズも制約する可能性がある。これにより、スマートカードの必要な機能に起因する制約の一部へのリンクが作成される。例えば、スマートカードは、電力使用量に一定の制限だけでなく、生体認証プロセスを完了するために使用された必要な最大時間でも生体認証確認を実行できるという要件がある場合がある。十分なクロック速度がない場合および／または認証プロセスが複雑すぎる計算を必要とする場合、必要なパフォーマンスのあるスマートカードを提供できない場合がある。スマートカードの機能に対する追加の制約には、必要なセキュリティレベルが含まれる場合がある。先行技術では、これは、スマートカード上のプロセッサ間で転送される、および／またはスマートカードとの間で転送されるデータの暗号化を使用することを伴い得る。暗号化により、カードの処理能力に対するさらなる要求が生ずる可能性がある。

【課題を解決するための手段】

【０００９】

第１の態様から見ると、本発明は、スマートカードの動作を制御するためのプロセッサと認証ユーザを識別するための生体認証センサとを備えるスマートカードであって、プロセッサが、（ｉ）スマートカードの物理的に複製不可能な特性に基づくスマートカードの身元の確認と（ｉｉ）生体認証センサによるユーザの身元の認証との両方を必要とする多要素認証プロセスに基づいて、スマートカードの１以上の安全機構へのアクセスを許可するように構成される、スマートカードを提供する。

【００１０】

このスマートカードは、ユーザの身元の生体認証確認に加えてスマートカードの物理的に複製不可能な特性を使用してスマートカードの身元を確認することにより、効率の問題におけるセキュリティの追加レイヤーを提供する。このようなシステムは、生体認証のみを使用する先行技術のデバイスと比較して、より高いセキュリティレベルを可能にする。代替的に、生体認証プロセスの複雑さを軽減しながら、同様のセキュリティレベルを提供できる。後者は、スマートカードの身元を確認する機能により、セキュリティの向上が知覚され得るために生ずる。これにより、生体認証受入閾値がそれに応じて低下することが可能になるかもしれない。

【００１１】

カードの安全機構としては、例えば、銀行カードの取引の認証、カードに保存されたデータへのアクセス、アクセスカードなどによるセキュアエリアへの立入が挙げられてもよい。本明細書に記載の多層認証プロセスは、生体認証もスマートカードの物理的特性に基づく認証もハッキングするために複数の不正行為が必要になるため、安全機構をより安全に保護するであろう。スマートカード自体もスマートカードのユーザもその身元を確認され

る。ある複製攻撃方法は、生体認証を破壊するかもしれないが、物理的スマートカードは同じことにならないため、スマートカードの物理的に複製不可能な特性の確認に対応できない。プロセッサは、物理的に複製不可能な特性を変更する方法でスマートカードが改ざんされた場合、認証の際の不正な試みを拒否することができてもよい。一方、スマートカードが盗まれて、不正ユーザが、スマートカードを所有しているため、物理的に複製不可能な特性の確認に対応することができる場合、不正ユーザは必要な生体認証の一致を提供できないため、プロセッサは安全機構へのアクセスを許可しないことになる。スマートカードは、ユーザの生体認証ＩＤもスマートカードの物理的ＩＤも同時に検証するように構成されてもよい。有利なことに、これは、小さな非常に低電力環境内で高確度に行うことができる。

【００１２】

物理的に複製不可能な特性は、登録プロセス中にスマートカードにより記録されてもよい。例えば、これは、連続して、または認証ユーザの生体認証データの登録と同時に行われてもよい。物理的に複製不可能な特性を表すデータは、スマートカードのメモリに保存されてもよい。以下のように、同じメモリを使用して生体認証データを保存してもよい。次いで、プロセッサは、後で、スマートカードが、物理的に複製不可能な特性の元々記録されたデータを提供したのと同じスマートカードであることを確認するために、物理的に複製不可能な特性の保存データを、同じ物理的に複製不可能な特性を表すと称する新たに取得されたデータと比較できる。

【００１３】

スマートカードの物理的に複製不可能な特性は、スマートカードの物理的エンティティに基づいてプロセッサにより測定できる特徴であってもよい。これには、センサの出力の測定やスマートカードの電気的機能の測定など、物理的パラメータに基づいて電気信号の測定を伴ってもよい。スマートカードの物理的に複製不可能な特性は、物理的に複製不可能な機能として説明できる。これは、物理的構造に具体化された特徴であってもよく、評価は容易であるが、予測が難しく、複製することは不可能であり得る。このような物理的に複製不可能な特性は、スマートカードに固有の特性であるため、多要素認証を提供する非常に効率的な方法である。既存のハードウェアは物理的に複製不可能な特性のために使用できるため、既存のスマートカード設計では、この多要素認証を利用するためにソフトウェアに対する変更のみを必要とする場合がある。

【００１４】

物理的に複製不可能な特性は、外部刺激または内部刺激に対するスマートカードの物理的反応の形をとってもよい。それは、別の部品から送信される信号などの入力に対する電気部品の反応として定義できる機能など、スマートカードの電気部品の物理的特性であってもよい。

【００１５】

一例では、物理的に複製不可能な特性は、スマートカードの加速度計によるスマートカードの振動パターンの測定など、外部影響に対するスマートカードの動的物理的反応であってもよい。振動パターンは、外部の加速度、力、または衝撃を受けているスマートカードの結果であってもよい。さらに以下に記載のように、量産スマートカードと量産加速度計を用いても、スマートカードの振動パターンに固有の特性がある可能性がある。さらに、以下により詳細に記載のように、振動パターンの特性の変化を増加させるために、製造中にオプションで変更してもよい。

【００１６】

別の例では、物理的に複製不可能な特性は、半導体部品の物理的に複製不可能な特性など、電気部品の複製不可能な特性の測定値であってもよい。半導体部品には微小な微視的なばらつきがあり、複製できない容易に測定可能な複製不可能な特性をもたらす。プロセッサは、スマートカード上の任意のこのような部品の物理的に複製不可能な特性、例えば、それ自体の物理的に複製不可能な特性、または切り替え目的のために使用される半導体デバイスまたは別のプロセッサ内の半導体デバイスなどの別の半導体デバイスの物理的に複

製不可能な特性を使用してもよい。例えば、プロセッサ内の半導体デバイスに基づいて物理的に複製不可能な特性を提供できる専用の生体認証プロセッサがあってもよい。別の可能性は、生体認証センサの複製不可能な特性を使用することである。生体認証センサの製造により、物理的特性にばらつきが生じ、センサからの読み取り値に影響するであろう。指紋エリアセンサとしては、個々のピクセルの反応のばらつきが挙げられ、これを使用して物理的に複製不可能な特性を提供できる。例えば、指が存在しないセンサから読み取り値を取得するか、センサを均一なターゲットに提示するなど、既知の刺激に対するセンサの反応を測定することにより、センサの物理的に複製不可能な特性を取得してもよい。スマートカードを作成するために使用される部品に応じて、容易に測定可能な物理的に複製不可能な特性を取得するための種々の方法があってもよいことが理解されよう。

【００１７】

複数の電気部品に関する物理的に複製不可能な特性など、異なる物理的に複製不可能な特性の組合せを使用してもよい。これは、スマートカードの異なる物理的に複製不可能な特性に対する特定の確認を組み込んだ多要素認証を可能にすることができ、物理的に複製不可能な特性が１つだけある２要素認証よりも高いセキュリティを提供できる。例えば、生体認証データに使用されるメモリ、１以上のプロセッサなど、いくつかの異なる部品に関して、置換または改ざんがないことを保証することが有益な場合がある。

【００１８】

多要素認証プロセスには、物理的に複製不可能な特性と生体認証に適用される重み付けが含まれる。スマートカードの身元の確認および／またはユーザの身元の確認のための精度閾値があってもよい。重み付けと精度閾値を調整して、必要なセキュリティレベルを提供してもよく、またはユーザの身元を確認するための「最良適合」アプローチを可能にしてもよい。これは、必要なコンピュータ処理を最小化しながら、検証プロセスの精度を最大化する（すなわち、誤った受入または拒否の発生を最小化する）目的で、データの分析を介して行ってもよい。コンピュータ処理の削減は、処理能力も使用可能な電力も制限され得るスマートカードにとって特別な利点である。例えば、マルチモードの生体認証システムと同様に、生体認証と物理的に複製不可能な特性によるスマートカードの身元確認を正規化する必要があるため、重み付けは利点を提供する。最良適合を提供するための分析では、例えば、ベイズ推定分析および／または他の同様の手法を適用することにより、テストを伴う目標探索最適化プロセスを利用してもよい。最良適合分析は、測定値の一意性の度合いに基づいて、認証の種々の要因で使用される種々の測定値（例えば、物理的に複製不可能な特性と生体認証ＩＤ）に重み係数を適用することにより、多要素認証プロセスのセキュリティを最適化することを含んでもよい。これにより、認証プロセスのセキュリティにおいて精度の向上と、より高い信頼度が可能になり得、処理サイクルが少なくなり、コンピュータの処理要件が低くなり得る。

【００１９】

多要素認証プロセスは、センサからの生体認証データおよび／または物理的に複製不可能な特性に関する経時的な変化を説明するために、時間の経過とともに適応できてもよい。例えば、生体認証データの外観を変更したり、および／またはセンサの物理的に複製不可能な特性を変更したりできる生体認証センサの摩耗があってもよい。ユーザは、年を取って、皮膚の老化につれて指紋の変化など、生体認証の変化をもたらす可能性がある。スマートカードは、物理的力／物理的接触の観点からも電磁力の観点からも外部の影響を受ける可能性がある。これは、振動パターンなどの物理的に複製不可能な特性に影響を与える可能性があり、部品自体の変更、または部品を組み込み部品との間でやり取りされる電気信号を処理するフレキシブル回路の変更のいずれかにより、スマートカードの電気部品の電気的応答にも影響を与える可能性がある。

【００２０】

多要素認証プロセスには、物理的に複製不可能な特性と、生体認証センサ情報の取得および処理が含まれ得る生体認証データとの一方または両方の変化に適応するため、ファジーロジックタイプのプロセスまたは機械学習タイプのプロセスが含まれてもよい。多要素認

証プロセスには、生体認証および／または物理的に複製不可能な特性の身元を経時的に監視すること、例えば、少なくとも１０個、少なくとも２０個、または少なくとも５０個の認証など、設定回数の直近の認証のすべてを記録することが含まれてもよい。次いで、予想される変化率に応じて、多要素認証で複数のこのような特性が使用される場合、異なる物理的に複製不可能な特性に対して異なる数だけでなく生体認証および物理的に複製不可能な特性に対して記録される認証の数が異なってもよい。過去の認証に対して記録されたデータを使用して、経時的な変化を識別したり、受入基準を更新したりしてもよい。例えば、生体認証テンプレートは、ユーザが年を取るにつれて生体認証データを適切に調整する目的で、設定回数の直近の生体認証に基づいて更新されてもよい。物理的に複製不可能な特性の時間の変化がある場合、すなわち、スマートカードが使用中に「古くなる」場合、物理的に複製不可能な特性の照合のための閾値は拡大してもよく、またはシフトしてもよい。

【００２１】

過去の認証から記録されたデータはまた、または代替的に、スマートカードの潜在的な不正使用を検出するために使用されてもよい。場合によっては、生体認証センサからのデータおよび／または以前の認証からのデータと同一の物理的に複製不可能な特性を確認することにより、これを行ってもよい。スマートカードのセキュリティに関して使用される攻撃の１つのタイプは、有効データを記録し、これを再生してプロセッサをだまして安全機構へのアクセスを許可することである。データが以前の認証と同一の状況では、安全機構へのアクセスを取得するための種々の有効な試みの間にデータの小さな変化が避けられないため、これはスマートカードをハッキングする試みとして扱うことができる。したがって、生体認証センサからのデータおよび／または物理的に複製不可能な特性からのデータの一方または両方が以前の認証からのデータと同一である場合、多要素認証プロセスは認証の試みを拒否することを含んでもよい。

【００２２】

スマートカードのプロセッサは多要素認証プロセスを実行するため、上記の手順を実行するように構成されてもよい。下記のように、これは単一のプロセッサでも、必要な機能を提供するために連携して動作する複数の別のプロセッサでもよい。

【００２３】

上記のように、使用できる１つの物理的に複製不可能な特性は、スマートカードの振動パターンである。したがって、スマートカードは、スマートカードの動きを感知するための加速度計を備えてもよく、プロセッサは、加速度計により感知された動き由来のスマートカードの物理的に複製不可能な特性を使用してもよい。これは、ユーザが特定の方法で、例えば、スマートカードを硬い面上でタップするか、スマートカードをフリックして振動させることにより、スマートカードと物理的に通信することを必要とする場合がある。ユーザからスマートカードへの入力に変化があり、場合によっては、これが加速度計の出力に大きな変化をもたらす可能性があることが理解されよう。しかし、振動パターンの一部の特徴は、入力が変化しても一意になると予想される。さらに、上記のように、提案された多要素認証では、種々の認証要素の重み付けだけでなく受入閾値に多少のばらつきがあり、これを使用して加速度計出力のばらつきに対処できる。

【００２４】

スマートカードがある種の振動を受けたときの加速度計の出力は、スマートカードに固有のものになる。各スマートカードは、他のカードとは異なる方法でユーザのカードとの通信に動的に反応するだけでなく固有周波数を有するようになる。加速度計により検出されるカードの動きには、スマートカードの動的反応の影響が含まれる。加速度計からの出力信号（すなわち、加速度計の出力データ）は、行われる動きだけでなくスマートカードの動的反応を表している。

【００２５】

加速度計の出力データはユーザにもカードにも固有であるため、データを複製することはできない。「偽の」カードが作成されると、新たなカードの動的反応は元のカードとは異

なるため、元のカードはハッキングできない。量産スマートカードの場合、スマートカードの構造の許容差と避けられない小さなばらつきが、スマートカードの動きの特性の違いにつながる可能性がある。同じ基本プロセスを用いて製造された量産スマートカード間の差異を増大させるために、製造方法には、個々のカードがより明確で固有の振動パターンを有するように加速度計の位置を変更したり、異なる特性のある質量／剛性要素をスマートカードに追加したりすることが含まれる。したがって、スマートカードは、いくつかの例では、追加の質量または剛性要素を含んでもよい。

【００２６】

加速度計はまた、加速度計により感知された動きに基づいてスマートカードの制御を可能にしてもよい。例えば、加速度計により感知された動きを使用して、カードの種々の動作モードをアクティブにしてもよい。有利なことに、スマートカードは非接触カードであるため、ユーザは、唯一の接点がユーザにより保持されているカードリーダを介してカードを使用するだけでなく異なるモード間で切り替えることができる。これにより、カードの操作性を損なうことなく、スマートカードの使用方法の機能と複雑さを増大させることができる。

【００２７】

プロセッサは、加速度計の出力に基づいてカードの動きを識別し、事前設定された動きに応じてスマートカードの動作モードを変更するように構成されてもよい。事前設定された動きとしては、移動、回転、加速、ジャーク／インパルスなどの一部またはすべてが挙げられてもよい。さらに、プロセッサは、動きのない期間の長さ、すなわちスマートカードのアクティブな使用がないことを示す期間を決定してもよい。これは、スマートカードの動作モードを変更したり、現在アクティブである安全機構などの機構を非アクティブ化したりするためにも使用できる。プロセッサはまた、ダブルタップなどの反復運動または一連の動き、またはスライド運動およびツイスト運動などの並進運動に続く回転を識別するように構成されてもよい。

【００２８】

加速度計により感知される動きにより制御されるスマートカードの動作モードは、高度な機能、例えば、カードのオン／オフ、またはアクセスカード、支払カード、交通スマートカード間の切り替え、同じタイプの異なるアカウント（例えば２つの銀行口座）間の切り替えなどカードの基本機能の変更に関連してもよい。

【００２９】

スマートカードは、休止／オフモードに入り、一定期間、例えば、アプリケーションに応じて数日間または数週間使用されなかった後、継続使用のために再アクティブ化または再認証が必要になる場合がある。再アクティブ化には、固有の一連の動きを検出するか、リーダとの通信によるアクティブ化が必要になる場合がある。

【００３０】

動きは単一の感知軸のある加速度計により検出できるが、すべての方向の加速度を検出できることが好ましい。これは複数の加速度計を介して行ってもよいが、好ましくは３軸加速度計など、すべての方向の加速度を検出できる単一の加速度計を使用する。

【００３１】

加速度計は、ＭＥＭＳ加速度計などの微細加工された加速度計であってもよい。代替的に、専用の圧電加速度計または加速度を感知できる別の圧電センサ（例えば、圧電サウンダまたは圧電マイクロホン）などの圧電センサを使用してもよい。これらのタイプのデバイスを使用すると、スマートカードのサイズを増やすことなく、スマートカードに取り付けることができる。また、低消費電力であるため、上記のスマートカードに対する設計上の制約になる可能性がある。圧電センサは、入力が圧電センサにより検出されるまで消費電力がゼロとなるように、デバイスに有利に組み込むことができる。加速度計は、微細加工されたカンチレバーまたは地震質量（ｓｅｉｓｍｉｃ　ｍａｓｓ）などの感知素子を使用してもよい。実施例では、加速度感知は、検知素子の加速誘導運動に起因する差動容量の原理に基づいている。使用できる加速度計には、米国ニューヨーク州イサカのＫｉｏｎｉ

ｘ、Ｉｎｃ．が提供するような３軸デジタル加速度計がある。実施例は、Ｋｉｏｎｉｘ ＫＸＣＪＢ－１０４１加速度計を使用する。

【００３２】

スマートカードは、ＲＦＩＤ通信またはＮＦＣ通信を用いるなど、無線通信が可能である。代替的または追加的に、スマートカードは、例えば「チップとピン」カードに使用されるような接触パッドなどによる接触接続を含んでもよい。種々の実施形態では、スマートカードは、無線通信も接触通信も許可してもよい。

【００３３】

プロセッサはまた、生体認証センサを介して生体認証データを登録するように構成されてもよい。これは、好ましくはカードに埋め込まれている指紋センサであってもよい。この特徴により、認証ユーザは、最初に指紋を実際のカードに登録し、次いでカードの一部またはすべての使用を許可するために指紋センサに指または親指を置く必要がある。プロセッサ上の指紋照合アルゴリズムを使用して、登録ユーザと指紋センサにより感知された指紋との間の指紋の一致を識別してもよい。

【００３４】

スマートカードは、アクセスカード、クレジットカード、デビットカード、支払カード、ポイントカード、ＩＤカードなどのいずれでもよい。スマートカードは、好ましくは、８５．４７ｍｍから８５．７２ｍｍの幅、および５３．９２ｍｍから５４．０３ｍｍの高さを有する。スマートカードは、０．８４ｍｍ未満、好ましくは約０．７６ｍｍ（例えば、±０．０８ｍｍ）の厚さを有してもよい。より一般的には、スマートカードは、スマートカードの仕様であるＩＳＯ７８１６に準拠してもよい。

【００３５】

本明細書でプロセッサが言及される場合、これには、連携して動作する複数のプロセッサが含まれてもよいことが理解されるべきである。例えば、生体認証センサおよび／または加速度計（存在する場合）には、スマートカードの他の機構を制御するメインプロセッサと通信する専用のプロセッサを各々設けてもよい。さらに、好ましい実施形態では、指紋認証エンジンの一部である指紋プロセッサだけでなくカードとの通信を制御するプロセッサがあると言われているが、これらの２つのプロセッサは、各々複数のプロセッサからなってもよく、または単一の結合プロセッサの別のソフトウェアモジュールである可能性があることを理解されたい。

【００３６】

第２の態様から見ると、本発明は、スマートカードを制御する方法であって、スマートカードが、スマートカードの動作を制御するためのプロセッサと、認証ユーザを識別するための生体認証センサとを備え、本方法が、多要素認証プロセスに基づいてスマートカードの動作を制御してスマートカードの１以上の安全機構へのアクセスを許可することを含み、多要素認証プロセスが、（ｉ）スマートカードの物理的に複製不可能な特性に基づくスマートカードの身元の確認と、（ｉｉ）生体認証センサによるユーザの身元の認証との両方を必要とする方法を提供する。

【００３７】

本方法は、第１の態様のスマートカードと同じ方法で、スマートカードのセキュリティに関する利点を提供する。

【００３８】

本方法は、第１の態様に関する上記特徴のいずれかを備えたスマートカードの使用を含んでもよい。したがって、物理的に複製不可能な特性は、上記のようであってもよい。本方法は、登録プロセス中に物理的に複製不可能な特性を記録することを含んでもよい。これは、上記のように、連続して、または認証ユーザの生体認証データの登録と同時に行われてもよい。

【００３９】

本発明はまた、スマートカードの製造方法を含んでもよい。これは、第１の態様のような特徴を提供することからなってもよい。製造方法はまた、上記任意の特徴の一部またはす

べてを提供することを含んでもよい。本方法は、上記のように機能するようにプロセッサをプログラムすることを含んでもよい。

【００４０】

振動パターンの差異を増大させることにより、同一または同様の動きに曝される同じプロセスを用いて製造されたカード間で加速度計の出力の差を大きくするために、製造方法は、スマートカード上に加速度計を提供し、個々のスマートカードが固有の振動パターンを有するように、加速度計の位置を変更したり、異なる特性のある質量／剛性要素を、および／または異なる位置でスマートカードに追加したりすることを含んでもよい。

【００４１】

本方法は、オプションで、質量および／または剛性要素を、カードに、例えばカードのフレキシブル回路基板上に追加することであって、異なる質量および／また剛性要素が、異なる質量および／また剛性要素の特性のある一組の要素から選択されることを含んでもよい。これにより、追加された質量および／または剛性要素を同じ位置に置くことが可能になる。これにより、追加された要素の質量および／または剛性が変化するため、カードの動きに対する可変効果を確保しながら、製造が容易になる。代替的または追加的に、質量および／または剛性要素は、カードごとに異なる位置でカードに追加されてもよい。これは、各カードに同一の質量および／または剛性要素を使用できるか、質量および／または剛性要素が、異なる質量および／または剛性特性のある一組の要素から選択される。

【００４２】

さらに別の態様では、本発明は、上記のスマートカードのプロセッサ上で実行されると、プロセッサにスマートカードの動作を制御させて多要素認証プロセスに基づいてスマートカードの１以上の安全機構へのアクセスを許可する命令を含むコンピュータプログラム製品を提供する。多要素認証プロセスでは、（ｉ）スマートカードの物理的に複製不可能な特性に基づくスマートカードの身元の確認と、（ｉｉ）生体認証センサによるユーザの身元の認証との両方が必要である。命令は、プロセッサを上記の任意の特徴および好ましい特徴の一部またはすべてに従って動作させるように構成されてもよく、スマートカードは、上記の特徴のいずれかから取得された対応する特徴を有してもよい。

【００４３】

ここで、本発明の特定の好ましい実施形態を、例示のみを意図して、添付の図面を参照して、より詳細に説明する。

【図面の簡単な説明】

【００４４】

【図１】指紋エリアセンサの形の生体認証センサに加えて加速度計を組み込んだスマートカードの回路図である。

【図２】外部ハウジングを備えたスマートカードを示す図である。

【図３】積層型スマートカードの実施例を示す図である。

【発明を実施するための形態】

【００４５】

例として、本発明は、非接触技術を使用するスマートカードという文脈において説明され、例示の実施形態では、リーダから収集された電力を使用する。これらの特徴は、提案された動きに敏感なスマートカードの有利な特徴であると想定されているが、必須の特徴とは見なされない。したがって、スマートカードは、代替的に、物理的接触を使用したり、例えば内部電力を供給するバッテリを含んだりしてもよい。

【００４６】

図１は、オプションの加速度計１６を備えたスマートカード１０２のアーキテクチャを示す。駆動中のカードリーダ１０４は、アンテナ１０６を介して信号を送信する。信号は、典型的には、ＮＸＰ　Ｓｅｍｉｃｏｎｄｕｃｔｏｒｓ製のＭＩＦＡＲＥ（登録商標）およびＤＥＳＦｉｒｅ（登録商標）システムでは１３．５６ＭＨｚであるが、ＨＩＤ　Ｇｌｏｂａｌ　Ｃｏｒｐ製の低周波数ＰＲＯＸ（登録商標）製品の場合は１２５ｋＨｚであってもよい。この信号は、同調コイルとコンデンサを備えるスマートカード１０２のアンテナ

１０８により受信され、次いで通信チップ１１０に渡される。受信された信号は、ブリッジ整流器１１２により整流され、整流器１１２のＤＣ出力は、通信チップ１１０からのメッセージングを制御するプロセッサ１１４に提供される。

【００４７】

プロセッサ１１４から出力された制御信号は、アンテナ１０８を横切って接続される電界効果トランジスタ１１６を制御する。トランジスタ１１６をオンとオフに切り替えることにより、信号は、スマートカード１０２により送信され、リーダ１０４内の適切な制御回路１１８により復号できる。このタイプのシグナリングは後方散乱変調として知られており、リーダ１０４がそれ自体への返送メッセージを駆動するために使用されるという事実により特徴付けられる。

【００４８】

加速度計１６は、存在する場合、適切な方法でプロセッサ１１４に接続される。加速度計１６は、米国ニューヨーク州イサカのＫｉｏｎｉｘ、Ｉｎｃ．により提供される３軸デジタル加速度計であってもよく、この実施例では、Ｋｉｏｎｉｘ　ＫＸＣＪＢ－１０４１加速度計である。加速度計１６は、カードの動きを感知し、出力信号をプロセッサ１１４に提供し、プロセッサ１１４は、下記のように、カード上の必要な動作モードに伴う動きを検出および識別するように構成される。下記のように、加速度計１６を使用して、多要素認証プロセスで使用するスマートカード１０２の物理的に複製不可能な特性を取得することもできる。加速度計１６は、電力が駆動中のカードリーダ１０４から収集されている場合にのみ使用されるか、または代替的に、スマートカード１０２には、加速度計１６とプロセッサ１１４の関連機能および、いつでも使用されるデバイスの他の機能も可能にするバッテリ（図示せず）を追加的に設けることができる。

【００４９】

指紋または拇印に基づくユーザの生体認証を可能にするために、指紋認証エンジン１２０がプロセッサ１１４に接続されている。指紋認証エンジン１２０は、カードが完全に受動的スマートカード１０２となるようにアンテナ１０８により給電できる。その場合、認証ユーザの指紋識別は、カードリーダ１０４から電力を収集している間のみ可能である。代替の構成では、スマートカード１０２には、指紋認証エンジン１２０と、いつでも使用されるプロセッサ１１４の関連機能も可能にするバッテリ（図示せず）を追加的に設けることができる。

【００５０】

本明細書で使用する「受動的スマートカード」という用語は、例えばカードリーダ１１８により生成された励起場から収集されたエネルギーのみにより通信チップ１１０に給電されるスマートカード１０２を意味すると理解されるべきである。すなわち、受動的スマートカード１０２は、放送のためにその電力を供給するリーダ１１８に依存する。受動的スマートカード１０２は通常バッテリを含まないが、バッテリは回路の補助部品（ただし放送目的でない）に給電するために含まれてもよい。このようなデバイスは、しばしば「準受動的デバイス」と呼ばれる。

同様に、「受動的指紋／生体認証エンジン」という用語は、励起場、例えばカードリーダ１１８により生成されたＲＦ励起場から収集されたエネルギーのみにより給電される指紋／生体認証エンジンを意味すると理解されるべきである。

代替の実施形態では、バッテリ駆動の、したがって非受動的スマートカードを提供することができ、加速度計、指紋センサ、多要素認証プロセスなどに関して同じ機能を有することに留意されたい。これらの代替手段により、スマートカードは、収集された電力の使用がカード本体内に含まれるバッテリからの電力に置き換えられることを除いて、同じ特徴を有することができる。

【００５１】

カード本体は、図２に示すようなカードハウジング１３４または図３に示すような積層カード本体１４０とすることができる。スマートカード１０２のサイズには大きな制約があることが理解されよう。

【００５２】
アンテナ１０８は、カードリーダ１０４からＲＦ信号を受信するように同調される誘導コイルとコンデンサを含む同調回路を備える。リーダ１０４により生成された励起場に曝されると、アンテナ１０８を横切って電圧が誘導される。
【００５３】
アンテナ１０８は、アンテナ１０８の各端部に第１端部出力線１２２および第２端部出力線１２４を備える。アンテナ１０８の出力線は指紋認証エンジン１２０に接続され、指紋認証エンジン１２０に電力を供給する。この構成では、整流器１２６は、アンテナ１０８により受信されたＡＣ電圧を整流するために提供される。整流されたＤＣ電圧は、平滑コンデンサを使用して平滑化され、指紋認証エンジン１２０に供給される。
【００５４】
指紋認証エンジン１２０は、指紋プロセッサ１２８と、図２に示すようにカードハウジング１３４に取り付けられるか、または図３に示すような積層カード本体１４０から露出するように取り付けられるエリア指紋リーダ１３０であり得る指紋リーダ１３０とを含む。カードハウジング１３４または積層体１４０は、図１のすべての部品を収容し、従来のスマートカードと同様のサイズである。指紋認証エンジン１２０は受動的であり得るため、アンテナ１０８からの電圧出力のみにより給電されるか、または上記のようにバッテリ電力があってもよい。指紋プロセッサ１２８は、妥当な時間内に生体認証照合を実行できるように、非常に低電力かつ非常に高速になるように選択されるマイクロプロセッサを備える。
【００５５】
指紋認証エンジン１２０は、指紋リーダ１３０に提示された指または親指をスキャンし、指または親指のスキャンされた指紋を、指紋プロセッサ１２８を用いて予め保存された指紋データと比較するように構成される。次いで、スキャンされた指紋は、予め保存された指紋データと一致するかどうかについて判定を行う。好ましい実施形態では、指紋画像を取り込み、カード１０２のベアラを認証するのに必要な時間は１秒未満である。
【００５６】
生体認証の一致が判定される場合、および／または適切な動きが加速度計１６を介して検出される場合、プロセッサ１１４は、そのプログラミングに応じて適切なアクションをとる。この例では、指紋認証プロセスが、多要素認証プロセスにおける少なくとも１つの追加認証の要件に加えて使用される。この多要素認証プロセスにより、スマートカードの安全機構への完全なアクセスには、生体認証（この例では指紋認証により具体化）も物理的に複製不可能な特性によるスマートカードの身元確認も必要である。多要素認証プロセスが、生体認証特性とも物理的に複製不可能な特性とも一致を発見する場合、プロセッサ１１４は、非接触カードリーダ１０４を備えたスマートカード１０４の使用を許可する。したがって、通信チップ１１０は、多要素認証プロセスが満たされると、信号をカードリーダ１０４に送信することのみが許可される。通信チップ１１０は、後方散乱変調により信号を送信する。
【００５７】
物理的に複製不可能な特性は、例えば、スマートカード上の半導体デバイスの物理的に複製不可能な機能であってもよい。代替的または追加的に、多要素認証プロセスは、所定の電気的刺激または物理的刺激を受けたときのセンサからの出力など、生体認証センサ１３０に基づく物理的に複製不可能な特性を利用してもよい。物理的に複製不可能な特性は、生体認証センサ１３０にもプロセッサ１１４にも、または指紋プロセッサ１２８にも基づいてもよい。半導体デバイスなどの電気部品は、名目上は同一であるが、実際には、提案されたスマートカード１０２が必要とする多要素認証プロセスに関する１以上の物理的に複製不可能な特性についての基礎として使用できる多数の小さなばらつきを有する。
【００５８】
加速度計１６が使用される場合、プロセッサ１１４は、加速度計１６からの出力を受け取り、これにより、プロセッサ１１４は、スマートカード１０２のどの動きが行われたかを

判定してもよい。プロセッサ１１４は、スマートカード１０２の動作モードへの必要な変更と連動する事前設定された動きを識別してもよい。上記のように、動きとしては、回転、並進、加速、ジャーク、インパルスおよび加速度計１６により検出可能な他の動きの任意のタイプまたは組合せが挙げられてもよい。

【００５９】

加速度計１６により検出される動きは、スマートカード１０２の構造および幾何形状によりさらに影響される。例えば、図２のようなハウジング１３４を備えたスマートカード１０２は、固有周波数と特定の動きに対する動的反応の観点から、図３のような積層体１４０を備えたスマートカード１０２とは異なる挙動を示すであろう。異なって製造された同じ基本型のカードにも同じことが当てはまるため、異なる製造業者または異なるプロセスにより製造された積層カードは異なる反応をするであろう。

【００６０】

これは、加速度計１６が、スマートカード１０２の振動パターンに基づく物理的に複製不可能な特性に関して使用され得ることを意味する。これは、上記のような電気部品からの物理的に複製不可能な特性の代わりに、またはそれに加えて可能性がある。「偽」カードが不正に作成され、不正者がスマートカードの振動パターンに関するデータをどうにかしてコピーし、このデータが「偽」カードのマイクロプロセッサに「注入」される場合、新たなカードの共振は、元のカードと異なる。そのため、「偽」カードは、それ自体を正しく識別できないことから、ハッキングされ得ない。したがって、加速度計１６を介して検出される動きのパターンは、ユーザにも個々のスマートカード１０２にも固有であり得る。

【００６１】

加速度計１６を介して登録された動きのパターンは、カード１０２のメモリ（例えば、プロセッサ１１４の一部として）および／または外部データベース内に保存されてもよい。動きのパターンの加速度計出力信号は各カードに固有である可能性があるため、生体認証データと異なり、データをカードから保存することを許可することによるセキュリティへのリスクはより低く、カード自体の真正性に関する追加の確認はカード上の加速度計データのある外部データベース中の加速度計データを確認することにより実行できる。

【００６２】

動作モードの必要な変更に伴う識別された動きに応じてプロセッサ１１４がアクティブ化するまたは切り替える動作モードには、カードをオン／オフにする、非接触支払いおよび／またはカードリーダ１０４との通信などカード１０２の安全面をアクティブ化する、または例えばアクセスカード、支払カード、交通スマートカードとしての動作間の切り替え、同じタイプの異なるアカウント（例：２つの銀行口座）間の切り替え、通信プロトコル（ｂｌｕｅｔｏｏｔｈ、Ｗｉｆｉ、ＮＦＣなど）間の切り替えによるカード１０２の基本機能の変更および／または通信プロトコルのアクティブ化、ＬＣＤやＬＥＤディスプレイなどのディスプレイのアクティブ化、ワンタイムパスワードなどのスマートカード１０２からの出力の取得、またはスマートカード１０２の標準動作を自動的に実行するようにカード１０２を促すなど上記のような動作モードが含まれてもよい。スマートカード１０２は、加速度計１６により検出された事象に反応してとられるアクションの観点から任意の必要な特性で容易にプログラムできることが理解されよう。

【００６３】

プロセッサ１１４は、どの動き（動きの組合せを含む）が特定の動作モードをアクティブ化すべきかをユーザが指定できるようにする学習モードを有する。学習モードでは、プロセッサ１１４は、ユーザに所望の一連の動きを行い、所定の一組の時間の間、動きを繰り返すように促す。次いで、これらの動きは、必要な動作モードに割り当てられる。プロセッサ１１４は、上記のように、落としたカードモードおよび／または生体認証バックアップモードを実施することができる。

【００６４】

場合によっては、生体認証スマートカード１０２の所有者が負傷して、カード１０２に登録されている指が損傷することになる場合がある。この損傷は、例えば、評価されている

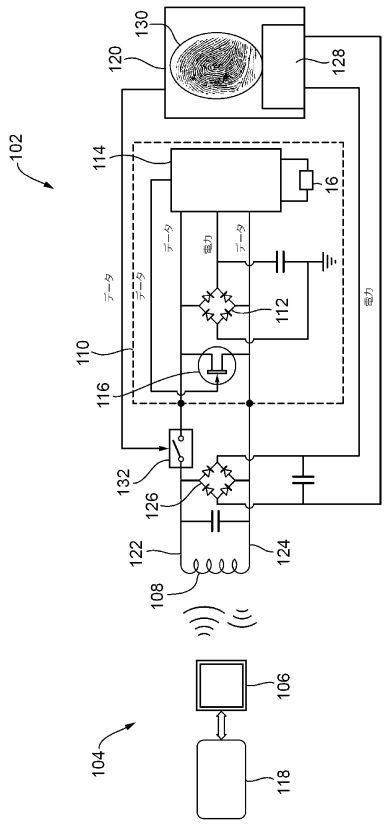
指の一部の傷跡である可能性がある。このような損傷は、指紋の照合が行われないため、所有者がカード１０２により認証されないことを意味する。この場合、プロセッサ１１４は、一連の動きを介して、バックアップ身元確認／認証確認をユーザに促すことができる。したがって、ユーザは、生体認証が失敗する場合に使用されるカードの動きを用いて「パスワード」を入力することができる。

【００６５】

このようなバックアップ認証の後、カード１０２を通常通り使用するように構成することができ、またはカード１０２のより少ない動作モードまたはより少ない機構が有効にされる劣化モードを備えることができる。例えば、スマートカード１０２が銀行カードとして機能できると、バックアップ認証により、カードの通常の最大限度よりも低い最大支出限度の取引が可能になる場合がある。

【図面】

【図１】


102
104
106
108
110
112
114
116
118
120
122
124
126
128
130
132
16
データ
電力

【図２】

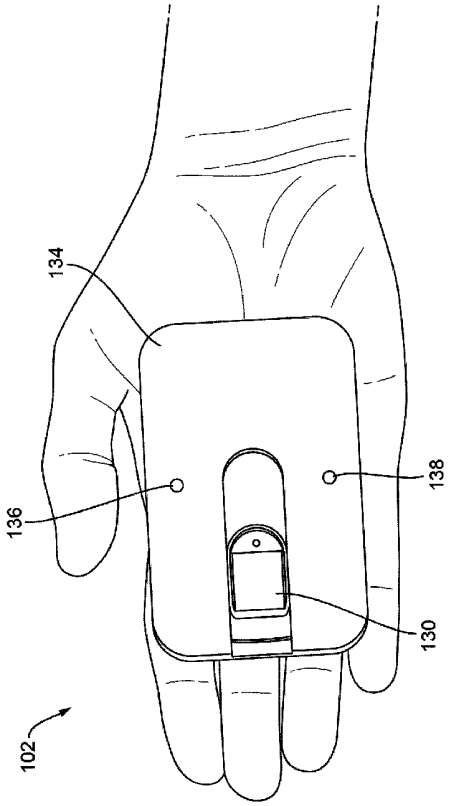


Fig. 2
102
130
134
136
138

【図３】

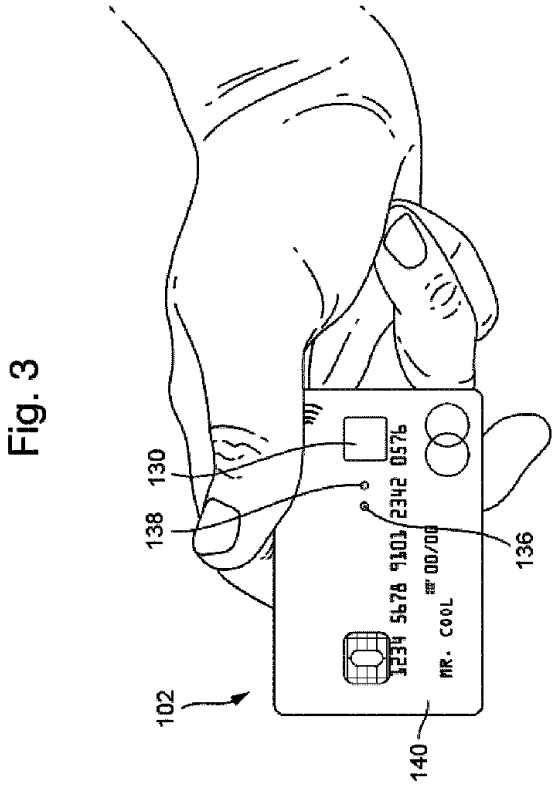


Fig. 3
102
130
136
138
140
1234 5678 9101 2342 0576
MR. COOL
00/00

フロントページの続き

(51)国際特許分類　　FI

G06F 21/34 (2013.01)		G06F	21/34	
G06T 7/00 (2017.01)		G06T	7/00	530
G06T 1/00 (2006.01)		G06T	1/00	400G
B42D 25/305 (2014.01)		B42D	25/305	100

(56)参考文献　　特表２０１６－５１１４６０（ＪＰ，Ａ）
米国特許出願公開第２０１１／０００２４６１（ＵＳ，Ａ１）
米国特許第０８８６８９２３（ＵＳ，Ｂ１）
国際公開第２０１４／１４６６８４（WO，Ａ１）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３１－２１／４６
Ｇ０６Ｋ　１９／０７－１９／０８
Ｇ０６Ｔ　７／００
Ｇ０６Ｔ　１／００
Ｂ４２Ｄ　２５／３０５