審決

不服２０１９－５２９２

（省略）
請求人　アーム・アイピー・リミテッド

（省略）
代理人弁理士　小野 誠

（省略）
代理人弁理士　金山 賢教

（省略）
代理人弁理士　坪倉 道明

（省略）
代理人弁理士　重森 一輝

（省略）
代理人弁理士　安藤 健司

（省略）
代理人弁理士　市川 英彦

（省略）
代理人弁理士　青木 孝博

（省略）
代理人弁理士　櫻田 芳恵

（省略）
代理人弁理士　川嵜 洋祐

（省略）
代理人弁理士　五味渕 琢也

（省略）
代理人弁理士　今藤 敏和

（省略）
代理人弁理士　飯野 陽一

（省略）
代理人弁理士　市川 祐輔

（省略）
代理人弁理士　森山 正浩

（省略）
代理人弁理士　岩瀬 吉和

（省略）
代理人弁理士　城山 康文

特願２０１６－５２０７３７「トラステッドデバイス」拒絶査定不服審判事件〔平成２６年１２月２４日国際公開，ＷＯ２０１４／２０２９５１，平成２８年　８月１２日国内公表，特表２０１６－５２４２４９〕について，次のとおり審決する。

結論
本件審判の請求は，成り立たない。

理由
第１．手続の経緯
本願は，２０１４年６月９日（パリ条約による優先権主張外国庁受理２０１３年６月１８日　アメリカ合衆国）を国際出願日とする出願であって，
平成２８年２月１０日付けで特許法１８４条の４第１項の規定による明細書，請求の範囲，及び，図面（図面の中の説明に限る）の日本語による翻訳文が提出され，平成２９年３月１５日付けで審査請求がなされ，平成２９年１２月２５日付けで審査官により拒絶理由が通知され，これに対して平成３０年７月４日付けで意見書が提出されると共に手続補正がなされたが，平成３０年１２月１４日付けで審査官により拒絶査定がなされ，これに対して平成３１年４月２２日付けで審判請求がなされると共に手続補正がなされ，令和１年６月２６日付けで審査官により特許法１６４条３項の規定に基づく報告がなされたものである。

第２．本願発明について
本願の請求項１に係る発明（以下，これを「本願発明」という）は，平成３１年４月２２日付けの手続補正により補正された特許請求の範囲の請求項１に記載された，次のとおりのものである。

「トラステッドデバイスであって，
認証動作によって，前記トラステッドデバイスを物理的に所持しているユー

ザを認証し，それによって，前記トラステッドデバイスを認証済み状態に切り替えるように構成されている認証回路と，
　前記認証動作に従って，前記ユーザによる前記トラステッドデバイスの物理的所持をモニタリングし，前記トラステッドデバイスが前記ユーザによってもはや物理的に所持されていない場合，前記トラステッドデバイスを前記認証済み状態から脱して切り替えるように構成されている，保持モニタリング回路であって，前記トラステッドデバイスが前記ユーザによって所持されているときに光から遮蔽される光検出器を含む一つ以上の検出回路を備える，前記保持モニタリング回路と，
　複数の異なる目標デバイスの１つである目標デバイスから受信される，通信を確立することを求める要求を検出するように構成されている通信トリガ回路と，
　前記トラステッドデバイスが前記認証済み状態にある場合に，前記目標デバイスと通信するように構成されている通信回路とを備える，トラステッドデバイス。」

第３．原査定における拒絶の理由
　原審における平成３０年１２月１４日付けの拒絶査定（以下，これを「原審拒絶査定」という）の拒絶の理由は，
１．この出願の請求項１に係る発明は，本願の優先権主張の日（以下「優先日」という。）前に日本国内又は外国において，頒布された又は電気通信回線を通じて公衆に利用可能となった下記の引用文献１～引用文献４に記載された発明及び引用文献５に記載の周知技術に基づいて，その優先日前にその発明の属する技術の分野における通常の知識を有する者が容易に発明をすることができたものであるから，特許法２９条２項の規定により特許を受けることができない，というものである。

〈引用文献〉
１．特表２００５－５３８４３０号公報
２．特表２００５－５２８６６２号公報
３．特開２００４－２８０２４５号公報
４．国際公開第２００９／０２８０１８号
５．特開２００１－１９５１４５号公報

２．本願は、請求項３の記載が下記の点で、特許法３６条６項２号に規定する要件を満たしていない。

記

＜以下略＞

第４．引用文献に記載の事項
１．原審における平成２９年１２月２５日付けの拒絶理由（以下，これを「原審拒絶理由」という）に引用された，本願の第１国出願前にすでに公知である，特表２００５－５３８４３０号公報（公表日；２００５年１２月１５日，以下，これを「引用文献１」という）には，関連する図面と共に，次の事項が記載されている。

Ａ．「【０００５】
［発明の要約］
使用ベースの状況セキュリティの方法および汎用装置を，説明し提供する。実施形態において，汎用装置を，腕時計として実施する。この腕時計を，認証されたユーザに対し無線トランザクションを補助するように構成し，かつ認証されたユーザの一部を取り巻くよう，認証されたユーザが着用するように，構成する。無線トランザクションは，いかなるタイプ（たとえば，クレジットカードタイプ，デビットカードタイプ，アクセス制御タイプ等）のものであってもよい。さらに，腕時計は，認証されたユーザが腕時計の使用を開始した後にその腕時計を着用し続けるか否かに基づき，腕時計の使用を制御する確認機構を備える。
【０００６】
特に，腕時計は，状況セキュリティ確認方式を実行し，そこでは，認証された使用を，腕時計の所有のみでなくその動作状況によっても確定する。動作状況により，腕時計は，その腕時計がアクティブ／セキュアステータス（active/secure status）状態にあるかまた非アクティブ状態にあるかに基づき，無線リンクを介して任意の外部サービス対話を受け入れるかまたは拒否することができるようになる。さらに，腕時計自体のストラップ内にデータチャネルを統合することにより，腕時計の使用を開始した認証されたユーザによりその腕時計が着用されているか否かの確認が可能になる。腕時計を取り外すことにより，その状況セキュリティが無効になって時計が非アクティブ状態になり，無線リンクを介するすべての外部対話が不能になる。」（下線は，当審にて，説明の都合上，付加したものである。以下，同じ。）

Ｂ．「【００１３】
図１は，本発明の実施形態による腕時計１００を示す。本発明の汎用装置１００を，認証されたユーザの身体の一部を取り巻くよう，認証されたユーザが着用するように，構成する。実施形態では，汎用装置１００を，図１に示すように腕時計１００として実施する。別法として，汎用装置１００を，腕輪またはアームバンド等，いかなる指，手，腕，足，脚，ウエスト，手首または他の身体着用品として実施してもよい。腕時計１００は他の構成を有してもよい，ということを理解しなければならない。
【００１４】
特に，腕時計１００は，１つまたは複数のアプリケーションと，セキュア認証／識別データと，トランザクションデータと，をホストするとともに，使用

ベース状況セキュリティ確認方式を実行することにより合法のユーザによる腕時計１００の使用および所有を確認することができる，電子回路５０を備える。腕時計１００を，認証されたユーザに対し無線トランザクションを補助するように構成し，認証されたユーザの手首等，認証されたユーザの一部を取り巻くよう，認証されたユーザが着用するように構成する。無線トランザクションは，いかなるタイプ（たとえば，クレジットカードタイプ，デビットカードタイプ，アクセス制御タイプ等）のものであってもよい。さらに，腕時計１００は，認証されたユーザが腕時計１００の使用を開始した後にその腕時計１００を着用し続けるか否かに基づいて腕時計１００の使用を制御する確認メカニズムを含む。確認メカニズムは，送信要素４０と，受信要素３０と，データチャネル８０と，データチャネル８０のステータスを監視する監視コンポーネント（電子回路５０に組み込まれている）と，を備える。

【００１５】

さらに，腕時計１００は，状況セキュリティ確認方式を実行し，そこでは，腕時計１００の所有によるのみではなくその動作状況によっても，認証された使用を確定する。動作状況により，腕時計１００は，その腕時計１００がアクティブ／セキュアステータス状態にあるかまたは非アクティブ状態にあるかに基づき，無線リンクを介して任意の外部サービス対話を受け入れるかまたは拒否することができる。特に，腕時計１００には，腕時計１００自体の第１および第２のストラップ１０および２０内に，腕時計１００がその腕時計１００の使用を開始した認証されたユーザによって着用されているか否かの確認を可能にする，データチャネル８０が統合されている。腕時計１００を取り外すことにより，その状況セキュリティが無効になって腕時計は非アクティブ状態となり，無線リンクを介するすべての外部対話が不可能になる。」

Ｃ．「【００１８】

図１に示すように，腕時計本体９０は，主機能部としての機能を果たす。腕時計本体９０は，盤面６０を介して時刻および日付機能を提供する。さらに，腕時計本体９０は，セキュアデータ記憶能力と，無線トランザクション能力と，確認メカニズムのための暗号化エンジンと，を提供する。さらに，腕時計１００には，腕時計１００自体の第１および第２のストラップ１０および２０内に，腕時計１００がその腕時計１００の使用を開始した認証されたユーザによって着用されているか否かの確認を可能にする，データチャネル８０が統合されている。腕時計本体９０は，埋込み電子機器サブシステム５０と，データチャネル８０を通してデータを送信する送信要素４０と，データチャネル８０を通して送信されたデータを受信する受信要素３０と，認証されたユーザが腕時計１００を着用しているか否かを検知する任意のバイオセンサ７０と，を有する。送信要素４０と受信要素３０との間のデータの正常な伝送は，腕時計１００が認証されたユーザによって着用されていることを示す。さらに，データチャネル８０を，認証されたユーザが腕時計１００の着用を停止する場合に動作不能とされるように構成する。特に，送信要素４０によって送信されるデータは，データチャネル８０の完全性およびステータスを監視することにより無許可の

干渉を回避するために，周期的に送信され時間変化する。特に，暗号化エンジンは，データチャネル８０によるデータのセキュアな送信を補助する。さらに，腕時計１００は，留め金またはストラップ接続機構８５を備える。」

Ｄ．「【００２０】
　腕時計１００は，第１および第２のストラップ１０および２０に統合されたデータチャネル８０の完全性を確実にすることにより，低コストかつ頑強な認証ソリューションを提供することができる。データチャネル８０自体の完全性に加えて，生体認証測定技術（たとえば，皮膚温度，光反射，湿度）を使用して，認証されたユーザの身体が存在するか存在しないかを検出する機能を提供する，任意のバイオセンササブシステム７０および７１を使用することによって，セキュリティを強化することができる。
【００２１】
　図３は，本発明の実施形態による図１の腕時計１００をセキュアに動作させる方法３００を示すフローチャートを示す。図１および図２を参照する。
【００２２】
　ブロック３１０において，ユーザは腕時計１００を着用する。さらに，ブロック３２０において，ユーザは，セキュリティ初期化手続きを踏む。この手続きは，認証されたユーザに対して種々の無線トランザクションを補助する腕時計１００のアプリケーションホスティング機能を，ユーザが一般的に運用することを可能にする前に，ユーザを認証する。初期化手続きは，単純な腕時計ベースの動作（たとえば，腕時計自体にＰＩＮ番号を入力する）であってもよく，あるいは，ブロック３２５における外部セキュリティシステムを含むより複雑なセキュリティ手続き（たとえば，網膜スキャンハードウェアを備えた外部装置を使用して，一意のユーザ確認を提供することができ，これを暗号化ＲＦデータ通信リンク３０２を介して腕時計１００に伝送する）であってもよい。いかなる初期化方法が選択されても，そのタスクは，ユーザと腕時計１００のストラップに統合されたデータチャネル８０との両方を確認することにより，腕時計１００の認証された使用を起動することである。任意のバイオセンシングサブシステム７０を使用する場合，初期化プロセスはまた，ユーザの身体の存在も確認する。
【００２３】
　ユーザが認証されると，腕時計１００は，アクティブ／セキュアステータス状態に入り（ブロック３３０），無線トランザクションおよびサービスを補助するように構成された１つまたは複数のアプリケーションの実行を開始する（ブロック３７０）。無線トランザクションおよびサービスはいかなるタイプ（たとえば，クレジットカードタイプ，デビットカードタイプ，アクセス制御タイプ等）のものであってもよい。
【００２４】
　ブロック３７５において，外部装置によって腕時計１００に対し，情報を要求するかまたは腕時計１００によってホストされる特定のアプリケーションによってサポートされる無線トランザクションを開始するために問合せがなされ

ると，ブロック３８０において，その特定のアプリケーションは，腕時計１００がアクティブ／セキュアステータス状態で動作しているか否かをチェックする。腕時計１００がアクティブ／セキュアステータス状態で動作していない場合，ブロック３９０において，特定のアプリケーションは，その特定のアプリケーションに対するユーザアクセスを拒否する。動作している場合，特定のアプリケーションは，ブロック３８５において，問合せの妥当性をチェックする（たとえば，ユーザが特定のサービスに加入したか，ユーザが特定のサービスに対して勘定を払ったか）。問合せが有効でない場合，ブロック３９０において，特定のアプリケーションは，その特定のアプリケーションが提供するサービスに対するユーザアクセスを拒否する。有効である場合，ブロック３９５において，特定のアプリケーションは，その特定のアプリケーションがサポートする所望のサービスまたはトランザクションを実行する。

【００２５】

ブロック３３５，３４０，３４５，３５０および３５５において，ストラップに統合されたデータチャネル８０の完全性を監視する。特に，周期的な間隔で，データチャネル８０にデータを送信することにより，腕時計１００のアクティブ／セキュアステータス状態を確認する。時間変化する暗号化データパケットを送受信することにより，データチャネル８０は攻撃または傍受に対しよりセキュアになる。確認プロセスは，ホストされるアプリケーションまたは腕時計１００に格納されるセキュアデータとは無関係に，データチャネル８０による送信のためにそれ自体のデータを使用する。

【００２６】

ブロック３５０において，認証されたユーザが腕時計１００を取り外したことを示してデータチャネルが動作不能となったために，アクティブ／セキュアステータス状態の変化が検出されると，腕時計１００は，そのアクティブ／セキュアステータス状態およびアプリケーションデータを消去し（ブロック３６０）その後非アクティブ状態すなわちオフに切り替わる（ブロック３６５）。オフに切り替わると，他人は腕時計１００を使用してサービスまたはトランザクションを実行することができない。オフに切り替わると，腕時計１００は，ユーザにより，腕時計１００を着用し上述した初期化手続きを再実行した後にのみ再起動することができる。任意のバイオセンシングサブシステム（ブロック３４０）は，ユーザの存在を，データチャネル８０のステータスおよび完全性の監視に対する補足として確定することにより，追加のレベルのセキュリティを提供する。バイオセンサによって検出される異常な変化により，上述したようにブロック３６０および３６５における動作が実行されることになる。」

Ｅ．「【００２７】

図４は，本発明の別の実施形態による腕時計４００を示し，光データチャネル４８０Ａおよび４８０Ｂを示す。腕時計４００は，第１および第２のプラスチックストラップ４５０および４５１とバックルファスナ４８５とを有する。実施形態では，バックルファスナ４８５は，もっとも低コストな時計で使用されるものの典型である。各ストラップ４５４および４５０を，光学光路４８０

Ａおよび４８０Ｂが統合されるように製造する。光学光路４８０Ａおよび４８０Ｂは，腕時計４００の光データチャネルを形成する。これを，各ストラップに光ファイバを埋め込むことによって達成してもよい。別法として，これを，適当な光学特性を有する材料から各ストラップを製造することによって達成してもよい。」

２．原審拒絶理由に引用された，本願の第１国出願前に既に公知である，特表２００５－５２８６６２号公報（公表日；２００５年９月２２日，以下，これを「引用文献２」という）には，関連する図面と共に，次の事項が記載されている。

Ｆ．「【００２３】
　本発明の本実施形態は，生体認証データの比較および確認という高セキュリティの恩恵を受け，さらに極めて便利なトランザクションが可能な，完全に非接触式のスマートカードトランザクションが可能な装置を提示する。思い描く実施形態の実施態様では，スマートカードチップは装着可能な機能的宝飾品，本実施態様では腕時計に包含される。考えられる商品名「ＡｕｔｈｅｎｔｉＳｗａｔｃｈ」を帯びることができ，本考察の大半ではそのように呼ばれる本実施態様は，スマートカード電子回路のみならず，生体認証データ読み取り器も提供する送受信装置も収容する。本発明の実施形態のいくつかのさらなる考察は，図を参照することによって助けることができる。本考察は時計としての本実施形態の実施態様に的を絞っているが，装着可能なセキュリティバッジ，ブローチ，およびおそらくネクタイピン，カフスボタン，ベルトのバックル，またはさらには筆記ペンまたはＰＤＡスタイラスを含め，他の多くの実施態様が思い描かれることに留意する。
【００２４】
　図１は，本発明の一実施形態の考えられる実施態様を示す。図１において，「ＡｕｔｈｅｎｔｉＳｗａｔｃｈ」１００は，時刻／日付表示１０１，リストバンド１０２，調整つまみ１０３，および本明細書ではＧＰＳ受信器からの緯度および経度表示とともに示される表示エリア１０４を備えて使用することができる。本実施態様では指紋スキャナとして使用可能なエリア１０５，およびベゼルリング１０６も示される。ベゼルリング１０６は，おそらく，ＰＩＮの入力を可能にするかまたはいくつかの機能からの選択を可能にする入力装置を実施する可能性を示すためだけに示される。アイテム１０７は，厳密に説明目的のためのものである。これは，非接触式通信を実施するために，赤外線またはＲＦ通信を時計の本体内に包含することの容易さを示すために含められている。
【００２５】
　図１に示す各アイテムは，説明および例の目的のためだけに含まれる。図示の機構はいずれも，本実施形態の本質的な部分であると解釈すべきではない。本実施形態の中心のスマートカードチップは図示されていないが，完全に実装されるものと理解する。

【００２６】
本実施態様において，スマートカードチップは，指紋スキャナ１０５とともに使用される生体認証データの存在場所である。思い描かれる一実施可能性では，使用者はしかるべき指で指紋スキャナに触れ，近接通信と結び付いたしかるべき確認により有効な使用者確認になる。
【００２７】
思い描かれる別の実施形態では，体温またはおそらく装着者の手首の静脈パターンを読み取ることができるしかるべき種類のセンサが時計１００の裏面に実装される。この場合，同じ装置にさらに別の生体認証データセキュリティのレイヤーを実装することができる。手首装着実施形態の考えられる一実施態様では，正しい指紋が読み取られた場合であっても，正しい使用者が装置を適宜装着するまで装置を無効にすることができる。この追加のセキュリティレイヤーはなお一層の泥棒阻害要因を提供しうる。実施可能な他の代替の生体認証入力は，スピーチパターン認識またはおそらく虹彩イメージでありうる。」

Ｇ．「【００３０】
無線トランザクションの応用範囲には，認識できる限度がない。しかし，本発明の本実施形態を十分に考察するために，例示的な２～３の応用をここに概説する。図３は，ｅキャッシュ装置としての本発明の本実施形態の応用を示す。図３において，使用者は，ｅキャッシュスマートカードを使用可能なＡｕｔｈｅｎｔｉＳｗａｔｃｈ１００を使用することによって購買商品の料金を支払っている。相手方の電子無線トランザクション装置は販売機３００である。
【００３１】
図４に示す本発明の実施形態では，使用可能なトランザクションは駐車場の公衆駐車メーターである。駐車メーターは，相手方のトランザクション装置４００がＡｕｔｈｅｎｔｉＳｗａｔｃｈ１００と無線通信することによって使用可能になる。本発明の本実施形態に関連する無線通信は短距離のタイプのものであることが思い描かれるため，この状況では，使用可能になった駐車メーターに近づくと所望のトランザクションを選択することができる。そして，認証が，使用者の生体認証データ読み取り器の起動によって送信される。この起動は，使用者が指紋読み取り器を触れることによって開始することができることが可能である。
【００３２】
図５は，別の，わずかに異なる種類のトランザクションを示す。ここで，使用者は入場が制限されたエリアに入ろうとしている，許可を受けた人物であると仮定する。ＡｕｔｈｅｎｔｉＳｗａｔｃｈ１００の生体認証データ読み取り器を起動することにより，使用者は，自分の身元をセキュリティドア５１０に隣接する相手方装置５００に伝送することができる。そして，安全確保エリアに関連するセキュリティシステムは，有効に識別された使用者が許可を受けた人物であるか否かを判断する。」

３．原審拒絶査定において，周知技術を例示するために示された，本願の第１

国出願前に既に公知である，特開２００１－１９５１４５号公報（２００１年７月１９日公開，以下，これを「周知文献」という）には，関連する図面と共に，次の事項が記載されている。

Ｈ．「【００１２】
【発明の実施の形態】以下に添付図面を参照して，この発明にかかる情報処理装置，個人認証方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体の好適な実施の形態を詳細に説明する。
（情報処理システムの構成）図１は，本実施の形態にかかる情報処理装置を含む個人認証システムの構成例を示す説明図である。図１において，外部装置（パーソナルコンピュータ）１００と，情報処理装置（腕時計型情報処理装置）１０１と，から構成される。
【００１３】外部装置１００は，パーソナルコンピュータのほか，携帯電話，ＰＤＡや，ドア・個人用の金庫・かばん・財布等の開閉をおこなうロック機構システム，各種システムの主電源のオン／オフ制御機構システム，家電製品の制御システム，自動車のドア・トランク・給油口の開閉をおこなうロック機構システム等，操作に認証が必要なシステムが考えられる。
【００１４】また，情報処理装置（腕時計型情報処理装置）１０１は，外部装置１００との間の短距離無線通信をおこなう。情報処理装置１０１は，本実施の形態においては腕時計型の情報処理装置であるので，通常，所有者（使用者）が常に腕に着用しており，それにより，所有者（使用者）と外部装置１００との距離が，短距離無線通信が可能な距離にあるのか否かを判断することもできる。」

Ｉ．「【００２５】送信部３０５は，セキュリティーの高いデジタル通信であり，たとえば，スペクトラム拡散方式等をもちいることできる。さらに，データ自体を暗号化するようにしてもよい。送信部３０５は，図２に示したＩ／Ｆ２０５によりその機能を実現することができる。また，着脱検出部３０８は，腕時計型情報処理装置１０１を腕から外したことを検知する。具体的には，着脱センサ２０４によりその機能を実現する。着脱センサ２０４としては，たとえば，温度センサ（たとえば，体温を認識し，着脱の際の温度変化を検知する），圧力センサ（たとえば，腕との密着度を認識し，着脱の際の密着度に基づく圧力を検知する），脈波センサ（たとえば，着脱の際の脈波の有無を検知する），光センサ（たとえば，着用することにより遮断される光を検知する）等をもちいることができる。
【００２６】着脱センサ２０４により腕時計型情報処理装置１０１が腕から外されたことを検知した場合は，その情報を送信部３０７から外部装置１００へ送信し，後述する認証を無効にする。これにより，腕時計型情報処理装置１０１が盗難等にあった場合でも，外部装置１０１のセキュリティーを担保することができる。また，外部装置１００は，受信部３０９と，更新情報記憶部３１０と，認証部３１１と，を含む構成である。ここで，受信部３０９は，情報処

理装置１０１から送信された認証用データ，さらには照合日時に関する情報のうち最新の情報を受信する。さらに受信したデータをデコードする。受信部３０９は，図示は省略するが，図２に示したＩ／Ｆ２０５と同様のハードウエアによりその機能を実現することができる。」

第５．引用文献１に記載の発明
１．上記Ａの「汎用装置を，腕時計として実施する。この腕時計を，認証されたユーザに対し無線トランザクションを補助するように構成し，かつ認証されたユーザの一部を取り巻くよう，認証されたユーザが着用するように，構成する」という記載，上記Ｂの「腕時計１００は，１つまたは複数のアプリケーションと，セキュア認証／識別データと，トランザクションデータと，をホストするとともに，使用ベース状況セキュリティ確認方式を実行することにより合法のユーザによる腕時計１００の使用および所有を確認することができる，電子回路５０を備える」という記載，及び，上記Ｄの「ユーザは腕時計１００を着用する。さらに，ブロック３２０において，ユーザは，セキュリティ初期化手続きを踏む。この手続きは，認証されたユーザに対して種々の無線トランザクションを補助する腕時計１００のアプリケーションホスティング機能を，ユーザが一般的に運用することを可能にする前に，ユーザを認証する。初期化手続きは，単純な腕時計ベースの動作（たとえば，腕時計自体にＰＩＮ番号を入力する）であってもよく，あるいは，ブロック３２５における外部セキュリティシステムを含むより複雑なセキュリティ手続き（たとえば，網膜スキャンハードウェアを備えた外部装置を使用して，一意のユーザ確認を提供することができ，これを暗号化ＲＦデータ通信リンク３０２を介して腕時計１００に伝送する）であってもよい。いかなる初期化方法が選択されても，そのタスクは，ユーザと腕時計１００のストラップに統合されたデータチャネル８０との両方を確認することにより，腕時計１００の認証された使用を起動することである」という記載，同じく，上記Ｄの「ユーザが認証されると，腕時計１００は，アクティブ／セキュアステータス状態に入り（ブロック３３０），無線トランザクションおよびサービスを補助するように構成された１つまたは複数のアプリケーションの実行を開始する」という記載から，引用文献１においては，
“腕時計として実施する汎用装置であって，ユーザを認証するセキュア認証をホストする電子回路を備え，前記ユーザが認証されると，前記腕時計は，アクティブ／セキュアステータス状態に入”るものであることが読み取れる。

２．上記Ａの「腕時計自体のストラップ内にデータチャネルを統合することにより，腕時計の使用を開始した認証されたユーザによりその腕時計が着用されているか否かの確認が可能になる。腕時計を取り外すことにより，その状況セキュリティが無効になって時計が非アクティブ状態になり」という記載，上記Ｂの「腕時計１００は，認証されたユーザが腕時計１００の使用を開始した後にその腕時計１００を着用し続けるか否かに基づいて腕時計１００の使用を制御する確認メカニズムを含む。確認メカニズムは，送信要素４０と，受信要素３０と，データチャネル８０と，データチャネル８０のステータスを監視する

監視コンポーネント（電子回路５０に組み込まれている）と，を備える」という記載，同じく，上記Ｂの「腕時計１００がその腕時計１００の使用を開始した認証されたユーザによって着用されているか否かの確認を可能にする，データチャネル８０が統合されている。腕時計１００を取り外すことにより，その状況セキュリティが無効になって腕時計は非アクティブ状態となり，無線リンクを介するすべての外部対話が不可能になる」という記載，上記Ｃの「腕時計１００には，腕時計１００自体の第１および第２のストラップ１０および２０内に，腕時計１００がその腕時計１００の使用を開始した認証されたユーザによって着用されているか否かの確認を可能にする，データチャネル８０が統合されている。腕時計本体９０は，埋込み電子機器サブシステム５０と，データチャネル８０を通してデータを送信する送信要素４０と，データチャネル８０を通して送信されたデータを受信する受信要素３０と，認証されたユーザが腕時計１００を着用しているか否かを検知する任意のバイオセンサ７０と，を有する。送信要素４０と受信要素３０との間のデータの正常な伝送は，腕時計１００が認証されたユーザによって着用されていることを示す。さらに，データチャネル８０を，認証されたユーザが腕時計１００の着用を停止する場合に動作不能とされるように構成する」という記載，上記Ｄの「データチャネル８０自体の完全性に加えて，生体認証測定技術（たとえば，皮膚温度，光反射，湿度）を使用して，認証されたユーザの身体が存在するか存在しないかを検出する機能を提供する，任意のバイオセンササブシステム７０および７１を使用することによって，セキュリティを強化することができる」という記載，同じく，上記Ｄの「認証されたユーザが腕時計１００を取り外したことを示してデータチャネルが動作不能となったために，アクティブ／セキュアステータス状態の変化が検出されると，腕時計１００は，そのアクティブ／セキュアステータス状態およびアプリケーションデータを消去し（ブロック３６０）その後非アクティブ状態すなわちオフに切り替わる（ブロック３６５）」という記載，及び，同じく，上記Ｄの「任意のバイオセンシングサブシステム（ブロック３４０）は，ユーザの存在を，データチャネル８０のステータスおよび完全性の監視に対する補足として確定することにより，追加のレベルのセキュリティを提供する」という記載から，引用文献１においては，
“腕時計本体は，前記腕時計の使用を開始した認証されたユーザによりその腕時計が着用されているか否かの確認を可能にするデータチャネルと，認証された前記ユーザの身体が存在するか存在しないかを検出する機能を提供するバイオセンサと，を有し，前記腕時計を取り外すことにより，その状況セキュリティが無効になって前記腕時計は非アクティブ状態となり，無線リンクを介するすべての外部対話が不可能になるよう構成される”ものであることが読み取れる。

３．上記Ｂの「腕時計１００は，その腕時計１００がアクティブ／セキュアステータス状態にあるかまたは非アクティブ状態にあるかに基づき，無線リンクを介して任意の外部サービス対話を受け入れるかまたは拒否することができる」という記載，上記１．に引用した上記Ｄの記載内容，同じく，上記Ｄの「外部

装置によって腕時計１００に対し，情報を要求するかまたは腕時計１００によってホストされる特定のアプリケーションによってサポートされる無線トランザクションを開始するために問合せがなされると，ブロック３８０において，その特定のアプリケーションは，腕時計１００がアクティブ／セキュアステータス状態で動作しているか否かをチェックする」という記載，同じく，上記Ｄの「動作している場合，特定のアプリケーションは，ブロック３８５において，問合せの妥当性をチェックする」という記載，及び，同じく，上記Ｄの「有効である場合，ブロック３９５において，特定のアプリケーションは，その特定のアプリケーションがサポートする所望のサービスまたはトランザクションを実行する」という記載から，引用文献１においては，
“ユーザが認証されると，腕時計は，アクティブ／セキュアステータス状態に入り，前記アクティブ／セキュアステータス状態で，外部装置によって前記腕時計に対し，情報を要求するかまたは前記腕時計によってホストされる特定のアプリケーションがサポートする無線トランザクションを開始するために問合せがなされると，問合せの妥当性をチェックし，前記問合せが有効である場合，前記特定のアプリケーションは，前記特定のアプリケーションがサポートする無線トランザクションを実行する”ものであることが読み取れる。

４．以上，上記１．～３．において検討した事項から，引用文献１には，次の発明（以下，これを「引用発明」という）が記載されているものと認める。

「腕時計として実施する汎用装置であって，ユーザを認証するセキュア認証をホストする電子回路を備え，前記ユーザが認証されると，前記腕時計は，アクティブ／セキュアステータス状態に入るものであって，
　前記腕時計本体は，前記腕時計の使用を開始した認証されたユーザにより前記腕時計が着用されているか否かの確認を可能にするデータチャネルと，
　認証された前記ユーザの身体が存在するか存在しないかを検出する機能を提供するバイオセンサと，を有し，
　前記腕時計を取り外すことにより，その状況セキュリティが無効になって前記腕時計は非アクティブ状態となり，無線リンクを介するすべての外部対話が不可能になるよう構成され，
　前記アクティブ／セキュアステータス状態のとき，外部装置によって前記腕時計に対し，情報を要求するかまたは前記腕時計によってホストされる特定のアプリケーションがサポートする無線トランザクションを開始するために問合せがなされると，前記問合せの妥当性をチェックし，前記問合せが有効である場合，前記特定のアプリケーションは，前記特定のアプリケーションがサポートする無線トランザクションを実行する，腕時計として実施する汎用装置。」

第６．本願発明と引用発明との対比
１．引用発明における「腕時計として実施する汎用装置」は，「ユーザ」が，「認証」された状態が維持されているときに「トランザクション」を実行するものであるから，

本願発明における「トラステッドデバイス」に相当する。

２．引用発明においては，「ユーザ」は「腕時計」を装着している状態で「認証」され，「ユーザ」が「認証」されると「アクティブ／セキュアステータス状態」になるものであるから，
引用発明における「腕時計」が，「アクティブ／セキュアステータス状態」となることが，
本願発明における「トラステッドデバイスを認証済み状態に切り替える」ことに相当するので，
引用発明における「ユーザが認証されると，前記腕時計は，アクティブ／セキュアステータス状態に入る」ことが，
本願発明における「それによって，前記トラステッドデバイスを認証済み状態に切り替える」ことに相当し，
引用発明において，「腕時計」が有する「電子回路」は，「ユーザを認証するセキュア認証をホストする」ものであって，それによって，「腕時計」が，「アクティブ／セキュアステータス状態」に移行するのであるから，
引用発明における「電子回路」が，
本願発明における「認証回路」に相当し，
上記で指摘した“「ユーザ」が，「腕時計」を装着している状態で「認証」される”ということは，
“ユーザが物理的に腕時計を所持している状態を認証する”ことにほかならないので，
引用発明における「腕時計として実施する汎用装置であって，ユーザを認証するセキュア認証をホストする電子回路を備え，前記ユーザが認証されると，前記腕時計は，アクティブ／セキュアステータス状態に入るもの」が，
本願発明における「認証動作によって，前記トラステッドデバイスを物理的に所持しているユーザを認証し，それによって，前記トラステッドデバイスを認証済み状態に切り替えるように構成されている認証回路」に相当する。

３．引用発明において，「データチャネル」は，「腕時計の使用を開始した認証されたユーザにより前記腕時計が着用されているか否かの確認を可能にする」ものであって，
引用発明において，「腕時計の使用を開始した認証されたユーザにより前記腕時計が着用されているか否かの確認」することが，
本願発明における「認証動作に従って，前記ユーザによる前記トラステッドデバイスの物理的所持をモニタリング」することに相当し，
引用発明において，「腕時計を取り外すことにより，その状況セキュリティが無効になって前記腕時計は非アクティブ状態とな」ることが，
本願発明における「トラステッドデバイスが前記ユーザによってもはや物理的に所持されていない場合，前記トラステッドデバイスを前記認証済み状態から脱して切り替える」に相当し，
引用発明における「データチャネル」が，“腕時計の使用を開始した認証さ

れたユーザにより前記腕時計が着用されていない”ことを「確認」することで，「ユーザ」が「腕時計を外」したことを検出し，それによって，“セキュリティが無効になって腕時計が非アクティブ状態になる”のであるから，

引用発明における「データチャネル」は，“腕時計の使用を開始した認証されたユーザが，前記腕時計を外したことを検出した場合に，腕時計を非アクティブにする”態様を含むものである。

したがって，上記検討の，

引用発明における“腕時計の使用を開始した認証されたユーザが，前記腕時計を外したことを検出した場合に，腕時計を非アクティブにするデータチャネル”が，

本願発明における「認証動作に従って，前記ユーザによる前記トラステッドデバイスの物理的所持をモニタリングし，前記トラステッドデバイスが前記ユーザによってもはや物理的に所持されていない場合，前記トラステッドデバイスを前記認証済み状態から脱して切り替えるように構成されている，保持モニタリング回路」に相当する。

４．引用発明における「外部装置」と，

（１）本願発明における「複数の異なる目標デバイスの１つである目標デバイス」とは，“外部デバイス”である点で共通し，

引用発明における「外部装置によって前記腕時計に対し，情報を要求するかまたは前記腕時計によってホストされる特定のアプリケーションがサポートする無線トランザクションを開始するために問合せ」と，

本願発明における「複数の異なる目標デバイスの１つである目標デバイスから受信される，通信を確立することを求める要求」とは，

“外部デバイスから受信される，通信を確立することを求める要求”である点で共通する。

（２）引用発明において「問合せがなされると，前記問合せの妥当性をチェックし」ていることから，引用発明において，「腕時計」内のいずれかの構成が，前記「問合せ」が受信されたことを「検出」していることは明らかであるので，引用発明においても，前記「腕時計」内のいずれかの構成が，前記「問合せ」を「検出」するための「検出手段」であることは明らかである。

したがって，引用発明における「外部装置によって前記腕時計に対し，情報を要求するかまたは前記腕時計によってホストされる特定のアプリケーションがサポートする無線トランザクションを開始するために問合せがなされると，前記問合せの妥当性をチェック」する「検出手段」と，

本願発明における「複数の異なる目標デバイスの１つである目標デバイスから受信される，通信を確立することを求める要求を検出するように構成されている通信トリガ回路」とは，

“外部デバイスから受信される，通信を確立することを求める要求を検出するように構成されている通信トリガ回路”である点で共通する。

（３）引用発明においては，「問合せが有効である場合，前記特定のアプリケーションは，前記特定のアプリケーションがサポートする無線トランザクショ

ンを実行する」ものであって，このことは，「外部装置」との「通信」を行うことに他ならず，このことから，「腕時計」が，「外部装置」との間で「通信」を行うための「通信回路」を有していることは明らかである。
　そして，当該“外部装置との通信”は，“腕時計が，アクティブ／セキュアステータス状態のとき”に行われるものであり，
　引用発明における「アクティブ／セキュアステータス状態」が，
　本願発明における「トラステッドデバイスが前記認証済み状態」に相当するので，
　引用発明における「問合せが有効である場合，前記特定のアプリケーションは，前記特定のアプリケーションがサポートする無線トランザクションを実行する」と，
　本願発明における「トラステッドデバイスが前記認証済み状態にある場合に，前記目標デバイスと通信するように構成されている通信回路」とは，
“トラステッドデバイスが前記認証済み状態にある場合に，外部デバイスと通信するように構成されている通信回路”である点で共通する。

５．以上，上記１．～上記４．において検討した事項から，本願発明と，引用発明との一致点，及び，相違点は，次のとおりである。

［一致点］
　トラステッドデバイスであって，
　認証動作によって，前記トラステッドデバイスを物理的に所持しているユーザを認証し，それによって，前記トラステッドデバイスを認証済み状態に切り替えるように構成されている認証回路と，
　前記認証動作に従って，前記ユーザによる前記トラステッドデバイスの物理的所持をモニタリングし，前記トラステッドデバイスが前記ユーザによってもはや物理的に所持されていない場合，前記トラステッドデバイスを前記認証済み状態から脱して切り替えるように構成されている，保持モニタリング回路と，
　外部デバイスから受信される，通信を確立することを求める要求を検出するように構成されている通信トリガ回路と，
　前記トラステッドデバイスが前記認証済み状態にある場合に，前記外部デバイスと通信するように構成されている通信回路とを備える，トラステッドデバイス。

［相違点１］
“保持モニタリング回路”に関して，
　本願発明においては，「トラステッドデバイスが前記ユーザによって所持されているときに光から遮蔽される光検出器を含む一つ以上の検出回路を備える，前記保持モニタリング回路」であるのに対して，
　引用発明においては，「ユーザによって所持されているときに光から遮蔽される光検出器を含む一つ以上の検出回路を備える」ことについては，言及されていない点。

［相違点２］について
“外部デバイス”に関して，
　本願発明においては，「複数の異なる目標デバイスの１つである目標デバイス」であるのに対して，
　引用発明においては，「外部装置」である点。

第７．相違点についての当審の判断
１．［相違点１］について
　上記Ｈ，及び，上記Ｉに引用した周知文献の記載内容にもあるとおり，“腕時計型情報処理装置の着脱を，着用することにより遮断される光を検出する光センサを用いる”こと（上記Ｈ，及び，上記Ｉの下線を付加した記載等を参照）は，本願の第１国出願前に当業者には，周知の技術事項であり，引用発明と，周知文献に記載の「腕時計型情報処理装置」とは，ほぼ同様の構成を有するものであって，引用発明においても，上記Ｅに引用した記載にもあるとおり，方式は異なるものの「光」を用いて，「ユーザ」の「腕時計」の着脱の検出を行っているので，
　引用発明において，上記Ｅに引用した記載に変えて，周知文献に記載の「光センサ」を用いて，「腕時計」の着脱を検出するよう構成することは，当業者が適宜なし得る事項である。
　よって，［相違点１］は，格別のものではない。

２．［相違点２］について
　上記Ｆ，及び，上記Ｇに引用した引用文献２には，
“生体認証データを用いて認証された正しい使用者が，装着することによって有効になる腕時計型の装置（本願発明における「トラステッドデバイス」に相当）において，複数の異なる無線トランザクション装置（本願発明における「目標デバイス」に相当）と，無線通信を行う”ことが記載されていて，本願の第１国出願前において，「複数の異なる目標デバイスの１つである目標デバイスから受信する」こと（上記Ｆ，及び，上記Ｇの下線を付加した記載等参照）は，当業者には周知の技術事項である。
　引用発明と，引用文献２に記載の技術事項とは，“認証を行った後に，正当なユーザが装着した場合に使用可能となる装置であって，外部の装置と無線通信を行うもの”である点で共通し，引用発明における「外部装置」には，特に限定がないので，引用発明において，「外部装置」として，“複数の異なる外部装置の１つである外部装置から受信される，通信を確立する”よう構成することは，当業者が適宜なし得る事項である。
　よって，［相違点２］は，格別のものではない。

３．上記１．，及び，２．に検討したとおりであるから，［相違点１］，及び，［相違点２］は，いずれも格別のものではなく，そして，本願発明の構成によってもたらされる効果も，当業者であれば容易に予測できる程度のものであっ

て，格別なものとは認められない。

第８．３６条６項２号について
　平成３１年４月２２日付けの手続補正によって補正された請求項（以下，これを「本願の請求項」という）３に，
「・・・認証プロセスにおいて使用可能なクレデンシャルの作成を含む」，
　と記載されているが，当該「クレデンシャルの作成」をどのように実現しているのか，本願の請求項３，及び，本願の他の請求項に記載の内容を検討しても，依然として不明である。

第９．むすび
　したがって，本願発明は，引用発明，引用文献２に記載の技術事項，及び，周知文献に記載の技術事項に基づいて当業者が容易に発明をすることができたものであるので，特許法２９条２項の規定により特許を受けることができない。
　加えて，本願は，特許法３６条６項２号に規定する要件を満たしていない。

　よって，結論のとおり審決する。

　　令和　２年　４月２２日

審判長　特許庁審判官　田中 秀人
特許庁審判官　石井 茂和
特許庁審判官　山崎 慎一

（行政事件訴訟法第４６条に基づく教示）
　この審決に対する訴えは，この審決の謄本の送達があった日から３０日（附加期間がある場合は，その日数を附加します。）以内に，特許庁長官を被告として，提起することができます。

審判長　田中　秀人
　出訴期間として在外者に対し９０日を附加する。

〔審決分類〕Ｐ１８．１２１－Ｚ（Ｇ０６Ｆ）
５３７

　審判長　特許庁審判官　田中　秀人　9066
　特許庁審判官　山崎　慎一　9174
　特許庁審判官　石井　茂和　8837