令和元年１２月２５日判決言渡　同日原本交付　裁判所書記官

平成３０年（ワ）第３９９１４号　特許権侵害に基づく損害賠償請求事件

口頭弁論終結日　令和元年１０月３０日

判　　決

原　　告	株式会社モビリティ
同訴訟代理人弁護士	飯　田　秀　郷
	隈　部　泰　正
	清　水　紘　武
	保　志　周　作
同訴訟代理人弁理士	黒　田　博　道
被　　告	シャープ株式会社
同訴訟代理人弁護士	生　田　哲　郎
	名　越　秀　夫
	高　橋　隆　二
	佐　野　辰　巳
	吉　浦　洋　一

主　　文

１　原告の請求を棄却する。

２　訴訟費用は原告の負担とする。

事　実　及　び　理　由

第１　請求

被告は，原告に対し，１億円及びこれに対する平成３０年１月１日から支払済みまで年５分の割合による金員を支払え。

第２　事案の概要

１　本件は，その発明の名称を「携帯電話，Ｒバッジ，受信装置」とする特許第４７８９０９２号（以下「本件特許」という。）に係る特許権（以下「本件特

許権」という。）を有する原告が，別紙物件目録記載の各スマートフォン（以下「被告製品」という。）は，本件特許の特許請求の範囲の請求項１に係る発明（後記２(3)イによる訂正後のもの。以下「本件発明」という。）の技術的範囲に属し，被告は被告製品を製造・販売等することにより本件特許権を侵害したとして，民法７０９条に基づき，損害額の一部である１億円及びこれに対する最後の出荷日の後の日である平成３０年１月１日から支払済みまで民法所定の年５分の割合による遅延損害金の支払を求める事案である。

２　前提事実（当事者間に争いのない事実又は文中に掲記した証拠及び弁論の全趣旨により認定できる事実。なお，本判決を通じ，証拠を摘示する場合には，特に断らない限り，枝番を含むものとする。）

(1) 当事者

原告は，情報処理に関する研究，開発及びソフトウェア，ハードウェアの開発，制作及び販売等を業とする株式会社であり（乙７），被告は，通信機械器具の製造・販売等を業とする株式会社である。

(2) 原告の特許権

原告は，以下の本件特許権を有している（甲１，２）。

登録番号：第４７８９０９２号

発明の名称：「携帯電話，Ｒバッジ，受信装置」

出願日：平成２０年５月７日（特願２００２－５８２４５１の分割）

原出願日：平成１４年４月１７日

優先日：平成１３年４月１７日

優先権主張国：日本

登録日：平成２３年７月２９日

(3) 特許請求の範囲の記載

ア　本件特許に係る特許請求の範囲における請求項１（後記イによる訂正後のもの）は，以下のとおりである（以下，同訂正後の特許明細書及び図面

（甲２）を「本件明細書等」という。）。

「ＲＦＩＤインターフェースを有する携帯電話であって，当該携帯電話のスイッチを押すことで生成されるトリガ信号又はリーダライタから送信されるトリガ信号を，当該携帯電話の所有者が第三者による閲覧や使用を制限し，保護することを希望する被保護情報に対するアクセス要求として受け付ける受付手段と，前記トリガ信号に応答して，Ｒバッジに対して要求信号を送信する送信手段と，前記Ｒバッジより識別情報を受け取って，該受け取った識別情報と当該携帯電話に予め記録してある識別情報との比較を行う比較手段と，前記比較手段による比較結果に応じて前記受付手段で受け付けた前記アクセス要求を許可または禁止するアクセス制御手段とを備え，前記アクセス制御手段は，当該比較手段で前記アクセス要求を許可するという比較結果が得られた場合は，前記アクセス要求が許可されてから所定時間が経過するまでは前記被保護情報へのアクセスを許可することを特徴とする携帯電話。」

イ　上記アの下線部は，確定した平成３１年１月２９日付け審決（甲１３）によって訂正（以下「本件訂正」という。）が認められた部分であり，これにより「前記アクセス要求から」は「前記アクセス要求が許可されてから」と訂正された。なお，これに併せて，本件明細書等の段落【００１１】の「前記アクセス要求から」という記載も「前記アクセス要求が許可されてから」と訂正された。

(4) 構成要件の分説

Ａ　ＲＦＩＤインターフェースを有する携帯電話であって，

Ｂ　当該携帯電話のスイッチを押すことで生成されるトリガ信号又はリーダライタから送信されるトリガ信号を，当該携帯電話の所有者が第三者による閲覧や使用を制限し，保護することを希望する被保護情報に対するアクセス要求として受け付ける受付手段と，

C　前記トリガ信号に応答して，Rバッジに対して要求信号を送信する送信手段と，

D　前記Rバッジより識別情報を受け取って，該受け取った識別情報と当該携帯電話に予め記録してある識別情報との比較を行う比較手段と，

E　前記比較手段による比較結果に応じて前記受付手段で受け付けた前記アクセス要求を許可または禁止するアクセス制御手段とを備え，

F　前記アクセス制御手段は，当該比較手段で前記アクセス要求を許可するという比較結果が得られた場合は，前記アクセス要求が許可されてから所定時間が経過するまでは前記被保護情報へのアクセスを許可する

G　ことを特徴とする携帯電話。

(5) 被告の行為

被告は，携帯電話会社各社に対し，被告製品を販売し，これらの携帯電話会社各社は，それぞれ平成２９年２月９日から同年７月７日にかけ，一般消費者に対し，被告製品の販売を開始した。

(6) 被告製品の構成

原告は，被告製品の概要は，別紙被告製品説明書記載１(1)のとおりであると説明し，被告製品が，同(2)の条件（以下「本件前提条件」という。）の下で，同(3)の構成ａ～ｇを備えると主張し，被告は，被告製品の構成は，同説明書記載２の構成(a)～(g)のとおりであると主張する。

(7) 先行文献等

ア　本件特許の優先日前に，以下の公開特許公報が存在した。

(ｱ)　発明の名称を「電子機器及びその制御方法」とする特開平１１－５５２４６号の公開特許公報（乙１１。以下「乙１１公報」といい，同公報に記載された発明を「乙１１発明」という。）

(ｲ) 発明の名称を「携帯情報機器」とする特開平１０－１３９４２号の公開特許公報（乙１２。以下「乙１２公報」といい，同公報に記載された

発明を「乙１２発明」という。）

(ｳ) 発明の名称を「自動車電話端末装置」とする特開平３－６０５４３号の公開特許公報（乙１３。以下「乙１３公報」といい，同公報に記載された発明を「乙１３発明」という。）

(ｴ) 発明の名称を「携帯電話機」とする特開２０００－２９５３４１号の公開特許公報（乙１４。以下「乙１４公報」といい，同公報に記載された発明を「乙１４発明」という。）

(ｵ) 発明の名称を「携帯端末装置」とする特開２０００－３１２３８２号の公開特許公報（乙１５。以下「乙１５公報」という。）

(ｶ) 発明の名称を「カード類の所有権確認方法」とする特開平４－３０６７６０号の公開特許公報（乙１７。以下「乙１７公報」という。）

イ　発明の名称を「携帯電話機の自動ダイヤルロックシステム」とする特開２００１－２４５３５４号は，本件発明の優先日前である平成１２年３月１日に出願され，平成１３年９月７日に公開された特許出願に係る公開特許公報（乙１６。以下「乙１６公報」といい，同公報に記載された発明を「乙１６発明」という。）である。

３　争点

(1) 被告製品の構成（争点１）

(2) 構成要件充足性

ア　構成要件Ｅ及びＦの「アクセス制御手段」の具備の有無（争点２－１）

イ　構成要件Ｂ及びＦの「被保護情報」の具備の有無（争点２－２）

ウ　構成要件Ｂ及びＣの「トリガ信号」及び構成要件Ｂ，Ｅ及びＦの「アクセス要求」の具備の有無（争点２－３）

エ　構成要件Ｄ，Ｅ及びＦの「比較手段」の具備の有無（争点２－４）

オ　構成要件Ｃ及びＤの「Ｒバッジ」の具備の有無(争点２－５）

(3) 無効理由の存否

ア　訂正要件違反（争点３－１）

イ　乙１１発明に基づく進歩性の欠如（争点３－２）

ウ　乙１６発明に基づく拡大先願違反（争点３－３）

(4) 損害額（争点４）

第３　当事者の主張

１　被告製品の構成（争点１）

(原告の主張)

(1) 本件前提条件

被告製品は，オペレーティングシステムの下に動作する情報機器であり，プログラム上の種々の設定や条件に従って動作・機能するものであるが，ある特定の設定や条件の下で本件発明の全ての構成要件を充足すれば，本件発明の技術的範囲に属する。被告製品が他の条件の下で動作した場合に本件発明の構成要件を充足しないことがあるとしても，それは被告製品が本件特許を侵害しているという結論を左右するものではない。

(2) 構成ｂ

被告製品の電源キーが押下されると，画面表示信号が出力され，画面ロックを解除するためのロック画面が表示されるから，当該信号は，構成ｂにおける「ロック画面表示信号」であって，構成要件Ｂにいう「トリガ信号」にも相当する。そして，トリガ信号を受信した被告製品は，画面ロック解除を実行するプログラムに同信号を受け渡し，その解除プロセスを進行させることになる。このため，被告製品は，「画面ロック解除プロセスを実行するプログラムに対して，当該トリガ信号を画面ロック解除の要求として受け付けて当該プログラムに受け渡す受付手段」を有するということができる。

したがって，被告製品は，構成ｂを備える。

(3) 構成ｃ

被告製品では，電源キーを押下しないと，ロック画面が表示されることは

なく，電源キーを押下しロック画面が表示されたとき，ＮＦＣインターフェースに基づく通信が，被告製品と登録済ＩＣカード（ＮＦＣ）との間で行われる。当該通信は，「トリガ信号（ロック画面表示信号）」に応答して行われる通信であり，ＩＣカード（ＮＦＣ）に対し，格納されているＩＤ情報などの識別情報を送信することを要求する信号である。

したがって，被告製品は，「前記トリガ信号（ロック画面表示信号）に応答して，ＩＣカードに対して識別情報を要求する信号（ＮＦＣの信号）を送信する送信手段」（構成ｃ）を備えている。

(4) 構成ｄ

被告製品が，ＩＣカードに記憶された識別情報を用い，当該ＩＣカードが登録済ＩＣカード（ＮＦＣ）であるか否かを比較することは当事者間に争いがない。そうである以上，被告製品が，そのための比較手段を備えることも明らかである。

したがって，被告製品は構成ｄを備える。

(5) 構成ｅ

被告製品において，構成ｄの比較の結果が一致していれば，画面ロックが解除され，画面を介しての操作が可能となり，比較の結果が一致していなければ，画面ロックが解除されず，ロック画面のままであることは当事者間に争いがない。このように，画面ロックを解除し，画面を介した操作を可能にするような制御を行う手段は「画面ロック解除制御手段」ということができるので，被告製品は，構成ｅを備える。

(6) 構成ｆ

被告製品において，画面ロック解除後，無操作状態が所定時間経過するまで，画面を介しての操作が可能となり，これが所定時間継続すると，画面の表示が消え，画面を介しての操作が行うことができなくなる。

したがって，被告製品は，構成ｆを備える。

（被告の主張）

（1）本件前提条件

本件前提条件のうち，条件①については，被告が携帯電話会社に販売する時はＳＩＭカードは装着されていないので，妥当しない。また，条件②～⑤は，ユーザによる被告製品の使用方法にすぎないのであり，被告製品の構成はその使用方法とは関係なく特定されるべきである。

（2）構成ｂ

被告製品は，構成ｂにいう「トリガ信号（ロック画面表示信号）」は出力しない。被告製品において，電源キーの押下の際に出力される信号は一種類の「画面表示信号」であり，その際，画面ロック機能が設定されている場合であれば，ロック画面が表示されるものの，それが設定されていない場合においては，直近に表示されていた画面が表示される。このため，被告製品において，ロック画面表示信号が出力されたとしても，ロック画面又は直近に表示されていた画面が表示されることによって，その処理が終了するのであり，原告が主張するような「画面ロック解除プロセス」は進行しない。

また，画面ロックを解除するかどうかは，構成ｄにおける比較結果に基づくものである。そのような比較をしない段階で，携帯電話のスイッチを押すことで生成されるロック画面表示信号を画面ロック解除要求として処理するのでは画面ロック機能としての意味がない。

（3）構成ｃ

構成(c)のとおり，被告製品において，所定の設定条件を満たされた場合，ＮＦＣの信号がＩＣカードに送信されることは認めるが，これはグーグル社が開発し，提供する機能によるものであり，被告は，その具体的な設定条件を知らない。

（4）構成ｄ

被告製品は，構成(d)のとおり，ＩＣカードの識別情報を受信し，何らかの

比較をするものであるが，これはグーグル社が開発し，提供する機能によるものであり，被告は，その具体的な処理方法を知らない。

(5) 構成ｅ

被告製品では，画面ロックを解除することで，画面を介しての操作が可能となることは認める。ただし，画面ロック状態であっても，電話帳，着信履歴，写真など，各種データなどにアクセスすることは可能である。

(6) 構成ｆ

被告製品では，構成(f)のとおり，画面が表示されてから，又は画面に対する何らかの操作が行われた時点から，無操作状態が一定時間経過するまでは画面を介しての操作が可能である。原告が主張するように，画面ロックを解除した時点から，無操作状態が所定時間を経過するまで操作ができるものではないので，構成ｆを備えない。

２　構成要件充足性

(1) 構成要件Ｅ及びＦの「アクセス制御手段」の具備の有無（争点２－１）

（原告の主張）

被告製品では，構成ｄの「画面ロック解除制御手段」によって，画面ロックが解除されるまで，画面を介した操作で端末内情報の閲覧や使用ができず，他方，画面ロックが解除されると，アクセスが許可された状態になる。すなわち，画面ロックが解除されることは，「アクセス要求」（画面ロック解除要求）に対する許可に相当し，その要求にもかかわらず，画面ロック状態のままであることは，これに対する禁止に相当するので，被告製品の「画面ロック解除制御手段」は，構成要件Ｅ及びＦの「アクセス制御手段」に相当する。

被告の指摘するとおり，被告製品は，画面ロック状態であっても，各種データに全くアクセスできないわけではないが，電話帳や着信履歴，電子メール，スケジュールのデータについては，かかる一定の情報が，そのような設

定をしたときにロック画面に表示されるにすぎず，画面を介した操作により端末内情報を閲覧し，又は使用することが可能になるものではない。

また，画面ロックを解除することなくカメラ機能を起動して撮影し，撮影したデータを表示・保存できることについても，ロック画面が表示された時点で格納されているアルバム内の多数の写真を閲覧したり使用したりできるものではなく，画面を介した操作で端末内情報の閲覧や使用ができないことに変わりはない

（被告の主張）

本件発明にいう「アクセス制御手段」とは，本件明細書等の段落【００３８】，【００３９】，【図４】の自動改札機の例でいえば，携帯端末をＲバッジに近づけて認証させ，同端末の乗車券のデータに対するアクセス要求が許可された後，これを自動改札機にかざすことで，改札機を通ることができるというように機能し，被保護情報に対するアクセス要求を制御することで，その不正使用を確実に防止するものである。

このような不正使用は，個人情報やデータへの読出しや書込みによって行われるものであるから，本件発明「アクセス」は，被保護情報の「データやプログラムの読出し，書き込みをすること」を意味すると解すべきであるところ，被告製品では，画面ロック状態であっても，電話帳データや着信履歴データ，写真データ，電子メールデータ，スケジュールデータ，おサイフケータイの電子マネーのデータ，定期券や乗車券のデータ，録音データなどの読出しや書込みをすること，すなわち「アクセス」が可能である。

このように，被告製品にいう画面ロック機能は，端末内のデータを保護するものではなく，データを保護するためには，データの暗号化など，別の機能を用いる必要があるから，被告製品は，構成要件Ｅ及びＦの「アクセス制御手段」を具備していない。

(2) 構成要件Ｂ及びＦの「被保護情報」の具備の有無（争点２－２）

（原告の主張）

本件明細書等の段落【００２８】は，「被保護情報」を「所有者が第三者による閲覧や使用を制限し，保護することを希望する情報」であるとし，私的な住所録やドキュメント，画像データなどを例示する。そうすると，被告製品において，ロック画面が表示された時点で端末内に格納されていた電話帳，アルバム，メール，メッセージ，ラインなどの送受信情報は，構成要件Ｂ及びＦの「被保護情報」に当たる。

（被告の主張）

本件明細書等の段落【０００９】や【００２８】は，アクセスが許可されることによって，第三者による不正使用や悪用を防止することができるとし，構成要件Ｆは，アクセス要求が許可されるのは「所定時間」が経過するまでであるとする。そうすると，「被保護情報」とは，「アクセス要求が許可されるまではアクセスが禁止されている」ものでなければならないと解されるところ，前記のとおり，被告製品の端末内の電話帳や写真などのデータは，画面ロックがされた状態でもアクセスが可能であるから，構成要件Ｂ及びＦの「被保護情報」には該当しない。

(3) 構成要件Ｂ及びＣの「トリガ信号」及び構成要件Ｂ，Ｅ及びＦの「アクセス要求」の具備の有無（争点２－３）

（原告の主張）

構成要件Ｂは，「当該携帯電話のスイッチを押すことで生成されるトリガ信号…を，…被保護情報に対するアクセス要求として受け付ける受付手段と，」というものであるところ，被告製品において電源キーが押下されたときに出力されるロック画面表示信号は，構成要件Ｂの「トリガ信号」に該当する。そして，被告製品は，このロック画面表示信号を，ロック画面解除プロセス（解除プログラム）において，画面ロック解除要求として受け付けるところ，この画面ロック解除要求は，本件発明における，被保護情報に対す

るアクセス要求に相当する。

（被告の主張）

被告製品における「画面表示信号」は，直近表示画面又はロック画面を表示することでその処理を終了する。そして，被告製品でＩＣカードをその背面にかざして画面ロックを解除したとしても，「画面表示信号」に対する処理は，直近表示画面又はロック画面の表示処理によって終了しているから，既に処理が終了している「画面表示信号」に対して許可又は禁止することは，技術的にもあり得ない。そうすると，被告製品における「画面表示信号」は，構成要件Ｂ及びＣの「トリガ信号」には該当しない。

原告は，「ロック画面表示信号」なるものが「トリガ信号」であると主張しているが，そうすると，「ロック画面表示信号」が「アクセス要求」になるはずであるが，他方で，「画面ロック解除要求」が「アクセス要求」であるとも主張している。原告の主張は，「ロック画面表示信号」と「画面ロック解除要求」という異なる時系列における異なる信号又は要求が「アクセス要求」に該当するという技術的・論理的にあり得ない解釈である。

(4) 構成要件Ｄ，Ｅ及びＦの「比較手段」の具備の有無（争点２－４）

（原告の主張）

構成要件Ｄは，背面にかざされたＩＣカードからの識別情報と登録されたＩＣカードの識別情報との比較に当たり，何らかの演算を用いるか否かを含め，何ら限定をしていないから，両者を比較することにより，背面にかざされたＩＣカードが信頼できるＩＣカードとして登録されたものであるか否かを比較することができるものであれば足りる。

本件明細書等の段落【００２８】には，「暗号化したものなどを照合用データとして利用することができる」と記載されているので，携帯電話に予め記録されている識別情報が，Ｒバッジに格納された識別情報をハッシュ関数で暗号化したものであってもよい。本件発明の目的に照らすと，携帯電話に

予め記録してある識別情報とＲバッジの識別情報とが一意に関連付けられていれば，満たすべき所定の条件を設定し，その条件を満たすか否かを判定することはできるので，携帯電話に予め記録してある識別情報が，Ｒバッジに格納された識別情報を暗号化したものであってもよいし，Ｒバッジに格納された識別情報をハッシュ関数で演算した値としたものであってもよい。

被告製品は，ＩＣカードに記憶した識別情報を受信し，その識別情報を用いた何らかの方法により登録済みＩＣカードであるか否かの比較を行うものであるから，構成要件Ｄ及びＥの「比較手段」を充足する。

（被告の主張）

構成要件Ｄの文言上，その「比較手段」は，Ｒバッジから受け取った識別情報と事前に携帯電話に記録した識別情報とを比較するものである必要がある。他方，被告製品においては，ＩＣカードから受信した識別情報の比較方法として，様々な方法が想定されるのであり，ＩＣカードの識別情報についてハッシュ関数を利用してハッシュ化するなどして，ＩＣカードの識別情報を記憶せずに比較処理を実行する方法も考えられる。

原告は，被告製品における「比較手段」が，Ｒバッジから受け取った識別情報と事前に携帯電話に記録した識別情報とを比較するものであることを立証していないので，被告製品が構成要件Ｄ及びＥを充足しているということはできない。

(5) 構成要件Ｃ及びＤの「Ｒバッジ」の具備の有無（争点２－５）

（原告の主張）

ア　本件明細書等の段落【００１６】には「携帯電話との間で送受信するためのＲＦＩＤインターフェースを有し，前記携帯電話からの要求に応じて前記識別情報を送信する手段を有することを特徴とするＲバッジ」と記載されているので，本件発明の「Ｒバッジ」は，ＲＦＩＤ技術におけるＲＦタグを意味する。そして，同段落【００３３】には「ＩＣアセンブリを装

飾品や衣類など所有者の身近におくことが可能な物体に埋め込んだものを『Ｒバッジ』と総称する」などと記載されていることによれば，「Ｒバッジ」は，ＲＦタグとして機能するものであれば足りるというべきである。ＲＦＩＤインターフェースを備えるＩＣカードは，ＲＦタグの一種であるＮＦＣタグであり，身近に置くことができるものであるので，構成要件Ｃ及びＤの「Ｒバッジ」に当たる。

イ　原告は，その出願過程において，「Ｒバッジ」が，乙１７公報の「携帯物」に相当するという特許庁の認定を受け入れたにすぎず，ＩＣカードが本件発明のＲバッジに当たらないことまでを認めたものではない。

（被告の主張）

ア　本件明細書等において，「Ｒバッジ」は，「ＩＣアセンブリを装飾品や衣類など所有者の身近におくことが可能な物体に埋め込んだもの」をいうものと記載されているが，ＩＣカードは，イヤリング，ネクタイピン，財布などと異なり，身近に置くものではないので，「Ｒバッジ」には当たらない。また，本件明細書等の段落【０１３８】においては「ＩＣカード」と「レッドバッジ」との用語が明確に使い分けられているのであるから，「Ｒバッジ」にはＩＣカードは含まれない。

イ　原告は，本件特許の原出願の審査経過において，「第２アセンブリ」を「Ｒバッジ」に減縮した上，それが乙１７公報にいう「携帯物」（「例えば，時計，ネクタイピン，指輪，またはブローチ等の装身具を用いて，これらの装身具内に処理／記憶手段を埋め込んで作る」もの）と一致する旨の主張していた（乙１８，１９）。乙１７公報において，「携帯物」と「カード類」は区別されているのであるから，本件発明の「Ｒバッジ」は装身具内に処理手段や記憶手段を埋め込んで作るものを意味し，「ＩＣカード」は含まれないと解すべきである。

３　無効理由の存否

(1) 訂正要件違反（争点３－１）

（被告の主張）

本件訂正は，実質上特許請求の範囲を変更するものであり，また，明瞭でない記載の釈明を目的とするものでもない。

ア　本件訂正は，実質上特許請求の範囲を変更するものであり，特許法１２６条６項に違反する。

すなわち，被保護情報へのアクセスが許可される所定時間の開始時点について，本件訂正前の構成要件Ｆは「アクセス要求」の時点（ｔ０）としていたが，本件訂正により，その時点は「アクセス要求が許可された」時（ｔ１）に訂正されたので，その開始時点が，時間軸上，遅い時点に変更されたことになる（ｔ０→ｔ１）。しかるに，被保護情報に対するアクセスを許可する間隔については，本件訂正の前後を通じ，同一の「所定時間」（Δｔ）とされている。

そうすると，訂正前は，アクセスが許可されなかった時間帯（ｔ０＋Δｔ～ｔ１＋Δｔの間）について，訂正後は，アクセスが許可されることとなる。このように，アクセスが許可される時間帯に相違が生じている以上，実質上特許請求の範囲が変更されたというべきである。

イ　また，本件訂正は，明瞭でない記載の釈明を目的とするものでもないから，特許法１２６条１項ただし書にも違反する。この点，被告は，本件訂正前の構成要件Ｆの「アクセス要求から」の文言が，「アクセス要求」の時からとも，「アクセス要求の許可」の時からとも解釈し得る点で不明瞭であったと主張する。しかし，構成要件Ｂによれば，トリガ信号が「アクセス要求」として受け付けられるのであるから，前記の文言は，トリガ信号を受け付けた時点をいうものとして，明瞭に特定することができるのであって，「明瞭でない記載」には当たらない。

ウ　また，この点について，本件明細書等の記載を参酌するにしても，原告

が本件訂正を請求する根拠とした段落【００３０】，【００３１】，【００３６】の記載を含め，「所定時間」の開始時点が，「アクセス要求の許可」の時点であるとする明示的な記載は存在しない。

(ｱ) むしろ，本件明細書等の段落【００３６】には「照合結果が所定の条件を満たした後所定時間が経過する前に被保護情報へのアクセスがなされた場合はそれを許可し，この所定時間が経過した後の場合はアクセスを禁止する…。この場合，例えば，ＩＣアセンブリ１３０または１４０のいずれか一方または両方にタイマを設けることで，上述のような所定時間が経過したか否かを検出することが可能となる。」との記載があるが，被保護情報へのアクセスを許可するには，所定時間が経過する前にアクセスがされることが条件となるから，その判断をする前に所定時間の計時の開始時点が存在していなければならないはずである。

(ｲ) また，本件明細書等の段落【００３６】には，上記記載に引き続き，「このような方法をとることで，ＩＣアセンブリ１３０と１４０との間の距離が通信可能距離よりも長い場合であっても本発明を実現することが可能である。」との記載がある。

そして，同明細書等の段落【００３９】には，ＩＣアセンブリ１３０と１４０との間の距離が通信可能距離より長い場合について，携帯電話を自動改札機からのプリチャージ信号に応答可能な範囲に置いた後，一定時間の間に，ＩＣアセンブリを実装した帽子やイヤリングと携帯電話とを通信可能距離に近づけて認証するとの実施例が示されているが，この実施例は，多目的携帯端末３００を自動改札機のリーダライタ１５０にかざし，同端末を帽子などに１０ｃｍ以内の距離まで近づけて認証を行って乗車券のデータを利用可能にし，さらに，同端末を自動改札機のリーダライタにかざすことで，乗車券のデータへのアクセスを許可する処理である。そうすると，段落【００３６】の「所定時間」には，乗車

券のデータを利用可能とするまでのタイムラグも含まれると理解すべきである。

(ｳ) 原告が，本件訂正の根拠として段落【００３６】を挙げていながら，その「所定時間」にアクセス要求からアクセス許可までの時間が含まれないと解することは，禁反言に当たるものとして許されない。

(原告の主張)

本件訂正は，その訂正審決が正当に判断するとおり，訂正前の特許請求の範囲の記載に２個の解釈があり不明瞭なため，これを本件明細書等に記載と整合するように訂正するものであり，不明瞭な記載の釈明に当たり，実質上特許請求の範囲を拡張し，又は変更するものでもない。

ア　本件明細書等の段落【００３０】，【００３１】，【００３６】，【０１２０】，【図２】のＳ１５６～Ｓ１５８によれば，「所定時間」の計時の開始時点は，「アクセス要求の許可」の時であることが明らかであったが，本件訂正前の構成要件Ｆには，「アクセス要求から所定時間が経過するまで」などという文言が用いられていた。そのため，当該文言は，その計時の開始時点につき，「アクセス要求」の時からとも，「アクセス要求の許可」の時からとも解釈し得る不明瞭な記載となっていた。本件訂正は，このような不明瞭な記載を明瞭にしたにすぎない。

イ　これに対し，被告は，本件明細書等の段落【００３６】が，「所定時間」の計時の開始時点を「アクセス要求の許可」の時より前とするものであると主張するが，同段落の前半部分は，所定の条件を満たした後という条件の下，「所定時間」が経過する前に，被保護情報に対するアクセスがあれば，そのアクセスを許可するという意味に理解されるから，実際に被保護情報に対するアクセスが可能な期間は，所定の条件を満たしてアクセス要求が許可された時から開始することになる。すなわち，同段落の前半部分の記載は，アクセス要求が許可された時を開始時点として「所定時間」の

計時を開始することをいうと当然に理解し得るものである。

ウ　被告は，本件明細書等の段落【００３６】に係る被告の解釈の裏付けとして，同明細書等の段落【００３９】の実施形態の記載を指摘する。しかし，当該記載は，「タイマを設けて一定のタイムラグを許容することで」とあるように，Ｒバッジによる認証をするまでの「タイムラグ」に係るものであり，被保護情報に対するアクセスを許す「所定時間」に係るものではない。両者は，同明細書等の段落【０１１６】～【０１２０】，【図２１】で明確に区別されており，そこにいう「所定の時間ｔ１」がＲバッジの認証のための「タイムラグ」に相当し，「所定の時間ｔ２」が被保護情報に対するアクセスを許す「所定時間」に対応する。これを参酌すれば，段落【００３６】の後半部分の「このような方法をとることで」は，「タイマを設けて一定のタイムラグを許容することで」の明らかな誤記というべきである。

被告は，原告の以上の主張が，本件訂正との関係で禁反言に当たると主張するが，原告は，必要な範囲で訂正を求め，その根拠を主張していたにすぎず，本件訴訟における主張に何ら矛盾はない。

(2) 乙１１に基づく進歩性の欠如（争点３－２）

（被告の主張）

本件発明は，乙１１発明に，乙１２発明，乙１３発明又は乙１４発明を適用することにより，当業者が容易に想到し得たものである。

ア　本件発明と乙１１発明との一致点及び相違点

本件発明と乙１１発明は，以下の点において相違し，その余の構成において一致する。

（相違点１）

本件発明の構成要件Ｄが，受け取った識別情報と当該携帯電話に予め記録してある情報の比較をしているのに対し，乙１１発明は，ＩＤカードか

ら受け取ったデータ９と携帯電話に記憶したデータ１１の和と，パスワードとして入力を受け付けて携帯電話に記憶されたデータ１０との比較をしている点

（相違点２）

本件発明の「所定時間」の計時の開始時点は，アクセス要求が許可された時点であるのに対し，乙１１発明では，電源が投入されている状態のとき，計時装置が電源が投入されてからの時間を計時し，そこから一定時間毎にデータ９の送信要求を行っているが，この一定時間の計時の開始時点が，「アクセス要求が許可」された時点かどうかは明らかではない点

（相違点３）

仮に，本件発明の「Ｒバッジ」にＩＣカードが含まれない場合には，乙１１発明との関係でこの点が相違点となる。

イ　相違点に関する原告の主張について

原告は，構成要件Ａ及びＤが有機的に関連しているとして，相違点１に代え，相違点①を主張する。しかし，両者を組み合わせたところで，無線通信インターフェースを採用すれば当然の事項が生じるにすぎず，相乗的な効果という意味での有機的な関連性は生じない。また，原告は，相違点①に関し，乙１１発明では「携帯電話が受け取る情報は定期的に書き換えられる」とするが，構成要件Ｄは，Ｒバッジから受け取る「識別情報」について何らの限定もしていないので，その点も相違点とはなり得ない。

したがって，原告の主張する相違点①の認定は誤りである。

ウ　相違点１について

当業者は，乙１１発明に乙１２発明を適用すれば，相違点１に係る構成を容易に想到することができた。

(ｱ) 乙１２公報の段落【００１３】，【００１４】には，「識別ユニット

２に記憶した識別コードが情報ユニット１に送られ，この識別コードと，情報ユニット１のキーコードメモリに記憶したキーコードとを比較して一致するかを比較する」方法が開示されているが，この処理は，構成要件Ｄにおける比較方法と一致する。

(ｲ) 乙１１発明と乙１２発明は，いずれも携帯電話や携帯電話を含む携帯情報機器に関する発明であって，その技術分野は共通している。また，乙１１発明は，第三者による使用や内部データの盗用，破壊を防止とする点に課題があり（乙１１公報の段落【０００３】，【０００４】），乙１２発明は，セキュリティ機能を意識せず，かつ，セキュリティのための余分な操作を不要とし，第三者の不正使用を回避する点に課題があったのであるから（乙１２公報の段落【０００４】，【０００５】，【００１７】），乙１１発明と乙１２発明の解決しようとする課題は，いずれも共通しているということができる。

(ｳ) したがって，乙１１発明の「ＩＤカードから受け取ったデータ９とパスワードとして入力を受け付けたデータ１１との和と，携帯電話にあらかじめ記憶したデータ１０との比較をする」という構成に代え，乙１２発明の前記構成を適用すれば，当業者は，構成要件Ｄを容易に想到することができる。

(ｴ) これに対し，原告は，３つのデータを用いた構成にすることが，乙１１発明の課題解決には不可欠であったと主張する。

しかし，乙１１公報の段落【０００２】，【０００３】によれば，乙１１発明の課題は，パスワードのみによる被害の防止にあったというべきである。乙１１発明は，従来のパスワードだけでは不正使用されるという課題を解決するため，パスワード以外のデータ，すなわち，ＩＤカードから受信したデータ９と，携帯電話に予め記憶されたデータ１１などを用いた比較処理をすることにより，従来のパスワードだけの場合よ

りも携帯電話の不正使用等を防止するところに発明の要旨があるのであり，３つのデータを用いることは，課題解決に不可欠な構成ではない。

エ　相違点２について

(ｱ) 乙１１発明において，電源が投入された時点その他の任意の時点を計時の開始時点にしても，①携帯電話１が使用可能になってから，②上記一定時間が経過するまでは携帯電話１が使用可能なのであるから，前記①から②までの時間が，構成要件Ｆの「所定時間」に相当する。

したがって，相違点２は，実質的な相違点ではない。

(ｲ) 仮に，本件発明と乙１１発明が相違点２において相違するとしても，乙１１発明に乙１３に記載された技術的事項を適用することにより，当業者は相違点２に係る構成を容易に想到することができた。

すなわち，乙１３公報には，ロックを外してから一定時間経過した際に，自動的にロックがかかる機能の具体的処理として，前回ロックを外した時間を読み出し，現在の時間まで一定時間以上経過している場合にはロックｏｎ状態とし，そうでない場合にはロックｏｆｆ状態とする構成が開示されている。この点，ロックを外すことは，アクセス要求の許可に相当するから，前記構成は所定時間経過するまでは被保護情報に対するアクセスの許可に当たる。

乙１１発明と乙１３発明は，いずれも移動体通信端末に関する発明であり，その技術分野は共通している。そして，乙１１発明は，第三者による使用や内部データの盗用，破壊を防止とする点に課題があり（乙１１公報の段落【０００３】，【０００４】），乙１３発明は，第三者による無断使用を防止するために発信終了後にすぐにロックをかけておかなければならないなどの負担の軽減を課題とするものであったから（乙１３公報の〔発明が解決しようとする課題〕欄），いずれも課題が共通している。

したがって，乙１１発明における「電源が投入されてから一定時間ごとに比較処理を実行して携帯電話の使用の可否を判定している」構成に代えて，乙１３公報に記載された前記構成を適用すれば，当業者は，相違点２に係る構成を容易に想到し得たものである。

(ｳ) 仮に，本件発明と乙１１発明が相違点２において相違するとしても，乙１１発明に乙１４に記載された技術的事項を適用することにより，当業者は相違点２に係る構成を容易に想到することができた。

すなわち，乙１４公報の段落【００１９】～【００２１】には，動作開始直後は本体がロックされて使用不能であるが，キー信号を受信したとき，ロックを解除した上，時間のカウンタｔ１をリセットして計時を開始し，カウンタｔ１が所定値ｔ１０より大きくなったとき，ロックを作動するが，カウンタｔ１が所定値ｔ１０より小さい間にキー信号を受信すれば，カウンタｔ１がリセットされるといった構成が開示されている。他方，ここにいうロックの解除は「アクセス要求を許可」することであるから，当該構成は，「アクセス要求の許可」の時点から計時をするというものであり，また，そのカウンタｔ１が所定値ｔ１０より小さいと判定されている場合にロックがされていないということは，「アクセス要求が許可されてから所定時間が経過するまでは前記被保護情報へのアクセスを許可する」ことを意味する。

乙１１発明と乙１４発明は，いずれも携帯電話機に関する発明であるから，その技術分野は共通する。そして，乙１１発明は，第三者による使用や内部データの盗用，破壊を防止する点に課題があり（乙１１公報の段落【０００３】，【０００４】），乙１４発明は，紛失時や盗難時には確実にロック機能を作動させる点に課題があるのであるから（乙１４公報の段落【０００２】～【０００４】），課題も共通するということができる。

したがって，乙１１発明における「電源が投入されてから一定時間ごとに比較処理を実行して携帯電話の使用の可否を判定している」構成に代えて，乙１４公報に記載された前記構成を適用すれば，当業者は，相違点２に係る構成を容易に想到し得たものである。

オ　相違点３について

仮に，相違点３が相違点であるとしても，当業者は，乙１１発明の「ＩＣカード」に代えて，乙１５公報に記載された「ＩＣカードの形状を，指輪，時計，イヤリング，ネックレス，ペンダント等の身につけやすい形状に変更する」という技術的事項を適用すれば，当業者は，相違点３に係る構成を容易に想到し得る。

（原告の主張）

本件発明と乙１１発明との間には，少なくとも相違点①，②が存在し，同各相違点に係る構成は当業者が容易に想到し得たものではない。

ア　本件発明と乙１１発明との相違点

（相違点①）

本件発明は，ＲＦＩＤインターフェースを有する携帯電話であり，Ｒバッジより識別情報を受け取って，該受け取った識別情報と，当該携帯電話に予め記録してある識別情報とを比較するものであるのに対し，乙１１発明は，ＩＤカードと無線通信はするものの，ＲＦＩＤインターフェースを有するか不明であり，携帯電話が受け取る情報は定期的に書き換えられるＩＤカードに記録されたデータ９であってＩＤカードの識別情報ではなく，ＩＤカードより受け取ったデータ９，携帯電話に記録されたデータ１１及び電波信号Ａの送信と同時に当該携帯電話の使用者に入力を求めて入力されたパスワードの三者が一定の関係を有するか否かを比較するものである点

（相違点②）

本件発明は，アクセス制御手段が比較手段でアクセス要求を許可するという比較結果が得られた場合は，アクセス要求が許可されてから所定時間が経過するまでは被保護情報へのアクセスを許可するものであるのに対し，乙１１発明は，ＩＤカードから受け取ったデータ９と携帯電話に記憶されたデータ１１及び入力されたパスワードの三者が一定の関係を有するという比較結果が得られた後，一定の時間ごとに前記データ１１を書き換え，同時に前記ＩＤカードに対して電波信号Ａを送信し，前記ＩＤカード内のデータ９を書き換え，一定時間ごとに前記ＩＤカードに対してデータ９の送信を要求し，前記ＩＤカードより前記データ９を受け取って，該受け取ったデータ９，データ１０（パスワードの値に等しいデータ）及び前記データ１１の三者を比較し，該三者が一定の関係を有するときは使用可能にし，一定の関係を有しないときは自動的に電源を切り使用不可能にするものであって，電源が投入されてからの時間を計時はするものの，識別情報を比較した結果が一致した時点からの所定時間を計時せず，所定時間が経過するまでアクセス可能とするものではない点

イ　被告の主張する相違点１について

被告は，構成要件Ａに係る相違は実質的な相違でないとし，原告が主張する相違点①に相当するものとして，相違点１を認定する。

しかし，構成要件Ａが規定する携帯電話と構成要件Ｄが規定するＲバッジは，ＲＦＩＤインターフェースに基づき，携帯電話の要求信号に応答して，Ｒバッジに格納された一意に識別できるように割り振った固有の識別情報を携帯電話に送信し，これを受け取った携帯電話は，予め記録してある識別情報との比較を行うものである（本件明細書等の段落【００１６】，【０１０７】）。

このように，Ｒバッジに格納された識別情報は，ＲＦＩＤタグとして好ましくは製造時に書換え不能な固有の識別情報を書き込まれたもので

あって，パスワードのような任意に変更可能な情報ではなく，Ｒバッジの固有の識別情報を利用することにより，被保護情報に対する第三者の不正アクセスを防止することを目的としている。この意味において，構成要件ＡとＤとには有機的な関連性があり，この点を考慮すると，本件発明と乙１１発明との相違点は，前記相違点①のように認定されるべきである。

ウ　相違点①について

被告は，乙１２発明を乙１１発明に適用すれば，本件発明を容易に想到することができると主張するが，以下のとおり失当である。

(ｱ) 乙１２発明は，従来技術が，第三者の不正使用に備え，暗証番号を設定させ，暗証番号に続いて電話番号を入力したときにのみ電話の発信を可能とする構成であったのに対し，４桁程度の暗証番号の入力に代え，キーコードを入力させ，いったんキーコードが記憶された後は，発信操作をする場合に，送受信部を介した識別コードを受信して認証する構成とし，これを前記従来技術の電話発信時に先頭に入力すべき暗証番号による認証に代替させ，発信処理を続行させて電話番号を発信することができるようにするものである。そして，そのキーコードは，ＲＦＩＤインターフェースの一意に識別できるように割り振られた固有の識別情報ではなく，携帯情報機器の操作者が任意に設定する。

(ｲ) 他方，乙１１発明は，携帯電話のスイッチを押したときにパスワードを入力する必要があり，これに加えて，ＩＤカードからのデータ９を受け取って，予め記憶しているデータ１１の３つのデータが一定の関係を満足するものであるか否かを比較することで，その課題を解決するものであるから，これら３つのデータを用いた複雑な構成にすることは，その課題解決にとって不可欠なものである。そのため，乙１１発明のデータ９を乙１２発明のキーコードとする動機付けは存在しない。

したがって，相違点①に係る構成について，乙１１発明及び乙１２発明から容易に想到し得たということはできない。

エ　相違点②について

(ｱ) 被告は，乙１１発明における一定時間の計時の開始時点につき，どのタイミングとするかは当業者が適宜設定する事項にすぎないなどと主張する。

しかし，乙１１発明は，一定時間ごとに変化するデータ９，データ１１及び電源投入又はキー５を押したときに入力されたパスワードに等しいデータ１０という三者のデータに一定の関係がある場合であって，その一定の関係を有するデータ９をＩＤカードから受信している期間，その携帯電話を使用可能とするものである。

このようにデータ９，データ１０及びデータ１１を用いることが，単なるパスワードによる保護に付加する不可欠な課題解決手段であり，乙１１発明に不可欠な構成であるから，被告の前記主張は失当である。

(ｲ) 被告は，乙１１発明に乙１３公報に記載された技術的事項を適用し得ると主張する。

しかし，乙１３発明は，ロック解除コード（パスワード）でロックを解除し，それから一定時間経過すると自動的にロックするという構成を有するにすぎない。これに対し，乙１１発明は，単なるパスワードによる保護に比較して第三者の不正使用をより強く防止することを目的とするための構成を不可欠としているのであるから，この構成に代え，乙１３発明の前記構成を適用する動機付けはない。

したがって，乙１３公報に記載された技術的事項によっても，相違点②に係る構成を容易に想到し得たということはできない。

(ｳ) 被告は，乙１１発明に乙１４公報に記載された技術的事項を適用し得ると主張する。

しかし，乙１４発明においては，時間のカウンタが所定値を超えたとき，ロック作動となるが，キー信号が受信されると，カウンタがリセットされるから，カウンタが所定値を超えないうちにキー信号を受信している限り，ロック解除の状態が継続する。すなわち，乙１４発明でロックが解除されるのは，「一定時間ごとに比較処理を実行して携帯電話の使用の可否を判定している」間であって，この構成自体は，携帯電話の使用可能時間に係る乙１１発明の構成と異ならない。

したがって，乙１１発明に乙１４公報に記載された技術的事項を適用したところで，相違点②に係る構成には至らない。

オ　相違点３について

争点２－５で主張したとおり，「Ｒバッジ」に「ＩＣカード」は含まれる。なお，乙１５発明は，携帯端末装置固有の機器ＩＤと個人認証用ＩＣカードより受信したユーザＩＤについてサービス提供局と通信を行い，そこから個人認証を受けるというものであるから，携帯電話に予め記憶された識別情報とＲバッジより受信した識別情報を比較して携帯電話において認証するという本件発明とは全く異なる。

(3) 乙１６に基づく拡大先願違反（争点３－３）

（被告の主張）

本件発明は，本件特許の優先日前に出願され，本件特許の優先日後に出願公開された乙１６公報に記載された発明と同一の発明である。

ア　構成要件Ａ，Ｇとの一致

(ｱ) 乙１６公報の段落【００２５】には，乙１６発明の「携帯電話機１０内において，１１は携帯電話機１０全体の制御を行う制御部であり，１２はロック解除装置２０に微弱電波を用いてロック解除コードを送信するロック解除コード送信部であり，…１８は，ロック解除コード送信部１２がロック解除コードをロック解除装置２０に送信した後，該ロック

解除装置２０から送られて（返送されて）きた認証演算結果を制御部１１に通知する認証結果受信部であり」との記載があり，同段落【００２６】には，「携帯電話機１０とロック解除装置２０間にて授受される信号の通信媒体として電波が用いられる」との記載がある。

(ｲ) このように，乙１６発明は，携帯電話機とロック解除装置との間で微弱電波を用いてロック解除コード及び認証演算結果を送受信するものであり，乙１６公報の段落【００３３】の記載によれば，その電波強度は「１ｍ程度」のものであると解される。

他方，ＲＦＩＤインターフェースは，本件明細書等の段落【００２７】もいうように，標準規格化が進められていた無線通信インターフェースであって，「数メートル離れた距離」のものを含む近距離無線通信であり（乙２５，２６），構成要件Ａはその方式を何ら限定していない。

そうすると，「ロック解除コード送信部」及び「認証結果受信部」を有する乙１６発明の携帯電話機は，構成要件Ａと実質的に一致し，構成要件Ｇも充たす。

イ　構成要件Ｂ，Ｃとの一致

(ｱ) 乙１６公報の段落【００３１】には，「次に，携帯電話機使用者により，発信またはメモリダイヤル等の個人情報へのアクセス等の操作を行うべく，入力装置１４のキーボードより，一連のキー操作によるデータの入力（動作処理要求等）が行われると，この一連のキー操作によるデータの入力に対応する操作内容が制御部１１に供給（通知）される。制御部１１は，入力装置１４から前記操作内容が供給されたタイミングにて，コード記憶回路１６よりロック解除コードを読み出してロック解除コード送信部１２に供給する。ロック解除コード送信部１２は，ロック解除コードを微弱電波にのせ，携帯電話機使用者が所持している（身に付けている）ロック解除装置２０に送信する」との記載があり，同【０

０４４】に，「この実施の形態１によれば，従来方式ではロック解除装置４０側から携帯電話機３０に対して一定周期でロック解除コードを送信していたのに対し，携帯電話機１０の使用者により発信またはメモリダイヤル等の個人情報へのアクセス等の操作（キー入力）が行われた場合に，ロック解除装置２０から携帯電話機１０に対して認証演算結果が送信されるので，ロック解除装置２０の電力消費を格段に押さえる効果が得られる」との記載がある。

(ｲ) これらの記載におけるキー入力は個人情報へのアクセス等の操作であって，本件発明にいう「被保護情報に対するアクセス要求」に相当し，その操作内容が制御部に通知されるのであるから，乙１６発明の「制御部」は，構成要件Ｂと一致する。また，ロック解除コード送信部は，操作内容が供給されたタイミングで読み出されたロック解除コードをロック解除装置に送信するから，使用者が身に付けているというロック解除装置が，本件発明の「Ｒバッジ」に相当し，乙１６発明の「ロック解除コード送信部」が，構成要件Ｃに一致する。

ウ　構成要件Ｄとの一致

(ｱ) 乙１６公報の段落【００３２】には，「ロック解除装置２０のロック解除コード受信部２２は，携帯電話機１０から微弱電波で送信されたロック解除コードを受信すると，該ロック解除コードを認証装置２３に供給する。このロック解除装置２０の認証装置２３は，ロック解除コードが供給（受信）された時点で，ＩＤ情報記憶回路２１にあらかじめ記憶されているＩＤ情報を読み出し，該ＩＤ情報と受信したロック解除コードとで認証演算を行い…，該認証演算の結果を認証結果送信部２４に供給する。また，認証結果送信部２４は認証装置２３より供給された認証演算の結果（第２の認証演算結果）を，携帯電話機１０に送信する。」と記載され，同段落【００３４】には，「次に，携帯電話機１０の認証

結果受信部１８は，ロック解除装置２０から微弱電波で送信された認証演算の結果（第２の認証演算結果）を受信すると，制御部１１に供給する。制御部１１は，コード記憶回路１６に既に記憶されている認証演算の結果（第１の認証演算結果）を読み出して，受信した認証演算の結果（第２の認証演算結果）との比較認証（認証処理による認証判定）を行う」と記載されている。

(ｲ) このように，乙１６発明では，ロック解除装置が，携帯電話機から受信したロック解除コードとＩＤ情報とを用いて演算した第２の認証演算結果を携帯電話機に送信し，これを受け取った携帯電話機は，制御部において，既に記憶済みの第１の認証演算結果との比較をするのであるから，同発明の「制御部」は，構成要件Ｄと一致する。

(ｳ) これに対し，原告は，乙１６発明の携帯電話機が受け取るのが「Ｒバッジの識別情報」ではない点で本件発明と相違すると主張する。しかし，構成要件Ｄには「Ｒバッジの識別情報」を受け取るとの限定はない。乙１６発明は，受け取った演算結果に基づき，前記の比較認証をするのであるから，構成要件Ｄの「比較手段」を備える。

エ　構成要件Ｅとの一致

(ｱ) 乙１６公報の段落【００３５】には，「制御部１１は，比較認証の結果が一致していた場合，前記ステップＳＴ４におけるキー入力は，特定の使用者（使用が許可されている携帯電話機使用者）によるキー入力であるものと判断し，ロック解除状態とし，前記ステップＳＴ４にて入力装置１４から入力された発信操作及びメモリダイヤル等の操作を有効として…，発信処理等を継続する（一連のキー入力による処理が完了するまでの処理の継続を可能とする）。」と記載され，同段落【００３６】には，「前記比較認証の結果が不一致となった場合，制御部１１は，前記ステップＳＴ４におけるキー入力が，特定の使用者でない者（使用が

許可されていない携帯電話機使用者）によるキー入力であると判断し，ロック解除は行わず，前記ステップＳＴ４にて入力された操作を無効として破棄し」と記載されている。

(ｲ) このように，乙１６発明の携帯電話機の「制御部」では，比較認証の結果が一致すればロック解除として操作を有効とし，不一致であればロック解除を行わず操作を無効とするのであるから，同発明における「制御部」は，構成要件Ｅと一致する。

オ　構成要件Ｆ

(ｱ) 乙１６公報の段落【００３７】には，「制御部１１は，許可された発信処理（発信，メモリダイヤル等の個人情報へのアクセス操作等）が実施中，新たに入力装置１４から通知（入力）された操作に対しては，ロック状態として扱う。さらに，許可された発信処理が完了した後，新たに入力装置１４から通知された操作に対しては，制御部１１は，再びロック解除コードをロック解除装置２０に送信して認証処理を実施する。すなわち，一旦，ダイヤルロックが解除された操作に対し，一連の処理が完了するまでの期間についてのみ，キー入力された一連の処理要求に対する動作の継続が可能となる。」と記載されている。

(ｲ) このように，乙１６発明の携帯電話機の制御部では，ダイヤルロックを解除した操作に対し，動作の継続が可能であることから，本件発明にいう「アクセス要求が許可されてから」に相当する構成を備えている。そして，その動作の継続は，「一連の処理が完了するまでの期間」について可能であるとされる一方，本件発明の「所定時間」に何らの限定もないのであるから，前記「一連の処理が完了するまでの期間」は，構成要件Ｆの「所定時間」に相当する。

したがって，乙１６発明の携帯電話機の制御部における前記の構成は，構成要件Ｆに一致する。

（原告の主張）

乙１６発明は，ＲＦＩＤインターフェースに係る特定を欠き，本件発明の課題を開示するものでもなく，本件発明とは解決手段も異にする。

ア　本件発明と乙１６発明の相違点

乙１６発明は，本件発明と異なり，ＲＦＩＤインターフェースを有する携帯電話であるとの特定がない上，その課題も異なり，課題を解決するための構成についても，少なくとも以下の点において相違する。

(ｱ) 相違点１

本件発明は，ＲＦＩＤインターフェースを有する携帯電話がＲバッジより受信するものがＲバッジの識別情報であるのに対し，乙１６発明では，携帯電話がロック解除装置から微弱電波等を用いて受信するものが当該ロック解除装置に供給されたロック解除コードと予め当該ロック解除装置内に記憶されている特定の使用者を示すＩＤ情報とにより認証演算を行うことにより得られた値である点

(ｲ) 相違点２

本件発明は，被保護情報に対するアクセス要求を許可するという比較結果が得られた場合は，アクセス要求が許可されてから所定時間が経過するまでは被保護情報へのアクセスを許可するものであるのに対し，乙１６発明は，動作処理要求に伴った一連の操作が前記携帯電話機に対して行われると個人認証を行い，個人認証が完了すると当該一連の操作のみが可能になるのであって，当該処理中に他の処理を行うことも，当該処理が終了後に他の処理を行うこともできず，また，所定時間を計時することもなく，所定時間が経過するまで携帯電話機内の情報に対するアクセスを含む何らかの操作を許可するものではない点

イ　上記アのとおり，乙１６発明の携帯電話はＲＦＩＤインターフェースを有するかどうかは不明である上，上記相違点１のとおり，乙１６発明では，

ロック解除装置から携帯電話機に送信されるのは，ロック解除コードを用いた演算結果であり，ＲＦＩＤインターフェースに基づく識別情報ではない。

また，上記相違点２のとおり，乙１６発明は，動作処理要求に伴った一連の操作が携帯電話機に対して行われると個人認証を行い，個人認証が完了すると当該一連の操作としての発信のみが可能になるにすぎず，本件発明のように，アクセス要求が許可されてから所定時間が経過するまでは被保護情報にアクセスを許可するものではない。

したがって，乙１６発明が本件発明と同一ということはできない。

４　損害額（争点４）

（原告の主張）

被告は，平成２９年１月から１２月まで（１月１日を第１四半期の始期とする第１四半期から第４四半期）の間に少なくとも合計９７万２０００台の被告製品を出荷した。他方，本件特許権の実施許諾料は，１台当たり３８０円を下らない。したがって，特許法１０２条３項による損害額は，前者に後者を乗じた３億６９３６万円であり，本件請求は，その一部請求である。

（被告の主張）

争う。

第４　当裁判所の判断

１　本件発明の内容

(1) 本件明細書等（甲２，１３）には，以下の記載がある。

ア　技術分野

「本発明はＲＦＩＤインターフェースを利用した情報保護技術に関するものである。」（段落【０００１】）

イ　背景技術

「近年，市場には膨大な数の磁気カードが流通している。一例として，

クレジットカード，キャッシュカード，プリペイドカード，社員証や学生証，通行証，各種証明書発行用カード，図書館の貸出カード，入退室管理カードなどがあげられる。これらのカードは特定の目的ごとに提供されているため，場合によっては外出時に何枚ものカードを携行しなければならない。しかしながら，カードの枚数によっては非常にかさばる上に，必要なときに必要なカードをすぐに取り出しにくいなどの問題がある。」（段落【０００２】）

「そこで，携帯電話，ＰＨＳ，携帯情報端末（ＰＤＡ），ノートパソコンなどの携帯端末に多目的ＩＣカードを統合したり，複数のＩＣカードの機能を搭載したり，あるいは搭載可能な仕組み（ＩＣカードとしての機能を実行するためのソフトを所定のサーバ等にダウンロード可能な形態で提供し，そのソフトをダウンロードする，あるいはこのようなソフトが搭載された，カード用専用チップを装着する等）を用意するなどし，この端末に対してセキュリティ対策を施す方法が検討されている。ＩＣカードには大きく分けて接触型と非接触型の２種類があり，カードに記録されたデータを利用するには接触型の場合は専用の端末（以下，「リーダライタ」と呼ぶ）にカードを挿入しなければならないが，非接触型ではその必要がなく，リーダライタにかざすだけでよい。したがって，携帯端末をパスワードで保護し，端末にあらかじめ記録されたパスワードと所有者が入力するパスワードとが一致した場合にのみＩＣカードの機能を利用できるようにする方式が考えられる。しかしながら，このような方式ではカード機能を利用するたびに端末にパスワードを入力しなければならない煩わしさがあり，リーダライタにかざすだけでよいという非接触型ＩＣカードの利点が半減してしまう。また，パスワード自体は所有者個人を特定する手段にはならず，何らかの理由でパスワードが漏洩した場合に，悪意の拾得者が不正入手したパスワードを利用して端末にアクセスする可能性もある。」

（段落【０００７】）

ウ　発明が解決しようとする課題

「本発明は上記課題に鑑みてなされたものであり，その目的とするところは，個人情報や金銭的価値のある情報を統合して管理する場合に当該情報の第三者による不正使用を確実に防止するための情報保護システムを提供することにある。」（段落【０００９】）

エ　課題を解決するための手段

「本発明の第１の態様によれば，ＲＦＩＤインターフェースを有する携帯電話であって，当該携帯電話のスイッチを押すことで生成されるトリガ信号又はリーダライタから送信されるトリガ信号を，当該携帯電話の所有者が第三者による閲覧や使用を制限し，保護することを希望する被保護情報に対する前記アクセス要求として受け付ける受付手段と，前記トリガ信号に応答して，Ｒバッジに対して要求信号を送信する送信手段と，前記Ｒバッジより識別情報を受け取って，該受け取った識別情報と当該携帯電話に予め記録してある識別情報との比較を行う比較手段と，前記比較手段による比較結果に応じて前記受付手段で受け付けた前記アクセス要求を許可または禁止するアクセス制御手段とを備え，前記アクセス制御手段は，当該比較手段で前記アクセス要求を許可するという比較結果が得られた場合は，前記アクセス要求が許可されてから所定時間が経過するまでは前記被保護情報へのアクセスを許可することを特徴とする携帯電話が得られる。」（段落【００１１】）

「上記携帯電話において，前記被保護情報は，例えば，プリペイドカード，キャッシュカード，デビッドカード，クレジットカード，定期券，乗車券，電子マネー，鍵，会員権，診察券，健康保険証，身分証明書，アミューズメント施設のチケット，公共施設のチケット，社員証，学生証，通行証，各種証明書発行用カード，図書館の貸出カード，入退室管理カード

などに記録されたデータであってよい。」（段落【００１２】）

オ　発明の効果

「以上詳細に説明したように，本発明では，携帯端末に定期券・クレジットカード・運転免許書などの個人情報を携帯端末に登録することができる。」（段落【００１７】）

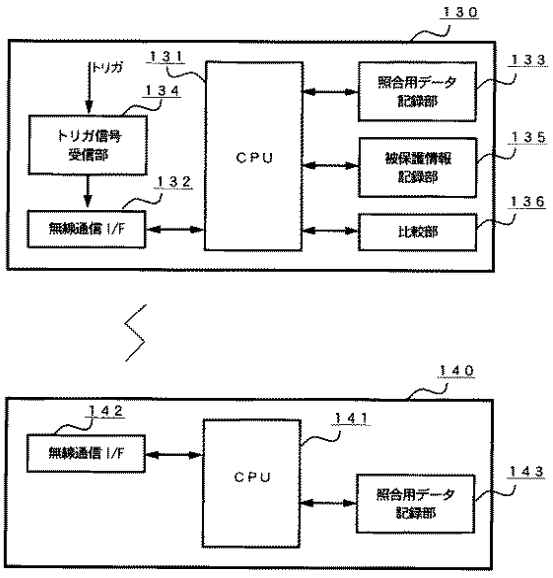
「また，携帯端末に一意に割り振られる識別情報をもとに携帯端末の利用状況の履歴を取ることが確実に行われ悪用を防ぐことができる。」（段落【００１８】）

「さらに，携帯端末が悪意を持つ第３者に渡っても，対応するレッドバッジ（ＩＣチップ）などがない限り悪用できない。」（段落【００１９】）

「また，これにより，利用した覚えのない料金を支払う必要がない。」（段落【００２０】）

「或いは，携帯端末に記憶されている個人データの流出を防ぐことが可能になる。」（段落【００２１】）

カ　発明を実施するための最良の形態



【図１】

「図１は，本発明の一実施形態による情報保護システムの概要を示すブロック図である。この情報保護システムは，第１のＩＣアセンブリ１３０と第２のＩＣアセンブリ１４０とで構成される。…」（段落【００２４】）

「第１のＩＣアセンブリ１３０および第２のＩＣアセンブリ１４０は，

無線を利用して互いにデータの送受信が可能なように構成されている。この場合，本願明細書において使用する「無線通信」という用語は，金属端子による電気的な接触を使用せずに行う通信全般を意味し，一例として，非接触自動識別システム（ＲＦＩＤ：Ｒａｄｉｏ　Ｆｒｅｑｕｅｎｃｙ　Ｉｄｅｎｔｉｆｙｃａｔｉｏｎ）で用いられている電磁結合方式，電磁誘導方式，マイクロ波方式，光方式の無線通信があげられる。…」（段落【００２５】）

「ＣＰＵ１３１は，第１のＩＣアセンブリ１３０の各構成要素を制御し，ＣＰＵ１４１は第２のＩＣアセンブリ１４０の各構成要素を制御する。無線通信インタフェース部１３２および１４２は，それぞれが送信機能と受信機能の両方を有する。この無線通信インタフェース部１３２および１４２は，たとえばＲＦＩＤ技術において用いられているようなアンテナやコイルなどを有し，互いにデータの送受信を行うものである。」（段落【００２６】）

「ＲＦＩＤにはさまざまな変調方式や周波数，通信プロトコルを利用したものがあるが，本発明は特定の方式に限定されるものではなく，どのような方式を利用してもよい。ＩＣアセンブリに設けられる無線通信インタフェース部の数にも特に制限はなく，必要に応じて異なる変調方式で機能する無線通信インタフェース部を複数設けるようにしてもよい。なお，汎用性の観点から見ると，非接触型ＩＣカードの分野で標準規格化が進められている仕様に準拠するなどの方式を採用すると好ましい。日本においては，次世代ＩＣカードシステム研究会（ｔｈｅ　Ｎｅｘｔ　Ｇｅｎｅｒａｔｉｏｎ　ＩＣ　Ｃａｒｄ　Ｓｙｓｔｅｍ　Ｓｔｕｄｙ　Ｇｒｏｕｐ）やＩＣカードシステム利用促進協議会（Ｊａｐａｎ　ＩＣ　Ｃａｒｄ　Ｓｙｓｔｅｍ　Ａｐｐｌｉｃａｔｉｏｎ　Ｃｏｕｎｃｉｌ）が標準化活動を行っている。また，すでに確立されている国際規格として，ＩＳＯ／ＩＥＣ

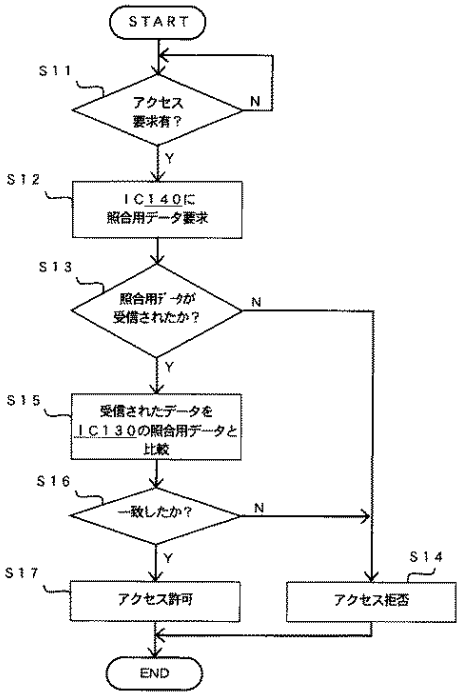
１０５３６，ＩＳＯ／ＩＥＣ１４４４３，ＩＳＯ／ＩＥＣ１５６９３がある。このような規格に準拠した無線通信インタフェース部１３２および１４２とすることで，より一層汎用的かつ実用性の高い情報保護システムを構築できる可能性がある。」（段落【００２７】）

「照合用データ記録部１３３および１４３には，第１および第２のＩＣアセンブリの照合を行うためのデータが記録されている。この照合用データが所定の条件を満たした場合に限り，被保護情報記録部１３５へのアクセス，例えば被保護情報記録部１３５に格納されたデータやプログラムへのアクセスが許可される。照合用データとは，ＩＣアセンブリの所有者を一意に特定するためのデータであり，その内容は特に限定されるものではない。たとえばＣＰＵの固有記号や製品番号，クレジットカード番号，これらの一意なデータを複数組み合わせたものや，さらにこれを暗号化したものなどを照合用データとして利用することができる。被保護情報とは，個人情報や金銭的価値のある情報など，ＩＣアセンブリの所有者が第三者による閲覧や使用を制限し，保護することを希望する情報またはデータであれば，どのような情報またはデータであってもよい。一例として，クレジットカード，キャッシュカード，プリペイドカード，各種会員権，診察券，健康保険証，身分証明書，公共施設のチケットなど従来のカード類に記録されたデータの他，電子マネーや電子取引情報，私的な住所録やドキュメント，画像データなど，さまざまなものが考えられる。」（段落【００２８】）

「図２に，ＩＣアセンブリ１３０へのアクセス要求に対してのＩＣアセンブリ１３０のＣＰＵ１３１における認証処理を表すフローチャートを示

す。」（段落【００２９】）

「無線通信インタフェース部１３２は，トリガ信号受信部１３４と接続され，後述するトリガ信号を受信する。ＣＰＵ１３１は，トリガ信号受信部１３４でトリガ信号が受信されないときは，ＩＣアセンブリ１３０に対するアクセス要求は無しと判定し，トリガ信号が受信された場合はアクセス要求有りと判定する（Ｓ１１）。トリガ信号が検出された場合，ＣＰＵ１３０は，無線通信インターフェース１３２を通じて，当該トリガ信号に応答して第２のＩＣアセンブリ１４０に対して照合用データの送信を要求する要求信号を送信する（Ｓ１２）。第２のＩＣアセンブリ１４０は，この要求信号に応答して，自己の照合用データ記録部１４３に格納された照合用データを第１のＩＣアセンブリに送信する。ＣＰＵ１３１は，無線通信インターフェース１３２を通じて照合用データが受信されたか否かを判定し（Ｓ１３），受信さない場合はアクセスを拒否する（Ｓ１４）。照合用データが受信された場合，ＣＰＵ１３１は，第２のＩＣアセンブリ１４０から受信した照合用データとＩＣアセンブリ１３０の照合用データ記録部１３３に格納された照合用データとの比較処理を開始させる（Ｓ１５）。この例では，この比較は，比較部１３６によって行われる。」（段落【００３０】）



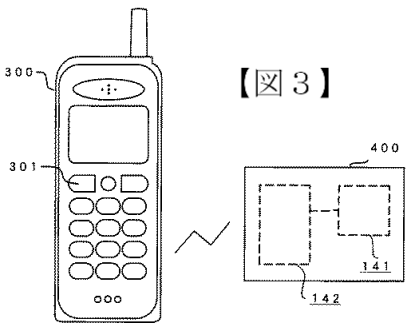
【図２】

「比較部１３６における比較の結果，所定の条件が満たされたか否かを判定する。この例では，ＩＣアセンブリ１４０から受信したデータとＩＣ照合用データとが一致するか否かを判定し（Ｓ１６），一致した場合には，

ＣＰＵ１３１は，アクセスを許可し（Ｓ１７），被保護情報記録部から必要な情報を抽出する。一方，所定の条件が満たされなかった場合は，ＣＰＵ１３１は被保護情報記録部１３５に格納されたデータへのアクセスを禁止する（Ｓ１４）。」（段落【００３１】）

「…ＩＣアセンブリは，小型チップとしてさまざまな物体に埋め込むことが可能なものである。以上，本発明の目的において，ＩＣアセンブリを装飾品や衣類など所有者の身近におくことが可能な物体に埋め込んだものを「Ｒバッジ」と総称する。また，個人情報や金銭的価値の付帯する情報を携帯端末に統合したものを「多目的携帯端末」と総称する。」（段落【００３３】）

「次に，図３を参照すると，第１のＩＣアセンブリを多目的携帯端末３００の形で実現し，第２のＩＣアセンブリをＲバッジ４００の形で実現した例が示されている。多目的携帯端末３００はスイッチ３０１を備え，端末の所有者がスイッチ３０１を押すことでトリガ信号が生成される。トリガ信号受信部１３４（図１）は，トリガ信号を受信すると，無線通信インタフェース部１３２に対して第２のＩＣアセンブリとの間での通信を開始するよう指示する。これ以降の照合動作については図１を参照して説明したとおりである。このようにすることで，多目的携帯端末とＲバッジとの間で照合用データを照合し，照合の結果が所定の条件を満たした場合に限って多目的携帯端末を使用可能とすることができる。」（段落【００３４】）

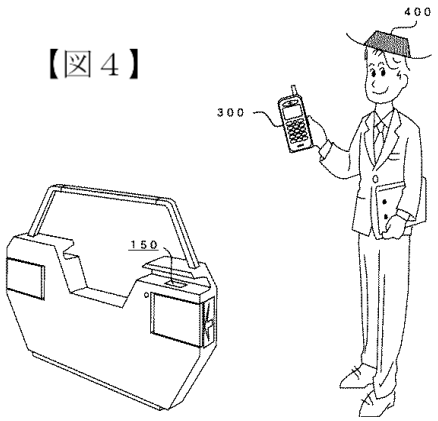


【図３】

「図４は，自動改札機に非接触型ＩＣカード用のリーダライタ１５０を設け，このリーダライタから送信される信号（プリチャージ信号）をトリ

ガ信号として利用した例を示している。この場合，リーダライタから発信される信号は，周知のＲＦＩＤシステムにおいて利用されている信号と同様のものである。利用者が多目的携帯端末３００を自動改札機に近づけると，リーダライタ１５０から発信されるプリチャージ信号に応答して多目的携帯端末３００がＲバッジ４００との通信を開始する。これ以降の照合動作については図１を参照して説明したとおりである。利用者は多目的携帯端末を自動改札機に近づけるだけで，改札を通ることができるという利点がある。自動改札機に限らず，金融機関のＡＴＭや公衆電話など，決済や金銭の移動を伴う行為に関わる多くの設備に同様の方式を応用することが可能である。」（段落【００３５】）

【図４】



「また，照合結果が所定の条件を満たした後所定時間が経過する前に被保護情報へのアクセスがなされた場合はそれを許可し，この所定時間が経過した後の場合はアクセスを禁止するようにしてもよい。この場合，例えば，ＩＣアセンブリ１３０または１４０のいずれか一方または両方にタイマを設けることで，上述のような所定時間が経過したか否かを検出することが可能となる。このような方法をとることで，ＩＣアセンブリ１３０と１４０との間の距離が通信可能距離よりも長い場合であっても本発明を実現することが可能である。」（段落【００３６】）

「以下，多目的携帯端末３００に乗車券を統合して自動改札機を通過する場合を例に説明する。なお，この例では，多目的携帯端末３００（ＩＣアセンブリ３０）とＩＣアセンブリ１４０との間の通信可能距離が１０ｃｍであるものとする。通常の自動改札機においては，多目的端末３００を

手で保持した状態で自動改札機のリーダライタ１５０に近づけて認証を行う。ＩＣアセンブリ１４０が例えば指輪に実装されているのであれば，多目的端末３００内のＩＣアセンブリと指輪との間隔は１０ｃｍよりより短いので，問題なく認証を行うことができる。しかし，ＩＣアセンブリ１４０が帽子あるいはイヤリングに実装されている場合，ＩＣアセンブリ１３０とＩＣアセンブリ１４０との間の距離は，通常は１０ｃｍよりも長くなり，認証を行うことができなくなる。」（段落【００３７】）

「このような場合，多目的携帯端末３００を帽子あるいはイヤリングに近づけてＩＣアセンブリ１３０とＩＣアセンブリ１４０との距離を１０ｃｍ以下としたうえで，ＩＣアセンブリ１４０とＩＣアセンブリ１３０との間での認証を行わせる。この動作は，例えば図３の例では，多目的携帯端末３００を帽子またはイヤリングの近傍に持っていった状態で，多目的携帯端末３００のスイッチ３０１を押してトリガ信号を発信させることにより認証を行う。」（段落【００３８】）

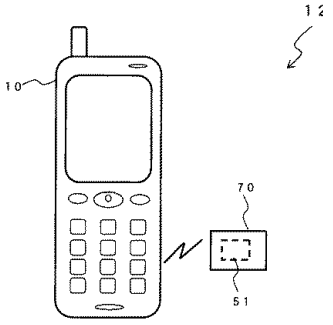
「また，図４の例では，リーダライタ１５０から発信されるプリチャージ信号に応答可能な範囲内に多目的携帯端末３００がある状態で，多目的端末３００を耳元に近づけて帽子又はイヤリングに実装されたＩＣアセンブリ１４０との距離を１０ｃｍ以下とすることで，認証を行い，携帯端末３００に記録された乗車券のデータを利用可能とすることができる。このように，タイマを設けて一定のタイムラグを許容することで，ＩＣアセンブリ１３０とＩＣアセンブリ１４０とを実際に使用するときの距離が比較的長い場合であっても，通信可能距離の短い通信方式を採用することが可能になる。」（段落【００３９】）

「第３の実施の形態では，識別情報を記憶するＩＣチップを利用して携帯端末１０の使用者を識別する使用者識別システムについて説明する。前述の実施の形態と同一のものには同一符号を付して詳細な説明を省略す

る。」（段落【０１００】）

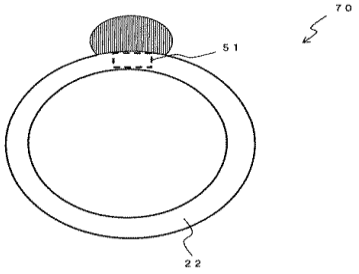
「いつも身に付けているものや身近におくものにＩＣチップを埋め込んだものを総称して，以下，レッドバッジと呼ぶ。」（段落【０１０１】）

「第３の実施の形態における使用者識別システム１２は，図１５に示すように，携帯端末１０と識別情報を記憶する携帯記録素子とで概略構成される。以下，携帯記録素子としてＩＣチップ５１とアンテナ２２を組み込んだレッドバッジ７０を例に説明する。」（段落【０１０２】）

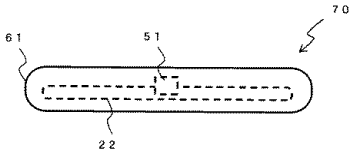


【図１５】

「ここで，ＩＣチップ５１を内蔵したレッドバッジ７０の例について説明する。レッドバッジ７０は，第１のタイプとして，図１６に示すように，指輪・イヤリング等の本体をアンテナ２２として本来の目的と共用し，それにＩＣチップ５１が備えられるタイプがある。」（段落【０１０３】）

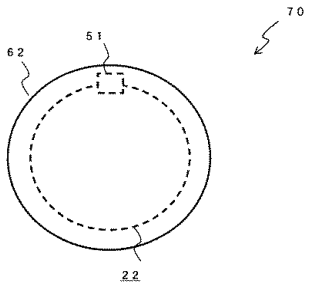


【図１６】



【図１７】

「第２のタイプとして，図１７に示すように，ネクタイピン等の本体６１にＩＣチップ５１とアンテナ２２が内蔵される。或いは，図１８に示すように，カフスボタン・バッジ・ブローチ・ペンダント・コンタクトレンズ等の本体６２にＩＣチップ５１とアンテナ２２が内蔵された



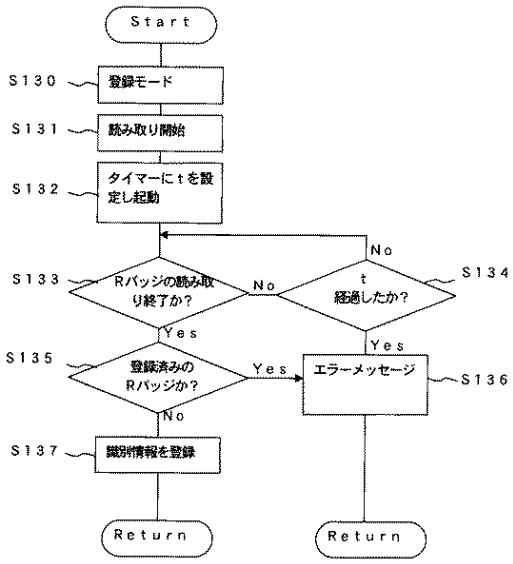
【図１８】

ものなど身につけるものに内蔵されるタイプがある。」（段落【０１０４】）

「他にも，財布・パスケース等の本体にＩＣチップ５１とアンテナ２２が内蔵される。筆記用具・ライター等の本体にＩＣチップ５１とアンテナ２２が内蔵されたものなど身近におくものに内蔵されるタイプがある。」（段落【０１０５】）

「以上，例に挙げたものだけでなく，様々なものにＩＣチップ５１を内蔵することができアンテナ２２の形状も多様である。」（段落【０１０６】）

「識別情報３５０を登録する動作について，図２０のフローチャートを用いて説明する。以下，フローチャートではレッドバッジ７０をＲバッジとする。」（段落【０１１１】）



【図２０】

「まず，携帯端末１０にレッドバッジ７０の識別情報３５０を登録するための登録モードにする（Ｓ１３０）。この登録モードにする際には，暗証番号やバイオメトリックス（アイリス，声紋，指紋など）を入力しないと登録モードにならないようにし，第３者では登録できないようにする。登録モードになると，読み取り開始のコマンドを制御部４０から通信制御用ＩＣ２１に送信するとアンテナ２２から発信要求（パワーパルスなど）を発信してレッドバッジ７０の読み取りを開始する（Ｓ１３１）。」（段落【０１１２】）

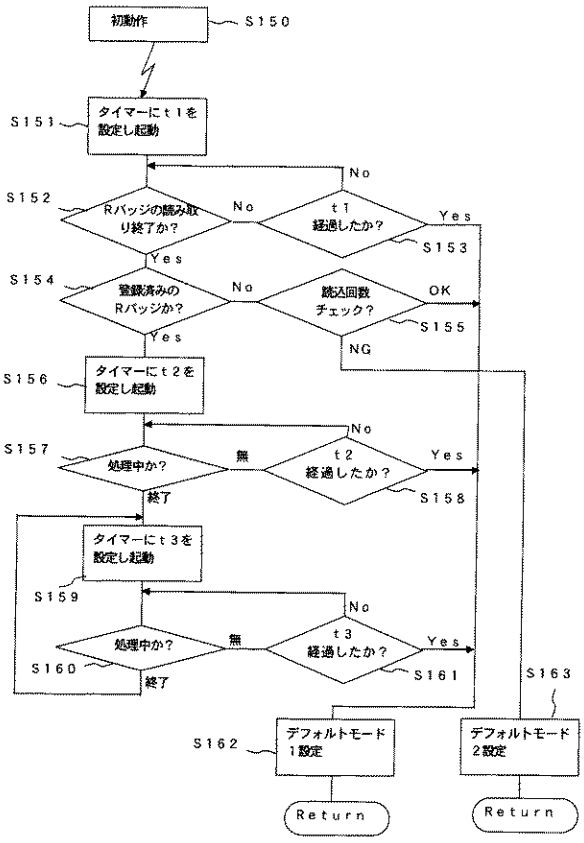
「ここで，携帯端末１０のタイマーに所定の時間ｔを設定する（Ｓ１３

２）。そこで，時間ｔが経過するまで（Ｓ１３４），レッドバッジ７０から識別情報３５０を受信したか繰り返しチェックする（Ｓ１３３）。」（段落【０１１３】）

「時間ｔが経過しても，レッドバッジ７０から識別情報３５０の受信が完了しない場合は，携帯端末１０の画面上にエラーメッセージを表示する（Ｓ１３５）。或いは，受信した識別情報がすでに登録済みの識別情報の場合には，携帯端末１０の画面上にエラーメッセージを表示する（Ｓ１３５）。」（段落【０１１４】）

「受信した識別情報３５０が登録済みの識別情報でない場合は，識別情報３５０を携帯端末１０のメモリ３０に格納して登録する。」（段落【０１１５】）

「携帯端末１０を使用する際に，近傍にあるレッドバッジ７０の識別情報３５０を確認する動作について，図２１のフローチャートを用いて説明する。図２１のフローチャートで説明するデフォルトモード１は，操作を開始しレッドバッジ７０の識別情報３５０が読み込まれたときに解除されるもので，通常操作を行っていない状態とする。また，デフォルトモード２は，いたずらされている可能性があるため，解除には暗証番号やバイオメトリックスなどを入力して本人である確認をする必要がある状態と



【図２１】

して以下説明する。」（段落【０１１６】）

「まず，携帯端末１０を使用する者がキー入力などの携帯端末１０を使用するための初動作を行った時点で，制御部４０のＣＰＵには割り込みが発生する（Ｓ１５０）。割り込みが発生すると，読み取り開始のコマンドを制御部４０から通信制御用ＩＣ２１に送られる。通信制御用ＩＣ２１は，読み取り開始のコマンドを受け取るとアンテナ２２から発信要求を発信して読み取りを開始する。」（段落【０１１７】）

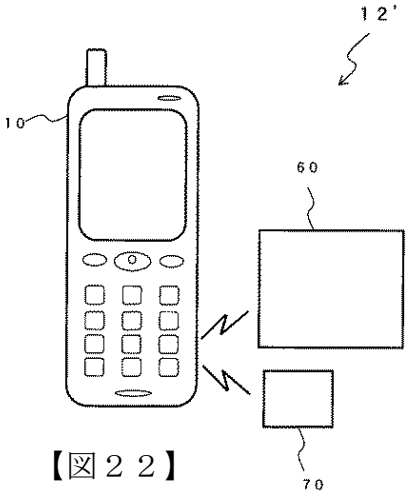
「ここで，制御部４０はタイマーに所定の時間ｔ１を設定し（Ｓ１５１），レッドバッジ７０から発信した識別情報３５０を受信したかチェックする（Ｓ１５２）。時間ｔ１が経過するまで識別情報３５０の受信したかを繰り返しチェックする（Ｓ１５３）。時間ｔ１が経過しても，レッドバッジ７０から識別情報３５０の受信が完了しない場合は，デフォルトモード１を設定する（Ｓ１６２）。」（段落【０１１８】）

「識別情報３５０の受信が完了した場合は，受信した識別情報がメモリ３０に予め登録されている識別情報と比較し，該当するものがある場合には，登録済みのレッドバッジ７０が近くにあるので携帯端末１０の利用が可能である（Ｓ１５４）。該当するものがない場合には，登録済みのレッドバッジ７０ではない。そこで，登録されてない識別情報の受信回数が指定の回数より少ない場合は，デフォルトモード１を設定する（Ｓ１６２）が，登録されてない識別情報の受信回数が指定の回数より多い場合は，デフォルトモード２を設定する（Ｓ１６３）。」（段落【０１１９】）

「登録されている識別情報を受信した場合には（Ｓ１５４），さらに，所定の時間ｔ２をタイマーに設定する（Ｓ１５６）。時間ｔ２が経過するまでに（Ｓ１５８），通話・メール受信・インターネットのアクセスなどの処理を開始しなかった場合は（Ｓ２０７），デフォルトモード１を設定する（Ｓ１６２）。」（段落【０１２０】）

「時間ｔ２が経過するまでに（Ｓ１５８），開始した通話・メール受信・インターネットのアクセスなどの処理が終了した場合は（Ｓ１５７），所定の時間ｔ３をタイマーに設定する（Ｓ１５９）。時間ｔ３が経過するまでに（Ｓ１６１），通話・メール受信・インターネットのアクセスなどの次の処理を開始した場合には（Ｓ１６０），レッドバッジ７０の読み込みをすることはなく，引き続き作業を行うことができる。一つの作業が終了するたびにｔ３が起動され（Ｓ１５９），ｔ３以内に次の作業が開始されないときは（Ｓ１６１），デフォルトモード１になる（Ｓ１６２）。」（段落【０１２１】）

「さらに，図２２に示す使用者識別システム１２'のように，第２の実施の形態で説明したように，携帯端末１０に定期券・乗車券・クレジットカード・鍵などの機能を内蔵させ，その機能を受信装置６０で受け取る場合に，まず，携帯端末１０の使用者が正当な使用者かをレッドバッジ７０で確認を取るようにすることも可能である。」（段落【０１２６】）



【図２２】

「以上，説明したようにレッドバッジに組み込んだ携帯記録素子の識別情報を確認して携帯端末１０の使用を可能にすることができ，正当な使用者にのみ使用を許可することができる。」（段落【０１２７】）

(2) 本件発明の特許請求の範囲の記載及び本件明細書等における上記記載によれば，本件発明は，①ＲＦＩＤインターフェースを利用した情報保護技術の分野において，②携帯電話に個人情報や金銭的価値のある情報を統合して管理する場合に当該情報の第三者による不正使用を確実に防止するための情報保護システムを提供するという課題を解決するため，③携帯電話にＲＦＩＤ

インターフェースを備えるとともに，当該携帯電話のスイッチを押すことなどで生成されるトリガ信号に応答し，Ｒバッジと通信することで識別情報を受け取り，当該識別情報と当該携帯電話に予め記録してある識別情報とを比較し，その比較結果に応じて，被保護情報に対するアクセス要求を許可又は禁止するアクセス制御手段を備えるものであり，アクセス要求を許可する場合は，前記アクセス要求から所定時間が経過するまでは前記被保護情報へのアクセスを許可することを特徴とするものであるということができる。

２　争点３－２（乙１１に基づく進歩性の欠如）

事案に鑑み，争点３－２から判断するに，本件発明は，以下の点から進歩性を欠くというべきである。

(1) 乙１１公報の記載

ア　特許請求の範囲

「一定時間ごとあるいは操作ごとに電磁波信号を送受信し，データの授受を行い，かつ前記データを記憶する手段を有する第１のデータ読み取り装置を含み，かつデータ入力装置を備えた電子情報機器と，前記電磁波信号を送受信し，前記データの授受を行い，かつ前記データを記憶する手段を有する第２のデータ読み取り装置を含むＩＤカードとを有することを特徴とする電子機器。」（【請求項１】）

イ　発明の属する技術分野

「本発明は，携帯電話あるいはパーソナルコンピュータ等の電子機器およびその制御方法に関するものである。」（段落【０００１】）

ウ　従来の技術

「従来より，携帯電話やパーソナルコンピュータ等の電子情報機器においては，第三者による盗難あるいは内部データの盗用による被害が問題となっている。そのような被害を防止する方法として，携帯電話あるいはパーソナルコンピュータに対して，パスワードの設定を行うといった方法が

とられている。」（段落【０００２】）

エ　発明が解決しようとする課題

「しかし，上記のような従来の方法では，例えば第三者に携携帯電話あるいはパーソナルコンピュータを盗難されると，設定されたパスワードは試行錯誤を繰り返すことにより破られる場合があり，第三者の使用，内部データの盗用あるいは破壊を防止することは困難であった。」（段落【０００３】）

「本発明は，上記のような問題を解決するためになされたものであり，盗難防止，または内部データの保護を可能にした電子機器およびその制御方法を提供するものである。」（段落【０００４】）

オ　課題を解決するための手段

「本発明の電子機器は，一定時間ごとあるいは操作ごとに電磁波信号を送受信し，データの授受を行い，かつ前記データを記憶する手段を有する第１のデータ読み取り装置を含み，かつデータ入力装置を備えた電子情報機器と，前記電磁波信号を送受信し，前記データの授受を行い，かつ前記データを記憶する手段を有する第２のデータ読み取り装置を含むＩＤカードとを有する。」（段落【０００５】）

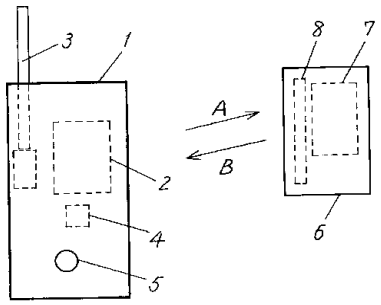
「本発明の電子機器の制御方法は，データ入力時，例えば電源投入時あるいは一定時間ごとに前記第１のデータ読み取り装置により読み出された，前記ＩＤカード内に記録されたデータと，前記第１のデータ読み取り装置内にあらかじめ記憶されているデータと，さらに前記データ入力装置により入力されたデータとを比較することにより，前記電子機器の動作を制御することを特徴とするものである。」（段落【０００６】）

「本発明によれば，第１のデータ読み取り装置により読み出された，ＩＤカード内に記録されたデータと，第１のデータ読み取り装置内にあらかじめ記憶されているデータと，さらにデータ入力装置により入力されたデ

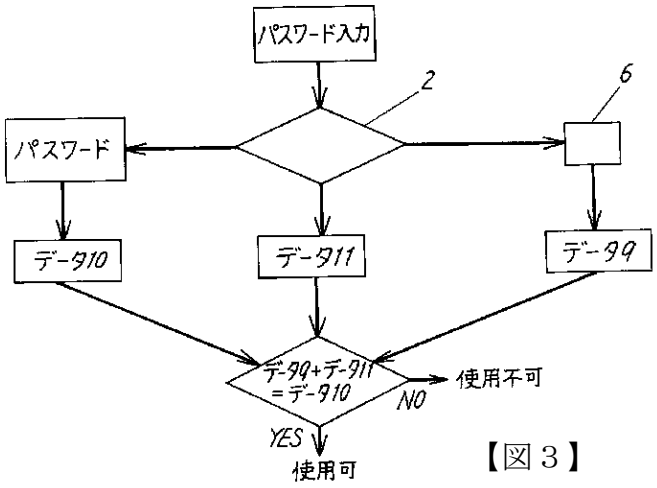
ータとの三者を比較し，これらのデータ間に一定の関係がある場合にのみ携帯電話あるいはパーソナルコンピュータ等の電子機器の使用あるいは動作を可能にするものである。」（段落【０００７】）

カ　発明の実施の形態

「図１および図３は本発明の第１の実施の形態である携帯電話用電子機器およびその動作を示す。図１に示すように携帯電話用電子機器は，第１のマイクロプロセッサーユニット（ＭＰＵ）および第１の強誘電体メモリ（ＦＲＡＭ）を有する第１のデータ読み取り装置２と，第１のアンテナおよび第１のフロントエンドＩＣを有する第１の電波信号送受信装置３と，水晶発振器を有する計時装置４と，キー５とを備えた携帯電話１と，第２のＭＰＵおよび第２のＦＲＡＭを有する第２のデータ読み取り装置７と，第２のアンテナおよび第２のフロントエンドＩＣを有する第２の電波信号送受信装置８とを備えたＩＤカード６とから構成されている。第１の電波信号送受信装置３と計時装置４とキー５との間は導線により接続されている。また，第２のデータ読み取り装置７と，第２の電波信号送受信装置８との間は導線により接続されている。携帯電話１とＩＤカード６との間のデータの授受は，電波信号Ａおよび電波信号Ｂを介して行われる。」（段落【０００９】）



【図１】



【図３】

「図３は，図１に示す携帯電話用電子機器の動

作を表す流れ図である。データ９は，ＩＤカードに記憶されているデータ，データ１０およびデータ１１は第１のデータ読み取り装置２内に記憶されているデータであり，データ１０はパスワードの値に等しいデータである。表１はデータ９，データ１０およびデータ１１の時間変化を表す表である。データ９とデータ１１との和がデータ１０に等しい場合にのみ携帯電話１が使用可能である。」（段落【００１０】）

「携帯電話１の電源を投入した時あるいは通話のためにキー５を押したときに携帯電話１より第１の電波信号送受信装置３を介して電波信号Ａを送信する。ＩＤカード６は電波信号Ａを受信するとＩＤカード６にあらかじめ記憶されたデータ９を，電波信号Ｂを介して自動的に送信する。例として，ここではデータ９の値を４桁の数字３０００とする。データ読み取り装置２はデータ９を受信する。一方，携帯電話１はＩＤカード６への電波信号Ａを送信すると同時に使用者に対しパスワードの入力を要求する。パスワードは携帯電話のキー５を用いて入力する。例として，ここではパスワードの値を４桁の数字５４３２とする。このパスワードは携帯電話１の持主しか知らない。入力されたパスワードはデータ１０として第１のデータ読み取り装置２内に記憶される。また，第１のデータ読み取り装置２内にはあらかじめデータ１１が記憶されている。例として，ここではデータ１１の値を４桁の数字２４３２とする。ここで，ＩＤカード６より受信したデータ９と，パスワードとして入力されたデータ１０と，第１のデータ読み取り装置２内にあらかじめ記憶されたデータ１１とを比較し，データ９とデータ１１との和がデータ１０になる場合にのみ携帯電話１が使用可能である。すなわち，

	データ９	データ１１	データ１０
電源投入時	３０００	２４３２	５４３２
⋮	⋮	⋮	⋮
書き換え前	２０００	３４３２	５４３２
書き換え後	１５００	３９３２	５４３２
⋮	⋮	⋮	⋮

【表１】

表１に示すように３０００＋２４３２＝５４３２となったときにのみ，携帯電話１が使用可能になる。」（段落【００１２】）

「携帯電話１の電源が投入されている状態のとき，計時装置４は電源が投入されてからの時間を計時する。計時装置４の計時時間をもとに，表１に示すように一定時間，例えば１０分ごとに第１のデータ読み取り装置２内にてデータ１１を書き換え，同時にＩＤカード６に電波信号Ａを送信し，ＩＤカード６内のデータ９を書き換える。例として，書き換えられる前のデータ９およびデータ１１の値をそれぞれ２０００，３４３２，書き換えられた後のデータ９およびデータ１１の値をそれぞれ１５００，３９３２とする。そして一定時間，例えば１０分ごとにＩＤカード６に対しデータ９の送信を要求する。携帯電話１とＩＤカード６との間でデータのやりとりが行われ，データ９とデータ１１の和がデータ１０になるときは常に携帯電話１を使用可能にする。すなわち，上記の例では２０００＋３４３２＝１５００＋３９３２＝５４３２となる場合にのみ携帯電話１が使用可能になる。携帯電話１とＩＤカード６の距離が離れていると，ＩＤカード６からデータ９が送信されることはない。ここでデータ９の送信がなければ自動的に電源が切れ，携帯電話１の使用を不可能にする。再び携帯電話１を使用したい場合には，ＩＤカード６を携帯電話１に近づけた後電源をオンし，パスワードを入力することから始めなければならない。従って，ＩＤカード６と携帯電話１との間でデータの授受がある限りパスワードの再入力をする必要はなくなる。」（段落【００１３】）

「万一，ＩＤカード６を紛失したり，盗難にあう等して携帯電話１とＩＤカード６との間でデータの授受ができなくなったとき，携帯電話１の使用が不可能である。また，第三者のＩＤカードを持ってきて携帯電話に近づけた後電源を投入し，パスワードを入力しても，ＩＤカード内のデータ９が，データ９とデータ１１の和がデータ１０であるという関係を満たさ

ないので携帯電話１の使用が不可能である。すなわち第三者による携帯電話１の使用が不可能である。」（段落【００１４】）

「なお，携帯電話１がＩＤカード６に電波を送信する時間を，本実施の形態においては１０分としたが，使用者により自由に設定をしてもよく，例えば１分あるいは１時間としてもよい。」（段落【００１５】）

「また，データ１１の書き換えを行う時間を，本実施の形態においては１０分としたが，使用者により自由に設定をしてもよく，例えば１分あるいは１時間としてもよい。また，データ１１の書き換えを行う時間とＩＤカード６に電波を送信する時間とが異なっていてもよい。」（段落【００１６】）

「データ９，データ１０およびデータ１１を関係づけるのに，データ９とデータ１１の和がデータ１０になるという数式を用いる代わりに，一定の数式または論理式で関係づけられていればよい。例えば，データ９とデータ１１の積がデータ１０になるようにしてもよい。また，データ９，データ１０およびデータ１１を関係づける一定の数式または論理式は，一定の時間ごとに変化してもよい。」（段落【００１８】）

「携帯電話１とＩＤカード６との間のデータの授受を行うのに，電波の代わりに赤外線または可視光等の電磁波を用いてもよい。」（段落【００１９】）

(2) 乙１１発明の内容

前記(1)によれば，乙１１発明は，携帯電話とＩＤカードから成る電子機器であって，当該携帯電話の電源又はキーを押した際に，ＩＤカードと無線通信を行うとともに操作者にパスワードを要求し，ＩＤカードから受信したデータ及び入力されたパスワードのデータと当該携帯電話に記憶していたデータの３者を演算処理し，その演算結果が所定の条件を満たす場合には携帯電話の使用を可能とし，その後，一定時間ごとにＩＤカードと通信し，新た

にＩＤカードから受信したデータ及び先に入力されたパスワードのデータと当該携帯電話に記憶していたデータの３者を演算処理し，その演算結果が所定の条件を満たす場合に携帯電話の使用を可能とし続けることなどを特徴とするものであると認めることができる。

(3) 本件発明との対比

前記(1)及び(2)によれば，本件発明と乙１１発明は，以下の相違点Ａ～Ｄにおいて相違し，その余の点においては一致するということができる。

ア　相違点Ａ

本件発明は，「ＲＦＩＤインターフェースを有する携帯電話」（構成要件Ａ）であるのに対し，乙１１発明は，ＩＤカードと無線通信はするものの，ＲＦＩＤインターフェースを有するか不明である点

イ　相違点Ｂ（被告主張に係る相違点３）

本件発明は，携帯電話が「Ｒバッジ」（構成要件Ｃ，Ｄ）と送受信をするとされるの対し，乙１１発明は，携帯電話が「ＩＤカード」と無線通信をするとされ，両者の関係が不明である点

ウ　相違点Ｃ（被告主張に係る相違点１）

本件発明が，「受け取った識別情報と当該携帯電話に予め記録してある情報の比較」（構成要件Ｄ）をするのに対し，乙１１発明は，ＩＤカードから受け取ったデータとパスワードとして入力されたデータとの和と携帯電話に記憶されていたデータとの比較をする点

エ　相違点Ｄ（被告主張に係る相違点２）

本件発明が，「アクセス要求が許可されてから所定時間が経過するまでは前記被保護情報へのアクセスを許可する」（構成要件Ｆ）のに対し，乙１１公報には，携帯電話の使用が可能となる「一定時間」が「アクセス要求が許可」された時点からであることの記載がない点

(4) 相違点の認定について

原告は，相違点Ａについて，構成要件Ａ及びＤが有機的な関連性を有するとして，本件発明と乙１１発明の相違点は前記相違点①のとおり認定されるべきであると主張する。

しかし，本件発明の構成要件Ａは「ＲＦＩＤインターフェースを有する携帯電話であって，」と規定するのみであり，同記載によれば，携帯電話がＲＦＩＤインターフェースを備えていれば足りると解するのが相当であり，その作用効果や用途についての限定は存在しない。他方，構成要件Ｄについても，「前記Ｒバッジより識別情報を受け取って，該受け取った識別情報と当該携帯電話に予めしてある識別情報との比較を行う比較手段と，」と規定しているのみであり，Ｒバッジが受け取る識別情報について，ＲＦＩＤインターフェースとの関連で限定がされているものではない。

これに対し，原告は，本件明細書等の段落【００１６】，【０１０７】の記載に基づき，本件発明においては，Ｒバッジの固有の識別情報を利用することにより，被保護情報に対する第三者の不正アクセスを防止することを目的としており，その意味において構成要件Ａ及びＤには有機的な関連性があると主張するが，構成要件Ｄの識別情報がＲバッジの固有の識別情報に限定されないことは，構成要件Ｄの文言や，本件明細書等の段落【００２８】における「照合用データとは，ＩＣカードアセンブリの所有者を一意に特定するためのデータであり，その内容は特に限定されるものではない。」との記載などに照らしも明らかである。

したがって，構成要件Ａ及びＤとの間に原告が主張するような有機的関連性があるということはできず，本件発明と乙１１発明の相違点は，各構成要件に即して認定すれば足りるというべきである。

(5) 相違点Ａについて

相違点Ａのとおり，乙１１公報には，乙１１発明に係る携帯電話がＲＦＩＤインターフェースを有する旨の明示的な記載は存在しない。

しかし，乙１１発明の携帯電話１は，第１の電波信号送受信装置３を有しており（乙１１公報の段落【０００９】），これは無線通信を行うインターフェースといい得る上，乙１１公報のＩＤカード６には電源は存在せず，上記電波信号送受信装置を介して送信される電波信号Ａに応答して，ＩＤカード６に予め記憶されたデータ９が電波信号Ｂを介して携帯電話１に自動的に送信されるのであり（同公報の段落【０００９】，【００１２】），このようなデータの送受信の処理はＲＦＩＤを用いた場合の処理と同一であるということができる。

また，乙１１公報の段落【００１９】には，「携帯電話１とＩＤカード６との間のデータの授受を行うのに，電波の代わりに赤外線または可視光等の電磁波を用いてもよい。」と記載され，他方，本件明細書等の段落【００２７】には，「ＲＦＩＤにはさまざまな変調方式や周波数，通信プロトコルを利用したものがあるが，本発明は特定の方式に限定されるものではなく，どのような方式を利用してもよい。」との記載がある。

そうすると，乙１１発明の「第１の電波信号送受信装置３」は本件発明の「ＲＦＩＤインターフェース」と実質的に一致するというべきであり，仮にそうでないとしても，ＲＦＩＤインターフェースは本件明細書等の段落【００２７】に記載されているとおり，本件特許出願時には既に確立されていた技術であるから，当業者であれば，相違点Ａに係る構成を容易に想到し得たものというべきである。

(6) 相違点Ｂについて

本件発明の「Ｒバッジ」に関し，本件明細書等の段落【００３３】には「…ＩＣアセンブリは，小型チップとしてさまざまな物体に埋め込むことが可能なものである。以上，本発明の目的において，ＩＣアセンブリを装飾品や衣類など所有者の身近におくことが可能な物体に埋め込んだものを「Ｒバッジ」と総称する。」と記載されている。

他方，乙１１発明における「ＩＤカード」は，乙１１公報の記載によれば，ＭＰＵ及びＦＲＡＭを有するデータ読み取り装置とアンテナ及びフロントエンドＩＣを有する電波信号送受信装置とを備えるものであるから（段落【０００９】），ＩＣアセンブリを埋め込んだものということができる。また，ＩＤカードは，その性質上，所有者の身近に置くことが想定されるものであるから，乙１１発明における「ＩＤカード」は本件発明の「Ｒバッジ」に相当する。

したがって，相違点Ｂは実質的な相違点ではない。

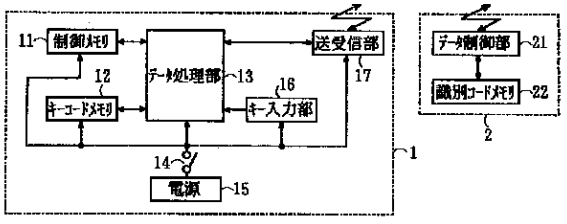
(7) 相違点Ｃについて

ア　相違点Ｃは，要するに，本件発明においては，携帯電話側の情報とＲバッジ側の情報という２つのデータの比較に基づいて認証処理が行われるのに対し，乙１１発明においては，これにパスワードを加えた３つのデータの演算に基づいて認証処理が行われるということにある。

イ　被告は，乙１１発明に乙１２発明を適用すれば，当業者は，相違点Ｃに係る構成を容易に想到することができたと主張する。

(ｱ) そこで，検討するに，乙１２公報には，以下の記載がある。

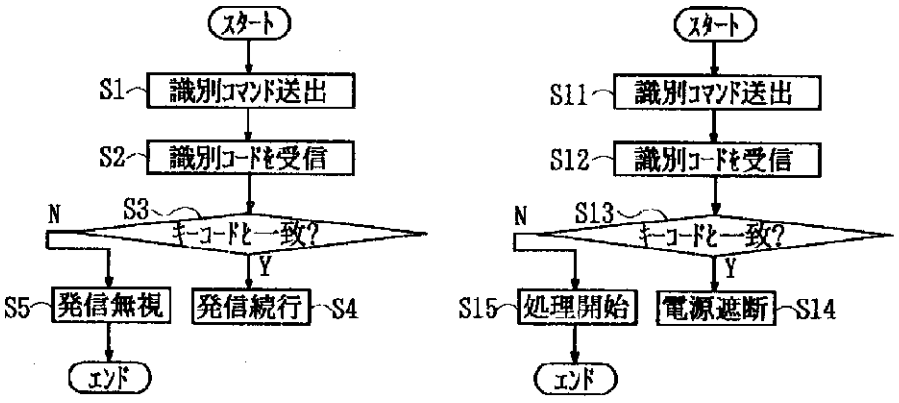
「本発明の一実施の形態による携帯情報機器は，図１に示すように，予め正当な操作者の識別コードを記憶した識別コードメモリ２２と，この識別コードメモリ２２に記憶された識別コードを送出するデータ制御部２１とを有する識別ユニット２と，電源１５のオン／オフを行なうスイッチ１４と，このスイッチ１４の操作者を確認するキーコードを記憶するキーコードメモリ１２と，このキーコードメモリ１２に記憶されたキーコードに基づき，スイッチ１４による電源１５オンによって識別コ



【図１】

マンドを送出し，このキーコードと識別コードとを比較するデータ処理部１３と，このデータ処理部１３にキーコード及び識別コマンドを入力するキー入力部１６と，データ処理部１３から送出された識別コマンドを識別ユニット２へ送出して識別コードを受信し，かつデータ処理部１３に送出する送受信部１７と，キー入力部１６から入力されたキーコード及び識別コマンドを一時記憶する制御メモリ１１とを備えた情報ユニット１とで構成される。」（段落【００１０】）

「本発明の一実施の形態による携帯情報機器の動作は，図１に示すように，携帯電話発信時を例にすると，まず，キー入力部１６からキーコード＂３９３５５３０＂を入力してキーコードメモリ１２にデータ処理部１３が記憶し，かつ送受信部１７を介して識別ユニット２のデータ制御部２１に送出され，キーコード＂３９３５５３０＂が識別コードとして識別コードメモリ２２に記憶される。」（段落【００１２】）



（A）　　（B）

【図２】

「その後，図２の（Ａ）に示すように，正当な操作者が発信操作をする場合，送受信部１７を介してデータ処理部１３から識別コマンドが送出され（ステップＳ１），この識別コマンドをデータ制御部２１が受信（ステップＳ２）して識別コードメモリ２２の識別コード＂３９３５５３０＂を送受信部１７へ送出し，この識別コード＂３９３５５３０＂と

キーコードメモリ１２のキーコード＂３９３５５３０＂とをデータ処理部１３が比較（ステップＳ３）して一致すれば発信処理を続行（ステップＳ４）させ，電話番号を発信することができる。」（段落【００１３】）

「一方，図２の（Ａ）に示すように，第三者が発信操作をする場合，送受信部１７を介してデータ処理部１３から識別コマンドが送出され（ステップＳ１），この識別コマンドをデータ制御部２１が受信（ステップＳ２）する識別ユニット２を第三者が所持していないため，識別コード＂３９３５５３０＂とキーコード＂３９３５５３０＂とを比較（ステップＳ３）できずに発信無視され，あるいは第三者が所持する識別コードが＂９５６４２２２＂の時は，キーコード＂３９３５５３０＂と不一致となり，発信無視（ステップＳ５）となって電話番号を発信できない。」（段落【００１４】）

(ｲ) 上記(ｱ)によれば，乙１２公報には，情報ユニット及び識別ユニットのそれぞれが有する２個のデータの比較によって，情報ユニットの認証処理をするという技術的事項が開示されているということができる。そして，乙１２発明は，乙１１発明と技術分野及び課題が共通しているのであるから，当業者にとって，乙１１発明に前記の技術的事項を適用し，使用者が入力するパスワードを含む３つのデータの演算による認証処理に代え，本件発明のように，２個のデータの比較による認証処理を採用することは，容易に想到し得たというべきである。

ウ　これに対し，原告は，乙１１発明において，パスワードを含む３つのデータを用いた複雑な構成にすることは，その課題解決にとって不可欠なものであるので，乙１１発明に乙１２発明を組み合わせる動機付けは存在しないと主張する。

しかし，乙１１発明は，携帯電話等にパスワードを設定するのみでは不

正使用の防止としては十分ではないという課題を解決するため，ＩＤカード等の携帯電話以外の物体に記憶されたデータを利用し，携帯電話等に予め記憶されたデータとの間で比較・照合することにより，不正使用を防止しようとするものであって，この点において，本件発明及び乙１２発明とその技術的な思想を共通にしているということができる。

もとより，乙１１発明は，携帯電話等に記憶されたデータとＩＣカードに記憶されたデータという二種類のデータを使用するにとどまらず，使用者が入力したパスワードも加えて比較・照合を行う点で本件発明と異なるが，これは，比較・照合に使用するデータを更に一種類増やすことにより安全性を高めようとしたものであって，上記技術思想と基本的に異なるものではなく，また，乙１１公報には，ＩＤカード６と携帯電話１との間でデータの授受がある限りパスワードの再入力をする必要がないようにするなど（乙１１公報の段落【００１４】），パスワードの入力作業により生じる操作の煩瑣性の軽減という課題も示唆されているということができる。

そして，本件明細書等の段落【００２８】に記載されているように，３つのデータを利用する代わりに２つのデータを利用したとしても，一意なデータを複数組み合わせたものやこれを暗号化したものを照合用データとして利用するなど，様々な工夫をすることにより不正使用の防止という課題を解決することは可能であるから，乙１１公報に接した当業者は，操作の煩瑣性を軽減するため，３つのデータを利用する代わりに，乙１２公報に開示されているような２つのデータによる比較・照合する構成を容易に想到し得たというべきであり，かかる構成を採用したとしても，上記のとおり，不正使用の防止という効果を奏することが可能であることを十分に認識し得たものと考えられる。

したがって，相違点Ｃに係る構成は，乙１１発明に乙１２発明を適用することにより，当業者が容易に想到し得たものというべきである。

(8) 相違点Ｄについて

相違点Ｄに関し，乙１１公報には，「携帯電話１の電源を投入した時あるいは通話のためにキー５を押したときに携帯電話１より第１の電波信号送受信装置３を介して電波信号Ａを送信する。ＩＤカード６は電波信号Ａを受信するとＩＤカード６にあらかじめ記憶されたデータ９を，電波信号Ｂを介して自動的に送信する。…ＩＤカード６より受信したデータ９と，パスワードとして入力されたデータ１０と，第１のデータ読み取り装置２内にあらかじめ記憶されたデータ１１とを比較し，データ９とデータ１１との和がデータ１０になる場合にのみ携帯電話１が使用可能である。」（段落【００１２】），「携帯電話１の電源が投入されている状態のとき，計時装置４は電源が投入されてからの時間を計時する。計時装置４の計時時間をもとに，…一定時間…ごとに第１のデータ読み取り装置２内にてデータ１１を書き換え，同時にＩＤカード６に電波信号Ａを送信し，ＩＤカード６内のデータ９を書き換える。携帯電話１とＩＤカード６との間でデータのやりとりが行われ，データ９とデータ１１の和がデータ１０になるときは常に携帯電話１を使用可能にする。…携帯電話１とＩＤカード６の距離が離れていると，ＩＤカード６からデータ９が送信されることはない。ここでデータ９の送信がなければ自動的に電源が切れ，携帯電話１の使用を不可能にする。」（段落【００１３】）との記載がある。

上記記載によれば，乙１１発明においては，最初に携帯電話の電源を投入した際の演算結果を満たせば，少なくとも一定時間，携帯電話の使用が可能になるものと認められる。そして，携帯電話１の電源の投入は本件発明の「アクセス要求」に相当するから，乙１１発明は，「アクセス要求が許可されてから所定時間が経過するまでは前記被保護情報へのアクセスを許可する」構成を備えるということができる。

したがって，相違点Ｄは，実質的な相違点には当たらない。

(9) 小括

以上のとおり，本件発明と乙１１発明の相違点Ａ～Ｄに係る各構成は，相違点に該当しないか，当業者が容易に想到し得たものであるので，乙１１発明は進歩性を欠き，特許無効審判によって無効とされるべきものである。

３　争点３－３（乙１６に基づく拡大先願違反）

また，念のため，争点３－３も検討するに，以下のとおり，本件発明は，いわゆる拡大された先願と同一の発明にも当たるということができる。

(1) 乙１６公報の記載

ア　特許請求の範囲

「操作者が特定の使用者であると認証判定された場合に，ダイヤルロックの解除を行う携帯電話機の自動ダイヤルロックシステムにおいて，

動作処理要求に伴った一連の操作が発生すると，前記認証を行うためのトリガとなるロック解除コードを出力する携帯電話機と，前記ロック解除コードに基づいて認証演算を実施し，該認証演算の結果を前記携帯電話機に対して出力するロック解除装置とからなり，

前記携帯電話機は，ロック解除装置より供給された認証演算結果に基づいて認証処理を実施し，認証判定を行うことを特徴とする携帯電話機の自動ダイヤルロックシステム。」（【請求項１】）

「認証処理は，携帯電話機の電源投入時に該携帯電話機内部にて演算された第１の認証演算結果と，ロック解除装置より供給された第２の認証演算結果を，前記携帯電話機内部にて比較し，前記第１及び第２の認証演算結果が一致した場合に，当該操作者が特定の使用者であると認証判定することを特徴とする請求項１記載の携帯電話機の自動ダイヤルロックシステム。」（【請求項２】）

「第１の認証演算結果は，携帯電話機内部にて生成されたロック解除コードと，あらかじめ携帯電話機内部に記憶されている特定の使用者を示す

ＩＤ情報とで認証演算を行うことにより得られた値であって，第２の認証演算結果は，ロック解除装置内部にて，前記携帯電話機より供給されたロック解除コードと，あらかじめロック解除装置内部に記憶されている前記特定の使用者を示すＩＤ情報とで，前記携帯電話機内部で行われたのと同一の認証演算を行うことにより得られた値であることを特徴とする請求項２記載の携帯電話機の自動ダイヤルロックシステム。」（【請求項３】）

「ロック解除コードは，携帯電話機の電源投入時に該携帯電話機内部にて生成された乱数であることを特徴とする請求項１から請求項３のうちのいずれか１記載の携帯電話機の自動ダイヤルロックシステム。」（【請求項５】）

「携帯電話機とロック解除装置間で行われる通信における信号の最大強度は，前記信号の到達距離が１ｍ程度となるように設定されることを特徴とする請求項１から請求項３のうちのいずれか１記載の携帯電話機の自動ダイヤルロックシステム。」（【請求項９】）

イ　発明の属する技術分野

「この発明は携帯電話機の自動ダイヤルロックシステムに係り，特に携帯電話機のセキュリティー保護を高度に実現し得る携帯電話機の自動ダイヤルロックシステムに関するものである。」（段落【０００１】）

ウ　従来の技術

「従来より，携帯電話機等の携帯端末のセキュリティー保護を実現するための方法や装置等がいくつか提案されている。例えば，特開平６－２７６１４８号公報に示された移動体無線機では，あらかじめ移動体無線機本体固有のデジタルコードを該移動体無線機本体内部の不揮発性メモリに格納しておき，前記移動体無線機とは別に移動体無線機本体内のデジタルコードと一致するコードを送出する携帯可能な無線発信機を設け，前記移動体無線機が前記無線発信機より送出されるコードを受信すると，移動体無

線機本体の電子ロックが解除され使用可能な状態となるように構成された装置が開示されている。」（段落【０００２】）

エ　発明が解決しようとする課題

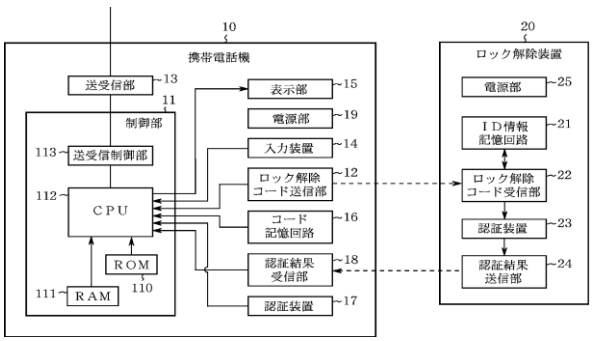
「従来の携帯電話機のダイヤルロックシステムは以上のように構成されているので，ロック解除装置側から所定の送信周期で微弱電波（ロック解除コード）を携帯電話機に送信しなければならず，ロック解除装置側の電力消費が大きくなるという課題があった。」（段落【００１２】）

「また，電力消費を少なくするために，微弱電波（ロック解除コード）の送信周期を長くした場合，ダイヤルロック状態で特定（正規）の使用者（ロック解除装置を身に付けた使用者）が携帯電話機に近づき発信しようとしても，所定時間（送信周期）経過しなければダイヤルロックが解除されない（待ち時間が発生する）という課題があった。」（段落【００１３】）

「この発明は上記のような課題を解決するためになされたもので，ダイヤルロックが待ち時間なくリアルタイムに解除され，且つロック解除装置側の電力消費の少ない携帯電話機の自動ダイヤルロックシステムを得ることを目的とする。」（段落【００１４】）

オ　発明の実施の形態

「図１において，１０は携帯電話機，２０はロック解除装置である。携帯電話機１０内において，１１は携帯電話機１０全体の制御を行う制御部であり，１２はロック解除装置２０に微弱電波を用いてロック解除コードを送信するロック解除コード送信部であり，１３は無線基地局との間で音声またはデータ呼の発着



【図１】

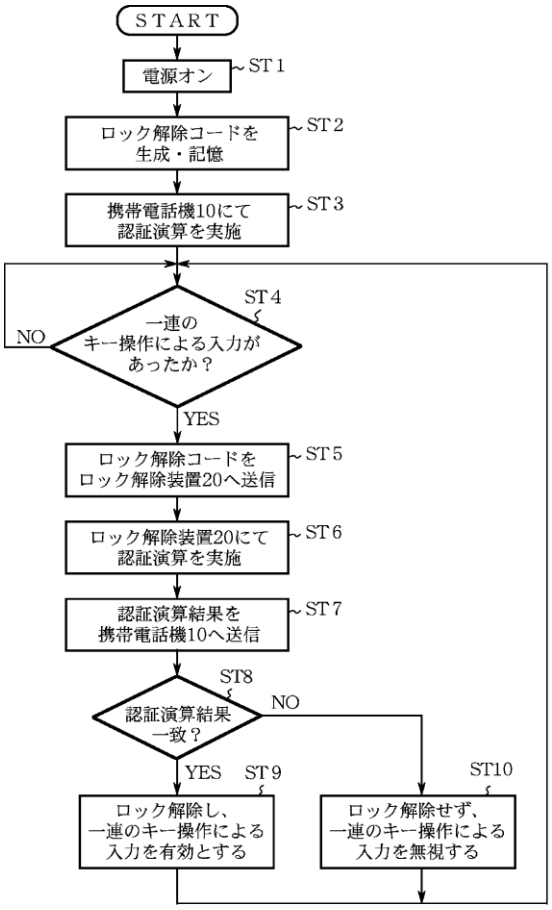
信を行う送受信部であり，１４はキーボード等を備え，該キーボードにより携帯電話機使用者からの操作指示情報や発信の相手先番号等のデータを入力し制御部１１へ通知する入力装置であり，１５は制御部１１からの各種の情報を表示するための表示部であり，１６はロック解除コード，ＩＤ情報，並びに認証演算結果をあらかじめ記憶したＥＥＰＲＯＭ等から成るコード記憶回路であり，１７はこれらロック解除コード，ＩＤ情報を用いて認証演算を行う認証装置であり，１８は，ロック解除コード送信部１２がロック解除コードをロック解除装置２０に送信した後，該ロック解除装置２０から送られて（返送されて）きた認証演算結果を制御部１１に通知する認証結果受信部であり，１９は上記各部に必要な電源を供給する電源部である。」（段落【００２５】）

「また，制御部１１内において，１１２はプログラムを格納したＲＯＭ１１０及びデータ処理用のＲＡＭ１１１を用いて全体の制御を行うＣＰＵであり，１１３は送受信部１３を制御する送受信制御部である。尚，上述の実施の形態１における携帯電話機の自動ダイヤルロックシステムの構成の説明において，携帯電話機１０とロック解除装置２０間にて授受される信号の通信媒体として電波が用いられるものとして説明したが，これに限定されるものではなく，例えば赤外線や可視光等を用いるようにしてもよい。」（段落【００２６】）

「さらに，ロック解除装置２０内において，２１はあらかじめ携帯電話機１０のコード記憶回路１６に記憶されたものと同一のＩＤ情報が記憶されているＩＤ情報記憶回路であり，２２は携帯電話機１０のロック解除コード送信部１２より微弱電波にて送信されてきたロック解除コードを受信するロック解除コード受信部であり，２３はロック解除コード受信部２２から通知されたロック解除コードとＩＤ情報記憶回路２１に記憶されたＩＤ情報とから認証演算（認証装置１７と同一の処理）を行う認証装置であ

り，２４は認証装置２３による演算結果を携帯電話機１０に送信する認証結果送信部であり，２５は上記ロック解除装置２０の各部に電源を供給する電源部である。」（段落【００２７】）

「次に，図２を参照しながら動作について説明する。図２はこの発明の実施の形態１による携帯電話機の自動ダイヤルロックシステムの動作を示したフローチャートである。」（段落【００２８】）



【図２】

「まず，携帯電話機１０の特定（正規）の使用者あるいはサービス提供者等は，あらかじめ設定された所定のＩＤ情報を，携帯電話機１０のコード記憶回路１６とロック解除装置２０のＩＤ情報記憶回路２１に，図示しないＲＯＭライタ等を介して入力し記憶させる。尚，携帯電話機１０のコード記憶回路１６へのＩＤ情報の入力は，入力装置１４を介して行うようにしても良い。また，携帯電話機１０の電源投入時，携帯電話機１０はロック状態であるものとする。」（段落【００２９】）

「さて，携帯電話機１０に電源が投入されると（ステップＳＴ１），携帯電話機１０の認証装置１７は乱数を生成し，制御部１１に供給する。制御部１１は，この乱数をロック解除コードとしてコード記憶回路１６に記

憶する（ステップＳＴ２）。コード記憶回路１６にロック解除コードが記憶されると，認証装置１７はＩＤ情報と電源投入時に記憶されたロック解除コードを，コード記憶回路１６から読み出し，認証演算（任意の算術演算等）を実施し（ステップＳＴ３），該認証演算の結果を制御部１１に供給する。前記認証演算の結果の供給を受けた制御部１１は，該認証演算の結果（第１の認証演算結果）をコード記憶回路１６に記憶する。」（段落【００３０】）

「次に，携帯電話機使用者により，発信またはメモリダイヤル等の個人情報へのアクセス等の操作を行うべく，入力装置１４のキーボードより，一連のキー操作によるデータの入力（動作処理要求等）が行われると，この一連のキー操作によるデータの入力に対応する操作内容が制御部１１に供給（通知）される。制御部１１は，入力装置１４から前記操作内容が供給されたタイミングにて，コード記憶回路１６よりロック解除コードを読み出してロック解除コード送信部１２に供給する。ロック解除コード送信部１２は，ロック解除コードを微弱電波にのせ，携帯電話機使用者が所持している（身に付けている）ロック解除装置２０に送信する（ステップＳＴ４，５）。」（段落【００３１】）

「ロック解除装置２０のロック解除コード受信部２２は，携帯電話機１０から微弱電波で送信されたロック解除コードを受信すると，該ロック解除コードを認証装置２３に供給する。このロック解除装置２０の認証装置２３は，ロック解除コードが供給（受信）された時点で，ＩＤ情報記憶回路２１にあらかじめ記憶されているＩＤ情報を読み出し，該ＩＤ情報と受信したロック解除コードとで認証演算を行い（ステップＳＴ６），該認証演算の結果を認証結果送信部２４に供給する。また，認証結果送信部２４は認証装置２３より供給された認証演算の結果（第２の認証演算結果）を，携帯電話機１０に送信する。（ステップＳＴ７）」（段落【００３２】）

「なお，携帯電話機１０におけるロック解除コード送信部１２の送信出力及びロック解除装置２０におけるロック解除コード受信部２２の受信感度は，例えば，障害物（遮蔽物）の無い状態での電波の到達距離が，１ｍ程度となるように調整しておく。また，ロック解除装置２０の認証装置２３で用いる認証演算アルゴリズムは，携帯電話機１０の認証装置１７の認証演算アルゴリズムと同一のものを用いるものとする。」（段落【００３３】）

「次に，携帯電話機１０の認証結果受信部１８は，ロック解除装置２０から微弱電波で送信された認証演算の結果（第２の認証演算結果）を受信すると，制御部１１に供給する。制御部１１は，コード記憶回路１６に既に記憶されている認証演算の結果（第１の認証演算結果）を読み出して，受信した認証演算の結果（第２の認証演算結果）との比較認証（認証処理による認証判定）を行う（ステップＳＴ８）。」（段落【００３４】）

「制御部１１は，比較認証の結果が一致していた場合，前記ステップＳＴ４におけるキー入力は，特定の使用者（使用が許可されている携帯電話機使用者）によるキー入力であるものと判断し，ロック解除状態とし，前記ステップＳＴ４にて入力装置１４から入力された発信操作及びメモリダイヤル等の操作を有効として（ステップＳＴ９），発信処理等を継続する（一連のキー入力による処理が完了するまでの処理の継続を可能とする）。」（段落【００３５】）

「一方，携帯電話機１０のコード記憶回路１６に記憶されたＩＤ情報とロック解除装置２０のＩＤ情報記憶回路２１に記憶されたＩＤ情報とが異なっていたり，或いは，携帯電話機１０の認証装置１７における認証アルゴリズムとロック解除装置２０の認証装置２３における認証アルゴリズムが異なっていた場合（携帯電話機１０とロック解除装置２０の対応がとれていない場合）等によって，前記比較認証の結果が不一致となった場合，

制御部１１は，前記ステップＳＴ４におけるキー入力が，特定の使用者でない者（使用が許可されていない携帯電話機使用者）によるキー入力であると判断し，ロック解除は行わず，前記ステップＳＴ４にて入力された操作を無効として破棄し（ステップＳＴ１０），例えば，表示部１５に，前記ステップＳＴ４にて入力された発信操作またはメモリアクセス操作が無効である旨の表示を行う。」（段落【００３６】）

「また，制御部１１は，許可された発信処理（発信，メモリダイヤル等の個人情報へのアクセス操作等）が実施中，新たに入力装置１４から通知（入力）された操作に対しては，ロック状態として扱う。さらに，許可された発信処理が完了した後，新たに入力装置１４から通知された操作に対しては，制御部１１は，再びロック解除コードをロック解除装置２０に送信して認証処理を実施する。すなわち，一旦，ダイヤルロックが解除された操作に対し，一連の処理が完了するまでの期間についてのみ，キー入力された一連の処理要求に対する動作の継続が可能となる。」（段落【００３７】）

「また，制御部１１は，ロック解除コードをロック解除装置２０に送信した後，所定の時間が経過してもロック解除装置２０からの認証演算結果が受信されない場合には，当該携帯電話機１０の近辺には特定の使用者（使用を許可されている使用者）が存在しないものと判断し，ロック解除を行わず，当該入力された操作を破棄し，携帯電話機１０の表示操作部１５に，当該入力された発信操作またはメモリアクセス操作が無効である旨の表示を行う。」（段落【００３８】）

カ　発明の効果

「以上のように，この発明によれば，携帯電話機から操作者の認証を行うためのロック解除コードをロック解除装置に対して出力することにより，該ロック解除装置から，このロック解除コードに基づいた認証演算結果が

前記携帯電話機に対して出力され，この認証演算結果に基づき，前記携帯電話機にて該携帯電話機の操作者の認証処理を行うように構成したので，携帯電話機のロック状態からロック解除状態への遷移がリアルタイムに行われると共に，ロック解除装置の電力消費を格段に押さえることができるという効果がある。」（段落【００４８】）

「この発明によれば，携帯電話機の電源投入時に，該携帯電話機内部にて生成された第１の認証演算結果と，ロック解除装置内部にて生成された第２の認証演算結果とを，前記携帯電話機内部にて比較し，前記第１及び第２の認証演算結果が一致した場合に，当該操作者が特定の使用者であると認証判定を行うように構成したので，治具等による不正なロック解除装置の制作が難しくなり，携帯電話機の第三者による不正使用を高度に防止する効果がある。」（段落【００４９】）

「この発明によれば，第１の認証演算結果を，携帯電話機の電源投入時に，該携帯電話機内部にて生成された所定のロック解除コードと，あらかじめ携帯電話機内部に記憶されている特定の使用者を示すＩＤ情報とで，所定の認証演算を行うことにより生成し，第２の認証演算結果を，ロック解除装置内部にて前記携帯電話機より供給されたロック解除コードと，あらかじめロック解除装置内部に記憶されている前記特定の使用者を示すＩＤ情報とで，前記所定の認証演算を行うことにより生成するように構成したので，前記第１または第２の認証演算結果を不正に生成（模倣）することを困難とすることができるという効果がある。」（段落【００５０】）

「この発明によれば，携帯電話機とロック解除装置間で行われる通信に使用される信号（微弱電波等）の最大強度を，前記信号の到達距離が１ｍ程度となるように構成したので，携帯電話機及びロック解除装置それぞれにおける電池等の消耗をさらに少なくすることができ，さらに，携帯電話機とロック解除装置間通信における最大電力消費量を概ね把握できること

から，ロック解除装置にて使用される電池等の寿命をある程度の精度にてシミュレートすることができるという効果がある。」（段落【００５６】）

(2) 乙１１発明の内容

前記(1)によれば，乙１６発明は，操作者の認証判定によって，ダイヤルロックを解除する自動ダイヤルロックシステムであって，互いに無線通信する携帯電話機及びロック解除装置から成り，一連の操作が発生すると，携帯電話機が，前記認証のトリガとなるロック解除コードを出力し，当該ロック解除コードに基づき，ロック解除装置が，同装置の記憶するＩＤ情報を用いた認証演算結果を出力し，当該認証処理結果に基づき，携帯電話機が，これと当該携帯電話機の記憶するＩＤ情報を用いた認証演算結果を比較することで前記の認証判定をすることを特徴とするものであると認めることができる。

(3) 本件発明との対比

ア　ＲＦＩＤインターフェースの有無について

原告は，乙１６発明の携帯電話は，ＲＦＩＤインターフェースを有する携帯電話であると特定されていないと主張するが，乙１６公報の記載によれば，「携帯電話機１０におけるロック解除コード送信部１２の送信出力及びロック解除装置２０におけるロック解除コード受信部２２の受信感度は，例えば，障害物（遮蔽物）の無い状態での電波の到達距離が，１m程度となるように調整しておく。」（段落【００３３】）とされているので，同発明の携帯電話は，ロック解除システムとの間で「微弱電波」（段落【００３３】）による無線通信をする機能を備えるものであって，その電波の到達距離が「１m程度」に調整されるものであるということができる。

乙２５，２６によれば，一般に，ＲＦＩＤは，近距離無線通信を用いた自動認識技術であり，「数m離れた距離でも読み取り可能」な無線通信方式であると認められる。そして，本件発明の「ＲＦＩＤ」については，本件明細書等に「ＲＦＩＤにはさまざまな変調方式や周波数，通信プロトコ

ルを利用したものがあるが，本発明は特定の方式に限定されるものではなく，どのような方式を利用してもよい。」と記載され，その方式に制限はない。乙１６発明の携帯電話は，上記のとおり，電波の到達距離を「１ｍ程度」に調整された無線通信機能を備えるものであるから，構成要件Ａの「ＲＦＩＤインターフェースを有する携帯電話」に相当するということができる。

したがって，乙１６発明は，構成要件Ａ及びＧと一致する。

イ　原告主張に係る相違点１について

(ｱ) 原告は，「本件発明は，ＲＦＩＤインターフェースを有する携帯電話がＲバッジより受信するものがＲバッジの識別情報であるのに対し，乙１６発明では，携帯電話がロック解除装置から微弱電波等を用いて受信するものが当該ロック解除装置に供給されたロック解除コードと予め当該ロック解除装置内に記憶されている特定の使用者を示すＩＤ情報とにより認証演算を行うことにより得られた値である点である点」において相違すると主張する。

(ｲ) しかし，乙１６発明の「ロック解除装置」は「携帯電話機使用者が所持している（身に付けている）」（乙１６公報の段落【００３１】）ものであることから，本件発明の「Ｒバッジ」に該当すると解されるところ，乙１６発明のロック解除装置は，同装置内に記憶していたＩＤ情報を用いた「第２の認証演算結果」を携帯電話機に送信し，これを受信した携帯電話機は，これと当該携帯電話機内に記憶していたＩＤ情報を用いた「第１の認証演算結果」とを比較し，認証判定を行うのであるから（【請求項３】，段落【００３２】，同【００３４】），本件発明の構成要件Ｄに一致する。

(ｳ) これに対し，原告は，本件発明において，ＲＦＩＤインターフェースを有する携帯電話がＲバッジより受信するものがＲバッジの識別情報で

あるとするが，本件発明の「識別情報」が，Ｒバッジの固有の識別情報に限定されないことは前記判示のとおりである。

他方，乙１６発明における「第１の認証演算結果」とは，携帯電話が生成した乱数である「ロック解除コード」（請求項５）と当該携帯電話が記憶する「特定の使用者を示すＩＤ情報」（請求項３）とを用いた算術演算等の結果であり（段落【００３０】），ロック解除装置より受信する「第２の認証演算結果」とは，ロック解除装置が受信した「ロック解除コード」と同装置が記憶する「特定の使用者を示すＩＤ情報」とを用いて同様の認証演算をした結果なのであるから（段落【００３２】），乙１６発明で比較している演算結果は「特定の使用者を示すＩＤ情報」に相当するものであり，構成要件Ｄの「識別情報」に当たるというべきである。

ウ　原告主張に係る相違点２について

(ｱ) 原告は，「本件発明は，被保護情報に対するアクセス要求を許可するという比較結果が得られた場合は，アクセス要求が許可されてから所定時間が経過するまでは被保護情報へのアクセスを許可するものであるのに対し，乙１６発明は，動作処理要求に伴った一連の操作が前記携帯電話機に対して行われると個人認証を行い，個人認証が完了すると当該一連の操作のみが可能になるのであって，当該処理中に他の処理を行うことも，当該処理が終了後に他の処理を行うこともできず，また，所定時間を計時することもなく，所定時間が経過するまで携帯電話機内の情報に対するアクセスを含む何らかの操作を許可するものではない点」において相違すると主張する。

(ｲ) そこで，検討するに，乙１６公報の段落【００３５】には，「制御部１１は，比較認証の結果が一致していた場合，前記ステップＳＴ４におけるキー入力は，特定の使用者（使用が許可されている携帯電話機使用

者）によるキー入力であるものと判断し，ロック解除状態とし，前記ステップＳＴ４にて入力装置１４から入力された発信操作及びメモリダイヤル等の操作を有効として（ステップＳＴ９），発信処理等を継続する（一連のキー入力による処理が完了するまでの処理の継続を可能とする）。」との記載がある。これによれば，乙１６発明においては，被保護情報へのアクセスが許可されると，「一連の処理が完了するまでの」時間，アクセスが許可されるものということができる。

他方，本件発明の構成要件Ｆは，「前記アクセス制御手段は，当該比較手段で前記アクセス要求を許可するという比較結果が得られた場合は，前記アクセス要求が許可されてから所定時間が経過するまでは前記被保護情報へのアクセスを許可する」というものであり，「所定期間」に関する限定は付されていない。

また，本件明細書等の段落【０１２０】及び【０１２１】には，アクセスが許可されると，タイマに所定の時間ｔ２を設定し，時間ｔ２が経過するまでに開始した処理が終了した場合には，時間ｔ３をタイマに設定し，時間ｔ３が経過するまでに次の作業を開始した場合には，レッドバッジの読み込みをすることなく，引き続き次の作業を行うことができ，更に一つの作業が終了するたびにｔ３が起動されることが記載されているものと認められる。これによれば，本件発明においても，アクセスが許可された後，一連の作業が継続している間は，アクセスが許可されているということができる。

以上によれば，乙１６発明における「一連の処理が完了するまでの」時間も，構成要件Ｆの「所定時間」に当たるというべきである。

(ｳ) これに対し，原告は，乙１６発明は，一連の処理中に他の処理を行うことも，当該処理が終了後に他の処理を行うこともできず，また，所定時間を計時することもなく，所定時間が経過するまで携帯電話機内の情

報に対するアクセスを含む何らかの操作を許可するものではないので，本件発明と異なると主張する。

しかし，前記判示のとおり，乙１６発明においては，「一連の処理が完了するまでの」時間は，被保護情報へのアクセスが許可されているのであるから，仮にその間に他の処理を行うことができないとしても，構成要件Ｆの「前記アクセス要求が許可されてから所定時間が経過するまでは前記被保護情報へのアクセスを許可する」との構成を満たすとの結論を左右するものではない。

また，構成要件Ｆの「所定期間」には特段の限定は付されていないので，これを計時された一定の長さの時間に限定されると解することもできない。

したがって，原告の上記主張は理由がない。

エ　小括

そうすると，本件発明は，本件特許の優先日前に出願され，本件特許の優先日後に出願公開された乙１６公報に記載された発明と同一の発明であるので，特許無効審判によって無効とされるべきものである。

４　結論

以上によれば，その余の点について判断するまでもなく，原告の請求は理由がないから棄却することとし，よって，主文のとおり判決する。

東京地方裁判所民事第４０部

裁判長裁判官

佐　　藤　　達　　文

裁判官

三　　井　　大　　有

裁判官

吉　　野　　俊　太　郎

（別紙）

物　　件　　目　　録

次の商品名（機種番号）の携帯端末

１　ＡＱＵＯＳ　Ｒ　（６０５ＳＨ）Android バージョン ７

２　ＡＱＵＯＳ　Ｒ　（ＳＨ－０３Ｊ）Android バージョン ７

３　ＡＱＵＯＳ　Ｒ　（ＳＨＶ３９）Android バージョン ７

４　Ｄｉｓｎｅｙ　Ｍｏｂｉｌｅ　ｏｎ　ｄｏｃｏｍｏ（ＤＭ－０１Ｊ）Android バージョン ６

５　Ａｎｄｒｏｉｄ　Ｏｎｅ　Ｘ１　Android バージョン ７

（別紙）

被　告　製　品　説　明　書

1　原告の主張

⑴　概要

ア　ＮＦＣインターフェースを有するスマートフォンであること

被告製品は，いずれもＲＦＩＤインターフェースの一種であるＮＦＣインターフェースを有するスマートフォンである。

ＮＦＣインターフェースを有する被告製品は，非接触ＩＣチップが付いたＮＦＣ対応端末との間で送受信することができる機能を有している。

イ　画面（ディスプレイ）の消灯

被告製品を一定時間何も操作しないと画面（ディスプレイ）が消灯する。画面点灯時に電源スイッチを押すことによって，画面を消灯することができる。

ウ　ロック機能（ロックとセキュリティ）

被告製品は，画面ロックの解除方法をなしまたはスワイプ（またはタッチ）以外に設定した場合，電源キー（電源ボタン）を押すとロック画面が表示され，設定した方法で画面ロックの解除ができる。

画面ロックを解除するための設定は，「ロックとセキュリティ」において，設定することができる。画面ロック時は，被告製品中に格納された電話帳データや写真などにアクセスすることができない。

エ　スマートロック（SmartLock）

画面ロックの解除は，複数の方法が用意され，所有者が任意の方法を設定することができる。

画面ロックを解除する方法の１つとして，被告製品は，スマートフォンのＯＳであるAndroid5.0以降に標準搭載されたスマートロックを有する。

スマートロックのうち，信頼できる端末としてＩＣカード（ＮＦＣ）を登録した場合，ロック画面表示時に，登録した当該ＩＣカード（ＮＦＣ）を被告製品の背面にかざす（重ねる）ことによって，自動的に前記画面ロックが解除される。

オ　ロック画面表示の信号

被告製品の画面が消灯している状態で，スマートロックのうち信頼できる端末として登録したＩＣカード（ＮＦＣ）をかざしても被告製品は何ら反応しない。画面ロックを解除するためには，前記ロック画面が表示されている必要がある。

被告製品は，その電源キーを押すことにより，画面が点灯しロック画面が表示されるから，電源キーを押すことを契機とするロック画面表示のための信号が生成される。

そして，ロック画面は，当該スマートフォンについて，第三者による閲覧や使用を制限している状態を示すものである。この画面ロックが解除されない限り，被告製品に格納された電話帳や写真などにアクセスできない。

被告製品は，ロック画面が表示されている状態で登録済ＩＣカード（ＮＦＣ）を背面に重ねることによって画面ロックを解除することができる。

つまり，被告製品に格納された電話帳や写真などの被保護情報へのアクセスをしようとする所有者は，電源キーを押し，これを契機に生成されるロック画面表示のための信号に基づきロック画面が表示され，登録済ＩＣカード（ＮＦＣ）を背面に重ねれば画面ロックを解除することになって当該被保護情報へのアクセスが可能になる。

カ　ＩＤ情報等を要求する信号

ＩＣカード（ＮＦＣ）には，当該ＩＣカード（ＮＦＣ）に固有に割り振られたＩＤ情報が格納されている。当該ＩＣカード（ＮＦＣ）を前記信頼できる端末として登録すると，当該ＩＣカード（ＮＦＣ）のＩＤ情報が被告製品

に予め記憶される。

被告製品は，ロック画面が表示された状態で登録済ＩＣカード（ＮＦＣ）により画面ロックを解除できる。他方，ロック画面が表示されていない状態で登録済ＩＣカード（ＮＦＣ）を背面に重ねても何ら反応しない（甲第１１号証）。したがって，ロック画面が表示されると，ＩＣカード（ＮＦＣ）に向けて，ＩＣカード（ＮＦＣ）に格納されているＩＤ情報などを送信することを要求する信号を送信する送信手段を備える。

キ　ＩＤ情報の受け取り・比較

ＩＣカード（ＮＦＣ）がＩＤ情報等を要求されると，被告製品に対してＩＤ情報などを送信し，被告製品はこれを受け取る。

被告製品は，ＩＣカード（ＮＦＣ）から受け取ったＩＤ情報が，登録済ＩＣカード（ＮＦＣ）のＩＤ情報に適合するか否かを比較する比較手段を備える。

ク　画面ロック解除

上記判定の結果，受け取ったＩＤ情報が登録済みＩＣカード（ＮＦＣ）のＩＤ情報と一致したときは，画面ロックを解除し，不一致のときは画面ロックを解除しない。画面ロックが解除されると，被告製品内に格納された電話帳や写真などのデータにアクセスすることが可能になる。

ケ　所定時間の無操作

画面ロックが解除されて被告製品内に格納されたデータへのアクセスが可能になった後，無操作状態が所定時間経過すると被告製品は画面を消灯する。被告製品が操作されている限り画面は消灯せず，被告製品内に格納された電話帳や写真などのデータにアクセスすることができるようになっている。いったん画面が消灯すると，電源スイッチを再び押してロック画面を表示しても画面ロックを解除しない限り被告製品内に格納された電話帳や写真などのデータにアクセスすることはできない。

⑵　前提条件

①　ＳＩＭカードが装着されていること

②　画面ロック機能を「解除なし」またはスワイプ（またはタッチ）以外に設定していること

③　ＮＦＣを利用する設定をしていること（「機内モード」に設定されておらず，「ＮＦＣ／おサイフケータイ　ロック」設定がＯＦＦになっており，かつ「Ｒｅａｄｅｒ／Ｗｒｉｔｅｒ，Ｐ２Ｐ」設定がＯＮになっていること）

④　スマートロック（Ｓｍａｒｔ　Ｌｏｃｋ）において，信頼できる端末としてＩＣカード（ＮＦＣ）を登録していること

⑤　スマートフォンの電源が入れられた後，画面が消灯している状態にあること

⑶　構成

ａ　ＮＦＣインターフェースを有するスマートフォンである。

ｂ　当該スマートフォンの電源キーを押すことで生成されるトリガ信号（ロック画面表示信号）を受信し，画面ロック解除プロセスを実行するプログラムに対して，当該トリガ信号を画面ロック解除の要求として受け付けて当該プログラムに受け渡す受付手段を備える。

ｃ　前記トリガ信号（ロック画面表示信号）に応答して，ＩＣカードに対して識別情報を要求する信号（ＮＦＣの信号）を送信する送信手段を備える。

ｄ　背面にかざされたＩＣカードに記憶された識別情報を受信し，その識別情報を用いて，当該ＩＣカードが信頼できる端末として登録されたＩＣカード（登録済ＩＣカード（ＮＦＣ））であるか否かの比較を行う比較手段を備える。

ｅ　前記比較手段の比較の結果に応じて，画面ロックを解除し，または画面ロックを継続する画面ロック解除制御手段を備える。

ｆ　前記画面ロック解除制御手段は，前記比較手段で画面ロックを解除すると

いう比較結果が得られた場合（登録済ＩＣカード（ＮＦＣ）であると判定された場合）は，画面ロックが解除されてから所定時間が経過するまでは，画面を介して操作することができる。

ｇ　スマートフォンである。

２　被告の主張

⑷　ＮＦＣインターフェースを有するスマートフォンである。

⑹　電源キーが押下されることで「画面表示信号」が出力され，その信号に応じて，

①　画面ロック機能が設定されていなければ，画面を介しての操作が可能となり，直近に表示していた画面が表示される。

②　画面ロック機能が設定されていれば，画面ロックを解除するためのロック画面が表示される。

⑹　ＮＦＣの信号を送信するための所定の設定条件を充足した場合には，ＮＦＣの信号をＩＣカードに送信する。

⑹　ＩＣカードに記憶した識別情報を受信し，その識別情報を用いた何らかの方法による比較を行う。

⑹　前記比較の結果に応じて「画面表示信号」に対する許可または禁止をしておらず，比較の結果が一致していれば，直近で表示していた画面を表示して，画面を介しての操作が可能となり，比較の結果が一致していなければロック画面のままである。

⑹　画面ロックがされている場合においても，スマートフォンのデータへのアクセスは可能である。

①　電話着信があった場合には電話帳データにアクセスして発信元の名前を抽出してロック画面に表示が可能であり，

②　電話着信があった場合には電話の着信履歴データに追加して更新が可能であり，

③　電子メールの受信時には，受信した電子メールのデータを追加して更新し，ロック画面に表示が可能であり，

④　スケジュールデータに登録されたアラーム時刻が到来すると，スケジュールデータにアクセスし，スケジュールのラベル（タイトル）内容のロック画面への表示が可能であり，

⑤　画面ロックを解除することなく，カメラ機能を起動して撮影し，撮影した写真データを表示し，またはスマートフォンの写真データのフォルダへの保存が可能であり，

⑥　おサイフケータイで用いる電子マネーのデータにアクセスして決済処理が可能であり，

⑦　おサイフケータイで用いる定期券，乗車券などのデータにアクセスして自動改札の通過が可能であり，

⑧　スマートフォンとコンピューターとを接続して画面ロックを解除した後，再度，画面ロックがされた場合に，コンピューターからの操作でスマートフォンに保存した写真データにアクセスし，その写真データを取得することが可能であり，

⑨　会議や会話を録音した録音データを再生することが可能である。

そして，構成(d)における何らかの方法による比較の結果が一致していた場合には，画面ロックが解除される。

画面を介しての操作が行われていない場合には画面が表示されてから，または画面を介しての操作が行われた場合には画面に対する何らかの操作が行われた時点から起算して，無操作状態が一定時間経過するまでは画面を介しての操作が可能となり，画面を介しての無操作状態が一定時間継続すると，画面の表示が消え，画面を介しての操作が行えない。

(g)　スマートフォンである。