(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2022-183444
(P2022-183444A)
(43)公開日　令和4年12月13日(2022.12.13)

(51)Int.Cl.		F I		テーマコード（参考）
Ｇ０６Ｆ　21/34	*(2013.01)*	Ｇ０６Ｆ　21/34		３Ｃ０６４
Ｂ２５Ｆ　5/00	*(2006.01)*	Ｂ２５Ｆ　5/00	Ｃ	
		Ｂ２５Ｆ　5/00	Ｈ	

審査請求 未請求　請求項の数 15　ＯＬ　（全 22 頁）

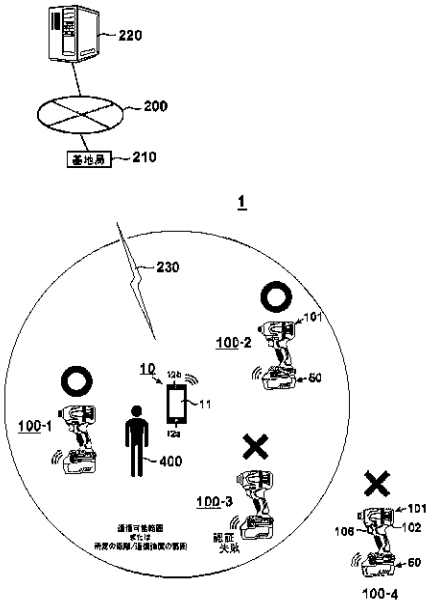
(21)出願番号　特願2021-90757(P2021-90757)
(22)出願日　令和3年5月31日(2021.5.31)

(71)出願人　000005094
工機ホールディングス株式会社
東京都港区港南二丁目１５番１号
(74)代理人　110001689
青稜弁理士法人
(72)発明者　山口　聡史
茨城県ひたちなか市武田１０６０番地
(72)発明者　塙　浩之
茨城県ひたちなか市武田１０６０番地

Ｆターム(参考) 3C064 AA02 AB02 AC02 BA23 BA24
BB10 BB89 CA53 CA78 CA79
CA80 CB17 CB62 CB71 DA03
DA11 DA43 DA56 DA89 DA91
EA02 EA03

(54)【発明の名称】電気機器及び電気機器システム

(57)【要約】
【課題】使用する人の正当性の認証を要求する電気機器において、認証プロセスが完了する前に、電気機器１００の制限的な作動を可能とする。
【解決手段】電気機器１００の制御部は、トリガスイッチの操作開始に伴って、モータの稼働を許可すると共に、ユーザ４００が正当であるか否かを近接無線通信により接続された認証機器（端末装置１０）に照合する。端末装置１０から所定時間内に認証情報が受信できなかった場合や、認証情報の不一致により認証失敗の場合は、制御部はモータの回転を禁止する。このように認証プロセスが終了する前に電気機器の使用を制限付きで可能としたので、電気機器１００の即時使用性が向上する。
【選択図】図１



【特許請求の範囲】
【請求項１】
負荷部と、前記負荷部の駆動を指示する操作部と、前記操作部の操作に応じて前記負荷部を制御する制御部と、を有し、前記操作部を操作する使用者が正当であるか否かの認証を要求する電気機器であって、
前記制御部は、前記操作部の操作開始に伴って前記負荷部の稼働を許可すると共に、使用するユーザ又は使用機器が正当であるか否かを外部機器に照合し、
前記外部機器によって所定時間内に認証が許可された場合には前記電気機器の通常使用を許可し、制限内に認証が許可されなかった場合には前記負荷部の動作を阻止する、ことを特徴とする電気機器。
【請求項２】
請求項１に記載の電気機器において、
前記制限内に認証が許可されなかった場合とは、前記負荷部の駆動を開始してから前記認証が許可されないまま所定時間経過後が経過した場合、又は、前記電気機器と前記外部機器との間の認証情報が一致しない場合、の少なくとも一方であることを特徴とする電気機器。
【請求項３】
請求項１又は２に記載の電気機器において、
前記制御部は、前記外部機器との間を近接無線通信によって接続し、前記電気機器は前記外部機器により入力された認証コードと、予め登録されている認証コードを比較することによって前記ユーザが正当であるか否かを判断することを特徴とする電気機器。
【請求項４】
請求項１から３のいずれか一項に記載の電気機器において、
前記電気機器と前記外部機器との間の認証が成功した後に、一定期間毎に認証をおこなうことを特徴とする電気機器。
【請求項５】
請求項１から４のいずれか一項に記載の電気機器において、
前記電気機器と前記外部機器との間の認証情報が一致しない場合であっても、一定期間後に再照合することにより認証が許可された場合には、前記負荷部の駆動を許可することを特徴とする電気機器。
【請求項６】
請求項１から５のいずれか一項に記載の電気機器と、
前記電気機器と無線通信可能な携帯端末と、を備えた電気機器システムであって、
前記電気機器又は複数の前記使用機器のいずれかは、制御部と、前記制御部に接続された機器側通信部と、を備え、
前記携帯端末は、前記機器側通信部と無線通信可能な端末側通信部を有し、
前記機器側通信部と前記端末側通信部とが互いに無線通信可能エリア内に位置する状態で前記機器側通信部と前記端末側通信部との無線通信が不能な状態において、前記負荷部を駆動可能にした、ことを特徴とする電気機器システム。
【請求項７】
負荷部と、前記負荷部の駆動を指示する操作部と、前記操作部の操作に応じて前記負荷部を制御する制御部と、を有し、外部機器との認証を行う電気機器であって、
前記制御部は、前記操作部の操作がされた際に前記認証が完了していない場合は未認証停止モードにて、制限を付けた状態で前記電気機器の稼働を許容し、
その後、前記認証が完了した場合には電気機器を通常作動モードに移行させ、前記認証が完了しなかった場合には前記電気機器の稼働を禁止する未認証停止モードに移行させることを特徴とする電気機器。
【請求項８】
請求項７に記載の電気機器において、
前記制限は、所定時間によって決定されるか、認証情報の照合制限回数によって決定さ

れることを特徴とする電気機器。
【請求項９】
負荷部と、前記負荷部の駆動を指示する操作部と、を有する電気機器において、
前記電気機器に選択的に接続可能な複数の外部機器のうちの１つを接続した状態において、所定の駆動条件を満たさなくても前記操作部を操作すると前記負荷部を駆動する第１モードと、前記所定の駆動条件を満たすまで前記操作部を操作しても前記負荷部を駆動しない第２モードを有することを特徴とする電気機器。
【請求項１０】
請求項９に記載の電気機器において、
前記所定の駆動条件は、前記電気機器と前記接続した外部機器との間の認証が成功した場合であることを特徴とする電気機器。
【請求項１１】
請求項９又は１０に記載の電気機器において、
前記第１モードを選択した場合、所定の停止条件を満たすと前記第２モードに移行することを特徴とする電気機器。
【請求項１２】
請求項１１に記載の電気機器において、
前記所定の停止条件は、前記負荷部の駆動を開始してから所定時間経過後が経過した場合、前記電気機器と前記接続した外部機器との間の認証が失敗した場合、の少なくとも一方であることを特徴とする電気機器。
【請求項１３】
請求項９から１２のいずれか一項に記載の電気機器において、
前記負荷部と前記操作部は電気機器本体に設けられ、
前記外部機器は、前記電気機器本体に着脱可能な電池パックである、
ことを特徴とする電気機器。
【請求項１４】
請求項１から１２のいずれか一項に記載の電気機器と、
前記電気機器と無線通信可能な携帯端末と、を備えた電気機器システムであって、
前記電気機器は、制御部と、前記制御部に接続された機器側通信部と、を備え、
前記携帯端末は、前記機器側通信部と無線通信可能な端末側通信部を有し、
前記機器側通信部と前記端末側通信部とが互いに無線通信可能エリア内に位置する状態で前記機器側通信部と前記端末側通信部との無線通信が不能な状態において、前記負荷部を駆動可能にしたことを特徴とする電気機器システム。
【請求項１５】
負荷部と、前記負荷部の駆動を指示する操作部と、前記操作部の操作に応じて前記負荷部を制御する制御部と、を有する電気機器本体と、前記電気機器本体に対して着脱可能な電池パックと、を有し、前記電気機器本体と前記電池パックとの間で認証可能な電気機器であって、
前記制御部は、
前記電気機器本体に前記電池パックとして第１の電池パックを接続した状態で前記操作部を操作すると、前記負荷部の駆動を開始し、その後、前記操作部を操作している間は前記負荷部の駆動を継続し、
前記電気機器本体に前記電池パックとして第２の電池パックを接続した状態で前記操作部を操作すると、前記負荷部の駆動を開始し、その後、前記操作部を操作している間に前記負荷部の駆動を停止する、
よう構成される、ことを特徴とする電気機器。

【発明の詳細な説明】
【技術分野】
【０００１】

本発明は電気機器及び電気機器システムに関する。

【背景技術】

【０００２】

認証用に記憶したパターン情報（パスコード）が一致した場合にだけ作動可能に構成され、不一致の場合には作動不能とされる電気機器が知られている。認証を必要とするのは、第三者による使用を不可にして電気機器の盗難防止を図るため、盗難された品の転売を防止するため、正規品以外の装着品(電池パック等)の使用を防止するため等、それらの目的は様々である。特許文献１には、電池パックと電気機器（電動工具）との間で認証を行い、その結果、それらの使用を許可するか、使用を禁止するかを決定する電気機器が記載されている。このような認証機能付きの電気機器は、通常、使用に先立って認証を行い、認証が成功した場合にのみ作動を許可する。

【先行技術文献】

【特許文献】

【０００３】

【特許文献１】国際公開第２０１８／０７９２３３号

【発明の概要】

【発明が解決しようとする課題】

【０００４】

電気機器（例えば電動工具）の使用時にユーザの認証を行う場合は、認証に要する時間が大きいため、トリガスイッチの操作から作動開始までの時間が遅れてしまうという問題がある。特に、電池駆動機器の場合は、省電力が要求され、通信機器やセンサを省電力（休止や断続駆動など）で駆動させるため、省電力モードから通常作動モードへの復帰を行った上で認証を行うので即応性が損なわれる虞がある。また、電気機器の認証を、無線通信を介してスマートフォン等の外部機器を用いて行う場合には、通信相手を検索する必要があり、無線通信路を確立するための時間も要するため、認証に必要とされる時間がさらに大きくなってしまう。このように外部機器によって無線通信を用いた認証を前提とする場合、即応性が良くないという問題がある。特許文献１では、認証の結果が出るまで電気機器を使用することができないため、認証に要する時間によっては作業性を悪くする可能性があった。

【０００５】

本発明は上記背景に鑑みてなされたもので、その目的は、使用する人の正当性の認証や、装着される機器（使用機器）の正当性の認証を前提に稼働が許可される電気機器において、認証プロセスが完了する前に、電気機器本体の制限的な作動を許可する電気機器及び電気機器システムを提供することにある。

本発明の他の目的は、認証が失敗した際には稼働中であっても使用を阻止するようにして、ユーザの限定や、装着される機器の正当性を確保できるようにした電気機器及び電気機器システムを提供することにある。

本発明のさらに他の目的は、無線にて接続可能な外部機器を用い、容易な操作でユーザの認証を行うことができる電気機器及び電気機器システムを提供することである。

本発明の他の目的は、作業性の良い電気機器及び電気機器システムを提供することにある。

【課題を解決するための手段】

【０００６】

本願において開示される発明のうち代表的な特徴を説明すれば次のとおりである。

本発明の一つの特徴によれば、負荷部と、負荷部の駆動を指示する操作部と、操作部の操作に応じて負荷部を制御する制御部とを有し、操作部を操作する使用者が正当であるか否かの認証を要求する電気機器であって、制御部は、操作部の操作開始に伴って負荷部の稼働を許可すると共に、使用するユーザ又は使用機器（装着される機器）が正当であるか否かを外部機器に照合し、外部機器によって所定時間内に認証が許可された場合には電気機器の通常使用を許可し、制限内に認証が許可されなかった場合には負荷部の動作を阻止

するようにした。ここで、制限内に認証が許可されなかった場合とは、負荷部の駆動を開始してから認証が許可されないまま所定時間経過後が経過した場合、又は、電気機器と外部機器との間の認証情報が一致しない場合、の少なくとも一方である。

【０００７】

本発明の他の特徴によれば、電気機器の制御部は、外部機器との間を近接無線通信によって接続し、電気機器は外部機器により入力された認証コードと、予め登録されている認証コードを比較することによってユーザが正当であるか否かを判断する。また、電気機器と外部機器との間の認証が成功した後に、一定期間毎に認証をおこなう。ここで、電気機器と外部機器との間の認証情報が一致しない場合であっても、一定期間後に再照合することにより認証が許可された場合には、負荷部の駆動を許可する。このような電気機器と、電気機器と無線通信可能な携帯端末と、を備えた電気機器システムを構成し、電気機器又は複数の使用機器のいずれかは、制御部と機器側通信部を備え、携帯端末は端末側通信部を有するようにした。そして、機器側通信部と端末側通信部とが互いに無線通信可能エリア内に位置する状態で機器側通信部と端末側通信部との無線通信が不能な状態において、負荷部を駆動可能にした。

【０００８】

本発明のさらに他の特徴によれば、電気機器において、制御部は、操作部の操作がされた際に認証が完了していない場合は未認証停止モードにて制限を付けた状態で電気機器の稼働を許容し、その後、認証が完了した場合には電気機器を通常作動モードに移行させ、認証が完了しなかった場合には電気機器の稼働を禁止する未認証停止モードに移行させる。この制限は、所定時間によって決定されるか、認証情報の照合制限回数によって決定されるようにすると良い。

【０００９】

本発明のさらに他の特徴によれば、電気機器に選択的に接続可能な複数の外部機器のうちの１つを接続した状態において、所定の駆動条件を満たさなくても操作部を操作すると負荷部を駆動する第１モードと、所定の駆動条件を満たすまで操作部を操作しても負荷部を駆動しない第２モードを設けた。ここで所定の駆動条件は、電気機器と接続した外部機器との間の認証が成功した場合である。また、第１モードを選択した場合、所定の停止条件を満たすと第２モードに移行するようにした。所定の停止条件は、負荷部の駆動を開始してから所定時間経過後が経過した場合、電気機器と接続した外部機器との間の認証が失敗した場合、の少なくとも一方である。外部機器の一例は電気機器本体に着脱可能な電池パックである。

【００１０】

本発明のさらに他の特徴によれば、前記電気機器と、電気機器と無線通信可能な携帯端末と、を備えた電気機器システムであって、電気機器は、制御部と機器側通信部を備え、携帯端末は端末側通信部を有し、機器側通信部と端末側通信部とが互いに無線通信可能エリア内に位置する状態で機器側通信部と端末側通信部との無線通信が不能な状態において、負荷部を駆動可能にした。また、負荷部と、負荷部の駆動を指示する操作部と、操作部の操作に応じて負荷部を制御する制御部と、を有する電気機器本体と、電気機器本体に対して着脱可能な電池パックと、を有し、電気機器本体と電池パックとの間で認証可能な電気機器であって、制御部は、電気機器本体に電池パックとして第１の電池パックを接続した状態で操作部を操作すると、負荷部の駆動を開始し、その後、操作部を操作している間は負荷部の駆動を継続し、電気機器本体に電池パックとして第２の電池パックを接続した状態で操作部を操作すると、負荷部の駆動を開始し、その後、操作部を操作している間に負荷部の駆動を停止するように構成した。

【発明の効果】

【００１１】

本発明によれば、認証プロセスが完了する前に、電気機器本体の制限的な作動を可能とし、制限的な作動中に認証プロセスを並行して実行するので、電気機器本体の稼働の即応性を損ねることなく、従来の電気機器と同じ使い勝手の電気機器及び電気機器システムを

提供できる。また、認証が失敗した場合は電気機器の作動を停止させるので、不正使用者による作動や、不正機器を接続した状態での作動を抑制でき、信頼性の高い電気機器及び電気機器システムを提供できる。さらに、認証プロセスにはユーザ認証機能付きの情報端末を用い、無線通信にて情報端末と電気機器が情報のやりとりを行うため、認証作業が容易な電気機器及び電気機器システムを提供できる。よって、作業性の良い電気機器及び電気機器システムを提供できる。

【図面の簡単な説明】

【００１２】

【図１】本発明の実施例に係る電気機器システム１の全体構成図である。

【図２】図１の電気機器１００及び情報端末１０の回路構成を示すブロック図である。

【図３】図１の電気機器１００に示す認証モードの遷移図である。

【図４】図１の情報端末１０、電池パック５０、電気機器本体１０１の操作と、通信を用いた認証手順を説明するシーケンス図である（認証成功時）。

【図５】図１の電気機器本体１０１のマイコン１１６における作動モードの設定手順を説明するフローチャートである。

【図６】図１の電気機器本体１０１のマイコン１１６における認証処理の実行判断手順を説明するフローチャートである。

【図７】図１の情報端末１０、電池パック５０、電気機器本体１０１の操作と、通信を用いた認証手順を説明するシーケンス図である（認証失敗時）。

【図８】本発明の第２の実施例に係る電気機器１００Ａ及び情報端末１０の回路構成を示すブロック図である。

【図９】本発明の第３の実施例に係る認証プロセス手順を説明するためのフローチャートである。

【発明を実施するための形態】

【実施例１】

【００１３】

以下、本発明の実施例を図面に基づいて説明する。なお、以下の図において、同一の部分には同一の符号を付し、繰り返しの説明は省略する。図１は本発明の実施例に係る電気機器システム１の全体構成図である。本実施例の電気機器システムは、認証を行うことを前提に稼働が許可される被認証機器（例えば電気機器１００）と、電気機器に対して認証を行う認証機器（例えば情報端末１０）によって構成される。電気機器１００の数は、単数でも良いし複数でも良い。

【００１４】

４つの電気機器１００（１００－１～１００－４）は、それぞれ電気機器本体１０１と電池パック５０により構成され、電池パック５０を電源としてモータ等の負荷装置を駆動させる携帯型の機器である。電気機器１００は、それぞれトリガスイッチ１０６を有し、ユーザ４００がトリガスイッチ１０６を引くことによって電気機器１００のモータ（図では見えない）の回転が開始され、図示しない先端工具が回転する。図１では、電気機器１００として同一の機器１００－１～１００－４を図示しているが、同一機種である必要性はなく、異なる種類の電気機器１００を用いても良い。電気機器１００は、使用を正当に許可されたユーザ４００だけが作動できるように事前設定でき、許可されていないユーザ（不正使用者）に対しては使用を阻止することが可能である。また、電気機器１００はユーザの認証を必要とせずに、誰でも使用することができるセキュリティ設定無しのモードも有しているので、ユーザがいずれか（認証有りのモード、認証なしのモード）を選択して電気機器本体１０１に事前設定しておくことが可能である。なお本明細書では、電気機器本体１０１を電気機器、電池パック５０を外部機器と称する場合もある。

【００１５】

電気機器１００のユーザ４００に対する正当性の認証は、外部機器たる情報端末１０を用いて行われる。電気機器１００側に、ユーザ認証用の装置（例えば、パスワード入力用のキーボード、指紋認証用のタッチパッド、顔認証用のカメラ）を装着することも考えら

れるが、それらは電気機器１００の価格の高騰に繋がるので現実的ではない。そこで、電気機器１００から、近接無線通信可能な情報端末１０を用いて、ユーザ４００の認証を行うようにした。

【００１６】

情報端末１０は、電気機器１００に対する初回の認証コード登録が行われたら、それを記憶部内に登録しておき、電気機器１００からの認証要求を受けた際に、自動的に電気機器１００の使用のための認証コードを返信する。このように構成することで、電気機器１００の使用開始のたびにユーザ４００が情報端末１０から認証コードを入力する必要が無くなるため、使い勝手を良くすることができる。

【００１７】

情報端末１０は、例えばスマートフォンを用いることができる。情報端末１０には、情報を表示する表示部と、作業者からの操作を受け付けるための操作部が設けられる。これら表示部と操作部は、タッチパネル式の表示部１１にて実現できる。さらに、情報端末１０には、指紋認証用のタッチパッド１２ａ、画像入力用のカメラ１２ｂが設けられる。情報端末１０は電話通信網を用いて基地局２２０経由でインターネット等のネットワーク網２００に接続可能であり、電気機器１００のメーカのサーバ装置２２０に電話回線２３０やインターネット回線を介して接続可能である。

【００１８】

本実施例の電気機器システム１の初期設定として、ユーザ４００は情報端末１０に、電気機器１００－１～４との無線通信を行い、認証プロセスを実行するための専用のアプリケーションソフトウェア（以下、「アプリ」と称する）をインストールする。そのアプリは、サーバ装置２２０からダウンロード可能である。次に、情報端末１０は、近接無線通信によって、自ら所有（又は使用）する電気機器１００－１～４のそれぞれに対して、電気機器１００－１～４の制限的な使用のための認証情報（パスワード等）の設定を行う。情報端末１０としてスマートフォンを用いれば、スマートフォンには使用するユーザ４００の認証を行う機能を有しているので、その機能を用いることにより、ユーザ４００の所有する情報端末１０のアプリを利用して無線通信によるペアリングが成功したことで、認証成功と見做すことが可能である。例えば、専用のアプリによって、情報端末１０のロック状態を解除するだけで電気機器１００の認証プロセスが実行できる。尚、ロック状態の解除をすることなく近接無線通信が可能な状態の情報端末１０を電気機器１００の通信可能範囲内に位置づけるだけで認証プロセスが実行できるように構成したりしても良い。

【００１９】

情報端末１０は近接無線通信を介して電気機器１００と接続し、認証に必要な手順を実行する。基本的には、電気機器１００から認証要求（パスワード等の認証コードの要求）を受けて、ユーザ４００が情報端末１０から入力した認証情報を、近接無線通信を介して電気機器１００に返信する。この認証情報の返信は、最初の認証時だけユーザ４００の操作が必要とされるものの、電気機器１００の作動時の定期的な認証（再認証）においては、ユーザ４００の操作を必要とせずに情報端末１０が自動的に電気機器１００に対して認証情報を返信するように構成できる。認証情報を受信した電気機器１００は、受け取った認証情報と、予め電気機器１００の制御部内に登録されている認証情報を照合して、それらが一致すれば"認証成功"、不一致ならば"認証失敗"と判断する。認証情報が一致した場合は、電気機器１００を通常使用することができ、認証情報が不一致の場合は電動工具１００の使用が阻止される。

【００２０】

情報端末１０にインストールされた専用のアプリは、通信可能範囲内にある電気機器１００、ここでは電気機器１００－１～１００－３との通信を行い、それぞれの認証プロセスを実行する。図１の例では、稼働が許可された電気機器を丸印で、稼働が許可されない電気機器をバツ印で示している。電気機器１００－１と１００－２は、近接無線通信を用いた確認により認証コードの一致により稼働が許可され（後述の"通常作動モード"に移行）、電気機器１００－３は、近接無線通信を用いた確認により認証コードの不一致が発

生して稼働が禁止される（後述の"未認証停止モード"に移行）状態を示している。一方、電気機器１００－４は、情報端末１０と電気機器１００との近接無線通信ができない、つまり無線可能範囲を超えた離れた位置にあるため、認証プロセスの実行ができない状態にあるのでその作動が禁止される（後述の"未認証停止モード"に移行）。

【００２１】

近接無線通信手段として、例えばブルートゥース（Bluetooth: Bluetooth SIG, Inc. USAの登録商標）を用いることができる。採用する無線通信方式は任意であるが、ブルートゥース（登録商標）の伝送距離が数ｍ～数十ｍであるため、電気機器１００の使用可能範囲の限定をするのに有利だからである。情報端末１０と電気機器１００のそれぞれには、ブルートゥース（登録商標）による通信を行う無線通信部（図２で後述）が設けられる。

【００２２】

近年、情報端末１０では端末を使用するユーザ４００を限定するために、情報端末１０のユーザ登録とログインが必須とされ、ユーザ認証が成功しないとロック機構によって情報端末１０の使用ができないように構成される。このログイン機能を利用すれば、図１のシステムで利用する専用アプリの使用者がユーザ４００であることを保証できるので、電気機器１００は情報端末１０との通信成立によりユーザ４００が正当であると確認できる。

【００２３】

電気機器１００の制御部は、起動時にユーザ４００の正当性の認証のための認証プロセスを実行する。この認証は、電気機器１００を使用する人（ユーザ）が正当であるかを検証する人的正当性の認証と、電気機器１００に装着される機器（例えば電池パック５０）の正当性の認証等、様々に設定可能である。電気機器１００を使用する人（ユーザ）の認証プロセスの方法として、電気機器１００にユーザ４００に対する認証情報（パスコードや、指紋・顔・声など生体情報）を予め登録しておき、認証プロセスの実行時に情報端末１０側から送信される認証情報との比較を行う。

【００２４】

図２は電気機器１００及び情報端末１０の回路構成を示すブロック図である。電気機器１００は、電気機器本体１０１と、電気機器本体１０１に対して着脱可能な電池パック５０により構成される。電池パック５０は、合成樹脂製のケース内に二次電池６５を収容したものである。二次電池６５は定格電圧３．６Ｖのリチウムイオン電池セルを５本直列接続して、正極端子５１と負極端子５２に定格１８Ｖの電力を供給する。二次電池６５への充放電は制御部５５によって制御される。制御部５５には、マイコン５６と、記憶部５７が含まれる。記憶部５７は、マイコン５６とは別に設けられる不揮発性のメモリであるが、マイコン５６に内蔵された不揮発性メモリを用いても良く、制御部５５のハードウェア構成は任意である

【００２５】

マイコン５６は、二次電池６５の状態、例えば電圧、電流や電池セルの温度を監視する。電圧は電圧検出部５８によって検出され、その出力は制御部５５のマイコン５６に入力される。５本の電池セル（二次電池６５）には、電池保護ＩＣ６０が接続される。電池保護ＩＣ６０は、いわゆる"リチウムイオン電池用保護ＩＣ"として市販されている集積回路であり、二次電池６５の各電池セルの両端電圧を入力することにより、電池セル各々の電圧を検出し、検出された電圧を用いて過充電保護機能、過放電保護機能の他、セルバランス機能、カスケード接続機能、断線検出機能等のいずれか一つ以上を実行する。電池保護ＩＣは、二次電池６５に対する過充電状態を検出したら、マイコン５６に対して過充電検出信号６１を出力し、過放電状態を検出したら、マイコン５６に対して過放電検出信号６２を出力する。

【００２６】

二次電池６５から流れる又は二次電池６５に対して流れる電流は、二次電池６５と直列に接続されたシャント抵抗５９を用いて検出される。シャント抵抗５９の両端電圧は電流検出部６４により測定され、電流値としてマイコン５６に出力される。二次電池６５の温

度は、その近傍に設けられたサーミスタ等のセル温度検出部６３によって検出されマイコン５６に入力される。マイコン５６は、過放電検出信号６２を受信した状態、即ち、二次電池６５の電圧が規定の下限値を下回った際には、"放電禁止"とする放電許可／禁止信号６９をＬＤ端子５３、１１３を介して電気機器本体１０１の制御部１１５に送出する。

【００２７】

電池パック５０には、情報端末１０と近接無線通信を行うための無線通信部６８が設けられる。無線通信部６８としてブルートゥース（登録商標）用の送受信機が用いられる。無線通信部６８は電池パック５０のマイコン５６により制御される。電池パック５０と電気機器本体１０１の接続端子の一つとして通信端子５４、１１４が設けられ、電池パック５０の制御部５５（マイコン５６）と、電気機器本体１０１の制御部１１５（マイコン１１６）が通信可能である。従って、無線通信部６８、通信端子５４、１１４を用いて、電気機器本体１０１のマイコン１１６は情報端末１０との双方向通信（点線矢印で示す中継通信モード３２の通信経路を介して、外部機器（情報端末１０等）から認証情報の受信が可能となる。

【００２８】

電池パック５０の制御部５５には、ユーザ４００の指示を入力するための操作部６６が設けられる。操作部６６としては、電池残量を４段階で表示するための残量チェックボタン（状態表示指示）、無線通信部６８によってマイコン５６が外部機器（例えば情報端末１０）と通信を行う通信モードへの切替えるための通信スイッチ（通信設定）等が含まれる。

【００２９】

制御部５５にはさらに、ユーザ４００に対して情報を表示するための表示部６７が設けられる。表示部としては、複数（例えば４つ）の多色表示可能なＬＥＤを用いて実現でき、電池残量を赤色の４段階で表示したり（残量表示）、電池パック５０の異常状態を赤色ＬＥＤの点滅で表示したり（異常状態表示）、近接無線によるペアリングが確立しているか否かを１つの青色ＬＥＤの点灯で表示したり（通信状態表示）、認証が成功したことを１つの緑色のＬＥＤの点灯で表示したりする（認証状態表示）。尚、表示部６７を複数個の多色ＬＥＤによって実現するだけでなく、複数個の単色ＬＥＤ、セグメントＬＥＤ、液晶ディスプレイ、その他の視覚的出力装置を用いるようにしても良い。また、電池の残量の表示スイッチ（図示せず）と、近接無線通信によるペアリング開始のための通信スイッチを兼用として、ボタンを普通に押す操作で電池の残量の表示をし、ボタンの長押しをしたらペアリングを開始するように構成しても良い。

【００３０】

電気機器本体１０１にはモータ１０４が設けられ、図示しない先端工具を駆動する。電気機器本体１０１が電動工具の場合は、モータ１０４が、電池パック５０の電力の大部分を消費する主な負荷部である。正極端子１１１から負極端子１１２に至る電力経路中には、トリガスイッチ１０６と、モータ１０４と、電力回路を遮断する半導体スイッチング素子１０７が介在される。トリガスイッチ１０６は、図示しない先端工具を起動するために作業者によって操作されるもので、ユーザ４００がトリガスイッチ１０６をオンにするとモータ１０４が回転する。使用されるモータ１０４の種類は任意であり、例えばブラシ付きの直流モータや、図示しないインバータ回路を用いて駆動されるブラシレスモータを用いることができる。半導体スイッチング素子１０７として、例えばＦＥＴ（電界効果トランジスタ）を用いることができ、制御部１１５からゲート信号を制御されることにより、電力経路を接続又は遮断（導通していない状態）に切り替える。

【００３１】

電気機器本体１０１の制御部に１１５は、マイコン１１６と記憶部１１７が含まれる。制御部１１５はモータ１０４の回転制御を行うと共に、異常発生時にはスイッチング素子１０７を遮断状態にしてモータ１０４の回転を阻止（停止）する。また制御部１１５は、異常信号端子であるＬＤ端子１１３を介して電池パック５０のＬＤ端子５３から放電禁止信号が伝達されると、半導体スイッチング素子１０７のゲート信号をＬｏｗにしてソース

－ドレイン間をオフ状態（非導通状態）にすることによりモータ１０４の回転を禁止（停止）する。図２では図示していないが、電気機器本体１０１内にも電流検出部を設け、電力経路に過電流が流れたことをマイコン１１６により監視する。

【００３２】

制御部１１５の記憶部１１７は、不揮発性メモリで構成されており、プログラムを予め格納しておくと共に、ユーザ４００に関する"認証情報"を格納し、また、情報端末１０の無線接続用の識別情報を格納する。ここで"認証情報"は、ユーザ４００が設定した英数字数桁からなるパスワード、生体情報をコード化した識別情報であるが、情報端末１０が認証機能付きの場合は前記の識別情報に加えて、又は、前記の識別情報に代えて、ユーザ４００が所有する情報端末１０の固有番号（機器番号、ブルートゥース（登録商標）のＩＤ番号等）としても良い。

【００３３】

制御部１１５のマイコン１１６は、ペアリング登録された外部機器（ここでは情報端末１０）との無線通信を行う。ここでは、電池パック５０側に無線通信部６８が設けられるため、電池パック５０が電気機器本体１０１側のマイコン１１６と、情報端末１０側の制御部１５との通信を中継する。制御部１１５には初回の情報端末１０とのペアリングの際に、ユーザ４００が使用する情報端末１０の固有情報（近接無線通信に基づくＩＤ等）を格納する。そのため２回目以降の接続の場合は、ブルートゥース（登録商標）の接続手順に沿って自動的にペアリングを行うことができる。電気機器１００側と情報端末１０のペアリングが完了すると、情報端末１０にインストールされた専用のアプリによって、電気機器本体１０１側のマイコン１１６との通信が行われ、認証情報の送受信が行われる。外部機器がスマートフォン等のユーザ４００が専用に使用する機器であって、外部機器の使用に指紋認証がフェイス認証等の情報端末１０に固有の認証（ログイン）が必要とされる場合は、情報端末１０の認証結果をユーザ４００の正当性判断に利用しても良い。この場合は、ユーザ４００の所有するスマートフォン（情報端末１０）と近接無線通信によるペアリングが確立したことで、電気機器本体１０１へのユーザ４００の認証が完了した扱いとすれば良い。また、特定のタイミングでユーザ４００の再確認が必要な場合は、ユーザ４００に情報端末１０へのログイン操作を再度行わせるようにすれば良い。

【００３４】

制御部１１５には、ユーザ４００の指示を入力するための操作部１１８が設けられる。操作部１１８としては、現在の状態（認証済みか否を示すＬＥＤ、動作異常を示すＬＥＤ等）を表示するためのチェックボタンと、電気機器本体１０１の作動モードの設定スイッチ等が含まれる。制御部１１５にはさらに、ユーザ４００に対して情報を表示するための表示部１１９が設けられる。電気機器本体１０１としてどの作動モードが設定されているかを示す作動モード表示、動作異常が発生しているか否かを示す表示（異常状態表示）、ユーザ４００に対する人的認証が正常に行われたか否かを示す表示（認証状態表示）等が含まれる。表示部１１９は、１つ又は複数のＬＥＤにより実現できるが、複数個の単色又は多色ＬＥＤ、セグメントＬＥＤ、液晶ディスプレイ、その他の視覚的出力装置を用いても良い。

【００３５】

情報端末１０は、図示しないＣＰＵ（Central Processing Unit）を含む制御部１５を有し、制御部１５は必要な情報を表示部１１に表示させる。表示部１１は、タッチ式のディスプレイを用いることにより情報を表示する出力機器（表示部１１）と共に、ユーザ４００による操作を入力するための入力機器（指示受付部１２）として機能させることができる。情報端末１０にはブルートゥース（登録商標）用の無線通信部１３（端末側無線通信部）が設けられ、無線通信部１３には図示しないアンテナが接続される。電池パック５０の無線通信部６８と、情報端末１０の無線通信部１３は所定の無線通信可能範囲で行うことができ、無線通信可能範囲を外れる（例えば機器同士の距離が遠すぎる等）と無線通信が不能となる。

【００３６】

以上のように、電気機器１００側（具体的には電池パック５０）に無線通信部６８を設けることにより、電気機器１００と外部機器（ここでは情報端末１０）との無線通信が可能となる。本実施例において電池パック５０は、中継機器として、外部電気機器（情報端末１０）と電池パックが装着された電気機器本体１０１との間の通信を可能としている（電池パック５０の動作モードを"中継通信モード"と呼ぶ）が、電池パック５０内でなく電気機器本体１０１内に無線通信部（図示せず）を設けるようにすれば、電池パック５０を介することなく電気機器本体１０１のマイコン１１６と外部機器（ここでは情報端末１０）が直接通信できる。

【００３７】

上記構成において、情報端末１０は専用アプリの起動時に、登録した相手（電池パック５０Ａ）と自動で無線接続し、認証用の情報を送信する。電池パック５０は、未認証状態では無線通信接続試行状態として未認証作動モードとし、通信接続した場合に認証情報を受信して、記憶された認証情報と一致したら通常作動モードになる。電池パック５０の制御部５５は省電力のため、所定時間不使用状態が継続したらスリープ状態、又は、シャットダウンさせても良い。その場合、電源をオンにしたとき（電池パック５０の制御部５５がスリープ状態又はシャットダウン状態から復帰したとき）に改めて無線通信接続・認証処理を行う。これは、ユーザ４００の操作なし（情報端末１０のロック解除もなし）に認証処理が行われることを意図している。認証情報が記憶されている情報端末１０において専用アプリがバックグラウンドで実行されており、設定済みの相手（電気機器１００）と自動で通信接続及び認証処理が可能な構成を想定している。その構成の場合、省電力のために通信を解除しても、再び電源をオンにしたときに、自動で通信接続及び認証処理が行われるため、作業性を損なわない利点がある。

【００３８】

図３は図１の電気機器１００に示す認証モードの遷移図である。（Ａ）は従来例の認証手順の例である。電気機器１００を使用するに当たって、ユーザ４００は電気機器本体１０１に対して個人認証を行う。図３（Ａ）において、時刻０において電気機器本体１０１のマイコン１１６が起動（スリープ状態又はシャットダウン状態から復帰）すると、マイコン１１６は認証プロセスを開始する。電気機器本体１０１がインパクト工具等の電動工具である場合は、トリガスイッチ１０６が引かれると制御部１１５に動作用の定電圧（５Ｖ又は３．３Ｖ）が供給されるので、マイコン１１６が起動する。起動したマイコン１１６は情報端末１０に対して認証コードの送信要求をする。情報端末１０から認証情報を受信した電気機器本体１０１のマイコン１１６は、記憶部１１７内に登録されている認証情報と比較し、一致するならば"認証成功"、不一致ならば"認証失敗"との判定を行う。図３（Ａ）は従来例で認証が成功した場合を示しており、時刻t_1にて、認証プロセス１２１が完了して"認証成功"との結果となると、電気機器本体１０１は初めて動作が可能となる。本発明では、この通常の動作が可能な作動モードを「通常作動モード」と呼ぶ。尚、図示していないが、時刻t_1にて認証失敗した場合は、電気機器本体１０１の使用ができない。

【００３９】

図３（Ｂ）は本実施例に係る認証モードの遷移図である。時刻０にてシャットダウン中の電気機器本体１０１のトリガスイッチ１０６が引かれると、電気機器本体１０１は情報端末１０とのとの通信を開始し、認証プロセス１２１を開始する。認証プロセス１２１では、情報端末１０に対して認証コードの送信要求をする。同時に、電気機器本体１０１のマイコン１１６は、制限的な条件の下でモータ１０４を起動し、電気機器本体１０１を稼働させる（未認証作動モード１２３）。このように未認証状態でも作動する"未認証作動モード"を設け、"未認証作動モード"では、所定時間の経過まで、または、認証失敗が数回まで作動可能とした。未認証作動モード"と"通常作動モード"の違いは、"未認証作動モード"では、時間的制限又は／及び認証プロセス終了までの作業を可能とした期間的な制限、電気機器の主機能が作動しない等の機能的な制限、電気機器の出力が低くなる等の出力的な制限、のいずれか一つ以上が付加される。ここで、「未認証でも作動する」

とは、機器の主目的の機能が作動することを意味し、その作動のために必要な処理を含む。例えば、電動機器ならアクチュエータへの通電、熱電機器（冷温庫、ヒーター、炊飯器など）なら熱電装置や素子への通電、照明機器なら発光素子への通電（特に照明として期待される程度の光量・時間が得られる通電）である。未認証作動モード１２３では、通常作動モード１２２とは異なる状態で電気機器本体１０１を稼働させることにより、ユーザに対して未認証状態での使用であること、又は、制限付きの使用モードであることを報知器（特定のＬＥＤの点灯態様による区別）やモータ動作（例えば、通常作動モードに比べて、モータ１０４の回転の立ち上がりが遅い、回転数が低い、回転の立ち下がりが遅い等による区別）で報知するようにしてもよい。

【００４０】

未認証作動モードでの制限を稼働期間による制限とする場合は、期間が満了するまでは未認証作動モード１２３でも通常と同等の作動を実行できる。この未認証作動モード１２３の実行と並行して、マイコン１１６による認証プロセス１２１が並行して実行される。つまり、図３（Ｂ）で示すように、電気機器本体１０１に、未認証でも作動する"未認証作動モード１２３"を設けて、未認証状態でのトリガスイッチ１０６を引いたらすぐに電気機器本体１０１が稼働するようにした。次に、未認証作動モード１２３の実行と並行して行われる認証プロセス１２１によって、時刻t_1において、認証プロセス１２１が完了して"認証成功"との結果がでると、電気機器本体１０１のマイコン１１６は、"未認証作動モード１２３"から"通常作動モード１２２"に移行させる。"通常作動モード"は、未認証作動モード１２３の制限を解除した作動モードである。なお、再認証については、一定周期ではなく、不使用状態が一定時間継続した場合に行っても良い。又は、通常作動モードでは再認証せず、省電力のために不使用状態が一定時間継続してマイコンがシャットダウンしたら、次の起動時に未認証作動モードとなるようにしても良い。

【００４１】

通常作動モード１２２では電気機器本体１０１の通常の使用を許可し、マイコン１１６がシャットダウンするまで使用許可状態を維持しても良い。しかしながら、セキュリティの向上のために、通常作動モード１２２の所定時間毎に認証を行うようにし、認証失敗したら未認証作動モード（又は未認証停止モード１２４）へ移行させても良い。ここでは、認証完了してから所定時間T_2だけ経過したあとに、認証プロセス１２１ａを再度実行する。そして時刻t_3にて認証結果が"認証成功"の場合はそのまま"通常作動モード"を維持し（通常作動モード１２２ａ）、認証結果が"認証失敗"の場合は"未認証停止モード１２４"に移行する。"未認証停止モード１２４"では半導体スイッチング素子１０７のソース－ドレイン間を遮断（非導通）することによりモータ１０４の回転が阻止（停止）される。このように、本実施例では認証が失敗したら、未認証停止モード１２４へ移行することにより、認証されていないユーザによる電気機器１００の使用を禁止する。

【００４２】

図３（Ｃ）は本実施例に係る最初の認証プロセスで認証失敗した際の遷移図である。時刻０～時刻t_1付近までの動作は、図３（Ｂ）の手順と同じである。ここでは時刻t_1よりも後の時刻t_2において認証失敗になっている。認証失敗が起こる具体的な例としては（１）近接無線通信による通信可能範囲外である場合、（２）認証コード不一致による場合、があげられる。近接無線通信による通信可能範囲外である場合は、近接無線通信路が確立しないため時刻t_1を過ぎても認証が未完了のままとなり、時刻t_2にて制限時間到達（タイムアウト時間T_1経過）により"認証失敗"が確定する。すると、電気機器本体１０１のマイコン１１６は、電気機器本体１０１の動作を停止させるべくスイッチング素子１０７のゲート信号をＬｏｗにすることにより、スイッチング素子１０７のソース－ドレイン間を遮断し、モータ１０４の回転を阻止（停止）する。この状態が"未認証停止モード１２４"である。

【００４３】

未認証作動モード１２４への移行は、所定時間T_1経過の時点（時刻t_2）、又は、未認証失敗が確定した時点（例えば認証コードが複数回不一致した時点）であり、それまで

未認証作動モード１２３で稼働していた電気機器本体１０１は、認証できないことが確定した時点にて稼働が阻止（停止）される。また、未認証作動モード１２３で認証が成功したら、認証が成功した旨を示す特定のＬＥＤの点灯表示をすると良い。さらに、図３（Ｂ）、（Ｃ）の未認証停止モード１２４では、所定時間毎（例えばT_2時間毎）に認証を試行するようにして、認証が成功したら、通常作動モード１２２に切り替えて半導体スイッチング素子１０７のソース－ドレイン間を導通させるようにしても良い。

【００４４】

以上、本実施例のように未認証作動モード１２３を設けることで、作動開始前の認証に要する時間がかかって作業開始が遅れるという問題を解消できる。また、認証機器たる情報端末１０の制御部１５が省電力モードやスリープモードになっている場合であっても、電気機器本体１０１をすぐに動作させることができるので、ユーザにとって便利であり、作業性を向上することができる。また、近接無線通信の場合は、電気機器本体１０１側と情報端末１０とのリンク確立に時間がかかるが、その遅延の問題も解消できる。多くの認証を要する電気機器の場合は、未認証状態では全く使わせないようにするのが普通である。しかしながら、未認証でも使用を開始させた方が良い電気機器も存在する。例えば、個人認証を用いて電気機器の盗難抑止を図るような場合である。盗難防止を図る目的であるならば、未認証だとすぐに停止してしまうような電気機器ならば、盗難後は実質的に電動工具として役に立たないので、盗難抑制効果は十分達成できる。

【００４５】

次に図４のシーケンス図を用いて、情報端末１０、電池パック５０、電気機器本体１０１の操作と、通信を用いた認証手順を説明する。図４の例では電池パック５０を電気機器本体１０１に装着し、情報端末１０とペアリングを行い（認証モード）、ペアリング状態を維持したままで電気機器本体１０１の駆動を行う（通常作動モード）。

【００４６】

まず、電池パック５０と情報端末１０のペアリングを行うために、作業者（ユーザ４００）は電池パック５０が装着された状態で電気機器本体１０１の作動スイッチ（ここではトリガスイッチ１０６）を操作する（ステップ４０１）。すると、シャットダウン又はスリープ状態にあった電気機器本体１０１のマイコン１１６（図２参照）と、電池パック５０のマイコン５６（図２参照）が起動する。次に、電気機器本体１０１のマイコン１１６は、動作モードを"未認証作動モード"に設定し（ステップ１５１）、電力で駆動される負荷装置（ここではモータ１０４）の稼働を許可する（ステップ１５２）ことによってモータ１０４がオンになる（ステップ１２５）。この稼働許可は、マイコン１１６がスイッチング素子１０７のゲート信号をＨｉｇｈにして、ソース－ドレイン間を導通させることで、トリガスイッチ１０６の操作によりモータ１０４への電力が供給される。

【００４７】

次に、電気機器本体１０１のマイコン１１６は、電池パック５０のマイコン５６に対して、認証情報を取得して返信するように要求する（ステップ１５３）。認証情報要求を受けた電池パック５０のマイコン５６は、情報端末１０への通信接続を試行する（ステップ７１）。まず、近接無線通信（ここではブルートゥース（登録商標））を用いて情報端末１０に機器情報を送信する（ステップ７２）。情報端末１０は、受信した機器情報から情報端末１０と接続可能な機器であるか否かを判定し（ステップ２２）、接続可能な機器ならば接続要求を行う（ステップ２３）。次に、通信接続の確立、いわゆるペアリング登録を行う。ここで「ペアリング」とは、無線通信を用いて情報端末１０と、電池パック５０側の関連づけ登録を行う作業であり、これらの登録作業（ペアリング）を行うことにより、情報端末１０は、ペアリングされた特定の電池パック５０との通信を行うことができる。このペアリング相手の関係は、情報端末１０：電池パック５０の数＝１：１でも良いが、１：ｎ（ｎは自然数）であっても良い。ｎがいくつまでペアリングできるかは、使用する無線通信規格に依存する。また、所有するすべての無線接続可能な電池パックと同時にペアリングさせても良いが、必ずしも全数を同時に行う必要は無く、稼働させる電気機器本体１０１に装着された電池パック５０だけを選択してペアリングさせるようにすれば良

い。

【００４８】

情報端末１０と電池パック５０の無線通信接続が確立されると（ステップ２４）、電池パック５０のマイコン５６は中継通信モードを設定し（ステップ７３）、情報端末１０に対して認証情報の送信要求を行う（ステップ７４）。送信要求を受けた情報端末１０は、専用のアプリによって入力された情報、又は、予め登録されている情報に従って認証情報を電池パック５０に送信する（ステップ２５）。電池パック５０のマイコン５６は、受け取ったデータを通信端子５４、１１４（図２参照）を介して電気機器本体１０１に伝達する（ステップ７５）。電気機器本体１０１のマイコン１１６は、情報端末１０から受け取った認証情報と、自らの記憶部１１７（図２参照）に登録されている認証情報を照合して正当性を判定する。ここで、認証が成功すると（ステップ１５４）、電気機器本体１０１のマイコン１１６は、認証結果を電池パック５０を介して情報端末１０に送信する（ステップ１５５、７６）し、作動モードを"未認証作動モード"から"通常作動モード"に切り替える（ステップ１５６）。この切り替えタイミングが、図３（Ｂ）の時刻t_1の操作に対応する。通常作動モードでは、電気機器本体１０１の機能を制限無く使用することができる。また、ステップ７６にて認証結果（ここでは"成功"）を受け取った情報端末１０は、その旨を示す可視的な情報を表示部１１に表示する（ステップ２６）。

【００４９】

以上のように、電池パック５０を装着して電気機器本体１０１を使用する際に認証動作を行い、認証が成功したら"通常作動モード"にて使用が可能になる。しかしながら、認証は１回だけでなく、所定の間隔（例えば絶対時間間隔、実作業時間間隔、作業回数間隔）にて再認証プロセスが実行される。ここでは認証成功から所定時間T_2が経過したら（ステップ１５７）、通信端子１１４、５４を介して電池パック５０のマイコン５６に対して認証情報を情報端末１０に要求する（ステップ１５８）。認証情報要求を受け取った電池パック５０のマイコン５６は、中継通信モードに切り替えて（ステップ７７）、無線通信にて情報端末１０に認証情報の送信要求を行う（ステップ７８）。

【００５０】

送信要求を受けた情報端末１０は、登録済みの認証情報を電池パック５０に再送信する（ステップ２７）。電池パック５０のマイコン５６は、受け取ったデータを通信端子５４、１１４を介して電気機器本体１０１に転送し（ステップ７９）、電気機器本体１０１のマイコン１１６は、情報端末１０から受け取った認証情報を用いて認証の整合性を再判定する。ここで、認証が成功すると（ステップ１５９）、電気機器本体１０１のマイコン１１６は、それまでの"通常作動モード"を維持し、認証結果を電池パック５０を介して情報端末１０に送信する（ステップ１６０、８０）。ステップ８０にて認証結果（ここでは"成功"）を受け取った情報端末１０は、その旨を示す可視的な情報、即ちステップ２６で表示済みの情報を表示部１１に継続表示する（ステップ２８）。

【００５１】

以上のように、電気機器本体１０１のマイコン１１６は、認証モードをモータ１０４の実際の稼働とは並列して行うことにより、図中のステップ４０１からステップ１５４までに至る最初の認証プロセスの最中に、モータ１０４の稼働を行うことができる。尚、図４の例では電気機器本体１０１の例として電動工具とし、その負荷部の例として図示しないインパクト機構を駆動するモータ１０４の例で説明したが、電気機器本体１０１の種類や作業内容は任意であり、電池パック５０を用いて何らかの作業、例えば、モータの回転、照明装置の点灯、音響装置の稼働、発熱又は吸熱装置の稼働を行う機器であって、外部機器との通信を行う制御部を有するものであるならば、任意の電気機器本体１０１であっても良い。また、電池パック５０は着脱可能である必要は無く、電気機器１００に内蔵するタイプの電気機器であっても、同様に本実施例を適用できる。

【００５２】

次に、図５を用いて電気機器本体１０１のマイコン１１６における作動モードの設定手順を説明する。図５で示す一連の手順は、電気機器本体１０１のマイコン１１６にあらか

じめ格納されたプログラムによってソフトウェア的に実行される。図５のフローは、電池パック５０が電気機器本体１０１に装着され、マイコン１１６が起動状態になって認証判定（図４で言えばステップ１５４、１５９）ごとに実行される。又は、所定時間間隔毎、或いは、認証判定毎に実行されるようにしても良い。また、図５のフローチャートは動作モードの設定手順であって、並行して行われるモータ１０４の回転制御とは別の処理である。

【００５３】

最初にマイコン１１６は、電気機器本体１０１を使用する個人が正当であるか否かの人的認証が完了しているか否かを判定する（ステップ１３１）。ここで、人的な認証が完了していない場合は、マイコン１１６は"未認証停止モード"に設定済みか否かを判定する（ステップ１３２）。ここで"未認証停止モード"が設定されている場合はステップ１３４に進み、設定されていない場合は電気機器本体１０１の動作モードを"未認証作動モード"に設定してからステップ１３４に進む（ステップ１３３）。

【００５４】

ステップ１３４では、"未認証作動モード"が設定されているか否を判定する。"未認証作動モード"が設定済みでない場合は、ステップ１３８に進む。"未認証作動モード"が設定されている場合は、作動開始から所定時間T_1が経過しているか否かを判定し（ステップ１３５）、経過していたら電気機器本体１０１の動作モードを"未認証停止モード"に設定して、モータ１０４の稼働を禁止（停止）する（ステップ１３７）。この所定時間（T_1＝図３の時刻０～t_2）は、いわゆるタイムアウトであり、例えば数十秒～数分程度に設定可能である。ステップ１３５で所定時間T_1が経過していない場合は、認証プロセスの実行の結果、認証が成功しているか否かを判定する（ステップ１３６）。ここで、認証が失敗の場合は、電気機器本体１０１の動作モードを"未認証停止モード"に設定して、モータ１０４の稼働を禁止し（ステップ１３７）、認証が成功の場合はステップ１３８に進む。

【００５５】

ステップ１３８にて認証が成功しているか否かを判定し、成功ならば動作モードとして"通常作動モード"を設定する（ステップ１３９）。認証が成功していない場合は、ステップ１４０に進む。ステップ１４０では"通常作動モード"であるか否かを判定し、"通常作動モード"が設定済みでない場合は処理を終了し（ステップ１４０）、"通常作動モード"である場合は、認証が失敗したか否かを判定する（ステップ１４１）。ステップ１４１で認証が失敗ならば、電気機器本体１０１の動作モードを"未認証作動モード"に設定し（ステップ１４２）、失敗でない場合は処理を終了する。以上の手順によって、電気機器本体１０１の作動モードとして、"未認証作動モード"、"通常作動モード"、"未認証停止モード"のいずれかが設定されることになる。

【００５６】

次に図６のフローチャートを用いて、電気機器本体１０１のマイコン１１６における認証処理の実行判断手順を説明する。この認証処理は図３の認証プロセス１２１、１２１ａ…として、作動モードにかかわらず定期的な時間間隔T_2で実行される処理である。最初に、電気機器本体１０１のマイコン１１６は、それまで設定されていたモードが"未認証作動モード"か否かを判定する（ステップ１６１）。ここで、未認証作動モードの場合は認証処理を行う（ステップ１６２）。これらステップ１６１と１６２の処理手順が図４のステップ１６４で行われる処理に相当する。

【００５７】

ステップ１６３では、設定されているモードが未認証停止モードであるか否かを判定する。未認証停止モードの場合は、前回の認証失敗の時から所定時間T_2が経過しているか否かを判定し（ステップ１６４）、所定時間T_2が経過したら認証処理を行い（ステップ１６５）、所定時間T_2が経過していなかったらステップ１６６に移行する。

【００５８】

ステップ１６６では、設定されているモードが通常作動モードであるか否かを判定する

。通常作動モードの場合は、前回の認証失敗の時から所定時間T_2が経過しているか否かを判定し（ステップ１６７）、所定時間T_2が経過したら認証処理を行い（ステップ１６８）、所定時間T_2が経過していなかったら図６に示す処理を終了する。これらステップ１６６～１６８の処理手順が図４のステップ１５７、１５９で実行される処理に相当し、作動モードにかかわらず定期的な時間間隔毎に実行される。

【００５９】

次に図７のシーケンス図を用いて、電気機器本体１０１における認証失敗時の処理手順を説明する。図７において、鎖線Ａ１から上側に示す処理は図３で示したシーケンス図と同一手順であり、同一番号の符号を付している。ステップ１７０が、図６のステップ１６１、１６２に至る処理であり、その認証処理の結果、認証が失敗し、"未認証停止モード"となった手順を示している。ステップ１７０における認証結果が"認証失敗"の場合は、その認証結果を電池パック５０を介して情報端末１０に伝達する（ステップ１７１、７６Ａ）。同時に、自らの動作モードを"未認証停止モード"に設定し（ステップ１７２）、半導体スイッチング素子１０７のソース－ドレイン間を遮断することでモータ１０４の動作を禁止する（ステップ１７３）。尚、図７のステップ番号において、図４に対応するステップ番号の末尾にＡを付加しているのは、図４に示すステップの処理と同じ処理であるが、伝達される情報内容が異なる場合を示している。"認証失敗"の結果を受信した情報端末１０は、その結果を表示部１１に表示することによりユーザ４００に、電気機器本体１０１が"未認証停止モード"に設定され、再認証が行われない限り稼働できないことを報知する（ステップ２６Ａ）

【００６０】

電気機器本体１０１のマイコン１１６は、ステップ１７３における認証失敗から設定された所定時間（＝T_2）が経過したか否かを監視し、所定時間T_2が経過したら（ステップ１７４）、再認証を行うべく、電池パック５０を介して情報端末１０に対して認証情報の送信要求を行う（ステップ１７５）。認証情報の送信要求を受け取った電池パック５０のマイコン５６は、中継通信モードを実行し（ステップ７７Ａ、７８Ａ）、電気機器本体１０１から受け取った認証情報要求を近接無線通信を用いて情報端末１０に伝達する（ステップ７７Ａ）。

【００６１】

認証情報の送信要求を受け取った情報端末１０は、近接無線通信を用いて電池パック５０に認証情報を送信し（ステップ２７）、電池パック５０のマイコン５６は、受け取った認証情報を通信端子５４、１１４を介して電気機器本体１０１に転送する（ステップ７９Ａ）。認証情報を受け取った電気機器本体１０１のマイコン１１６は、認証処理を実行する（ステップ１７６）。図７の処理は、図６のフローチャートのステップ１６３～１６５の処理に相当する。

【００６２】

ステップ１７６にて"認証成功"になると、電池パック５０を介して情報端末１０に対して認証結果の伝達を行う（ステップ１７７）と共に、電気機器１００を通常作動モードに設定し（ステップ１７８）、半導体スイッチング素子１０７のゲート信号をハイにすることによりモータ１０４の起動を許可する（ステップ１７９）。認証結果を受け取った電池パック５０のマイコン５６は、中継通信モードの実行であるので、電気機器本体１０１から受け取った認証結果を近接無線通信を用いて情報端末１０に伝達する（ステップ８０Ａ）。認証結果を受け取った情報端末１０は、その結果を表示部１１に表示する（ステップ２８Ａ）。この結果、ユーザ４００は、電気機器本体１０１が"通常作動モード"に設定され、電気機器本体１０１を正常に稼働できるようになったことを認識できる。その後、ユーザ４００は、作業スイッチ（トリガスイッチ１０６）をオンにすることで、電気機器本体１０１のモータ１０４が起動する（ステップ４０２、１２６）。

【００６３】

以上説明した実施例においては、電気機器本体１０１には無線通信部が設けられておらず、電池パック５０に無線通信部６８を設けることで、電気機器１００（電気機器本体１

０１と電池パック）が外部機器である情報端末１０と通信できるように構成した。本発明はこの構成に限定されるものではなく、電気機器本体１０１に無線通信部１２８（後述の図８参照）を設けて、電気機器本体１０１のマイコン１１６と情報端末１０が無線通信によって直接通信するように構成しても良い。その構成を示すのが図８である。

【実施例２】

【００６４】

図８は本発明の第２の実施例に係る電気機器１００Ａ及び情報端末１０の回路構成を示すブロック図である。電気機器１００Ａと電池パック５０Ａの構成は、無線通信部１２８と無線通信部６８（図２参照）の有無を除き、図２で示した電気機器１００と同一であり、同一の部分には同じ符号を伏しているので、繰り返しの説明は省略する。第２の実施例では、電気機器本体１０１Ａに無線通信部１２８を設けて、制御部１１５のマイコン１１６が、近接無線通信を用いて情報端末１０と直接通信を行う。従って、電池パック５０Ａ側には無線通信部６８（図２参照）を設ける必要がない（但し、無線通信部６８が有っても良い）。

【００６５】

情報端末１０の構成は、図１、図２で示したものと同一で有り、専用のアプリを入れる点も同様であるが、情報端末１０から見た接続先ＩＤ情報が第１の実施例では電池パック５０の無線通信部６８の接続ＩＤであるのに、第２の実施例では電気機器本体１０１Ａの無線通信部１２８の接続ＩＤが設定される点で異なる。通信を用いた認証手順のシーケンスは、情報端末１０と電気機器本体１０１Ａの通信が、電池パック５０を介さずに直接行われることを除いて図４、図７と同様である。つまり、図４、図７から電池パック５０を除いた構成とほぼ同様になる。

【００６６】

第２の実施例の特徴は、電池パック５０に無線通信部６８を設ける必要がなくなる点である。また、電気機器本体１０１を用いた作業を行う場合に、複数の電池パック５０を準備して、それらを交換しながら作業を行うが、その場合であっても情報端末１０から見た接続先が固定（無線通信部１２８）であるので、電池パック５０、５０Ａの交換時においても迅速に承認プロセスを実行できる。

【００６７】

以上、第１及び第２の実施例では、電気機器本体１０１を使用するユーザが正当であるか否かの認証（人的認証）において、"未認証作動モード"を設けるように構成したが、同様の認証及び稼働手順を、電気機器本体１０１に装着又接続される機器の正当性の認証プロセス時に適用することも可能である。例えば、電池パック５０、５０Ａが、純正品（正規品）であるかの認証（物的認証）を行う際に、認証プロセスが完了する前にモータ１０４の起動を可能にして、認証プロセスが終了した時点で、電池パック５０、５０Ａが、非正規品と判断された場合（この場合は、認証失敗となる）は、"未認証停止モード"に移行させるようにすれば良い。つまり、電気機器本体１０１のマイコン１１６は、図６のフローチャートの認証処理時に、ユーザ４００の正当性を認証することに加えて、又は、代えて、装着されている電池パック５０、５０Ａが正規品（純正品）又は管理されている電池パックであるか否かを検証する。

【００６８】

電気機器本体１０１のマイコン１１６は、ユーザ４００の認証（第１の認証）及び／又は電池パック５０、５０Ａの認証（第２の認証）を行うようにして、双方又は一方の認証が成功したら"通常作動モード"に移行させる。このように電池パック５０の正当性も合わせて認証するようにすれば、コピー商品の使用を抑制できる。尚、電池パック５０、５０Ａが、電気機器１００、１００Ａに対して純正品であるか否かの認証プロセスは、通信端子５４、１１４、又は／及び、その他の図示しない通信端子を介して有線による通信で行うことができる。例えば、使用機器の一つである電池パックとして、第１の電池パック（正規品、管理されている電池パック）が電気機器本体１０１に接続された状態でトリガスイッチ１０６を操作すると、未認証作動モード１２２でモータの駆動を開始する。その

後、第１の電池パックと電気機器本体１０１との間での認証が成功すると、トリガスイッチ１０６が操作されている間、第１の電池パックが正常の場合、通常動作モード１２３にてモータの駆動を継続する。一方、第２の電池パック（非正規品、管理されていない電池パック）が電気機器本体１０１に接続された状態でトリガスイッチ１０６を操作すると、未認証作動モード１２２でモータの駆動を開始する。その後、第２の電池パックと電気機器本体１０１との間での認証が失敗すると、トリガスイッチ１０６が操作されていても未認証停止モードに移行し、モータの駆動を停止する。

【実施例３】

【００６９】

次に図９を用いて本発明の第３の実施例を説明する。第１及び第２の実施例では電気機器本体１０１のマイコン１１６が情報端末１０と通信を行うことにより、認証プロセスを行っていた。第３の実施例では電池パック５０に無線通信部６８を持たせると共に、ユーザ４００に関する認証を行わせるようにしたものである。ハードウェア構成は図２で示したものと同じであり、電池パック５０の記憶部５７と、電気機器本体１０１の記憶部１１７に格納されているプログラムが異なる。図９は、電池パック５０のマイコン５６がコンピュータプログラムを実行することによって実現される制御である。

【００７０】

電池パック５０が電気機器本体１０１に装着され、最初にトリガスイッチ１０６がオンにされると電気機器本体１０１のマイコン１１６（図２参照）が起動する。すると、マイコン１１６は、認証処理を実行するように通信端子１１４、５４を介して電池パックに要求するので、電池パック５０のマイコン５６は認証要求を受信する（ステップ１８８）。この要求には、電気機器本体１０１の使用が許可されるユーザ４００に関する情報（認証情報）を含まれる。認証情報は、一時的に電池パック５０の記憶部５７に格納される。

【００７１】

次に電池パック５０のマイコン５６は、近接無線通信を用いて情報端末１０との接続を試行する（ステップ１８９）。この手順は、近接無線通信がブルートゥース（登録商標）の場合は、その規格に沿って行われる。ステップ１９０で通信接続が確立したら（ステップ１９０でＹＥＳ）、電池パック５０のマイコン５６は、通信相手たる情報端末１０に対して認証のためのパターン情報を送信するように要求する（ステップ１９１）。この際、電気機器本体１０１の記憶部１１７には、認証用に記憶したパターン情報（パスコードや生体情報（指紋，顔，声など））記録されている。ステップ１９０にて通信接続が確立しなかったらステップ１９０に戻る。次に、電池パック５０のマイコン５６はパターン情報を受信したか否かを判定する（ステップ１９２）。

【００７２】

ステップ１９２にて、パターン情報を受け取れなかったら、パターン情報を要求してからの時間が所定の時間（タイムアウト時間）を越えたか否かを判定し、越えていたら認証失敗であるとしてステップ１９５に進む。ステップ１９２にてパターン情報を受信したら、電池パック５０のマイコン５６は、ステップ１８８にて情報端末１０から受信した認証情報とパターン情報を比較することにより、それらが一致するか否かを判定する（ステップ１９３）。一致した場合は、認証成功であるので、"認証成功"との認証結果を通信端子５４、１１４（図２参照）で電気機器本体１０１に伝達すると共に、近接無線通信にて情報端末１０にも認証成功である旨を伝達して処理を終了する。"認証成功"との認証結果を受け取った後の電気機器本体１０１のマイコン１１６の制御は、図４のシーケンス図のステップ１５４以降の制御（１５５～１６０）と同じである。また、"認証成功"との認証結果を受け取った後の情報端末１０の制御は、図３のシーケンス図のステップ２６、２８と同じである。

【００７３】

ステップ１９３にて電気機器本体１０１から受信した認証情報と情報端末１０から受け取ったパターン情報が一致しなかった場合は認証失敗であるので（ステップ１９７）、認証のリトライを行う。ここでは、失敗回数３回目まではステップ１９１に戻ることにより

再認証を行う。失敗回数が３回続いたらステップ１９５に進み、"認証失敗"との認証結果を通信端子５４、１１４（図２参照）で電気機器本体１０１に伝達すると共に、近接無線通信にて情報端末１０にも伝達して処理を終了する。"認証失敗"との認証結果を受け取った後の電気機器本体１０１のマイコン１１６の制御は、図７のシーケンス図のステップ１７０以降の制御（１７３、１７４）と同じであり、モードが"未認証停止モード"に変更される。また、"認証失敗"との認証結果を受け取った後の情報端末１０の制御は、図７のシーケンス図のステップ２６と同じである。

【００７４】

第３の実施例では認証機能付きの電池パック５０Ａを用いることで、ユーザ認証機能をもたない従来の電気機器本体１０１でも、ユーザ４００の正当性を判断することができる。また、認証プロセスに要する時間が、作動時間に影響しないので、電気機器の迅速な作業開始が可能となる。また、電池パック５０Ａに認証機能を持たせることにより、電気機器本体１０１の認証機能の有無が作動時間に影響しない。さらに、認証技術や環境（情報端末の種類／設定を含む）によって、作動時間が遅れることが無く安定した使用感の電動工具を実現できる。

【００７５】

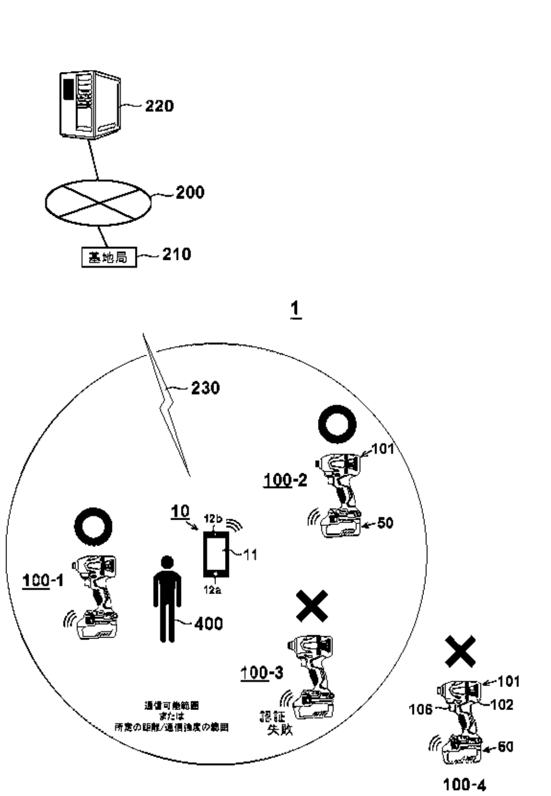
以上、本発明を実施例に基づいて説明したが、本発明は上述の実施例に限定されるものではなく、その趣旨を逸脱しない範囲内で種々の変更が可能である。例えば、上述の実施例では電気機器の一例として電動工具の一つであるインパクト工具で説明したが、電気機器は、ユーザ認証の必要な機器であれば任意の機器でも実現可能である。尚、本発明の認証装置は、情報端末１０だけでなく、被認証機器（電気機器１００）からの無線による要求に応じて、予め決められた認証コードを無線にて返信する小型無線装置、いわゆる電子キーを用いた認証装置であっても良い。この場合は、ユーザは被認証機器（電子キー）を持つか、または、近接の場所に置かないと電気機器１００を通常作動モードで動作できないようなシステムになる。

【符号の説明】

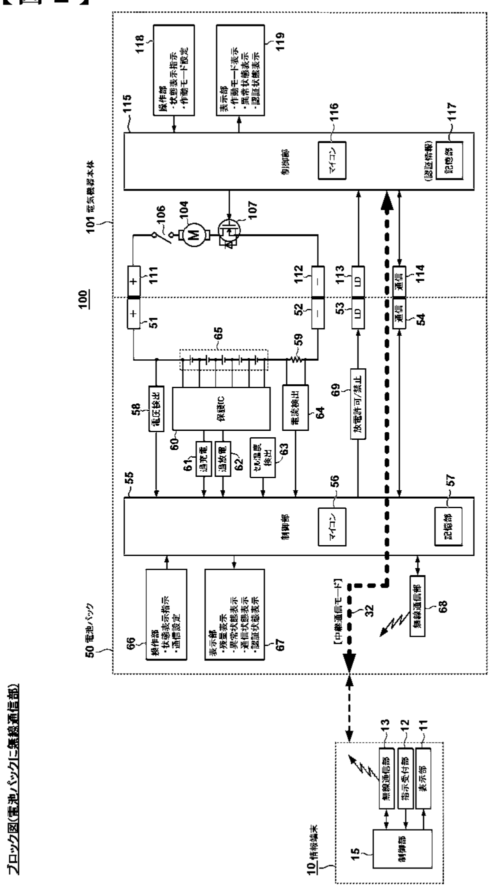
【００７６】

１　電気機器システム　　１０　情報端末　　１１　表示部　　１２　指示受付部
１２ａ　タッチパッド　　１２ｂ　カメラ　　１３　無線通信部　　１５　制御部
３２　中継通信モード　　５０、５０Ａ　電池パック　　５１　正極端子
５２　負極端子　　５３　ＬＤ端子　　５４　通信端子　　５５　制御部
５６　マイコン　　５７　記憶部　　５８　電圧検出部　　５９　シャント抵抗
６０　電池保護ＩＣ　　６１　過充電検出信号　　６２　過放電検出信号
６３　セル温度検出部　　６４　電流検出部　　６５　二次電池　　６６　操作部
６７　表示部　　６８　無線通信部　　６９　禁止信号
１００、１００Ａ　電気機器　　１０１、１０１Ａ　電気機器本体
１０４　モータ　　１０６　トリガスイッチ　　１０７　半導体スイッチング素子
１１１　正極端子　　１１２　負極端子　　１１３　ＬＤ端子
１１４　通信端子　　１１５　制御部　　１１６　マイコン　　１１７　記憶部
１１８　操作部　　１１９　表示部　　１２１、１２１ａ　認証プロセス
１２２、１２２ａ　通常作動モード　　１２３　未認証作動モード
１２４　未認証停止モード　　１２８　無線通信部　　１３１　未認証作動モード
１３２、１３２ａ　通常作動モード　　１３３　未認証停止モード
２００　ネットワーク網　　２２０　サーバ装置　　２３０　電話回線
２３５　通信スイッチ　　４００　ユーザ

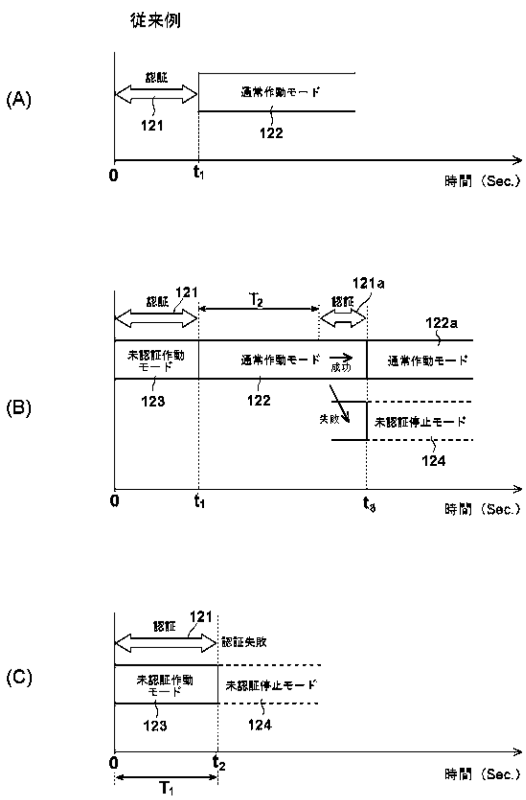
【図１】


220
200
基地局
210
1
230
10
12b
11
12a
100-1
100-2
101
50
400
100-3
認証
失敗
101
102
106
50
100-4
通信可能範囲
または
所定の距離/通信強度の範囲

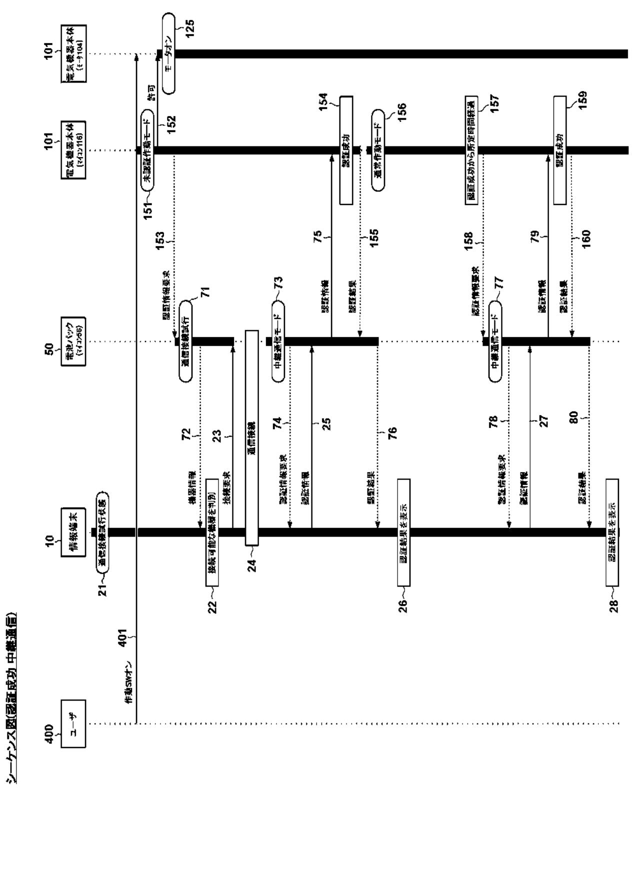
【図２】



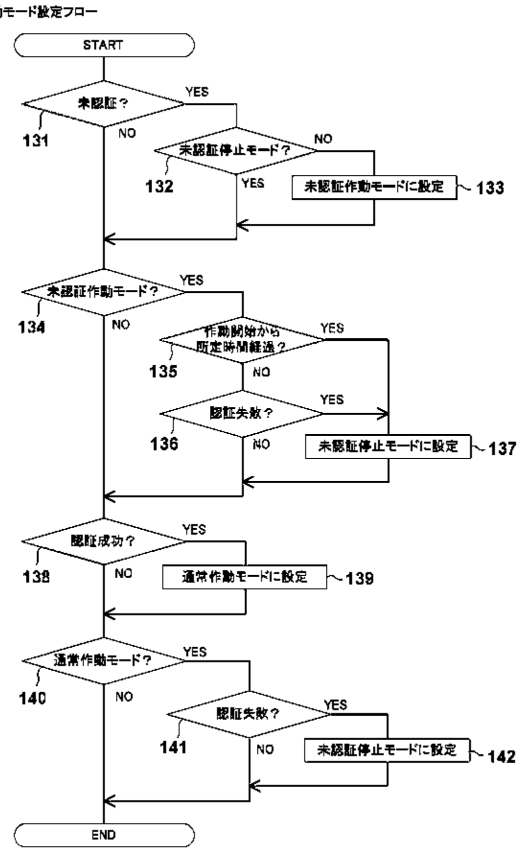
【図３】


従来例
(A)
認証
121
通常作動モード
122
0
t_1
時間（Sec.）
(B)
認証
121
T_2
121a
認証
122a
未認証作動
モード
通常作動モード
成功
通常作動モード
123
122
失敗
未認証停止モード
124
0
t_1
t_3
時間（Sec.）
(C)
認証
121
認証失敗
未認証作動
モード
未認証停止モード
123
124
0
t_2
T_1
時間（Sec.）

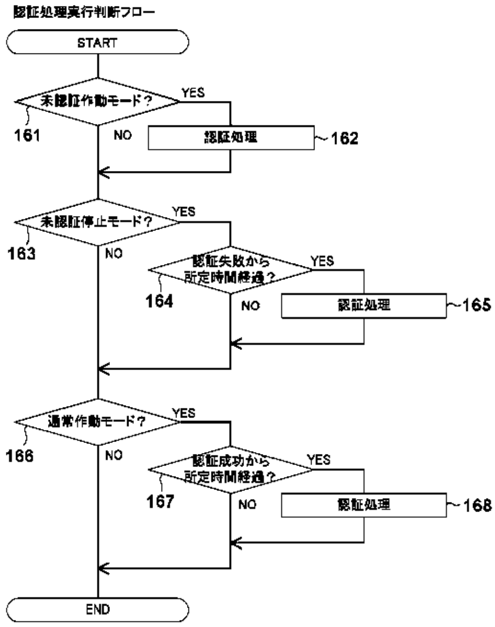
【図４】



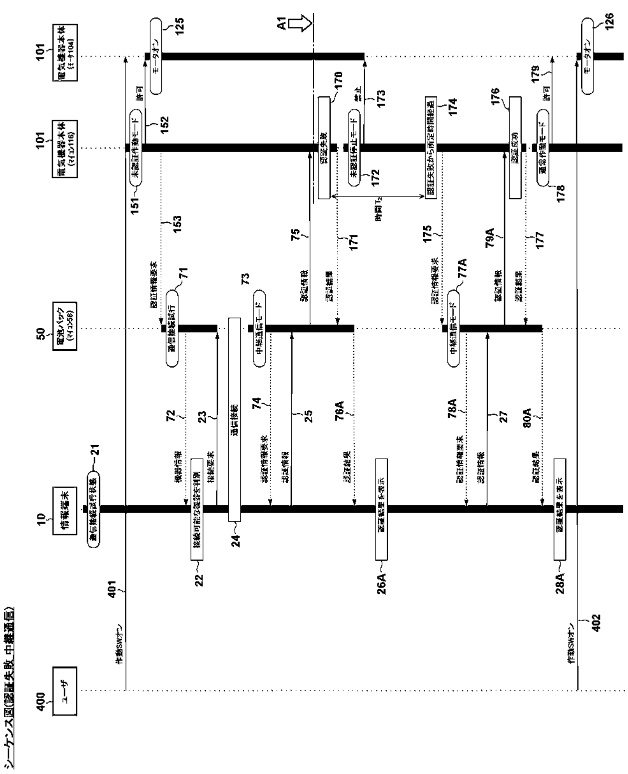
【図５】


作動モード設定フロー
START
未認証？
YES
NO
131
未認証停止モード？
NO
132
YES
未認証作動モードに設定
133
未認証作動モード？
YES
134
NO
作動開始から所定時間経過？
YES
135
NO
認証失敗？
YES
136
NO
未認証停止モードに設定
137
認証成功？
YES
138
NO
通常作動モードに設定
139
通常作動モード？
YES
140
NO
認証失敗？
YES
141
NO
未認証停止モードに設定
142
END

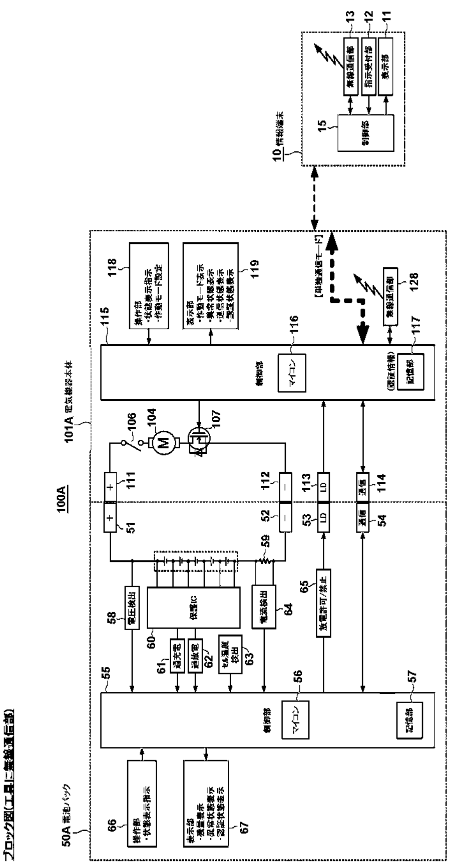
【図６】


認証処理実行判断フロー
START
未認証作動モード？
YES
161
NO
認証処理
162
未認証停止モード？
YES
163
NO
認証失敗から所定時間経過？
YES
164
NO
認証処理
165
通常作動モード？
YES
166
NO
認証成功から所定時間経過？
YES
167
NO
認証処理
168
END

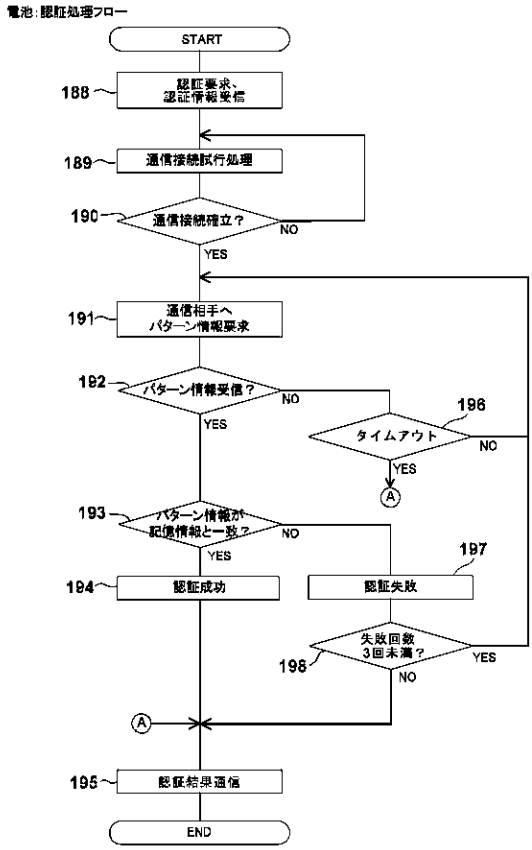
【図７】


シーケンス図(認証失敗_中継通信)

【図８】


ブロック図(工具に無線通信部)

【図９】


電池：認証処理フロー
START
188
認証要求、
認証情報受信
189
通信接続試行処理
190
通信接続確立？
NO
YES
191
通信相手へ
パターン情報要求
192
パターン情報受信？
NO
YES
196
タイムアウト
NO
YES
A
193
パターン情報が
記憶情報と一致？
NO
YES
197
194
認証成功
認証失敗
198
失敗回数
3回未満？
YES
NO
A
195
認証結果通信
END