(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4970221号
(P4970221)

(45)発行日　平成24年7月4日(2012.7.4)　(24)登録日　平成24年4月13日(2012.4.13)

(51)Int.Cl.　F I
H04Q 9/00 (2006.01)　H04Q 9/00 301Z
G06F 21/20 (2006.01)　G06F 21/20 131Z

請求項の数 8　(全 24 頁)

(21)出願番号　特願2007-298417 (P2007-298417)
(22)出願日　平成19年11月16日 (2007.11.16)
(65)公開番号　特開2009-124592 (P2009-124592A)
(43)公開日　平成21年6月4日 (2009.6.4)
審査請求日　平成22年10月15日 (2010.10.15)

(73)特許権者　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100109830
弁理士　福原　淑弘
(74)代理人　100075672
弁理士　峰　隆司
(74)代理人　100095441
弁理士　白根　俊郎

最終頁に続く

(54)【発明の名称】省電力制御装置及び方法

(57)【特許請求の範囲】
【請求項１】
認証符号を含む無線操作信号を受信する受信手段と、
1番目からＮ（Ｎは２以上の自然数）番目までの異なる複数の認証符号を記憶するメモリと、
前記受信手段で前記無線操作信号を受信する度に、該無線操作信号中の前記認証符号が、前記メモリに記憶されている前記複数の認証符号のうちの１つと一致する有効な認証符号であるか否かを判定する判定手段と、
前記判定手段で前記無線操作信号中の前記認証符号が有効と判定されたとき、主装置へ操作信号を出力する出力手段と、
前記受信手段で受信された各無線操作信号中の前記認証符号が、前記メモリに記憶されている前記複数の認証符号のうちの１番目の認証符号に一致する回数を計数するカウンタと、
（ａ）前記カウンタの値が予め定められた設定値に等しいとき、または（ｂ）前記無線操作信号中の前記認証信号が前記メモリに記憶されている前記複数の認証符号のうちの２番目以降の認証符号と一致するとき、新たな認証符号を生成し、前記メモリに記憶されている前記複数の認証符号のうちの少なくとも一つを削除して、前記新たな認証符号を前記メモリに記憶する制御手段と、
を具備することを特徴とする省電力制御装置。
【請求項２】

第１認証符号及び第２認証符号を含む無線操作信号、もしくは第１認証符号を含む無線操作信号と第２認証符号を含む無線操作信号とを受信する受信手段と、
1番目からＮ（Ｎは２以上の自然数）番目までの異なる複数の第１認証符号を記憶する第１メモリと、
１番目からＭ（Ｍは２以上の自然数）番目までの異なる複数の第２認証符号を記憶する第２メモリと、
前記受信手段で前記無線操作信号を受信する度に、該無線操作信号中の前記第１認証符号が、前記第１メモリに記憶されている前記複数の第１認証符号のうちの１つと一致する有効な認証符号であるか否かを判定する第１判定手段と、
前記第１判定手段で前記無線操作信号中の前記第１認証符号が有効と判定されたとき起動され、前記受信手段で受信された前記無線操作信号中の前記第２認証符号が、前記第２メモリに記憶されている前記複数の第２認証符号のうちの１つと一致する有効な認証符号であるか否かを判定する第２判定手段と、
前記第２判定手段で前記無線操作信号中の前記第２認証符号が有効と判定されたとき、主装置に対する操作信号を出力する出力手段と、
前記第２判定手段で前記無線操作信号中の前記第２認証符号が有効と判定される度に、新たな第２の認証符号を生成し、前記第２メモリに記憶されている前記複数の第２認証符号のうちの少なくとも１つを削除して、前記新たな第２認証符号を前記第２メモリに記憶する第１制御手段と、
前記受信手段で受信された各無線操作信号中の前記第１認証符号が、前記第１メモリに記憶されている前記複数の第１認証符号のうちの１番目の第１認証符号に一致する回数を計数するカウンタと、
（ａ）前記カウンタの値が予め定められた設定値に等しいとき、または（ｂ）前記無線操作信号中の前記第１認証信号が、前記第１メモリに記憶されている前記複数の第１認証符号のうちの２番目以降の認証符号と一致するとき、新たな第１認証符号を生成し、前記第１メモリに記憶されている前記複数の第１認証符号のうちの少なくとも１つを削除して、前記新たな第１認証符号を前記第１メモリに記憶する第２制御手段と、
を含む省電力制御装置。
【請求項３】
前記第２制御手段は、前記第１判定手段で前記無線操作信号中の前記第１認証符号が有効と判定され、且つ前記第２判定手段で前記無線操作信号中の前記第２認証符号が無効と判定されたときには、新たな第１認証符号を生成し、前記第１メモリに記憶されている前記複数の第１認証符号のうちの少なくとも１つを削除して、前記新たな第１認証符号を前記第１メモリに記憶する請求項２記載の省電力制御装置。
【請求項４】
前記制御手段は、前記メモリから前記１番目の認証符号を削除することを特徴とする請求項１記載の省電力制御装置。
【請求項５】
前記第２制御手段は、前記第１メモリから前記１番目の第１認証符号を削除することを特徴とする請求項２または３記載の省電力制御装置。
【請求項６】
前記受信手段は、
アンテナと、
前記アンテナで受信された前記無線操作信号を整流して整流電圧を発生する整流器と、
前記整流電圧の供給を受けて電流を発生して、該電流を増幅し、増幅された電流の大きさに応じた電圧信号を出力する起動回路と、
を含むことを特徴とする請求項１または２記載の省電力制御装置。
【請求項７】
認証符号を含む無線操作信号を受信する受信手段と、
1番目からＮ（Ｎは２以上の自然数）番目までの異なる複数の認証符号を記憶するメモ

リを含み、前記受信手段で前記無線操作信号を受信する度に、該無線操作信号中の前記認証符号が、前記メモリに記憶されている前記複数の認証符号のうちの１つと一致する有効な認証符号であるか否かを判定する認証手段と、
前記認証手段での判定結果を用いて、主装置へ操作信号を出力するための制御を行う制御手段と、
を含む省電力制御装置における省電力制御方法であって、
前記受信手段が、前記無線操作信号を受信する受信ステップと、
前記認証手段が、前記受信ステップで受信された前記無線操作信号中の前記認証符号が有効な認証符号であるか否かを判定する判定ステップと、
前記判定ステップで前記無線操作信号中の前記認証符号が有効と判定されたとき、前記認証手段が前記制御手段を起動するステップと、
前記制御手段が、前記操作信号を出力するステップと、
前記受信ステップで受信された前記無線操作信号中の前記認証符号が、前記メモリに記憶されている前記複数の認証符号のうちの１番目の認証符号に一致するとき、前記制御手段がカウンタ値を１つインクリメントするステップと、
（ａ）前記カウンタ値が予め定められた設定値に等しいとき、または（ｂ）前記無線操作信号中の前記認証信号が前記メモリに記憶されている前記複数の認証符号のうちの２番目以降の認証符号と一致するとき、前記制御手段が、新たな認証符号を生成し、前記メモリに記憶されている前記複数の認証符号のうちの少なくとも１つを削除して、前記新たな認証符号を前記メモリに記憶するステップと、
を含む省電力制御方法。
【請求項８】
第１認証符号及び第２認証符号を含む無線操作信号、もしくは第１認証符号を含む無線操作信号と第２認証符号を含む無線操作信号とを受信する受信手段と、
1番目からＮ（Ｎは２以上の自然数）番目までの異なる複数の認証符号を記憶する第１メモリを含み、前記受信手段で前記無線操作信号を受信する度に、該無線操作信号中の前記第１認証符号が、前記第１メモリに記憶されている前記複数の第１認証符号のうちの１つと一致する有効な認証符号であるか否かを判定する第１認証手段と、
１番目からＭ（Ｍは２以上の自然数）番目までの異なる複数の第２認証符号を記憶する第２メモリを含み、前記受信手段で受信された前記無線操作信号中の前記第２認証符号が、前記第２メモリに記憶されている前記複数の第２認証符号のうちの少なくとも１つと一致する有効な認証符号であるか否かを判定する第２認証手段と、
前記第１認証手段及び前記第２認証手段での判定結果を用いて、主装置へ操作信号を出力するための制御を行う制御手段と、
を含む省電力制御装置における省電力制御方法であって、
前記受信手段が、前記無線操作信号を受信する受信ステップと、
前記第１認証手段が、前記受信ステップで受信された前記無線操作信号中の前記第１認証符号が有効な認証符号であるか否かを判定する第１判定ステップと、
前記第１判定ステップで前記無線操作信号中の前記第１認証符号が有効と判定されたとき、前記第１認証手段が前記第２認証手段及び前記制御手段を起動するステップと、
前記第２認証手段が、前記受信ステップで受信された前記無線操作信号中の前記第２認証符号が有効な認証符号であるか否かを判定する第２判定ステップと、
前記第２判定ステップで前記無線操作信号中の前記第２認証符号が有効と判定されたとき、前記制御手段が前記操作信号を出力するステップと、
前記第２判定ステップで前記無線操作信号中の前記第２認証符号が有効と判定されたとき、前記制御手段が、新たな第２の認証符号を生成し、前記第２メモリに記憶されている前記複数の第２認証符号のうちの1つを削除して、前記新たな第２認証符号を前記第２メモリに記憶するステップと、
前記受信ステップで受信された前記無線操作信号中の前記第１認証符号が、前記第１メモリに記憶されている前記複数の認証符号のうちの１番目の第１認証符号に一致するとき

、前記制御手段がカウンタ値を１つインクリメントするステップと、
（ａ）前記カウンタ値が予め定められた設定値に等しいとき、または（ｂ）前記無線操作信号中の前記第１認証信号が前記第１メモリに記憶されている前記複数の第１認証符号のうちの２番目以降の第１認証符号と一致するとき、または（ｃ）前記第１判定ステップで前記無線操作信号中の前記第１認証符号が有効と判定され、且つ前記第２判定ステップで前記無線操作信号中の前記第２認証符号が無効と判定されたとき、前記制御手段が、新たな第１認証符号を生成し、前記第１メモリに記憶されている前記複数の第１認証符号のうちの少なくとも１つを削除して、前記新たな第１認証符号を前記第１メモリに記憶するステップと、
を含む省電力制御方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、電子機器（主装置）の省電力制御装置に関する。
【背景技術】
【０００２】
認証が成功する度に認証符号を変えるワンタイムパスワードである、非特許文献１に記載のS/Key（登録商標）による認証では、認証装置から被認証装置に対して認証OK/NGをフィードバックするため、常に認証符号の同期が取れる。しかし、被認証装置から認証装置（該電力制御装置）への一方向通信のみ可能な場合にS/Key（登録商標）のようなワンタイムパスワード方式での認証を行うと、同期をとる手段（認証が成功したことの確認応答を認証装置から被認証装置へ伝える手段）がないため、認証符号の同期がずれることがある。
【０００３】
時刻同期式のワンタイムパスワード認証では、同期ずれ（＝時刻ずれ）を修正するため、認証装置が認証OKとする複数の認証符号の候補を保持しておく方法が取られている。例えば、非特許文献２に示したRSA セキュリティ社製 の認証トークンであるＳｅｃｕｒＩＤ（登録商標）がある。
【０００４】
しかし、前記省電力制御装置で多数の認証符号との照合を行うと、回路規模や消費電力が増大してしまうという問題がある。ほぼ「０」の極めて微弱な電力によって信号の照合を行う装置で複数の認証符号との照合を行う際には、回路規模や消費電力を最小化するため、照合を行う認証符号の数を最小限にする必要がある。
【非特許文献１】Ｈａｌｌｅｒ，　Ｎ．，　“Ｔｈｅ　Ｓ／ＫＥＹ　Ｏｎｅ・Ｔｉｍｅ　Ｐａｓｓｗｏｒｄ　Ｓｙｓｔｅｍ”，　ＩＳＯＣ，１９９４
【非特許文献２】“ＲＳＡ　ＳｅｃｕｒＩＤ”、［online］、［平成１９年１０月２６日検索］、インターネット＜ＵＲＬ：ｈｔｔｐ：／／ｗｗｗ．ｒｓａ．ｃｏｍ／ｎｏｄｅ．ａｓｐｘ？ｉｄ＝１１５６＞
【発明の開示】
【発明が解決しようとする課題】
【０００５】
上述したように、多数の認証符号との照合を行うと、回路規模や消費電力が増大してしまうという問題があった。
【０００６】
そこで本発明は上記問題点に鑑み、照合する認証符号の候補を最小限にし、回路規模や消費電力を最小限に抑えることができる省電力制御装置及び方法を提供することを目的とする。
【課題を解決するための手段】
【０００７】
認証符号を含む無線操作信号を受信する受信手段と、

1番目からＮ（Ｎは２以上の自然数）番目までの異なる複数の認証符号を記憶するメモリと、
前記受信手段で前記無線操作信号を受信する度に、該無線操作信号中の前記認証符号が、前記メモリに記憶されている前記複数の認証符号のうちの１つと一致する有効な認証符号であるか否かを判定する判定手段と、
前記判定手段で前記無線操作信号中の前記認証符号が有効と判定されたとき、主装置へ操作信号を出力する出力手段と、
前記受信手段で受信された各無線操作信号中の前記認証符号が、前記メモリに記憶されている前記複数の認証符号のうちの１番目の認証符号に一致する回数を計数するカウンタと、
（ａ）前記カウンタの値が予め定められた設定値に等しいとき、または（ｂ）前記無線操作信号中の前記認証信号が前記メモリに記憶されている前記複数の認証符号のうちの２番目以降の認証符号と一致するとき、新たな認証符号を生成し、前記メモリに記憶されている前記複数の認証符号のうちの少なくとも１つを削除して、前記新たな認証符号を前記メモリに記憶する制御手段と、
を具備する。
【０００８】
また、前記受信手段は、
アンテナと、
前記アンテナで受信された前記無線操作信号を整流して整流電圧を発生する整流器と、
前記整流電圧の供給を受けて電流を発生して、該電流を増幅し、増幅された電流の大きさに応じた電圧信号を出力する起動回路と、を含む。
【発明の効果】
【０００９】
本発明によれば、回路規模や消費電力を最小限に抑えることができる。
【発明を実施するための最良の形態】
【００１０】
以下、図面を参照して本発明の実施形態について説明する。
【００１１】
（第１の実施形態）
図１は、本実施形態に係る省電力制御装置１と、これに関連する周辺の装置との関係を概念的に示したものである。操作端末２は、省電力制御装置１を無線信号によって操作するための無線端末である。主装置３は、省電力制御装置１が電力を制御する対象となる電子機器である。例えば、省電力制御装置１をテレビ受像機のリモコン受信部に使用する場合は、主装置３はテレビ受像機本体、操作端末２は電波でテレビ受像機を操作するリモコン、省電力制御装置１はリモコン受信部またはテレビ受像機の電源を操作する部分に相当する。なお省電力制御装置１はテレビ受像機に限らず、照明装置や空調装置、通信端末や通信基地局、計算機、自動車など、無線信号で遠隔から操作を行うあらゆる電子機器、電気機器にて実施可能である。
【００１２】
図２は、第１の実施形態に係る省電力制御装置１の構成例を示したものである。省電力制御装置１は、アンテナ１０１、整流器１０２、起動回路１０３、電源制御部１０４、第１認証部１５１及び主制御部１５３を含む。第１認証部１５１は第１信号判定部１０５及び第１メモリ１０６を含み、主制御部１５３は制御部１０７、演算部１０８及び第２メモリ１０９を含む。
【００１３】
アンテナ１０１は、操作端末１０２からの特定周波数の無線信号を受信する。
【００１４】
省電力制御装置１が電源オフ状態のとき、特定の周波数に整合するアンテナ１０１により到来電波が受信されると、整流器１０２、起動回路１０３、及び電源制御部１０４の機

能により省電力制御装置１のうちの少なくとも第１認証部１５１の電源がオンする。

【００１５】

操作端末２から送信された信号を受信したアンテナ１０１から出力されたＲＦ信号は、整流器１０２に入力される。

【００１６】

整流器１０２は、アンテナ１０１から出力されたＲＦ信号を整流して整流電圧（直流電圧）を発生する。つまり、アンテナ１０１と整流器１０２とで、外部のエネルギーを受けて発電する発電部をなしている。なお、整流器１０２は図３に示すように電源供給は特に必要ない（具体的には後述する）。ただし、電位基準のため、グランドのみ起動回路１０３からの接続がある。

【００１７】

起動回路１０３は、整流器１０２が出力する整流電圧に応じてレベル（ハイ・ロー）が変動する信号を出力する。この出力信号は、電源制御部１０４と、第１の信号判定部１０５に供給される。

【００１８】

電源制御部１０４は、第１認証部１５１の電源オンオフを制御する電源スイッチである。電源制御部１０４に起動回路１０３からの出力信号が一旦入力されると、電源オンとする状態を保持可能に構成されている。第１認証部１５１がオン状態となると、第１信号判定部１０５及び第１メモリ１０６が動作する。

【００１９】

アンテナ１０１で受信された信号のうち、プリアンブル部分に続く無線操作信号の第１認証符号部分により、起動回路１０３の電流電圧変換器１２の出力は、該第１認証符号に応じて出力レベル（ハイ／ロー）が変動する。この電流電圧変換器１２からの出力信号が第1信号判定部１０５に入力されると、第１信号判定部１０５は、この信号と第１メモリ１０６に記録されている複数の第１認証符号とを比較し、該信号が、該複数の第１認証符号のうちのいずれか１つ一致する有効な認証符号であるか否かを判定する。第１信号判定部１０５は、起動回路１０３の電流電圧変換器１２からの第１認証符号に相当する出力信号が第１メモリ１０６内に記憶されているいずれか１つの第１認証符号と一致して有効な認証符号であると判定された場合（すなわち、第１認証が成功した場合）には、主制御部１５３（制御部１０７、演算部１０８、第２メモリ１０９）を起動するための起動信号を出力する。該出力信号が第１メモリ１０６内に記憶されているどの第１認証符号とも一致せず、有効な認証符号でない、すなわち無効と判定された場合（すなわち、第１認証が失敗した場合）には、該起動信号は出力されない（制御部１０７、演算部１０８、第２メモリ１０９は起動しない）。起動信号として用いる符号は設計事項であり任意である。

【００２０】

第１メモリ１０６は、第１認証符号を記憶するためのもので、常時電源が供給されなくても情報を保持することが可能なフラッシュメモリなどの記憶装置で構成される。

【００２１】

第１メモリ１０６は、同期ずれが発生した際に次の認証符号での認証を可能とするため、第１認証符号となる異なる２つの符号を記憶する。なお、第１認証符号は１つの符号に限らず、複数の符号を持つことが望ましい。複数の符号を持つ理由は、操作端末２からの信号のうち幾つかが省電力制御装置１に到達できなかった場合に（認証符号の同期がずれてしまった場合に）、第１認証符号として操作端末２から次の認証符号が送信される可能性があるためである。具体例については後述する。

【００２２】

制御部１０７は、第１信号判定部１０５からの起動信号を受けた際に起動し、主装置３に対し操作信号を出力する。また、第１メモリ１０６に記憶する第１認証符号を計算するよう演算部１０８に対して指示する。

【００２３】

演算部１０８は、第２メモリ１０９が記憶している秘密鍵情報と乱数を基に新たな第１

認証符号を生成し第１メモリ１０６に記録する。認証符号を生成する計算アルゴリズムは任意であり、例えばＤＥＳ、３ＤＥＳ、ＡＥＳ等の暗号アルゴリズムを用いればよい。秘密鍵情報と乱数は、省電力制御装置１と操作端末２との間で共有される符号であり、符号の長さや種類や内容は任意であるが、符号の長さについては、認証符号を生成するために使用する計算アルゴリズム毎に制限がある場合がある。例えば、計算アルゴリズムとしてＤＥＳを使用する際は、秘密鍵情報として５６ビットの符号を、乱数として６４ビットの整数倍の長さの符号を用いる。

【００２４】

また、計算アルゴリズムとしてＭＤ５、ＳＨＡ１、ＳＨＡ２５６等の一方向性ハッシュ関数を用いてもよい。この場合は、第２メモリ１０９が秘密鍵情報を保持する必要はなく、乱数を保持すればよい。乱数として使用する符号の長さや種類は、暗号アルゴリズムを使用する場合と同様に任意である。

【００２５】

第２メモリ１０９は、演算部１０８が認証符号を生成するのに必要な秘密鍵情報、乱数、第一認証符号の認証回数カウンタを保持する。秘密鍵情報、乱数に関しては前述したとおりであり、認証符号を生成するアルゴリズムに基づいて必要なものを保持すればよい。

【００２６】

制御部１０７は、第１認証符号で認証が成功したら第１認証符号の認証回数カウンタの値（以降Ｎと表記）に「１」を加算し、カウンタ値が予め定められた値（以降Ｎｍａｘと表記）に達したら、該カウンタ値Ｎを「１」とし、第１メモリ１０６が保持する第１認証符号を更新する。

【００２７】

なお、本実施形態は、カウンタ値を第２メモリ１０９に記録する場合に限るものではない。第１認証符号が同じとなる所定の回数が数えられればどのような形態であってもよい。例えば、第１認証符号で認証が成功した際にＮに「１」以外の値を加算してもよいし、認証符号が同じとなる所定の回数に達した際にＮを「１」とせず他の値にしてもよい（例えばＮ＝Ｎｍａｘとし、認証が成功した際にＮから「１」を減算するようにしてもよい）。

【００２８】

制御部１０７、演算部１０８、第２メモリ１０９、及び主装置３が消費する電力は電灯線や乾電池・蓄電池など省電力制御装置１の外部から得られるように構成されている。主制御部１５３は、電灯線や電池など外部の電源を入切するスイッチを含み、電源オフ状態（待機状態）のときに、第１信号判定部１０５から出力される起動信号を受けて、該スイッチがオンし（電源オン状態となり）動作する。一連の処理が終了すると該スイッチがオフし、電源オフ状態となる。

【００２９】

図３は、整流器１０２の構成例を示している。この整流器１０２は、ｎＭＯＳトランジスタＭＲ１、ＭＲ２の直列接続構成を有しており、それぞれゲートソース間が短絡接続（すなわちトランジスタＭＲ１、ＭＲ２は一種のダイオード接続）になっている。それらの中間のノードにコンデンサＣ１を介して、アンテナ１０１からＲＦ信号が入力される。また、トランジスタＭＲ１のドレインとトランジスタＭＲ２のソースとの間に出力電圧（整流電圧）を発生させるべく、それらと並列に平滑コンデンサＣ２が接続されている。

【００３０】

このような構成により、ＲＦ入力による半波の電流がトランジスタＭＲ１、コンデンサＣ２、トランジスタＭＲ２の経路で流れ、コンデンサＣ２の両端に直流電圧（整流電圧）が発生する。よって、図示の下側端子ＤＣ－はグランドに、図示の上側端子ＤＣ＋は整流器１０２の出力端子として起動回路１０３にそれぞれ接続される。

【００３１】

図４は、起動回路１０３の構成例を示したものである。起動回路１０３は、電流発生部および電流増幅部１１、電流電圧変換器１２、バッテリ電源１３を有する。電流発生部は

、ｎＭＯＳトランジスタＭ１が相当し、整流器１０２が出力する整流電圧が、グランド（基準電位または第２の基準電位）を基準に、トランジスタＭ１のドレインゲート共通接続側とソース側との間に印加されることにより、電流発生部１１に電流が生じる。電流増幅部は、ｎＭＯＳトランジスタＭ２、ｐＭＯＳトランジスタＭ３、Ｍ４が相当し、トランジスタＭ１と、これとカレントミラー回路ＣＭ１を構成するトランジスタＭ２とで１段目の電流増幅がなされ、トランジスタＭ３とトランジスタＭ４とで構成されるカレントミラー回路ＣＭ２により２段目の電流増幅がなされる。

【００３２】

電流発生部および電流増幅部１１の出力である増幅電流は、トランジスタＭ４のドレインから出力され電流電圧変換器１２に電流入力される。電流電圧変換器１２は、入力された電流の大きさに応じた電圧を発生する。電流入力から出力電圧への極性は、電源制御部２４以降の構成に依存して正極性、負極性いずれもあり得る。なお、電流電圧変換器１２においてグランド側が実線で示され、電源（第２の基準電位、または基準電位）側が破線で示されているのは、電源側の接続を必要としない場合もあり得るためである。バッテリ電源１３は、起動回路１０３の電源として機能する。また、バッテリ電源１３は、主制御部１５３（制御部107、演算部１０８、第２メモリ１０９）の電源として機能してもよい。

【００３３】

バッテリ電源１３からの電力消費は、起動回路１０３においては、整流器１０２からの整流電圧の入力がない状態では基本的にない。これは、整流電圧の発生のない状態ではトランジスタＭ１に電流が流れないので、カレントミラー回路ＣＭ１、ＣＭ２にも電流が流れず、さらに電流電圧変換器１２も例えばＣＭＯＳ回路などによれば状態が固定しており電流が流れないからである。

【００３４】

さらに、制御部１０７、演算部１０８及び第２メモリ１０９における電力消費も、電流電圧変換器１２と事情は同じである。これはやはり例えばＣＭＯＳ回路などにより構成することが可能だからである。

【００３５】

主装置３における電力消費は、例えば制御部１０７を介してオン状態にされていれば開始されるが、オフ状態では当然その電力消費はない。

【００３６】

本実施形態では、整流器１０２とグランドとの電位差Ｖ１を、カレントミラー回路ＣＭ１とグランドとの電位差Ｖ２と等しくしているので、これらがオフの状態においても電流が流れなくなり、待機状態における電力消費をより効果的に抑制することができる。

【００３７】

以上より、図１に示す、省電力制御装置１、および主装置３は、待機状態（電源オフ状態）では、基本的に電力消費がない。この点は省電力の意味で大きな利点である。アンテナ１０１で電波を受け、整流器１０２の出力に整流電流が発生したときのみ起動回路１０３で電力が消費される。その後、起動回路１０３からの出力信号により、電源制御部１０４が第1認証部１５１をオン状態にすると、省電力制御装置１での電力消費が発生するが、その状態においても、電波の到来が止むことで省電力制御装置１での電力消費はなくし得る。

【００３８】

なお、図４では、初段のカレントミラー回路ＣＭ１がｎＭＯＳトランジスタで構成されており入力電流が流し込まれることで動作する。したがって、これに接続する整流器１０２としては、図３に示すようにその上側端子（正側端子）が整流電圧の出力端子である。

【００３９】

図５は、起動回路１０３の他の構成例を示したものである。なお、図５において、図４と同一部分には同一符号を付し、図４と異なる部分についてのみ説明する。すなわち、図５では、電流得電圧変換器１２の出力に同期回路３２が接続されている。同期回路３２は

、例えば、電源制御部１０４が省電力制御装置１をオン状態にすると動作する。

【００４０】

同期回路３２は、電流電圧変換器１２の出力レベル変動周期に同期して所定周波数、所定タイミングのクロック信号を発生する。その内部に例えばＰＬＬを有する。例えば、電源制御部１０４によって同期回路３２が動作する状態にされると、続けて電流電圧変換器１２の出力は、無線操作信号のプリアンブル部分に応じてある周期で変動する。この周期に同期してクロック信号を生成する。同期回路３２で生成されたクロック信号に基づき、第１信号判定部１０５が動作するように構成されていてもよい。

【００４１】

図６は、第１信号判定部１０５の構成例を示したもので、ここでは、例えば、起動回路１０３が、図５に示すように、同期回路３２を含む場合の構成例を示している。

【００４２】

図６において、フリップフロップ３３、３４、３５は、シフトレジスタを構成している。そのシフト動作は同期回路３２からのクロック信号による。例えば、電源制御部１０４によってフリップフロップ３３、３４、３５が動作する状態にされると、プリアンブル部分に続く無線操作信号の第１認証符号部分により、電流電圧変換器１２の出力は、該認証符号に応じて出力レベル（ハイ／ロー）が変動する。この変動履歴をシフトレジスタであるフロップフロップ３３、３４、３５に記憶する。記憶された変動履歴は判定部３６に送られる。

【００４３】

第１メモリ１０６は、上述したように、第１認証符号をあらかじめ保持している。例えば、第１メモリ１０６が電源制御部１０４３１によって動作可能な状態にされると、その第1認証符号が読み出され判定部３６に送られる。

【００４４】

判定部３６は、フリップフロップ３３、３４、３５からの情報と、第１メモリ１０６からの情報とを比較し、一致する場合には、起動信号を制御部１０７に出力する。

【００４５】

なお、フリップフロップ３３、３４、３５（シフトレジスタ）の段数は、このような3段に限られず認証符号の情報量に応じてさらに多段にしてもよい。

【００４６】

図７は、省電力制御装置１が操作端末２を認証する際に使用する認証符号を示している。

【００４７】

Ｓ／Ｋｅｙ（登録商標）方式では認証が成功する度に認証符号を変更するが、本実施形態では、１つの認証符号は、予め定められた回数（Ｎｍａｘ）だけ認証が成功するまで使用される。例えば、図７では、認証が４回成功するごとに認証符号を変更する場合（つまりＮｍａｘ＝４）を示しており、Ｎｏ．１００からＮｏ．９７までは認証符号（Ｔ（２５））を、Ｎｏ．９６からＮｏ．９３までは認証符号（Ｔ（２４））を使用、以降も同様に４回成功するごとに認証符号を変更してゆく。なお、同じ認証符号で認証する回数（Ｎｍａｘ）は、高々想定される同期ずれ回数の最大値に設定すればよい。

【００４８】

該回数（Ｎｍａｘ）を決定する方法の例としては、設計段階において省電力制御装置１と操作端末２を典型的な使用環境に設置して同期ずれ回数がどの程度発生するかを計測する方法や、省電力制御装置１ならびに操作端末２に同期ずれ回数を計測する機能（以降キャリブレーション機能と表記）、装置の使用を開始する際や装置の設置場所を変更して使用環境が変化した際などに該キャリブレーション機能を使用して該所定の回数を設定する方法が挙げられるが、いかなる手法を採用するかは本発明の主張するところではない。但し、同じ認証符号で認証する回数（Ｎｍａｘ）を増やすと再送攻撃がなされる可能性が高まるため、できるだけ少ない回数を設定することが望ましい。

【００４９】

使用形態の一例として、操作端末２が主装置３のリモコンである場合は、リモコンの電源ボタンを押すたびに図７で示したような第１認証符号を送信し、省電力制御装置１は受信した第１認証符号により認証を行って認証が成功すれば主装置３の電源をオンすることになる。

【００５０】

操作端末２は、図７に示したような第１認証符号を省電力制御装置１へ送信し、省電力制御装置１は受信した第１認証符号により認証を行う。

【００５１】

操作端末２の構成は、本発明の要旨ではないので簡単に説明する。操作端末２は第１認証符号を生成するための演算部や秘密鍵情報を保持するメモリ、電池などの電源、操作ボタンやタッチパネルなど操作画面を具備するよう構成すればよい。また、演算部を具備せず、予め認証符号のリストや配列をメモリに保持するよう構成してもよい。

【００５２】

図８は、省電力制御装置１が無線信号を受信した際の処理動作を説明するためのフローチャートである。以下、図８を参照して、図２の省電力制御装置１の処理動作について説明する。

【００５３】

省電力制御装置１は、検知感度に達する電波（無線操作信号）が到来するまで電源オフ状態で待機している。操作端末２から送信された、検知感度に達する無線操作信号がアンテナ１０１で受信されると（ステップＳ１）、整流器１０２、起動回路１０３、電源制御部１０４の機能により、第１認証部１５１の電源がオンとなり動作状態となる。

【００５４】

起動回路１０３が、図５に示すような構成の場合、無線操作信号のプリアンブル部分に応じて、電流電圧変換器１２の出力電圧が変動するので、この変動周期に同期するようなクロック信号が同期回路３２から出力され、第１の信号判定部１０５に入力する。

【００５５】

次に、無線操作信号の（例えばプリアンブルに続く）認証符号部分に応じた信号が電流電圧変換器１２から出力され、この信号が第１の信号判定部１０５に入力する（ステップＳ２）。

【００５６】

第１信号判定部１０５は、入力された信号と第１メモリ１０６が保持している第１認証符号とを比較し（ステップＳ３）、一致している場合には（ステップＳ３のＹ）、起動信号を主制御部１５３に出力する。主制御部１５３（制御部１０７、演算部１０８、第２メモリ１０９）は、この起動信号を受けて、電源オン状態となる。また、制御部１０７は、この起動信号を受けて主装置３へ操作信号を出力する（ステップＳ５）。

【００５７】

次に、制御部１０７は、起動回路１０３から第１信号判定部１０５に入力された信号を基に、第１メモリ１０６が保持している情報を更新する必要があるか否かを判断する。制御部１０７は、以下の２つの条件（条件ａ１）（条件ａ２）のうちの少なくとも１つを満足する場合、第１メモリ１０６を更新する必要があると決定する（ステップＳ６）。

【００５８】

（条件ａ１）第２メモリ１０９が保持しているカウンタ値ＮとＮｍａｘ（この例では「４」）とが一致する。

【００５９】

（条件ａ２）第１信号判定部１０５に入力された信号が第１メモリ１０６が保持している複数の（ここでは２つの）第１認証符号のうち２番目の認証符合と一致する。

【００６０】

更新すると決定した場合（ステップＳ６のＹ）、第２メモリ１０６内のカウンタ値Ｎを「１」に更新し（ステップＳ７）、演算部１０８が新たな第１認証符号を計算し（ステップＳ８）、これを第１メモリ１０６が記憶する（ステップＳ９）。例えば、第１メモリ１

０６が保持している複数の（ここでは２つの）の第１認証符号のうち１番目の認証符合を削除して、新たな第１認証符号を第１メモリ１０６に記憶する。なお、第１メモリ１０６に3つ以上の第１認証符号を記憶している場合、上記（条件ａ２）を満たすときには、一致した認証符号よりも前の符号は全て削除してもよい。

【００６１】

一方、ステップＳ６において、上記２つの条件のいずれも満たさない場合には、ステップＳ１１へ進み、第２メモリ１０９内のカウンタ値を１つインクリメントし、「Ｎ＋１」に更新する（ステップＳ１１）。

【００６２】

制御部１０７は、例えばタイマを含み、起動信号を受信してからの経過時間を計測し、起動信号を受信してから予め定められた時間経過すると、自動的に主制御部１５３（制御部１０７、演算部１０９、第２メモリ１０９）の電源をオフするようにしてもよい。

【００６３】

また、電源制御部１０４も、例えばタイマを含み、第１認証部１５１の電源をオンにしてからの経過時間を計測し、第１認証部１５１の電源をオンしてから予め定められた時間経過すると、第１の認証部１５１の電源をオフするようにしてもよい。

【００６４】

次に、同期ずれが発生しなかった場合と発生した場合の認証の様子を、図９および図１０を参照して説明する。図９は、同期ずれが発生しなかった場合の省電力制御装置１と操作端末２との間の通信シーケンスを示している。この例では、操作端末２が図７に示した認証符号を順に省電力制御装置１に無線送信する。

【００６５】

第２メモリ１０９内のカウンタ値Ｎが「１」、省電力制御装置１の第１メモリ１０６に、第一認証符号としてＴ（２５）およびＴ（２４）が保持されているとする。

【００６６】

省電力制御装置１は、受信した無線信号に重畳された第１認証符号と、第１メモリ１０６が保持している２つの第１認証符号とを比較する（図８のステップＳ１～３）。

【００６７】

図９では、Ｎｏ．９７まで（図９（１）～（４））は第１認証符号としてＴ（２５）が操作端末２から送信されるため、第１メモリ１０６が保持している１番目の第１認証符号Ｔ（２５）と一致する（ステップＳ３）。図９（１）～（３）では、図８のステップＳ１～ステップＳ６、ステップＳ１１を行う。

【００６８】

図９（４）では、Ｎｏ．９７での認証が成功したとき、Ｎ＝Ｎｍａｘ＝４であるため（図８のステップＳ６）、第１メモリ１０６を更新する（ステップＳ７～ステップＳ９）。更新後の第１メモリが保持している第一認証符号は、Ｔ（２５）が削除され、Ｔ（２４）およびＴ（２３）となる。Ｎｏ．９６以降も同様に繰り返すことで認証が実施される。

【００６９】

図１０は、同期ずれが発生した場合の省電力制御装置１と操作端末２との間の通信シーケンスを示している。図９と同様、操作端末２が図７に示した認証符号を順に省電力制御装置１に無線送信する。

【００７０】

第２メモリ１０９内のカウンタ値Ｎが「１」のときに、省電力制御装置１の第１メモリ１０６には、第一認証符号としてＴ（２５）およびＴ（２４）が保持されている。

【００７１】

省電力制御装置１は、受信した無線操作信号に重畳されている第１認証符号と、第１メモリ１０６が保持している第１認証符号とを比較する（図８のステップＳ１～３）。

【００７２】

図１０（１）のＮｏ．１００では、操作端末２から第１認証符号としてＴ（２５）が送信されるため、第１メモリ１０６が保持している１番目の第１認証符号Ｔ（２５）と一致

する（ステップＳ３）。従って、図８のステップＳ４～ステップＳ６、ステップＳ１１へ進む。

【００７３】

その後、図１０（２）～（４）に示すように、操作端末２が発信したＮｏ．９９、Ｎｏ．９８、Ｎｏ．９７の無線操作信号が省電力制御装置１に到達せず、同期ずれが発生した後、図１０（５）に示すように、Ｎｏ．９６の無線操作信号が省電力制御装置１に到達したとする（ステップＳ１、ステップＳ２）。省電力制御装置１は、第１信号判定部１０５に入力された信号が第１メモリ１０６に記憶されている２番目の第１認証符号Ｔ（２４）と一致するため（ステップＳ３）、ステップＳ４、ステップＳ５、さらに、ステップＳ６へ進む。ステップＳ６では、第２メモリ１０９のカウンタ値ＮがＮｍａｘ（この例では「４」）に達していないが、第１信号判定部１０５に入力された信号が２番目の認証符号Ｔ（２４）と一致するため、ステップＳ７～ステップＳ９を実行し、第１メモリ１０６を更新する。この結果、第１メモリ１０６内の第１認証符号はＴ（２４）及びＴ（２３）に更新される。

【００７４】

図１０に示したように、同期ずれが発生した場合も、同期ずれがＮｍａｘ－１回以内であれば認証を継続することが可能となる。

【００７５】

なお、図９のフローチャートでは、ステップＳ９の新たな第１認証符号の生成（計算）を認証が成功した際に実施しているが、予め図７で示したような第１認証符号のリストや配列を第２メモリ１０９などの記憶装置に記憶しておき、その値で第１メモリ１０６を更新するよう構成してもよい。

【００７６】

従来の手法では、同期ずれ回数がＮｍａｘ－１となる場合、第１認証符号としては少なくともＮｍａｘ個の符合を保持する必要があったが、本実施形態では第１認証符号としては高々２つの認証符合を保持すればよいため、第１メモリ１０６が記憶する認証符号の候補数を減らすことが可能となる。

【００７７】

以上説明したように、上記第１の実施形態によれば、連続する複数の認証で同じ認証符号を用いることで、第１メモリ１０６が記憶する認証符号の数を少なく抑えることができ、その結果、回路規模や消費電力を最小限に抑えることができる。また、第１メモリ１０６に記憶する認証符号の数を少なくしても、同期がずれた際も認証を継続することが可能となる。

【００７８】

また、アンテナ１０１で受信された無線操作信号を整流して整流電圧を発生する整流器１０２と、整流電圧の供給を受けて電流を発生して、該電流を増幅し、増幅された電流の大きさに応じた電圧信号を出力する起動回路１０３とを用いることで、ほぼ「０」の待機電力で無線操作信号を受信できる。整流器１０２及び起動回路１０３を用いることにより、さらなる省電力化を図ることができる。

【００７９】

（第２の実施形態）

図１１は、第２の実施形態に係る省電力制御装置１の構成例を示したものである。なお、図１１において、図２と同一部分には同一符号を付し、異なる部分について説明する。すなわち、図１１では、第２の認証部１５２が追加され、主制御部１５３からは第２メモリ１０９が削除されている。第２認証部１５２は、第２信号判定部１２１と第２メモリ１２２を含む。

【００８０】

第１信号判定部１０５は、第１の実施形態と同様、例えば、操作端末２からの無線操作信号中の第１認証符号に相当する信号と第１メモリ１０６に記憶されている複数の第１認証符号とを比較する。無線操作信号中の第１認証符号が第１メモリ１０６に記憶されてい

る複数の第１認証符号のうちの１つと一致する場合（すなわち、無線操作信号中の第１認証符号が有効な認証符号である場合）には、第１信号判定部１０５は、第２認証部１５２及び主制御部１５３を起動するための起動信号を第２認証部１５２及び主制御部１５３に出力する。起動信号として用いる符号は任意である。

【００８１】

第２認証部１５２が消費する電力は、電灯線や乾電池・蓄電池など省電力制御装置１の外部から得られるように構成されている。第２認証部１５２は、電灯線や電池など外部の電源を入切するスイッチを含み、電源オフ状態（待機状態）のときに、第１信号判定部１０５から出力される起動信号を受けて、該スイッチがオンし（電源オン状態となり）動作する。一連の処理が終了すると該スイッチがオフし、電源オフ状態となる。

【００８２】

第２信号判定部１２１には、整流器１０２、起動回路１０３、及び第１信号判定部１０５を経由して入力される、操作端末２からの無線操作信号中の第1認証符号に続く第２認証符号に相当する信号が入力され、この信号と、第２メモリ１２２に記憶されている複数の第２認証符号とを比較する。無線操作信号中の第２の認証符号と第２メモリ１２２内の複数の第２認証符号のうちの１つとが一致する場合（すなわち、無線操作信号中の第２認証符号が有効である場合）には、その旨を制御部１０７へ通知する。

【００８３】

第２信号判定部１２１は、例えば、図６に示した第１信号判定部１０５と同様の構成であってもよい。この場合、起動回路１０３は、図５に示すような構成を有し、同期回路３２で精製されたクロック信号が第２信号精製部１２１にも入力される。

【００８４】

第２メモリ１２２は、演算部１０８が認証符号を生成するのに必要な秘密鍵情報、乱数、第１認証符号の認証回数を最大Ｎｍａｘまで計数するカウンタ、並びに第２認証符号を記憶するための記憶装置であり、電源が供給されなくても情報を保持することが可能な記憶装置で構成される。

【００８５】

第２メモリ１２２は、同期ずれが発生した際に次の認証符号での認証を可能とするため、第２認証符号となる複数の符号を保持する。保持する符号の数は同期ずれの最大数＋１とすればよい。例えば、３回までの同期ずれを許容するのであれば、保持する符号の数は「４」となる。

【００８６】

制御部１０７は、例えば第１信号判定部１０５から出力される起動信号を受けた際に起動され、第２信号判定部１２１から第２認証符号による認証が成功した旨が通知された場合、主装置３に対し操作信号を出力する。また、第１メモリ１０６に記憶する第１認証符号及び第２メモリ１２２に記憶する第２認証符号を計算するよう演算部１０８に対して指示する。

【００８７】

演算部１０８は、第２メモリ１２２が記憶する秘密鍵情報と乱数を基に、第１認証符号、第２認証符号を生成し、生成された第１認証符号及び第２認証符号は、第１メモリ１０６及び第２メモリ１２２にそれぞれ記憶される。

【００８８】

第１メモリ１０６に記憶される第１認証符号については、第１の実施形態と同様であり、説明を省略する。第２メモリ１２２に記憶される第２認証符号についても第１の実施形態と同様に、暗号アルゴリズムまたは一方向性ハッシュアルゴリズムによって認証符号を生成すればよいが、第２認証部１５２は第１認証部１５１よりも多くの電力を用いて複雑な処理が可能であるため、第１認証部１５１で実施した認証よりも高度な認証を行うことができる特徴がある。高度な認証とは、例えば、秘密鍵や乱数、認証符号を第１認証部１５１で実施した場合よりも長くした認証や、より高度な計算アルゴリズムを使用した認証が挙げられる。ただし、どの程度高度な認証を実施するかはどの程度の安全性を求めるか

に依存し、その手法は設計事項である。

【００８９】

制御部１０７、演算部１０８、及び主装置３が消費する電力も、電灯線や乾電池・蓄電池など省電力制御装置１の外部から得られるように構成されている。主制御部１５３（制御部１０７及び演算部１０８）は、電灯線や電池など外部の電源を入切するスイッチを含み、電源オフ状態（待機状態）のときに、第１信号判定部１０５から出力される起動信号を受けて、該スイッチがオンし（電源オン状態となり）動作する。一連の処理が終了すると該スイッチがオフし、電源オフ状態となる。

【００９０】

図１２は、省電力制御装置１が操作端末２を認証する際に使用する認証符号を示している。第１認証符号は第１の実施形態で述べたものと同一である。第２の実施形態ではさらに第２認証符号を使用する。第２認証符号は認証が成功する度に符号が変わるため、Ｓ／Ｋｅｙ方式などのワンタイムパスワード方式で実施されているものと同様である。操作端末２は第１認証符号と第２認証符号を含む無線操作信号を省電力制御装置１へ送信し、省電力制御装置１は受信した無線操作信号中の第１認証符号と第２認証符号により認証を行う。

【００９１】

制御部１０７は、第１の実施形態と同様に、第１認証符号で認証が成功したら、第２メモリ１２２内の第１認証符号のカウンタの値Ｎに「１」を加算し、該カウンタ値Ｎが、予め定められた回数Ｎｍａｘに達したら、該カウンタの値を「１」に戻し、第１メモリ１０６が保持する第１認証符号を更新する。

【００９２】

また、制御部１０７は、第２認証符号で認証が成功したら、第２メモリ１２２が保持する第２認証符号を更新する。

【００９３】

図１３は、省電力制御装置１が無線信号を受信した際の処理動作を説明するためのフローチャートである。以下、図１３を参照して、図１１の省電力制御装置１の処理動作について説明する。

【００９４】

省電力制御装置１は、検知感度に達する電波（無線操作信号）が到来するまで電源オフ状態で待機している。操作端末２から送信された、検知感度に達する無線操作信号がアンテナ１０１で受信されると（ステップＳ１０１）、整流器１０２、起動回路１０３、電源制御部１０４の機能により、第１認証部１５１の電源がオンとなり動作状態となる。このとき、第１の認証符号及び第２の認証符号を含む無線操作信号、あるいは、第１の認証符号を含む無線操作信号及び第２の認証符号を含む無線操作信号を受信する。

【００９５】

起動回路１０３が、図５に示すような構成の場合、無線操作信号のプリアンブル部分に応じて、電流電圧変換器１２の出力電圧が変動するので、この変動周期に同期するようなクロック信号が同期回路３２から出力され、第１の信号判定部１０５、第２の信号判定部１２に入力する。

【００９６】

次に、無線操作信号中の（例えばプリアンブルに続く）第１認証符号部分に相当する信号が電流電圧変換器１２から出力され、この信号が第１信号判定部１０５に入力する（ステップＳ１０２）。

【００９７】

第１信号判定部１０５は、入力された信号（無線操作信号中の第１認証符号）と第１メモリ１０６が保持している複数の第１認証符号とを比較し（ステップＳ１０３）、無線操作信号中の第１認証符号が第１メモリ１０６内の複数の第１認証符号のうちの１つと一致している場合（すなわち、無線操作信号中の第１認証符号が有効である場合）には（ステップＳ１０３のＹ）、起動信号を第２認証部１５２及び主制御部１５３に出力する。第２

の認証部１５２は、この起動信号を受けて、電源オン状態となる（ステップＳ１０４）。また、制御部１０７及び演算部１０８は、この起動信号を受けて電源オン状態となる。

【００９８】

次に、無線操作信号中の第１の認証符号に続く第２の認証符号部分に相当する信号、あるいは、次の無線操作信号中の第２の認証符号部分に相当する信号が電流電圧変換器１２から出力され、この信号が、第１の信号判定部１０５を介して第２の信号判定部１２１に入力する。

【００９９】

第２信号判定部１２１は、入力された信号（無線操作信号中の第２認証符号）と第２メモリ１２２が保持している複数の第２認証符号とを比較し（ステップＳ１０５）、無線操作信号中の第２認証符号が第２メモリ１２２内の複数の第２認証符号のうちの１つと一致している場合（すなわち、無線操作信号中の第２認証符号が有効である場合）には（ステップＳ１０５のＹ）、その旨を制御部１０７に通知する。制御部１０７は、この通知を受けて主装置３へ操作信号を出力する（ステップＳ１０６）。

【０１００】

次に、制御部１０７は、第２メモリ１２２に記憶されている第２認証符号を更新するために、演算部１０８に新たな第２認証符号の計算を指示する。演算部１０８は、この指示を受けて、新たな第２認証符号を計算し（ステップＳ１０７）、これを第２メモリ１２２が記憶する（ステップＳ１０８）。

【０１０１】

次に、制御部１０７は、第２信号判定部１２１から入力された信号を基に、第１メモリ１０６が保持している情報を更新する必要があるか否かを判断する。制御部１０７は、以下の２つの条件（条件ｂ１）（条件ｂ２）のうちの少なくとも１つを満足する場合、第１メモリ１０６を更新する必要があると決定する（ステップＳ１０９）。

【０１０２】

（条件ｂ１）第２メモリ１０９が保持しているカウンタ値ＮとＮｍａｘ（この例では「４」）とが一致する。

【０１０３】

（条件ｂ２）第１信号判定部１０５に入力された信号が第１メモリ１０６が保持している複数の（ここでは２つの）の第１認証符号のうち２番目以降の認証符合と一致する。

【０１０４】

更新すると決定した場合（ステップＳ１０９のＹ）、第２メモリ１２２内のカウンタ値Ｎを「１」に戻し（ステップＳ１１０）、演算部１０８が新たな第１認証符号を計算し（ステップＳ１１１）、第１メモリ１０６から１番目の第１認証符号を削除して、新たな第２認証符号を記憶する（ステップＳ１１２）。なお、第１メモリ１０６に３つ以上の第１認証符号を記憶している場合、上記（条件ｂ２）を満たすときには、一致した認証符号よりも前の符号は全て削除してもよい。

【０１０５】

一方、ステップＳ１０９において、上記２つの条件のいずれも満たさない場合には、ステップＳ１１３へ進み、第２メモリ１２２内のカウンタ値を１つインクリメントし、「Ｎ＋１」に更新する（ステップＳ１１３）。

【０１０６】

制御部１０７は、第１認証符号による認証が成功した後のステップＳ１０５において、第２信号判定部１２１の入力信号が第２メモリ１２２に記憶されている認証符号のいずれかと一致した場合（第２認証符号による認証が成功した場合）には、上記（条件ｂ１）（条件ｂ２）によらず、第２メモリ７０８に記憶されている第２認証符号を更新するため、演算部１０８に第２認証符号の計算を指示するが、ステップＳ１０５において第２認証符号により認証が失敗（ＮＧ）の場合には、第２メモリ１２２内の第２認証符号の更新は行わない。

【０１０７】

なお、図１３のフローチャートでは、ステップＳ１１１の第１認証符号の計算やステップＳ１０７の第２認証符号の計算を、第１認証符号や第２の認証符号を用いた認証後に実施しているが、予め図１２に示したような第１認証符号や第２認証符号のリストや配列を第２メモリ１２２などの記憶装置に保持しておき、該記憶装置が値を読み出して第１メモリ１０６や第２メモリ１２２を更新するよう構成してもよい。

【０１０８】

また、制御部１０７は、例えばタイマを含み、起動信号を受信してからの経過時間を計測し、起動信号を受信してから予め定められた時間経過すると、自動的に主制御部１５３の電源をオフするようにしてもよい。

【０１０９】

第２認証部１５２は、例えばタイマを含み、第１認証部１５１からの起動信号を受信してからの経過時間を計測し、起動信号を受信してから予め定められた時間経過すると、自動的に第２認証部１５２の電源をオフするようにしてもよい。

【０１１０】

また、電源制御部１０４も、例えばタイマを含み、第１認証部１５１の電源をオンにしてからの経過時間を計測し、第１認証部１５１の電源をオンしてから予め定められた時間経過すると、第１の認証部１５１の電源をオフするようにしてもよい。

【０１１１】

なお、第２認証符号を計算するステップ（Ｓ１０７）および第２メモリを更新するステップ（Ｓ１０８）は、Ｓ１０５にてＹと判定された後に実行されればよいため、必ずしも図１３の通りでなくてもよい。例えば、Ｓ１１２やＳ１１３の後にＳ１０７およびＳ１０８を実行してもよい。

【０１１２】

次に、同期ずれが発生した場合の認証の様子を、図１４を参照して説明する。図１４は、同期ずれが発生した場合の省電力制御装置１と操作端末２との間の通信シーケンスを示している。この例では、操作端末２が図１２に示した認証符号を順に省電力制御装置１に無線送信する。省電力制御装置１の第１メモリ１０６は、第１認証符号としてＴ（２５）およびＴ（２４）を保持し、第２メモリ１２２は、第２認証符号としてＨ（１００）、Ｈ（９９）、Ｈ（９８）、Ｈ（９７）を保持している。

【０１１３】

このとき、省電力制御装置１は、受信した無線操作信号に重畳された認証符号と、第１メモリ１０６が保持している第１認証符号とを比較する（図１３のステップＳ１０１～ステップＳ１０３）。

【０１１４】

図１４（１）のＮｏ．１００では、操作端末２から第１認証符号としてＴ（２５）、第２認証符号としてＨ（１００）が送信される。この無線操作信号中の第１認証符号と第１メモリ１０６が保持している１番目のＴ（２５）と一致するので（ステップＳ１０３）、第２認証部１５２を起動する（ステップＳ１０４）。第２認証部１５２の第２信号判定部１２１は、該無線操作信号に重畳された第２認証符号Ｈ（１００）に一致する認証符号が第２メモリ１２２に保持されているので、演算部１０８は新たな第２認証符号Ｈ（９６）を計算し（ステップＳ１０７）、これを第２メモリ１２２に記憶する（ステップＳ１０８）。この時点で第２メモリ１２２は第２認証符号としてＨ（９９）、Ｈ（９８）、Ｈ（９７）、Ｈ（９６）を保持する。また、第２メモリ１２２内のカウンタ値は「２」となる（ステップＳ１１３）。

【０１１５】

その後、図１４（２）～（４）に示すように、操作端末２が発信したＮｏ．９９、Ｎｏ．９８、Ｎｏ．９７の無線信号が省電力制御装置１に到達せず、同期ずれが発生した後、図１４（５）に示すように、Ｎｏ．９６の無線操作信号が省電力装置１に到達したとする。省電力制御装置１は、受信した無線操作信号中の第１認証符号と、第１メモリ１０６が保持している２番目の第１認証符号であるＴ（２４）とが一致するため（ステップＳ１０

１～ステップＳステップＳ１０３）、第２認証部１５２を起動する（ステップＳ１０４）。

【０１１６】

第２信号判定部１２１は、該無線操作信号中の第２認証符号と、第２メモリ１２２が保持している４番目の第２認証符号であるＨ（９６）とが一致するため、認証成功となり、主装置３へ操作信号を出力する（ステップＳ１０５、ステップＳ１０６）。

【０１１７】

このように、第２の実施形態によれば、第１の実施形態と同様に、同期ずれが発生した場合も、同期ずれがＮｍａｘ－１回以内であれば認証を継続することが可能となる。

【０１１８】

次に、図１５を参照して、第三者（攻撃者）によって再送攻撃が実施された場合の例を説明する。

【０１１９】

図１５では、Ｎｏ．１００～Ｎｏ．９８の３回の認証が成功したあと、Ｎｏ．９８の無線操作信号を受信した攻撃者から、Ｎｏ．９８の無線操作信号を繰り返し送信される再送攻撃を受けた例を示している。従って、図１５（１）のＮｏ．９８の無線操作信号中の第１認証符号（Ｔ（２５））及び第２認証符号（Ｈ（９８））の認証が成功した後、第１メモリ１０６には、第１認証符号としてＴ（２５）とＴ（２４）が記憶され、第２メモリ１２２には、第２認証符号としてＨ（９８）が削除されて、Ｈ（９７）、Ｈ（９６）、Ｈ（９５）、Ｈ（９４）が記憶されている。また、第２メモリ122内のカウンタ値は「４」となる。

【０１２０】

図１５（２）の１回目の再送攻撃を受ける時点では、第２メモリ１２２内のカウンタ値が「４」であり、第１認証符号Ｔ（２５）が第１メモリ１０６にまだ記憶されているため、１回目の再送攻撃の際、第１認証は成功する（ステップＳ１０１～ステップＳ１０４）。ただし、第２認証ではＨ（９８）は第２メモリ１２２に記憶されていないため（Ｈ（９７）以降の認証符号しか保持されていないため）、第２認証は成功しない（ステップＳ１０５のＮ）。従って、ステップＳ１０９へ進む。ステップＳ１０９において、カウンタ値は「４」であることからステップＳ１１０へ進み、第２メモリ１２２内のカウンタ値が「１」にもどる。また、ステップＳ１１１～ステップＳ１１２の処理により、第１メモリ１０６には、第１認証符号としてＴ（２４）とＴ（２３）が記憶される。なお、この場合、主装置３に操作信号が送出されることもない。

【０１２１】

図１５（３）～（６）の２回目以降の再送攻撃では、第１信号判定部１０５の入力信号Ｔ（２５）は、第１メモリ１０６に第１認証符号として記憶されていないため、無効である。従って、第１認証符号による認証も成功しないから、主装置３に操作信号が送出されることがない。

【０１２２】

その後、図１５（７）に示すように、操作端末２からＮｏ．９７の無線操作信号を受信した際、Ｎｏ．９７の第１認証符号はまだＴ（２５）であり、省電力制御装置１ではＴ（２５）がすでに無効であるため（第１メモリ１０６には記憶されていないため）、認証が成功しない（ステップＳ１０３のＮ）。従って、主装置３には操作信号も送出されることはない。そして、次に、操作端末２から送信された図１５（８）のＮｏ．９６の無線操作信号を受信した際、Ｎｏ．９６の第１認証符号はＴ（２４）、第２認証符号はＨ（９６）であるので、第１認証と第２認証が共に成功し（ステップＳ１０３のＹ、ステップＳ１０５のＹ）、第２メモリ１２２内の認証符号の更新（ステップＳ１０７、ステップＳ１０８）、第２メモリ１２２内のカウンタ値を更新した後（ステップＳ１１３）、主装置３に操作信号を出力する。

【０１２３】

なお、再送攻撃を受けた際は、上述したように、第１認証が成功または失敗し、第２認

証が必ず失敗する。従って、図１５（２）において、制御部１０７は、第１認証が成功し、第２認証が失敗した場合に、再送攻撃を受けていると判定することが可能である。

【０１２４】

この場合にはカウンタ値ＮがＮｍａｘに達していなくても攻撃を受けている該第１認証符号（例えば、図１５において、攻撃対象の第１認証符号Ｔ（２５））を無効にする（すなわち第１メモリ１０６から該第１認証符号Ｔ（２５）を削除して、新たな第１認証符号Ｔ（２３）を第１メモリ１０６に記憶する）ように構成してもよい。例えば、図１３のステップＳ１０９の条件に、

（条件ｂ２）第１認証が成功し、且つ第２認証が失敗

という条件を追加し、（条件ｂ１）から（条件ｂ３）の３つの条件うちの少なくとも１つを満足する場合、ステップＳ１１０へ進み、第１メモリ１０６の更新を行う。

【０１２５】

第１の実施形態では再送攻撃がなされた場合、第２メモリ１０９のカウンタ値ＮがＮｍａｘに達するまでは攻撃が成功してしまった（主装置３に操作信号が出力される）が、上述の第２の実施形態では再送攻撃が成功することがないため、第１の実施形態よりも安全性を高めることが可能となる。また、再送攻撃を受けた場合にも第２認証部１５２は高々Ｎｍａｘ－１回（第１認証が成功し第２認証が失敗した場合に再送攻撃を受けたと判定するよう構成した場合は高々１回）しか起動しないため、再送攻撃を受けた際の消費電力の増大も一定範囲に抑えることが可能となる。

【０１２６】

以上説明したように、上記第２の実施形態によれば、連続する複数の認証で同じ認証符号を用いることで、第１メモリ１０６が記憶する第１認証符号の数を少なく抑えることができる。第２認証符号を用いた認証を行う第２認証部１５２と、主制御部１５３は、第１認証符号を用いた認証を行う第１認証部１５１での認証が成功したときに、電源オンとなり起動するため、回路規模や消費電力を最小限に抑えることができる。また、第１メモリ１０６に記憶する認証符号の数を少なくしても、同期がずれた際も認証を継続することが可能となり、第２認証符号を用いた認証を行う第２認証部１５２を追加することで、再送攻撃を防止することが可能となり、セキュリティ上の脅威を抑制できる。

【０１２７】

さらに、アンテナ１０１で受信された無線操作信号を整流して整流電圧を発生する整流器１０２と、整流電圧の供給を受けて電流を発生して、該電流を増幅し、増幅された電流の大きさに応じた電圧信号を出力する起動回路１０３とを用いることで、ほぼ「０」の待機電力で無線操作信号を受信できる。整流器１０２及び起動回路１０３を用いることにより、さらなる省電力化を図ることができる。

【図面の簡単な説明】

【０１２８】

【図１】省電力制御装置、操作端末及び主装置を含むシステム全体の概略構成例を示した図。

【図２】第１の実施形態に係る省電力制御装置の構成例を示した図。

【図３】整流器の構成例を示した図。

【図４】起動回路の構成例を示した図。

【図５】起動回路の他の構成例を示した図。

【図６】第１信号判定部の構成例を示した図。

【図７】省電力制御装置が操作端末を認証する際に用いる認証符号を示した図。

【図８】図２の省電力制御装置の処理動作を説明するためのフローチャート。

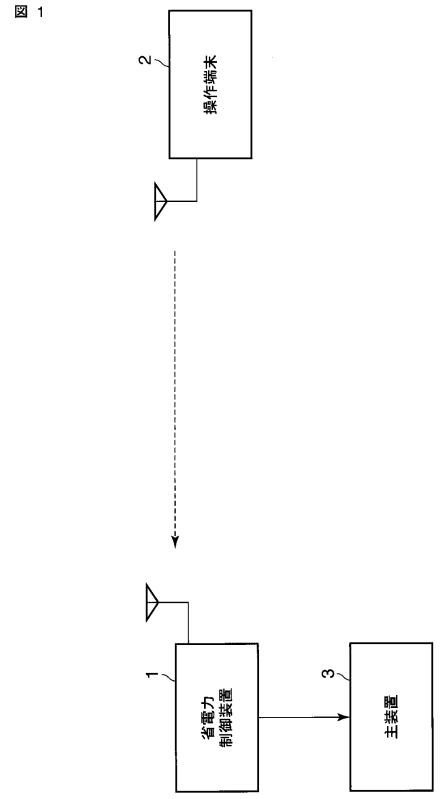
【図９】同期ずれが発生しなかった場合の省電力制御装置と操作端末との間の通信シーケンスを示した図。

【図１０】同期ずれが発生した場合の省電力制御装置と操作端末との間の通信シーケンスを示した図。

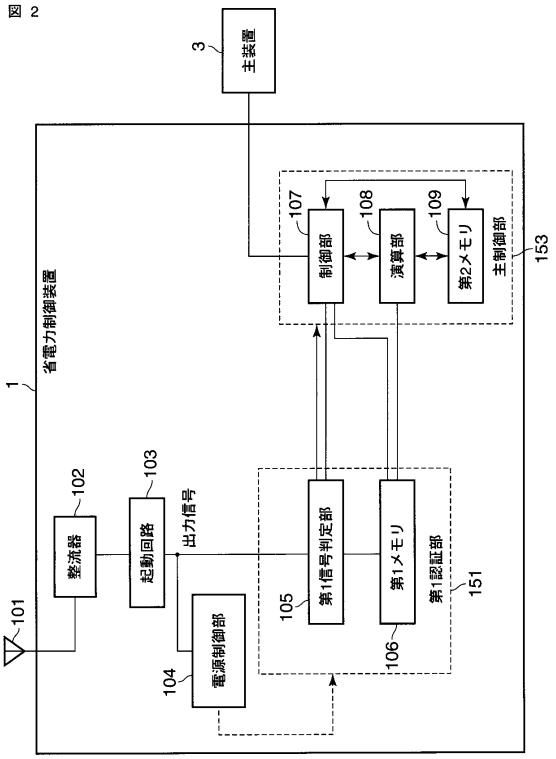
【図１１】第２の実施形態に係る省電力制御装置の構成例を示した図。

【図１２】省電力制御装置が操作端末を認証する際に用いる認証符号を示した図。
【図１３】図１１の省電力制御装置の処理動作を説明するためのフローチャート。
【図１４】同期ずれが発生した場合の省電力制御装置と操作端末との間の通信シーケンスを示した図。
【図１５】第三者（攻撃者）によって再送攻撃が実施された場合の省電力制御装置と操作端末との間の通信シーケンスを示した図。
【符号の説明】
【０１２９】
１…省電力制御装置
２…操作端末
３…主装置
１０１…アンテナ
１０２…整流器
１０３…起動回路
１０４…電源制御部
１０５…第１信号判定部
１０６…第１メモリ
１０７…制御部
１０８…演算部
１０９…第２メモリ
１２１…第２信号判定部
１２２…第２メモリ
１５１…第１認証部
１５２…第２認証部
１５３…主制御部

【図１】

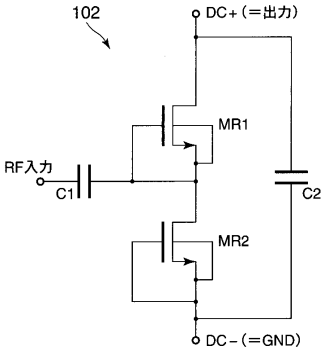


【図２】



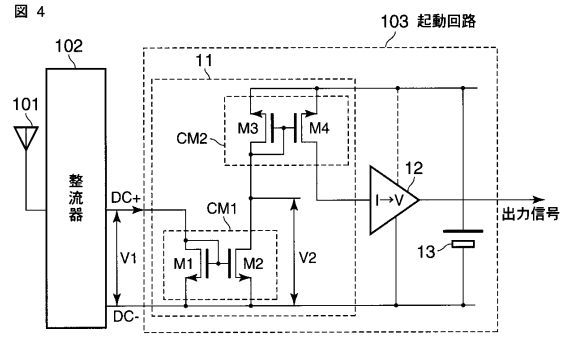
【図３】

図 3



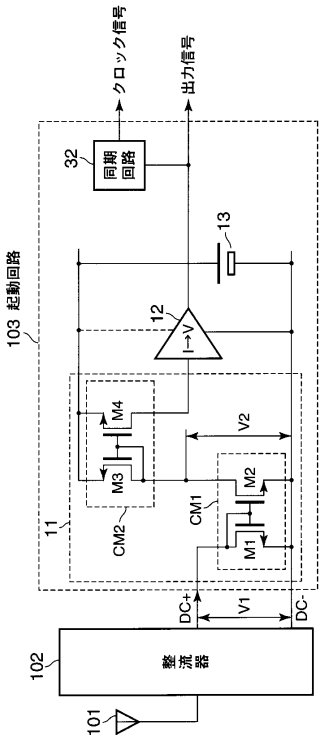
【図４】

図 4



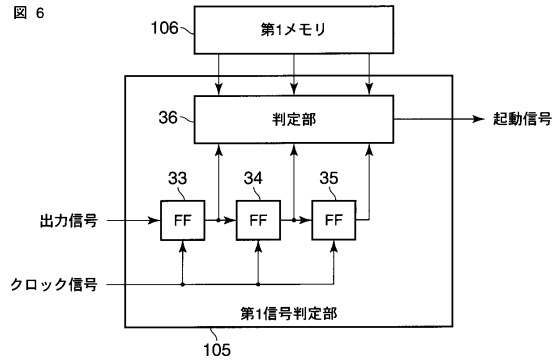
【図５】

図 5



【図６】

図 6



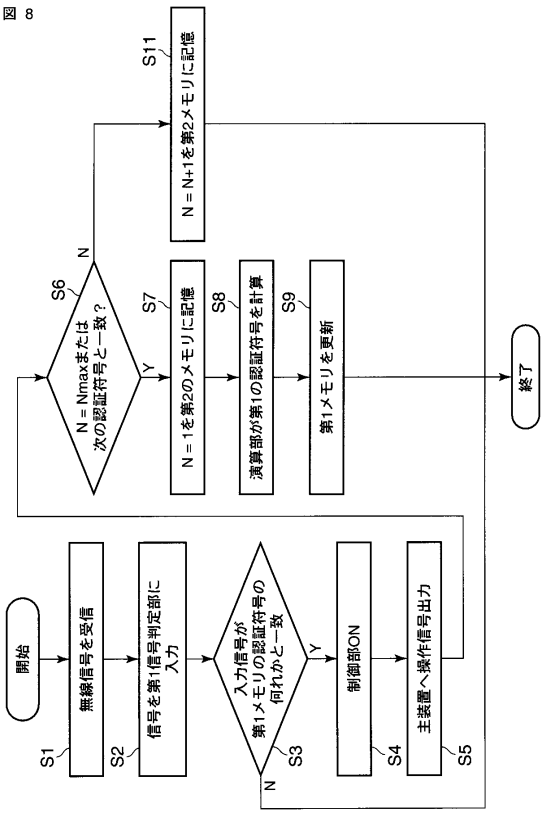
【図７】

図 7

認証No.	第1認証符号	
100	T(25)	Nmax = 4
99	T(25)	
98	T(25)	
97	T(25)	
96	T(24)	
95	T(24)	
・・・	・・・	
4	T(1)	Nmax = 4
3	T(1)	
2	T(1)	
1	T(1)	

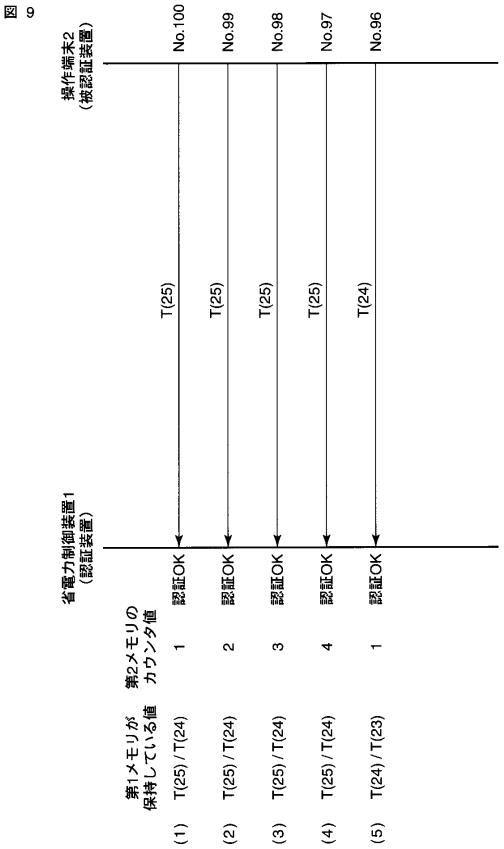
【図８】

図 8



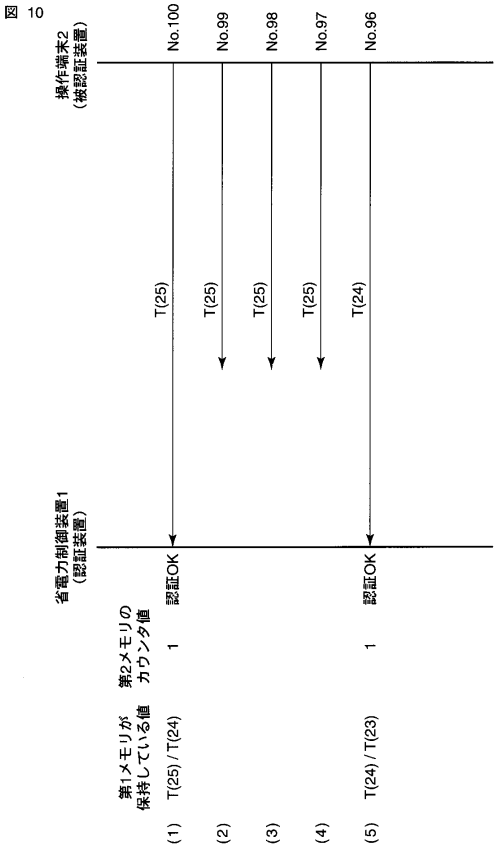
【図９】

図 9



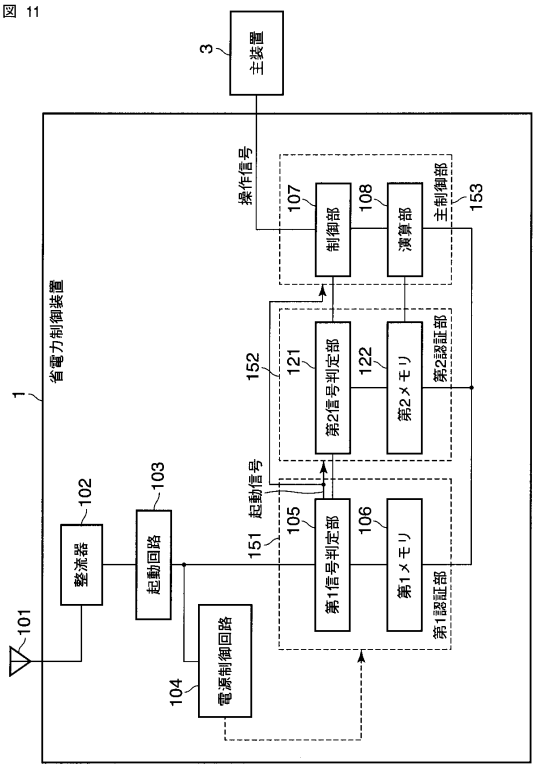
【図１０】

図 10



【図１１】

図 11



【図１２】

図 12

認証No.	第1認証符号	第2認証符号	
100	T(25)	H(100)	Nmax = 4
99	T(25)	H(99)	
98	T(25)	H(98)	
97	T(25)	H(97)	
96	T(24)	H(96)	
95	T(24)	H(95)	
・ ・ ・	・ ・ ・	・ ・ ・	
4	T(1)	H(4)	Nmax = 4
3	T(1)	H(3)	
2	T(1)	H(2)	
1	T(1)	H(1)	

【図１３】

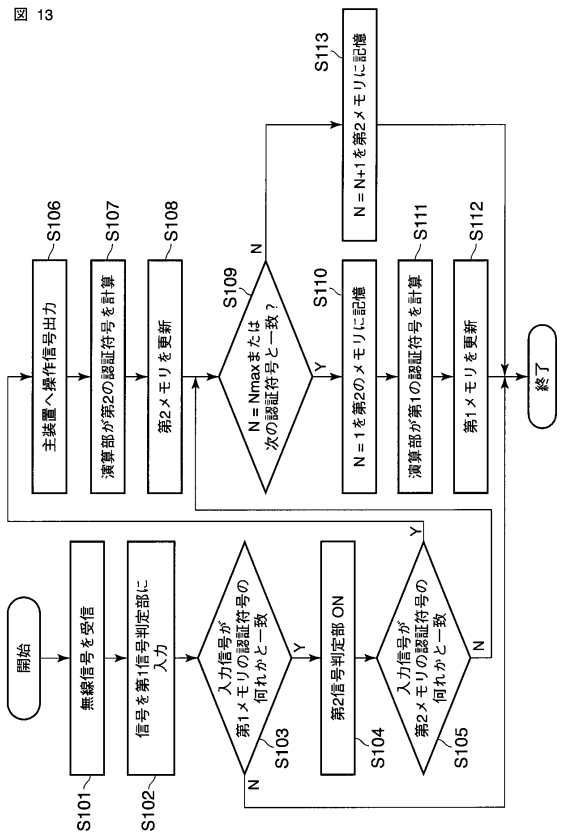


図 13
開始
S101
無線信号を受信
S102
信号を第1信号判定部に入力
S103
入力信号が第1メモリの認証符号の何れかと一致
N
Y
S104
第2信号判定部 ON
S105
入力信号が第2メモリの認証符号の何れかと一致
N
Y
S106
主装置へ操作信号出力
S107
演算部が第2の認証符号を計算
S108
第2メモリを更新
S109
N = Nmax または次の認証符号と一致？
N
Y
S110
N = 1 を第2のメモリに記憶
S111
演算部が第1の認証符号を計算
S112
第1メモリを更新
S113
N = N+1 を第2メモリに記憶
終了

【図１４】

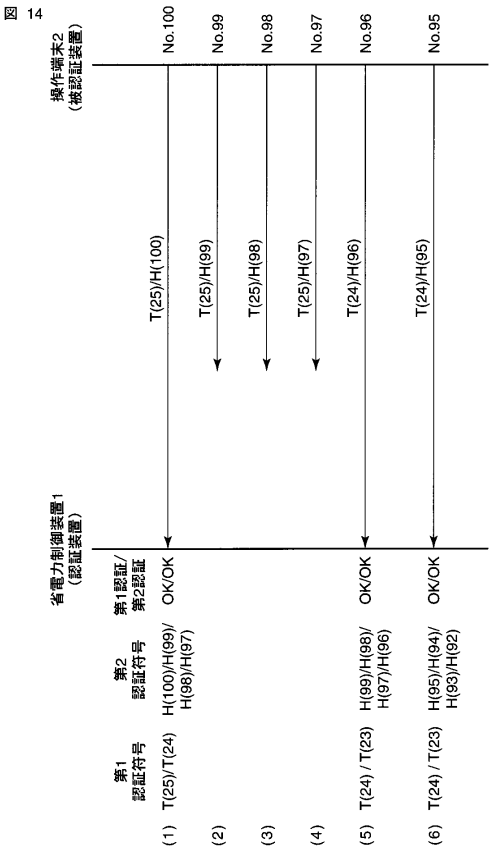


図 14
操作端末2
(被認証装置)
省電力制御装置1
(認証装置)
No.100
No.99
No.98
No.97
No.96
No.95
T(25)/H(100)
T(25)/H(99)
T(25)/H(98)
T(25)/H(97)
T(24)/H(96)
T(24)/H(95)
第1
認証符号
第2
認証符号
第1認証/
第2認証
(1) T(25)/T(24) H(100)/H(99)/H(98)/H(97) OK/OK
(2)
(3)
(4)
(5) T(24) / T(23) H(99)/H(98)/H(97)/H(96) OK/OK
(6) T(24) / T(23) H(95)/H(94)/H(93)/H(92) OK/OK

【図１５】

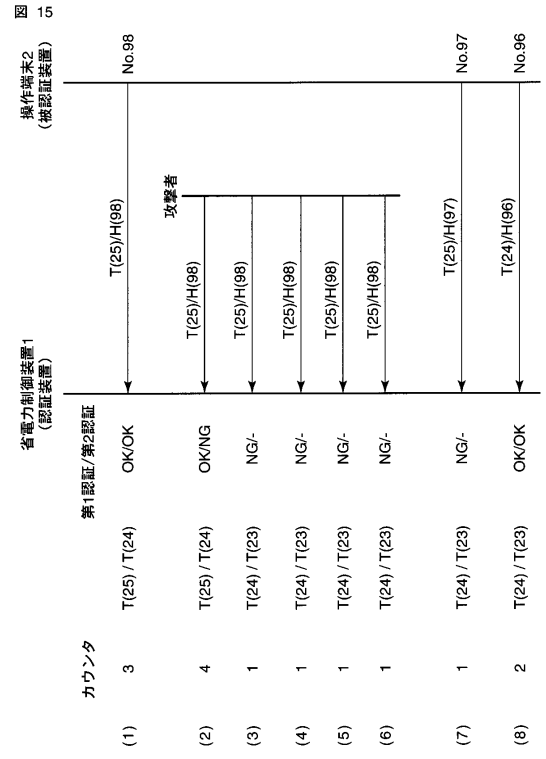


図 15
操作端末2
(被認証装置)
省電力制御装置1
(認証装置)
No.98
No.97
No.96
攻撃者
T(25)/H(98)
T(25)/H(97)
T(24)/H(96)
T(25)/H(98)
カウンタ
第1認証/第2認証
(1) 3 T(25) / T(24) OK/OK
(2) 4 T(25) / T(24) OK/NG
(3) 1 T(24) / T(23) NG/-
(4) 1 T(24) / T(23) NG/-
(5) 1 T(24) / T(23) NG/-
(6) 1 T(24) / T(23) NG/-
(7) 1 T(24) / T(23) NG/-
(8) 2 T(24) / T(23) OK/OK

フロントページの続き

(74)代理人 100084618
弁理士 村松 貞男
(74)代理人 100103034
弁理士 野河 信久
(74)代理人 100119976
弁理士 幸長 保次郎
(74)代理人 100153051
弁理士 河野 直樹
(74)代理人 100140176
弁理士 砂川 克
(74)代理人 100101812
弁理士 勝村 紘
(74)代理人 100092196
弁理士 橋本 良郎
(74)代理人 100100952
弁理士 風間 鉄也
(74)代理人 100070437
弁理士 河井 将次
(74)代理人 100124394
弁理士 佐藤 立志
(74)代理人 100112807
弁理士 岡田 貴志
(74)代理人 100111073
弁理士 堀内 美保子
(74)代理人 100134290
弁理士 竹内 将訓
(74)代理人 100127144
弁理士 市原 卓三
(74)代理人 100141933
弁理士 山下 元
(72)発明者 米良 恵介
東京都港区芝浦一丁目１番１号 株式会社東芝内
(72)発明者 土井 裕介
東京都港区芝浦一丁目１番１号 株式会社東芝内
(72)発明者 坂本 岳文
東京都港区芝浦一丁目１番１号 株式会社東芝内
(72)発明者 梅田 俊之
東京都港区芝浦一丁目１番１号 株式会社東芝内
(72)発明者 大高 章二
東京都港区芝浦一丁目１番１号 株式会社東芝内

審査官 町井 義亮

(56)参考文献 特開２００５－１９０４４７（ＪＰ，Ａ）
特開平０８－１８２０７７（ＪＰ，Ａ）
特開２００６－０２５０６９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)

G06F 21/00、21/20、
H03J 9/00－ 9/06、
H04Q 9/00－ 9/16