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

特許第5082767号
(P5082767)

(45)発行日　平成24年11月28日(2012.11.28)　(24)登録日　平成24年9月14日(2012.9.14)

(51)Int.Cl.			F I		
H04L	9/32	(2006.01)	H04L	9/00	675A
G09C	1/00	(2006.01)	G09C	1/00	640E
H04L	9/08	(2006.01)	H04L	9/00	601C

請求項の数 2　(全 11 頁)

(21)出願番号　特願2007-279561 (P2007-279561)
(22)出願日　平成19年10月26日 (2007.10.26)
(65)公開番号　特開2009-111529 (P2009-111529A)
(43)公開日　平成21年5月21日 (2009.5.21)
審査請求日　平成22年2月16日 (2010.2.16)

(73)特許権者　000237710
富士電機リテイルシステムズ株式会社
東京都品川区大崎一丁目１１番２号　ゲートシティ大崎イーストタワー
(74)代理人　100089118
弁理士　酒井　宏明
(72)発明者　武藤　健二
東京都千代田区外神田六丁目１５番１２号　富士電機リテイルシステムズ株式会社内
(72)発明者　達知　裕二
東京都千代田区外神田六丁目１５番１２号　富士電機リテイルシステムズ株式会社内
(72)発明者　生貝　浩二
東京都千代田区外神田六丁目１５番１２号　富士電機リテイルシステムズ株式会社内
最終頁に続く

(54)【発明の名称】制御機器

(57)【特許請求の範囲】
【請求項１】
暗号化された鍵取得用鍵と認証データとを記憶してある機器共通鍵により復号化するとともに、復号化された認証データを復号化された鍵取得用鍵によって再度暗号化するセキュリティ機器と、
前記セキュリティ機器との間でデータを送受信可能であって、鍵取得用鍵と認証データとを記憶してある本体共通鍵により暗号化して前記セキュリティ機器に送信する一方、前記セキュリティ機器から再度暗号化された認証データを受信するとともに受信した再度暗号化された認証データを前記鍵取得用鍵によって復号化し、前記本体共通鍵によって暗号化する前の認証データと前記鍵取得用鍵によって復号化した認証データとが一致した場合にセキュリティ機器を認証する制御機器本体と
を有した制御機器であって、
前記制御機器本体は、前記本体共通鍵によって暗号化する前の認証データと前記鍵取得用鍵によって復号化した認証データとが一致しない場合に、前記鍵取得鍵と認証データとを記憶してある前記セキュリティ機器の出荷時に前記セキュリティ機器に記憶した機器出荷鍵と同一の出荷鍵により暗号化して前記セキュリティ機器に送信する一方、前記セキュリティ機器から再度暗号化された認証データを受信するとともに、受信した再度暗号化された認証データを前記鍵取得用鍵によって復号化し、
さらに、前記出荷鍵によって暗号化する前の認証データと鍵取得用鍵によって復号化した認証データとが一致した場合に新たな機器共通鍵を生成するための機器共通鍵生成デー

タをセキュリティ機器に送信することを特徴とする制御機器。
【請求項２】
制御機器本体に設けられ、許可された者が操作した場合にのみ機器出荷鍵により暗号化した認証データをセキュリティ機器に送信するように制限するデバイステスト制限手段を備えたことを特徴とする請求項１に記載の制御機器。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、指紋認証機又はカードリーダライタ等のセキュリティ機器と、現金自動預払機（ＡＴＭ）、現金自動払出機（ＣＤ）又は自動販売機等の制御機器本体との間で暗号化したデータを送受信する制御機器に関するものである。
【背景技術】
【０００２】
セキュリティ機器と、セキュリティ機器が接続された制御機器本体との間で送受信されるデータは、個人情報に関するものであったり、金銭情報に関するものであったりするので、盗聴等の被害にあった場合には、取り返しのつかない損害を被る可能性がある。そこで、セキュリティ機器と制御機器本体との間で暗号化されたデータを送受信するように構成し、盗聴被害を免れるようにした制御機器が提案されている。このような制御機器によれば、たとえ盗聴されたとしても情報の解読が極めて困難であるため、損害を被る可能性を著しく低減することができる。
【０００３】
ところで、セキュリティ機器を製造販売するメーカと制御機器を製造販売するメーカとが異なる場合がある。この場合に、セキュリティ機器を製造販売するメーカがセキュリティ機器に設定した暗号鍵を照合するように制御機器を製造販売するメーカが制御機器本体に暗号鍵を設定すると、制御機器を製造販売するメーカのほかに、セキュリティ機器を製造販売するメーカでも暗号化されたデータを復号化することができることになる。
【０００４】
このような事態を防止するため、制御機器を製造販売するメーカにおいて、セキュリティ機器を製造販売するメーカでセキュリティ機器に設定された暗号鍵を照合するとともに、制御機器を製造販売するメーカがセキュリティ機器に新たに暗号鍵を設定するようにしている。
【０００５】
なお、セキュリティ機器であるユーザ端末を交換する場合に、ユーザ端末に記憶してある暗号鍵をユーザ管理データベースに格納し、その後、新たなユーザ端末がユーザ管理データベースから暗号鍵を取得する先行技術が知られている（例えば、特許文献１参照）。
【０００６】
【特許文献１】特開２００６－３３１９９号公報
【発明の開示】
【発明が解決しようとする課題】
【０００７】
しかしながら、制御機器を製造するメーカにおいてセキュリティ機器に新たに暗号鍵を設定することとすると、セキュリティ機器が故障した場合にも制御機器を製造するメーカにおいてセキュリティ機器に新たに暗号鍵を設定しなければならないことになる。このため、制御機器の設置管理者が交換用のセキュリティ機器を準備していても、そのまま交換することはできなかった。
【０００８】
本発明は、上記実情に鑑みて、交換したセキュリティ機器に新たに暗号鍵を設定することができる制御機器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】
【００１０】

上記の目的を達成するために、本発明の請求項１に係る制御機器は、暗号化された鍵取得用鍵と認証データとを記憶してある機器共通鍵により復号化するとともに、復号化された認証データを復号化された鍵取得用鍵によって再度暗号化するセキュリティ機器と、前記セキュリティ機器との間でデータを送受信可能であって、鍵取得用鍵と認証データとを記憶してある本体共通鍵により暗号化して前記セキュリティ機器に送信する一方、前記セキュリティ機器から再度暗号化された認証データを受信するとともに受信した再度暗号化された認証データを前記鍵取得用鍵によって復号化し、前記本体共通鍵によって暗号化する前の認証データと前記鍵取得用鍵によって復号化した認証データとが一致した場合にセキュリティ機器を認証する制御機器本体とを有した制御機器であって、前記制御機器本体は、前記本体共通鍵によって暗号化する前の認証データと前記鍵取得用鍵によって復号化した認証データとが一致しない場合に、前記鍵取得鍵と認証データとを記憶してある前記セキュリティ機器の出荷時に前記セキュリティ機器に記憶した機器出荷鍵と同一の出荷鍵により暗号化して前記セキュリティ機器に送信する一方、前記セキュリティ機器から再度暗号化された認証データを受信するとともに、受信した再度暗号化された認証データを前記鍵取得用鍵によって復号化し、さらに、前記出荷鍵によって暗号化する前の認証データと鍵取得用鍵によって復号化した認証データとが一致した場合に新たな機器共通鍵を生成するための機器共通鍵生成データをセキュリティ機器に送信することを特徴とする。

【００１１】

また、本発明の請求項２に係る制御機器は、上記請求項１において、制御機器本体に設けられ、許可された者が操作した場合にのみ機器出荷鍵により暗号化した認証データをセキュリティ機器に送信するように制限するデバイステスト制限手段を備えたことを特徴とする。

【発明の効果】

【００１２】

本発明に係る制御機器は、セキュリティ機器を交換したときのように、制御機器本体において暗号化する前の認証データと制御機器本体が受信し、かつ本体共通鍵により復号化した認証データとが一致しない場合に、制御機器本体に記憶してある機器出荷鍵と同一の出荷鍵により認証データを暗号化してセキュリティ機器に送信する一方、セキュリティ機器から再度暗号化された認証データを受信する。そして、機器出荷鍵と同一の出荷鍵により暗号化する前の認証データと受信し、かつ機器出荷鍵と同一の出荷鍵により復号化した認証データが一致した場合には、制御機器本体が、セキュリティ機器の製造販売メーカから正規に出荷されたものであるとみなして、機器共通鍵を生成するための機器共通鍵生成データをセキュリティ機器に送信する。その後、セキュリティ機器は制御機器本体によって認証されるので、以後、制御機器本体とセキュリティ機器との間では暗号化されたデータを送受信することができる。すなわち、本発明に係る制御機器は、交換したセキュリティ機器に新たに暗号鍵を設定することができる。

【発明を実施するための最良の形態】

【００１３】

以下に添付図面を参照して、本発明に係る制御機器の好適な実施の形態を詳細に説明する。なお、この実施の形態によりこの発明が限定されるものではない。

【００１４】

図１は、本発明に係る制御機器の実施の形態である制御機器を示す図であり、図２は、図１に示した制御機器における認証及びデバイステストの内容を示すフローチャートである。

【００１５】

実施の形態である制御機器１は、指紋認証機又はカードリーダライタ等のセキュリティ機器２と、現金自動預払機（ＡＴＭ）、現金自動払出機（ＣＤ）又は自動販売機等の制御機器本体３との間で暗号化したデータを送受信する制御機器であって、ＤＥＳ（Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）等の共通暗号鍵によって送信するデータを暗号化し、受信するデータを復号化するようになっている。

【００１６】
図１に示すように、セキュリティ機器２は、機器制御部４と、機器制御部４に接続された通信部５とを有している。機器制御部４は、セキュリティ機器２の制御を司るものであり、鍵記憶手段４１、暗号化手段４２、復号化手段４３及び記憶手段４４を有している。
【００１７】
鍵記憶手段４１には、機器共通鍵Ａが記憶してある。機器共通鍵Ａは、制御機器の製造販売メーカによって設定される鍵であり、制御機器の製造販売メーカが設定するまでは、セキュリティ機器の製造販売メーカが設定した機器出荷鍵が機器共通鍵Ａとして設定されている。なお、機器出荷鍵は、販売先（制御機器の製造販売メーカ）ごとに決定されており、セキュリティ機器の製造販売メーカのほか、制御機器の製造販売メーカも入手できるようになっている。
【００１８】
暗号化手段４２は、個人情報又は金銭情報等のセキュリティ機器２が取得した情報を機器共通鍵Ａによって暗号化するものであり、セキュリティ機器の認証時には制御機器本体３から受信した鍵取得用鍵Ｂによって認証データを暗号化するようになっている。
【００１９】
復号化手段４３は、制御機器本体３から受信した暗号化された制御情報を機器共通鍵Ａによって復号化するものであり、復号化された制御情報によって、機器制御部４がセキュリティ機器２を制御するようになっている。
【００２０】
記憶手段４４は、セキュリティ機器２が必要とする情報を記憶するものであって、少なくとも、セキュリティ機器を制御する制御プログラム及び制御データが記憶してある。
【００２１】
通信部５は、制御機器本体３に接続するためのインタフェースであって、制御機器本体３から暗号化された情報を受信する一方、機器制御部４（暗号化手段４２）において暗号化された情報を制御機器本体３に送信するようになっている。
【００２２】
制御機器本体３は、本体制御部６と、本体制御部６に接続された通信部７とを有している。本体制御部６は、セキュリティ機器２を含めた制御機器１の制御を司るものであり、鍵記憶手段６１、暗号化手段６２、復号化手段６３、記憶手段６４を有している。
【００２３】
鍵記憶手段６１には、本体共通鍵Ａと機器出荷鍵とが記憶してある。本体共通鍵Ａは、制御機器の製造販売メーカによって設定される鍵であり、上述した機器共通鍵Ａと対を成すように構成されている。機器出荷鍵は、セキュリティ機器の製造販売メーカから入手した鍵であって、購入直後のセキュリティ機器２は機器出荷鍵で暗号化した情報しか復号できないようになっている。
【００２４】
暗号化手段６２は、セキュリティ機器２に送信する制御情報を本体共通鍵Ａによって暗号化するものであり、セキュリティ機器の認証時には後述する鍵取得用鍵Ｂ及び認証データＣを本体共通鍵Ａ又は機器出荷鍵によって暗号化するようになっている。
【００２５】
復号化手段６３は、セキュリティ機器２から受信した暗号化された情報を本体共通鍵Ａによって復号化するものであり、セキュリティ機器の認証時には後述する鍵取得用鍵Ｂによって認証データＣを復号化するようになっている。
【００２６】
記憶手段６４は、制御機器が必要とする情報を記憶するものであって、制御機器を制御する制御プログラム及び制御データのほか、少なくとも、認証データＣ、鍵取得用鍵Ｂ、鍵データＤ、ベクトルＥが記憶してある。
【００２７】
認証データＣは、鍵取得用鍵Ｂとともにセキュリティ機器２の認証に用いられるもので

、制御機器本体３において本体共通鍵Ａあるいは機器出荷鍵によって鍵取得用鍵とともに暗号化され、制御機器本体３において本体共通鍵Ａあるいは機器出荷鍵によって復号化された情報と照合される。

【００２８】

鍵取得用鍵Ｂは、上述したようにセキュリティ機器２の認証に用いられるほか、セキュリティ機器２において機器共通鍵Ａを生成するためもので、制御機器本体３において鍵取得用鍵Ｂによって暗号化された鍵データＤ及びベクトルＥは、セキュリティ機器２において復号化され、機器共通鍵が生成される。

【００２９】

通信部７は、セキュリティ機器２を接続するためのインタフェースであって、本体制御部６（暗号化手段６２）において暗号化された情報を送信する一方、セキュリティ機器２から暗号化された情報を受信するようになっている。なお、通信部７は、複数のセキュリティ機器２を接続可能としても構わない。

【００３０】

このように構成された制御機器１は、機器設置時及び電源投入時に制御機器本体３（本体制御部６）がセキュリティ機器２の認証を行うようになっている。

【００３１】

図２に示すように、セキュリティ機器２を認証する場合には、本体制御部６が記憶手段６４に記憶してある鍵取得用鍵Ｂと認証データＣとを鍵記憶手段６１に記憶してある本体共通鍵Ａによって暗号化し、セキュリティ機器２に送信する。

【００３２】

暗号化された情報をセキュリティ機器２が受信すると、機器制御部４が鍵記憶手段４１に記憶してある機器共通鍵Ａによって暗号化された情報を復号する。この時、機器制御部４は、鍵取得用鍵Ｂと認証データＣを取得する。

【００３３】

すると、機器制御部４は、取得した鍵取得用鍵Ｂによって認証データＣを再度暗号化し、制御機器本体３に送信する。

【００３４】

鍵取得用鍵Ｂによって暗号化された情報を制御機器本体３が受信すると、本体制御部６が記憶手段６４に記憶してある鍵取得用鍵によって暗号化された情報を復号する。この時、本体制御部６は認証データＣを取得する。

【００３５】

すると、本体制御部６は、取得した認証データＣ（復号した認証データ）と記憶手段６４に記憶してある認証データＣ（暗号化した認証データ）とが一致するか否かを判定する（ステップＳ１）。

【００３６】

取得した認証データＣと記憶してある認証データＣとが一致する場合には（ステップＳ１：Ｎｏ）、セキュリティ機器２が認証されたことになるので（相互認証）、制御機器１は運用モードに移行し（ステップＳ２）、以後、セキュリティ機器２と制御機器本体３との間では暗号化された情報を送受信することになる。

【００３７】

一方、取得した認証データＣと記憶してある認証データＣとが一致しない場合には（ステップＳ１：Ｙｅｓ）、セキュリティ機器２を認証できないので、認証エラーとなり（ステップＳ３）、少なくともセキュリティ機器２の使用を制限する。

【００３８】

このように、認証エラーとなった場合、あるいはセキュリティ機器２を交換した場合等にデバイステストを実行することができるようになっている（ステップＳ４）。

【００３９】

デバイステストが実行されると（ステップＳ４）、まず、制御機器本体３がセキュリティ機器２を認証することになる。セキュリティ機器２の認証は、上記した認証と異なると

ころはないので、説明を省略する。

【００４０】

デバイステストの認証において、取得した認証データＣと記憶してある認証データとが一致する場合には（ステップＳ５：Ｎｏ）、上記認証と同様に、セキュリティ機器２が認証されたことになるので（相互認証）、制御機器１は運用モードに移行し（ステップＳ２）、以後、セキュリティ機器２と制御機器本体との間では暗号化された情報を送受信することになる。

【００４１】

一方、デバイステストの認証において、取得した認証データＣと記憶してある認証データとが一致しない場合には（ステップＳ５：Ｙｅｓ）、セキュリティ機器２が交換された可能性があるので、本体制御部６は、鍵記憶手段６１に記憶してある機器出荷鍵を共通鍵Ａに設定する（ステップＳ６）。

【００４２】

そして、共通鍵Ａに設定した機器出荷鍵を用いてセキュリティ機器２を認証することになる。

【００４３】

具体的に説明すると、本体制御部６が記憶手段６４に記憶してある鍵取得用鍵Ｂと認証データＣとを鍵記憶手段６１に記憶してある機器出荷鍵によって暗号化し、セキュリティ機器２に送信する。

【００４４】

暗号化された情報をセキュリティ機器２が受信すると、機器制御部４が鍵記憶手段４１に記憶してある機器共通鍵Ａによって暗号化された情報を復号する。ここで、機器共通鍵が機器出荷鍵であれば、機器制御部４は、鍵取得用鍵Ｂと認証データＣを取得することになる。

【００４５】

そして、鍵取得用鍵Ｂと認証データＣを取得した機器制御部４は、鍵取得用鍵Ｂを記憶手段４４に記憶するとともに、鍵取得用鍵Ｂによって認証データＣを再度暗号化し、制御機器本体３に送信する。

【００４６】

鍵取得用鍵Ｂによって暗号化された情報を制御機器本体３が受信すると、本体制御部６が記憶手段６４に記憶してある鍵取得用鍵によって暗号化された情報を復号する。この時、本体制御部６は認証データＣを取得する。

【００４７】

すると、本体制御部６は、取得した認証データＣ（復号した認証データ）と記憶手段６４に記憶してある認証データＣ（暗号化した認証データ）とが一致するか否かを判定する（ステップＳ７）。

【００４８】

取得した認証データＣと記憶してある認証データＣとが一致しない場合には（ステップＳ７：Ｎｏ）、セキュリティ機器２を認証できないので、認証エラーとなり（ステップＳ３）、少なくともセキュリティ機器２の使用を制限する。なお、ここで認証エラーとなる場合として想定されるのは、セキュリティ機器２が故障している場合や正規なセキュリティ機器２に交換されなかった場合等である。

【００４９】

一方、取得した認証データＣと記憶してある認証データとが一致する場合には、正規なセキュリティ機器２に交換されたとみなし、記憶手段６４に記憶してある鍵データＤとベクトルＥを鍵取得用鍵Ｂで暗号化してセキュリティ機器２に送信する。

【００５０】

鍵取得用鍵によって暗号化された情報をセキュリティ機器２が受信すると、セキュリティ機器２は機器出荷鍵を用いて認証において記憶手段４４に記憶した鍵取得用鍵Ｂによって暗号化された情報を復号化する。この時、機器制御部は、鍵データＤとベクトルＥを取

得する。

【００５１】

鍵データＤとベクトルＥを取得した機器制御部は、機器共通鍵Ａを生成し、鍵記憶手段に記憶する。そして、制御機器１は運用モードに移行し（ステップＳ２）、以後、セキュリティ機器２と制御機器本体３との間では暗号化された情報を送受信することになる。

【００５２】

上述した実施の形態である制御機器１によれば、セキュリティ機器２を交換したときのように、制御機器本体３において暗号化した認証データＣと制御機器本体３が受信した認証データＣとが一致しない場合に、機器出荷鍵を用いてセキュリティ機器２を認証する。そして、セキュリティ機器２が認証できた場合には、制御機器本体３が機器共通鍵を生成するための鍵データＤとベクトルＥ（機器共通鍵生成データ）をセキュリティ機器２に送信するので、以後、制御機器本体３とセキュリティ機器２との間では暗号化されたデータを送受信することができる。すなわち、本実施の形態である制御機器１は、交換したセキュリティ機器２に新たに機器共通鍵Ａを設定することができる。

【００５３】

上述した実施の形態である制御機器１によれば、鍵取得用鍵Ｂと認証データＣとを認証データとして用いたが、必ずしも鍵取得用鍵Ｂを必要とするものではなく、認証データＣのみで認証するものとしてもよい。なお、この場合には、セキュリティ機器２において、機器共通鍵Ａを用いて認証データＣを再度暗号化することになる。

【００５４】

また、許可された者（例えば、制御機器の管理者）のみが操作可能であって、許可された者が操作した場合にのみデバイステストが実行できるようにしたデバイステスト制限手段（図示せず）を制御機器本体３に設けても良い。デバイステスト制限手段は、鍵、カード、暗証番号等により許可された者を照合し、許可された者の操作のみを受け付ける操作手段（図示せず）と、操作手段が操作を受け付けた場合にのみデバイステストに移行し、セキュリティ機器２に機器出荷鍵により暗号化した認証データＣ、鍵取得用鍵Ｂによって暗号化された鍵データＤ及びベクトルＥの送信を可能とする制限手段（図示せず）とを有し、操作手段が操作を受け付けた場合にのみがデバイステストに移行し、セキュリティ機器２に機器出荷鍵により暗号化した認証データＣを送信するようになっている。このように、デバイステスト制限手段を制御機器本体３に設ければ、セキュリティ機器２を交換した場合に安全にセキュリティ機器２を認証でき、より安全にセキュリティ機器２に機器共通鍵Ａを設定することができる。

【図面の簡単な説明】

【００５５】

【図１】本発明の実施の形態である制御機器を示すブロック図である。

【図２】図１に示した制御機器における認証及びデバイステストの内容を示すフローチャートである。

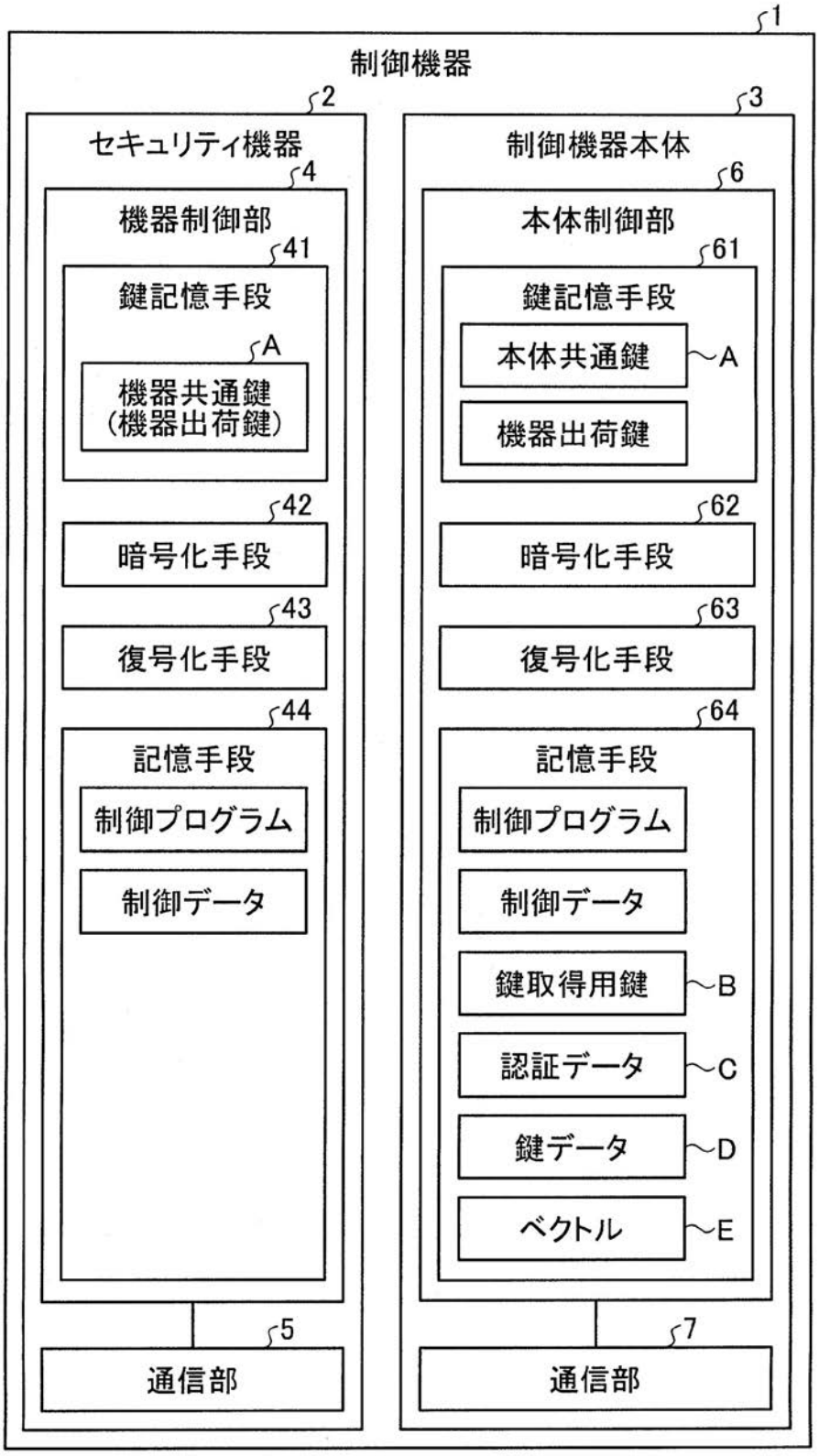
【符号の説明】

【００５６】

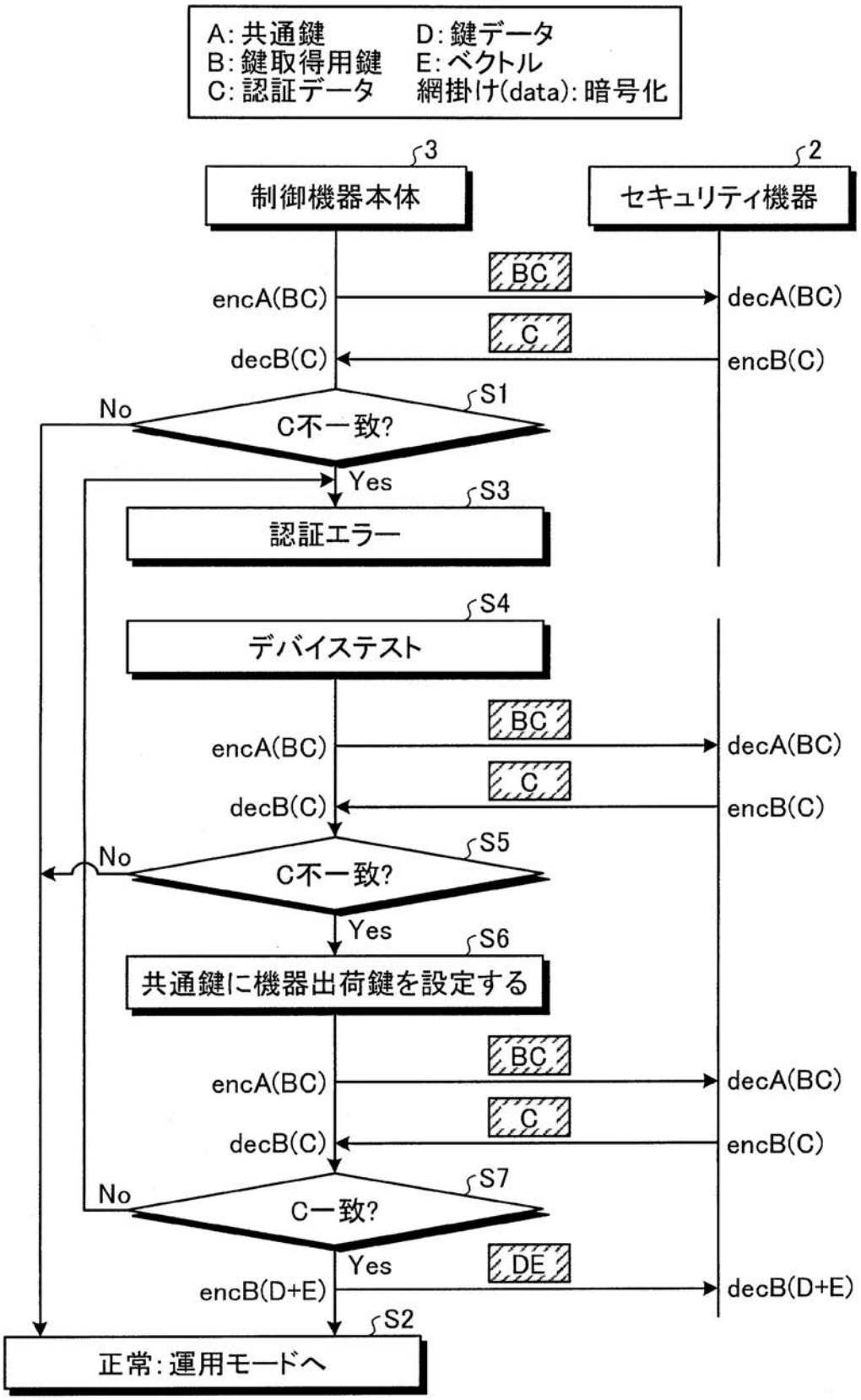
１　制御機器
２　セキュリティ機器
３　制御機器本体
４　機器制御部
４１　鍵記憶手段
４２　暗号化手段
４３　復号化手段
４４　記憶手段
５　通信部
３　制御機器本体
６　本体制御部

６１　鍵記憶手段
６２　暗号化手段
６３　復号化手段
６４　記憶手段
７　通信部
Ａ　共通鍵
Ｂ　鍵取得用鍵
Ｃ　認証データ
Ｄ　鍵データ
Ｅ　ベクトル

【図１】


1
制御機器
2
セキュリティ機器
4
機器制御部
41
鍵記憶手段
A
機器共通鍵
(機器出荷鍵)
42
暗号化手段
43
復号化手段
44
記憶手段
制御プログラム
制御データ
5
通信部
3
制御機器本体
6
本体制御部
61
鍵記憶手段
本体共通鍵
A
機器出荷鍵
62
暗号化手段
63
復号化手段
64
記憶手段
制御プログラム
制御データ
鍵取得用鍵
B
認証データ
C
鍵データ
D
ベクトル
E
7
通信部

【図２】


A: 共通鍵
B: 鍵取得用鍵
C: 認証データ
D: 鍵データ
E: ベクトル
網掛け(data): 暗号化
3
制御機器本体
2
セキュリティ機器
BC
encA(BC)
decA(BC)
C
decB(C)
encB(C)
S1
No
C不一致?
Yes
S3
認証エラー
S4
デバイステスト
BC
encA(BC)
decA(BC)
C
decB(C)
encB(C)
S5
No
C不一致?
Yes
S6
共通鍵に機器出荷鍵を設定する
BC
encA(BC)
decA(BC)
C
decB(C)
encB(C)
S7
No
C一致?
Yes
DE
encB(D+E)
decB(D+E)
S2
正常: 運用モードへ

フロントページの続き

(72)発明者　森　久直
東京都千代田区外神田六丁目１５番１２号　富士電機リテイルシステムズ株式会社内

審査官　青木　重徳

(56)参考文献　特開平０５－３３６１０８（ＪＰ，Ａ）
特開２００１－１５６７７０（ＪＰ，Ａ）
特開２００２－３３０１２５（ＪＰ，Ａ）
特開２００５－０６５２３６（ＪＰ，Ａ）
特開２００６－２５１９６１（ＪＰ，Ａ）
特開２００６－３５２２１５（ＪＰ，Ａ）
特開２００７－０７４４２６（ＪＰ，Ａ）
特開２００７－２６７３０１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３２
Ｇ０９Ｃ　　１／００
Ｈ０４Ｌ　　９／０８