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

特許第4608857号
(P4608857)

(45)発行日　平成23年1月12日(2011.1.12)　(24)登録日　平成22年10月22日(2010.10.22)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675Z
B60R 25/10	(2006.01)	B60R	25/10	607
G06F 21/20	(2006.01)	G06F	15/00	330C

請求項の数 4　(全 10 頁)

(21)出願番号　特願2003-287616(P2003-287616)
(22)出願日　平成15年8月6日(2003.8.6)
(65)公開番号　特開2005-57571(P2005-57571A)
(43)公開日　平成17年3月3日(2005.3.3)
審査請求日　平成17年9月20日(2005.9.20)

(73)特許権者　000004260
株式会社デンソー
愛知県刈谷市昭和町１丁目１番地
(74)代理人　100071135
弁理士　佐藤　強
(74)代理人　100119769
弁理士　小川　清
(72)発明者　小木曽　治比古
愛知県刈谷市昭和町１丁目１番地　株式会社デンソー内

審査官　新田　亮

最終頁に続く

(54)【発明の名称】接続確認情報管理システム

(57)【特許請求の範囲】

【請求項１】

車両に搭載されている複数の車載機器の各々が相互に接続確認を行って全ての車載機器同士の間で接続確認が正常である旨が検出された場合に車載機器群として正常に動作する一方でいずれかの車載機器同士の間で接続確認が正常でない旨が検出された場合に車載機器群として動作を停止するように構成され、複数の車載機器が車載機器同士の間で接続確認を行うのに用いられる接続確認情報を管理するシステムであって、

接続確認情報を車載機器との間で通信網を通じて通信することにより車載機器からの接続確認情報の読取りや車載機器への接続確認情報の書込みを行うセンターを備え、

センターは、車載機器や設備の所有者情報を記憶し、それら所有者情報が正当である場合に、車載機器からの接続確認情報の読取りや車載機器への接続確認情報の書込みを行うことを特徴とする接続確認情報管理システム。

【請求項２】

請求項１に記載した接続確認情報管理システムにおいて、

センターは、車載機器からの接続確認情報の読取りや車載機器への接続確認情報の書込みを暗号化して行うことを特徴とする接続確認情報管理システム。

【請求項３】

請求項１または２に記載した接続確認情報管理システムにおいて、

センターは、車載機器が特定の区域に位置しているときや特定の時間帯であるときに、車載機器からの接続確認情報の読取りや車載機器への接続確認情報の書込みを行うことを

特徴とする接続確認情報管理システム。
【請求項４】
請求項１ないし３のいずれかに記載した接続確認情報管理システムにおいて、
センターは、車載機器からの接続確認情報の読取りや車載機器への接続確認情報の書込みを特定の設備を通じて行うことを特徴とする接続確認情報管理システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、複数の機器が機器同士の間で接続確認を行うのに用いられる接続確認情報を管理するシステムに関する。
【背景技術】
【０００２】
例えば車両が盗難されることを防止するものとして、車載機器同士が接続確認を行い、接続確認が正常である旨が検出されると、複数の車載機器が正常に動作し、これに対して、接続確認が正常でない旨が検出されると、複数の車載機器が動作を停止するように構成された盗難防止システムが考えられている。このものによれば、車両が盗難されて窃盗者により悪意を持って車載機器が取替えられると、窃盗者により新たに取付けられた車載機器との間で接続確認が正常でない旨が検出されることにより、例えばエンジンＥＣＵの動作が強制的に停止されることになるので、盗難する側の盗難意欲を激減することができ、車両が盗難されることを適切に防止することができる。
【０００３】
ところで、窃盗者が悪意を持ってではなく、車両のユーザが例えば機能向上などを目的として意図的に車載機器を取替える場合がある。しかしながら、この場合、新たに取付ける車載機器に正確な接続確認情報が記憶されていないと、車載機器群としては接続確認が正常でない旨が検出されることになるので、車両が盗難されて車載機器が取替えられてないのにも拘らず、車両が盗難されて車載機器が取替えられていると誤判定してしまうことになり、盗難防止システムを適切に機能させることができないという問題がある。
【０００４】
ここで、センターが車載機器に情報を書込むものがある（例えば特許文献１参照）。
【特許文献１】特許第２８７６４６９号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかしながら、上記した特許文献１に記載されているものは、センターが車載機器自体に関する情報を車載機器に書込むものであるので、上記した問題が解消されるには至っていない。
【０００６】
本発明は、上記した事情に鑑みてなされたものであり、その目的は、ユーザが意図的に機器を取替えた後であっても機器同士が接続確認を適切に行うことができると共に、機器同士の間で接続確認を行うことで機器群の盗難を防止する盗難防止システムを適切に機能させることができる接続確認情報管理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】
【０００７】
請求項１に記載した発明によれば、センターは、複数の車載機器が車載機器同士の間で接続確認を行うのに用いられる接続確認情報を車載機器との間で通信網を通じて通信することにより車載機器からの接続確認情報の読取りや車載機器への接続確認情報の書込みを行う。これにより、センターが接続確認情報を管理し、センターが車載機器からの接続確認情報の読取りや車載機器への接続確認情報の書込みを行うことにより、ユーザが意図的に車載機器を取替えるときでは、センターが新たに取付けられた車載機器に正規の接続確認情報を書込むことにより、ユーザが意図的に車載機器を取替えた後であっても車載機器

同士が接続確認を適切に行うことができると共に、車載機器同士の間で接続確認を行うことで車載機器群の盗難を防止する盗難防止システムを適切に機能させることができる。

また、センターは、車載機器や設備の所有者情報を記憶し、それら所有者情報が正当である場合に、車載機器からの接続確認情報の読取りや車載機器への接続確認情報の書込みを行う。これにより、車載機器や設備の正当な所有者以外による車載機器からの接続確認情報の読取りや車載機器への接続確認情報の書込みを拒絶することができ、安全性をより高めることができる。

【０００８】

請求項２に記載した発明によれば、センターは、車載機器からの接続確認情報の読取りや車載機器への接続確認情報の書込みを暗号化して行うよう。これにより、センターと車載機器との間で通信されている接続確認情報が不用に解読されてしまうことを未然に防止することができ、安全性を高めることができる。

【０００９】

請求項３に記載した発明によれば、センターは、車載機器が特定の区域に位置しているときや特定の時間帯であるときに、車載機器からの接続確認情報の読取りや車載機器への接続確認情報の書込みを行う。これにより、接続確認情報の読取りや書込みを行う区域や時間帯を制限することにより、不正な区域や不正な時間帯での接続確認情報の読取りや書込みが行われることを未然に防止することができ、安全性をより高めることができる。

【００１０】

請求項４に記載した発明によれば、センターは、車載機器からの接続確認情報の読取りや車載機器への接続確認情報の書込みを特定の設備を通じて行う。これにより、接続確認情報の読取りや書込みを行う設備を制限することにより、不正な設備による接続確認情報の読取りや書込みが行われることを未然に防止することができ、安全性をより高めることができる。

【発明を実施するための最良の形態】

【００１２】

（第１の実施形態）

以下、本発明の第１の実施形態について、図１ないし図６を参照して説明する。図１は、システムの全体構成を概略的に示している。接続確認情報管理システム１は、センター（Ｚ）２と、機器（Ａ）３～機器（Ｄ）６とを備えて構成されている。センター（Ｚ）２は、機器（Ａ）３との間で電話網を通じて通信可能に構成されている。機器（Ａ）３と機器（Ｂ）４および機器（Ｃ）５とは、第１の通信ライン７を通じて接続されており、機器（Ｃ）５と機器（Ｄ）６とは、第２の通信ライン８を通じて接続されている。これら機器（Ａ）３～機器（Ｄ）６は、例えば車両に搭載されている車載機器である。

【００１３】

この場合、機器（Ａ）３は、機器（Ｂ）４～機器（Ｄ）６との間で接続確認を行う。具体的に説明すると、機器（Ａ）３は、第１の通信ライン７を通じて機器（Ｂ）４との間で接続確認を行う。また、機器（Ａ）３は、第１の通信ライン７を通じて機器（Ｃ）５との間で接続確認を行う。さらに、機器（Ａ）３は、第１の通信ライン７、機器（Ｃ）５および第２の通信ライン８を通じて機器（Ｄ）６との間で接続確認を行う。また、機器（Ｂ）４～機器（Ｄ）６の各々は、機器（Ａ）３との間で接続確認を行う。図２は、上記した機器間の接続確認の関係を一覧として示しており、各機器が接続確認対象機器との間で接続確認を行うときの接続確認経路を示している。そして、各機器は、データ通信を行うことにより接続確認を行い、データ通信が正常に完了したときに、接続確認が正常である旨を検出し、データ通信が正常に完了しなかったときに、接続確認が正常でない旨を検出する。

【００１４】

さて、上記した構成において、センター（Ｚ）２および機器（Ａ）３～機器（Ｄ）６の各々は、機器同士が接続確認を暗号化して行うときに用いられる暗号鍵を保持している。図３は、センター（Ｚ）２および機器（Ａ）３～機器（Ｄ）６の各々が保持している暗号

鍵を示している。この場合、センター（Ｚ）２は、$C_{(z-a)}$、$C_{(z-b)}$、$C_{(z-c)}$、$C_{(z-d)}$の暗号鍵を保持していると共に、機器（Ａ）３～機器（Ｄ）６の接続構成に関する情報および各機器が保持している暗号器をも保持している。

【００１５】

機器（Ａ）３は、$C_{(a-z)}$、$C_{(a-b)}$、$C_{(a-c)}$、$C_{(a-d)}$の暗号鍵を保持している。機器（Ｂ）４は、$C_{(b-z)}$、$C_{(b-a)}$の暗号鍵を保持している。機器（Ｃ）５は、$C_{(c-z)}$、$C_{(c-a)}$の暗号鍵を保持している。機器（Ｄ）６は、$C_{(d-z)}$、$C_{(d-a)}$の暗号鍵を保持している。

そして、機器（Ａ）３は、機器（Ｂ）４～機器（Ｄ）６の各々との間で接続確認を以下のようにして行う。ここでは、図４を参照し、機器（Ａ）３が機器（Ｂ）４との間で接続確認を行う手順を代表して説明する。

【００１６】

機器（Ａ）３は、乱数Ｘ１を生成し（ステップＳ１）、乱数Ｘ１を含めた信号ｍ１を機器（Ｂ）４に送信する。機器（Ｂ）４は、機器（Ａ）３から信号ｍ１が受信されると、信号ｍ１から乱数Ｘ１を抽出し、乱数Ｘ１を暗号鍵$C_{(b-a)}$により暗号化して乱数Ｘ２を生成すると共に（ステップＳ２）、乱数Ｙ１を生成する（ステップＳ３）。次いで、機器（Ｂ）４は、乱数Ｘ２および乱数Ｙ１を含めた信号ｍ２を機器（Ａ）３に送信する。

【００１７】

機器（Ａ）３は、機器（Ｂ）４から信号ｍ２が受信されると、信号ｍ２から乱数Ｘ２および乱数Ｙ１を抽出し、乱数Ｘ２を識別することにより、機器（Ｂ）４にて暗号化が正常に行われたか否かを判定する（ステップＳ４）。次いで、機器（Ａ）３は、機器（Ｂ）４にて暗号化が正常に行われた旨を検出すると、乱数Ｙ１を暗号鍵$C_{(a-b)}$により暗号化して乱数Ｙ２を生成し（ステップＳ５）、乱数Ｙ２を含めた信号ｍ３を機器（Ｂ）４に送信する。

【００１８】

機器（Ｂ）４は、機器（Ａ）３から信号ｍ３が受信されると、信号ｍ３から乱数Ｙ２を抽出し、乱数Ｙ２を識別することにより、機器（Ａ）３にて暗号化が正常に行われたか否かを判定する（ステップＳ６）。次いで、機器（Ｂ）４は、機器（Ａ）３にて暗号化が正常に行われた旨を検出すると、信号ｍ４を機器（Ａ）３に送信する。そして、機器（Ａ）３は、機器（Ｂ）４から信号ｍ４が受信されることにより、機器（Ｂ）４との間でデータ通信を正常に行えた旨を検出し、機器（Ｂ）４との間で接続が正常である旨を検出する。

【００１９】

機器（Ａ）３は、このようにして機器（Ｂ）４との間で接続確認を暗号化して行い、これと同様の手順により、機器（Ｃ）５との間でも接続確認を暗号化して行うと共に、機器（Ｄ）６との間でも接続確認を暗号化して行う。つまり、上記した構成では、機器（Ａ）３～機器（Ｄ）６は、相互に接続確認を行うことで、機器群の盗難を防止するものであり、全ての機器同士の間で接続確認が正常である旨が検出されると、機器群として正常に動作し、これに対して、いずれかの機器同士の間で接続確認が正常でない旨が検出されると、機器群として動作を停止するように構成されている。尚、接続確認に用いられる暗号化方式は、暗号化を公開鍵で行うと共に復号化を秘密鍵で行う公開鍵暗号方式であっても良いし、暗号化と復号化とを同じ秘密鍵で行う秘密鍵暗号方式であっても良い。

【００２０】

さて、ここで、図５に示すように、ユーザが意図的に機器（Ｄ）６を機器（Ｐ）９に取替える場合を説明する。この場合、ユーザは、センター（Ｚ）２に機器取替申請を行う。申請は、紙を郵送するなどで行っても良いし、電子的に電話回線を使用して行っても良い。センター（Ｚ）２は、機器（Ｐ）９がユーザの正当な所有物であるか否かなどの検査を行い、機器の取替が正当であるかを確認する。そして、センター（Ｚ）２は、機器の取替が正当でなければ、その旨をユーザに伝えると共に、必要に応じて警察などに連絡を行い、一方、機器の取替が正当であれば、以下の手順で接続確認情報の書込みを行う。

【００２１】

まず、車両の電源を遮断し、機器（Ｄ）６を機器（Ｐ）９に取替える。次に、車両の電源を投入し、機器（Ａ）３を操作して機器群とセンター（Ｚ）２とを接続し、図６に示す処理を行う。

【００２２】

センター（Ｚ）２は、機器（Ａ）３を通じて機器群（機器（Ａ）３～機器（Ｐ）９）の接続状況を調査する（ステップＳ１１）。次いで、センター（Ｚ）２は、機器群の接続状況に基づいて機器（Ｄ）６から機器（Ｐ）９に取替えられた旨を確認し、この変更に合わせた接続確認情報を生成する（ステップＳ１２）。

【００２３】

次いで、センター（Ｚ）２は、接続確認情報の変化を調査し、接続確認情報の書換えが必要な機器を特定する（ステップＳ１３）。この場合では、センター（Ｚ）２は、機器（Ａ）３および機器（Ｐ）９の接続確認情報の書換えが必要であると判断し、機器（Ａ）３の接続確認情報を書換え（ステップＳ１４）、続いて、機器（Ｐ）９の接続確認情報を書換える（ステップＳ１５）。

【００２４】

この場合、センター（Ｚ）２は、機器（Ａ）３に対する接続確認情報を暗号鍵$C_{(z-a)}$により暗号化して機器（Ａ）３に送信し、機器（Ａ）３は、センター（Ｚ）２から受信された自身に対する接続確認情報を暗号鍵$C_{(a-z)}$を復号鍵として復号する。これにより、機器（Ａ）３に対する接続確認情報が不用に解読されてしまうことを未然に防止することが可能となる。また、ここでいう機器（Ａ）３に対する接続確認情報とは、例えば機器（Ａ）３と機器（Ｐ）９との間の接続確認経路や接続確認に用いる暗号鍵などである。

【００２５】

次いで、センター（Ｚ）２は、機器（Ａ）３に対する接続確認情報を電話網を通じて機器（Ａ）３に送信した後に、機器（Ｐ）９に対する接続確認情報を作成し（ステップＳ１５）、機器（Ｐ）９に対する接続確認情報を電話網を通じて機器（Ａ）３に送信する。機器（Ａ）３は、センター（Ｚ）２から機器（Ｐ）９に対する接続確認情報が受信されると、機器（Ｐ）９に対する接続確認情報を機器（Ｐ）９に送信する。そして、機器（Ｐ）９は、機器（Ａ）３から自身に対する接続確認情報が受信されると、自身に対する接続確認情報を記憶する（ステップＳ１６）。

【００２６】

この場合、センター（Ｚ）２は、接続確認情報を暗号鍵$C_{(z-p)}$により暗号化して機器（Ａ）３を通じて機器（Ｐ）９に送信し、機器（Ｐ）９は、センター（Ｚ）２から機器（Ａ）３を通じて受信された接続確認情報を暗号鍵$C_{(p-z)}$を復号鍵として復号する。これにより、機器（Ｐ）９に対する接続確認情報が不用に解読されてしまうことを未然に防止することが可能となる。また、ここでいう機器（Ｐ）３に対する接続確認情報とは、例えば機器（Ｐ）９と機器（Ａ）３との間の接続確認経路や接続確認に用いる暗号鍵などである。

【００２７】

以上に説明した処理により、センター２は、機器（Ｄ）６が機器（Ｐ）９に取替えられると、機器（Ｄ）６が機器（Ｐ）９に取替えられたことに伴って接続確認情報を変更する必要が発生した機器、つまり、この場合であれば、機器（Ａ）３および機器（Ｐ）９に正規の接続確認情報を書込むことになる。

【００２８】

ところで、以上に説明した構成において、センター（Ｚ）２において、機器群から送信された機器群の現在位置を示す現在位置信号が受信されると、機器群の現在位置を識別し、機器群が特定の区域に位置しているときにのみ、接続確認情報を送信するように構成することも可能である。これは、車両に搭載されている機器群の接続確認情報が例えば自宅付近でしか変更できないようにすることを想定するものである。また、特定の時間帯であるときにのみ、接続確認情報を送信するように構成することも可能である。これは、車両に搭載されている機器群の接続確認情報が例えば日曜日の１２時から１７時の間でしか変

更できないようにすることを想定するものである。これにより、車両窃盗者が接続確認情報を不正に変更することを困難とする。この場合、特定の区域や特定の時間帯は、システムを管理する管理者などが設定するものであっても良いし、機器群を使用するユーザが設定するものであっても良い。

【００２９】

また、以上は、センター（Ｚ）２が機器への接続確認情報の書込みを行う場合を説明したものであるが、必要に応じて、センター（Ｚ）２が機器からの接続確認情報の読込みを行い、読込まれた接続確認情報を識別した後に、機器への接続確認情報の書込みを行うように構成することも可能である。

【００３０】

以上に説明したように第１の実施形態によれば、センター（Ｚ）２は、機器（Ａ）３～機器（Ｄ）６の接続確認で用いられる接続確認情報を管理し、機器からの接続確認情報の読取りや機器への接続確認情報の書込みを行うように構成したので、例えばユーザが意図的に機器（Ｄ）６を機器（Ｐ）９に取替えたときに、センター（Ｚ）２が機器（Ａ）３や機器（Ｐ）９に正規の接続確認情報を書込むことにより、ユーザが意図的に機器を取替えた後であっても機器同士が接続確認を適切に行うことができると共に、機器同士の間で接続確認を行うことで機器群の盗難を防止する盗難防止システムを適切に機能させることができる。

【００３１】

また、センター（Ｚ）２が機器からの接続確認情報の読取りや機器への接続確認情報の書込みを暗号化して行うように構成したので、センター（Ｚ）２と機器との間で通信されている接続確認情報が不用に解読されてしまうことを未然に防止することができ、安全性を高めることができる。

【００３２】

また、センター（Ｚ）２が機器群が特定の区域に位置しているときや特定の時間帯であるときにのみ機器からの接続確認情報の読取りや機器への接続確認情報の書込みを行うように構成すれば、接続確認情報の読取りや書込みを行う区域や時間帯を制限することにより、不正な区域や不正な時間帯での接続確認情報の読取りや書込みが行われることを未然に防止することができ、安全性をより高めることができる。

【００３３】

（第２の実施形態）

次に、本発明の第２の実施形態について、図７を参照して説明する。尚、上記した第１の実施形態と同一部分については説明を省略し、異なる部分について説明する。

上記した第１の実施形態は、センター（Ｚ）２が接続確認情報を電話網を通じて機器（Ａ）３に直接送信するように構成したものであるが、これに対して、第２の実施形態は、センター（Ｚ）２が接続確認情報を電話網を通じて読取・書込専用装置１０（本発明でいう特定の設備）に送信し、読取・書込専用装置１０と機器（Ａ）３とが有線（例えばケーブス１１）またはコードレスで接続されているときに、読取・書込専用装置１０が接続確認情報を機器（Ａ）３に送信するように構成したものである。

【００３４】

これは、車載機器の中に電話網に接続可能な機能を持ったものが存在しない場合などに、接続確認情報を書込む場合方法である。具体的には、車両メーカでの車載機器組付け後、整備工場やカー用品販売店での車載機器取替え・新規取付け後などが考えられる。尚、読取・書込専用装置１０は、機器（Ａ）３と接続されずに、第１の通信ライン７に接続されても良い。

【００３５】

以上に説明したように第２の実施形態によれば、センター（Ｚ）２が機器からの接続確認情報の読取りや機器への接続確認情報の書込みを読取・書込専用装置１０を通じて行うように構成したので、接続確認情報の読取りや書込みを行う設備を制限することにより、不正な設備による接続確認情報の読取りや書込みが行われることを未然に防止することが

でき、安全性をより高めることができる。

【００３６】

（その他の実施形態）

本発明は、上記した実施形態にのみ限定されるものではなく、以下のように変形または拡張することができる。

車両に搭載されている機器群に適用する構成に限らず、他の装置に搭載されている機器群に適用する構成であっても良い。

【図面の簡単な説明】

【００３７】

【図１】本発明の第１の実施形態の全体構成を概略的に示す図

【図２】各機器の接続確認対象機器および接続確認経路を示す図

【図３】センターおよび各機器の暗号鍵を示す図

【図４】シーケンス図

【図５】図３相当図

【図６】図４相当図

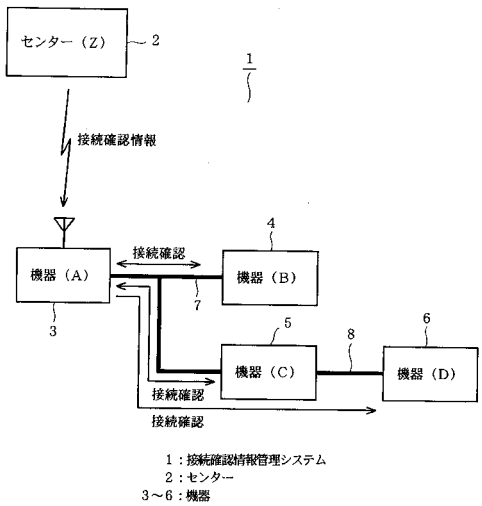
【図７】本発明の第２の実施形態の全体構成を概略的に示す図

【符号の説明】

【００３８】

図面中、１は接続確認情報管理システム、２はセンター、３～６は機器、９は機器、１０は読取・書込専用装置（特定の設備）である。

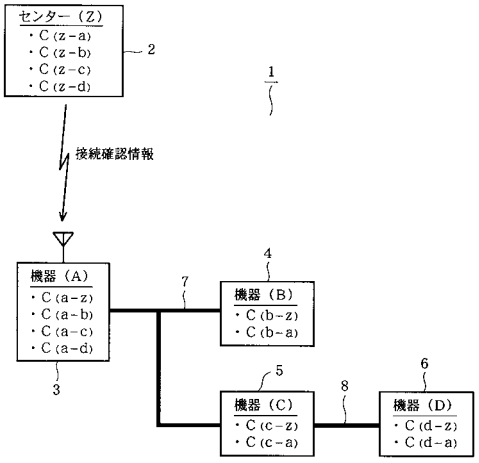
【図１】



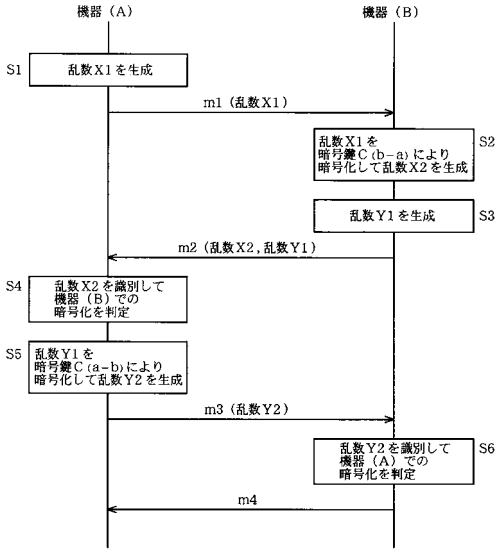
【図２】

機器	接続確認対象機器	接続確認経路
機器（A）	機器（B）	第１の通信ライン
	機器（C）	第１の通信ライン
	機器（D）	第１の通信ライン ― 機器（C） ― 第２の通信ライン
機器（B）	機器（A）	第１の通信ライン
機器（C）	機器（A）	第１の通信ライン
機器（D）	機器（A）	第２の通信ライン ― 機器（C） ― 第１の通信ライン

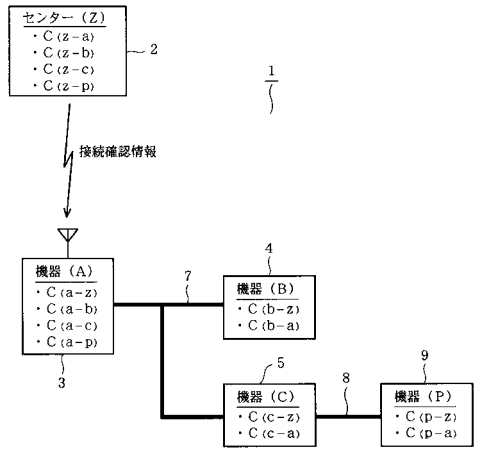
【図３】


センター（Z）
・C（z－a）
・C（z－b）
・C（z－c）
・C（z－d）
2
1
接続確認情報
機器（A）
・C（a－z）
・C（a－b）
・C（a－c）
・C（a－d）
3
7
4
機器（B）
・C（b－z）
・C（b－a）
5
機器（C）
・C（c－z）
・C（c－a）
8
6
機器（D）
・C（d－z）
・C（d－a）

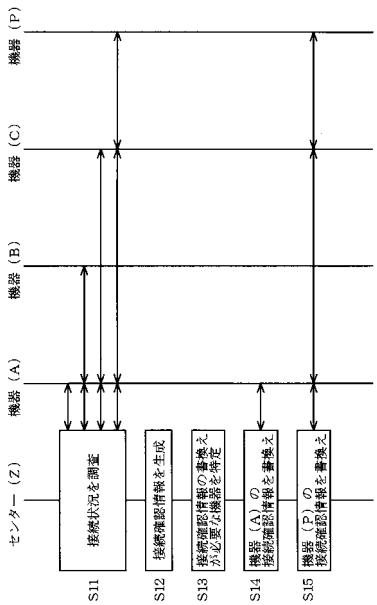
【図４】


機器（A）
機器（B）
S1
乱数X1を生成
m1（乱数X1）
乱数X1を
暗号鍵C（b－a）により
暗号化して乱数X2を生成
S2
乱数Y1を生成
S3
m2（乱数X2，乱数Y1）
S4
乱数X2を識別して
機器（B）での
暗号化を判定
S5
乱数Y1を
暗号鍵C（a－b）により
暗号化して乱数Y2を生成
m3（乱数Y2）
乱数Y2を識別して
機器（A）での
暗号化を判定
S6
m4

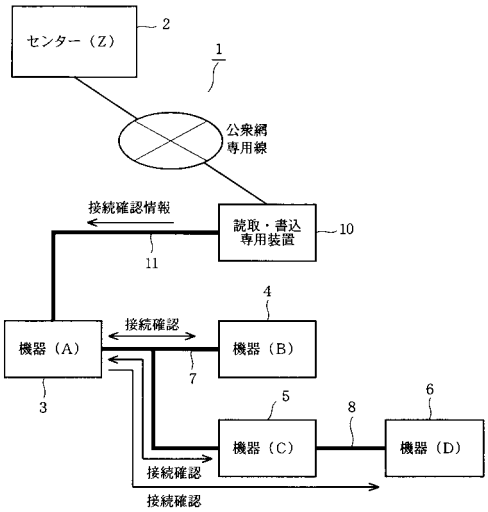
【図５】


センター（Z）
・C（z－a）
・C（z－b）
・C（z－c）
・C（z－p）
2
1
接続確認情報
機器（A）
・C（a－z）
・C（a－b）
・C（a－c）
・C（a－p）
3
7
4
機器（B）
・C（b－z）
・C（b－a）
5
機器（C）
・C（c－z）
・C（c－a）
8
9
機器（P）
・C（p－z）
・C（p－a）

【図６】


機器（P）
機器（C）
機器（B）
機器（A）
センター（Z）
接続状況を調査
接続確認情報を生成
接続確認情報の書換えが必要な機器を特定
機器（A）の接続確認情報を書換え
機器（P）の接続確認情報を書換え
S11
S12
S13
S14
S15

【図７】


センター（Z）
2
1
公衆網
専用線
接続確認情報
読取・書込
専用装置
10
11
4
接続確認
機器（A）
機器（B）
7
3
5
6
8
機器（C）
機器（D）
接続確認
接続確認

フロントページの続き

(56)参考文献 特開２００３－１５２７１７（ＪＰ，Ａ）
特開平１０－３３６７４５（ＪＰ，Ａ）
特開昭６２－１８１５４３（ＪＰ，Ａ）
特開２００２－２９０３９７（ＪＰ，Ａ）
特開平１０－３２７１４２（ＪＰ，Ａ）
岡本　栄司，暗号理論入門，日本，共立出版株式会社，１９９３年　2月２５日，p.111-112

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３２
Ｂ６０Ｒ　２５／１０
Ｇ０６Ｆ　２１／２０