

(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2005-38411

(P2005-38411A)

(43) 公開日 平成17年2月10日(2005.2.10)

(51) Int.CI.⁷**G 06 F 15/00**
H 04 L 9/32

F 1

G 06 F 15/00
H 04 L 9/00

テーマコード(参考)

5 B 0 8 5
5 J 1 0 4

審査請求 未請求 請求項の数 38 O L (全 33 頁)

(21) 出願番号 特願2004-179562 (P2004-179562)
 (22) 出願日 平成16年6月17日 (2004.6.17)
 (31) 優先権主張番号 特願2003-188139 (P2003-188139)
 (32) 優先日 平成15年6月30日 (2003.6.30)
 (33) 優先権主張国 日本国 (JP)

(71) 出願人 000002185
ソニー株式会社
東京都品川区北品川6丁目7番35号
 (74) 代理人 100096655
弁理士 川井 隆
 (74) 代理人 100091225
弁理士 仲野 均
 (72) 発明者 勝部 友浩
東京都品川区北品川6丁目7番35号 ソ
ニー株式会社内
 (72) 発明者 伊達 秀樹
東京都品川区北品川6丁目7番35号 ソ
ニー株式会社内

最終頁に続く

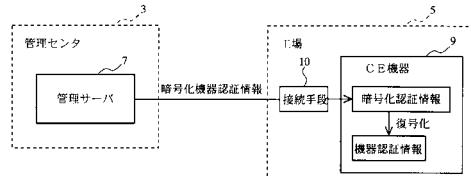
(54) 【発明の名称】機器認証情報組込システム、端末機器、機器認証情報処理方法、機器認証情報処理プログラム、提供サーバ、機器認証情報提供方法、機器認証情報提供プログラム、及び記憶媒体

(57) 【要約】

【課題】 CE 機器内に機器認証情報を安全に組み込むこと。

【解決手段】 管理サーバ 7 は、機器認証情報を暗号化して工場 5 に送信する。接合具 10 は、工場の作業者により CE 機器 9 のコネクタに接続され、管理サーバ 7 から送信されてきた機器認証情報を暗号化されたまま CE 機器 9 に入力する。CE 機器 9 の内部には、暗号化された機器認証情報を復号化して格納するための書き込みモジュールが内蔵されている。接合具 10 から入力された機器認証情報は、書き込みモジュールにより復号化され、CE 機器 9 内部の記憶装置に記憶される。機器認証情報は、暗号化されたまま CE 機器 9 に入力されるので安全に機器認証情報を組み込むことができる。

【選択図】 図 1



【特許請求の範囲】**【請求項 1】**

提供サーバと端末機器から成り、機器認証サーバで機器認証する際の機器認証情報を端末機器に組み込む機器認証情報組込システムであって、

前記提供サーバは、

機器認証情報を生成する元となる元情報を前記端末機器に提供すると共に、前記機器認証情報、又は前記元情報を、前記端末機器の機器認証を行う機器認証サーバに提供し、

前記端末機器は、

前記提供された元情報を用いて、機器認証情報を送信するために必要な情報を記憶し、機器認証時に、前記記憶した情報を用いて前記元情報から生成した機器認証情報を、前記機器認証サーバに送信する

10

ことを特徴とする機器認証情報組込システム。

【請求項 2】

前記提供サーバは、前記元情報から生成される機器認証情報を所定の一方向性関数で変換した変換値を前記端末機器に提供し、

前記端末機器は、前記提供された元情報から生成した機器認証情報を前記一方向性関数で変換して変換値を生成し、

前記生成した変換値と、前記提供サーバから提供された変換値の同一性を判断することを特徴とする請求項 1 に記載の機器認証情報組込システム。

20

【請求項 3】

前記端末機器は、前記提供された元情報から生成した機器認証情報を所定の一方向性関数で変換して変換値を前記提供サーバに提供し、

前記提供サーバは、前記元情報から生成される機器認証情報を前記一方向性関数で変換した変換値と、前記端末機器から提供された変換値の同一性を判断することを特徴とする請求項 1 に記載の機器認証情報組込システム。

20

【請求項 4】

提供サーバから提供される、機器認証情報を生成する元となる元情報を取得する元情報取得手段と、

前記取得した元情報を機器認証情報を生成する生成手段と、

機器認証時に、前記生成した機器認証情報を機器認証サーバに送信する機器認証情報送信手段と、

30

を具備したことを特徴とする端末機器。

【請求項 5】

前記元情報は、前記機器認証情報を暗号化した暗号化機器認証情報であり、

前記生成手段は、前記暗号化機器認証情報を復号化することにより、前記機器認証情報を生成することを特徴とする請求項 4 に記載の端末機器。

40

【請求項 6】

前記生成手段で生成した機器認証情報を暗号化して記憶する記憶手段を具備し、

前記機器認証情報送信手段は、前記記憶手段に記憶された機器認証情報を復号化して送信することを特徴とする請求項 4 に記載の端末機器。

【請求項 7】

前記記憶手段に記憶する機器認証情報の暗号化、及び復号化に使用する暗号鍵を、前記暗号鍵の使用時に前記端末機器に固有な情報を用いて生成する鍵生成手段を具備したことを特徴とする請求項 6 に記載の端末機器。

【請求項 8】

前記生成した暗号鍵を、前記暗号鍵の使用後の所定期間内に消去する鍵消去手段を具備したことを特徴とする請求項 7 に記載の端末機器。

【請求項 9】

前記提供サーバから前記機器認証情報を所定の一方向性関数で変換した変換値を取得する変換値取得手段と、

50

前記生成した機器認証情報を、前記一方向性関数で変換して変換値を算出する変換値算出手段と、

前記取得した変換値と、前記算出した変換値の同一性を判断し、その判断結果を出力する判断手段と、

を具備したことを特徴とする請求項4に記載の端末機器。

【請求項10】

前記生成した機器認証情報を他の一方向性関数で変換して変換値を算出する変換値算出手段と、

前記算出した変換値を前記提供サーバに提供する変換値提供手段と、

を具備したことを特徴とする請求項9に記載の端末機器。

10

【請求項11】

前記生成した機器認証情報を所定の一方向性関数で変換して変換値を算出する変換値算出手段と、

前記算出した変換値を前記提供サーバに提供する変換値提供手段と、

を具備したことを特徴とする請求項4に記載の端末機器。

【請求項12】

前記取得した元情報を記憶する記憶手段を具備し、

前記機器認証情報送信手段は、前記記憶した元情報から機器認証情報を生成して前記機器認証サーバに送信することを特徴とする請求項4に記載の端末機器。

20

【請求項13】

元情報取得手段と、生成手段と、機器認証情報送信手段と、を備えたコンピュータで構成された端末機器において、

提供サーバから提供される、機器認証情報を生成する元となる元情報を前記元情報取得手段で取得する元情報取得ステップと、

前記取得した元情報から機器認証情報を、前記生成手段で生成する生成ステップと、

機器認証時に、前記生成した機器認証情報を、前記機器認証情報送信手段で機器認証サーバに送信する機器認証情報送信ステップと、

から構成されたことを特徴とする機器認証情報処理方法。

【請求項14】

前記元情報は、前記機器認証情報を暗号化した暗号化機器認証情報であり、

30

前記生成ステップでは、前記暗号化機器認証情報を復号化することにより、前記機器認証情報を生成することを特徴とする請求項13に記載の機器認証情報処理方法。

【請求項15】

前記コンピュータは、記憶手段を備え、

前記生成手段で生成した機器認証情報を暗号化して前記記憶手段で記憶する記憶ステップを備え、

前記機器認証情報送信ステップでは、前記記憶手段に記憶された機器認証情報を復号化して送信することを特徴とする請求項13に記載の機器認証情報処理方法。

【請求項16】

前記コンピュータは、鍵生成手段を備え、

前記記憶手段に記憶する機器認証情報の暗号化、及び復号化に使用する暗号鍵を、前記鍵生成手段で前記暗号鍵の使用時に前記端末機器に固有な情報を用いて生成する鍵生成ステップを備えたことを特徴とする請求項15に記載の機器認証情報処理方法。

40

【請求項17】

前記コンピュータは、鍵消去手段を備え、

前記生成した暗号鍵を、前記暗号鍵の使用後の所定期間内に前記鍵消去手段で消去する鍵消去ステップを備えたことを特徴とする請求項16に記載の機器認証情報処理方法。

【請求項18】

前記コンピュータは、変換値取得手段と、変換値算出手段と、判断手段と、を備え、

前記提供サーバから前記機器認証情報を所定の一方向性関数で変換した変換値を前記変

50

換値取得手段で取得する変換値取得ステップと、

前記変換値算出手段で前記生成した機器認証情報を、前記一方向性関数で変換して変換値を算出する変換値算出手段と、

前記判断手段で、前記取得した変換値と、前記算出した変換値の同一性を判断し、その判断結果を出力する判断ステップと、

を備えたことを特徴とする請求項13に記載の機器認証情報処理方法。

【請求項19】

前記コンピュータは、変換値算出手段と、変換値提供手段と、を備え、

前記変換値算出手段で、前記生成した機器認証情報を他の一方向性関数で変換して変換値を算出する変換値算出手段と、

前記変換値算出手段で、前記算出した変換値を前記提供サーバに提供する変換値提供ステップと、

を備えたことを特徴とする請求項18に記載の機器認証情報処理方法。

【請求項20】

前記コンピュータは、変換値算出手段と、変換値提供手段と、を備え、

前記変換値算出手段で、前記生成した機器認証情報を所定の一方向性関数で変換して変換値を算出する変換値算出手段と、

前記変換値提供手段で、前記算出した変換値を前記提供サーバに提供する変換値提供ステップと、

を備えたことを特徴とする請求項13に記載の機器認証情報処理方法。

【請求項21】

前記コンピュータは、前記取得した元情報を記憶する記憶手段を具備し、

前記機器認証情報送信ステップでは、前記記憶した元情報を機器認証情報を生成して前記機器認証サーバに送信することを特徴とする請求項13に記載の機器認証情報処理方法。

【請求項22】

提供サーバから提供される、機器認証情報を生成する元となる元情報を取得する元情報取得機能と、

前記取得した元情報を機器認証情報を生成する生成機能と、

機器認証時に、前記生成した機器認証情報を機器認証サーバに送信する機器認証情報送信機能と、

をコンピュータで実現する機器認証情報処理プログラム。

【請求項23】

前記元情報は、前記機器認証情報を暗号化した暗号化機器認証情報であり、

前記生成機能は、前記暗号化機器認証情報を復号化することにより、前記機器認証情報を生成することを特徴とする請求項22に記載の機器認証情報処理プログラム。

【請求項24】

前記生成機能で生成した機器認証情報を暗号化して記憶する記憶機能を実現し、

前記機器認証情報送信機能は、前記記憶機能に記憶された機器認証情報を復号化して送信することを特徴とする請求項22に記載の機器認証情報処理プログラム。

【請求項25】

前記記憶機能に記憶する機器認証情報の暗号化、及び復号化に使用する暗号鍵を、前記暗号鍵の使用時に前記端末機器に固有な情報を用いて生成する鍵生成機能をコンピュータで実現する請求項24に記載の機器認証情報処理プログラム。

【請求項26】

前記生成した暗号鍵を、前記暗号鍵の使用後の所定期間内に消去する鍵消去機能をコンピュータで実現する請求項25に記載の機器認証情報処理プログラム。

【請求項27】

前記提供サーバから前記機器認証情報を所定の一方向性関数で変換した変換値を取得する変換値取得機能と、

10

20

30

40

50

前記生成した機器認証情報を、前記一方向性関数で変換して変換値を算出する変換値算出機能と、

前記取得した変換値と、前記算出した変換値の同一性を判断し、その判断結果を出力する判断機能と、

をコンピュータで実現する請求項22に記載の機器認証情報処理プログラム。

【請求項28】

前記生成した機器認証情報を他の一方向性関数で変換して変換値を算出する変換値算出機能と、

前記算出した変換値を前記提供サーバに提供する変換値提供機能と、

をコンピュータで実現する請求項27に記載の機器認証情報処理プログラム。 10

【請求項29】

前記生成した機器認証情報を所定の一方向性関数で変換して変換値を算出する変換値算出機能と、

前記算出した変換値を前記提供サーバに提供する変換値提供機能と、

をコンピュータで実現する請求項22に記載の機器認証情報処理プログラム。

【請求項30】

前記取得した元情報を記憶する記憶機能をコンピュータで実現し、

前記機器認証情報送信機能は、前記記憶した元情報から機器認証情報を生成して前記機器認証サーバに送信することを特徴とする請求項22に記載の機器認証情報処理プログラム。 20

【請求項31】

提供サーバから提供される、機器認証情報を生成する元となる元情報を取得する元情報取得機能と、

前記取得した元情報を機器認証情報を生成する生成機能と、

機器認証時に、前記生成した機器認証情報を機器認証サーバに送信する機器認証情報送信機能と、

をコンピュータで実現する機器認証情報処理プログラムを記憶したコンピュータが読み取り可能な記憶媒体。

【請求項32】

端末機器に機器認証情報を生成する元となる元情報を提供する元情報提供手段と、 30

前記機器認証情報、又は前記元情報を、前記端末機器の機器認証を行う機器認証サーバに提供する機器認証情報提供手段と、

前記端末機器から、前記元情報から生成された機器認証情報の、所定の一方向性関数で変換した変換値を取得する変換値取得手段と、

前記機器認証情報を前記一方向性関数で変換して変換値を算出する変換値算出手段と、

前記取得した変換値と前記算出した変換値の同一性を判断し、その判断結果を出力する判断手段と、

を具備したことを特徴とする提供サーバ。

【請求項33】

前記判断手段で出力された判断結果を、前記元情報の組込主体に送信する判断結果送信手段を具備したことを特徴とする請求項32に記載の提供サーバ。 40

【請求項34】

元情報提供手段と、機器認証情報提供手段と、変換値取得手段と、変換値算出手段と、判断手段と、を備えたコンピュータにおいて、

端末機器に機器認証情報を生成する元となる元情報を、前記元情報提供手段で提供する元情報提供ステップと、

前記機器認証情報、又は前記元情報を、前記機器認証情報提供手段で前記端末機器の機器認証を行う機器認証サーバに提供する機器認証情報提供ステップと、前記変換値取得手段で、前記端末機器から、前記元情報から生成された機器認証情報の、所定の一方向性関数で変換した変換値を取得する変換値取得ステップと、 50

前記変換値算出手段で、前記機器認証情報を前記一方向性関数で変換して変換値を算出する変換値算出ステップと、

前記判断手段で、前記取得した変換値と前記算出した変換値の同一性を判断し、その判断結果を出力する判断ステップと、

から構成されたことを特徴とする機器認証情報提供方法。

【請求項 3 5】

前記コンピュータは、判断結果送信手段を備え、

前記判断手段で出力された判断結果を、前記判断結果送信手段で前記元情報の組込主体に送信する判断結果送信ステップを備えたことを特徴とする請求項 3 4 に記載の機器認証情報提供方法。

10

【請求項 3 6】

端末機器に機器認証情報を生成する元となる元情報を提供する元情報提供機能と、

前記機器認証情報、又は前記元情報を、前記端末機器の機器認証を行う機器認証サーバに提供する機器認証情報提供機能と、

前記端末機器から、前記元情報から生成された機器認証情報の、所定の一方向性関数で変換した変換値を取得する変換値取得機能と、

前記機器認証情報を前記一方向性関数で変換して変換値を算出する変換値算出機能と、

前記取得した変換値と前記算出した変換値の同一性を判断し、その判断結果を出力する判断機能と、

をコンピュータで実現する機器認証情報提供プログラム。

20

【請求項 3 7】

前記判断機能で出力された判断結果を、前記元情報の組込主体に送信する判断結果送信機能をコンピュータで実現する請求項 3 6 に記載の機器認証情報提供プログラム。

【請求項 3 8】

端末機器に機器認証情報を生成する元となる元情報を提供する元情報提供機能と、

前記機器認証情報、又は前記元情報を、前記端末機器の機器認証を行う機器認証サーバに提供する機器認証情報提供機能と、

前記端末機器から、前記元情報から生成された機器認証情報の、所定の一方向性関数で変換した変換値を取得する変換値取得機能と、

前記機器認証情報を前記一方向性関数で変換して変換値を算出する変換値算出機能と、

前記取得した変換値と前記算出した変換値の同一性を判断し、その判断結果を出力する判断機能と、

30

をコンピュータで実現する機器認証情報提供プログラムを記憶したコンピュータが読み取り可能な記憶媒体。

【発明の詳細な説明】

【技術分野】

【0 0 0 1】

本発明は、端末機器などに関し、特に、機器認証情報を暗号化して機器に書き込み、これを機器内で復号化することにより、機器認証情報を安全に機器内に書き込むものに関する。

40

【背景技術】

【0 0 0 2】

近年、CE(C E : C onsumer E lectr onics)機器の普及が広まりつつある。CE機器とは、例えば、ビデオデッキ、ステレオ、テレビなどのオーディオビジュアル機器や、炊飯器、冷蔵庫などの家電製品や、その他の電子機器にコンピュータを内蔵させ、ネットワークを介してサービスを利用できるものである。

サーバが提供するサービスには、CE機器の機器認証を要するものがある。そのため、CE機器には、機器認証を行うための機器認証情報を予め製造工場にて組み込まれる。

【0 0 0 3】

50

図18は、従来の機器認証情報の組み込み方法を説明するための図である。CE機器に組み込まれる機器認証情報は、管理センタ103の管理サーバ107で管理されている。

管理サーバ107は、機器認証情報をCE機器の製造工場である工場105に送信する。

機器認証情報は、機密性を要する秘密情報であるので、外部に漏出しないように暗号化されて送信される。

【0004】

工場105では、接続手段110をCE機器109のコネクタに接続して、管理サーバ107から送信されてきた機器認証情報をCE機器109に入力する。接続手段110には、暗号化された機器認証情報を復号化する機能が内蔵されており、管理サーバ107から送信されてきた機器認証情報は、接続手段110にて復号化される。10

機器認証情報は、復号化された状態で接続手段110からCE機器109に入力されて、CE機器109の記憶装置に記憶される。

このような、CE機器に機器認証情報を組み込む発明としては、次の電子機器製造システム及び電子機器製造方法がある。

【0005】

【特許文献1】特開2001-134654

【0006】

この発明は、CE機器に貼付したバーコードラベルシールに書かれた製品シリアル番号から、データベースに登録されている機器認証情報を読み出して機器に組み込むものである。20

【発明の開示】

【発明が解決しようとする課題】

【0007】

ところが、従来の方法では、接続手段110で機器認証情報を復号化してしまうため、接続手段110から機器認証情報が漏出してしまう可能性があった。

特に近年では、コストの低い海外の事業者に生産を委託する場合なども多く、工場105に送った機器認証情報が外部に漏出することなく確実にCE機器109に組み込める仕組みが必要とされていた。

【0008】

そこで、本発明の第1の目的は、機器内に機器認証情報を安全に組み込むことができる端末機器などを提供することである。

また、本発明の第2の目的は、機器内に機器認証情報が適切に組み込まれたことを機器認証情報の秘密状態を保持した状態で確認することである。

【課題を解決するための手段】

【0009】

本発明は、前記目的を達成するために、提供サーバと端末機器から成り、機器認証サーバで機器認証する際の機器認証情報を端末機器に組み込む機器認証情報組込システムであって、前記提供サーバは、機器認証情報を生成する元となる元情報を前記端末機器に提供すると共に、前記機器認証情報、又は前記元情報を、前記端末機器の機器認証を行う機器認証サーバに提供し、前記端末機器は、前記提供された元情報を用いて、機器認証情報を送信するために必要な情報を記憶し、機器認証時に、前記記憶した情報を用いて前記元情報から生成した機器認証情報を、前記機器認証サーバに送信することを特徴とする機器認証情報組込システムを提供する（第1の構成）。

第1の構成において、前記提供サーバは、前記元情報から生成される機器認証情報を所定の一方向性関数で変換した変換値を前記端末機器に提供し、前記端末機器は、前記提供された元情報を生成した機器認証情報を前記一方向性関数で変換して変換値を生成し、前記生成した変換値と、前記提供サーバから提供された変換値の同一性を判断するように構成することができる（第2の構成）。

また、第1の構成において、前記端末機器は、前記提供された元情報から生成した機器

10

30

40

50

認証情報を所定の一方指向性関数で変換して変換値を前記提供サーバに提供し、前記提供サーバは、前記元情報から生成される機器認証情報を前記一方指向性関数で変換した変換値と、前記端末機器から提供された変換値の同一性を判断するように構成することもできる（第3の構成）。

また、本発明は、前記目的を達成するために、提供サーバから提供される、機器認証情報を生成する元となる元情報を取得する元情報取得手段と、前記取得した元情報から機器認証情報を生成する生成手段と、機器認証時に、前記生成した機器認証情報を機器認証サーバに送信する機器認証情報送信手段と、を具備したことを特徴とする端末機器を提供する（第4の構成）。

また、第4の構成において、前記元情報は、前記機器認証情報を暗号化した暗号化機器認証情報であり、前記生成手段は、前記暗号化機器認証情報を復号化することにより、前記機器認証情報を生成するように構成することもできる（第5の構成）。

更に、第4の構成において、前記生成手段で生成した機器認証情報を暗号化して記憶する記憶手段を具備し、前記機器認証情報送信手段は、前記記憶手段に記憶された機器認証情報を復号化して送信するように構成することもできる（第6の構成）。

また、第6の構成において、前記記憶手段に記憶する機器認証情報の暗号化、及び復号化に使用する暗号鍵を、前記暗号鍵の使用時に前記端末機器に固有な情報を用いて生成する鍵生成手段を具備するように構成することもできる（第7の構成）。

また、第7の構成において、前記生成した暗号鍵を、前記暗号鍵の使用後の所定期間内に消去する鍵消去手段を具備するように構成することもできる（第8の構成）。

また、第4の構成において、前記提供サーバから前記機器認証情報を所定の一方指向性関数で変換した変換値を取得する変換値取得手段と、前記生成した機器認証情報を、前記一方指向性関数で変換して変換値を算出する変換値算出手段と、前記取得した変換値と、前記算出した変換値の同一性を判断し、その判断結果を出力する判断手段と、を具備するように構成することもできる（第9の構成）。

また、第9の構成において、前記生成した機器認証情報を他の一方指向性関数で変換して変換値を算出する変換値算出手段と、前記算出した変換値を前記提供サーバに提供する変換値提供手段と、を具備するように構成することもできる（第10の構成）。

また、第4の構成において、前記生成した機器認証情報を所定の一方指向性関数で変換して変換値を算出する変換値算出手段と、前記算出した変換値を前記提供サーバに提供する変換値提供手段と、を具備するように構成することもできる（第11の構成）。

また、第4の構成において、前記取得した元情報を記憶する記憶手段を具備し、前記機器認証情報送信手段は、前記記憶した元情報を前記機器認証情報を生成して前記機器認証サーバに送信するように構成することもできる（第12の構成）。

また、本発明は、前記目的を達成するために、元情報取得手段と、生成手段と、機器認証情報送信手段と、を備えたコンピュータで構成された端末機器において、提供サーバから提供される、機器認証情報を生成する元となる元情報を前記元情報取得手段で取得する元情報取得ステップと、前記取得した元情報を前記機器認証情報を、前記生成手段で生成する生成ステップと、機器認証時に、前記生成した機器認証情報を、前記機器認証情報送信手段で機器認証サーバに送信する機器認証情報送信ステップと、から構成したことを特徴とする機器認証情報処理方法を提供する（第13の構成）。

また、第13の構成において、前記元情報は、前記機器認証情報を暗号化した暗号化機器認証情報であり、前記生成ステップでは、前記暗号化機器認証情報を復号化することにより、前記機器認証情報を生成するように構成することもできる（第14の構成）。

また、第13の構成において、前記コンピュータは、記憶手段を備え、前記生成手段で生成した機器認証情報を暗号化して前記記憶手段で記憶する記憶ステップを備え、前記機器認証情報送信ステップでは、前記記憶手段に記憶された機器認証情報を復号化して送信するように構成することもできる（第15の構成）。

また、第15の構成において、前記コンピュータは、鍵生成手段を備え、前記記憶手段に記憶する機器認証情報の暗号化、及び復号化に使用する暗号鍵を、前記鍵生成手段で前

10

20

30

40

50

記暗号鍵の使用時に前記端末機器に固有な情報を用いて生成する鍵生成ステップを備えるように構成することもできる(第16の構成)。

また、第16の構成において、前記コンピュータは、鍵消去手段を備え、前記生成した暗号鍵を、前記暗号鍵の使用後の所定期間内に前記鍵消去手段で消去する鍵消去ステップを備えるように構成することもできる(第17の構成)。

また、第13の構成において、前記コンピュータは、変換値取得手段と、変換値算出手段と、判断手段と、を備え、前記提供サーバから前記機器認証情報を所定の一方向性関数で変換した変換値を前記変換値取得手段で取得する変換値取得ステップと、前記変換値算出手段で前記生成した機器認証情報を、前記一方向性関数で変換して変換値を算出する変換値算出ステップと、前記判断手段で、前記取得した変換値と、前記算出した変換値の同一性を判断し、その判断結果を出力する判断ステップと、を備えるように構成することもできる(第18の構成)。

また、第18の構成において、前記コンピュータは、変換値算出手段と、変換値提供手段と、を備え、前記変換値算出手段で、前記生成した機器認証情報を他の一方向性関数で変換して変換値を算出する変換値算出ステップと、前記変換値算出手段で、前記算出した変換値を前記提供サーバに提供する変換値提供ステップと、を備えるように構成することができる(第19の構成)。

第13の構成において、前記コンピュータは、変換値算出手段と、変換値提供手段と、を備え、前記変換値算出手段で、前記生成した機器認証情報を所定の一方向性関数で変換して変換値を算出する変換値算出ステップと、前記変換値提供手段で、前記算出した変換値を前記提供サーバに提供する変換値提供ステップと、を備えるように構成することができる(第20の構成)。

また、第13の構成において、前記コンピュータは、前記取得した元情報を記憶する記憶手段を具備し、前記機器認証情報送信ステップでは、前記記憶した元情報を前記機器認証情報を生成して前記機器認証サーバに送信するように構成することができる(第21の構成)。

また、本発明は、前記目的を達成するために、提供サーバから提供される、機器認証情報を生成する元となる元情報を取得する元情報取得機能と、前記取得した元情報から機器認証情報を生成する生成機能と、機器認証時に、前記生成した機器認証情報を機器認証サーバに送信する機器認証情報送信機能と、をコンピュータで実現する機器認証情報処理プログラムを提供する(第22の構成)。

第22の構成において、前記元情報は、前記機器認証情報を暗号化した暗号化機器認証情報であり、前記生成機能は、前記暗号化機器認証情報を復号化することにより、前記機器認証情報を生成するように構成することができる(第23の構成)。

第22の構成において、前記生成機能で生成した機器認証情報を暗号化して記憶する記憶機能を実現し、前記機器認証情報送信機能は、前記記憶機能に記憶された機器認証情報を復号化して送信するように構成することができる(第24の構成)。

第24の構成において、前記記憶機能に記憶する機器認証情報の暗号化、及び復号化に使用する暗号鍵を、前記暗号鍵の使用時に前記端末機器に固有な情報を用いて生成する鍵生成機能をコンピュータで実現するように構成することもできる(第25の構成)。

また、第25の構成において、前記生成した暗号鍵を、前記暗号鍵の使用後の所定期間に消去する鍵消去機能をコンピュータで実現するように構成することもできる(第26の構成)。

第22の構成において、前記提供サーバから前記機器認証情報を所定の一方向性関数で変換した変換値を取得する変換値取得機能と、前記生成した機器認証情報を、前記一方向性関数で変換して変換値を算出する変換値算出機能と、前記取得した変換値と、前記算出した変換値の同一性を判断し、その判断結果を出力する判断機能と、をコンピュータで実現するように構成することができる(第27の構成)。

第27の構成において、前記生成した機器認証情報を他の一方向性関数で変換して変換値を算出する変換値算出機能と、前記算出した変換値を前記提供サーバに提供する変換値

10

20

30

40

50

提供機能と、をコンピュータで実現するように構成することができる（第28の構成）。

第22の構成において、前記生成した機器認証情報を所定の一方向性関数で変換して変換値を算出する変換値算出機能と、前記算出した変換値を前記提供サーバに提供する変換値提供機能と、をコンピュータで実現するように構成することができる（第29の構成）。

第22の構成において、前記取得した元情報を記憶する記憶機能をコンピュータで実現し、前記機器認証情報送信機能は、前記記憶した元情報から機器認証情報を生成して前記機器認証サーバに送信するように構成することができる（第30の構成）。

また、本発明は、前記目的を達成するために、提供サーバから提供される、機器認証情報を生成する元となる元情報を取得する元情報取得機能と、前記取得した元情報から機器認証情報を生成する生成機能と、機器認証時に、前記生成した機器認証情報を機器認証サーバに送信する機器認証情報送信機能と、をコンピュータで実現する機器認証情報処理プログラムを記憶したコンピュータが読み取り可能な記憶媒体を提供する（第31の構成）。

また、本発明は、前記目的を達成するために、端末機器に機器認証情報を生成する元となる元情報を提供する元情報提供手段と、前記機器認証情報、又は前記元情報を、前記端末機器の機器認証を行う機器認証サーバに提供する機器認証情報提供手段と、前記端末機器から、前記元情報から生成された機器認証情報の、所定の一方向性関数で変換した変換値を取得する変換値取得手段と、前記機器認証情報を前記一方向性関数で変換して変換値を算出する変換値算出手段と、前記取得した変換値と前記算出した変換値の同一性を判断し、その判断結果を出力する判断手段と、を具備したことを特徴とする提供サーバを提供する（第32の構成）。

第32の構成において、前記判断手段で出力された判断結果を、前記元情報の組込主体に送信する判断結果送信手段を具備するように構成することができる（第33の構成）。

また、本発明は、前記目的を達成するために、元情報提供手段と、機器認証情報提供手段と、変換値取得手段と、変換値算出手段と、判断手段と、を備えたコンピュータにおいて、端末機器に機器認証情報を生成する元となる元情報を、前記元情報提供手段で提供する元情報提供ステップと、前記機器認証情報、又は前記元情報を、前記機器認証情報提供手段で前記端末機器の機器認証を行う機器認証サーバに提供する機器認証情報提供ステップと、前記変換値取得手段で、前記端末機器から、前記元情報から生成された機器認証情報の、所定の一方向性関数で変換した変換値を取得する変換値取得ステップと、前記変換値算出手段で、前記機器認証情報を前記一方向性関数で変換して変換値を算出する変換値算出ステップと、前記判断手段で、前記取得した変換値と前記算出した変換値の同一性を判断し、その判断結果を出力する判断ステップと、から構成されたことを特徴とする機器認証情報提供方法を提供する（第34の構成）。

第34の構成において、前記コンピュータは、判断結果送信手段を備え、前記判断手段で出力された判断結果を、前記判断結果送信手段で前記元情報の組込主体に送信する判断結果送信ステップを備えるように構成することができる（第35の構成）。

また、本発明は、前記目的を達成するために、端末機器に機器認証情報を生成する元となる元情報を提供する元情報提供機能と、前記機器認証情報、又は前記元情報を、前記端末機器の機器認証を行う機器認証サーバに提供する機器認証情報提供機能と、前記端末機器から、前記元情報から生成された機器認証情報の、所定の一方向性関数で変換した変換値を取得する変換値取得機能と、前記機器認証情報を前記一方向性関数で変換して変換値を算出する変換値算出機能と、前記取得した変換値と前記算出した変換値の同一性を判断し、その判断結果を出力する判断機能と、をコンピュータで実現する機器認証情報提供プログラムを提供する（第36の構成）。

第36の構成において、前記判断機能で出力された判断結果を、前記元情報の組込主体に送信する判断結果送信機能をコンピュータで実現するように構成することができる（第37の構成）。

また、本発明は、前記目的を達成するために、端末機器に機器認証情報を生成する元と

10

20

30

40

50

なる元情報を提供する元情報提供機能と、前記機器認証情報、又は前記元情報を、前記端末機器の機器認証を行う機器認証サーバに提供する機器認証情報提供機能と、前記端末機器から、前記元情報から生成された機器認証情報の、所定の一方向性関数で変換した変換値を取得する変換値取得機能と、前記機器認証情報を前記一方向性関数で変換して変換値を算出する変換値算出機能と、前記取得した変換値と前記算出した変換値の同一性を判断し、その判断結果を出力する判断機能と、をコンピュータで実現する機器認証情報提供プログラムを記憶したコンピュータが読み取り可能な記憶媒体を提供する（第38の構成）。

【発明の効果】

【0010】

本発明によれば、機器内に機器認証情報を安全に組み込むことができる。また、機器内に機器認証情報が適切に組み込まれたことを機器認証情報の秘密状態を保持したまま確認することができる。

【発明を実施するための最良の形態】

【0011】

以下、本発明の好適な実施の形態について、図を参照して詳細に説明する。

[第1の実施の形態の概要]

図1は、第1の実施の形態の概要を説明するための図である。

機器認証情報を管理する管理サーバ7は、管理センタ3に設置されており、機器認証情報を暗号化して工場5に送信する。

接続手段10は、工場の作業者によりCE機器9のコネクタに接続され、管理サーバ7から送信してきた機器認証情報を暗号化されたままの状態でCE機器9に入力する。

CE機器9の内部には、暗号化された機器認証情報を復号化して格納するための書き込みモジュールが内蔵されている。

接続手段10から入力された機器認証情報は、書き込みモジュールにより復号化され、CE機器9内部の記憶装置に記憶される。

接続手段10は、従来例で使用している接続手段110とは異なり、管理サーバ7から送信してきた機器認証情報を復号化せずにCE機器9に入力する。

【0012】

このように、本実施の形態では、管理サーバ7（提供サーバ）から送信してきた機器認証情報が暗号化されたままCE機器9（端末機器）に入力されてCE機器9内部で復号化されるので、機器認証情報組み込み作業におけるセキュリティを高めることができる。

なお、以上の説明は、本実施の形態の基本的な概念を説明するためのものであり、各種の変形が可能である。

例えば、以下の実施の形態の詳細で説明するように、復号化した機器認証情報を他の暗号鍵で再度暗号化して記憶装置に記憶することにより、よりセキュリティを高めることができる。

また、本実施の形態では、CE機器9に機器認証情報が適切に組み込まれたことを工場5、及び管理センタ3が確認する手段も提供する。

【0013】

[第1の実施の形態の詳細]

図2は、CE機器の製造認証システム1の構成の一例を示した図である。製造認証システム1は、CE機器9の製造と機器認証を行うシステムであり、CE機器9にサービスを提供するサービスサーバなどは図示していない。

製造認証システム1は、事業体11、管理センタ3、工場5、CE機器9、機器認証サーバ8などから構成されている。

事業体11は、CE機器9の製造会社であり、CE機器9の企画、開発、販売など、CE機器9を市場に供給する事業体である。

管理センタ3は、CE機器9に組み込む機器認証情報の管理を行う部門であり、機器認証情報の発行や、機器認証情報に関する暗号情報を管理している。

10

20

30

40

50

【0014】

工場5は、事業体11からの依頼により、CE機器9の製造を行う部門である。工場5は、事業体11が有する場合もあるし、また、事業体11の委託を受けてCE機器9を製造する第三者が運営する工場である場合もある。

CE機器9は、工場5で製造されたCE機器であり、内部に管理センタ3が発行した機器認証情報が組み込まれている。

機器認証サーバ8は、管理センタ3から機器認証情報の提供を受けると共に、CE機器9から機器認証情報を受信してCE機器9を機器認証するサーバ装置である。

CE機器9は、機器認証サーバ8で機器認証されることにより、サービスサーバなどが提供するサービスを受けることができる。

10

【0015】

以下、製造認証システム1でCE機器9が製造されるプロセスを図中の番号を参照しながら説明する。

(1)まず、事業体11が、CE機器9の企画設計を行う。そして、管理センタ3から、CE機器9にインストールするファームウェアを作成するための情報を取得する。

このファームウェアは、機器認証情報を組み込むためのプログラムやCE機器9を動作させるためのプログラムなどから成り、工場5でCE機器9にインストールされる。事業体11は、管理センタ3からは、暗号鍵などの機器認証情報を組み込むための情報を取得する。

20

【0016】

(2)事業体11は、CE機器9の製造を工場5に依頼すると共に、CE機器9にインストールするファームウェアをCD-ROM(Compact Disc - Read Only Memory)に記録して送付したり、あるいは、ネットワークを介して送信するなどして工場5に渡す。

(3)工場5は、CE機器9を組み立てた後、事業体11から取得したファームウェアをCE機器9にインストールする。そして、CE機器9のコネクタに接続手段10(図1)を接続し、管理センタ3に対して機器認証情報の送信を要求する。

【0017】

(4)管理センタ3は、工場5からの要求に応じてCE機器9に組み込むための機器認証情報をネットワークを介して工場5に送信する。この機器認証情報は、暗号化されている。

30

この暗号化された機器認証情報は、復号化すると機器認証情報が得られるので、機器認証情報を生成するための元情報に該当する。機器認証情報の内容については後に詳細に説明する。

(5)工場5は、管理センタ3から送信してきた機器認証情報を接続手段10を介してCE機器9に入力する。機器認証情報は、CE機器9のファームウェアが提供する暗号鍵によりCE機器9内で復号化された後、ファームウェアが提供する他の暗号鍵により再び暗号化されて記憶装置に記憶される。

(6)そして、後述する方法により、CE機器9に機器認証情報が正しく組み込まれたか否かを、工場5と管理センタ3が確認する。これを用いて、工場5が管理センタ3に製造実績報告を行うことができる。

40

【0018】

(7)工場5は、CE機器9の組み立て、及び機器認証情報の組み込みを完了した後、CE機器9を出荷する。

(8)管理センタ3は、CE機器9の機器認証情報を機器認証サーバ8に提供する。

(9)機器認証サーバ8は、CE機器9から機器認証情報を送信してもらい、これを管理センタ3から提供された機器認証情報と比較することによりCE機器9を機器認証する。

【0019】

図3は、機器認証部99の一例を示した図である。機器認証部99は、工場5でファームウェアをインストールすることにより、CE機器9の内部で構成された機能部である。

50

機器認証部 9 9 は、認証モジュール 2 0 、書き込みモジュール 3 0 、認証情報メモリ 4 0 、本体識別情報メモリ 5 0 などから構成されている。

【 0 0 2 0 】

認証モジュール 2 0 は、C E 機器 9 を機器認証サーバ 8 で機器認証するための機能部である。

認証モジュール 2 0 は、機器認証サーバ 8 に認証情報を送信する際に使用する公開鍵 2 1 、固有鍵 2 3 を生成するための固有鍵生成子 2 2 を備えている。

【 0 0 2 1 】

固有鍵 2 3 は、認証情報メモリ 4 0 に記憶する機器認証情報を暗号化、及び復号化するための鍵情報であり、使用時に固有鍵生成子 2 2 と M A C アドレス 5 1 から動的に生成される。
10

M A C アドレス 5 1 は、C E 機器 9 に固有の情報である。そして、固有鍵 2 3 も C E 機器 9 に固有の鍵情報となるように構成されている。

本実施の形態では、一例として M A C アドレス 5 1 を用いて固有鍵 2 3 を生成するが、この他に、i . L i n k (I E E E 1 3 9 4) のアドレスなど、C E 機器 9 に固有な情報であればよい。

【 0 0 2 2 】

即ち、C E 機器 9 に固有な情報を用いて、C E 機器 9 に固有な固有鍵 2 3 が生成されるようになっている。

このように、製造される各 C E 機器 9 に組み込む固有鍵生成子 2 2 が共通であっても、生成される固有鍵 2 3 は、各 C E 機器 9 に固有なものとなり、固有鍵生成子 2 2 の管理が容易になる。
20

このように構成された認証モジュール 2 0 は、機器認証時に認証情報メモリ 4 0 から機器認証情報を読み出して復号化し、機器 I D 4 1 と共に機器認証サーバ 8 に送信する。

固有鍵 2 3 は、使用された後、所定期間内に速やかに消去される。所定期間は、例えば、機器認証情報を復号化してから機器認証部 9 9 が機器認証を終えるまでなど、各種の設定が可能である。

なお、本実施の形態では、固有鍵 2 3 は、使用後に消去されるように構成したが、必ずしも消去する必要はない。

【 0 0 2 3 】

書き込みモジュール 3 0 は、工場 5 で C E 機器 9 に機器認証情報を書き込むための機能部である。
30

書き込みモジュール 3 0 は、書き込み前鍵 3 1 、固有鍵生成子 3 2 、機器側確認ハッシュ関数 3 4 、サーバ側確認ハッシュ関数 3 5 などを備えている。

書き込み前鍵 3 1 は、管理センタ 3 から送信されてきた暗号化された機器認証情報を復号化するための鍵情報である。

固有鍵生成子 3 2 は、固有鍵 3 3 を生成するための元（シード）となる情報であり、認証モジュール 2 0 の固有鍵生成子 2 2 と同じものである。

【 0 0 2 4 】

固有鍵 3 3 は、書き込み前鍵 3 1 によって復号化された機器認証情報を暗号化するための鍵情報であり、固有鍵生成子 3 2 と、M A C アドレス 5 1 から使用時に動的に生成される。固有鍵 3 3 は、認証モジュール 2 0 で生成される固有鍵 2 3 と同じものである。
40

このように構成された書き込みモジュール 3 0 は、管理センタ 3 から送信されてきた機器認証情報を書き込み前鍵 3 1 で復号化し、固有鍵 3 3 で再度暗号化して認証情報メモリ 4 0 に記憶する。

【 0 0 2 5 】

本実施の形態では、機器認証情報を固有鍵 3 3 にて暗号化された状態で記憶することによりセキュリティを高めている。

なお、書き込み前鍵 3 1 で復号化した機器認証情報を暗号化せずに記憶装置に記憶するよう構成することもできる。この場合は、認証モジュール 2 0 は、認証時に機器認証情報を
50

復号化する必要がないので固有鍵 2 3 を生成する必要はない。

【 0 0 2 6 】

機器側確認ハッシュ関数 3 4 は、機器認証情報が適切に認証情報メモリ 4 0 に記憶されたことを書込モジュール 3 0 が確認するための関数である。後述するように、書込モジュール 3 0 は、管理センタ 3 から送信されてきたハッシュ値と、機器側確認ハッシュ関数 3 4 による機器認証情報のハッシュ値を比較することにより機器認証情報が組み込まれたことを確認する。

【 0 0 2 7 】

サーバ側確認ハッシュ関数 3 5 は、機器認証情報が適切に認証情報メモリ 4 0 に記憶されたことを管理センタ 3 側が確認するための関数である。

後述するように、書込モジュール 3 0 は、認証情報メモリ 4 0 に記憶した機器認証情報のサーバ側確認ハッシュ関数 3 5 によるハッシュ値を管理センタ 3 に送信する。

これに対し、管理センタ 3 は、発行した機器認証情報のサーバ側確認ハッシュ関数によるハッシュ値を生成し、書込モジュール 3 0 から取得したハッシュ値と比較することにより、機器認証情報が C E 機器 9 に組み込まれたことを確認する。

【 0 0 2 8 】

本実施の形態では、C E 機器 9 側で確認するための機器側確認ハッシュ関数 3 4 と、管理サーバ 7 側手確認するためのサーバ側確認ハッシュ関数 3 5 の 2 種類を用意した。

仮に、同じハッシュ関数を用いて C E 機器 9 側での確認と管理サーバ 7 側での確認を行うとすると、管理サーバ 7 が C E 機器 9 に送信したハッシュ値を第三者がそのまま管理サーバ 7 に返送した場合、管理サーバ 7 が、このハッシュ値が C E 機器 9 から送信されたものか、あるいは第三者から返送されたものか確認するのが困難である。

そのため、2 種類のハッシュ関数を用いることにより、第三者によるなりすましを防止することができる。

【 0 0 2 9 】

ところで、ハッシュ関数とは、電子文書をハッシュ化するための関数であり、電子文書をハッシュ化することにより電子文書から電子文書に固有な文字列（ハッシュ値、又はダイジェストメッセージとも呼ばれる）を生成することができる。

同じ電子文書からは同じハッシュ値が得られる。電子文書が一部でも変更されると、この文書のハッシュ値は、変更前のものと異なる。

更に、ハッシュ値を逆変換して元の電子文書を得ることは大変困難である。

このように、ハッシュ関数は、順方向の変換は容易であるが、変換後の値から元の値を得る逆変換が困難である一方向性関数と呼ばれる関数の一種である。

このように、秘密情報の確認する側と確認される側の双方で秘密情報のハッシュ値を生成し、これを比較することにより秘密情報の秘密状態を保ったまま、秘密情報の同一性を確認することができる。

【 0 0 3 0 】

認証情報メモリ 4 0 は、機器認証情報などの機器認証を行う際に使用する情報を記憶する記憶装置である。

本実施の形態では、認証情報メモリ 4 0 には、機器 I D 4 1 、暗号化（機器 I D + パスフレーズ）4 2 が記憶されている。

機器 I D 4 1 は、C E 機器 9 を識別するための I D 情報であって、工場 5 が機器 I D 管理機関から予め取得し、C E 機器 9 に書き込んだものである。

暗号化（機器 I D + パスフレーズ）4 2 は、機器 I D 4 1 の後尾にパスフレーズを配置したものと固有鍵 2 3 、又は固有鍵 3 3 で暗号化したものである。なお、配置の順序は、逆でもよい。

以降、ある情報 A の後尾にある情報 B を配置した情報を（情報 A + 情報 B ）などと表すことにして、更に（情報 A + 情報 B ）を暗号化した情報を暗号化（情報 A + 情報 B ）などと表すことにする。

【 0 0 3 1 】

10

20

30

40

50

例えば、機器 ID 4 1 を「1 2 3」とし、パスフレーズを「a b c」とした場合、(機器 ID + パスフレーズ)は、「1 2 3 a b c」となる。そして、これを固有鍵 2 3、又は固有鍵 3 3 で暗号化したものが暗号化(機器 ID + パスフレーズ) 4 2 となる。

パスフレーズは、工場 5 が CE 機器 9 に機器認証情報を組み込む際に管理サーバ 7 が発行した秘密情報である。

本実施の形態では、(機器 ID + パスフレーズ)を機器認証情報として使用する。

このように、パスフレーズに機器 ID を組み合わせることにより機器認証情報のデータ量が多くなるため、第三者による暗号化(機器 ID + パスフレーズ) 4 2 の解読が困難となり、セキュリティを高めることができる。

また、復号化された(機器 ID + パスフレーズ)と、送られてくる機器 ID を CE 機器 9 内で比較することにより、機器 ID と暗号化(機器 ID + パスフレーズ)の組合せが正しいことを検証することもできる。10

【0 0 3 2】

本体識別情報メモリ 5 0 は、CE 機器 9 の本体を識別するための情報が記憶されている。

本体を識別するための情報としては、ネットワーク上で CE 機器 9 を識別するための CE 機器 9 に固有な情報である MAC (Media Access Control) アドレス 5 1 や、 link などと呼ばれる情報などがある。

MAC アドレス 5 1 は、CE 機器 9 にユニークなハードウェアアドレスであって、例えネットワーク上で CE 機器 9 を移動したとしても変わらない。20

【0 0 3 3】

次に、以上のように構成された CE 機器 9 に機器認証情報を組み込む手順、組み込んだ機器認証情報を確認する手順、組み込んだ機器認証情報を用いて機器認証を行う手順についてフローチャートを用いて説明する。

【0 0 3 4】

図 4 は、CE 機器 9 に機器認証情報を組み込む準備段階での作業手順を説明するためのフローチャートである。

まず、事業体 1 1 が CE 機器 9 を企画する(ステップ 1 0)。この作業は、企画担当者などの人手により行われるものである。

次に、事業体 1 1 に設置された事業体システムから管理サーバ 7 にアクセスし、CE 機器 9 の書きモジュール 3 0 に組み込むための書き前鍵 3 1 を要求する(ステップ 1 2)。30

【0 0 3 5】

管理サーバ 7 は、図 8 に示したような鍵テーブル 7 0 0 を備えており、鍵テーブル 7 0 0 から書き前鍵 3 1 とこの書き前鍵 3 1 を他の書き前鍵から識別する鍵識別子を発行する。そして発行した書き前鍵 3 1 と鍵識別子を共に事業体システムに送信する(ステップ 2 0)。

また、事業体 1 1 は、製品の機種を特定する製品コードと後述する固有鍵生成子を管理サーバに要求するように構成することもできる。

管理サーバ 7 は、製品コードと固有鍵生成子が対応付けて管理している。

【0 0 3 6】

事業体システムは、管理サーバ 7 から書き前鍵 3 1 と鍵識別子を受信し、書き前鍵 3 1 を書きモジュール 3 0 に組み込むように構成されたファームウェアを作成する(ステップ 1 4)。また、後述する固有鍵生成子もファームウェアに組み込む。

次に、事業体システムは、作成したファームウェアと鍵識別子、及び CE 機器 9 の機種を特定する製品コードを工場 5 に設置された工場システムに送信する(ステップ 1 6)。

なお、工場 5 では、製品コードで特定される CE 機器 9 を複数台生産するが、何れの CE 機器 9 も同じ書き前鍵 3 1 を使用するものとする。そのため、ファームウェアと鍵識別子は一組工場に送信され、この一組のファームウェアと鍵識別子から複数台の CE 機器 9 が生産される。

【0 0 3 7】

10

20

30

40

50

工場システムは、事業体システムからこれらの情報を受信する。そして工場5は、受信した製品コードで特定されるCE機器9の製造を開始する。

このようにして製造されたのCE機器9(ファームウェア組み込み前)に対して工場システムは製品シリアル番号を発番する(ステップ30)。

製品シリアル番号は、個々のCE機器9に対して固有な番号であり、例えば、ラベルシールに数字やバーコードなどとして印刷され、CE機器9に外部から参照可能に貼付される。

【0038】

なお、本実施の形態では、製品シリアル番号がCE機器9を特定できる情報であるとするが、例えば、製品コードと製品シリアル番号を用いてCE機器9を特定できるように構成することもできる。10

この場合は、機器認証サーバ8は、製品コードと製品シリアル番号をCE機器9に貼付する。

即ち、CE機器9を特定できる情報であればよい。

【0039】

次に、工場システムは、CE機器9にファームウェアを組み込む(ステップ32)。

ファームウェアの組み込みは、CE機器9のコネクタからファームウェアを入力することにより行われる。

また、事業体11がファームウェアをCD-ROMなどの記憶媒体に記憶させて工場5に送付し、工場5でこれをCE機器9に読み込ませるために構成することもできる。20

【0040】

ファームウェアの組み込みにより、機器認証部99(図3)がCE機器9の内部に形成される。

なお、工場システムは、ファームウェア組み込みの際に、予め機器ID管理機関から取得しておいた機器ID41を認証情報メモリ40に記憶させる。ただし、この段階では認証情報メモリ40には暗号化(機器ID+パスフレーズ)42は記憶されていない。

【0041】

図5は、CE機器9に機器認証情報を組み込む(埋め込む)手順(即ち、認証情報メモリ40に暗号化(機器ID+パスフレーズ)42を記憶させる手順)を説明するためのフローチャートである。30

なお、以下の処理は、CE機器9に接続手段10が接続された状態で行う。

【0042】

工場システムは、図8に示したような鍵識別子管理テーブル500を備えており、製品(製品コード)と事業体システムから取得した鍵識別子を対応付けて管理している。

そして、工場システムは、管理サーバ7にアクセスし、パスフレーズの発行を要求すると共に、先に取得した機器ID41と鍵識別子管理テーブル500に記憶されているCE機器9の鍵識別子を送信する(ステップ40)。

【0043】

管理サーバ7は、パスフレーズの発行要求を受けてパスフレーズを発行する(ステップ50)。

なお、パスフレーズとは、文字や数字、あるいは記号などの文字列からなる秘密情報であって、パスワードと同種の情報である。

このような秘密情報のうち、文字列の比較的短いものをパスワードと呼び、比較的長いものをパスフレーズと呼んでいる。暗号化した場合に、文字列が長いほど第三者による解読が困難になる。

【0044】

次に、管理サーバ7は、工場システムから受信した鍵識別子に対応する書込前鍵31を鍵テーブル700(図8)から取得する。

そして、工場システムから受信した機器ID41とステップ50で発行したパスフレーズから(機器ID+パスフレーズ)を生成し、先に取得した書込前鍵31にてこれを暗号4050

化して暗号化（機器ID + パスフレーズ）42を生成する（ステップ52）。

この暗号化（機器ID + パスフレーズ）が機器認証情報として使用される。

【0045】

管理サーバ7は、CE機器9と同様に、機器側確認ハッシュ関数34と、サーバ側確認ハッシュ関数35を備えており、機器側確認ハッシュ関数34を用いて先に生成した（機器ID + パスフレーズ）のハッシュ値（第1のハッシュ値）を生成する（ステップ54）。

この第1のハッシュ値は、機器認証情報が適切に組み込まれたか否かをCE機器9内部で判断する際に使用される。

なお、サーバ側確認ハッシュ関数35は、後に、CE機器9に機器認証情報が適切に組み込まれたか否かを管理サーバ7が判断する際に使用される。 10

【0046】

管理サーバ7は、機器ID41、生成した暗号化（機器ID + パスフレーズ）42、及び第1のハッシュ値を工場システムに送信する（ステップ56）。これは、元情報提供手段に対応する。

なお、管理サーバ7は、図8に示した発行済み機器認証情報テーブル702を記憶しており、機器ID41、暗号化（機器ID + パスフレーズ）42、第1のハッシュ値を工場システムに送信すると共に、発行済み機器認証情報テーブル702を更新する。 10

これにより、発行したパスフレーズと、機器ID41、鍵識別子を対応付けることができる。 20

【0047】

工場システムは、これらの情報を管理サーバ7から受信し、これらの情報を接続手段10を介してCE機器9に入力する（ステップ42）。

すると、CE機器9内部では、書込モジュール30がこれらの情報を受信する（ステップ60）。これは、暗号化（機器ID + パスフレーズ）42は、元情報に対応し、そのため書込モジュール30は、元情報取得手段を備えている。

また、第1のハッシュ値は、機器認証情報を一方向性関数で変換した変換値に対応し、そのため、書込モジュール30は、変換値取得手段を備えている。 30

【0048】

次に、書込モジュール30は、書込前鍵31を用いて暗号化（機器ID + パスフレーズ）42を復号化する（ステップ62）。 30

この復号化により、CE機器9は、管理センタ3から取得した機器認証情報、即ち（機器ID + パスフレーズ）を得ることができる。

このように、書込モジュール30は、元情報から機器認証情報を生成する生成手段を有している。 40

【0049】

CE機器9は、復号化した（機器ID + パスフレーズ）をそのまま保持してもよいが、本実施の形態では、セキュリティを高めるため、（機器ID + パスフレーズ）を再度暗号化して保持することにする。

そのため、書込モジュール30は、まず、MACアドレス51と固有鍵生成子32から固有鍵33を生成する（ステップ64）。 40

このステップは、CE機器9に固有の暗号化鍵を得ることが目的であって、一例としてMACアドレス51を用いて固有鍵33を生成するが、これに限定するものではなく、CE機器9に固有の情報であれば（例えば、製品シリアル番号）何でもよい。

また、後述するように、認証モジュール20も固有鍵33と同じ暗号化鍵を生成することができ、書込モジュール30、認証モジュール20は、共に鍵生成手段を有している。

【0050】

次に、書込モジュール30は、生成した固有鍵33を用いて（機器ID + パスフレーズ）を暗号化して暗号化（機器ID + パスフレーズ）42を生成する（ステップ66）。 50

なお、暗号化に使用する暗号鍵が異なるので、暗号化（機器ID + パスフレーズ）42

と、管理サーバ7が送信してきた暗号化（機器ID+パスフレーズ）は、異なるものである。

【0051】

次に、書き込みモジュール30は、生成した暗号化（機器ID+パスフレーズ）42を認証情報メモリ40に書き込み（ステップ68）、認証情報メモリ40は、暗号化（機器ID+パスフレーズ）42を記憶する（ステップ70）。

なお、固有鍵33は、機器認証部99が固有鍵33を消去するように構成されている場合は、使用された後、速やかに消去される（鍵消去手段）。

このように、暗号化（機器ID+パスフレーズ）42は、CE機器9に固有であり、しかも動的に生成される固有鍵33により暗号化されているので、セキュリティを高めることができる。10

また、認証情報メモリ40は、記憶手段を構成している。

【0052】

以上の手順により、管理サーバ7が発行した機器認証情報をCE機器9に組み込むことができる。

更に、機器認証情報は、暗号化された状態のままCE機器9に入力されるので、機器認証情報が工場5で漏出することを未然に防ぐことができ、機器認証情報組み込み時のセキュリティを高めることができる。

更に、機器認証情報は、CE機器9に固有な暗号鍵で暗号化した状態でCE機器9に記憶されるので、CE機器9を出荷した後にCE機器9から機器認証情報が漏出することを未然に防ぐことができ、出荷後のセキュリティも高めることができる。20

【0053】

図6は、CE機器9に機器認証情報が適切に組み込まれたことを管理センタ3、及び工場5が確認する手順を説明するためのフローチャートである。

この手順は、CE機器9のコネクタに接続手段10が接続した状態で行われる。通常は、工場システムがCE機器9に機器認証情報を組み込んだ後、自動的に行われる。

【0054】

まず、機器認証部99において、書き込みモジュール30が認証情報メモリ40から暗号化（機器ID+パスフレーズ）42を読み出し、認証情報メモリ40から書き込みモジュール30へ暗号化（機器ID+パスフレーズ）42が提供される（ステップ90）。30

次に、書き込みモジュール30は、固有鍵生成子32と、MACアドレス51から固有鍵33を生成し（ステップ100）、これを用いて暗号化（機器ID+パスフレーズ）42を復号化する（ステップ102）。

【0055】

次に、書き込みモジュール30は、機器側確認ハッシュ関数34を用いて、復号化した（機器ID+パスフレーズ）のハッシュ値（第1のハッシュ値）を生成する（ステップ104）。

次に、書き込みモジュール30は、管理サーバ7から送信してきた第1のハッシュ値と、ステップ104で生成したハッシュ値を比較し、これらのハッシュ値が一致するか否かの比較結果を得る（ステップ106）。

このように、書き込みモジュール30は、変換値（第1のハッシュ値）算出手段と、判断手段を備えている。

【0056】

ハッシュ値が一致することにより、管理サーバ7が生成した（機器ID+パスフレーズ）が、認証情報メモリ40に記憶されている（機器ID+パスフレーズ）と同一のものであることを確認することができる。

【0057】

次に、書き込みモジュール30は、サーバ側確認ハッシュ関数35を用いて（機器ID+パスフレーズ）のハッシュ値（第2のハッシュ値）を生成する（ステップ108）。

そして、書き込みモジュール30は、認証情報メモリ40から機器ID41を読み出し、ス50

ステップ106における第1のハッシュ値の比較結果、機器ID、第2のハッシュ値を工場システムに出力する(ステップ110)。そして、第2のハッシュ値は、管理サーバ7に送信される。

このように、書き込みモジュール30は、変換値算出手段と、変換値提供手段を備えている。

【0058】

工場は、CE機器9から出力された比較結果により、機器認証情報がCE機器9に適切に組み込まれたか否かを知ることができる。

ハッシュ値が一致しなかった場合は、機器ID41を廃棄し、新たな機器IDを採用して再度機器認証情報の組み込みを試みる。

組み込みに失敗した機器ID41を再度利用することも可能であるが、手違いなどにより同じ機器IDのCE機器9が複数市場に出回るのを防止するため、本実施の形態では、組み込みに失敗した機器ID41は廃棄するものとした。

【0059】

なお、従来の製造工程では、機器認証情報の機密性を保つため、一端CE機器9に組み込んだ後は、適切に機器認証情報が組み込まれたか否かを調べることは困難であり、確認を行わない場合もあった。

しかし、本実施の形態では、機器認証情報のハッシュ値をCE機器9内部で比較することにより、機器認証情報の機密性をCE機器9内部で保ったまま機器認証情報が組み込まれたか否かを調べることができる。

【0060】

工場システムは、機器認証情報が適切にCE機器9に組み込まれたことを確認した後、CE機器9から得た機器ID41と第2のハッシュ値に、CE機器9の製品シリアル番号を附加して管理サーバ7に送信する(ステップ120)。

【0061】

管理サーバ7は、これらの情報を工場システムから受信し、発行済み機器認証情報テーブル702(図8)を用いて機器ID41からパスフレーズを検索する(ステップ130)。

このように、管理サーバ7は、変換値(第2のハッシュ値)取得手段を備えている。

次に、管理サーバ7は、機器ID41と検索したパスフレーズから(機器ID+パスフレーズ)を生成し、これからサーバ側確認ハッシュ関数35を用いて第2のハッシュ値を生成する(変換値算出手段)。

【0062】

そして、工場システムから受信した第2のハッシュ値と、先に生成した第2のハッシュ値が一致するか否かを判断する(判断手段)(ステップ132)。

第2のハッシュ値が一致することにより、管理サーバ7は、CE機器9に対する機器認証情報の組み込みが成功したことを知ることができる。

逆に第2のハッシュ値が一致しなかった場合、機器認証情報の組み込みが失敗したことを知ることができる。

【0063】

管理サーバ7は、図8に示したような機器認証テーブル704を備えており、機器ID41、パスフレーズ、製品シリアル番号を対応付けて記憶している。

第2のハッシュ値が一致した場合、管理サーバ7は、機器ID41と製品シリアル番号をパスフレーズと共に紐付けて機器認証テーブル704に記憶する(ステップ134)。

なお、機器認証テーブル704は、機器認証サーバ8に提供され、機器認証サーバ8が機器認証を行うのに利用される(機器認証情報提供手段)。

【0064】

次に、管理サーバ7は、工場システムから受信したデータ(機器ID41、製品シリアル番号、第2のハッシュ値)に、データを受信した日の日付情報を附加して秘密鍵で署名(電子署名)して工場に送信する(判断結果送信手段)(ステップ136)。

10

20

30

40

50

工場システム（元情報組込主体）は、これを受信し、機器認証情報が適切に C E 機器 9 に組み込まれたことを確認する（ステップ 122）。

これにより、工場システム側では、管理サーバ 7 に機器 ID 41、製品シリアル番号、第 2 のハッシュ値（これらを以て製造実績とすることができる）を受け取ってもらえたことを確認することができる。

そして、工場 5 は、製造が完了した C E 機器 9 を出荷する。

【0065】

図 7 は、機器認証サーバ 8 が C E 機器 9 を機器認証する手順を説明するためのフローチャートである。

まず、機器認証部 99（図 3）の認証モジュール 20 が、認証情報メモリ 40 から暗号化（機器 ID + パスフレーズ）42 を読み出し、認証情報メモリ 40 から認証モジュール 20 に暗号化（機器 ID + パスフレーズ）42 が提供される（ステップ 140）。 10

【0066】

次に、認証モジュール 20 は、固有鍵生成子 22 と MAC アドレス 51 を用いて固有鍵 23 を生成する（ステップ 150）。

そして認証モジュール 20 は、暗号化（機器 ID + パスフレーズ）42 を固有鍵 23 を用いて復号化して（機器 ID + パスフレーズ）を取得し（ステップ 152）、機器認証サーバ 8 に送信する（ステップ 154）。このように、認証モジュール 20 は、機器認証情報送信手段を備えている。

なお、C E 機器 9 と機器認証サーバ 8 の間の通信経路は、例えば、SSL（Secure Sockets Layer）などの暗号化技術を使ってセキュアなものとなっている。 20

【0067】

機器認証サーバ 8 は、C E 機器 9 から（機器 ID + パスフレーズ）を受信し、これを公開鍵 21 に対応する秘密鍵で復号化し、管理センタ 3 から提供された機器認証テーブル 704 のパスフレーズと照合して C E 機器 9 を機器認証する（ステップ 160）。

更に、機器認証テーブル 704 を用いて C E 機器 9 の製品シリアル番号を特定する（ステップ 162）。

以上の手順により機器認証処理は行われる。

【0068】

図 9 は、C E 機器 9 のハードウェア的な構成の一例を示した図である。 30
CPU（Central Processing Unit）121 は、ROM（Read Only Memory）122 に記憶されているプログラムや、記憶部 128 から RAM（Random Access Memory）123 にロードされたプログラムに従って各種の処理を実行する中央処理装置である。

【0069】

ROM 122 は、C E 機器 9 を機能させる上で必要な基本的なプログラムやパラメータなどから構成されている。

RAM 123 は、CPU 121 が各種の処理を実行する上で必要なワーキングエリアを提供する。 40

【0070】

記憶部 128 は、C E 機器 9 が機能するために必要な各プログラムやデータを記憶しており、例えば、ハードディスクや半導体メモリなどの記憶装置により構成されている。

事業体 11 で作成されたファームウェアは、工場 5 で記憶部 128 に記憶され、このファームウェアが CPU 121 で実行されることにより、機器認証部 99（図 3）の各構成要素が生成される。

記憶部 128 に記憶されている他のプログラムとしては、ファイルの入出力を行ったり、C E 機器 9 の各部を制御したりなど、基本的な機能を実現するための OS（Operating System）などがある。

【0071】

C P U 1 2 1、R O M 1 2 2、及びR A M 1 2 3は、バス1 2 4を介して相互に接続されている。このバス1 2 4には、出入力インターフェース1 2 5も接続されている。

出入力インターフェース1 2 5には、キーボード、マウスなどによる入力部1 2 6、C R T (C a t h o d e - r a y T u b e)、L C D (L i q u i d C r y s t a l D i s p l a y)などによるディスプレイ、並びにスピーカなどにより出力部1 2 7、ハードディスクなどにより構成される記憶部1 2 8、モデム、ターミナルアダプタなどにより構成される通信部1 2 9が接続されている。

通信部1 2 9は、ネットワークを介しての通信処理を行う機能部であり、例えば、接続手段1 0と接続して機器認証情報の入力を受け付けたり、あるいは、機器認証サーバ8と接続して機器認証を行うための通信を行ったりする。

10

【0072】

また、出入力インターフェース1 2 5には、必要に応じてドライブ1 3 0が接続され、磁気ディスク1 4 1、光ディスク1 4 2、光磁気ディスク1 4 3、又はメモリカード1 4 4などが適宜装着され、それから読み出されたコンピュータプログラムが、必要に応じて記憶部1 2 8にインストールされる。

なお、管理サーバ7、機器認証サーバ8の構成は基本的にC E機器9と同様であるので説明は省略する。

【0073】

以上に説明した第1の実施の形態により、機器認証の際に必要となる機器認証情報（機器I D + パスフレーズ）を、管理サーバ7からC E機器9へ安全に送信することができる。また、機器認証情報が正しく書き込まれたことを工場5や管理サーバ7が確認することが可能となる。

20

【0074】

以上に説明した第1の実施の形態による効果を従来の問題点と対比しながら列挙すると以下のようになる。

(1) 従来は、機器認証情報である（機器I D + パスフレーズ）が平文でC E機器9に入力されていたため、意図の如何に関わらず工場5の作業者などの目に触れてしまう可能性があった。これに対し、本実施の形態では、この問題を（機器I D + パスフレーズ）を暗号化したままC E機器9に入力することにより対応した。

30

【0075】

(2) 従来は、例え機器認証情報を暗号化して工場5に送信したとしても、製品ごと、工場ごとに機器認証情報の組み込み方式の統一が取れず、セキュリティレベルのばらつきを生んでしまう可能性があった。これに対し、本実施の形態では、機器認証情報の組み込み方式を共通化することにより、セキュリティレベルのばらつきを軽減することができる。

(3) 従来は、暗号化鍵が漏出することにより他のC E機器9に影響が及ぶ場合があった。これに対し、本実施の形態では、C E機器9ごとに固有な固有鍵2 3を生成することにより例え固有鍵2 3が漏出したとしても他のC E機器9に影響が及ぶことはない。

また、書込前鍵3 1に関しては、鍵の単位を製品ごとや時期ごとなどにすることで影響範囲を限定することができる。

40

【0076】

(4) 従来は、C E機器9内に正しく機器認証情報が書き込まれたことを工場5や、機器認証情報の発行元である管理センタ3が確認するのは困難であった。これに対し、本実施の形態では、ハッシュ値などの固有情報を使って工場5や管理センタ3が機器認証情報が正しく組み込まれたことを確認することができる。

(5) 従来は、管理センタ3が、正しく実績報告を受け取ったことを工場5が確認することは困難であった。これに対し、本実施の形態では、管理サーバ7が工場システムから受信したデータに日時情報を付加して電子署名し、これを工場システムに送信するようにした。

(6) 従来は、機器認証情報として、電子証明書などの他の情報を用いることは困難であった。これに対し本実施の形態は、電子証明書を使った認証方式にも適用することができ

50

る。

【0077】

なお、本実施の形態では、一例として、機器認証情報をネットワーク経由で工場5に送信して接続具10からCE機器9に入力したが、機器認証情報は暗号化したままCE機器9に入力されるので、例えば、CD-ROMなどの記憶媒体に記憶して工場5に送付し、工場5において記憶媒体からCE機器9に機器認証情報を書き込むように構成してもよい。

更に、本実施の形態では、一例として、管理サーバ7から送信されてきた暗号化（機器ID+パスフレーズ）を書き前鍵で複合化した後に認証情報メモリ40に記憶するように構成したが、この他に、管理サーバ7から送信されてきた暗号化（機器ID+パスフレーズ）を復号化せずに認証情報メモリ40に記憶し、機器認証時に書き前鍵で復号化するように構成することもできる。10

【0078】

次に、第2の実施の形態について説明する。

[第2の実施の形態の概要]

図10は、第2の実施の形態の概要を説明するための図である。

本実施の形態では、機器認証情報を生成する元となる元情報を管理サーバ7とCE機器9で同じロジックを用いて（例えば、同じ暗号鍵を用いて同じ暗号方式により暗号化して）変換し、機器認証情報を生成する。20

【0079】

まず、管理サーバ7は、元情報を工場5に送信すると共に、元情報を変換して機器認証情報を生成する。

一方、工場5では、接続手段10を介して元情報をCE機器9に入力する。CE機器9は、入力された元情報を変換して機器認証情報を生成する。

以上のようにして、管理サーバ7とCE機器9は、機器認証情報を共有することができる。

また、仮に元情報が外部に漏出したとしてもロジックを知らなければ機器認証情報を知ることはできない。30

【0080】

以上のように、機器認証情報は、CE機器9の内部で生成されるため、工場5において、平文で出力されるのを防ぐことができる。

【0081】

[第2の実施の形態の詳細]

製造認証システム1の構成（図2）、及び機器認証部99（図3）は、第1の実施の形態と同様であるので説明を省略する。

また、第1の実施の形態と同じ構成要素には同じ符号を付して説明する。

以下に、CE機器9への機器認証情報の組み込み、組み込みの確認、及び機器認証の方法についてフローチャートを用いて説明する。

なお、CE機器9に機器認証情報を組み込む前準備は、第1の実施の形態と同様であるので（図4）説明を省略する。40

管理サーバ7は、第1の実施の形態と同様に、図14に示したような鍵テーブル706を備えており、鍵識別子と書き前鍵31を対応付けて管理している。

【0082】

図11は、CE機器9に機器認証情報を組み込む手順を説明するためのフローチャートである。

CE機器9は、既に組み立てがなされており、コネクタに接続手段10が接続された状態になっているものとする。

まず、工場システムは、管理サーバ7に対してパスフレーズの発行を要求すると共に、予め機器ID管理機関から取得しておいた機器ID41を管理サーバ7に送信する（ステップ200）。50

なお、この機器 I D 4 1 は認証情報メモリ 4 0 にも記憶させる。

【0083】

これに対して、管理サーバ 7 は、パスフレーズを発行する（ステップ 210）。

管理サーバ 7 は、図 14 に示したような発行済み機器認証情報テーブル 708 を備えており、工場システムから受信した機器 I D 4 1 と、この機器 I D 4 1 に対して発行したパスフレーズを対応付けて記憶している。

そして、管理サーバ 7 は、パスフレーズを発行した後、機器 I D 4 1 とパスフレーズを紐付けて発行済み機器認証情報テーブル 708 に記憶する（ステップ 212）。

【0084】

次に、管理サーバ 7 は、機器 I D 4 1 とパスフレーズから（機器 I D + パスフレーズ）10 を生成し、工場システムに送信する（ステップ 214）。

この（機器 I D + パスフレーズ）が機器認証情報を生成するための元情報となる。

工場システムは、管理サーバ 7 から（機器 I D + パスフレーズ）を受信し（ステップ 202）、接続手段 10 を介して C E 機器 9 に入力する（ステップ 204）。

【0085】

C E 機器 9 内部では、書き込みモジュール 30 が（機器 I D + パスフレーズ）を受信し（ステップ 220）、書き込み前鍵 31 を用いてこれを暗号化して暗号化（機器 I D + パスフレーズ）42 を生成する（ステップ 222）。

本実施の形態では、（機器 I D + パスフレーズ）を元情報として暗号化（機器 I D + パスフレーズ）42 を生成し、暗号化（機器 I D + パスフレーズ）42 を機器認証情報として使用する。20

即ち、（機器 I D + パスフレーズ）を、書き込み前鍵 31 を用いた変換式により変換し、変換後の値である暗号化（機器 I D + パスフレーズ）42 を機器認証情報として使用する。

【0086】

次に、書き込みモジュール 30 は、固有鍵生成子 32 と MAC アドレス 51 から固有鍵 33 を生成し（ステップ 224）、生成した固有鍵 33 によって、暗号化（機器 I D + パスフレーズ）42 を再度暗号化する（ステップ 226）。

これは、本実施の形態では、暗号化（機器 I D + パスフレーズ）42 を機器認証情報として使用するため、これを更に暗号化された状態で C E 機器 9 に保持することによりセキュリティを高めるものである。30

以降、暗号化（情報 A + 情報 B）を再度暗号化したものを再度暗号化（情報 A + 情報 B）などと記すことにする。

【0087】

書き込みモジュール 30 は、このようにして生成した再度暗号化（機器 I D + パスフレーズ）42（再度暗号化（機器 I D + パスフレーズ）42a とする）を認証情報メモリ 40 に書き込み（ステップ 228）、認証情報メモリ 40 は、再度暗号化（機器 I D + パスフレーズ）42a を記憶する（ステップ 230）。

このように、本実施の形態では、認証情報メモリ 40 に機器 I D 4 1 と、再度暗号化（機器 I D + パスフレーズ）42a が記憶されている。

【0088】

図 12 は、C E 機器 9 に機器認証情報が適切に組み込まれたことを管理センタ 3、及び工場 5 が確認する手順を説明するためのフローチャートである。

この手順は、C E 機器 9 のコネクタに接続手段 10 が接続した状態で行われる。通常は、工場システムが C E 機器 9 に機器認証情報を組み込んだ後、自動的に行われる。

【0089】

まず、書き込みモジュール 30 が認証情報メモリ 40 から再度暗号化（機器 I D + パスフレーズ）42a を読み出し、認証情報メモリ 40 から書き込みモジュール 30 へ再度暗号化（機器 I D + パスフレーズ）42a が提供される（ステップ 240）。

次に、書き込みモジュール 30 は、固有鍵生成子 32 と、MAC アドレス 51 から固有鍵 33 を生成し（ステップ 250）、これを用いて再度暗号化（機器 I D + パスフレーズ）440
3 を記憶する（ステップ 260）。

2 a を複合化し、暗号化（機器 ID + パスフレーズ）4 2 を得る（ステップ 252）。

【0090】

次に、書込モジュール 30 は、サーバ側確認ハッシュ関数 35 を用いて暗号化（機器 ID + パスフレーズ）4 2 から第 2 のハッシュ値を生成し（ステップ 254）、工場システムに出力する（ステップ 256）。

第 1 の実施の形態では、（機器 ID + パスフレーズ）から第 2 のハッシュ値を生成したが、第 2 の実施の形態では、暗号化（機器 ID + パスフレーズ）4 2 から第 2 のハッシュ値を生成する。

なお、第 2 の実施の形態では、第 1 のハッシュ値は利用しない。

工場システムは、CE 機器 9 から出力された第 2 のハッシュ値に、機器 ID 41、製品シリアル番号、鍵識別子を付加して管理サーバ 7 に送信する（ステップ 260）。 10

【0091】

管理サーバ 7 は、工場システムから受信した機器 ID 41 を発行済み機器認証情報テーブル 708（図 14）で検索し、この CE 機器 9 に対して発行したパスフレーズを取得する（ステップ 270）。

次に、管理サーバ 7 は、工場システムから受信した鍵識別子を鍵テーブル 706 で検索し、CE 機器 9 に記憶されているのと同じ書込前鍵 31 を取得する（ステップ 272）。 10

【0092】

次に、管理サーバ 7 は、工場システムから受信した機器 ID 41 と、ステップ 270 で検索したパスフレーズを用いて（機器 ID + パスフレーズ）を生成し、これをステップ 272 で検索した書込前鍵 31 で暗号化して暗号化（機器 ID + パスフレーズ）4 2 を生成する（ステップ 274）。 20

次に、管理サーバ 7 は、生成した暗号化（機器 ID + パスフレーズ）4 2 をサーバ側確認ハッシュ関数 35 を用いてハッシュ化し、第 2 のハッシュ値を生成する（ステップ 276）。

【0093】

次に、管理サーバ 7 は、ステップ 276 で生成した第 2 のハッシュ値と、工場システムから受信した第 2 のハッシュ値の一一致を比較することにより、CE 機器 9 に機器認証情報が適切に組み込まれたことを確認する（ステップ 278）。

【0094】

管理サーバ 7 は、図 14 に示したような機器認証テーブル 710 を備えており、機器 ID 41、暗号化（機器 ID + パスフレーズ）4 2（即ち、機器認証情報）、製品シリアル番号、鍵識別子を対応付けて記憶している。 30

管理サーバ 7 は、第 2 のハッシュ値の比較により、機器認証情報が CE 機器 9 に適切に組み込まれたことを検知すると、この暗号化（機器 ID + パスフレーズ）4 2 に、機器 ID 41、製品シリアル番号、鍵識別子を紐付けて機器認証テーブル 710 に記憶する（ステップ 280）。

なお、機器認証テーブル 710 は、機器認証サーバ 8 に提供され、CE 機器 9 を機器認証する際に利用される。

【0095】

次に、管理サーバ 7 は、工場システムから受信したデータに、受信した日時の日時情報を付加して秘密鍵で電子署名し、工場システムに送信する（ステップ 282）。

工場システムは、電子署名を確認し、機器認証情報が CE 機器 9 に適切に組み込まれたことを確認する（ステップ 262）。

工場 5 は、機器認証情報が組み込まれたことを確認した後、CE 機器 9 を市場に出荷する。

【0096】

図 13 は、機器認証サーバ 8 が CE 機器 9 を機器認証する手順を説明するためのフローチャートである。

まず、機器認証部 99（図 3）の認証モジュール 20 が、認証情報メモリ 40 から再度 50

暗号化（機器ID + パスフレーズ）42aを読み出し、認証情報メモリ40から認証モジュール20に再度暗号化（機器ID + パスフレーズ）42aが提供される（ステップ290）。

【0097】

次に、認証モジュール20は、固有鍵生成子22とMACアドレス51を用いて固有鍵23を生成する（ステップ300）。

そして認証モジュール20は、再度暗号化（機器ID + パスフレーズ）42aを固有鍵23を用いて復号化して暗号化（機器ID + パスフレーズ）42を取得し（ステップ302）、公開鍵21で暗号化して、機器ID41と共に機器認証サーバ8に送信する（ステップ304）。

10

【0098】

機器認証サーバ8は、CE機器9から暗号化（機器ID + パスフレーズ）42を受信し、これを公開鍵21に対応する秘密鍵で復号化する。そして、管理センタ3から提供された機器認証テーブル710を機器ID41で検索し、CE機器9の暗号化（機器ID + パスフレーズ）42を特定する。そして特定した暗号化（機器ID + パスフレーズ）42と、受信した暗号化（機器ID + パスフレーズ）42と照合してCE機器9を機器認証する（ステップ310）。

更に、機器認証テーブル710を用いてCE機器9の製品シリアル番号を特定する（ステップ312）。

以上の手順によりCE機器9の機器認証が行われる。

20

【0099】

以上に説明した第2の実施の形態による効果を従来の問題点と対比しながら列挙する。
(1) 従来は、管理サーバ7に機器認証情報を要求する場合、CE機器9に埋め込まれている書込前鍵31に応じた暗号化パスフレーズを要求する必要があった。しかし、本実施の形態では、CE機器9に埋め込まれている書込前鍵31を意識しないで（機器ID + パスフレーズ）を管理サーバ7に要求することができる。

【0100】

(2) 従来は、CE機器9の製造が停止した場合、取得しておいた（機器ID + パスフレーズ）が無駄になってしまっていた。しかし、本実施の形態では、管理サーバ7から取得した（機器ID + パスフレーズ）は、どのCE機器でも利用できるため、（機器ID + パスフレーズ）が余った場合は、他のCE機器に融通することができる。

30

(3) 従来は、CE機器9の製造ラインを考慮に入れると自由な書込前鍵31の単位の設定ができなかった。これに対し、本実施の形態では、製造ラインを気にすることなく書込前鍵31の単位を設定することができる。

【0101】

なお、本実施の形態では、管理サーバ7で元情報、（即ち（端末ID + パスフレーズ））から機器認証情報（即ち、暗号化（端末ID + パスフレーズ））を生成し、機器認証サーバ8に提供したが、これに限定せず、管理サーバ7は元情報を機器認証サーバ8に提供し、機器認証サーバ8で元情報から機器認証情報を生成するように構成することもできる。

40

【0102】

[第3の実施の形態]

次に、第3の実施の形態について説明する。

この実施の形態は、機器認証情報を暗号化・復号化するための鍵情報が含まれているアプリケーション（機器認証クライアント）を更新するものである。

機器認証クライアントは、CE機器やパーソナルコンピュータなどにインストールされ、機器認証部99（図3）と同様なモジュールが形成される。そして、モジュールに含まれる公開鍵（公開鍵21に対応）は、使用期限などが設定されており、新規なものに更新する必要がある場合がある。

従来は、このような場合、機器認証クライアントを全て新しいものに交換する必要があ

50

った。

本実施の形態では、機器認証クライアントに含まれる機器認証部99に対応するモジュールを新しいものに交換することにより、このモジュールに含まれる公開鍵の更新を行う。

【0103】

以下、CE機器9の機器認証部99を更新する場合を例にとり、図15のフローチャートを用いながら更新の手順を説明する。

なお、更新サーバは、機器認証クライアントを更新するサービスを提供するサーバ装置であり、更新サーバと、機器認証サーバは、製品コード（製品の機種を特定するコード）と固有鍵生成子との対応関係を同期させて保持しているものとする。

また、対象機器は、更新の対象となる機器認証クライアントを備えた端末機器である。

【0104】

まず、対象機器が更新サーバにアクセスし、モジュール（機器認証クライアントに組み込まれた機器認証部99）の更新を要求する（ステップ400）。

これに対し、更新サーバは対象機器の機器認証を要求する（ステップ410）。

対象機器は、機器認証サーバにアクセスし、機器認証サーバが機器認証を行う（ステップ402、ステップ422）。

この際に、機器認証サーバは、ワンタイムIDを発行して、対象機器の製品コードと対応付けて記憶すると共に、このワンタイムIDを対象機器に送信する。

【0105】

対象機器は、機器認証サーバからワンタイムIDを受信して、これを更新サーバに送信する（ステップ404）。

更新サーバは、対象機器からワンタイムIDを受信し、これを機器認証サーバに送信する（ステップ412）。

機器認証サーバは、更新サーバからワンタイムIDを受信し、これに対応付けておいた製品コードを更新サーバに送信する（ステップ424）。

【0106】

更新サーバは、機器認証サーバから製品コードを受信して、更新対象となっている機器認証クライアントを特定する。

そして、対象機器と通信し、対象機器側の機器認証クライアントのバージョンと最新バージョンの比較などを行いダウンロードするモジュールを確認する（ステップ406、ステップ414）。

【0107】

次に、更新サーバは、製品コードに対応した固有鍵生成子を検索し（ステップ416）、この固有鍵生成子に対応したモジュールを生成する（ステップ418）。

この際に、モジュールに含まれる公開鍵は、最新のものとなっている。

そして、更新サーバは、生成したモジュールを対象機器にダウンロードする（ステップ420）。

対象機器は、ダウンロードしたモジュールを保存する（ステップ408）。

【0108】

以上のように、本実施の形態では、モジュールを更新することにより、モジュールに含まれる公開鍵を更新することができる。

【0109】

[第4の実施の形態]

第1の実施の形態では、CE機器9は第2のハッシュ値を出力して管理サーバ7に送信し、管理サーバ7がこれを確認したが、本実施の形態では、CE機器9は、第1のハッシュ値の確認結果を管理サーバ7に送信する。

図16は、本実施の形態の機器認証部99aの構成の一例を示した図である。第1の実施の形態と同じ構成要素には同じ番号を付し、説明を省略する。

機器認証部99aは、第1のハッシュ値の確認結果を管理サーバ7に送信する認証情報

10

20

30

40

50

書込確認モジュール36を備える。

また、書込モジュール30aは、管理サーバ7に第2のハッシュ値を送信する必要がないため、サーバ側確認ハッシュ関数35(図3)を備えていない。

【0110】

書込モジュール30aは、管理センタ3から送信されてきた第1のハッシュ値と、機器側確認ハッシュ関数34による第1のハッシュ値を比較し、その比較結果を認証情報書込確認モジュール36に出力する。

認証情報書込確認モジュール36は、更に機器IDを取得し、確認結果と共に接続手段10を経由して工場システムに出力する。

工場システムは、これに更にシリアル番号を附加して管理サーバ7に送信し、管理センタ3は、確認結果を受け取ることにより、CE機器9に機器認証情報が組み込まれたことを確認することができる。10

【0111】

図17は、本実施の形態において、CE機器に機器認証情報が適切に組み込まれたことを確認する手順を説明するためのフローチャートである。

図6のフローチャートと同じ処理には同じステップ番号を付し、説明を省略又は簡略化する。

ステップ90～ステップ106までは第1の実施の形態と同じである。

【0112】

ただし、ステップ106においては、書込モジュール30aは、機器側確認ハッシュ関数34を用いて生成した第1のハッシュ値と管理サーバ7から受信した第1のハッシュ値が同一であるか否かを比較し、その比較結果を認証情報書込確認モジュール36に出力する(ステップ106)。20

【0113】

認証情報書込確認モジュール36は、書込モジュール30aから比較結果を取得し、また、認証モジュール20を経由するなどして機器ID41を取得し、これらを接続手段10を経由して工場システムに出力する(ステップ502)。

工場システムは、認証情報書込確認モジュール36から出力された比較結果、及び機器IDに製品シリアル番号を附加し、管理サーバ7に送信する(ステップ504)。

【0114】

管理サーバ7は、工場システムからこれらの情報を受信する。そして、比較結果により管理サーバ7が送信した第1のハッシュ値と機器側確認ハッシュ関数34を用いて生成された第1のハッシュ値が同一であることを確認し、これによって、機器認証情報がCE機器9に記憶されたことを認識する(ステップ506)。30

【0115】

後のステップは第1の実施の形態と同様であり、管理サーバ7は、機器IDと製品シリアル番号を紐付けて記憶し(ステップ134)、更に受信したデータに日時情報を付加して秘密鍵で署名し、工場システムに送信する(ステップ136)。

工場システムは、署名を確認し、機器認証情報がCE機器9に適切に組み込まれたことを確認する。40

【0116】

以上のように、本実施の形態では、管理サーバ7は確認結果により、機器認証情報がCE機器9に組み込まれたことを確認することができる。

また、管理サーバ7で第2のハッシュ値を生成する必要がないので管理サーバ7の負荷を低減することができる。

なお、本実施の形態では、書込モジュール30aで第1のハッシュ値を生成することとしたが、機器側確認ハッシュ関数34を認証モジュールに備え、認証モジュールでハッシュ値を生成するように構成してもよい。この場合、認証情報書込確認モジュール36は、認証モジュールから第1のハッシュ値と機器IDを受け取り、第1のハッシュ値の同一性を確認するように構成できる。50

更に、認証情報書込確認モジュール36の機能を書込モジュール30aに持たせ、書込モジュール30aが管理サーバ7に確認結果を送信するように構成することもできる。

【図面の簡単な説明】

【0117】

【図1】第1の実施の形態の概要を説明するための図である。

【図2】第1の実施の形態における製造認証システムの構成の一例を示した図である。

【図3】第1の実施の形態における機器認証部の構成の一例を示した図である。

【図4】第1の実施の形態において、機器認証情報を組み込む準備段階での作業手順を説明するためのフローチャートである。

【図5】第1の実施の形態において、CE機器に機器認証情報を組み込む手順を説明するためのフローチャートである。 10

【図6】第1の実施の形態において、CE機器に機器認証情報が適切に組み込まれたことを確認する手順を説明するためのフローチャートである。

【図7】第1の実施の形態において、機器認証サーバがCE機器を機器認証する手順を説明するためのフローチャートである。

【図8】第1の実施の形態の機器認証サーバなどに記憶されている各テーブルを説明するための図である。

【図9】第1の実施の形態のCE機器のハードウェア的な構成の一例を示した図である。

【図10】第2の実施の形態の概要を説明するための図である。

【図11】第2の実施の形態において、CE機器に機器認証情報を組み込む手順を説明するためのフローチャートである。 20

【図12】第2の実施の形態において、CE機器に機器認証情報が適切に組み込まれたことを確認する手順を説明するためのフローチャートである。

【図13】第2の実施の形態において、機器認証サーバがCE機器を機器認証する手順を説明するためのフローチャートである。

【図14】第2の実施の形態の機器認証サーバなどに記憶されている各テーブルを説明するための図である。

【図15】第3の実施の形態において、鍵情報が含まれているアプリケーションを更新する手順を説明するためのフローチャートである。

【図16】第4の実施の形態における機器認証部の構成の一例を示した図である。 30

【図17】第4の実施の形態において、CE機器に機器認証情報が適切に組み込まれたことを確認する手順を説明するためのフローチャートである。

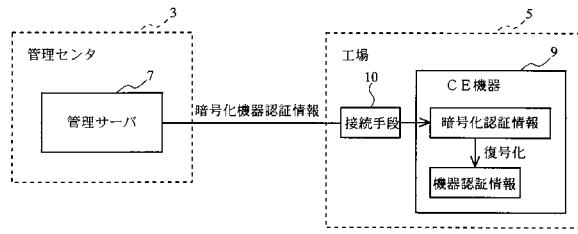
【図18】従来の認証情報の組み込み方法を説明するための図である。

【符号の説明】

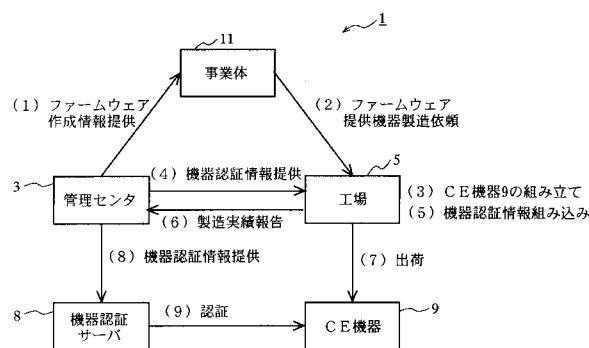
【0118】

1	製造認証システム	3	管理センタ
5	工場	7	管理サーバ
8	機器認証サーバ	9	CE機器
10	接続手段	11	事業体
20	認証モジュール	21	公開鍵
22	固有鍵生成子	23	固有鍵
30	書込モジュール	31	書込前鍵
32	固有鍵生成子	33	固有鍵
34	機器側確認ハッシュ関数	35	サーバ側確認ハッシュ関数
40	認証情報メモリ	41	機器ID
42	暗号化（機器ID + パスフレーズ）	50	本体識別メモリ
51	M A C アドレス	99	機器認証部

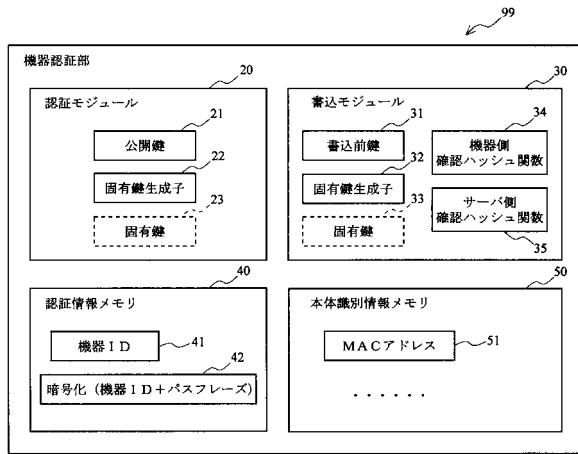
【図1】



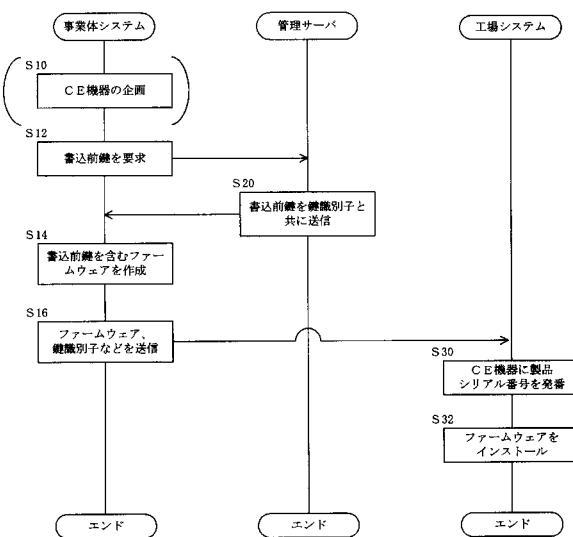
【図2】



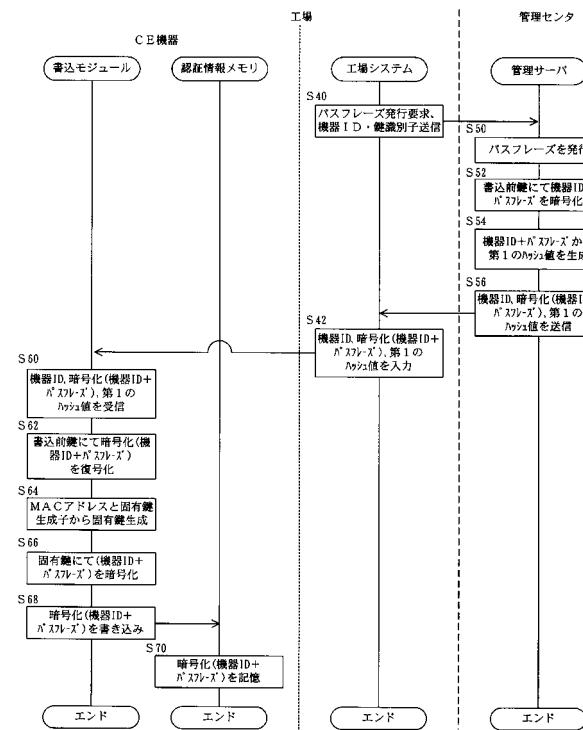
【図3】



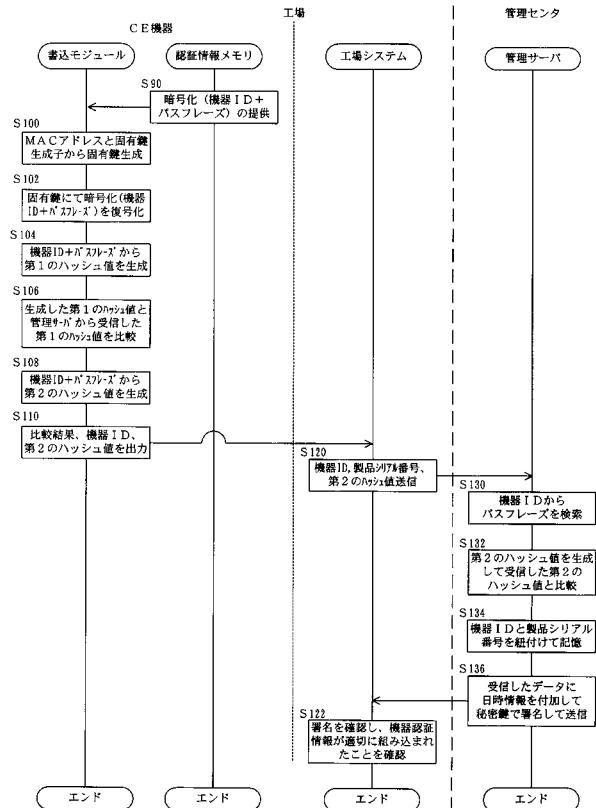
【図4】



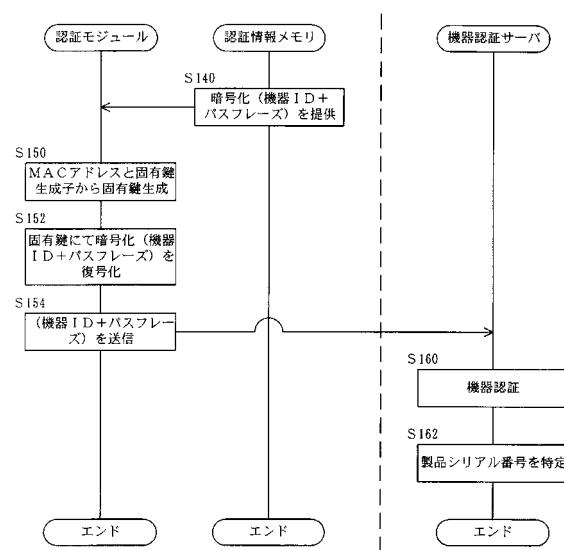
【図5】



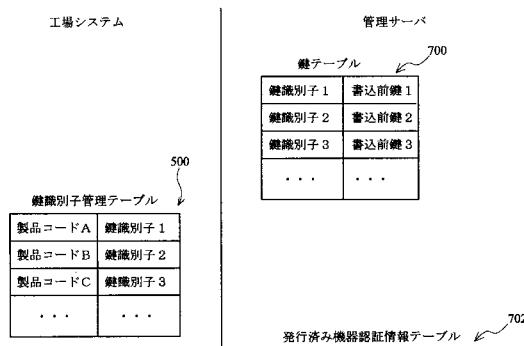
【図6】



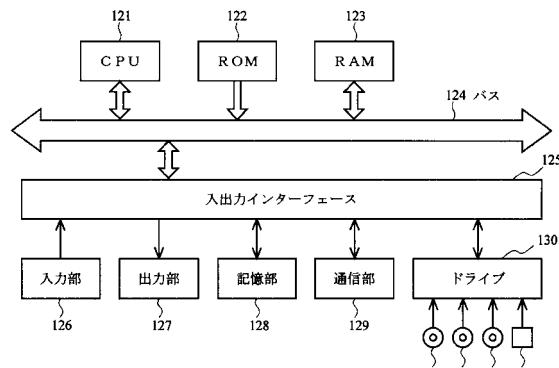
【図7】



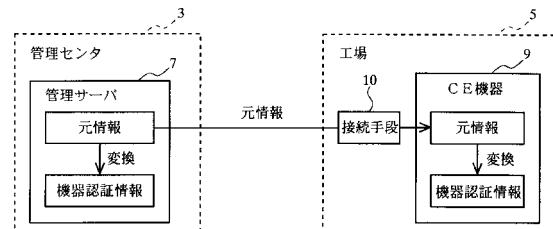
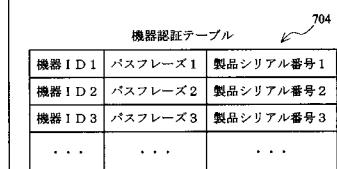
【図8】



【図9】



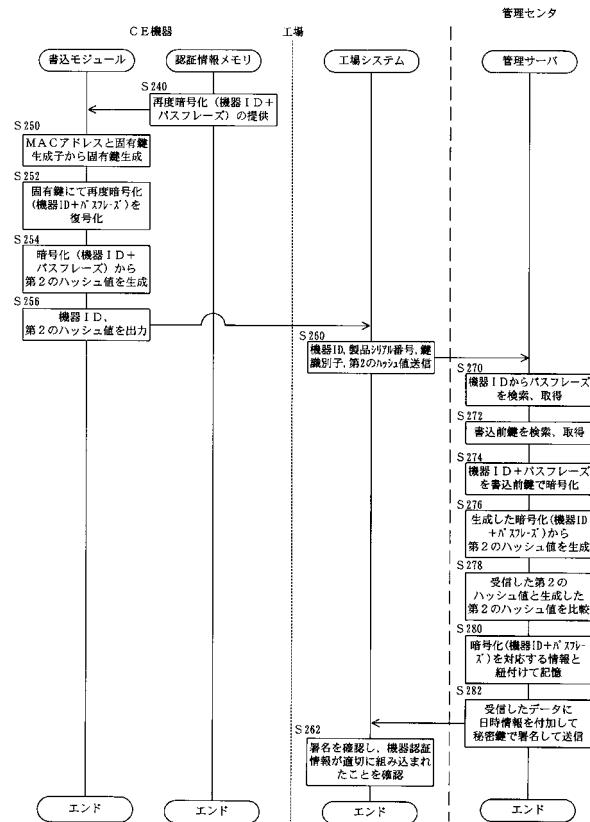
【図10】



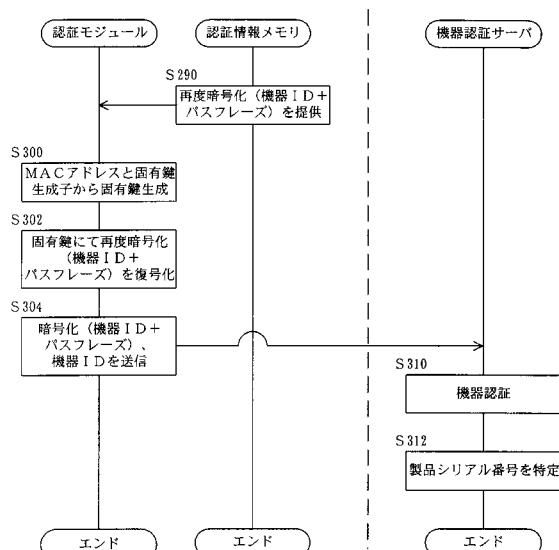
【図11】



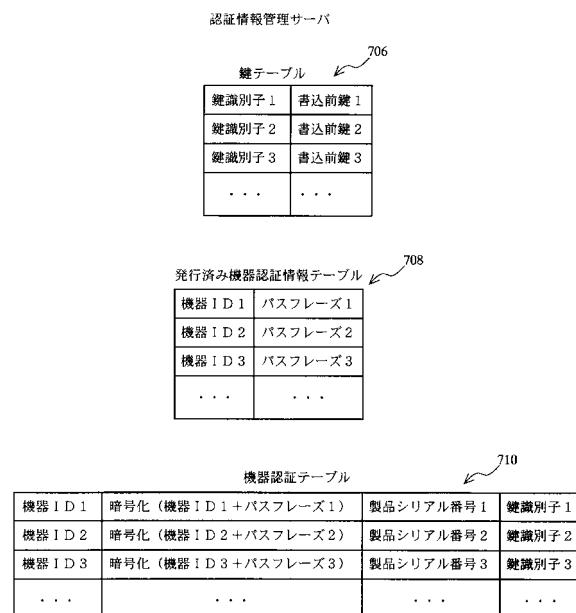
【図12】



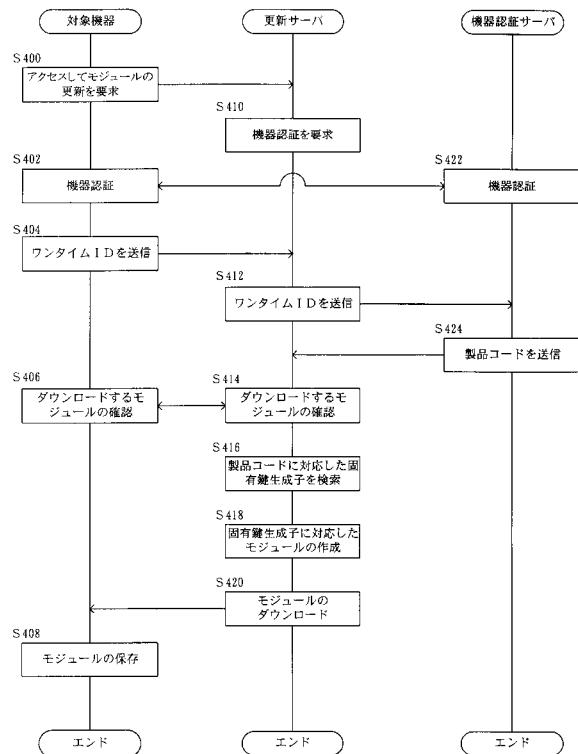
【図13】



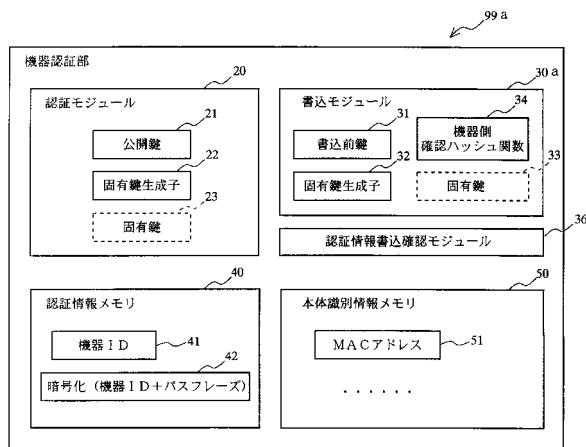
【図14】



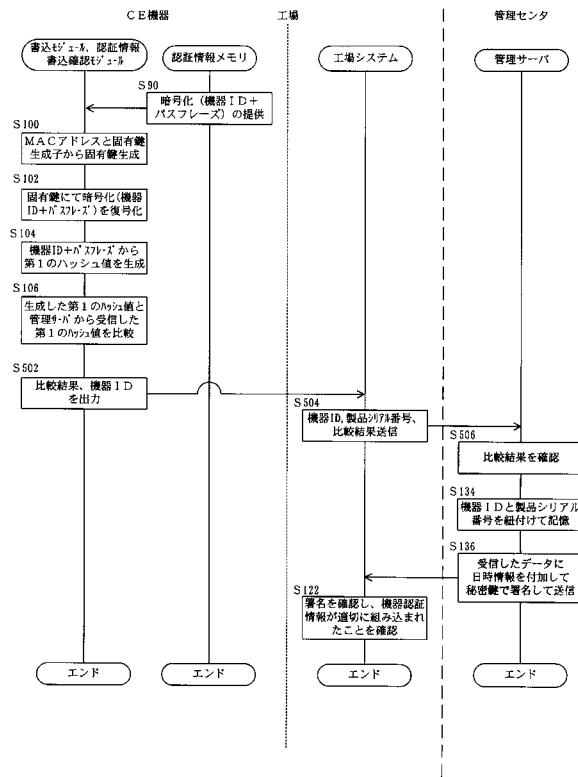
【図15】



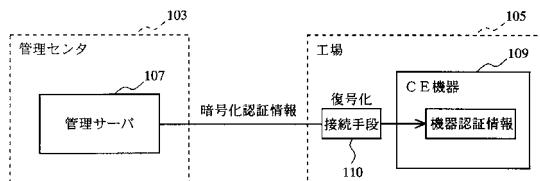
【図16】



【図17】



【図18】



フロントページの続き

(72)発明者 佐藤 敦司
東京都品川区北品川 4 - 7 - 35 ソニーグローバルソリューションズ株式会社内

(72)発明者 杉田 優
東京都品川区北品川 4 - 7 - 35 ソニーグローバルソリューションズ株式会社内

(72)発明者 三浦 貴之
東京都品川区北品川 6 丁目 7 番 35 号 ソニー株式会社内

(72)発明者 小野 剛
東京都品川区北品川 6 丁目 7 番 35 号 ソニー株式会社内

(72)発明者 宮田 耕自
東京都品川区北品川 6 丁目 7 番 35 号 ソニー株式会社内

F ターム(参考) 5B085 AA08 AE04 AE09
5J104 AA07