(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7353661号
(P7353661)

(45)発行日　令和5年10月2日(2023.10.2)

(24)登録日　令和5年9月22日(2023.9.22)

(51)国際特許分類
Ｇ０６Ｆ　21/33　(2013.01)

ＦＩ
Ｇ０６Ｆ　21/33

請求項の数　6　（全15頁）

(21)出願番号　特願2021-212404(P2021-212404)
(22)出願日　令和3年12月27日(2021.12.27)
(65)公開番号　特開2023-96560(P2023-96560A)
(43)公開日　令和5年7月7日(2023.7.7)
審査請求日　令和4年9月28日(2022.9.28)

(73)特許権者　515121634
株式会社制御システム研究所
神奈川県横浜市中区元浜町４－３５－３０２
(74)代理人　110002675
弁理士法人ドライト国際特許事務所
(72)発明者　森本 賢一
神奈川県横浜市中区元浜町４－３５－３０２ 株式会社制御システム研究所内
審査官　岸野 徹

最終頁に続く

(54)【発明の名称】　電子証明書の組み込み方法及び電子証明書の組み込みシステム

(57)【特許請求の範囲】

【請求項１】

単一の端末を複数のユーザが異なるタイミングで使用する場合に、証明局のサーバにより、ユーザごとに、前記端末を認証するための電子証明書を時系列で発行し、

前記複数のユーザのうちの一のユーザが前記端末を使用しているとき、前記端末で動作する所定のソフトウェアにより、

前記サーバにより発行された直前の電子証明書が前記端末に存在するか否かを確認し、

前記直前の電子証明書が前記端末に存在する場合、前記サーバにより発行された次の電子証明書を前記端末に組み込む、

電子証明書の組み込み方法。

【請求項２】

前記サーバにより、ユーザごとに、個人認証のためのユーザ証明書を発行し、

前記直前の電子証明書が前記端末に存在する場合、前記一のユーザの前記ユーザ証明書の情報と、前記直前の電子証明書の情報とを、ネットワークを介して前記端末から前記サーバに送信し、

前記端末から受信した前記ユーザ証明書の情報及び前記直前の電子証明書の情報に基づいて、前記サーバにより、前記一のユーザの個人認証及び前記端末の認証をすることができた場合、前記次の電子証明書を、前記ネットワークを介して前記サーバから前記端末に送信する、請求項１に記載の方法。

【請求項３】

前記サーバにより発行された各電子証明書には有効期限が設定されている、請求項１又は２に記載の方法。
【請求項４】
前記次の電子証明書を前記端末に組み込んだ後、前記端末の個体識別情報及びセットアップ情報を含む端末情報を、ネットワークを介して前記端末から前記サーバに送信し、
前記サーバは、前記端末から受信した前記端末情報を登録する、請求項１～３の何れか１項に記載の方法。
【請求項５】
前記サーバにより、多要素認証によって、前記端末を使用する前記複数のユーザの各々を特定する、請求項１～４の何れか１項に記載の方法。
【請求項６】
単一の端末と、
前記端末にネットワークを介して接続され、前記端末を複数のユーザが異なるタイミングで使用する場合に、ユーザごとに、前記端末を認証するための電子証明書を時系列で発行する証明局のサーバと、
を備え、
前記端末は、
前記複数のユーザのうちの一のユーザが前記端末を使用しているとき、所定のソフトウェアにより、
前記サーバにより発行された直前の電子証明書が前記端末に存在するか否かを確認し、
前記直前の電子証明書が前記端末に存在する場合、前記サーバにより発行された次の電子証明書を組み込む、
電子証明書の組み込みシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、電子証明書の組み込み方法及び電子証明書の組み込みシステムに関するものである。
【背景技術】
【０００２】
近年、工場やインフラストラクチャなどの設備の現場において、サイバーセキュリティ対策が求められており、設備のネットワークに不適切な端末を接続させないことが最重要課題となっている。
【０００３】
例えば、企業の事務部門で使用される端末は、従業員（ユーザ）が保有する個人認証端末であるため、ユーザのみが知るパスワードなどの情報を用いて、ユーザと端末とを紐付けることができる。よって、端末を保有するユーザの個人認証（ログイン）によって、適切な端末であるか否かを識別している。端末を認証するため、一般に、二要素認証（例えば、ユーザのみが知るメールアドレスとユーザ所有の携帯電話へのメッセージコードを用いた認証）によって、端末を識別する電子証明書を当該端末にインストールする手法が用いられている（例えば、特許文献１参照）。
【先行技術文献】
【特許文献】
【０００４】
【文献】国際公開第２０１３／００３４１９号
【発明の概要】
【発明が解決しようとする課題】
【０００５】
一方、設備の現場では、チームで共有するパーソナルコンピュータや操作パネルのように、各ユーザと直接的に紐付けられない端末が多く存在する。この場合、設備の責任者が

、設備内の各端末に電子証明書をインストールすることは困難である。また、操作パネルのように専用のソフトウェアが導入される端末では、端末の納入業者と受領者、そしてソフトウェアをインストールして設備と連動させるインテグレータが異なることも予想される。この場合、設備オーナー会社の従業員だけではなく外部の業者も、同一端末での作業の一部を受託することが予想される。このように、単一の端末のシステム構築に複数の組織の複数のユーザが関与する場合、上述のように、端末に電子証明書をインストールする各ユーザの個人認証によって端末を識別する手法では、設備のセキュリティを担保することができず、信頼性が損なわれてしまうという課題が生じる。

【０００６】

本発明は、上記課題に鑑みてなされたものであり、単一の端末のシステム構築に複数のユーザが関与する場合においても、信頼性を損なうことなく当該端末に電子証明書を組み込む方法及びシステム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】

本発明の一態様に係る電子証明書の組み込み方法は、単一の端末を複数のユーザが異なるタイミングで使用する場合に、証明局のサーバにより、ユーザごとに、端末を認証するための電子証明書を時系列で発行し、複数のユーザのうちの一のユーザが端末を使用しているとき、端末で動作する所定のソフトウェアにより、サーバにより発行された直前の電子証明書が端末に存在するか否かを確認し、直前の電子証明書が端末に存在する場合、サーバにより発行された次の電子証明書を端末に組み込む。

【０００８】

本発明の一態様に係る電子証明書の組み込みシステムは、単一の端末と、当該端末にネットワークを介して接続され、端末を複数のユーザが異なるタイミングで使用する場合に、ユーザごとに、端末を認証するための電子証明書を時系列で発行する証明局のサーバと、を備える。端末は、複数のユーザのうちの一のユーザが端末を使用しているとき、所定のソフトウェアにより、サーバにより発行された直前の電子証明書が端末に存在するか否かを確認し、直前の電子証明書が端末に存在する場合、サーバにより発行された次の電子証明書を組み込む。

【発明の効果】

【０００９】

本発明によれば、サーバにより発行された直前の電子証明書が端末に存在する場合に、次の電子証明書を当該端末に組み込むようにしたことにより、当該端末のシステム構築に複数のユーザが関与する場合においても、信頼性を損なうことなく当該端末に電子証明書を組み込むことができる。

【図面の簡単な説明】

【００１０】

【図１】本発明の各実施形態に係る電子証明書の組み込みシステムの構成を示す模式図である。

【図２】本発明の第１実施形態に係る電子証明書の組み込み方法を示すシーケンス図の一部である。

【図３】第１実施形態に係る電子証明書の組み込み方法を示すシーケンス図の一部である。

【図４】第１実施形態に係る電子証明書の組み込み方法を示すシーケンス図の一部である。

【図５】第１実施形態に係る電子証明書の組み込み方法を示すシーケンス図の一部である。

【図６】第１実施形態に係る電子証明書の組み込み方法を示すシーケンス図の一部である。

【図７】第１実施形態に係る電子証明書の組み込み方法を示すシーケンス図の一部である。

【図８】第１実施形態に係る電子証明書の組み込み方法を示すシーケンス図の一部である。

【図９】本発明の第２実施形態に係る電子証明書の組み込み方法を示すシーケンス図の一部である。

【図１０】第２実施形態に係る電子証明書の組み込み方法を示すシーケンス図の一部である。

【発明を実施するための形態】
【００１１】
以下、図面を参照して、本発明の実施形態に係る電子証明書の組み込み方法及び電子証明書の組み込みシステムについて説明する。
【００１２】
本実施形態では、工場などの設備に、電子証明書を用いたネットワーク接続の認証システムが導入されているものとする。このような認証システムでは、一般的に、ＩＥＥＥ８０２．１Ｘ認証又はＲＡＤＩＵＳ認証と呼ばれる認証プロトコルが用いられる。無線ＬＡＮの場合は、ＥＡＰ－ＴＬＳ認証が一般的に用いられる。これらの認証方式では、ユーザが入力するパスワード又は事前公開鍵のような入力文字列ではなく、端末内の電子証明書を用いて、ネットワークへの接続を許可するか否かを判断している。
【００１３】
図１に示すように、電子証明書の組み込みシステム１００は、電子証明書を発行する証明局１２０のサーバ１０２と、設備１４０に設置された端末１０４とから構成され、サーバ１０２と端末１０４とは、インターネットなどのネットワーク１０６を介して接続可能である。以下では、電子証明書を単に「証明書」と呼ぶことがある。
【００１４】
本実施形態では、端末１０４が、複数のシステム技術者が関与するケースの多いパーソナルコンピュータなどの汎用コンピュータであるものとして説明するが、端末１０４として、制御システムなどの組み込み型の専用コンピュータを採用してもよい。
【００１５】
本実施形態では、設備１４０のシステムに単一の端末１０４を追加する際に関与する複数のユーザをＣｉ（ｉ＝１、…、ｎ：ｎは２以上の整数）と表記し、ユーザＣｉが端末１０４を使用するときに端末１０４を認証するために発行される証明書をｂｉと表記し、ユーザＣｉが端末１０４上で実施する作業をＷｉと表記する。ここで、複数のユーザＣｉとして、外部の業者、設備１４０の従業員などが挙げられる。作業Ｗｉとしては、端末１０４への各種ソフトウェアのインストールやセットアップ作業などが挙げられる。
【００１６】
＜第１実施形態＞
次に、図２～図８のシーケンス図を参照して、第１実施形態に係る電子証明書の組み込み方法を説明する。
【００１７】
証明局１２０のサーバ１０２には、端末１０４で作業Ｗｉを実施する複数のユーザＣｉの情報（例えば、氏名、ＩＤコード、携帯電話の番号など）と、ユーザＣｉが作業Ｗｉを実施する順番ｉとが対応付けて登録されている。まず、サーバ１０２は、ユーザごとに、ユーザＣｉを認証するための電子証明書であるＣｉ証明書（ユーザ証明書）を作成するとともに、ｂｉ証明書を端末１０４にインストールするためのソフトウェアｂｓｗを作成する（図２のステップ２０２）。Ｃｉ証明書はドングルに格納され、ｂｓｗは、ＵＳＢメモリなどの記憶媒体に格納される。Ｃｉ証明書及びｂｉ証明書には、いずれも公開鍵が内包されており、対応する秘密鍵は、サーバ１０２に保存される。
【００１８】
ｂｓｗには、各ｂｉ証明書を端末１０４にインストールするための秘密の文字列（インストールキー）が組み込まれている。
【００１９】
Ｃｉ証明書及びｂｓｗが作成されると、証明局１２０から各ユーザＣｉに、Ｃｉ証明書が格納されたドングルとｂｓｗが格納された記憶媒体とが配付される（ステップ２０４）。なお、一つのドングル（又は一つの記憶媒体）にＣｉ証明書とｂｓｗの双方を格納し、各ユーザＣｉにドングルのみ（又は記憶媒体のみ）を配付するようにしてもよい。
【００２０】
次に、証明書の発行依頼者のコンピュータにおいて、端末１０４の名称が指定され（ス

テップ２０６）、ネットワーク１０６を介して、指定された端末名とともに証明書の発行要求がサーバ１０２に送信される（ステップ２０８）。

【００２１】

サーバ１０２は、証明書の発行要求を受けると、端末１０４にインストールされる予定のｂ１証明書、ｂ２証明書、…、ｂｎ証明書を作成する（ステップ２１０）。各ｂｉ証明書には有効期限ｌｉｍｉｔ（ｉ）が設定される。ｌｉｍｉｔ（ｉ）は、作業Ｗｉの順番、重要度などに応じて設定される。具体的には、最後に発行されるｂｎ証明書の有効期限ｌｉｍｉｔ（ｎ）を一番長くする。例えば、ｂ１証明書の有効期限ｌｉｍｉｔ（１）を９０日、ｂ２証明書～ｂ（ｎ－１）証明書の有効期限ｌｉｍｉｔ（２）～ｌｉｍｉｔ（ｎ－１）を３０日、ｂｎ証明書の有効期限ｌｉｍｉｔ（ｎ）を１０年に設定する。

【００２２】

次いで、サーバ１０２は、ｂ１証明書、その秘密鍵、指定された端末名、及びエージェントソフトウェアを暗号化したファイルｂ０を作成し（ステップ２１２）、ファイルｂ０を、ネットワーク１０６を介して、端末保有者の端末１０４に送信する（ステップ２１４）。ここで、エージェントソフトウェアとは、端末１０４の状態を表す端末情報を外部に報告するためのソフトウェアである。端末情報は、シリアルナンバー、Media Access Control（ＭＡＣ）アドレス、インストールされたアプリケーションの一覧、オペレーティングシステム（ＯＳ）のバージョン、アップデート日時など、端末１０４の個体識別情報及びセットアップ情報を含む。

【００２３】

ファイルｂ０は、端末１０４に保存される（図３のステップ３０２）。そして、端末１０４の名称が指定名に変更される（ステップ３０４）。その後、端末１０４は、端末保有者から最初のユーザＣ１に渡される（ステップ３０６）。

【００２４】

ユーザＣ１は、ステップ２０４で受領したドングルを端末１０４に接続し、端末１０４上で指定された作業Ｗ１を実施する（ステップ３０８）。その後、ユーザＣ１は、ステップ２０４で受領した記憶媒体を端末１０４に接続する。これにより、記憶媒体に格納されたｂｓｗが起動する（ステップ３１０）。ステップ３１０では、ファイルｂ０に含まれるｂ１証明書がインストールされるとともに（ステップ３１２）、エージェントソフトウェアがインストールされる（ステップ３１４）。ｂ１証明書は端末１０４内の所定の記憶エリアに格納される。ｂｓｗの実行が完了すると、端末１０４は次のユーザＣ２に渡される（ステップ３１６）。

【００２５】

なお、予めユーザＣ１に端末１０４を渡しておき、ステップ３０２及び３０４をユーザＣ１側で実行するようにしてもよい。

【００２６】

ユーザＣ２は、ステップ２０４で受領したドングルを端末１０４に接続し、端末１０４上で指定された作業Ｗ２を実施する（図４のステップ４０２）。次いで、端末１０４をネットワーク１０６に接続させる（ステップ４０４）。その後、ユーザＣ２は、ステップ２０４で受領した記憶媒体を端末１０４に接続する。これにより、記憶媒体に格納されたｂｓｗが起動し、端末１０４がネットワーク１０６を介して証明局１２０のサーバ１０２に接続され（ステップ４０６）、ｂｓｗの実行が開始される（ステップ４０８）。

【００２７】

ステップ４０８では、まず、端末１０４内に直前の証明書であるｂ１証明書が存在するか否か、ｂ１証明書が有効期限ｌｉｍｉｔ（１）内であるか否かが確認される（ステップ４１０）。有効期限内のｂ１証明書が存在しない場合（ステップ４１０：ＮＧ）、ｂｓｗが終了する。一方、端末１０４内に有効期限内のｂ１証明書が存在する場合（ステップ４１０：ＯＫ）、端末１０４は、Ｃ２証明書の情報及びｂ１証明書の情報を、ネットワーク１０６を介してサーバ１０２に送信するとともに、エージェントソフトウェアを起動して、端末１０４の現在の状態を表す端末情報（個体識別情報及びセットアップ情報）を、ネ

ットワーク１０６を介してサーバ１０２に送信する（ステップ４１２）。ここで、サーバ１０２に送信されるＣ２証明書の情報及びｂ１証明書の情報は、例えば、これらの証明書に内包された公開鍵であり、その証明書を発行した証明局１２０の証明書、すなわち証明局１２０の公開鍵を内包する。

【００２８】

なお、ステップ４１２において、Ｃ２証明書及びｂ１証明書の秘密鍵をサーバ１０２に送信してもよいが、この場合、秘密鍵を暗号化して送信する必要がある。

【００２９】

サーバ１０２は、受信したＣ２証明書に内包される証明局１２０の中間証明書およびルート証明書の公開鍵を自らが保有する秘密鍵を用いて確認するか、または別途暗号化されて送付されたＣ２証明書の公開鍵に対応する秘密鍵を用いて、Ｃ２証明書を確認する。さらに、受信したｂ１証明書に内包される証明局１２０の中間証明書およびルート証明書の公開鍵を自らが保有する秘密鍵を用いて確認するか、または別途暗号化されて送付されたｂ１証明書の公開鍵に対応する秘密鍵を用いて、ｂ１証明書を確認し、さらに、受信した端末情報から、端末１０４で作業Ｗ２が適切に行われたか否かを確認する（ステップ４１４）。

【００３０】

サーバ１０２により、Ｃ２証明書、ｂ１証明書、及び作業Ｗ２の少なくとも一つを確認することができなかった場合（ステップ４１４：ＮＧ）、サーバ１０２は、その旨を端末１０４に通知し、プロセスを終了する。この場合、端末１０４にｂ２証明書はインストールされない。

【００３１】

一方、サーバ１０２が、Ｃ２証明書、ｂ１証明書、及び作業Ｗ２の全てを確認することができた場合（ステップ４１４：ＯＫ）、サーバ１０２は、ｂ２証明書及びその秘密鍵を暗号化し（図５のステップ５０２）、暗号化されたファイルを、ネットワーク１０６を介して端末１０４に送信する（ステップ５０４）。

【００３２】

ｂｓｗを実行中の端末１０４は、サーバ１０２からダウンロードしたｂ２証明書をインストールする（ステップ５０６）。ｂ２証明書は端末１０４内の所定の記憶エリアに格納される。そして、端末１０４は、エージェントソフトウェアを起動して（ステップ５０８）、端末１０４の現在の状態を表す端末情報（上述の個体識別情報及びセットアップ情報）を、ネットワーク１０６を介してサーバ１０２に送信する（ステップ５１０）。

【００３３】

サーバ１０２は、受信した端末情報を登録するとともに（ステップ５１２）、ｂ２証明書のインストール完了を登録する（ステップ５１４）。その後、サーバ１０２は、ｂ２証明書を削除する（ステップ５１６）。

【００３４】

一方、端末１０４へのｂ２証明書のインストールが完了すると、端末１０４は次のユーザＣ３に渡される（ステップ５１８）。

【００３５】

次に、図６及び図７を参照して、３番目～（ｎ－１）番目のユーザＣｉ（ｉ＝３、４、…、ｎ－１）が端末１０４を使用するときのプロセスについて、図４及び図５と異なる点のみ説明する。なお、図６以降では、証明書の発行依頼者の図示を省略している。

【００３６】

図６のステップ６０２～６１４は、図４のステップ４０２～４１４において、Ｗ２、ｂ１、Ｃ２を、それぞれ、Ｗｉ、ｂ（ｉ－１）、Ｃｉに置き換えたものである。図７のステップ７０２～７１０は、図５のステップ５０２～５１０において、ｂ２をｂｉに置き換えたものである。以下、図７のステップ７１２以降を説明する。

【００３７】

サーバ１０２は、ステップ７１０で受信した端末１０４の端末情報と、サーバ１０２に

登録済みの端末情報とを比較する（ステップ７１２）。サーバ１０２は、ステップ７１２における比較の結果、同一の端末ではないと判断すると（ステップ７１２：ＮＧ）、不適切な端末である旨を端末１０４に通知し、プロセスを終了する。一方、サーバ１０２は、ステップ７１２において、同一の端末であると判断すると（ステップ７１２：ＯＫ）、ステップ７１０で受信した端末情報を登録するとともに、ｂｉ証明書のインストール完了を登録し（ステップ７１４）、ｂｉ証明書を削除する（ステップ７１６）。

【００３８】

一方、端末１０４へのｂｉ証明書のインストールが完了すると、端末１０４は次のユーザＣ（ｉ＋１）に渡される（ステップ７１８）。ここで、ユーザＣｉが使用している端末１０４が不適切な端末と判断された場合（ステップ７１２：ＮＧ）、たとえ、端末１０４が次のユーザＣ（ｉ＋１）に渡されたとしても、次のｂ（ｉ＋１）証明書が端末１０４にインストールされることはない。

【００３９】

最後のユーザＣｎが端末１０４を使用するときのプロセスは、図６及び図７においてｉ＝ｎとしたプロセスと同じであるが、ｂｎ証明書のインストール完了後、端末１０４が端末保有者に返還される点が異なる。

【００４０】

端末１０４がユーザＣｎから端末保有者に返還されると（図８のステップ８０２）、その端末１０４が適切な端末であるか否かを確認するため、端末保有者の操作により、端末１０４をサーバ１０２に接続させ、サーバ１０２に対し、端末１０４の端末情報の履歴とインストールの履歴を送付するように要求する（ステップ８０４）。サーバ１０２から、ネットワーク１０６を介して端末情報の履歴とインストールの履歴を受信すると（ステップ８０６）、端末１０４は、受信した履歴のデータと、端末１０４内の履歴のデータとを比較し（ステップ８０８）、比較結果を、ネットワーク１０６を介してサーバ１０２に送信する（ステップ８１０）。

【００４１】

サーバ１０２に登録された履歴と端末１０４内の履歴とが一致している場合（ステップ８１２：ＹＥＳ）、サーバ１０２は、プロセスを終了する。一方、履歴の不一致がある場合（ステップ８１２：ＮＯ）、サーバ１０２は、Ｃｉ証明書の情報、ｂｉ証明書の情報、端末情報の履歴、インストールの履歴などの全ての関連データを失効させ（ステップ８１４）、プロセスを終了する。

【００４２】

端末１０４側では、履歴の不一致があることが確認されると、不適切な端末であると判断し、端末１０４内の関連データ（Ｃｉ証明書の情報、ｂｉ証明書の情報、端末情報の履歴、インストールの履歴など）を初期化し、一方、履歴が一致していることが確認されると、プロセスを終了する（ステップ８１６）。

【００４３】

以上のように、第１実施形態によれば、単一の端末１０４を複数のユーザＣｉが異なるタイミングで使用する場合、端末１０４上で動作するｂｓｗは、直前のｂ（ｉ－１）証明書が端末１０４に存在しない限り、次のｂｉ証明書を端末１０４にインストールさせないようにしている。また、サーバ１０２は、Ｃｉ証明書の情報と直前のｂ（ｉ－１）証明書の情報とに基づき、端末１０４を使用しているユーザＣｉの個人認証と端末１０４の認証とを行った後に、次のｂｉ証明書を発行するようにしている。すなわち、ｂ１証明書、ｂ２証明書、…、ｂｎ証明書が、チェーンのように時系列につながって単一の端末１０４にインストールされることから、全てのユーザＣ１、Ｃ２、…、Ｃｎが結託しない限り、不適切な端末が設備１４０のネットワークに接続されることはない。したがって、単一の端末１０４のシステム構築に複数のユーザＣｉが関与する場合においても、信頼性を損なうことなく端末１０４に電子証明書を組み込むことができる。

【００４４】

また、各ｂｉ証明書には有効期限ｌｉｍｉｔ（ｉ）が設定されていることから、たとえ

、ユーザＣｉが不正にｂｉ証明書を複製したとしても、その複製されたｂｉ証明書は有効期限内しか機能しないため、セキュリティのリスクを低減させることができる。さらに、端末１０４で作業Ｗｉが適切に行われたことを確認した後にｂｉ証明書を発行するようにしているため、複数のユーザＣｉの作業Ｗｉが決められた順番で適切に行われたことを担保することができる。

【００４５】

さらに、ユーザＣｉが端末１０４で指定作業Ｗｉを実施し、ｂｉ証明書が端末１０４にインストールされた後、エージェントソフトウェアにより、端末１０４の状態を表す端末情報（個体識別情報及びセットアップ情報）がサーバ１０２に通知され、サーバ１０２は当該端末情報を登録している。これにより、単一の端末１０４へのセットアップ作業の推移がトレーサブルとなるため、不適切なソフトウェアやデータが端末１０４にインストールされても、そのような作業を行ったユーザを特定することができる。

【００４６】

なお、電子証明書をインストールするためのソフトウェアとして、全てのユーザＣｉが同一のソフトウェアｂｓｗを使い、各ユーザＣｉに配布されたドングルにＣｉ証明書が格納されている例を示したが、各ユーザＣｉが、自身のＣｉ証明書が組み込まれたソフトウェアｂｓｗｉを使うようにしてもよい。この場合、上述のドングルは不要である。

【００４７】

＜第２実施形態＞

上述の第１実施形態では、ユーザＣｉが端末１０４で指定作業Ｗｉを実施した後に、ユーザＣｉの個人認証、端末１０４の認証を実施し、ｂｉ証明書を端末１０４にインストールしているが、第２実施形態では、指定作業Ｗｉの後だけでなく、指定作業Ｗｉの前にも、個人認証及び端末認証を実施する。

【００４８】

図９及び図１０を参照して、第２実施形態に係る電子証明書の組み込み方法を説明する。

【００４９】

以下では、作業Ｗｉの直前にインストールされる電子証明書をｂｉ（１）、作業Ｗｉの直後にインストールされる電子証明書をｂｉ（２）と表記し、ｂｉ（１）証明書をインストールするためのソフトウェアをｂｓｗ（１）、ｂｉ（２）証明書をインストールするためのソフトウェアをｂｓｗ（２）と表記する。ｂｓｗ（１）及びｂｓｗ（２）には、それぞれ、ｂｉ（１）証明書及びｂｉ（２）証明書を端末１０４にインストールするためのインストールキーが組み込まれている。

【００５０】

ユーザＣｉは、予め受領した、Ｃｉ証明書が格納されたドングルと、ｂｓｗ（１）が格納された記憶媒体とを端末１０４に接続する。これにより、ｂｓｗ（１）が起動する（図９のステップ９０２）。ステップ９０２では、まず、端末１０４内に直前の証明書であるｂ（ｉ－１）（２）証明書が存在するか否か、ｂ（ｉ－１）（２）証明書が有効期限内であるか否かが確認される（ステップ９０４）。

【００５１】

有効期限内のｂ（ｉ－１）（２）証明書が端末１０４に存在しない場合（ステップ９０４：ＮＧ）、ｂｓｗ（１）が終了する。一方、端末１０４内に有効期限内のｂ（ｉ－１）（２）証明書が存在する場合（ステップ９０４：ＯＫ）、端末１０４は、Ｃｉ証明書の情報及びｂ（ｉ－１）（２）証明書の情報を、ネットワーク１０６を介してサーバ１０２に送信するとともに、エージェントソフトウェアを起動して、端末１０４の現在の状態を表す端末情報（個体識別情報及びセットアップ情報）を、ネットワーク１０６を介してサーバ１０２に送信する（ステップ９０６）。ここで、サーバ１０２に送信されるＣｉ証明書の情報及びｂ（ｉ－１）（２）証明書の情報は、例えば、これらの証明書に内包された公開鍵であり、その証明書を発行した証明局１２０の証明書、すなわち証明局１２０の公開鍵を内包する。

【００５２】

なお、ステップ９０６において、Ｃｉ証明書及びｂ（ｉ－１）（２）証明書の秘密鍵をサーバ１０２に送信してもよいが、この場合、秘密鍵を暗号化して送信する必要がある。

【００５３】

サーバ１０２は、受信したＣｉ証明書に内包される証明局１２０の中間証明書およびルート証明書の公開鍵を自らが保有する秘密鍵を用いて確認するか、または別途暗号化されて送付されたＣｉ証明書の公開鍵に対応する秘密鍵を用いてＣｉ証明書を確認する。さらに、受信したｂ（ｉ－１）（２）証明書に内包される証明局１２０の中間証明書およびルート証明書の公開鍵を自らが保有する秘密鍵を用いて確認するか、または別途暗号化されて送付されたｂ（ｉ－１）（２）証明書の公開鍵に対応する秘密鍵を用いてｂ（ｉ－１）（２）証明書を確認し、さらに、受信した端末情報から、端末１０４で作業Ｗ（ｉ－１）が適切に行われたか否かを確認する（ステップ９０８）。

【００５４】

サーバ１０２により、Ｃｉ証明書、ｂ（ｉ－１）（２）証明書、及び作業Ｗ（ｉ－１）の少なくとも一つを確認することができなかった場合（ステップ９０８：ＮＧ）、サーバ１０２は、その旨を端末１０４に通知し、プロセスを終了する。この場合、端末１０４にｂｉ（１）証明書はインストールされない。

【００５５】

一方、サーバ１０２が、Ｃｉ証明書、ｂ（ｉ－１）（２）証明書、及び作業Ｗ（ｉ－１）の全てを確認することができた場合（ステップ９０８：ＯＫ）、サーバ１０２は、ｂｉ（１）証明書及びその秘密鍵を暗号化し（ステップ９１０）、暗号化されたファイルを、ネットワーク１０６を介して端末１０４に送信する（ステップ９１２）。

【００５６】

ｂｓｗ（１）を実行中の端末１０４は、サーバ１０２からダウンロードしたｂｉ（１）証明書をインストールする（ステップ９１４）。ｂｉ（１）証明書は端末１０４内の所定の記憶エリアに格納される。そして、端末１０４は、エージェントソフトウェアを起動して、端末１０４の現在の状態を表す端末情報（個体識別情報及びセットアップ情報）を、ネットワーク１０６を介してサーバ１０２に送信する（ステップ９１６）。

【００５７】

サーバ１０２は、ステップ９１６で受信した端末１０４の端末情報と、サーバ１０２に登録済みの端末情報とを比較する（ステップ９１８）。サーバ１０２は、ステップ９１８における比較の結果、同一の端末ではないと判断すると（ステップ９１８：ＮＧ）、不適切な端末である旨を端末１０４に通知し、プロセスを終了する。一方、サーバ１０２は、ステップ９１８において、同一の端末であると判断すると（ステップ９１８：ＯＫ）、ステップ９１６で受信した端末情報を登録するとともに、ｂｉ（１）証明書のインストール完了を登録し（ステップ９２０）、ｂｉ（１）証明書を削除する（ステップ９２２）。

【００５８】

一方、端末１０４へのｂｉ（１）証明書のインストールが完了し、ｂｓｗ（１）の実行が終了すると、ユーザＣｉは、端末１０４上で指定された作業Ｗｉを実施する（ステップ９２４）。作業Ｗｉの終了後、ｂｓｗ（２）の実行が開始される（ステップ９２６）。ステップ９２６では、まず、端末１０４内に直前の証明書であるｂｉ（１）証明書が存在するか否か、ｂｉ（１）証明書が有効期限内であるか否かが確認される（図１０のステップ９２８）。

【００５９】

有効期限内のｂｉ（１）証明書が端末１０４に存在しない場合（ステップ９２８：ＮＧ）、ｂｓｗ（２）が終了する。一方、端末１０４内に有効期限内のｂｉ（１）証明書が存在する場合（ステップ９２８：ＯＫ）、端末１０４は、Ｃｉ証明書の情報及びｂｉ（１）証明書の情報を、ネットワーク１０６を介してサーバ１０２に送信するとともに、エージェントソフトウェアを起動して、端末１０４の現在の状態を表す端末情報（個体識別情報及びセットアップ情報）を、ネットワーク１０６を介してサーバ１０２に送信する（ステップ９３０）。ここで、サーバ１０２に送信されるＣｉ証明書の情報及びｂｉ（１）証明

書の情報は、例えば、これらの証明書に内包された公開鍵であり、その証明書を発行した証明局１２０の証明書、すなわち証明局１２０の公開鍵を内包する。

【００６０】

なお、ステップ９３０において、Ｃｉ証明書及びｂｉ（１）証明書の秘密鍵をサーバ１０２に送信してもよいが、この場合、秘密鍵を暗号化して送信する必要がある。

【００６１】

サーバ１０２は、受信したＣｉ証明書に内包される証明局１２０の中間証明書およびルート証明書の公開鍵を自らが保有する秘密鍵を用いて確認するか、または別途暗号化されて送付されたＣｉ証明書の公開鍵に対応する秘密鍵を用いてＣｉ証明書を確認する。さらに、受信したｂｉ（１）証明書に内包される証明局１２０の中間証明書およびルート証明書の公開鍵を自らが保有する秘密鍵を用いて確認するか、または別途暗号化されて送付されたｂｉ（１）証明書の公開鍵に対応する秘密鍵を用いてｂｉ（１）証明書を確認し、さらに、受信した端末情報から、端末１０４で作業Ｗｉが適切に行われたか否かを確認する（ステップ９３２）。

【００６２】

サーバ１０２により、Ｃｉ証明書、ｂｉ（１）証明書、及び作業Ｗｉの少なくとも一つを確認することができなかった場合（ステップ９３２：ＮＧ）、サーバ１０２は、その旨を端末１０４に通知し、プロセスを終了する。この場合、端末１０４にｂｉ（２）証明書はインストールされない。

【００６３】

一方、サーバ１０２が、Ｃｉ証明書、ｂｉ（１）証明書、及び作業Ｗｉの全てを確認することができた場合（ステップ９３２：ＯＫ）、サーバ１０２は、ｂｉ（２）証明書及びその秘密鍵を暗号化し（ステップ９３４）、暗号化されたファイルを、ネットワーク１０６を介して端末１０４に送信する（ステップ９３６）。

【００６４】

ｂｓｗ（２）を実行中の端末１０４は、サーバ１０２からダウンロードしたｂｉ（２）証明書をインストールする（ステップ９３８）。ｂｉ（２）証明書は端末１０４内の所定の記憶エリアに格納される。そして、端末１０４は、エージェントソフトウェアを起動して、端末１０４の現在の状態を表す端末情報（個体識別情報及びセットアップ情報）を、ネットワーク１０６を介してサーバ１０２に送信する（ステップ９４０）。

【００６５】

サーバ１０２は、ステップ９４０で受信した端末１０４の端末情報と、サーバ１０２に登録済みの端末情報とを比較する（ステップ９４２）。サーバ１０２は、ステップ９４２における比較の結果、同一の端末ではないと判断すると（ステップ９４２：ＮＧ）、不適切な端末である旨を端末１０４に通知し、プロセスを終了する。一方、サーバ１０２は、ステップ９４２において、同一の端末であると判断すると（ステップ９４２：ＯＫ）、ステップ９４０で受信した端末情報を登録するとともに、ｂｉ（２）証明書のインストール完了を登録し（ステップ９４４）、ｂｉ（２）証明書を削除する（ステップ９４６）。

【００６６】

一方、端末１０４へのｂｉ（２）証明書のインストールが完了すると、端末１０４は次のユーザＣ（ｉ＋１）に渡される（ステップ９４８）。ここで、ユーザＣｉが使用している端末１０４が不適切な端末と判断された場合（ステップ９４２：ＮＧ）、たとえ、端末１０４が次のユーザＣ（ｉ＋１）に渡されたとしても、次の電子証明書が端末１０４にインストールされることはない。

【００６７】

最後のユーザＣｎが、ｂｎ（２）証明書を端末１０４にインストールした後は、図８に示すプロセスが実行される。

【００６８】

以上のように、第２実施形態によれば、指定作業Ｗｉの前後において、それぞれ、ソフトウェアｂｓｗ（１）及びｂｓｗ（２）により、ｂｉ（１）証明書及びｂｉ（２）証明書

が端末１０４にインストールされる。これにより、設備１４０のセキュリティを一層高めることができる。

【００６９】

なお、本発明は、上述の実施形態に限定されるものではなく、本発明の趣旨を逸脱しない範囲内で種々の変更が可能であり、当業者によってなされる他の実施形態、変形例も本発明に含まれる。

【００７０】

例えば、上述の各実施形態では、端末１０４を使用するユーザＣｉを特定するために、電子証明書であるＣｉ証明書のみを用いているが、多要素認証を採用してもよい。例えば、サーバ１０２からユーザＣｉの携帯電話にショートメッセージサービス（ＳＭＳ）でワンタイムパスワードを送信し、そのワンタイムパスワードを端末１０４に入力し、サーバ１０２に送信することで、ユーザＣｉの携帯電話と端末１０４とを用いた二要素認証をすることができる。

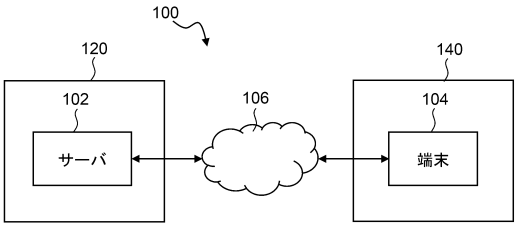
【符号の説明】

【００７１】

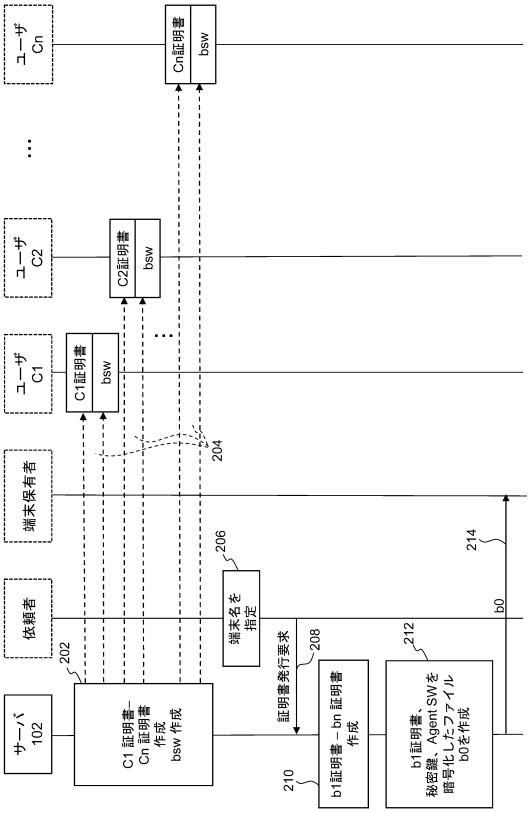
１００　電子証明書の組み込みシステム
１０２　サーバ
１０４　端末
１０６　ネットワーク
１２０　証明局
１４０　設備

【図面】

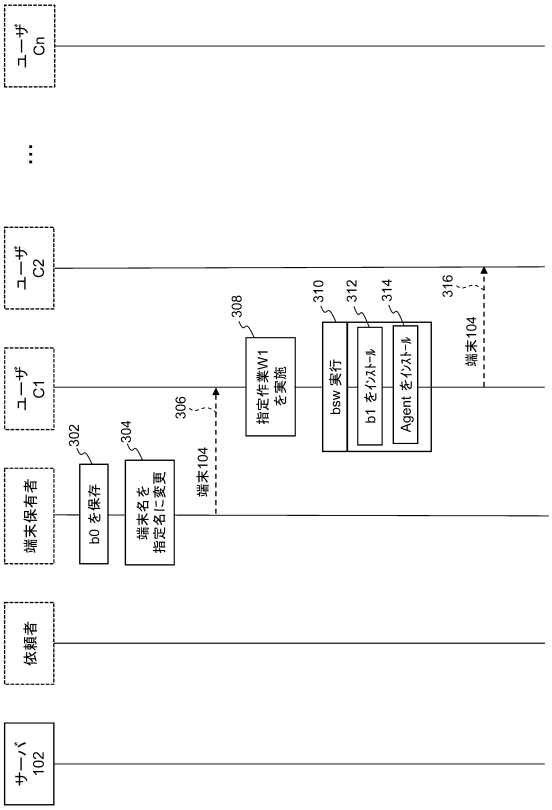
【図１】


100
120
102
サーバ
106
140
104
端末

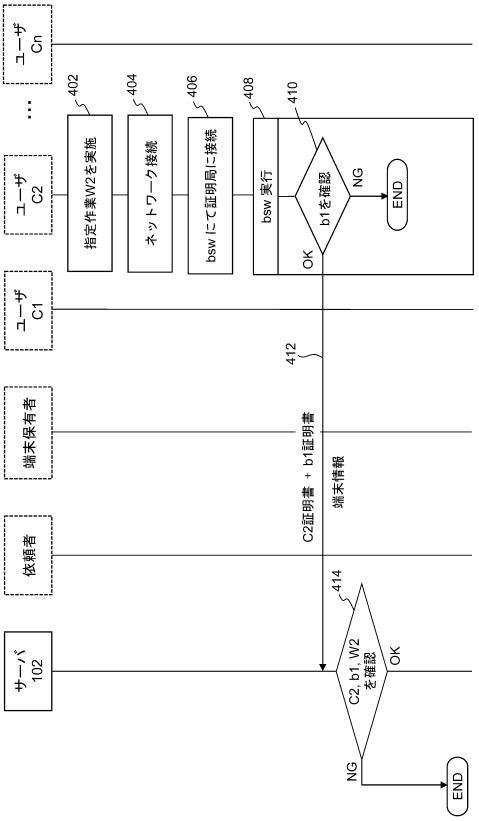
【図２】


ユーザ Cn
Cn証明書
bsw
ユーザ C2
C2証明書
bsw
ユーザ C1
C1証明書
bsw
204
端末保有者
206
端末名を指定
214
b0
依頼者
202
C1 証明書– Cn 証明書 作成 bsw 作成
証明書発行要求
208
212
b1証明書 – bn 証明書 作成
b1証明書、秘密鍵、Agent SWを暗号化したファイル b0を作成
サーバ 102
210

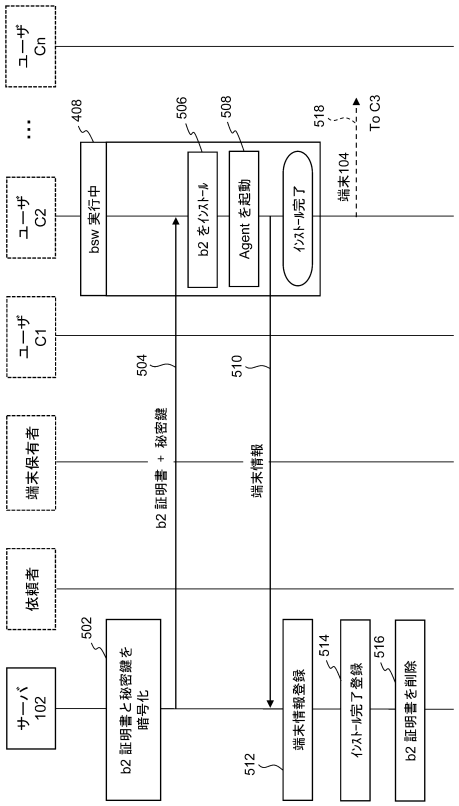
【図３】


ユーザ Cn
ユーザ C2
ユーザ C1
端末保有者
依頼者
サーバ 102
302
b0 を保存
304
端末名を 指定名に変更
306
端末104
308
指定作業W1 を実施
310
bsw 実行
312
b1 をインストール
314
Agent をインストール
316
端末104

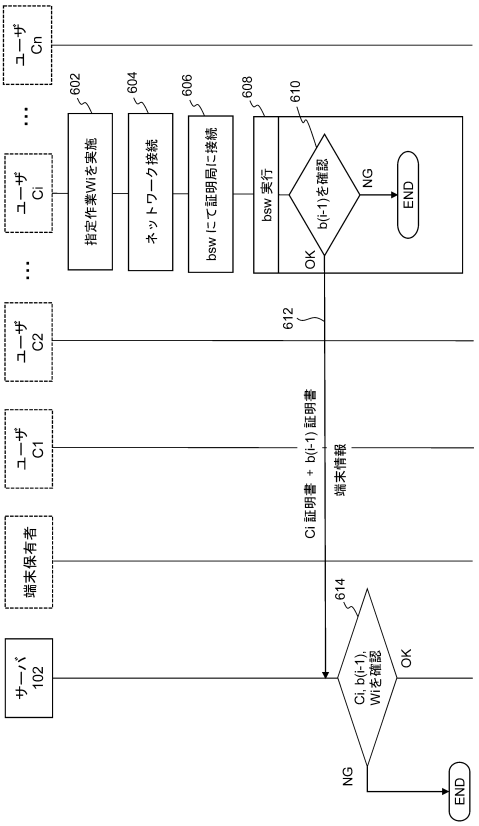
【図４】


ユーザ Cn
ユーザ C2
ユーザ C1
端末保有者
依頼者
サーバ 102
402
指定作業W2を実施
404
ネットワーク接続
406
bsw にて証明局に接続
408
bsw 実行
410
b1を確認
OK
NG
END
412
C2証明書 + b1証明書
端末情報
414
C2, b1, W2 を確認
OK
NG
END

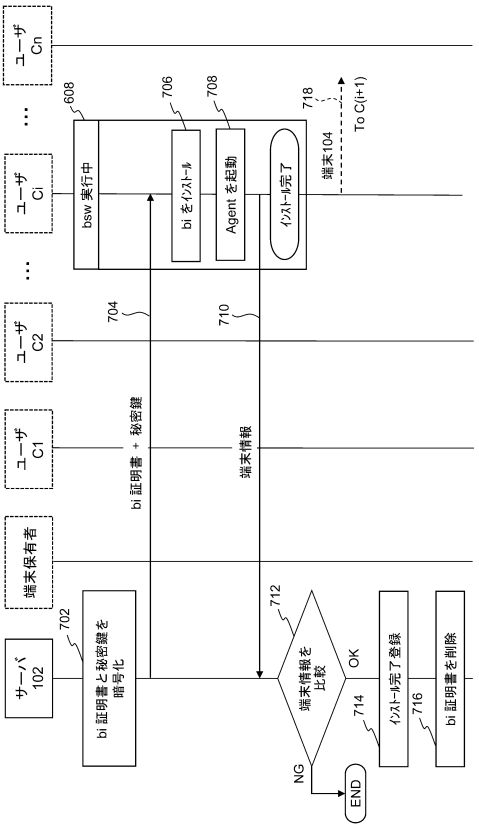
【図５】


ユーザ Cn
ユーザ C2
ユーザ C1
端末保有者
依頼者
サーバ 102
408
bsw 実行中
506
b2 をインストール
508
Agent を起動
インストール完了
518
To C3
端末104
502
b2 証明書と秘密鍵を暗号化
504
b2 証明書 + 秘密鍵
510
端末情報
512
端末情報登録
514
インストール完了登録
516
b2 証明書を削除

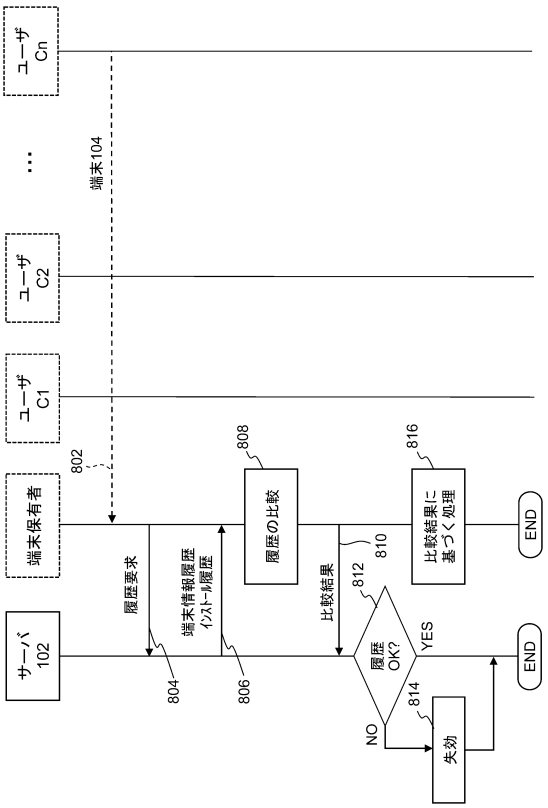
【図６】


ユーザ Cn
ユーザ Ci
ユーザ C2
ユーザ C1
端末保有者
サーバ 102
602
指定作業Wiを実施
604
ネットワーク接続
606
bsw にて証明局に接続
608
bsw 実行
610
b(i-1)を確認
OK
NG
END
612
Ci 証明書 + b(i-1) 証明書
端末情報
614
Ci, b(i-1), Wiを確認
OK
NG
END

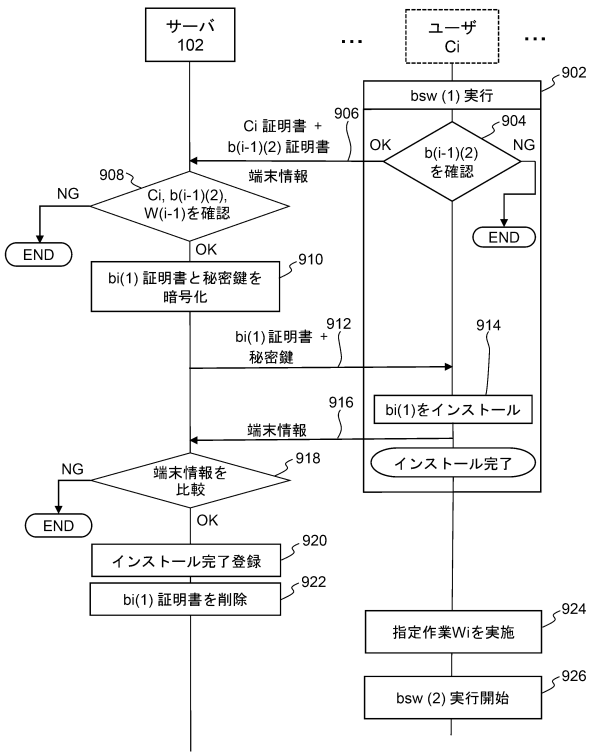
【図７】


ユーザ Cn
ユーザ Ci
ユーザ C2
ユーザ C1
端末保有者
サーバ 102
bsw 実行中
bi をインストール
Agent を起動
インストール完了
端末104
To C(i+1)
bi 証明書 + 秘密鍵
端末情報
bi 証明書と秘密鍵を暗号化
端末情報を比較
OK
NG
END
インストール完了登録
bi 証明書を削除

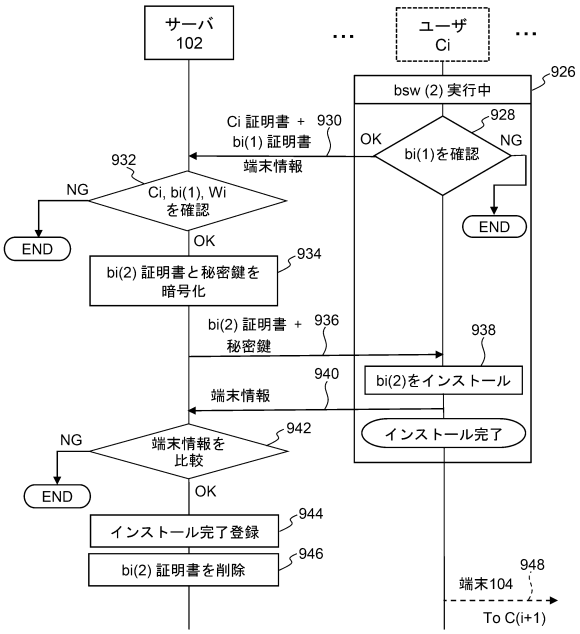
【図８】


ユーザ Cn
ユーザ C2
ユーザ C1
端末保有者
サーバ 102
端末104
履歴要求
端末情報履歴
インストール履歴
履歴の比較
比較結果
履歴 OK?
YES
NO
比較結果に基づく処理
失効
END

【図９】


サーバ 102
ユーザ Ci
bsw (1) 実行
Ci 証明書 + b(i-1)(2) 証明書
b(i-1)(2) を確認
端末情報
Ci, b(i-1)(2), W(i-1)を確認
bi(1) 証明書と秘密鍵を暗号化
bi(1) 証明書 + 秘密鍵
bi(1)をインストール
インストール完了
端末情報を比較
インストール完了登録
bi(1) 証明書を削除
指定作業Wiを実施
bsw (2) 実行開始
OK
NG
END

【図１０】


サーバ 102
ユーザ Ci
bsw (2) 実行中
Ci 証明書 + bi(1) 証明書
bi(1)を確認
端末情報
Ci, bi(1), Wi を確認
bi(2) 証明書と秘密鍵を暗号化
bi(2) 証明書 + 秘密鍵
bi(2)をインストール
インストール完了
端末情報を比較
インストール完了登録
bi(2) 証明書を削除
端末104
To C(i+1)
OK
NG
END

フロントページの続き

(56)参考文献 特開２０１５－１３９１０４（ＪＰ，Ａ）
米国特許第９１７２６９９（ＵＳ，Ｂ１）

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／３３