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

特許第6833658号
(P6833658)

(45)発行日　令和3年2月24日(2021.2.24)　(24)登録日　令和3年2月5日(2021.2.5)

(51)Int.Cl.　F I
H04L 9/32 (2006.01)　H04L 9/00 675Z
G06F 21/44 (2013.01)　H04L 9/00 675D
H04L 9/00 675B
G06F 21/44

請求項の数 11　(全 27 頁)

(21)出願番号　特願2017-214996(P2017-214996)
(22)出願日　平成29年11月7日(2017.11.7)
(65)公開番号　特開2019-87889(P2019-87889A)
(43)公開日　令和1年6月6日(2019.6.6)
審査請求日　令和1年8月14日(2019.8.14)

(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　110002147
特許業務法人酒井国際特許事務所
(72)発明者　安次富　大介
東京都港区芝浦一丁目１番１号　株式会社東芝内

審査官　寺谷　大亮

(56)参考文献　米国特許出願公開第２０１４／０１０８８１０（ＵＳ，Ａ１）
特開２０１８－７０３９（ＪＰ，Ａ）

最終頁に続く

(54)【発明の名称】サーバ装置、機器、証明書発行方法、証明書要求方法、証明書発行プログラム及び証明書要求プログラム

(57)【特許請求の範囲】
【請求項１】
第１ネットワークに接続されたサーバ装置であって、
第２ネットワークに接続された機器から、前記機器のドメインを含み、前記ドメインの正当性を証明する証明書の発行要求を受信すると、前記発行要求を識別する識別情報を前記機器に送信する発行要求応答部と、
前記機器から、前記識別情報が指定された確認方式取得要求を受信すると、前記ドメインの存在の確認に使用されるトークンを前記機器に送信する確認方式応答部と、
前記機器から、前記トークンと署名データとを含むドメイン確認要求を受信すると、前記発行要求と前記ドメイン確認要求とを特定する特定情報を含むサーバＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）を前記機器に送信する確認要求応答部と、
前記第２ネットワークに接続された端末から、前記サーバＵＲＬを介して接続を受け付け、前記端末から、前記特定情報が指定された機器ＵＲＬ取得要求を受信すると、前記特定情報から前記ドメインと前記トークンとを特定し、前記ドメインと前記トークンとを含む機器ＵＲＬを、前記端末に送信する機器ＵＲＬ応答部と、
前記機器ＵＲＬの接続に成功した前記端末から、前記機器ＵＲＬから取得された前記トークンと前記署名データとを含むドメイン確認登録要求を受信した場合、前記証明書を発行する発行部と、
を備えるサーバ装置。
【請求項２】

前記署名データは、前記機器により生成された公開鍵をハッシュ関数にかけ秘密鍵で暗号化したデータである、
請求項１に記載のサーバ装置。
【請求項３】
前記発行要求は、ＣＳＲ（Ｃｅｒｔｉｆｉｃａｔｅ Ｓｉｇｎｉｎｇ Ｒｅｑｕｅｓｔ）を含み、
前記発行部は、前記機器ＵＲＬの接続に成功した前記端末から、前記ドメイン確認登録要求を受信した場合、前記ＣＳＲを前記サーバ装置の秘密鍵で署名することにより前記証明書を発行する、
請求項１に記載のサーバ装置。
【請求項４】
前記第１ネットワークは、インターネットであり、
前記第２ネットワークは、ローカルエリアネットワークである、
請求項１に記載のサーバ装置。
【請求項５】
第１ネットワークに接続されたサーバ装置と通信し、第２ネットワークに接続された端末と通信する、前記第２ネットワークに接続された機器であって、
前記機器のドメインの正当性を証明する証明書の発行要求を前記サーバ装置に送信し、前記サーバ装置から、前記発行要求を識別する識別情報を受信する発行要求送信部と、
前記識別情報が指定された確認方式取得要求を送信し、前記サーバ装置から、前記ドメインの存在の確認に使用されるトークンを受信する確認方式取得要求部と、
前記トークンと署名データとを、前記ドメインを含む機器ＵＲＬに配置するサーバ処理部と、
前記トークンと前記署名データとを含むドメイン確認要求を前記サーバ装置に送信し、前記サーバ装置から、前記ドメイン確認要求を特定する特定情報を含むサーバＵＲＬ（Ｕｎｉｆｏｒｍ Ｒｅｓｏｕｒｃｅ Ｌｏｃａｔｏｒ）を受信する確認要求送信部と、
前記サーバ装置から前記サーバＵＲＬを介して前記ドメインと前記トークンとを含む機器ＵＲＬを取得した前記端末から、前記機器ＵＲＬを介して接続を受け付ける受付部と、
前記端末が前記機器ＵＲＬの接続に成功した場合、前記サーバ装置から前記証明書を取得する取得部と、
を備える機器。
【請求項６】
前記サーバＵＲＬを含むコード情報を表示部に表示する表示制御部、
を更に備える、
請求項５に記載の機器。
【請求項７】
前記サーバＵＲＬを、第３ネットワークを介して前記端末に送信する通信制御部、
を更に備える、
請求項５に記載の機器。
【請求項８】
第１ネットワークに接続されたサーバ装置の証明書発行方法であって、
第２ネットワークに接続された機器から、前記機器のドメインを含み、前記ドメインの正当性を証明する証明書の発行要求を受信すると、前記発行要求を識別する識別情報を前記機器に送信するステップと、
前記機器から、前記識別情報が指定された確認方式取得要求を受信すると、前記ドメインの存在の確認に使用されるトークンを前記機器に送信するステップと、
前記機器から、前記トークンと署名データとを含むドメイン確認要求を受信すると、前記発行要求と前記ドメイン確認要求とを特定する特定情報を含むサーバＵＲＬ（Ｕｎｉｆｏｒｍ Ｒｅｓｏｕｒｃｅ Ｌｏｃａｔｏｒ）を前記機器に送信するステップと、
前記第２ネットワークに接続された端末から、前記サーバＵＲＬを介して接続を受け付

け、前記端末から、前記特定情報が指定された機器ＵＲＬ取得要求を受信すると、前記特定情報から前記ドメインと前記トークンとを特定し、前記ドメインと前記トークンとを含む機器ＵＲＬを、前記端末に送信するステップと、
前記機器ＵＲＬの接続に成功した前記端末から、前記機器ＵＲＬから取得された前記トークンと前記署名データとを含むドメイン確認登録要求を受信した場合、前記証明書を発行するステップと、
を含む証明書発行方法。
【請求項９】
第１ネットワークに接続されたサーバ装置と通信し、第２ネットワークに接続された端末と通信する、前記第２ネットワークに接続された機器の証明書要求方法であって、
前記機器のドメインの正当性を証明する証明書の発行要求を前記サーバ装置に送信し、前記サーバ装置から、前記発行要求を識別する識別情報を受信するステップと、
前記識別情報が指定された確認方式取得要求を送信し、前記サーバ装置から、前記ドメインの存在の確認に使用されるトークンを受信するステップと、
前記トークンと署名データとを、前記ドメインを含む機器ＵＲＬに配置するステップと、
前記トークンと前記署名データとを含むドメイン確認要求を前記サーバ装置に送信し、前記サーバ装置から、前記ドメイン確認要求を特定する特定情報を含むサーバＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）を受信するステップと、
前記サーバ装置から前記サーバＵＲＬを介して前記ドメインと前記トークンとを含む機器ＵＲＬを取得した前記端末から、前記機器ＵＲＬを介して接続を受け付ける受付部と、
前記端末が前記機器ＵＲＬの接続に成功した場合、前記サーバ装置から前記証明書を取得するステップと、
を含む証明書要求方法。
【請求項１０】
第１ネットワークに接続されたサーバ装置を、
第２ネットワークに接続された機器から、前記機器のドメインを含み、前記ドメインの正当性を証明する証明書の発行要求を受信すると、前記発行要求を識別する識別情報を前記機器に送信する発行要求応答部と、
前記機器から、前記識別情報が指定された確認方式取得要求を受信すると、前記ドメインの存在の確認に使用されるトークンを前記機器に送信する確認方式応答部と、
前記機器から、前記トークンと署名データとを含むドメイン確認要求を受信すると、前記発行要求と前記ドメイン確認要求とを特定する特定情報を含むサーバＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）を前記機器に送信する確認要求応答部と、
前記第２ネットワークに接続された端末から、前記サーバＵＲＬを介して接続を受け付け、前記端末から、前記特定情報が指定された機器ＵＲＬ取得要求を受信すると、前記特定情報から前記ドメインと前記トークンとを特定し、前記ドメインと前記トークンとを含む機器ＵＲＬを、前記端末に送信する機器ＵＲＬ応答部と、
前記機器ＵＲＬの接続に成功した前記端末から、前記機器ＵＲＬから取得された前記トークンと前記署名データとを含むドメイン確認登録要求を受信した場合、前記証明書を発行する発行部、
として機能させるための証明書発行プログラム。
【請求項１１】
第１ネットワークに接続されたサーバ装置と通信し、第２ネットワークに接続された端末と通信する、前記第２ネットワークに接続された機器を、
前記機器のドメインの正当性を証明する証明書の発行要求を前記サーバ装置に送信し、前記サーバ装置から、前記発行要求を識別する識別情報を受信する発行要求送信部と、
前記識別情報が指定された確認方式取得要求を送信し、前記サーバ装置から、前記ドメインの存在の確認に使用されるトークンを受信する確認方式取得要求部と、
前記トークンと署名データとを、前記ドメインを含む機器ＵＲＬに配置するサーバ処理

部と、
前記トークンと前記署名データとを含むドメイン確認要求を前記サーバ装置に送信し、前記サーバ装置から、前記ドメイン確認要求を特定する特定情報を含むサーバＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）を受信する確認要求送信部と、
前記サーバ装置から前記サーバＵＲＬを介して前記ドメインと前記トークンとを含む機器ＵＲＬを取得した前記端末から、前記機器ＵＲＬを介して接続を受け付ける受付部と、
前記端末が前記機器ＵＲＬの接続に成功した場合、前記サーバ装置から前記証明書を取得する取得部、
として機能させるための証明書要求プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明の実施形態はサーバ装置、機器、証明書発行方法、証明書要求方法、証明書発行プログラム及び証明書要求プログラムに関する。
【背景技術】
【０００２】
機器のなりすましを防ぐ技術が従来から知られている。例えば、認証局が、機器のドメインの正当性を証明するＤＶ（Ｄｏｍａｉｎ　Ｖａｌｉｄａｔｉｏｎ）証明書を発行するための技術が従来から知られている。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開２０１２－０４９７５２号公報
【非特許文献】
【０００４】
【非特許文献１】ＡＣＭＥ（Ａｕｔｏｍａｔｉｃ　Ｃｅｒｔｉｆｉｃａｔｅ　Ｍａｎａｇｅｍｅｎｔ　Ｅｎｖｉｒｏｎｍｅｎｔ）、［ｏｎｌｉｎｅ］、［平成２９年１０月２４日検索］、インターネット〈ＵＲＬ：ｈｔｔｐｓ：／／ｄａｔａｔｒａｃｋｅｒ．ｉｅｔｆ．ｏｒｇ／ｄｏｃ／ｄｒａｆｔ－ｉｅｔｆ－ａｃｍｅ－ａｃｍｅ／〉
【発明の概要】
【発明が解決しようとする課題】
【０００５】
しかしながら、従来の技術では、異なるネットワークに接続された機器の正当性を、より簡便に証明することが難しかった。
【課題を解決するための手段】
【０００６】
実施形態のサーバ装置は、第１ネットワークに接続されたサーバ装置であって、発行要求応答部と確認方式応答部と確認要求応答部と機器ＵＲＬ応答部と発行部とを備える。発行要求応答部は、第２ネットワークに接続された機器から、前記機器のドメインを含み、前記ドメインの正当性を証明する証明書の発行要求を受信すると、前記発行要求を識別する識別情報を前記機器に送信する。確認方式応答部は、前記機器から、前記識別情報が指定された確認方式取得要求を受信すると、前記ドメインの存在の確認に使用されるトークンを前記機器に送信する。確認要求応答部は、前記機器から、前記トークンと署名データとを含むドメイン確認要求を受信すると、前記発行要求と前記ドメイン確認要求とを特定する特定情報を含むサーバＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）を前記機器に送信する。機器ＵＲＬ応答部は、前記第２ネットワークに接続された端末から、前記サーバＵＲＬを介して接続を受け付け、前記端末から、前記特定情報が指定された機器ＵＲＬ取得要求を受信すると、前記特定情報から前記ドメインと前記トークンとを特定し、前記ドメインと前記トークンとを含む機器ＵＲＬを、前記端末に送信する。発行部は、前記機器ＵＲＬの接続に成功した前記端末から、前記機器ＵＲＬから取得された

前記トークンと前記署名データとを含むドメイン確認登録要求を受信した場合、前記証明書を発行する。

【図面の簡単な説明】

【０００７】

【図１】第１実施形態の証明書発行システムの構成の例を示す図。

【図２Ａ】第１実施形態の証明書発行システムの動作例を示すシーケンス図。

【図２Ｂ】第１実施形態の証明書発行システムの動作例を示すシーケンス図。

【図３】第２実施形態の証明書発行システムの構成の例を示す図。

【図４Ａ】第２実施形態の証明書発行システムの動作例を示すシーケンス図。

【図４Ｂ】第２実施形態の証明書発行システムの動作例を示すシーケンス図。

【図４Ｃ】第２実施形態の証明書発行システムの動作例を示すシーケンス図。

【図５Ａ】第３実施形態の証明書発行システムの動作例を示すシーケンス図。

【図５Ｂ】第３実施形態の証明書発行システムの動作例を示すシーケンス図。

【図５Ｃ】第３実施形態の証明書発行システムの動作例を示すシーケンス図。

【図６】第４実施形態の証明書発行システムの構成の例を示す図。

【図７Ａ】第４実施形態の証明書発行システムの動作例を示すシーケンス図。

【図７Ｂ】第４実施形態の証明書発行システムの動作例を示すシーケンス図。

【図８】第１乃至第４実施形態のサーバ装置、機器及び端末の主要部のハードウェア構成の例を示す図。

【発明を実施するための形態】

【０００８】

以下に添付図面を参照して、サーバ装置、機器、証明書発行方法、証明書要求方法、証明書発行プログラム及び証明書要求プログラムの実施形態を詳細に説明する。

【０００９】

（第１実施形態）

はじめに、インターネット上のウェブサーバ（以降、単に「ウェブサービス」と呼ぶ）が、ローカルネットワーク上の機器で動作するウェブサーバ（以降、単に「機器」と呼ぶ）と、ウェブサービスへアクセスする端末のウェブブラウザを介して、相互認証に基づいた暗号化通信を行うことの困難性について説明する。ここで、暗号化通信とは、例えばＨＴＴＰＳ（Ｈｙｐｅｒｔｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ　Ｓｅｃｕｒｅ）等のＴＬＳ（Ｔｒａｎｓｐｏｒｔ　Ｌａｙｅｒ　Ｓｅｃｕｒｉｔｙ）を利用する通信である。

【００１０】

具体的には、ユーザによる何らかの手動設定を伴わずに、以下の問題を解決することが難しい。

［問題１］ウェブブラウザ、及び、ウェブブラウザ上で動作するウェブサービスのフロントエンド（ウェブページとして制御されるインタフェース）が、ローカルネットワーク上の機器を発見することができない。

［問題２］機器が正規のサーバ証明書を持っていない。すなわち、ウェブブラウザ、及び、ウェブブラウザ上で動作するウェブサービスのフロントエンドが、信頼できる機器であることを検証できない。

［問題３］機器が、ウェブサービスの認証及びアクセス制御、並びに、ユーザの認証及びアクセス制御をできない。

【００１１】

［問題１］については、例えば次の解決策により解決できる。まず、ウェブサービスが機器のＩＰアドレスを登録するための登録インタフェースを用意する。次に、ユーザが、登録インタフェースを使用して機器のＩＰアドレスをウェブサービスに登録する。

【００１２】

［問題２］については、例えば次の解決策により解決できる。まず、ユーザが、認証局と、認証局による署名付きのルート証明書とを作成する。次に、ユーザが、ユーザにより

作成されたルート証明書をウェブブラウザに信頼できるルート証明書として登録する。次に、ユーザが、ユーザにより作成された認証局による署名付きのサーバ証明書を作成する。そして、ユーザが、サーバ証明書を機器に設定する。

【００１３】

［問題３］については、例えば次の解決策により解決できる。まず、機器に予めユーザＩＤ及びパスワードを設定する。そして、ウェブブラウザが機器にアクセスする際に、ユーザＩＤ及びパスワードによる認証をかける。

【００１４】

しかしながら、上記いずれの解決策も、ユーザに手動設定作業を強いるものであり、ユーザビリティ上の問題がある。また、上記［問題２］及び［問題３］の解決策については、ウェブサービスが機器の正当性を、機器がウェブサービスの正当性を、それぞれ正規に検証できていない。そのため、悪意のあるユーザによって、悪意のある機器や、悪意のあるウェブサービスとの通信が容易に実現できてしまう。

【００１５】

上述の［問題２］は、機器が信頼できるサーバ証明書を持っていないことが主な原因である。しかしながら、正規の認証局は、グローバルアクセス可能なドメインを持ち、かつ、管理主体が明確なサーバに対して証明書を発行することが一般的である。そのため、インターネットとは異なるネットワークであるローカルネットワーク上の機器に対して正規のサーバ証明書を発行する方法は知られていない。

【００１６】

非特許文献１は、ウェブサービスに対して、ＤＶ証明書を発行する認証局の標準仕様を定めたものである。ＤＶ証明書とは、ドメインの存在検証のみを前提に発行するサーバ証明書のことであり、インターネット上のパブリックな認証局が発行する証明書の中で最も信頼性が低い証明書である。すなわち、ドメインの存在検証が、パブリックな認証局が発行するサーバ証明書の最低限のルールと言い換えることもできる。しかしながら、インターネット上の認証局は、ファイアウォールやＮＡＴ（Ｎｅｔｗｏｒｋ　Ａｄｄｒｅｓｓ　Ｔｒａｎｓｌａｔｉｏｎ）などの機能を有する中継装置が存在するため、ローカルネットワークの機器のドメイン存在検証ができない。

【００１７】

機器がサーバとして振る舞う場合、プライベートアドレス空間を持ち、更に、変化し得るＩＰアドレスを持つローカルサーバに対して、固定的な名前（ドメイン）をどの時点で付与するのか、そのドメインの存在検証をどのように行い、証明書を発行するのか等を解決することは難しい。

【００１８】

以下の説明では、ウェブサービスから、ローカルネットワーク上の機器に、ウェブブラウザを介して、安全に（クロスオリジン）アクセスできるようにする方法について説明する。ここでいう「安全に」とは、ウェブブラウザが、機器、ウェブサービス、及び、ウェブサービスのユーザが、正当であることを検証でき、かつ、暗号化通信を行うことができることを指す。

【００１９】

［証明書発行システムの構成の例］

図１は第１実施形態の証明書発行システム１００の構成の例を示す図である。第１実施形態の証明書発行システム１００は、サーバ装置１０、機器２０、端末３０及び中継装置４０を備える。

【００２０】

サーバ装置１０は、第１ネットワーク５０１に接続されている。第１ネットワークは、インターネット等のＷＡＮ（Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）である。第１実施形態では、サーバ装置１０と端末３０間の通信、及び、サーバ装置１０と機器２０間の通信は、第１ネットワーク５０１を介して行われる。第１実施形態では、第１ネットワーク５０１が、インターネットである場合を例にして説明する。

【００２１】
機器２０及び端末３０は、第２ネットワーク５０２に接続されている。第２ネットワーク５０２は、宅内、オフィスまたは工場などのローカルネットワークである。ローカルネットワークの媒体は、例えば上位プロトコルでＩＰ通信を実現できるイーサネット（登録商標）、及び、無線ＬＡＮ等である。なお、イーサネット（登録商標）、及び、無線ＬＡＮ等と同等の機能を実現できるネットワークであれば、具体的な媒体や上位通信プロトコルは問わない。第１実施形態では、第２ネットワーク５０２が、無線ＬＡＮで構築されたローカルネットワーク（ホームネットワーク）である場合を例にして説明する。
【００２２】
第１実施形態のサーバ装置１０は、機器２０のドメインの正当性を証明する証明書を発行する認証局である。第１実施形態では、サーバ装置１０は、機器２０のメーカが運用しているインターネット上のウェブサービスの機能の一部として、機器２０の証明書を発行する機能を実現する。なお、サーバ装置１０は、機器２０のメーカとは異なる第三者により運用される認証局でもよい。
【００２３】
第１実施形態の機器２０は、第１ネットワーク５０１のウェブサービスから、端末３０の実行部３０１（第１実施形態では、ウェブブラウザ）を介してアクセスされる第２ネットワーク５０２上の機器である。機器２０は、ＨＴＴＰ（ＨｙｐｅｒＴｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）サーバ機能を備える。第１実施形態では、機器２０は、デジタルテレビである。機器２０がデジタルテレビの場合、第１ネットワーク５０１のウェブサービスは、例えば宅内のデジタルテレビを発見し、テレビリモコン機能を提供するテレビリモコンサービス（テレビ用クラウドサービス）である。第１実施形態では、テレビリモコンサービスが、サーバ装置１０により提供されるウェブサービスの機能の一部として実現されている場合を例にして説明する。
【００２４】
第１実施形態の端末３０は、ユーザにより操作される端末である。ここで、ユーザは、機器２０及び端末３０の所有者であり、機器２０のメーカにより提供されるウェブサービスのユーザでもある。第１実施形態では、端末３０はスマートフォン及びタブレット端末等のスマートデバイスである。なお端末３０はパーソナルコンピュータ等でもよい。
【００２５】
端末３０は実行部３０１を備える。実行部３０１は、サーバ装置１０が端末３０に機能を提供するためのインタフェース１０７を実行する。第１実施形態のインタフェース１０７は、サーバ装置１０から端末３０へ送信されるウェブページであり、第１実施形態の実行部３０１は、当該ウェブページを実行するウェブブラウザである。インタフェース１０７は、基本的に、ＨＴＭＬ（ＨｙｐｅｒＴｅｘｔ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ）、ＣＳＳ（Ｃａｓｃａｄｉｎｇ　Ｓｔｙｌｅ　Ｓｈｅｅｔｓ）、及び、ＪａｖａＳｃｒｉｐｔ（登録商標）コードにより構成されており、機器２０のドメインの存在を確認する機能（ドメイン確認部１０８）を実現する。なお実行部３０１は、ウェブブラウザに限られず、例えば端末３０で動作するアプリケーションでもよい。ユーザは、機器２０（第１実施形態では、デジタルテレビ）を、端末３０（第１実施形態では、スマートデバイス）の実行部３０１（第１実施形態では、ウェブブラウザ）で、テレビリモコンサービスのウェブ画面を表示及び操作する。
【００２６】
中継装置４０は、第１ネットワーク５０１に接続されたサーバ装置１０と、第２ネットワーク５０２に接続された機器２０及び端末３０との間の通信を中継する装置である。
【００２７】
次に、第１実施形態のサーバ装置１０の機能構成について説明する。第１実施形態のサーバ装置１０は、機器登録部１０１、機器認証部１０２、発行要求応答部１０３、確認方式応答部１０４、確認要求応答部１０５、インタフェース提供部１０６、インタフェース１０７、ドメイン確認部１０８、機器ＵＲＬ応答部１０９、確認結果受付部１１０及び発

行部１１１を備える。インタフェース提供部１０６は、インタフェース１０７を端末３０に提供する。インタフェース１０７は、ドメイン確認部１０８を備える。

【００２８】

機器登録部１０１は、機器２０により生成された鍵ペア（公開鍵及び秘密鍵）の公開鍵の登録要求を、機器２０から受け付けることにより、当該機器２０の機器登録を行う。

【００２９】

なお、機器登録の具体的な方法は任意でよい。例えば、機器登録部１０１は、機器メーカに対してＭＡＣ（Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｄｅ）鍵を予め発行する。次に、機器メーカは出荷前にＭＡＣ鍵を機器２０に埋め込む。次に、機器２０は、このＭＡＣ鍵で公開鍵に署名を付与し、署名付きの公開鍵を含む登録要求を機器登録部１０１に送信する。機器登録部１０１は、機器２０から登録要求を受け付けた場合、署名を検証することにより、ＭＡＣ鍵を発行した機器２０からの登録要求であるか否かを判定する。機器登録部１０１は、ＭＡＣ鍵を発行した機器２０からの登録要求である場合、当該登録要求に含まれる公開鍵を登録する。

【００３０】

機器認証部１０２は、機器登録部１０１により登録された機器２０から送信された通信データに含まれるパラメータ（公開鍵及び署名）を参照して、機器２０を認証する。具体的には、機器認証部１０２は、通信データに含まれる公開鍵が登録済みであり、かつ、通信データに含まれる署名が正しい場合、機器２０を認証する。なお、機器認証部１０２は、リプレイ攻撃を防止するための乱数及びランダム文字列（ｎｏｎｃｅ）を、機器２０に発行する機能を備える。

【００３１】

発行要求応答部１０３は、機器登録部１０１により登録された機器２０から証明書の発行要求を受け付ける。具体的には、発行要求応答部１０３は、上記機器認証部１０２による機器認証が通った場合に、機器２０からＣＳＲ（Ｃｅｒｔｉｆｉｃａｔｅ Ｓｉｇｎｉｎｇ Ｒｅｑｕｅｓｔ）を、発行要求のパラメータとして受け付ける。なお、このＣＳＲは、ローカルネットワーク上で用いるドメイン名（ｄｉｇｉｔａｌ＿ｔｖ．ｌｏｃａｌ及びｄｉｇｉｔａｌ＿ｔｖ．ｈｏｍｅ．ａｒｐｈａ等、以降、「ローカルドメイン」と呼ぶ）に対する証明書署名要求である。

【００３２】

確認方式応答部１０４は、証明書の発行要求を送信した機器２０から、ドメインの確認方式（非特許文献１のＡＣＭＥでは、「チャレンジ」と呼ばれる）取得要求を受け付け、ＣＳＲがローカルドメインの証明書署名要求であった場合、確認方式情報を応答する。確認方式情報は、種別情報、識別情報及びトークンを含む。種別情報は、ローカルドメインに対する確認方法であることを示す情報（“ｈｔｔｐ－ｌｏｃａｌ－０１”等）を示す。識別情報は、チャレンジＩＤを示す。トークンは、ドメイン確認時に用いられる乱数などの数値列データ、及び、ランダム文字列データなどを含む。

【００３３】

確認要求応答部１０５は、機器２０から、チャレンジＩＤ、トークン、及び、登録時に用いた署名付きの公開鍵（以降、この公開鍵を「キー認可情報」とよぶ）を含むドメイン確認要求を受け付け、インタフェースのアドレスを示す検証ＵＲＬを応答する。検証ＵＲＬには、サーバ装置１０内で、機器２０からの証明書発行要求及びドメイン確認要求を一意に特定するための検証コード（特定情報）が含まれる。検証ＵＲＬの例は、例えば、ｈｔｔｐｓ：／／ｄｅｖｉｃｅ－ｃａ．ｅｘａｍｐｌｅ．ｃｏｍ／ｃｏｍｆｉｒｍ＿ｌｏｃａｌ＿ｄｏｍａｉｎ．ｈｔｍｌ＃ｃｏｄｅ＝ｘｘｘｘｘｘｘｘなどである。この例では、ｄｅｖｉｃｅ－ｃａ．ｅｘａｍｐｌｅ．ｃｏｍがサーバ装置１０のドメインであり、ｘｘｘｘｘｘｘｘが検証コードに相当する。

【００３４】

インタフェース提供部１０６は、機器２０のドメインをローカルネット上で確認するためのインタフェース１０７を提供する。第１実施形態では、インタフェース提供部１０６

は、ウェブサーバである。インタフェース提供部１０６は、ユーザ認証機能を備える。インタフェース提供部１０６は、ユーザ登録済みのログインユーザからの要求にのみ応答する。ログイン認証は、ウェブで広く用いられるＣｏｏｋｉｅベースのユーザセッション認証か、アクセストークン認証を用いるのが一般的であるが、これらに限定しない。インタフェース提供部１０６は、ログインしていないユーザからのアクセスには、ログイン画面を応答し、ユーザ認証を求める。

【００３５】

インタフェース１０７は、端末３０上で実現されるサーバ装置１０のフロントエンドである。第１実施形態では、インタフェース１０７はウェブページである。

【００３６】

ドメイン確認部１０８は、インタフェース１０７により実現される機能である。第１実施形態では、ドメイン確認部１０８は、ウェブページ内のＪａｖａＳｃｒｉｐｔ（登録商標）コードとして実現される。ドメイン確認部１０８は、上述の検証ＵＲＬに含まれる検証コードを、サーバ装置１０に送信する。次に、ドメイン確認部１０８は、機器２０によりサーバ装置１０に送信されたＣＳＲ情報及びトークン情報（より具体的には、機器のＨＴＴＰサーバ上のドメイン確認用の機器ＵＲＬ（ｈｔｔｐ（ｓ）：／／ｄｉｇｉｔａｌ－ｔｖ．ｌｏｃａｌ／．ｗｅｌｌ－ｋｎｏｗｎ／ａｃｍｅ－ｃｈａｌｌｅｎｇｅ／｛トークン｝など）を、サーバ装置１０から取得する。そして、ドメイン確認部１０８は、機器ＵＲＬにアクセスし、トークン及びキー認可情報を機器２０から取得する。

【００３７】

機器ＵＲＬ応答部１０９は、第２ネットワーク５０２に接続された端末３０上で、サーバ装置１０のフロントエンドとして実現されるドメイン確認部１０８から、検証ＵＲＬ（サーバＵＲＬ）を介して接続を受け付け、端末３０から、検証コード（特定情報）が指定された機器ＵＲＬ取得要求を受信すると、特定情報からドメインとトークンとを特定し、ドメインとトークンとを含む機器ＵＲＬを、端末３０に送信する。

【００３８】

確認結果受付部１１０は、機器ＵＲＬにアクセスしたドメイン確認部１０８から、トークン及びキー認可情報を含むパラメータを受け付ける。

【００３９】

発行部１１１は、確認結果受付部１１０により受け付けられたパラメータを使用して、チャレンジとして発行されたトークンが、チャレンジを発行した機器２０のドメインから取得出来たか否かを検証する。発行部１１１は、チャレンジとして発行されたトークンが、チャレンジを発行した機器２０のドメインから取得出来た場合、当該機器２０のＣＳＲを自身のもつサーバ証明書の秘密鍵で署名して、機器２０のドメインの証明書を生成する。発行部１１１は、機器２０から証明書の取得要求を受信すると、ドメイン確認が完了し、かつ、証明書の発行が完了していれば、当該取得要求の応答として、機器２０に証明書を送信する。

【００４０】

次に、第１実施形態の機器２０の機能構成について説明する。第１実施形態の機器２０は、入力制御部２０１、登録要求部２０２、ドメイン生成部２０３、ＣＳＲ生成部２０４、発行要求送信部２０５、確認方式取得要求部２０６、サーバ処理部２０７、確認要求送信部２０８、表示制御部２０９及び取得部２１０を備える。

【００４１】

入力制御部２０１は、ユーザによる入力操作を受け付ける。入力制御部２０１は、例えば端末３０の実行部３０１（第１実施形態では、ウェブブラウザ）からのアクセスを有効化する設定をＯＮにする入力操作を受け付ける。

【００４２】

登録要求部２０２は、機器２０で生成された公開鍵を含む機器登録用データを生成し、当該機器登録用データにより、サーバ装置１０の機器登録部１０１に登録要求を行う。機器登録用データの生成方法の説明は、図２Ａを用いて後述する。

【００４３】
ドメイン生成部２０３は、機器２０のドメインの名称であるドメイン名（ｄｏｍａｉｎ＿ｎａｍｅ）を生成する。
【００４４】
ＣＳＲ生成部２０４は、ドメイン生成部２０３により生成されたドメイン名（ｄｏｍａｉｎ＿ｎａｍｅ）の正当性を証明する証明書の署名要求（ＣＳＲ）を生成する。
【００４５】
発行要求送信部２０５は、機器２０のドメインの証明書の発行要求をサーバ装置１０に送信する。
【００４６】
確認方式取得要求部２０６は、確認方式取得要求（チャレンジ取得）をサーバ装置１０に送信し、ドメイン確認方式（チャレンジ）情報を取得する。確認方式取得要求及びドメイン確認方式（チャレンジ）情報の説明は、図２Ａを用いて後述する。
【００４７】
サーバ処理部２０７は、機器２０で動作させるＨＴＴＰサーバの処理を実行する。ＨＴＴＰサーバのアドレスは、ドメイン生成部２０３により生成されたドメイン名を含む。
【００４８】
確認要求送信部２０８は、機器２０のドメインの確認要求（チャレンジ選択）をサーバ装置１０に送信する。
【００４９】
表示制御部２０９は、ドメインの確認要求の応答として、サーバ装置１０から検証ＵＲＬを受信すると、この検証ＵＲＬをＱＲコード（登録商標）などのコード情報にして、表示部に表示する。
【００５０】
取得部２１０は、端末３０のインタフェース１０７からドメイン確認のためのアクセスを受けた契機で、証明書発行の可否をサーバ装置１０に定期的に問い合わせる。そして、取得部２１０は、サーバ装置１０の発行部１１１から証明書を取得すると、当該証明書を機器２０にインストールする。
【００５１】
［証明書発行システムの動作例］
次に、第１実施形態の証明書発行システム１００の動作例について説明する。
【００５２】
図２Ａ及び２Ｂは、第１実施形態の証明書発行システム１００の動作例を示すシーケンス図である。
【００５３】
はじめに、事前条件について説明する。
【００５４】
［事前条件１］サーバ装置１０（を運用する組織）は、事前に機器２０に対してＭＡＣ鍵（ｐｒｏｄｕｃｔ＿ｉｄ，ｐｒｏｄｕｃｔ＿ｓｅｃｒｅｔ）を払い出している。機器２０のメーカは、このＭＡＣ鍵を製造時に機器２０に埋め込んでいる。なお、このサーバ装置１０を運用する組織は、第１実施形態では、機器２０のメーカである。なお、ＭＡＣ鍵は、第１実施形態では、共通鍵としているが、例えばクライアント証明書のような非対称鍵であってもよい。
【００５５】
［事前条件２］ユーザは、機器２０（第１実施形態では、デジタルテレビ）の所有者であり、ウェブサービス（第１実施形態では、テレビリモコン機能等の遠隔制御などを実現するテレビ用クラウドサービス）に、例えばｅｍａｉｌアドレス及びパスワードによるユーザ登録を行っている。
【００５６】
はじめに、機器２０の入力制御部２０１が、端末３０の実行部３０１（第１実施形態で

は、ウェブブラウザ）からのアクセスを有効化する設定をＯＮにする入力操作を受け付ける（ステップＳ１）。この際、入力制御部２０１は、サーバ装置１０に登録済みのｅｍａｉｌアドレスを指定する入力操作を更に受け付けるようにしてもよい。また、入力制御部２０１は、認証局として動作するサーバ装置１０が複数ある場合、複数のサーバ装置１０の候補から、サーバ装置１０を選択する入力操作を更に受け付けてもよい。

【００５７】

次に、機器２０の登録要求部２０２が、機器登録用の鍵ペア（公開鍵（ｃｌｉｅｎｔ＿ｐｕｂ）及び秘密鍵（ｃｌｉｅｎｔ＿ｓｅｃｒｅｔ））を生成する（ステップＳ２）。

【００５８】

次に、機器２０の登録要求部２０２は、機器登録のためのｎｏｎｃｅの発行をサーバ装置１０に要求する（ステップＳ３）。サーバ装置１０の機器認証部１０２は、登録要求部２０２からｎｏｎｃｅの発行要求を受信すると、ｎｏｎｃｅを生成し、当該ｎｏｎｃｅを発行要求の応答として機器２０に送信する（ステップＳ３）。

【００５９】

次に、機器２０の登録要求部２０２は、機器登録用データを生成する。機器登録用データは、ｃｌｉｅｎｔ＿ｐｕｂ及びｎｏｎｃｅを少なくとも含む（ステップＳ４）。このとき、サーバ装置１０の機器登録部１０１が、事前にＭＡＣ鍵を払い出している製品（機器２０）からの登録のみを受け付けるようにする場合、機器２０の登録要求部２０２が、機器登録用データにｐｒｏｄｕｃｔ＿ｉｄを含め、これにｐｒｏｄｕｃｔ＿ｓｅｃｒｅｔで署名をつける。

【００６０】

次に、機器２０の登録要求部２２０は、ステップＳ４の処理により生成された機器登録用データで、サーバ装置１０の機器登録部１０１に登録要求を行う（ステップＳ５）。サーバ装置１０の機器登録部１０１は、ＭＡＣ、ｃｌｉｅｎｔ＿ｐｕｂ及びｎｏｎｃｅに対するｃｌｉｅｎｔ＿ｓｅｃｒｅｔによる署名を検証し、正しければ機器２０を登録する。

【００６１】

なお、上述のステップＳ２～ステップＳ５の処理は、サーバ装置１０への機器登録が既に実行されている場合は省略される。

【００６２】

次に、機器２０のドメイン生成部２０３が、ドメイン名（ｄｏｍａｉｎ＿ｎａｍｅ）を生成する（ステップＳ６）。このとき、ドメイン生成部２０３は、ｍＤＮＳを有効化し、ドメイン名（ｄｏｍａｉｎ＿ｎａｍｅ）が第２ネットワーク５０２上で衝突せずに使えることを確認する。例えば、１つの実現例として、ドメイン生成部２０３は、ｄｏｍａｉｎ＿ｎａｍｅを、＜ＵＵＩＤ＞．＜機器メーカが運用するサーバ装置のドメイン名＞．ｌｏｃａｌとする。ここで、ＵＵＩＤは、ＭＡＣ（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）アドレスなどから生成されるグローバルユニークな値である。サーバ装置１０のドメインが、ｄｔｖ．ｅｘａｍｐｌｅ．ｃｏｍだった場合には、例えば、２ｆａｃ１２３４－３１ｆ８－１１ｂ４－ａ２２２－０８００２ｂ３４ｃ００３．ｄｔｖ．ｅｘａｍｐｌｅ．ｃｏｍ．ｌｏｃａｌなどになる。この例はあくまで一例であり、第２ネットワーク５０２で衝突しない限りは、ドメイン名の生成方法は任意でよい。

【００６３】

次に、機器２０のＣＳＲ生成部２０４が、ステップＳ６の処理により生成されたｄｏｍａｉｎ＿ｎａｍｅの正当性を証明する証明書の署名要求（ＣＳＲ）を生成する（ステップＳ７）。なお、ＣＳＲ生成部２０４は、指定したユーザのｅｍａｉｌアドレスを、ＣＳＲのコンタクト情報に加えてもよい。

【００６４】

次に、機器２０の発行要求送信部２０５が、機器２０のドメインの証明書の発行要求をサーバ装置１０に送信する（ステップＳ８）。証明書の発行要求は、ステップＳ７の処理により生成されたＣＳＲを含む。サーバ装置１０の発行要求応答部１０３は、機器認証部１０２により機器２０が認証された場合、ＣＳＲを受け付け、応答として、識別情報（ａ

ｕｔｈｚ＿ｉｄ）、及び、パス情報（ｃｅｒｔ＿ｕｒｉ）を機器２０に送信する。識別情報（ａｕｔｈｚ＿ｉｄ）は、証明書の発行要求を識別する情報である。パス情報（ｃｅｒｔ＿ｕｒｉ）は、証明書が発行された場合に、当該証明書が置かれる場所を示す情報である。このとき発行要求応答部１０３は、ＣＳＲに含まれるドメイン名がローカル用のドメインであることを示す情報を、ＣＳＲと合わせて記憶しておく。なお、ＣＳＲ内の情報を用いず、証明書の発行要求に、ローカルネットワーク向け証明書の発行であることを明示的に示すパラメータを含めるようにしてもよい。

【００６５】

次に、機器２０の確認方式取得要求部２０６が、識別情報（ａｕｔｈｚ＿ｉｄ）が指定された確認方式取得要求（チャレンジ取得）をサーバ装置１０に送信し、ドメイン確認方式（チャレンジ）情報を取得する（ステップＳ９）。サーバ装置１０の発行要求応答部１０３は、機器認証部１０２により機器２０が認証された場合、ローカルドメイン向けチャレンジ情報を応答する。ローカルドメイン向けチャレンジ情報は、チャレンジ識別情報、種別情報（“ｈｔｔｐ－ｌｏｃａｌ－０１”など）、及び、トークンを含む。

【００６６】

次に、機器２０のサーバ処理部２０７が、トークン、及び、署名データ（キー認可情報（ｋｅｙ＿ａｕｔｈｏｒｉｚａｔｉｏｎ））を、機器２０で動作させるＨＴＴＰサーバの特定パス（．ｗｅｌｌ－ｋｎｏｗｎ／ａｃｍｅ－ｃｈａｌｌｅｎｇｅ／｛ｔｏｋｅｎ｝等）に設置する（ステップＳ１０）。署名データは、公開鍵（ｃｌｉｅｎｔ＿ｐｕｂ）をハッシュ関数にかけて秘密鍵（ｃｌｉｅｎｔ＿ｓｅｃｒｅｔ）で暗号化したデータである。

【００６７】

次に、機器２０の確認要求送信部２０８が、サーバ処理部２０７によりＨＴＴＰサーバの準備ができた後、機器２０のドメインの確認要求（チャレンジ選択）をサーバ装置１０に送信する（ステップＳ１１）。サーバ装置１０の確認要求応答部１０５は、機器認証部１０２により機器２０が認証された場合、当該ドメイン確認要求を特定する一時的に有効な検証コード（ｃｏｄｅ）を特定情報として含む検証ＵＲＬ（ｖｅｒｉｆｉｃａｔｉｏｎ＿ｕｒｉ）を応答する。この検証ＵＲＬは、サーバ装置１０により提供されるインタフェース（ウェブ画面）のパスである。検証ＵＲＬは、例えば、前述したように、ｈｔｔｐｓ：／／ｄｔｖ．ｅｘａｍｐｌｅ．ｃｏｍ／ｃｏｎｆｉｒｍ＿ｌｏｃａｌ＿ｄｏｍａｉｎ．ｈｔｍｌ＃ｃｏｄｅ＝ｘｘｘｘｘｘｘｘなどになっていて、インタフェースのＪａｖａＳｃｒｉｐｔ（登録商標）コードから、検証コード（ｃｏｄｅ）が参照できる形になっている。

【００６８】

次に、機器２０の表示制御部２０９が、ステップＳ１１の応答として、サーバ装置１０から検証ＵＲＬを受信すると、この検証ＵＲＬをＱＲコード（登録商標）などのコード情報にして、表示部に表示する（ステップＳ１２）。なお表示制御部２０９は、そのまま検証ＵＲＬの文字列を表示してもよいが、ユーザがインタフェース１０７のパスを予め知っているなどの場合は、検証コードのみを表示してもよい。

【００６９】

次に、端末３０の実行部３０１が、ステップＳ１２の処理により表示されたコード情報を読み込むことにより取得された検証ＵＲＬにアクセスし、インタフェース１０７（ドメイン確認ウェブ画面）に遷移する（ステップＳ１３）。

【００７０】

次に、端末３０のインタフェース１０７は、ユーザがログインしていなければ、ログイン操作を受け付ける（ステップＳ１４）。

【００７１】

次に、インタフェース１０７上のドメイン確認部１０８は、検証ＵＲＬに含まれる検証コード（ｃｏｄｅ）を、ドメイン確認要求を特定する特定情報として取得し、当該検証コードをパラメータとして含む機器ＵＲＬ取得要求をサーバ装置１０に送信する（ステップＳ１５）。サーバ装置１０の機器ＵＲＬ応答部１０９は、機器２０のＨＴＴＰサーバのド

メイン確認用ＵＲＬ情報である機器ＵＲＬ（ｄｅｖｉｃｅ＿ｕｒｉ）を、機器ＵＲＬ取得要求の応答として、端末３０に送信する。

【００７２】

機器ＵＲＬ（ｄｅｖｉｃｅ＿ｕｒｉ）は、機器のドメイン（ドメイン名）及びトークンを含む。ｄｅｖｉｃｅ＿ｕｒｉは、例えばｈｔｔｐ（ｓ）：／／｛ｄｏｍａｉｎ＿ｎａｍｅ｝／．ｗｅｌｌ－ｋｎｏｗｎ／ａｃｍｅ－ｃｈａｌｌｅｎｇｅ／｛ｔｏｋｅｎ｝などである。

【００７３】

次に、端末３０のインタフェース１０７（ドメイン確認部１０８）は、機器２０によりトークンが設置されているパスを示す機器ＵＲＬ（ｄｅｖｉｃｅ＿ｕｒｉ）を含むパラメータを実行部３０１に渡すことにより、実行部３０１に機器２０のドメインの存在確認を依頼する（ステップＳ１６）。

【００７４】

次に、端末３０の実行部３０１は、機器ＵＲＬにアクセスし、トークン及びキー認可情報を取得し、トークン及びキー認可情報をインタフェース１０７（ドメイン確認部１０８）に応答する（ステップＳ１７）。

【００７５】

次に、機器２０の取得部２１０が、端末３０のインタフェース１０７からのアクセスを契機に、証明書発行の可否をサーバ装置１０に定期的に問い合わせる（ステップＳ１８）。

【００７６】

次に、端末３０のインタフェース１０７（ドメイン確認部１０８）は、トークン及びキー認可情報を含むドメイン確認登録要求をサーバ装置１０の確認結果受付部１１０に送付する（ステップＳ１９）。

【００７７】

次に、サーバ装置１０の確認結果受付部１１０が、ステップＳ１９の処理により送信されたトークン及びキー認可情報を受け付けると、発行部１１１が、トークン及びキー認可情報を検証する（ステップＳ２０）。具体的には、確認結果受付部１１０は、ステップＳ１１の処理によりドメインの確認要求を送信した機器２０、及び、当該ドメイン確認要求に含まれていたトークンと、ステップＳ１９の処理により端末３０から受け付けたトークン及びキー認可情報（ステップＳ１７の処理により機器２０のＨＴＴＰサーバから取得されたトークン及びキー認可情報）とが一致するか否かを検証する。

【００７８】

次に、サーバ装置１０の発行部１１１は、ステップＳ２０の検証処理が成功した場合、ステップＳ８の処理により送信された証明書の発行要求により、機器２０から送信されたＣＳＲを、サーバ装置１０の秘密鍵で署名して証明書を発行する（ステップＳ２１）。

【００７９】

この際、発行部１１１は、ステップＳ１９の処理により送信されたドメイン確認登録要求への応答として、証明書を返してもよい（ｏｐｔｉｏｎａｌ）。この場合、端末３０のインタフェース１０７は、サーバ装置１０から受信した証明書を実行部３０１（第１実施形態では、ウェブブラウザ）に信頼できる証明書として登録するよう要求する（ステップＳ２２）。次に、実行部３０１は、ステップＳ２２の処理により登録の要求をされた証明書を、信頼できる証明書として登録する（ステップＳ２３）。この際、実行部３０１は、ステップＳ２３の処理により登録された証明書を信頼できる証明書として扱うドメインを合わせて登録し、他のドメインからは信頼できる証明書として見えないようにしてもよい。

【００８０】

一方、機器２０の取得部２１０は、定期的に送信する証明書発行要求への応答に含まれる状態情報が「発行済」になっていることを確認する（ステップＳ２４）。次に、取得部２１０は、サーバ装置１０の発行部１１１から証明書を取得すると（ステップＳ２５）、

当該証明書を機器２０にインストールする（ステップＳ２６）。
【００８１】
以上説明した第１実施形態の証明書発行システム１００によれば、第１ネットワーク５０１（インターネット）上のウェブサービスからアクセス可能なサーバ証明書が、第２ネットワーク５０２（ローカルネットワーク）上の機器２０のＨＴＴＰサーバに発行できている。
【００８２】
なお第１実施形態では、機器２０がデジタルテレビである場合を例にして説明したが、機器２０はデジタルテレビに限られない。機器２０は、例えば、デジタルテレビ以外の家電機器、住宅設備機器、工場の設備機器、及び、ビルの設備機器などであってもよい。第１実施形態の証明書発行システム１００は、インターネット上のウェブページからローカルネットワーク上の機器へ安全にアクセスする方法として、幅広い適用範囲が想定される。
【００８３】
（第２実施形態）
次に第２実施形態について説明する。第２実施形態の説明では、第１実施形態と同様の説明については省略し、第１実施形態と異なる箇所について説明する。
【００８４】
第１実施形態は、機器２０が、ＱＲコード（登録商標）などのコード情報を表示可能な相応の情報表示能力を持っていることを前提とした方式であった。第２実施形態では、コード情報などを用いて、上述の検証ＵＲＬ（ｖｅｒｉｆｉｃａｔｉｏｎ＿ｕｒｉ）を端末３０に伝えられない機器２０を対象にした実施形態について述べる。第２実施形態では、機器２０がエアコンである場合を例にして説明する。
【００８５】
［証明書発行システムの構成の例］
図３は第２実施形態の証明書発行システム１００の構成の例を示す図である。第２実施形態の証明書発行システム１００は、サーバ装置１０、機器２０、端末３０及び中継装置４０を備える。
【００８６】
第２実施形態では、第３ネットワーク５０３が追加されている。また、機器２０には、第３ネットワーク５０３を介して端末３０と通信する通信制御部２１１が追加されている。
【００８７】
第３ネットワーク５０３は、機器２０及び端末３０が安全に（情報漏洩せずに）通信できるネットワークである。具体的には、第３ネットワーク５０３の通信方式は、有線方式であっても無線方式であってもよい。有線方式の場合は、例えばＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）、ＨＤＭＩ（登録商標）（Ｈｉｇｈ－Ｄｅｆｉｎｉｔｉｏｎ　Ｍｕｌｔｉｍｅｄｉａ　Ｉｎｔｅｒｆａｃｅ）、及び、ＳＤＩＯ（Ｓｅｃｕｒｅ　Ｄｉｇｉｔａｌ　Ｉｎｐｕｔ／Ｏｕｔｐｕｔ）などである。無線方式の場合は、ＮＦＣ（Ｎｅａｒ　Ｆｉｅｌｄ　Ｃｏｍｍｕｎｉｃａｔｉｏｎ）などの近接無線、及び、ＢＬＥ（Ｂｌｕｅｔｏｏｔｈ（登録商標）　Ｌｏｗ　Ｅｎｅｒｇｙ）などの安全性の高い近距離無線通信である。第２実施形態では、第３ネットワーク５０３の通信方式がＢＬＥである場合を例にして説明する。
【００８８】
機器２０の通信制御部２１１は、第３ネットワーク５０３を介して端末３０と通信する。第２実施形態では、通信制御部２１１は、端末３０との間のＢＬＥ通信を制御する。
【００８９】
［証明書発行システムの動作例］
次に、第２実施形態の証明書発行システム１００の動作例について説明する。
【００９０】

図４Ａ乃至４Ｃは、第２実施形態の証明書発行システム１００の動作例を示すシーケンス図である。第１実施形態では、機器２０側から証明書の発行処理を開始したが、第２実施形態では、端末３０側から証明書の発行処理を開始する。

【００９１】

事前条件の説明は、第１実施形態と同じなので省略する。

【００９２】

はじめに、端末３０のユーザが、エアコン操作ウェブサービス（例えば、ｈｔｔｐｓ：／／ａｉｒｃｏｎ．ｅｘａｍｐｌｅ．ｃｏｍ）の画面をロードする（ステップＳ１）。

【００９３】

次に、サーバ装置１０が、ステップＳ１の処理によりロードされた画面を介して、ユーザのログインを受け付ける（ステップＳ２）。サーバ装置１０は、ログインを受け付けると、インタフェース１０７（第２実施形態では、機器２０のドメイン確認用ウェブ画面）を端末３０に送信する。

【００９４】

次に、端末３０のインタフェース１０７が、機器２０の証明書発行確認画面の表示要求を実行部３０１（ウェブブラウザ）に入力する（ステップＳ３）。このとき、ステップＳ２の処理によりログインしたユーザのユーザ情報（ｅｍａｉｌアドレスなど）や、サーバ装置情報（機器２０が証明書の発行要求などを送信するサーバ装置１０のＵＲＬドメイン名など）を、実行部３０１に渡すようにしてもよい。

【００９５】

次に、端末３０の実行部３０１が、証明書発行確認画面を表示する（ステップＳ４）。証明書発行確認画面は、例えば「ホームネットワークにあるエアコンを見つけて、このページから制御できるようにしますか？［ＯＫ］，［キャンセル］」などのメッセージを表示する。

【００９６】

次に、端末３０の実行部３０１は、ステップＳ４の処理により表示された証明書発行確認画面のＯＫボタンの押下を受け付ける（ステップＳ５）。

【００９７】

次に、端末３０の実行部３０１は、機器３０のＢＬＥ通信機能を利用して、ＨＴＴＰサーバ機能を持つ機器２０を探索する（ステップＳ６）。なお、検索の粒度は任意でよい。探索の粒度は、例えばエアコンを示す機器種別、特定機種、または、サーバ装置１０から機器２０に払い出されているＭＡＣ鍵ＩＤ（ｐｒｏｄｕｃｔ＿ｉｄ）などである。

【００９８】

次に、端末３０の実行部３０１は、ＨＴＴＰサーバ機能を持つ機器２０からステップＳ６の検索処理の応答を受信すると、ＭＡＣ鍵のＩＤ（ｐｒｏｄｕｃｔ＿ｉｄ）、及び、機器名などの機器情報の取得要求を当該機器２０に送信する（ステップＳ７）。

【００９９】

次に、端末３０の実行部３０１は、機器２０が複数みつかることもあるため、機器の選択画面を表示する（ステップＳ８）。

【０１００】

次に、端末３０の実行部３０１は、ステップＳ８の処理により表示された選択画面を介して、機器の選択を受け付ける（ステップＳ９）。

【０１０１】

次に、端末３０の実行部３０１は、端末３０のＢＬＥ通信機能を利用して、機器２０の証明書の発行要求を機器２０に送信する（ステップＳ１０）。この際、実行部３０１は、証明書の発行要求のパラメータに、上述のユーザ情報、及び、上述のサーバ装置情報を設定する。

【０１０２】

次に、機器２０の登録要求部２０２が、機器登録のためのｎｏｎｃｅの発行をサーバ装置１０に要求する（ステップＳ１１）。この際、登録要求部２０２は、ＨＴＴＰＳ通信を

用いることで、サーバ装置１０のサーバ証明書を検証することができる。
【０１０３】
次に、機器２０は、ＬＥＤ（Ｌｉｇｈｔ　Ｅｍｉｔｔｉｎｇ　Ｄｉｏｄｅ）を光らせることにより、ステップＳ１０の処理により送信された発行要求の受信を知らせる（ステップＳ１２）。
【０１０４】
次に、機器２０は、機器２０のボタンの押下等により、証明書の発行を許諾する操作を受け付ける（ステップＳ１３）。ユーザは、端末３０の実行部３０１で選択した機器２０と、実際の機器２０が一致していることを確認のうえ、機器２０のボタンを押下することにより、証明書の発行を改めて許諾する。
【０１０５】
ステップＳ１４～ステップＳ２２の処理の説明は、第１実施形態のステップＳ２、及び、ステップＳ４～ステップＳ１１の説明と同様のため省略する。
【０１０６】
次に、端末３０の実行部３０１は、ステップＳ１０の処理により送信された発行要求の応答（ｏｋ）を受信すると、サーバ装置１０の検証ＵＲＬ（ｖｅｒｉｆｉｃａｔｉｏｎ＿ｕｒｉ）を、ＢＬＥ機能を利用して取得し、当該検証ＵＲＬをインタフェース１０７に返す（ステップＳ２３）。
【０１０７】
ステップＳ２４～ステップＳ３５の処理の説明は、第１実施形態のステップＳ１５～ステップＳ２６の説明と同様のため省略する。
【０１０８】
以上説明した第２実施形態の証明書発行システム１００によれば、機器２０が表示機能を持たない場合であっても、セキュアな近距離通信（例えばＢＬＥ）を利用することにより、第１実施形態と同様の効果が得られる。
【０１０９】
（第３実施形態）
次に第３実施形態について説明する。第３実施形態の説明では、第１及び第２実施形態と同様の説明については省略し、第１及び第２実施形態と異なる箇所について説明する。
【０１１０】
第１及び第２実施形態では、機器２０が中継装置４０を介してサーバ装置１０と通信できることを前提としていた。第３実施形態では、インターネットなどの第１ネットワーク５０１への接続ができない機器２０を対象にした実施形態について説明する。
【０１１１】
第３実施形態の証明書発行システム１００の構成は、第１実施形態の証明書発行システム１００（図１参照）と同じである。
【０１１２】
［証明書発行システムの動作例］
次に、第３実施形態の証明書発行システム１００の動作例について説明する。
【０１１３】
図５Ａ乃至５Ｃは、第３実施形態の証明書発行システム１００の動作例を示すシーケンス図である。第３実施形態は、第２実施形態と同様に、端末３０側から機器２０の証明書の発行処理を開始する。
【０１１４】
事前条件の説明は、第１実施形態と同じなので省略する。
【０１１５】
ステップＳ１及びステップＳ２の処理の説明は、第２実施形態のステップＳ１～ステップＳ２の説明と同様のため省略する。
【０１１６】
次に、端末３０のインタフェース１０７が、ｎｏｎｃｅの発行をサーバ装置１０に要求

する（ステップＳ３）。
【０１１７】
次に、端末３０のインタフェース１０７は、機器２０の証明書の発行要求を実行部３０１（第３実施形態では、ウェブブラウザ）に依頼する（ステップＳ４）。証明書の発行要求は、ユーザ情報（ｕｓｅｒ＿ｉｎｆｏ）、サーバ装置１０のサーバ証明書（ｄｅｖｉｃｅ＿ｃａ＿ｉｎｆｏ）、及び、ステップＳ３の処理により取得されたｎｏｎｃｅを含む。
【０１１８】
ステップＳ５～ステップＳ１０の処理の説明は、第２実施形態のステップＳ４～ステップＳ９の説明と同様のため省略する。
【０１１９】
次に、端末３０の実行部３０１が、ＣＳＲ生成要求を機器２０に送信する（ステップＳ１１）。ＣＳＲ生成要求は、ユーザ情報（ｕｓｅｒ＿ｉｎｆｏ）、サーバ装置１０のサーバ証明書（ｄｅｖｉｃｅ＿ｃａ＿ｉｎｆｏ）、及び、ステップＳ３の処理により取得されたｎｏｎｃｅを含む。
【０１２０】
次に、機器２０は、ステップＳ１１の処理により送信されたＣＳＲ生成要求に含まれるサーバ証明書（ｄｅｖｉｃｅ＿ｃａ＿ｉｎｆｏ）を検証する（ステップＳ１２）。具体的には、機器２０は、予め機器の中にインストールされている信頼できる認証局の証明書を示す情報に基づいて、サーバ証明書（ｄｅｖｉｃｅ＿ｃａ＿ｉｎｆｏ）を検証する。
【０１２１】
ステップＳ１３の処理の説明は、第２実施形態のステップＳ１３の説明と同様のため省略する。ステップＳ１４及びステップＳ１５の説明は、第２実施形態のステップＳ１７及びステップＳ１８の説明と同様のため省略する。
【０１２２】
次に、機器２０のＣＳＲ生成部２０４が、ＣＳＲ及びｎｏｎｃｅをｐｒｏｄｕｃｔ＿ｓｅｃｒｅｔにより署名（ＭＡＣ）を生成する（ステップＳ１６）。機器２０のＣＳＲ生成部２０４は、署名（ＭＡＣ）が生成できた時点で、ステップＳ１１の処理により送信されたＣＳＲ生成要求の応答（ｏｋ）を端末３０に送信する。
【０１２３】
次に、端末３０の実行部３０１は、ＣＳＲ生成要求の応答（ｏｋ）を受信すると、ＣＳＲ取得要求を機器２０に送信する（ステップＳ１７）。機器２０のＣＳＲ生成部２０４は、ＣＳＲ取得要求の応答として、ＣＳＲ、ＭＡＣ及びｐｒｏｄｕｃｔ＿ｉｄを端末３０に送信する。端末３０の実行部３０１は、ＣＳＲ、ＭＡＣ及びｐｒｏｄｕｃｔ＿ｉｄを、ステップＳ４の処理により送信された証明書の発行要求の応答として、インタフェース１０７に返す。
【０１２４】
次に、端末３０のインタフェース１０７が、証明書の発行要求をサーバ装置１０に送信する（ステップＳ１８）。証明書の発行要求は、ＣＳＲ、ＭＡＣ、及びｐｒｏｄｕｃｔ＿ｉｄをパラメータとして含む。
【０１２５】
次に、サーバ装置１０の発行要求応答部１０３が、ステップＳ１８の処理により送信された発行要求に含まれるＭＡＣを検証し、ｐｒｏｄｕｃｔ＿ｓｅｃｒｅｔを持っている機器２０による署名であることを確認したら（ステップＳ１９）、成功応答を返す。応答内容は、第１実施形態のステップ８の発行要求の応答と同様である。
【０１２６】
ステップＳ２０の説明は、機器２０からではなく、インタフェース１０７からの要求である点を除いて、第１実施形態のステップＳ９の説明と同様である。
【０１２７】
次に、端末３０のインタフェース１０７は、ステップＳ２０の処理により送信された確認方式取得要求（チャレンジ取得）の応答として返されるチャレンジを選択して、機器２

０のドメインの確認要求をサーバ装置１０に送信する（ステップＳ２１）。サーバ装置１０の確認要求応答部１０５は、確認方式取得要求に含まれる識別情報（ａｕｔｈｚ＿ｉｄ）から、ステップＳ１８の処理により送信された証明書の発行要求により端末３０から受信したＣＳＲを特定する。確認要求応答部１０５は、特定されたＣＳＲに含まれる機器２０のドメイン名（ｄｅｖｉｃｅ＿ｄｏｍａｉｎ）、トークン及びｎｏｎｃｅを、確認要求の応答として端末３０に送信する。

【０１２８】

次に、端末３０のインタフェース１０７が、機器２０のドメインの確認要求を実行部３０１に送信する（ステップＳ２２）。ドメインの確認要求は、ステップＳ２１の処理により送信された確認方式取得要求の応答に含まれるドメイン名、トークン及びｎｏｎｃｅを含む。

【０１２９】

次に、端末３０の実行部３０１は、端末３０のＢＬＥ機能を利用して、トークン及びｎｏｎｃｅを含むチャレンジ設置要求を機器２０に送信することにより、機器２０にＨＴＴＰサーバの起動を要求する（ステップＳ２３）。

【０１３０】

次に、機器２０のサーバ処理部２０７は、トークン、並びに、サーバ装置１０により提供されたｎｏｎｃｅ及びｐｒｏｄｕｃｔ＿ｉｄをあわせたデータのＭＡＣ（以降、「キー認可情報」と呼ぶ）を自身のＨＴＴＰサーバ経由でアクセス可能なディレクトリ（ドメイン確認用の機器ＵＲＬ）に保存し、必要であればＨＴＴＰサーバを起動ないし再起動して、端末３０の実行部３０１に応答を返す（ステップＳ２４）。機器ＵＲＬは、例えばｈｔｔｐ（ｓ）：／／ｄｉｇｉｔａｌ－ｔｖ．ｌｏｃａｌ／．ｗｅｌｌ－ｋｎｏｗｎ／ａｃｍｅ－ｃｈａｌｌｅｎｇｅ／｛トークン｝などである。

【０１３１】

次に、端末３０の実行部３０１が、ステップＳ２３の処理により送信されたチャレンジ設置要求の応答を受信すると、機器ＵＲＬにアクセスし、当該機器ＵＲＬから、ステップＳ２３の処理により機器２０により保存されたトークン及びキー認可情報を取得する（ステップＳ２５）。実行部３０１は、機器２０から取得されたトークン及びキー認可情報をインタフェース１０７に返す。

【０１３２】

次に、端末３０のインタフェース１０７は、証明書の取得要求をサーバ装置１０に送信する（ステップＳ２６）。証明書の取得要求は、トークン及びキー認可情報を含む。

【０１３３】

次に、サーバ装置１０の発行部１１１が、ステップＳ２６の処理により送信された取得要求に含まれるトークン及びキー認可情報を検証する（ステップＳ２７）。

【０１３４】

次に、サーバ装置１０の発行部１１１は、ステップＳ２７の検証処理の結果、ｐｒｏｄｕｃｔ＿ｓｅｃｒｅｔで署名したデータであることが確認できれば、機器２０の証明書を生成し、ステップＳ２６の処理により送信された取得要求の応答として、当該証明書を端末３０に送信する（ステップＳ２８）。

【０１３５】

次に、端末３０のインタフェース１０７が、ステップＳ２８の処理により生成された証明書を、機器２０に渡すように実行部３０１に指示する（ステップＳ２９）。

【０１３６】

次に、端末３０の実行部３０１が、ステップＳ２８の処理により生成された証明書のインストール要求を機器２０に送信する（ステップＳ３０）。

【０１３７】

次に、機器２０の取得部２１０が、ステップＳ３０の処理により送信されたインストール要求に含まれる証明書をインストールする（ステップＳ３１）。この際、取得部２１０は、署名を検証するなどして、意図した認証局により証明書を署名されていることを確認

してもよい。
【０１３８】
次に、端末３０の実行部３０１は、このインストール要求のシーケンス（ステップＳ２９～ステップＳ３１）の後に、ステップＳ２８の処理により生成された証明書を信頼できる証明書として、自身にもインストールしてもよい（ステップＳ３２）。
【０１３９】
以上説明した第３実施形態の証明書発行システム１００によれば、機器２０が第１ネットワーク５０１に接続する通信（第３実施形態では、インターネット通信）をしなくても、第１実施形態と同様の効果が得られる。
【０１４０】
（第４実施形態）
次に第４実施形態について説明する。第４実施形態の説明では、第２及び第３実施形態と同様の説明については省略し、第２及び第３実施形態と異なる箇所について説明する。
【０１４１】
第１～第３実施形態では、端末３０が、サーバ装置１０により生成されたウェブページ（インタフェース１０７）を利用して、機器２０のＨＴＴＰサーバにアクセスする場合について説明した。第４実施形態では、第３者サービスにより提供される第２インタフェース１２２（図６参照）が、機器２０のＨＴＴＰサーバにアクセスする場合について説明する。第４実施形態の具体例は、例えば機器２０がデジタルテレビであり、サーバ装置１０により提供される認証局サービスの提供事業者がデジタルテレビメーカであり、デジタルテレビメーカとは異なる事業者（第３者）が、テレビ用クラウドサービスを提供する場合である。
【０１４２】
［証明書発行システムの構成の例］
図６は第４実施形態の証明書発行システム１００の構成の例を示す図である。第４実施形態の証明書発行システム１００は、サーバ装置１０、第２サーバ装置１２、機器２０、端末３０及び中継装置４０を備える。第４実施形態では、第２実施形態の構成に加えて、第２サーバ装置１２が追加されている。また、サーバ装置１０には、第２サーバ装置１２の登録及び認証を行う機能（クライアント登録部１１２及びクライアント認証部１１３）が追加されている。
【０１４３】
第２サーバ装置１２は、機器２０にサーバ証明書を発行するサーバ装置１０とは異なる事業者が運営するウェブサービスを提供する。第２サーバ装置１２は、第２インタフェース１２２を端末３０に提供する第２インタフェース提供部１２１を備える。
【０１４４】
第２インタフェース１２２は、第２サーバ装置１２が、端末３０を介して、機器２０のＨＴＴＰサーバにアクセスするためのインタフェースである。第４実施形態では、第２インタフェース１２２はウェブページである。
【０１４５】
サーバ装置１０のクライアント登録部１１２は、クライアント（第２サーバ装置１２）からの登録要求を受信すると、クライアントクレデンシャル（クライアントＩＤ及びクライアントシークレット）を生成し、当該クライアントクレデンシャルを応答する。なお、上述の機器登録部１０１のように、クライアントから公開鍵を受信し、当該公開鍵をクライアントＩＤとみなす実現形態も考えられる。また、第２サーバ装置１２の運用者が、サーバ装置１０が提供するウェブページを介して、ユーザ登録のうえクレデンシャルを発行するような実現形態も考えられる。
【０１４６】
サーバ装置１０のクライアント認証部１１３は、クライアントクレデンシャルを用いてクライアント（第２サーバ装置１２）からの通信を認証する。
【０１４７】

［証明書発行システムの動作例］
次に、第４実施形態の証明書発行システム１００の動作例について説明する。
【０１４８】
図７Ａ及び７Ｂは、第４実施形態の証明書発行システム１００の動作例を示すシーケンス図である。
【０１４９】
事前条件は、第２及び第３実施形態の事前条件１及び２のほかに、以下の事前条件３及び４を更に追加する。
【０１５０】
［事前条件３］ユーザは、第２サーバ装置１２にもユーザ登録を行っている。
［事前条件４］第２サーバ装置１２（を運用する組織）は、サーバ装置１０にクライアント登録を行い、上述のクライアントクレデンシャルを予め取得している。
【０１５１】
はじめに、端末３０のユーザが、第２サーバ装置１２にアクセスし、第２インタフェース１２２を実行部３０１にロードする（ステップＳ１）。
【０１５２】
次に、端末３０のユーザは、第２サーバ装置１２に第２インタフェース１２２を介してログインする（ステップＳ２）。
【０１５３】
次に、端末３０の第２インタフェース１２２は、第２実施形態のステップＳ３～ステップＳ２３と同様の処理を行い、検証ＵＲＬ（ｖｅｒｉｆｉｃａｔｉｏｎ＿ｕｒｉ）を得る（図７Ａ、ステップＳ３）。または、端末３０の第２インタフェース１２２は、第３実施形態のステップＳ４～ステップＳ１７と同様の処理を行い、ｐｒｏｄｕｃｔ＿ｉｄ、ＣＳＲ及びＭＡＣを得る（図７Ｂ、ステップＳ３）。いずれの場合も、インタフェース部１２２は、実行部３０１に、ユーザ情報（ｕｓｅｒ＿ｉｎｆｏ）、及び、サーバ装置１０のサーバ証明書（ｄｅｖｉｃｅ＿ｃａ＿ｉｎｆｏ）だけでなく、第２サーバ装置１２の情報（ドメイン名（オリジン）など）（以降、「ｗｅｂ＿ａｐｐ＿ｉｎｆｏ」と呼ぶ）を渡してもよい。
【０１５４】
次に、端末３０の第２インタフェース１２２は、第２実施形態にならう場合、ｖｅｒｉｆｉｃａｔｉｏｎ＿ｕｒｉに、証明書発行後に戻る画面のＵＲＩ情報（リダイレクトＵＲＩ）を渡して、画面をリダイレクトする（図７Ａ、ステップＳ４）。また、第３実施形態にならう場合は、第２サーバ装置１２は、第２インタフェース１２２からｐｒｏｄｕｃｔ＿ｉｄ，ＣＳＲ及びＭＡＣを取得すると、ｐｒｏｄｕｃｔ＿ｉｄ，ＣＳＲ及びＭＡＣをサーバ装置１０に渡し、ｖｅｒｉｆｉｃａｔｉｏｎ＿ｕｒｉを応答として得て、その後、リダイレクトＵＲＩを渡して、画面をリダイレクトする（図７Ｂ、ステップＳ４）。
【０１５５】
次に、サーバ装置１０の発行部１１１は、第２実施形態にならう場合、第２実施形態のステップＳ２４～ステップＳ３２と同様の処理を行うことにより、証明書を発行する（図７Ａ、ステップＳ５）。また、第３実施形態にならう場合は、サーバ装置１０の発行部１１１は、第３実施形態のステップＳ１８～ステップＳ３２と同様の処理を行うことにより、証明書を発行する（図７Ｂ、ステップＳ５）。このとき、機器２０は、ｗｅｂ＿ａｐｐ＿ｉｎｆｏを使って、自身のドメイン名を生成したり、ＨＴＴＰサーバへのアクセスを第２インタフェース１２２から受け付けるように設定（ＣＯＲＳ（Ｃｒｏｓｓ　Ｏｒｉｇｉｎ　Ｒｅｓｏｕｒｃｅ　Ｓｈａｒｉｎｇ）設定）したりしてもよい。
【０１５６】
次に、サーバ装置１０及びインタフェース１０７は、証明書発行後、上述のリダイレクトＵＲＬに画面を遷移する（ステップＳ６）。
【０１５７】
以上説明した第４実施形態の証明書発行システム１００によれば、第２サーバ装置１２

の第２インタフェース１２２を起点にした機器２０への証明書発行が可能になる。
【０１５８】
最後に、第１乃至第４実施形態のサーバ装置１０、機器２０及び端末３０の主要部のハードウェア構成の例について説明する。なお第４実施形態の第２サーバ装置１２の主要部のハードウェア構成は、サーバ装置１０の主要部のハードウェア構成と同様である。
【０１５９】
［ハードウェア構成の例］
図８は第１乃至第４実施形態のサーバ装置１０、機器２０及び端末３０の主要部のハードウェア構成の例を示す図である。第１乃至第４実施形態のサーバ装置１０、機器２０及び端末３０は、制御装置４０１、主記憶装置４０２、補助記憶装置４０３、表示装置４０４、入力装置４０５及び通信装置４０６を備える。制御装置４０１、主記憶装置４０２、補助記憶装置４０３、表示装置４０４、入力装置４０５及び通信装置４０６は、バス４１０を介して接続されている。
【０１６０】
制御装置４０１は補助記憶装置４０３から主記憶装置４０２に読み出されたプログラムを実行する。制御装置４０１は、例えばＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）等の汎用のプロセッサである。主記憶装置４０２はＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）、及び、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）等のメモリである。補助記憶装置４０３はメモリカード、及び、ＨＤＤ（Ｈａｒｄ　Ｄｉｓｋ　Ｄｒｉｖｅ）等である。
【０１６１】
表示装置４０４は情報を表示する。表示装置４０４は、例えば液晶ディスプレイである。なお、第２実施形態の機器２０（例えばエアコンなど）は、表示装置４０４を備えていなくてもよい。入力装置４０５は、情報の入力を受け付ける。入力装置４０５は、例えばハードウェアキー、キーボード及びマウス等である。なお表示装置４０４及び入力装置４０５は、表示機能と入力機能とを兼ねる液晶タッチパネル等でもよい。通信装置４０６は他の装置と通信する。
【０１６２】
第１乃至第４実施形態のサーバ装置１０、機器２０及び端末３０で実行されるプログラムは、インストール可能な形式又は実行可能な形式のファイルでＣＤ－ＲＯＭ、メモリカード、ＣＤ－Ｒ、及び、ＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｋ）等のコンピュータで読み取り可能な記憶媒体に記憶されてコンピュータ・プログラム・プロダクトとして提供される。
【０１６３】
また第１乃至第４実施形態のサーバ装置１０、機器２０及び端末３０で実行されるプログラムを、インターネット等の第１ネットワーク５０１に接続されたコンピュータ上に格納し、第１ネットワーク５０１経由でダウンロードさせることにより提供するように構成してもよい。また第１乃至第４実施形態のサーバ装置１０、機器２０及び端末３０が実行するプログラムを、ダウンロードさせずにインターネット等の第１ネットワーク５０１経由で提供するように構成してもよい。
【０１６４】
また第１乃至第４実施形態のサーバ装置１０、機器２０及び端末３０で実行されるプログラムを、ＲＯＭ等に予め組み込んで提供するように構成してもよい。
【０１６５】
第１乃至第４実施形態のサーバ装置１０、機器２０及び端末３０で実行されるプログラムは、実施形態のサーバ装置１０、機器２０及び端末３０の機能構成のうち、プログラムにより実現可能な機能を含むモジュール構成となっている。
【０１６６】
プログラムにより実現される機能は、制御装置４０１が補助記憶装置４０３等の記憶媒体からプログラムを読み出して実行することにより主記憶装置４０２にロードされる。す

なわちプログラムにより実現される機能は、主記憶装置４０２上に生成される。

【０１６７】

なお第１乃至第４実施形態のサーバ装置１０、機器２０及び端末３０の機能の一部を、ＩＣ（Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ）等のハードウェアにより実現してもよい。

【０１６８】

本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

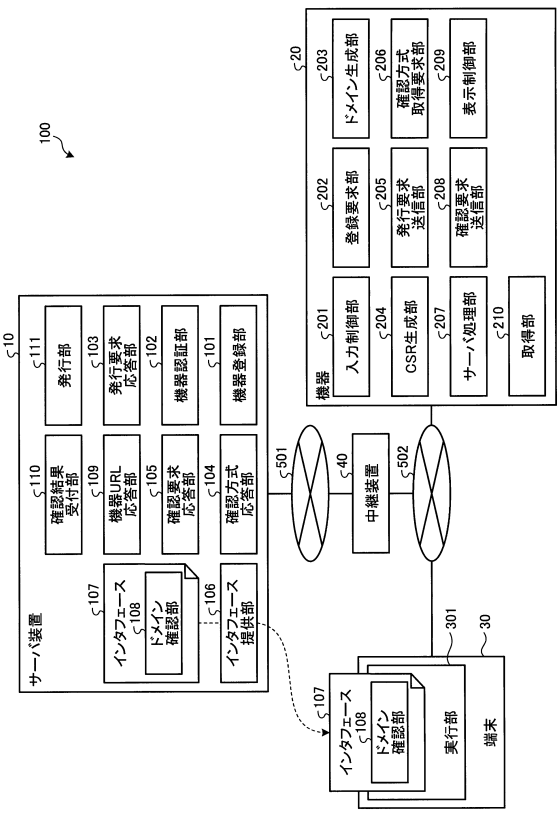
【符号の説明】

【０１６９】

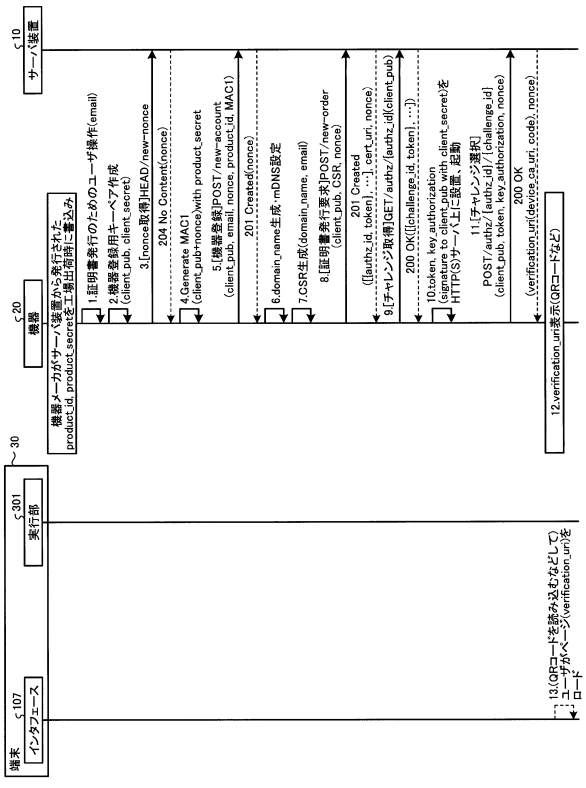
１０　サーバ装置
２０　機器
３０　端末
４０　中継装置
１００　証明書発行システム
１０１　機器登録部
１０２　機器認証部
１０３　発行要求応答部
１０４　確認方式応答部
１０５　確認要求応答部
１０６　インタフェース提供部
１０７　インタフェース
１０８　ドメイン確認部
１０９　機器ＵＲＬ応答部
１１０　確認結果受付部
１１１　発行部
１１２　クライアント登録部
１１３　クライアント認証部
２０１　入力制御部
２０２　登録要求部
２０３　ドメイン生成部
２０４　ＣＳＲ生成部
２０５　発行要求送信部
２０６　確認方式取得要求部
２０７　サーバ処理部
２０８　確認要求送信部
２０９　表示制御部
２１０　取得部
２１１　通信制御部
３０１　実行部
４０１　制御装置
４０２　主記憶装置
４０３　補助記憶装置
４０４　表示装置
４０５　入力装置
４０６　通信装置

４１０　バス

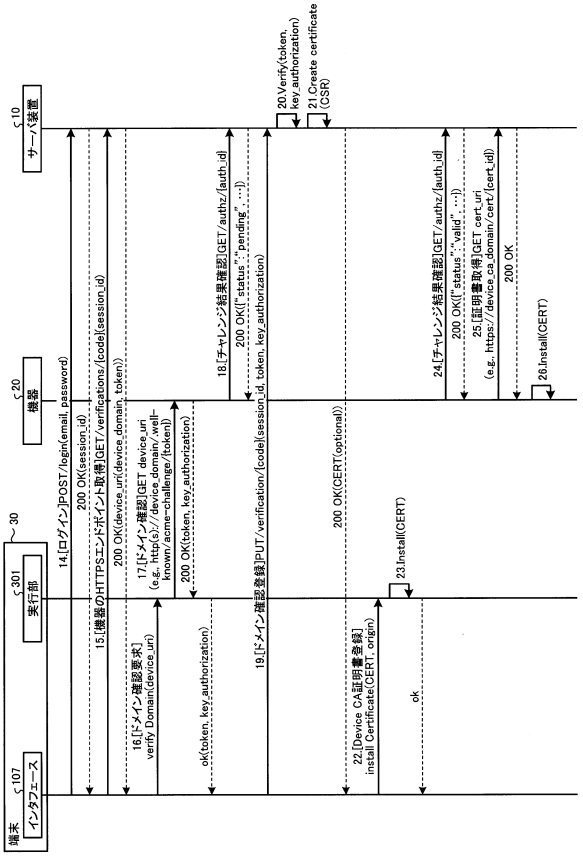
【図１】


100
10
サーバ装置
111 発行部
110 確認結果受付部
109 機器URL応答部
103 発行要求応答部
107 インタフェース
108 ドメイン確認部
105 確認要求応答部
102 機器認証部
106 インタフェース提供部
104 確認方式応答部
101 機器登録部
501
40 中継装置
502
20
203 ドメイン生成部
202 登録要求部
206 確認方式取得要求部
201 入力制御部
205 発行要求送信部
209 表示制御部
204 CSR生成部
208 確認要求送信部
207 サーバ処理部
210 取得部
301
30
107 インタフェース
108 ドメイン確認部
実行部
端末

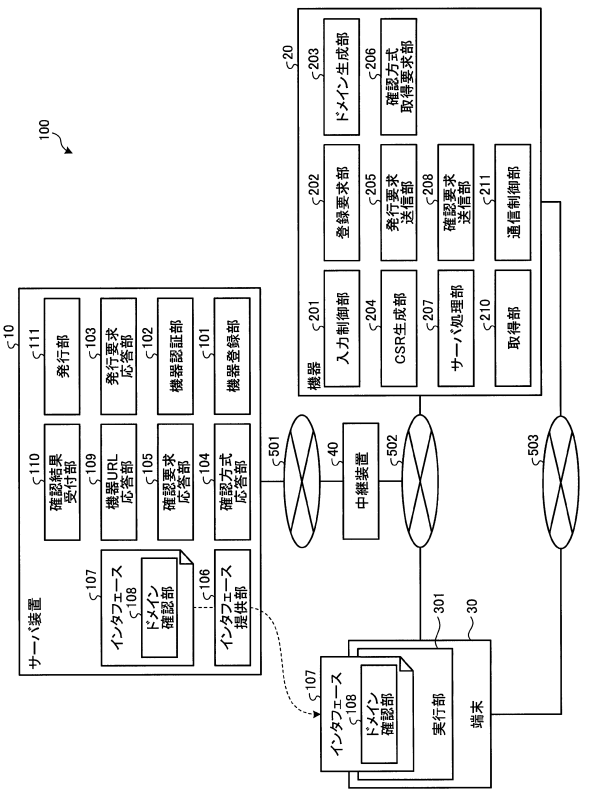
【図２Ａ】


10 サーバ装置
20 機器
機器メーカがサーバ装置から発行された product_id, product_secretを工場出荷時に書込み
30
301 実行部
107 インタフェース
端末
1.証明書発行のためのユーザ操作(email)
2.機器登録用キーペア作成 (client_pub, client_secret)
3.[nonce取得]HEAD/new-nonce
204 No Content(nonce)
4.Generate MAC1 (client_pub+nonce)with product_secret
5.[機器登録]POST/new-account (client_pub, email, nonce, product_id, MAC1)
201 Created(nonce)
6.domain_name生成・mDNS設定
7.CSR生成(domain_name, email)
8.[証明書発行要求]POST/new-order (client_pub, CSR, nonce)
201 Created ([authz_id, token], ...], cert_uri, nonce)
9.[チャレンジ取得]GET/authz/{authz_id}(client_pub)
200 OK([[challenge_id, token], ...])
10.token, key authorization (signature to client_pub with client_secret)を HTTP(S)サーバ上に設置_起動
11.[チャレンジ選択] POST/authz/{authz_id}/{challenge_id} (client_pub, token, key_authorization, nonce)
200 OK
(verification_uri(device_ca_uri, code), nonce)
12.verification_uri表示(QRコードなど)
13.(QRコードを読み込むなどして) ユーザがページ(verification_uri)を ロード

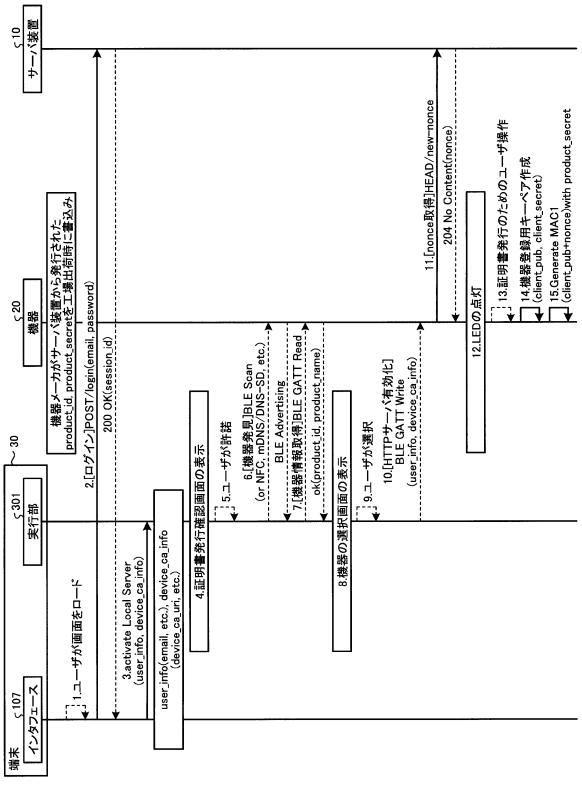
【図２Ｂ】



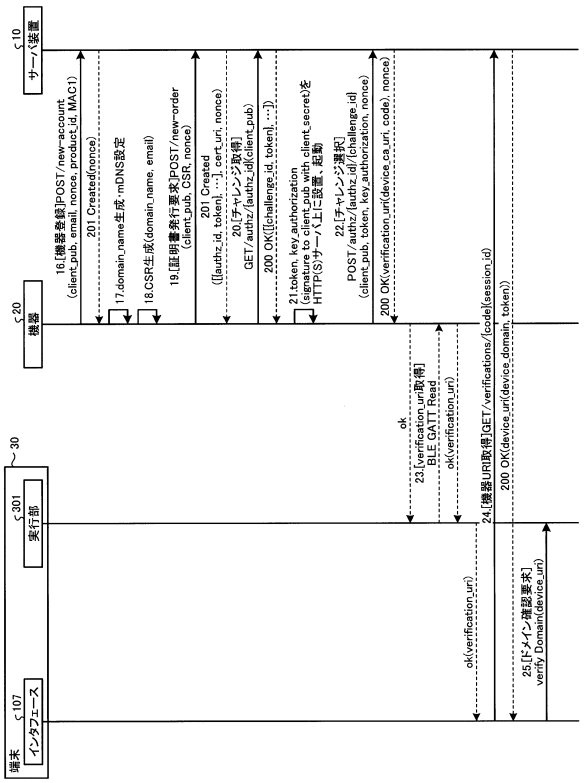
【図３】



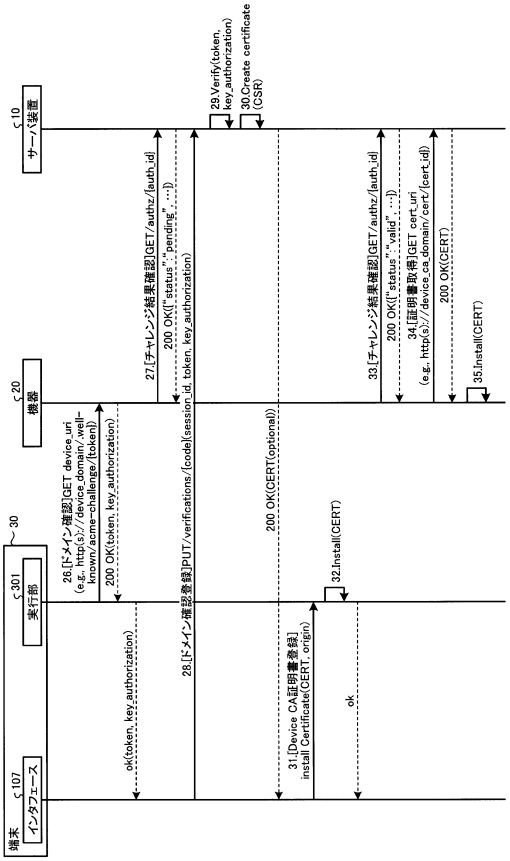
【図４Ａ】



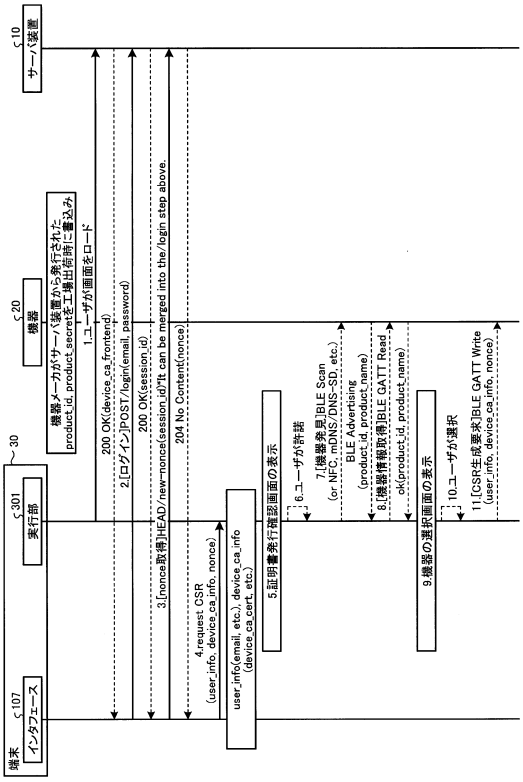
【図４Ｂ】



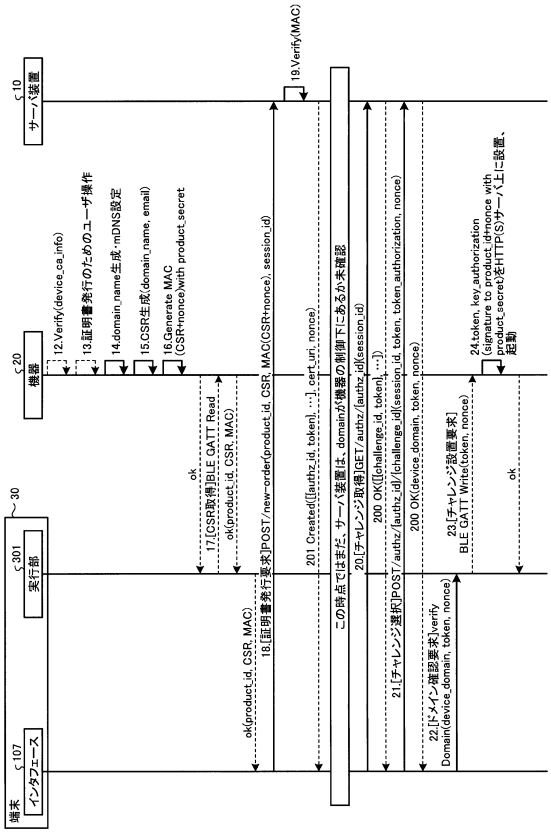
【図４Ｃ】



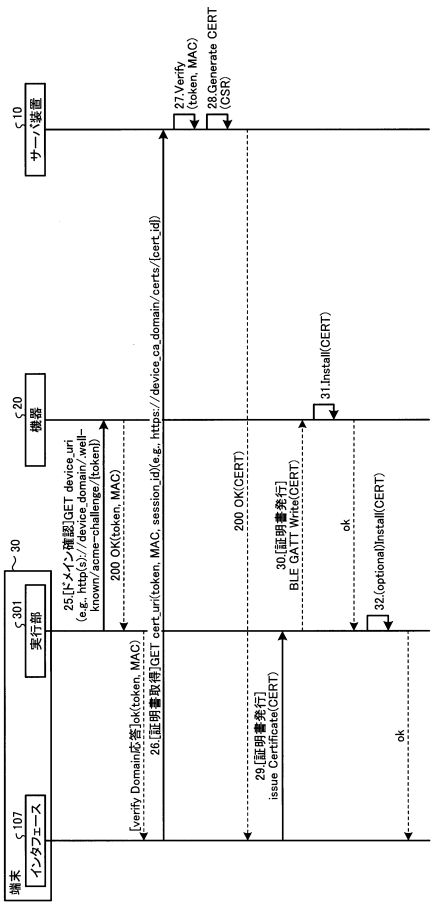
【図５Ａ】



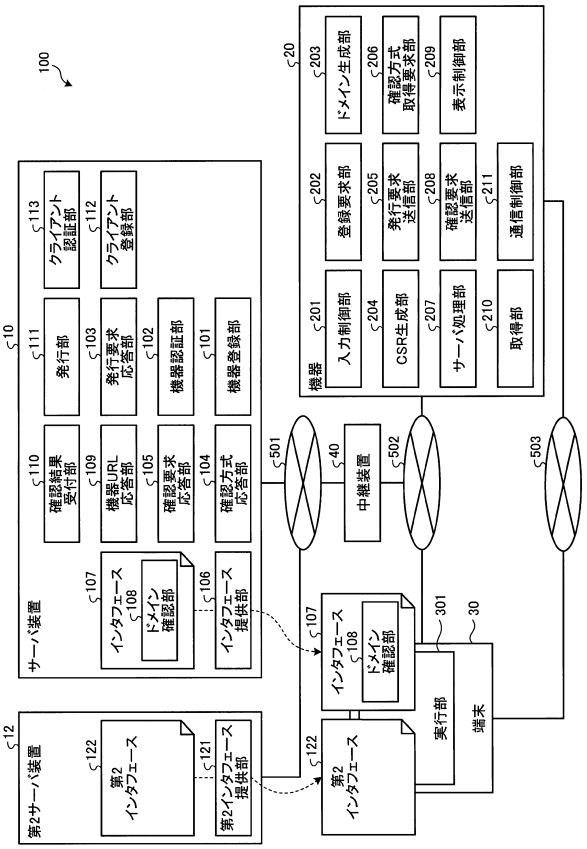
【図５Ｂ】



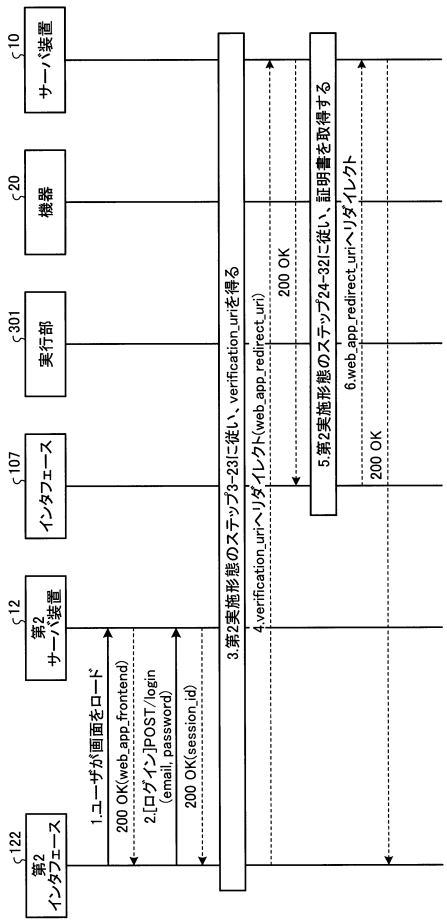
【図５Ｃ】



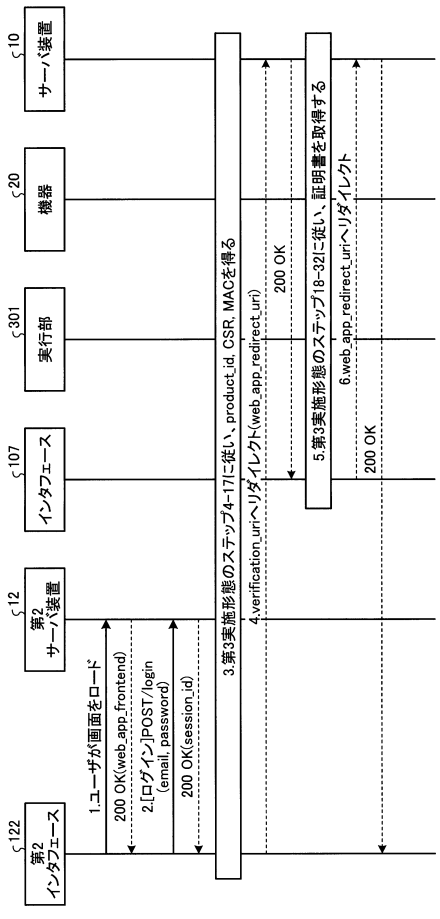
【図６】


100
10
サーバ装置
111 発行部
113 クライアント認証部
110 確認結果受付部
109 機器URL応答部
103 発行要求応答部
112 クライアント登録部
107 インタフェース
108 ドメイン確認部
105 確認要求応答部
102 機器認証部
106 インタフェース提供部
104 確認方式応答部
101 機器登録部
20
機器
201 入力制御部
202 登録要求部
203 ドメイン生成部
204 CSR生成部
205 発行要求送信部
206 確認方式取得要求部
207 サーバ処理部
208 確認要求送信部
209 表示制御部
210 取得部
211 通信制御部
501
40 中継装置
502
503
12
第2サーバ装置
122 第2インタフェース
121 第2インタフェース提供部
107 インタフェース
108 ドメイン確認部
301 実行部
30 端末

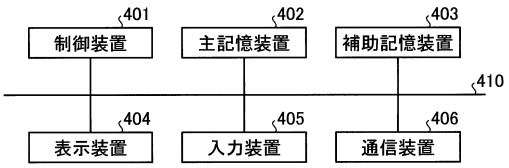
【図７Ａ】


10 サーバ装置
20 機器
301 実行部
107 インタフェース
12 第2サーバ装置
122 第2インタフェース
1.ユーザが画面をロード
200 OK(web_app_frontend)
2.[ログイン]POST/login (email, password)
200 OK(session_id)
3.第2実施形態のステップ3-23に従い、verification_uriを得る
4.verification_uriへリダイレクト(web_app_redirect_uri)
200 OK
5.第2実施形態のステップ24-32に従い、証明書を取得する
6.web_app_redirect_uriへリダイレクト
200 OK

【図７Ｂ】


10 サーバ装置
20 機器
301 実行部
107 インタフェース
12 第2サーバ装置
122 第2インタフェース
1.ユーザが画面をロード
200 OK(web_app_frontend)
2.[ログイン]POST/login (email, password)
200 OK(session_id)
3.第3実施形態のステップ4-17に従い、product_id, CSR, MACを得る
4.verification_uriへリダイレクト(web_app_redirect_uri)
200 OK
5.第3実施形態のステップ18-32に従い、証明書を取得する
6.web_app_redirect_uriへリダイレクト
200 OK

【図８】


401 制御装置
402 主記憶装置
403 補助記憶装置
410
404 表示装置
405 入力装置
406 通信装置

フロントページの続き

(58)調査した分野(Int.Cl., ＤＢ名)

Ｇ０６Ｆ	２１／００
	２１／３０－２１／４６
Ｇ０９Ｃ	１／００－５／００
Ｈ０４Ｋ	１／００－３／００
Ｈ０４Ｌ	９／００－９／３８