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

特許第6012888号
(P6012888)

(45)発行日　平成28年10月25日(2016.10.25)　(24)登録日　平成28年9月30日(2016.9.30)

(51)Int.Cl.		F I		
H04L 9/08	(2006.01)	H04L	9/00	601B
G06F 21/64	(2013.01)	H04L	9/00	601F
G06F 21/44	(2013.01)	G06F	21/64	350
H04L 12/70	(2013.01)	G06F	21/44	
		H04L	12/70	Z

請求項の数 8　(全 16 頁)

(21)出願番号　特願2015-558711 (P2015-558711)
(86)(22)出願日　平成26年1月27日(2014.1.27)
(86)国際出願番号　PCT/JP2014/051687
(87)国際公開番号　WO2015/111221
(87)国際公開日　平成27年7月30日(2015.7.30)
審査請求日　平成27年10月16日(2015.10.16)

(73)特許権者　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目７番３号
(74)代理人　100099461
弁理士　溝井　章司
(74)代理人　100122035
弁理士　渡辺　敏雄
(72)発明者　石黒　剛大
日本国東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内
(72)発明者　森　郁海
日本国東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内

審査官　青木　重徳

最終頁に続く

(54)【発明の名称】機器証明書提供装置、機器証明書提供システムおよび機器証明書提供プログラム

(57)【特許請求の範囲】

【請求項１】

第一の機器識別子と第一の通信アドレスとを記憶する機器識別子記憶部と、

前記機器識別子記憶部に記憶された前記第一の通信アドレスを宛先の通信アドレスとして含む機器識別子要求を一つ以上の通信機器が接続するネットワークに送信し、前記一つ以上の通信機器のうちの第一の通信機器から前記第一の通信機器を識別する通信機器識別子を受信する機器識別子問い合わせ部と、

前記機器識別子問い合わせ部によって受信された前記通信機器識別子が前記機器識別子記憶部に記憶された前記第一の機器識別子と同じ機器識別子であるか否かを判定する機器識別子判定部と、

前記機器識別子判定部によって前記通信機器識別子が前記第一の機器識別子と同じ機器識別子であると判定された場合、前記第一の通信機器の電子証明書である機器証明書を前記第一の通信機器に送信する機器証明書送信部と、

前記第一の機器識別子を取得する機器識別子取得部と、

前記機器識別子取得部によって取得された前記第一の機器識別子を前記第一の通信アドレスに対応付けて前記第一の機器識別子を記憶する機器情報サーバに送信し、前記機器情報サーバから前記第一の通信アドレスを受信する機器情報取得部とを備え、

前記機器識別子記憶部は、

前記機器識別子取得部によって取得された前記第一の機器識別子と、前記機器情報取得部によって取得された前記第一の通信アドレスとを記憶する

ことを特徴とする機器証明書提供装置。
【請求項２】
前記機器証明書提供装置は、
前記機器識別子判定部によって前記通信機器識別子が前記第一の機器識別子と同じ機器識別子であると判定された場合、前記第一の通信機器から公開鍵を取得する公開鍵取得部と、
前記公開鍵取得部によって取得された前記公開鍵を含む電子証明書を前記機器証明書として取得する機器証明書取得部と
を備えることを特徴とする請求項１に記載の機器証明書提供装置。
【請求項３】
前記機器証明書取得部は、電子証明書を生成する認証局サーバに前記公開鍵を送信し、前記認証局サーバから前記機器証明書を受信する
ことを特徴とする請求項２に記載の機器証明書提供装置。
【請求項４】
前記機器識別子記憶部は、第一の機器情報を記憶し、
前記機器証明書取得部は、前記公開鍵と前記第一の機器情報とを前記認証局サーバに送信し、前記認証局サーバから前記公開鍵と前記第一の機器情報とを含んだ電子証明書である前記機器証明書を受信する
ことを特徴とする請求項３に記載の機器証明書提供装置。
【請求項５】
前記機器情報サーバは、前記第一の通信アドレスと前記第一の機器情報とに対応付けて前記第一の機器識別子を記憶し、
前記機器情報取得部は、
前記機器識別子取得部によって取得された前記第一の機器識別子を前記機器情報サーバに送信し、前記機器情報サーバから前記第一の通信アドレスと前記第一の機器情報とを受信し、
前記機器識別子記憶部は、
前記機器識別子取得部によって取得された前記第一の機器識別子と、前記機器情報取得部によって取得された前記第一の通信アドレスと前記第一の機器情報とを記憶する
ことを特徴とする請求項４に記載の機器証明書提供装置。
【請求項６】
請求項１に記載の機器証明書提供装置と、
前記第一の機器識別子に対応付けて前記第一の通信アドレスを記憶し、前記機器証明書提供装置から前記第一の機器識別子を受信し、前記第一の通信アドレスを前記機器証明書提供装置に送信する機器情報サーバと
を備えることを特徴とする機器証明書提供システム。
【請求項７】
請求項２に記載の機器証明書提供装置と、
前記機器証明書提供装置から前記公開鍵を受信し、受信した前記公開鍵を含む前記機器証明書を生成し、生成した前記機器証明書を前記機器証明書提供装置に送信する認証局サーバと
を備えることを特徴とする機器証明書提供システム。
【請求項８】
第一の機器識別子に対応付けて記憶される第一の通信アドレスを宛先の通信アドレスとして含む機器識別子要求を一つ以上の通信機器が接続するネットワークに送信し、前記一つ以上の通信機器のうちの第一の通信機器から前記第一の通信機器を識別する通信機器識別子を受信する機器識別子問い合わせ処理と、
前記機器識別子問い合わせ処理によって受信された前記通信機器識別子が前記第一の機器識別子と同じ機器識別子であるか否かを判定する機器識別子判定処理と、
前記機器識別子判定処理によって前記通信機器識別子が前記第一の機器識別子と同じ機

器識別子であると判定された場合、前記第一の通信機器の電子証明書である機器証明書を前記第一の通信機器に送信する機器証明書送信処理と、
前記第一の機器識別子を取得する機器識別子取得処理と、
前記機器識別子取得処理によって取得された前記第一の機器識別子を前記第一の通信アドレスに対応付けて前記第一の機器識別子を記憶する機器情報サーバに送信し、前記機器情報サーバから前記第一の通信アドレスを受信する機器情報取得処理と
をコンピュータに実行させるための機器証明書提供プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、通信機器に電子証明書を導入する技術に関するものである。
【背景技術】
【０００２】
特許文献１は、サーバと認証局（ＣＡ）と機器と登録端末とが存在する認証システムに関する技術を開示している。
その技術において、機器がサーバに接続するために、機器情報に関連付けられていない仮公開鍵証明書と、機器情報に関連付けられている本公開鍵証明書とが、以下のように使用される。
まず、登録端末は認証局から仮公開鍵証明書を取得し、取得した仮公開鍵証明書をＩＣカード（ＩＣ：Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ）に書き込む。ＩＣカードには機器の秘密鍵および公開鍵が書き込まれている。
そして、利用者は機器にＩＣカードを接続し、機器は自身の機器情報とＩＣカードに書き込まれている仮公開鍵証明書とを用いて認証局に本公開鍵証明書の発行を要求し、認証局から本公開鍵証明書を取得する。
【０００３】
特許文献２は、認証装置と上位装置と下位装置とが相互にセキュアな通信を行うための技術を開示している。
その技術において、各装置がそれぞれ個別公開鍵証明書を用いて相互に認証することによってセキュアな通信が確保される。そして、下位装置の個別公開鍵証明書が破損してしまった場合、上位装置は下位装置の情報と各装置に共通な共通公開鍵証明書とに基づいて下位装置を認証し、下位装置は上位装置を経由して認証装置から個別公開鍵証明書を取得する。
つまり、特許文献２の技術によって個別公開鍵証明書を復旧するためには、共通公開鍵証明書が各装置に予め導入されている必要がある。
しかし、各装置に共通公開鍵証明書を予め導入することが困難な場合が考えられる。例えば、機器製造者とサービス提供者とが異なる場合、機器の製造時にサービス提供者が発行する共通公開鍵証明書を機器に導入することは難しい。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】国際公開第２００７／０９９６０８号
【特許文献２】特開２００５－６５２３６号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
本発明は、通信機器に安全に電子証明書を導入できるようにすることを目的とする。
【課題を解決するための手段】
【０００６】
本発明の機器証明書提供装置は、
第一の機器識別子と第一の通信アドレスとを記憶する機器識別子記憶部と、

前記機器識別子記憶部に記憶された前記第一の通信アドレスを宛先の通信アドレスとして含む機器識別子要求を一つ以上の通信機器が接続するネットワークに送信し、前記一つ以上の通信機器のうちの第一の通信機器から前記第一の通信機器を識別する通信機器識別子を受信する機器識別子問い合わせ部と、

前記機器識別子問い合わせ部によって受信された前記通信機器識別子が前記機器識別子記憶部に記憶された前記第一の機器識別子と同じ機器識別子であるか否かを判定する機器識別子判定部と、

前記機器識別子判定部によって前記通信機器識別子が前記第一の機器識別子と同じ機器識別子であると判定された場合、前記第一の通信機器の電子証明書である機器証明書を前記第一の通信機器に送信する機器証明書送信部とを備える。

【発明の効果】

【０００７】

本発明によれば、通信機器に安全に電子証明書を導入することができる。

【図面の簡単な説明】

【０００８】

【図１】実施の形態１における機器認証システム１００の構成図である。

【図２】実施の形態１におけるセキュリティＧＷ２００の機能構成図である。

【図３】実施の形態１における機器情報サーバ３００の機能構成図である。

【図４】実施の形態１における利用者情報ファイル３９１を示す図である。

【図５】実施の形態１における機器情報ファイル３９２を示す図である。

【図６】実施の形態１における通信機器４００の機能構成図である。

【図７】実施の形態１における機器認証システム１００の機器証明書導入処理を示すフローチャートである。

【図８】実施の形態１における機器情報取得処理（Ｓ１１０）を示すフローチャートである。

【図９】実施の形態１におけるセキュリティＧＷ２００のハードウェア構成の一例を示す図である。

【発明を実施するための形態】

【０００９】

実施の形態１.

通信機器に電子証明書を導入する形態について説明する。

【００１０】

図１は、実施の形態１における機器認証システム１００の構成図である。

実施の形態１における機器認証システム１００の構成について、図１に基づいて説明する。

【００１１】

機器認証システム１００（機器証明書提供システムの一例）は、通信機器４００が電子証明書を用いて通信を行うために、通信機器４００に電子証明書を導入するシステムである。電子証明書は公開鍵証明書ともいう。公開鍵証明書は公開鍵の所有者（例えば、通信機器４００）を証明する。

機器認証システム１００は、セキュリティＧＷ２００（ＧＷ：ゲートウェイ）と、機器情報サーバ３００と、通信機器４００と、認証局サーバ１１０とを備える。これらはネットワーク１０９を介して通信を行う。

【００１２】

セキュリティＧＷ２００（機器証明書提供装置の一例）は、通信機器４００に電子証明書を提供する装置である。

機器情報サーバ３００は、通信機器４００に関する機器情報を管理する装置である。

通信機器４００は、セキュリティＧＷ２００から提供される電子証明書を用いて通信を行う機器である。

【００１３】

認証局サーバ１１０は、電子証明書を発行する装置である。
認証局サーバ１１０は、電子証明書を発行する証明書発行部１１１を備える。
また、認証局サーバ１１０は、認証局サーバ１１０の秘密鍵（以下、認証局秘密鍵という）などを記憶する認証局記憶部を備える（図示省略）。

【００１４】
以下、通信機器４００の電子証明書を機器証明書といい、通信機器４００の公開鍵を機器公開鍵といい、通信機器４００の秘密鍵を機器秘密鍵という。
また、セキュリティＧＷ２００の電子証明書をＧＷ証明書といい、セキュリティＧＷ２００の公開鍵をＧＷ公開鍵といい、セキュリティＧＷ２００の秘密鍵をＧＷ秘密鍵という。
また、機器情報サーバ３００の電子証明書をサーバ証明書といい、機器情報サーバ３００の公開鍵をサーバ公開鍵といい、機器情報サーバ３００の秘密鍵をサーバ秘密鍵という。

【００１５】
図２は、実施の形態１におけるセキュリティＧＷ２００の機能構成図である。
実施の形態１におけるセキュリティＧＷ２００の機能構成について、図２に基づいて説明する。

【００１６】
セキュリティＧＷ２００（機器証明書提供装置の一例）は、相互認証部２１０と、暗号通信部２２０と、機器ＩＤ登録部２３０（ＩＤ：識別子）と、機器証明書導入部２４０と、セキュリティＧＷ記憶部２９０とを備える。

【００１７】
相互認証部２１０は、通信相手の電子証明書を用いて通信相手を認証し、自身の電子証明書（ＧＷ証明書）を用いて通信相手から認証される。

【００１８】
暗号通信部２２０は、通信相手の電子証明書に含まれる公開鍵を用いて通信データを暗号化し、暗号化した通信データを通信相手に送信する。
暗号通信部２２０は、暗号化された通信データを通信相手から受信し、受信した通信データを自身の秘密鍵（ＧＷ秘密鍵）を用いて復号する。

【００１９】
機器ＩＤ登録部２３０（機器識別子取得部、機器情報取得部の一例）は、通信機器４００を識別する機器ＩＤ２９１（例えば、製造番号）を機器情報サーバ３００に送信し、通信機器４００に関する機器情報２９２を受信する。
機器情報２９２は、ＩＰアドレス２９３（ＩＰ：Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）およびＭＡＣアドレス２９４（ＭＡＣ：Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）などを含む。

【００２０】
機器証明書導入部２４０は、機器証明書４９４を通信機器４００に導入する。
機器証明書導入部２４０は、機器ＩＤ問い合わせ部２４１と、機器ＩＤ判定部２４２と、公開鍵取得部２４３と、機器証明書取得部２４４と、機器証明書送信部２４５とを備える。
機器ＩＤ問い合わせ部２４１は、ネットワーク１０９に接続する通信機器４００または不正な通信機器から機器ＩＤを受信する。
機器ＩＤ判定部２４２は、受信された機器ＩＤがセキュリティＧＷ記憶部２９０に記憶されている機器ＩＤ２９１と同じであるか否かを判定する。
公開鍵取得部２４３は、機器ＩＤ２９１と同じ機器ＩＤを送信した通信機器４００から機器公開鍵４９２を受信する。
機器証明書取得部２４４は、機器公開鍵４９２を含んだ機器証明書４９４を認証局サーバ１１０から取得する。
機器証明書送信部２４５は、機器証明書４９４を通信機器４００に送信する。

【００２１】
セキュリティＧＷ記憶部２９０は、セキュリティＧＷ２００が使用、生成または入出力するデータを記憶する。
例えば、セキュリティＧＷ記憶部２９０は、機器ＩＤ２９１（第一の機器識別子の一例）に対応付けて、機器情報２９２（第一の通信アドレス、第一の機器情報の一例）と、機器公開鍵４９２と、機器証明書４９４とを記憶する。また、セキュリティＧＷ記憶部２９０は、ＧＷ公開鍵を含むＧＷ証明書、ＧＷ秘密鍵、サーバ公開鍵を含むサーバ証明書などを記憶する（図示省略）。
【００２２】
図３は、実施の形態１における機器情報サーバ３００の機能構成図である。
実施の形態１における機器情報サーバ３００の機能構成について、図３に基づいて説明する。
【００２３】
機器情報サーバ３００は、相互認証部３１０と、暗号通信部３２０と、利用者認証部３３０と、機器情報管理部３４０と、サーバ記憶部３９０とを備える。
【００２４】
相互認証部３１０は、通信相手の電子証明書を用いて通信相手を認証し、自身の電子証明書（サーバ証明書）を用いて通信相手から認証される。
【００２５】
暗号通信部３２０は、通信相手の電子証明書に含まれる公開鍵を用いて通信データを暗号化し、暗号化した通信データを通信相手に送信する。
暗号通信部３２０は、暗号化された通信データを通信相手から受信し、受信した通信データを自身の秘密鍵（サーバ秘密鍵）を用いて復号する。
【００２６】
利用者認証部３３０は、セキュリティＧＷ２００を利用する利用者を利用者情報ファイル３９１に基づいて認証する。
【００２７】
機器情報管理部３４０は、機器情報ファイル３９２に含まれる機器情報をセキュリティＧＷ２００に送信する。
【００２８】
サーバ記憶部３９０は、機器情報サーバ３００が使用、生成または入出力するデータを記憶する。
例えば、サーバ記憶部３９０は、利用者情報ファイル３９１と、機器情報ファイル３９２とを記憶する。また、サーバ記憶部３９０は、サーバ公開鍵を含むサーバ証明書、サーバ秘密鍵、ＧＷ公開鍵を含むＧＷ証明書などを記憶する（図示省略）。
利用者情報ファイル３９１は、セキュリティＧＷ２００を利用することを許可される利用者に関する利用者情報を含む。
機器情報ファイル３９２は、機器証明書が導入される通信機器４００に関する機器情報を含む。
【００２９】
図４は、実施の形態１における利用者情報ファイル３９１を示す図である。
実施の形態１における利用者情報ファイル３９１について、図４に基づいて説明する。
利用者情報ファイル３９１は利用者毎の利用者データを備える。
利用者データは、利用者データを識別するデータ番号と、利用者に関する利用者情報（利用者ＩＤ、パスワードなど）とを含む。
【００３０】
図５は、実施の形態１における機器情報ファイル３９２を示す図である。
実施の形態１における機器情報ファイル３９２について、図５に基づいて説明する。
機器情報ファイル３９２は、通信機器毎の機器データを備える。
機器データは、機器データを識別するデータ番号と、通信機器を識別する機器ＩＤと、

通信機器に関する機器情報（ＩＰアドレス、ＭＡＣアドレスなど）とを含む。
【００３１】
図６は、実施の形態１における通信機器４００の機能構成図である。
実施の形態１における通信機器４００の機能構成について、図６に基づいて説明する。
【００３２】
通信機器４００は、相互認証部４１０と、暗号通信部４２０と、暗号鍵生成部４３０と、機器証明書導入部４４０と、機器記憶部４９０とを備える。
【００３３】
相互認証部４１０は、通信相手の電子証明書を用いて通信相手を認証し、自身の電子証明書（機器証明書４９４）を用いて通信相手から認証される。
【００３４】
暗号通信部４２０は、通信相手の電子証明書に含まれる公開鍵を用いて通信データを暗号化し、暗号化した通信データを通信相手に送信する。
暗号通信部４２０は、暗号化された通信データを通信相手から受信し、受信した通信データを自身の秘密鍵（機器秘密鍵４９３）を用いて復号する。
【００３５】
暗号鍵生成部４３０は、公開鍵方式の鍵生成アルゴリズムに基づいて、機器公開鍵４９２と機器秘密鍵４９３とを生成する。
【００３６】
機器証明書導入部４４０は、セキュリティＧＷ２００から送信される機器証明書４９４を受信し、受信した機器証明書４９４を機器記憶部４９０に記憶する。
【００３７】
機器記憶部４９０は、通信機器４００が使用、生成または入出力するデータを記憶する。
例えば、機器記憶部４９０は、機器ＩＤ４９１と、機器公開鍵４９２と、機器秘密鍵４９３と、機器証明書４９４とを記憶する。また、機器記憶部４９０は、通信相手の公開鍵を含む通信相手の電子証明書を記憶する（図示省略）。
【００３８】
図７は、実施の形態１における機器認証システム１００の機器証明書導入処理を示すフローチャートである。
実施の形態１における機器認証システム１００の機器証明書導入処理について、図７に基づいて説明する。
【００３９】
まず、機器証明書導入処理の概要について説明する。
機器ＩＤ登録部２３０は、機器ＩＤ２９１に対応する機器情報２９２を機器情報サーバ３００から取得する（Ｓ１１０）。
機器ＩＤ問い合わせ部２４１は、機器情報２９２に含まれる情報を用いて通信機器４００から機器ＩＤ４９１を取得する（Ｓ１２０）。
機器ＩＤ２９１と同じ機器ＩＤ４９１が取得された場合、公開鍵取得部２４３は、通信機器４００から機器公開鍵４９２を取得する（Ｓ１４０）。
機器証明書取得部２４４は、機器公開鍵４９２を含む機器証明書４９４を認証局サーバ１１０から取得する（Ｓ１５０）。
機器証明書送信部２４５は、機器証明書４９４を通信機器４００に送信する（Ｓ１６０）。
以上の機器証明書導入処理によって、機器証明書４９４が通信機器４００に導入される。
【００４０】
次に、機器証明書導入処理の詳細について説明する。
Ｓ１１０において、セキュリティＧＷ２００の機器ＩＤ登録部２３０は、機器ＩＤ２９１に対応する機器情報２９２を機器情報サーバ３００から取得する。

機器情報取得処理（Ｓ１１０）の詳細については後述する。
Ｓ１１０の後、処理はＳ１２０に進む。
【００４１】
Ｓ１２０において、セキュリティＧＷ２００の機器ＩＤ問い合わせ部２４１は、機器情報２９２に含まれるＩＰアドレス２９３を宛先の通信アドレスとして用いて機器ＩＤ要求を生成し、生成した機器ＩＤ要求をネットワーク１０９に送信する。但し、機器ＩＤ問い合わせ部２４１は、ＭＡＣアドレス２９４を宛先の通信アドレスとして用いて機器ＩＤ要求を送信しても構わない。
機器ＩＤ要求は、機器ＩＤ２９１によって識別される通信機器４００に対して、通信機器４００に記憶されている機器ＩＤ４９１を要求する通信データである。
【００４２】
通信機器４００の機器証明書導入部４４０は機器ＩＤ要求を受信し、機器ＩＤ応答を生成し、生成した機器ＩＤ応答をセキュリティＧＷ２００に送信する。
機器ＩＤ応答は、機器記憶部４９０に記憶されている機器ＩＤ４９１を含んだ通信データである。
【００４３】
セキュリティＧＷ２００の機器ＩＤ問い合わせ部２４１は、機器ＩＤ４９１を含んだ機器ＩＤ応答を受信する。
このとき、機器ＩＤ問い合わせ部２４１は、不正な通信機器から送信される機器ＩＤ応答を受信する可能性がある。
また、通信機器４００がネットワーク１０９に接続されていない場合（通信機器４００がオフの場合を含む）、機器ＩＤ問い合わせ部２４１は、通信機器４００から機器ＩＤ応答を受信できない。
Ｓ１２０の後、処理はＳ１３０に進む。
【００４４】
Ｓ１３０において、セキュリティＧＷ２００の機器ＩＤ判定部２４２は、機器ＩＤ応答に含まれる機器ＩＤ４９１と、セキュリティＧＷ記憶部２９０に記憶されている機器ＩＤ２９１とを比較する。
機器ＩＤ４９１と機器ＩＤ２９１とが同じでない場合、機器ＩＤ判定部２４２は機器ＩＤ４９１を破棄し、機器ＩＤ２９１と同じ機器ＩＤ４９１を含む機器ＩＤ応答が受信されるまで待機する。
機器ＩＤ応答の待ち時間が経過するまでに、機器ＩＤ２９１と同じ機器ＩＤ４９１を含む機器ＩＤ応答が受信された場合（ＹＥＳ）、処理はＳ１４０に進む。
機器ＩＤ応答の待ち時間が経過するまでに、機器ＩＤ２９１と同じ機器ＩＤ４９１を含む機器ＩＤ応答が受信されなかった場合（ＮＯ）、機器ＩＤ判定部２４２は、通信機器４００がネットワーク１０９に接続されていない旨のメッセージを表示する。この場合、機器証明書４９４が通信機器４００に導入されずに、機器証明書導入処理は終了する。
【００４５】
Ｓ１４０において、セキュリティＧＷ２００の公開鍵取得部２４３は、通信機器４００に公開鍵要求を送信する。この通信機器４００は、機器ＩＤ２９１と同じ機器ＩＤ４９１を含む機器ＩＤ応答を送信した機器である。
公開鍵要求は、通信機器４００に対して機器公開鍵４９２を要求する通信データである。
【００４６】
通信機器４００の機器証明書導入部４４０は公開鍵要求を受信し、機器公開鍵４９２を含んだ通信データである公開鍵応答を生成し、生成した公開鍵応答をセキュリティＧＷ２００に送信する。
暗号鍵生成部４３０は、このタイミングで機器公開鍵４９２および機器秘密鍵４９３を生成してもよいし、機器公開鍵４９２および機器秘密鍵４９３を予め生成してもよい。
【００４７】

セキュリティＧＷ２００の公開鍵取得部２４３は、機器公開鍵４９２を含んだ公開鍵応答を受信する。
Ｓ１４０の後、処理はＳ１５０に進む。
【００４８】
Ｓ１５０において、セキュリティＧＷ２００の機器証明書取得部２４４は、機器公開鍵４９２と機器情報２９２（機器ＩＤ２９１を含んでもよい）とを含む証明書要求を生成し、生成した証明書要求を認証局サーバ１１０に送信する。
証明書要求は、機器証明書４９４を要求する通信データである。
【００４９】
認証局サーバ１１０の証明書発行部１１１は証明書要求を受信し、証明書要求から機器公開鍵４９２と機器情報２９２を取得し、機器公開鍵４９２と機器情報２９２と認証局秘密鍵とを用いて認証局サーバ１１０の電子署名（以下、認証局署名という）を生成する。
そして、証明書発行部１１１は、機器公開鍵４９２と機器情報２９２と認証局署名とを含む機器証明書４９４を生成し、生成した機器証明書４９４を含んだ通信データである証明書応答を生成し、生成した証明書応答をセキュリティＧＷ２００に送信する。
【００５０】
セキュリティＧＷ２００の機器証明書取得部２４４は、機器証明書４９４を含んだ証明書応答を受信する。
Ｓ１５０の後、処理はＳ１６０に進む。
【００５１】
Ｓ１６０において、セキュリティＧＷ２００の機器証明書送信部２４５は、機器証明書４９４を通信機器４００に送信する。
通信機器４００の機器証明書導入部４４０は機器証明書４９４を受信し、受信した機器証明書４９４を機器記憶部４９０に記憶する。
【００５２】
これにより、機器証明書４９４が通信機器４００に導入される。
機器証明書４９４が導入された後、通信機器４００は、機器証明書４９４および機器秘密鍵４９３を用いて通信相手から認証を受けることができる。また、通信機器４００は、機器証明書４９４および機器秘密鍵４９３を用いて暗号化通信（秘匿通信）を行うことができる。
一方、不正な通信機器は、機器証明書が導入されないため、通信相手（例えば、通信機器４００、セキュリティＧＷ２００または機器情報サーバ３００）から認証を受けることができず、通信相手と通信を行うことができない。
Ｓ１６０の後、機器証明書導入処理は終了する。
【００５３】
図８は、実施の形態１における機器情報取得処理（Ｓ１１０）を示すフローチャートである。
実施の形態１における機器情報取得処理（Ｓ１１０）について、図８に基づいて説明する。
【００５４】
Ｓ１１１において、セキュリティＧＷ２００の相互認証部２１０はＧＷ証明書を機器情報サーバ３００に送信し、機器情報サーバ３００からサーバ証明書を受信する。
相互認証部２１０は、受信したサーバ証明書に含まれるサーバ情報（機器情報サーバ３００に関する情報）に基づいて、通信相手が機器情報サーバ３００であることを確認する。
相互認証部２１０はＧＷ秘密鍵を用いて認証コードを暗号化し、暗号化した認証コードを機器情報サーバ３００に送信する。
相互認証部２１０は、サーバ秘密鍵を用いて暗号化された認証コードを機器情報サーバ３００から受信し、受信した認証コードをサーバ証明書に含まれるサーバ公開鍵を用いて復号する。

認証コードを復号することができた場合、相互認証部２１０は機器情報サーバ３００を認証する。

【００５５】

同様に、機器情報サーバ３００の相互認証部３１０はサーバ証明書をセキュリティＧＷ２００に送信し、セキュリティＧＷ２００からＧＷ証明書を受信する。

相互認証部３１０は、受信したＧＷ証明書に含まれるＧＷ情報（セキュリティＧＷ２００に関する情報）に基づいて、通信相手がセキュリティＧＷ２００であることを確認する。

相互認証部３１０はサーバ秘密鍵を用いて認証コードを暗号化し、暗号化した認証コードをセキュリティＧＷ２００に送信する。

相互認証部３１０は、ＧＷ秘密鍵を用いて暗号化された認証コードをセキュリティＧＷ２００から受信し、受信した認証コードをＧＷ証明書に含まれるＧＷ公開鍵を用いて復号する。

認証コードを復号することができた場合、相互認証部３１０はセキュリティＧＷ２００を認証する。

Ｓ１１１の後、処理はＳ１１２に進む。

【００５６】

Ｓ１１２において、利用者は、利用者ＩＤとパスワードとをセキュリティＧＷ２００に入力する。

セキュリティＧＷ２００の機器ＩＤ登録部２３０は、入力された利用者ＩＤとパスワードとを取得する。

Ｓ１１２の後、処理はＳ１１３に進む。

【００５７】

Ｓ１１３において、セキュリティＧＷ２００の機器ＩＤ登録部２３０は、利用者ＩＤとパスワードとを含む通信データである認証要求を機器情報サーバ３００に送信する。

Ｓ１１３の後、処理はＳ１１４に進む。

【００５８】

Ｓ１１４において、機器情報サーバ３００の利用者認証部３３０は認証要求を受信し、認証要求に含まれる利用者ＩＤと認証要求に含まれるパスワードとを含んだ利用者データが利用者情報ファイル３９１に含まれるか否かを判定する。

認証要求に含まれる利用者ＩＤと認証要求に含まれるパスワードとを含んだ利用者データが利用者情報ファイル３９１に含まれる場合、セキュリティＧＷ２００を利用している利用者は正当な利用者である。

セキュリティＧＷ２００を利用している利用者が正当な利用者である場合（ＹＥＳ）、利用者認証部３３０は認証されたことを示す通信データである認証応答をセキュリティＧＷ２００に送信し、セキュリティＧＷ２００の機器ＩＤ登録部２３０は認証応答を受信する。そして、処理はＳ１１５に進む。

【００５９】

セキュリティＧＷ２００を利用している利用者が正当な利用者でない場合（ＮＯ）、利用者認証部３３０は、認証されなかったことを示す通信データである認証応答をセキュリティＧＷ２００に送信する。

セキュリティＧＷ２００の機器ＩＤ登録部２３０は認証応答を受信し、認証されなかったことを示すエラーメッセージを表示する。

そして、セキュリティＧＷ２００が機器情報２９２を取得できずに機器情報取得処理（Ｓ１１０）は終了し、機器証明書４９４が通信機器４００に導入されずに機器証明書導入処理（図７参照）は終了する。

【００６０】

Ｓ１１５において、セキュリティＧＷ２００の機器ＩＤ登録部２３０は、認証されたことを示す認証メッセージを表示する。

利用者は、機器証明書４９４を導入したい通信機器４００の機器ＩＤ２９１をセキュリ

ティＧＷ２００に入力する。
セキュリティＧＷ２００の機器ＩＤ登録部２３０は入力された機器ＩＤ２９１を取得し、取得した機器ＩＤ２９１をセキュリティＧＷ記憶部２９０に記憶する。
Ｓ１１５の後、処理はＳ１１６に進む。
【００６１】
Ｓ１１６において、セキュリティＧＷ２００の機器ＩＤ登録部２３０は機器ＩＤ２９１を含んだ機器情報要求を生成し、生成した機器情報要求を機器情報サーバ３００に送信する。
機器情報要求は、機器情報２９２を要求する通信データである。
Ｓ１１６の後、処理はＳ１１７に進む。
【００６２】
Ｓ１１７において、機器情報サーバ３００の機器情報管理部３４０は機器情報要求を受信し、受信した機器情報要求に含まれる機器ＩＤ２９１と同じ機器ＩＤを含んだ機器情報データを機器情報ファイル３９２から選択する。
機器情報管理部３４０は選択した機器情報データから機器情報２９２を取得し、取得した機器情報２９２を含んだ通信データである機器情報応答を生成し、生成した機器情報応答をセキュリティＧＷ２００に送信する。
機器情報管理部３４０は、機器情報要求に含まれるセキュリティＧＷ２００に関する情報（例えば、ＩＰアドレス）を、選択した機器情報データに設定してもよい。
【００６３】
セキュリティＧＷ２００の機器ＩＤ登録部２３０は機器情報応答を受信し、受信した機器情報応答から機器情報２９２を取得し、取得した機器情報２９２をセキュリティＧＷ記憶部２９０に記憶する。
Ｓ１１７の後、機器情報取得処理（Ｓ１１０）は終了する。
【００６４】
図８のＳ１１３からＳ１１７で通信される通信データは、セキュリティＧＷ２００の暗号通信部２２０および機器情報サーバ３００の暗号通信部３２０によって、送信時に暗号化され、受信時に復号される。
【００６５】
図９は、実施の形態１におけるセキュリティＧＷ２００のハードウェア構成の一例を示す図である。
実施の形態１におけるセキュリティＧＷ２００のハードウェア構成の一例について、図９に基づいて説明する。但し、セキュリティＧＷ２００のハードウェア構成は図９に示す構成と異なる構成であってもよい。
なお、機器情報サーバ３００、通信機器４００および認証局サーバ１１０のそれぞれのハードウェア構成はセキュリティＧＷ２００と同様である。
【００６６】
セキュリティＧＷ２００は、演算装置９０１、補助記憶装置９０２、主記憶装置９０３、通信装置９０４および入出力装置９０５を備えるコンピュータである。
演算装置９０１、補助記憶装置９０２、主記憶装置９０３、通信装置９０４および入出力装置９０５はバス９０９に接続している。
【００６７】
演算装置９０１は、プログラムを実行するＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）である。
補助記憶装置９０２は、例えば、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）、フラッシュメモリまたはハードディスク装置である。
主記憶装置９０３は、例えば、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）である。
通信装置９０４は、有線または無線でインターネット、ＬＡＮ（ローカルエリアネットワーク）、電話回線網またはその他のネットワークを介して通信を行う。

入出力装置９０５は、例えば、マウス、キーボード、ディスプレイ装置である。

【００６８】

プログラムは、通常は補助記憶装置９０２に記憶されており、主記憶装置９０３にロードされ、演算装置９０１に読み込まれ、演算装置９０１によって実行される。

例えば、オペレーティングシステム（ＯＳ）が補助記憶装置９０２に記憶される。また、「～部」として説明している機能を実現するプログラムが補助記憶装置９０２に記憶される。そして、ＯＳおよび「～部」として説明している機能を実現するプログラムは主記憶装置９０３にロードされ、演算装置９０１によって実行される。「～部」は「～処理」「～工程」と読み替えることができる。

【００６９】

「～の判断」、「～の判定」、「～の抽出」、「～の検知」、「～の設定」、「～の登録」、「～の選択」、「～の生成」、「～の入力」、「～の出力」等の処理の結果を示す情報、データ、ファイル、信号値または変数値が主記憶装置９０３または補助記憶装置９０２に記憶される。また、セキュリティＧＷ２００が使用するその他のデータが主記憶装置９０３または補助記憶装置９０２に記憶される。

【００７０】

実施の形態１において、通信機器４００に機器証明書４９４を導入する形態について説明した。

【００７１】

実施の形態１により、例えば、以下のような効果を奏する。

通信機器４００にセキュア且つ簡易に機器証明書４９４を導入することができる。

ＩＣカードなどの外部記憶媒体を用いずに、通信機器４００に機器証明書４９４を導入することができる。つまり、外部記憶媒体を使用するための読み書き装置を備えない通信機器４００に機器証明書４９４を導入することができる。そして、ＩＣカードが盗難されることによって不正な通信機器に機器証明書４９４が導入されるのを防ぐことができる。

機器証明書４９４が不正な通信機器に導入されることを防ぎ、機器証明書４９４が導入されない不正な通信機器との通信を防ぐことができる。

【００７２】

実施の形態１は、機器認証システム１００の形態の一例である。

つまり、機器認証システム１００は、実施の形態１で説明した構成要素の一部を備えなくても構わない。また、機器認証システム１００は、実施の形態１で説明していない構成要素を備えても構わない。

例えば、セキュリティＧＷ２００は、認証局サーバ１１０の機能（証明書発行部１１１）を備え、認証局サーバ１１０に機器証明書４９４を要求せずに機器証明書４９４を生成しても構わない。この場合、機器認証システム１００が認証局サーバ１１０を備える必要はない。

【００７３】

実施の形態１においてフローチャート等を用いて説明した処理手順は、実施の形態１に係る方法およびプログラムの処理手順の一例である。実施の形態１に係る方法およびプログラムは、実施の形態１で説明した処理手順と一部異なる処理手順で実現されても構わない。

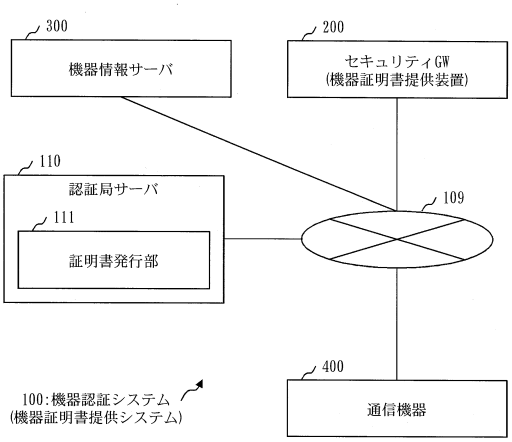
【符号の説明】

【００７４】

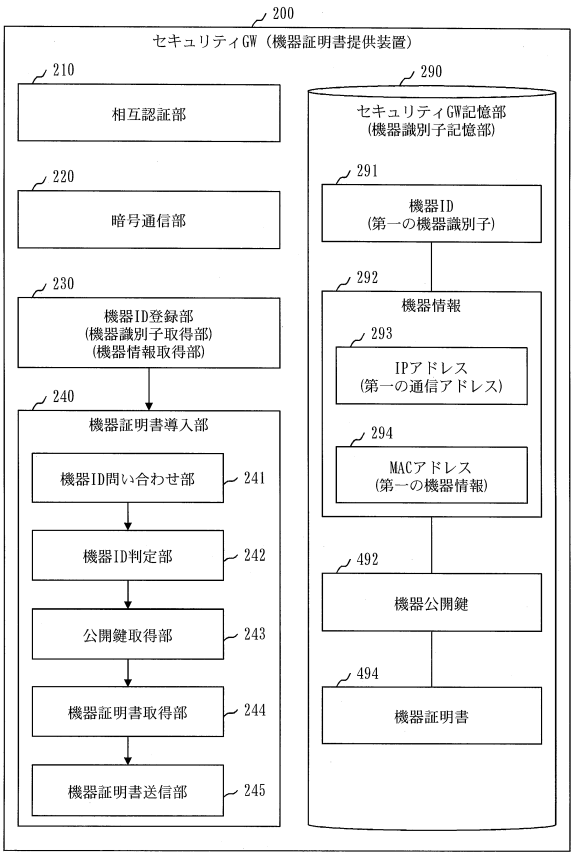
１００　機器認証システム、１０９　ネットワーク、１１０　認証局サーバ、１１１　証明書発行部、２００　セキュリティＧＷ、２１０　相互認証部、２２０　暗号通信部、２３０　機器ＩＤ登録部、２４０　機器証明書導入部、２４１　機器ＩＤ問い合わせ部、２４２　機器ＩＤ判定部、２４３　公開鍵取得部、２４４　機器証明書取得部、２４５　機器証明書送信部、２９０　セキュリティＧＷ記憶部、２９１　機器ＩＤ、２９２　機器情報、２９３　ＩＰアドレス、２９４　ＭＡＣアドレス、３００　機器情報サーバ、３１０　相互認証部、３２０　暗号通信部、３３０　利用者認証部、３４０　機器情報管理部

、３９０　サーバ記憶部、３９１　利用者情報ファイル、３９２　機器情報ファイル、４００　通信機器、４１０　相互認証部、４２０　暗号通信部、４３０　暗号鍵生成部、４４０　機器証明書導入部、４９０　機器記憶部、４９１　機器ＩＤ、４９２　機器公開鍵、４９３　機器秘密鍵、４９４　機器証明書、９０１　演算装置、９０２　補助記憶装置、９０３　主記憶装置、９０４　通信装置、９０５　入出力装置、９０９　バス。

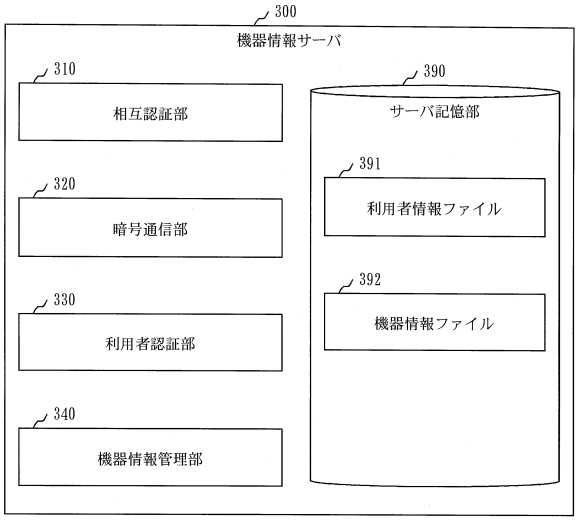
【図１】



【図２】



【図３】



【図４】

391:利用者情報ファイル

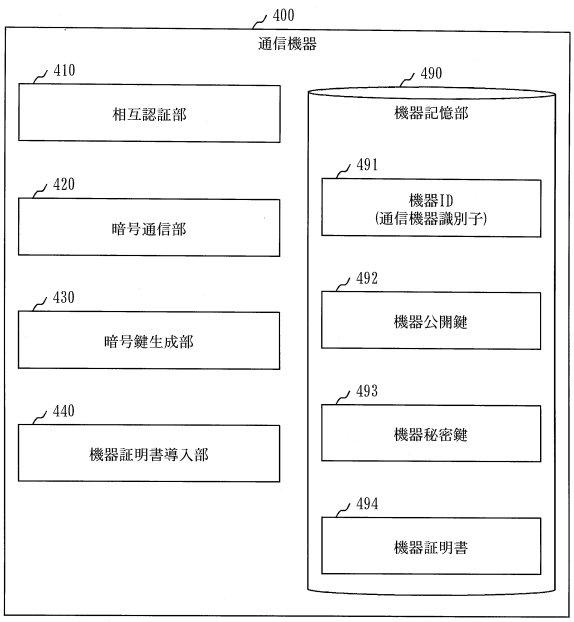
データ番号	利用者ID	パスワード	・・・
1	USER001	PW001	・・・
:	:	:	:

【図５】

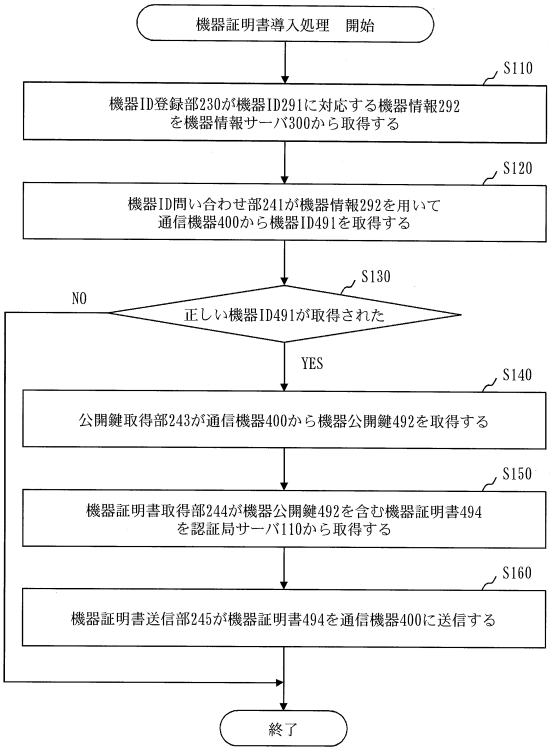
392:機器情報ファイル

データ番号	機器ID	IPアドレス	MACアドレス	・・・
1	JP00・・・	197.168.…	00-50-……	・・・
:	:	:	:	:

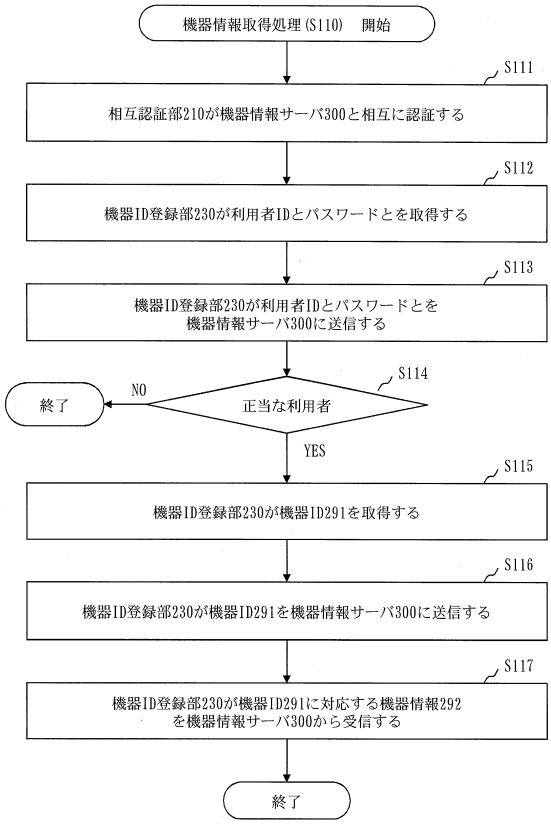
【図６】



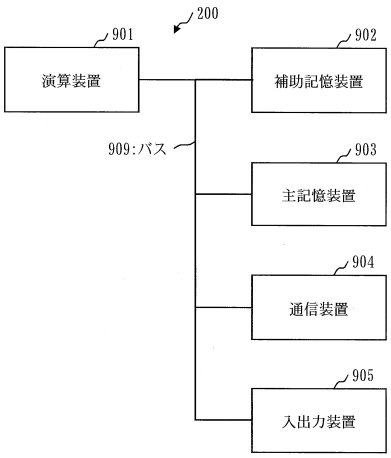
【図７】



【図８】


機器情報取得処理(S110)　開始
S111
相互認証部210が機器情報サーバ300と相互に認証する
S112
機器ID登録部230が利用者IDとパスワードとを取得する
S113
機器ID登録部230が利用者IDとパスワードとを
機器情報サーバ300に送信する
S114
正当な利用者
NO
終了
YES
S115
機器ID登録部230が機器ID291を取得する
S116
機器ID登録部230が機器ID291を機器情報サーバ300に送信する
S117
機器ID登録部230が機器ID291に対応する機器情報292
を機器情報サーバ300から受信する
終了

【図９】


200
901
演算装置
902
補助記憶装置
909:バス
903
主記憶装置
904
通信装置
905
入出力装置

フロントページの続き

(56)参考文献 特開２００６－１７４１５２（ＪＰ，Ａ）
特開２００５－１１０２１３（ＪＰ，Ａ）
特開２０１２－０２２５２０（ＪＰ，Ａ）
特開２００５－１０９９１３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／０８
Ｇ０６Ｆ　２１／４４
Ｇ０６Ｆ　２１／６４
Ｈ０４Ｌ　１２／７０