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

特許第5569440号
(P5569440)

(45)発行日　平成26年8月13日(2014.8.13)　(24)登録日　平成26年7月4日(2014.7.4)

(51)Int.Cl.		F I		
G06F 21/33	(2013.01)	G06F	21/20	133
G09C 1/00	(2006.01)	G09C	1/00	660E
G06F 3/12	(2006.01)	G06F	3/12	K
B41J 29/38	(2006.01)	B41J	29/38	Z
B41J 29/00	(2006.01)	B41J	29/00	Z

請求項の数 6　(全 20 頁)　最終頁に続く

(21)出願番号　特願2011-54069(P2011-54069)
(22)出願日　平成23年3月11日(2011.3.11)
(65)公開番号　特開2012-190320(P2012-190320A)
(43)公開日　平成24年10月4日(2012.10.4)
審査請求日　平成25年3月25日(2013.3.25)

(73)特許権者　000005267
ブラザー工業株式会社
愛知県名古屋市瑞穂区苗代町１５番１号
(74)代理人　110001058
特許業務法人鳳国際特許事務所
(72)発明者　松田　宗久
愛知県名古屋市瑞穂区苗代町１５番１号
ブラザー工業株式会社内
(72)発明者　前川　陽平
愛知県名古屋市瑞穂区苗代町１５番１号
ブラザー工業株式会社内
(72)発明者　三宅　猛
愛知県名古屋市瑞穂区苗代町１５番１号
ブラザー工業株式会社内

最終頁に続く

(54)【発明の名称】通信装置およびコンピュータプログラム

(57)【特許請求の範囲】
【請求項１】
通信装置であって、
電子証明書を格納する証明書格納部と、
ユーザの格納指示に応じて前記電子証明書を前記証明書格納部に格納する証明書格納処理部と、
第１のセキュリティレベルの通信にて送信されるデータ要求である第１のデータ要求と、前記第１のセキュリティレベルの通信より高いレベルのセキュリティが確保された第２のセキュリティレベルの通信であって、前記電子証明書を用いた接続処理を経て通信を確立するプロトコルを用いた前記第２のセキュリティレベルの通信にて送信されるデータ要求である第２のデータ要求とを受信する受信部と、
特定データを要求するデータ要求である特定データ要求が前記受信部によって受信された場合に、前記特定データ要求が前記第１のデータ要求であるか前記第２のデータ要求であるかを判断する判断部と、
前記特定データ要求が前記第２のデータ要求である場合には、前記特定データ要求の送信元である装置に対して前記特定データを送信し、前記特定データ要求が前記第１のデータ要求である場合には、前記送信元である装置に対して前記特定データとは異なる別データであって、前記送信元である装置に、前記特定データ要求を前記第２のセキュリティレベルの通信にて再送させるための表示情報を含む前記別データを送信する送信部と、
を備え、

前記証明書格納部は、前記証明書格納処理部によって格納される前記電子証明書である第１の電子証明書を格納するための第１証明書格納部と、前記証明書格納処理部を介さずに格納される前記電子証明書である第２の電子証明書を格納するための第２証明書格納部と、を有し、
前記通信装置は、さらに、
前記第１証明書格納部に前記第１の電子証明書が格納されている場合には、前記第１の電子証明書を選択し、前記第１証明書格納部に前記第１の電子証明書が格納されていない場合には、前記第２の電子証明書を選択する証明書選択部を備え、
前記送信部は、前記証明書選択部によって選択された前記電子証明書を用いた接続処理を経て確立された通信にて、前記特定データの送信を行う、通信装置。

【請求項２】
請求項１に記載の通信装置であって、さらに、
前記証明書選択部による選択結果を示す情報を格納する選択結果格納部を備え、
前記証明書選択部は、前記第２のデータ要求を受信するための前記接続処理の前に、前記電子証明書の選択を行い、前記選択結果を示す情報を前記選択結果格納部に格納する、通信装置。

【請求項３】
請求項１または請求項２のいずれかに記載の通信装置であって、さらに、
前記判断部は、前記特定データ要求とともに送信される情報、または、前記特定データ要求に含まれる情報を用いて、前記特定データ要求が前記第１のデータ要求であるか前記第２のデータ要求であるかを判断する、通信装置。

【請求項４】
請求項１ないし請求項３のいずれかに記載の通信装置であって、さらに、
前記証明書格納部に前記電子証明書が格納されていない場合に、前記電子証明書を生成する証明書生成部を備える、通信装置。

【請求項５】
請求項４に記載の通信装置であって、さらに、
前記証明書生成部によって生成された前記電子証明書の有効期限までの期間が、特定期間より短い場合に、前記証明書生成部によって生成された前記電子証明書を更新する証明書更新部を備える、通信装置。

【請求項６】
電子証明書を格納する証明書格納部を備える通信装置の制御プログラムであって、
ユーザの格納指示に応じて前記電子証明書を前記証明書格納部に格納する証明書格納処理機能と、
第１のセキュリティレベルの通信にて送信されるデータ要求である第１のデータ要求と、前記第１のセキュリティレベルの通信より高いレベルのセキュリティが確保された第２のセキュリティレベルの通信であって、前記電子証明書を用いた接続処理を経て通信を確立するプロトコルを用いた前記第２のセキュリティレベルの通信にて送信されるデータ要求である第２のデータ要求とを受信する受信機能と、
特定データを要求するデータ要求である特定データ要求が前記受信機能によって受信された場合に、前記特定データ要求が前記第１のデータ要求であるか前記第２のデータ要求であるかを判断する判断機能と、
前記特定データ要求が前記第２のデータ要求である場合には、前記特定データ要求の送信元である装置に対して前記特定データを送信し、前記特定データ要求が前記第１のデータ要求である場合には、前記送信元である装置に対して前記特定データとは異なる別データであって、前記送信元である装置に、前記特定データ要求を前記第２のセキュリティレベルの通信にて再送させるための表示情報を含む前記別データを送信する送信機能と、
を前記通信装置のコンピュータに実現させ、
前記証明書格納部は、前記証明書格納処理機能によって格納される前記電子証明書である第１の電子証明書を格納するための第１証明書格納部と、前記証明書格納処理機能を介

さずに格納される前記電子証明書である第２の電子証明書を格納するための第２証明書格納部と、を有し、
前記制御プログラムは、さらに、
前記第１証明書格納部に前記第１の電子証明書が格納されている場合には、前記第１の電子証明書を選択し、前記第１証明書格納部に前記第１の電子証明書が格納されていない場合には、前記第２の電子証明書を選択する証明書選択機能を前記通信装置のコンピュータに実現させ、
前記送信機能は、前記証明書選択機能によって選択された前記電子証明書を用いた接続処理を経て確立された通信にて、前記特定データの送信を行う、制御プログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、セキュリティレベルが異なる複数種類の通信によってデータ要求を受信可能な通信技術に関する。

【背景技術】

【０００２】

複数の通信装置の間の通信として、セキュリティレベルが異なる複数種類の通信が用いられている。例えば、特許文献１には、ＷＥＢサーバからクライアントにＷＥＢページデータを送信する際の通信として、ＨＴＴＰ通信と、ＨＴＴＰ通信よりセキュリティレベルが高いＨＴＴＰＳ通信とが開示されている。ここで、ＨＴＴＰ通信とは、電子証明書を用いて暗号化通信を行うプロトコルであるＳＳＬ（Secure Socket Layer）を用いることなく、ＷＥＢサーバと端末装置との通信に用いられる標準プロトコルであるＨＴＴＰ（HyperText Transfer Protocol）を用いて行う通信を指す。また、ＨＴＴＰＳ通信とは、ＳＳＬを、ＨＴＴＰの下位レイヤーとして実装したプロトコルであるＨＴＴＰＳ（HyperText Transfer Protocol Secure）を用いた通信を指す。

【先行技術文献】

【特許文献】

【０００３】

【特許文献１】特開２００７－９４５１０号公報

【発明の概要】

【発明が解決しようとする課題】

【０００４】

しかしながら、上記技術では、ＨＴＴＰ通信によるＷＥＢページデータの要求と、ＨＴＴＰＳ通信によるＷＥＢページデータの要求と、の両方をクライアントに許容するように、ＷＥＢサーバを構成することについては、考慮されていなかった。このように構成すると、ＨＴＴＰＳ通信とＨＴＴＰ通信のどちらを用いるかはクライアントに委ねられるので、クライアントの処理の自由度は向上するものの、不都合を生じる場合があった。例えば、クライアントが要求するデータがセキュリティを確保すべき特定データ（例えば、個人情報を含み得るＷＥＢページデータ）が含まれる場合に、その特定データの通信のセキュリティが確保されない可能性があった。このような問題は、上記ＷＥＢサーバに限らず、セキュリティレベルが異なる複数種類の通信によってデータ要求を受信可能な通信装置において共通する問題であった。

【０００５】

本発明の主な利点は、セキュリティレベルが異なる複数種類の通信によってデータ要求を受信可能な通信装置において、特定データに対するセキュリティを向上することである。

【課題を解決するための手段】

【０００６】

本発明は、上述の課題の少なくとも一部を解決するためになされたものであり、以下の態様または適用例として実現することが可能である。

［態様］通信装置であって、
　電子証明書を格納する証明書格納部と、
　ユーザの格納指示に応じて前記電子証明書を前記証明書格納部に格納する証明書格納処理部と、
　第１のセキュリティレベルの通信にて送信されるデータ要求である第１のデータ要求と、前記第１のセキュリティレベルの通信より高いレベルのセキュリティが確保された第２のセキュリティレベルの通信であって、前記電子証明書を用いた接続処理を経て通信を確立するプロトコルを用いた前記第２のセキュリティレベルの通信にて送信されるデータ要求である第２のデータ要求とを受信する受信部と、
　特定データを要求するデータ要求である特定データ要求が前記受信部によって受信された場合に、前記特定データ要求が前記第１のデータ要求であるか前記第２のデータ要求であるかを判断する判断部と、
　前記特定データ要求が前記第２のデータ要求である場合には、前記特定データ要求の送信元である装置に対して前記特定データを送信し、前記特定データ要求が前記第１のデータ要求である場合には、前記送信元である装置に対して前記特定データとは異なる別データであって、前記送信元である装置に、前記特定データ要求を前記第２のセキュリティレベルの通信にて再送させるための表示情報を含む前記別データを送信する送信部と、　を備え、
　前記証明書格納部は、前記証明書格納処理部によって格納される前記電子証明書である第１の電子証明書を格納するための第１証明書格納部と、前記証明書格納処理部を介さずに格納される前記電子証明書である第２の電子証明書を格納するための第２証明書格納部と、を有し、
　前記通信装置は、さらに、
　前記第１証明書格納部に前記第１の電子証明書が格納されている場合には、前記第１の電子証明書を選択し、前記第１証明書格納部に前記第１の電子証明書が格納されていない場合には、前記第２の電子証明書を選択する証明書選択部を備え、
　前記送信部は、前記証明書選択部によって選択された前記電子証明書を用いた接続処理を経て確立された通信にて、前記特定データの送信を行う、通信装置。

【０００７】

［適用例１］通信装置であって、
　第１のセキュリティレベルの通信にて送信されるデータ要求である第１のデータ要求と、前記第１のセキュリティレベルの通信より高いレベルのセキュリティが確保された第２のセキュリティレベルの通信にて送信されるデータ要求である第２のデータ要求とを受信する受信部と、
　特定データを要求するデータ要求である特定データ要求が前記受信部によって受信された場合に、前記特定データ要求が前記第１のデータ要求であるか前記第２のデータ要求であるかを判断する判断部と、
　前記特定データ要求が前記第２のデータ要求である場合には、前記特定データ要求の送信元である装置に対して前記特定データを送信し、前記特定データ要求が前記第１のデータ要求である場合には、前記送信元である装置に対して前記特定データとは異なる別データであって、前記送信元である装置に、前記特定データ要求を前記第２のセキュリティレベルの通信にて再送させるための表示情報を含む前記別データを送信する送信部と、
　を備える通信装置。

【０００８】

　上記構成によれば、第１のセキュリティレベルの通信にて特定データ要求を通信装置に対して送信した装置は、特定データとは異なる別データを取得し、別データを取得した後に、容易に第２のセキュリティレベルの通信にて特定データ要求を再送することができる。この結果、第１のセキュリティレベルの通信にて特定データを要求する特定データ要求が通信装置に対して行われた場合であっても、特定データは、第２のセキュリティレベルの通信にて送信される。したがって、セキュリティレベルが低い通信にて特定データが送

信されることを抑制して特定データに対するセキュリティを向上することができる。
【０００９】
なお、本発明は、種々の形態で実現可能であり、例えば、画像処理装置、印刷装置、通信方法、これらの装置の機能または方法を実現するためのコンピュータプログラム、そのコンピュータプログラムを記録した記録媒体、等の形態で実現することができる。
【図面の簡単な説明】
【００１０】
【図１】第１実施例におけるネットワークシステムの概略構成を示す図。
【図２】クライアントとプリンタとの通信処理について説明するシーケンス図。
【図３】第１実施例における証明書選択処理の処理ステップを示すフローチャート。
【図４】通知ページの一例を示す図。
【図５】送信ページデータ選択処理の処理ステップを示すフローチャート。
【図６】特定情報登録ページの一例を示す図。
【図７】警告ページの一例を示す図。
【図８】特定ＷＥＢページとは異なるＷＥＢページの一例を示す図。
【図９】第２実施例における証明書選択処理の処理ステップを示すフローチャート。
【図１０】証明書更新処理の処理ステップを示すフローチャート。
【発明を実施するための形態】
【００１１】
Ａ．第１実施例：
Ａ－１．ネットワークシステムの構成：
次に、本発明の実施の形態を実施例に基づき説明する。図１は、第１実施例におけるネットワークシステムの概略構成を示す図である。ネットワークシステム１０００は、プリンタ１００と、クライアントとしての計算機（以下、単にクライアントという。）２００と、サーバとしての計算機（以下、単にサーバという。）３００とを備えている。プリンタ１００と、クライアント２００は、第１のローカルエリアネットワーク４００に接続されている。サーバ３００は、第２のローカルエリアネットワーク５００に接続されている。第１のローカルエリアネットワーク４００は、ファイアウォール６００を介して、インターネット７００に接続されている。第２のローカルエリアネットワーク５００は、インターネット７００に接続されている。ファイアウォール６００は、ファイアウォールとしての機能を有する周知のスイッチまたは計算機である。
【００１２】
クライアント２００は、インストールされたプログラムを実行することにより、ＷＥＢブラウザ２０１の機能と、文書作成、画像作成などのアプリケーション２０２の機能と、印刷ジョブ生成部２０３の機能と、を実現する。印刷ジョブ生成部２０３は、アプリケーション２０２から印刷データと印刷指示を受け取り、印刷データを印刷するための印刷ジョブを生成する。印刷ジョブ生成部２０３は、具体的には、プリンタ１００に対応したプリンタドライバ、または、後述する外部プリントサービスに対応したドライバである。
【００１３】
サーバ３００は、サーバプログラムを実行することにより、クライアント２００に対して外部プリントサービスを提供するプリントサーバ部３０２の機能を実現する。
【００１４】
外部プリントサービスを用いない場合には、クライアント２００には、印刷ジョブ生成部２０３としてプリンタ１００に対応したプリンタドライバがインストールされる。印刷ジョブ生成部２０３は、プリンタ１００が解釈可能な印刷ジョブを生成して、プリンタ１００に送信する。プリンタ１００は、受信した印刷ジョブに基づいて印刷を実行する。
【００１５】
外部プリントサービスを用いる場合には、クライアント２００には、印刷ジョブ生成部２０３として外部プリントサービスに対応したドライバがインストールされる。クライアント２００のユーザは、サーバ３００に、特定情報（例えば、アカウント名およびパスワ

ード）を登録するとともに、プリンタ１００を登録する。印刷ジョブ生成部２０３は、サーバ３００が解釈可能な印刷ジョブを生成して、サーバ３００に送信する。この印刷ジョブには、上述した特定情報と、プリンタ１００を特定する情報が含まれる。プリンタ１００は、サーバ３００からの通知、または、サーバ３００に対する定期的な問い合わせにより、クライアント２００からの印刷要求を認識すると、サーバ３００に対して印刷ジョブを要求する。サーバ３００は、クライアント２００の印刷ジョブ生成部２０３から受信した印刷ジョブに基づいて、プリンタ１００が解釈可能な印刷ジョブを生成して、プリンタ１００に送信する。プリンタ１００は、受信した印刷ジョブに基づいて印刷を実行する。

【００１６】

外部プリントサービスを利用すれば、例えば、クライアント２００のユーザが、複数種類のプリンタを利用する場合に、プリンタ毎に異なるプリンタドライバを印刷ジョブ生成部２０３としてインストールする必要がない利点がある。

【００１７】

ここで、サーバ３００に対して印刷ジョブを要求する際には、プリンタ１００は、クライアント２００のユーザがサーバ３００に登録した上述した特定情報を必要とする。このために、クライアント２００のユーザは、外部プリントサービスを利用する前に、プリンタ１００に、上述した特定情報を登録する。この特定情報の登録は、後述するプリンタ１００のＷＥＢサーバ部Ｍ１０がＷＥＢページの形式で提供するユーザインタフェースに、ユーザがクライアント２００のＷＥＢブラウザ２０１を用いてアクセスすることによって行われる。

【００１８】

また、クライアント２００とサーバ３００との通信、および、サーバ３００とプリンタ１００との通信は、ＳＳＬを用いた暗号化通信（以下、ＳＳＬ通信とも呼ぶ。）を用いて行われる。ＳＳＬ通信は、ＳＳＬを用いない非暗号化通信（以下、単に、非暗号化通信とも呼ぶ。）より高いセキュリティレベルが確保されている。

【００１９】

プリンタ１００は、ＣＰＵ（Central processing unit）１１０と、揮発性メモリであるＲＡＭ（Random Access Memory）１２０と、書き換え不可能な不揮発性メモリであるマスクＲＯＭ（Mask Read Only Memory）１３０と、書き換え可能な不揮発性メモリであるＥＥＰＲＯＭ（Electrically Erasable Programmable Read-Only Memory）１４０と、ユーザの操作を受け付ける各種のボタンを含む操作部１５０と、周知の方式（例えば、レーザー、インクジェット）で印刷媒体に画像を形成する印刷部１６０と、ネットワークに接続するためのインタフェース部（Ｉ／Ｆ部）１７０と、を備えている。

【００２０】

ＣＰＵ１１０は、マスクＲＯＭ１３０に格納されたコンピュータプログラムを実行することにより、ＷＥＢサーバ部Ｍ１０、証明書管理部Ｍ２０、印刷制御部Ｍ３０として機能する。

【００２１】

ＷＥＢサーバ部Ｍ１０は、プリンタ１００に関する種々の設定を行うためのユーザインタフェースをＷＥＢページの形式でクライアント２００に提供するＨＴＴＰサーバとして機能する。ＷＥＢサーバ部Ｍ１０は、受信部Ｍ１１と、送信部Ｍ１２と、受信プロトコル判断部Ｍ１３とを備えている。

【００２２】

受信部Ｍ１１は、クライアント２００からＨＴＴＰリクエストを受信する。送信部Ｍ１２は、ＨＴＴＰリクエストに応じて、クライアント２００に対してＨＴＴＰレスポンスを送信する。受信部Ｍ１１および送信部Ｍ１２は、ＨＴＴＰの下位レイヤーのプロトコルとしてＳＳＬを実装している。すなわち、受信部Ｍ１１は、ＳＳＬ通信にてＨＴＴＰリクエストを受信することが可能である。また、受信部Ｍ１１は、非暗号化通信にてＨＴＴＰリクエストを受信することが可能である。送信部Ｍ１２は、ＳＳＬ通信にて受信されたＨＴＴＰリクエストに対する応答として、ＳＳＬ通信にてＨＴＴＰレスポンスを送信すること

が可能である。送信部Ｍ１２は、非暗号化通信にて受信されたＨＴＴＰリクエストに対する応答として、非暗号化通信にてＨＴＴＰレスポンスを送信することが可能である。

【００２３】

受信プロトコル判断部Ｍ１３は、受信部Ｍ１１がＨＴＴＰリクエストを受信した場合に、そのＨＴＴＰリクエストが、クライアント２００からＳＳＬ通信にて送信されたリクエストであるか、非暗号化通信に送信されたリクエストであるかを判断する。

【００２４】

ここで、ＳＳＬ通信の接続処理（ＳＳＬハンドシェイク）では、サーバ証明書を用いる。このサーバ証明書は、公開鍵と、その公開鍵に関連付けられた所有者情報および署名者情報と、有効期限を表す情報を含む電子証明書である。所有者情報は、公開鍵の所有者を特定する情報である。署名者情報は、公開鍵の所有者が所有者情報にて特定される者であると宣言する者（署名者）を特定する情報である。サーバ証明書は、サーバ証明書と関連付けられた秘密鍵とセットでサーバ（例えば、本実施例では、ＷＥＢサーバとして機能するプリンタ１００）に格納される。

【００２５】

プリンタ１００が扱うサーバ証明書には、プリンタ１００への格納方法による分類で以下のような種類がある。

１）ユーザの格納指示に応じてプリンタ１００に格納されたサーバ証明書（以下、ユーザインストール証明書とも呼ぶ。）

２）プリンタ１００の製造時にプリンタ１００に格納されたサーバ証明書（以下、プリインストール証明書とも呼ぶ。）

【００２６】

証明書管理部Ｍ２０は、サーバ証明書を管理する機能部である。証明書管理部Ｍ２０は、証明書選択部Ｍ２１と、証明書格納処理部Ｍ２２と、を備えている。証明書管理部Ｍ２０は、さらに、証明書生成部Ｍ２３と、証明書更新部Ｍ２４とを備えても良い。証明書生成部Ｍ２３および証明書更新部Ｍ２４を備える構成については、第２実施例として後述する。

【００２７】

証明書選択部Ｍ２１は、クライアント２００とＳＳＬ通信を行う際に使用するサーバ証明書を、ＳＳＬ通信の接続処理が行われる前（本実施例では、プリンタ１００の起動時）に予め選択する証明書選択処理を実行する。

【００２８】

証明書格納処理部Ｍ２２は、ユーザの格納指示に応じてサーバ証明書を所定の格納領域に格納する証明書格納処理を実行する。証明書格納処理部Ｍ２２により格納されるサーバ証明書は、上述したユーザインストール証明書となる。

【００２９】

印刷制御部Ｍ３０は、印刷ジョブを受信して、印刷部１６０に受信した印刷ジョブに基づいた印刷を実行させる。印刷制御部Ｍ３０は、クライアント２００から印刷ジョブを受信することが可能である。また、印刷制御部Ｍ３０は、上述した外部プリントサービスが実行される場合に、サーバ３００から印刷ジョブを受信することが可能である。

【００３０】

ＲＡＭ１２０は、ＣＰＵ１１０が処理を行う際に一時的にデータを格納するバッファ領域として用いられる。また、ＲＡＭ１２０は、上述した証明書選択部Ｍ２１が証明書選択処理を行った際に、サーバ証明書の選択結果を示す情報を格納する選択結果格納領域１２１を有している。ＲＡＭ１２０は、さらに、自動生成証明書格納領域１２２を有しても良い。自動生成証明書格納領域１２２を有する構成については、第２実施例として後述する。

【００３１】

マスクＲＯＭ１３０には、ＣＰＵ１１０が用いる種々のプログラムおよびデータが格納されている。また、マスクＲＯＭ１３０は、プリインストール証明書格納領域１３１を有

し、上述したプリインストール証明書が格納されている。プリインストール証明書格納領域１３１がマスクＲＯＭ１３０に備えられることにより、プリインストール証明書格納領域１３１がＥＥＰＲＯＭ１４０に備えられる場合と比較して、マスクＲＯＭ１３０よりコストの高いＥＥＰＲＯＭ１４０の必要容量を抑制することができる。

【００３２】

ＥＥＰＲＯＭ１４０は、プリンタ１００に関する設定情報などの格納に用いられる。また、ＥＥＰＲＯＭ１４０は、ユーザインストール証明書格納領域１４２を有している。ユーザインストール証明書格納領域１４２には、上述した証明書格納処理部Ｍ２２により、ユーザインストール証明書が格納される。ユーザインストール証明書格納領域１４２は、複数のユーザインストール証明書を格納可能である。なお、本実施例では、プリインストール証明書格納領域１３１は、マスクＲＯＭ１３０に設けられているが、これに代えて、ＥＥＰＲＯＭ１４０においてユーザインストール証明書格納領域１４２とは異なる領域に設けてもよい。

【００３３】

Ａ－２．クライアント２００とプリンタ１００との通信処理

図２は、クライアント２００とプリンタ１００との通信処理について説明するシーケンス図である。図２（ａ）には、証明書格納処理の処理ステップを示すシーケンス図が示されている。図２（ｂ）には、ＷＥＢブラウザ２０１とＷＥＢサーバ部Ｍ１０との通信処理の処理ステップを示すシーケンス図が示されている。

【００３４】

Ａ－２－１．証明書格納処理

まず、プリンタ１００の証明書格納処理部Ｍ２２が実行する証明書格納処理について説明する。証明書格納処理部Ｍ２２は、サーバ証明書を上述したユーザインストール証明書格納領域１４２に格納することをプリンタ１００に対して要求するユーザインストール証明書格納要求に応じて、証明書格納処理を実行する。図２（ａ）に示すように、プリンタ１００のユーザ（例えば、第１のローカルエリアネットワーク４００の管理者）は、クライアント２００を操作して、クライアント２００からプリンタ１００に対してユーザインストール証明書格納要求を送信することができる（ステップＳ１０）。

【００３５】

証明書格納処理において格納されるユーザインストール証明書には、署名者による分類で以下の２種類がある。

１）パブリック認証局（Public CA(Certification Authority)）が署名者であるサーバ証明書（以下、パブリックＣＡ署名証明書と呼ぶ。）

２）ユーザが署名者であるサーバ証明書（以下、ユーザ署名証明書と呼ぶ。）。この場合、ユーザによる署名は、プライベート認証局（private CA）による署名とも呼ばれる。

【００３６】

また、証明書格納処理において、格納対象であるユーザインストール証明書を証明書格納処理部Ｍ２２が取得する取得処理には、以下の３種類がある。

取得処理Ａ）証明書格納処理部Ｍ２２は、秘密鍵とＣＳＲ（Certificate Signing Request）とを生成する。ユーザは、ＣＳＲをパブリック認証局に送信して、パブリックＣＡ署名証明書の暗号化データをパブリック認証局から取得する。証明書格納処理部Ｍ２２は、秘密鍵と暗号化データを用いてパブリックＣＡ署名証明書を復号して取得する。

取得処理Ｂ）証明書格納処理部Ｍ２２は、秘密鍵とＣＳＲとを生成する。証明書格納処理部Ｍ２２は、ユーザからの指示に応じてＣＳＲに署名する処理を行い、ユーザ署名証明書を生成する。なお、ユーザ署名証明書を生成する場合には、クライアント２００のＷＥＢブラウザ２０１にインポートするためのプライベートＣＡ証明書を生成して、クライアント２００に提供しても良い。

取得処理Ｃ）証明書格納処理部Ｍ２２は、外部（例えば、クライアント２００）にエクスポートされているサーバ証明書と秘密鍵を、インポートする。

【００３７】

証明書格納処理部Ｍ２２は、クライアント２００との通信を介して、ユーザと必要な情報の遣り取りを行いながら、上記取得処理を実行する（ステップＳ２０）。ここで、ユーザと遣り取りされる情報には、例えば、上述したＣＳＲの生成に必要なディスティングイッシュネームなどが含まれる。証明書格納処理部Ｍ２２は、ユーザインストール証明書を取得すると、取得したユーザインストール証明書を秘密鍵と関連付けて、ＥＥＰＲＯＭ１４０のユーザインストール証明書格納領域１４２に格納する（ステップＳ３０）。

【００３８】

また、証明書格納処理部Ｍ２２は、ユーザインストール証明書の格納とともに、ユーザインストール証明書に関連する種々の関連情報をＥＥＰＲＯＭ１４０に格納する（ステップＳ３０）。例えば、ユーザインストール証明書の取得処理の種類（上記取得処理Ａ～Ｃのいずれかの処理）を特定する情報を、ユーザインストール証明書と関連付けてＥＥＰＲＯＭ１４０に格納する。また、証明書格納処理部Ｍ２２は、複数のユーザインストール証明書がユーザインストール証明書格納領域１４２に格納されている場合に、使用するユーザインストール証明書を指定する指定指示をユーザから受け付けることができる。証明書格納処理部Ｍ２２は、ユーザから指定指示を受け付けた場合には、ユーザが指定するユーザインストール証明書を特定するためのユーザ指定情報をＥＥＰＲＯＭ１４０に格納する。

【００３９】

ステップＳ３０に続いて、証明書格納処理部Ｍ２２は、プリンタ１００を再起動する処理を実行し（ステップＳ４０）、証明書格納処理を終了する。

【００４０】

なお、証明書格納処理において、証明書格納処理部Ｍ２２とユーザとの情報の遣り取りは、プリンタ１００のＷＥＢサーバ部Ｍ１０がＷＥＢページの形式で提供するユーザインタフェースに、ユーザがクライアント２００のＷＥＢブラウザ２０１を用いてアクセスすることによって行われる。

【００４１】

Ａ－２－２．証明書選択処理

上述したように、クライアント２００のユーザに対して、種々のユーザインタフェースをＷＥＢページの形式で提供するプリンタ１００のＷＥＢサーバ部Ｍ１０と、クライアント２００のＷＥＢブラウザ２０１との通信処理について説明する。

【００４２】

図２（ｂ）に示すように、ＷＥＢブラウザ２０１とＷＥＢサーバ部Ｍ１０との通信処理の前（本実施例では、プリンタ１００の起動時）に、証明書選択部Ｍ２１は、証明書選択処理を実行する（ステップＳ５０）。「プリンタ１００の起動時」には、電源投入時、および、再起動時が含まれる。上述した証明書格納処理の終了時には、プリンタ１００の再起動が行われるので、再起動後に直ぐに証明書選択処理が行われる。

【００４３】

図３は、証明書選択処理の処理ステップを示すフローチャートである。証明書選択処理が開始されると、証明書選択部Ｍ２１は、ユーザインストール証明書は利用可能であるか否かを判断する（ステップＳ５０２）。証明書選択部Ｍ２１は、ユーザインストール証明書格納領域１４２に、有効期限が切れていない少なくとも１つのユーザインストール証明書が格納されている場合には、ユーザインストール証明書は利用可能であると判断する。証明書選択部Ｍ２１は、ユーザインストール証明書格納領域１４２に、有効期限が切れていないユーザインストール証明書が格納されていない場合には、ユーザインストール証明書は利用可能でないと判断する。

【００４４】

証明書選択部Ｍ２１は、ユーザインストール証明書は利用可能であると判断すると（ステップＳ５０２：ＹＥＳ）、優先順位に従って、利用可能なユーザインストール証明書の中から、使用するサーバ証明書を選択する（ステップＳ５０４）。

【００４５】

ユーザインストール証明書の優先順位を以下に示す。若い番号ほど優先順位が高い。
１．ユーザ指定情報により特定されるユーザインストール証明書
２．上述した取得処理Ａによって取得されたユーザインストール証明書
３．上述した取得処理Ｃによって取得されたユーザインストール証明書
４．上述した取得処理Ｂによって取得されたユーザインストール証明書

【００４６】

パブリックＣＡ署名証明書は、ユーザ署名証明書より信頼性が高いと考えられる。ここで、取得処理Ａによって取得されたユーザインストール証明書は、パブリックＣＡ署名証明書である。取得処理Ｂによって取得されたユーザインストール証明書は、ユーザ署名証明書である。取得処理Ｃによって取得されたユーザインストール証明書は、パブリックＣＡ署名証明書である場合と、ユーザ署名証明書である場合とがある。以上を考慮して、ユーザによる指定指示があった場合には、ユーザによる指定指示を優先し、ユーザによる指定指示がない場合には、パブリックＣＡ署名証明書がユーザ署名証明書より優先して選択されるように、上記の優先順位が規定されている。利用可能なユーザインストール証明書が１つしかない場合には、そのユーザインストール証明書が選択される。

【００４７】

証明書選択部Ｍ２１は、ユーザインストール証明書は利用可能でないと判断すると（ステップＳ５０２：ＮＯ）、プリインストール証明書を、使用するサーバ証明書として選択する（ステップＳ５０６）。すなわち、ユーザインストール証明書が利用可能である場合には、ユーザインストール証明書を優先して使用し、ユーザインストール証明書が利用不可能である場合に限って、プリインストール証明書を使用するように、使用するサーバ証明書が選択される。

【００４８】

使用するサーバ証明書が選択されると、証明書選択部Ｍ２１は、選択結果を示す情報をＲＡＭ１２０の選択結果格納領域１２１に格納し（ステップＳ５０８）、証明書選択処理を終了する。選択結果を示す情報は、例えば、選択されたサーバ証明書と、ＷＥＢサーバ部Ｍ１０に実装されたＳＳＬプロトコルと、を対応付けるバインド情報として選択結果格納領域１２１に格納される。

【００４９】

Ａ－２－３．ＷＥＢブラウザ２０１と、ＷＥＢサーバ部Ｍ１０との通信処理

上述したようにクライアント２００のユーザに対して、種々のユーザインタフェースをＷＥＢページの形式で提供するプリンタ１００のＷＥＢサーバ部Ｍ１０と、クライアント２００のＷＥＢブラウザ２０１との通信処理（図２（ｂ））について説明する。

【００５０】

ＷＥＢページは、ＵＲＬ（Uniform Resource Locator）によって特定される。ＵＲＬの基本な形式は、以下のように表される。

<scheme>://<host>/<path>

<scheme>は、リソースの取得方法を規定する部分であり、例えば、プロトコル名が記述される。<host>は、ＷＥＢサーバを指定する部分であり、例えば、ＷＥＢサーバに割り当てられたＩＰアドレスまたはドメインネームが記述される。<path>は、ＷＥＢサーバ上のリソース名（位置）が記述される。

【００５１】

ユーザは、クライアント２００のＷＥＢブラウザ２０１の表示画面（ブラウザ画面）において、ＵＲＬを指定することにより、ＵＲＬによって特定されるＷＥＢページのデータ（以下、単に、ページデータと呼ぶ）を要求するＷＥＢページ要求（ＨＴＴＰリクエスト）を送信する。ユーザによるＵＲＬの指定は、例えば、１）ブラウザ画面におけるＵＲＬ入力欄にＵＲＬを入力する、２）ブラウザ画面に表示されたＷＥＢページにおけるＵＲＬと対応付けられた項目（例えば、文字列や画像：以下では、リンク項目とも呼ぶ）を選択する、３）予め登録されたＵＲＬを選択する、ことによって行われる。

【００５２】

プリンタ１００のＷＥＢサーバ部Ｍ１０は、上述したように、ＳＳＬ通信と、非暗号化通信の両方に対応している。いずれの通信を用いるかは、ユーザの裁量に委ねられている。ユーザは、非暗号化通信を用いる場合には、<scheme>を「http」としたＵＲＬを指定すれば良く、ＳＳＬ通信を用いる場合には、<scheme>を「https」としたＵＲＬを指定すれば良い。

【００５３】

例えば、プリンタ１００に「192.168.11.16」というＩＰアドレスが割り当てられている場合には、ＷＥＢサーバ部Ｍ１０が提供するＷＥＢページのトップページのページデータを要求するためのＵＲＬとして、「http://192.168.11.16/」、または、「https://192.168.11.16/」を指定することができる。

【００５４】

ＷＥＢサーバ部Ｍ１０が提供するトップページ以外のＷＥＢページのページデータのＵＲＬの指定は、例えば、トップページを始めとするＷＥＢサーバ部Ｍ１０によって提供されるＷＥＢページに表示されたリンク項目を選択することによって行われる。本実施例のＷＥＢサーバ部Ｍ１０が提供するＷＥＢページでは、リンク項目に対応付けられたＵＲＬは、相対パス形式、すなわち、<scheme>と<host>を省略した形式で記述されている。ユーザが、相対パス形式のＵＲＬを指定した場合、対応するリンク項目を含むＷＥＢページのページデータを取得したときと同じ<scheme>および<host>を指定したとみなされる。

【００５５】

ユーザが<scheme>を「https」としたＵＲＬを指定した場合には、図２（ｂ）に示すように、クライアント２００のＷＥＢブラウザ２０１は、ＨＴＴＰリクエストの送信の前に、プリンタ１００のＷＥＢサーバ部Ｍ１０に対して、ＳＳＬ通信を要求するＳＳＬ通信要求を送信する（ステップＳ６０）。ＳＳＬ通信要求に続いて、ＷＥＢブラウザ２０１とＷＥＢサーバ部Ｍ１０との間で、ＳＳＬハンドシェイクが行われる（ステップＳ７０）。以下では、ステップＳ６０とステップＳ７０の処理を、ＳＳＬ通信確立処理とも呼ぶ。

【００５６】

ＳＳＬハンドシェイクは、ＷＥＢサーバ部Ｍ１０からＷＥＢブラウザ２０１へのサーバ証明書の送信、暗号化鍵（共通鍵）の交換を行い、ＳＳＬ通信を確立する手続処理である。ＷＥＢサーバ部Ｍ１０は、ＳＳＬハンドシェイクにおいてＷＥＢブラウザ２０１に送信するサーバ証明書として、上述した証明書選択処理（図３）にて選択したサーバ証明書を用いる。ＷＥＢブラウザ２０１は、ＳＳＬハンドシェイクにおいて、ＷＥＢサーバ部Ｍ１０から送信されたサーバ証明書を検証し、サーバ証明書が信頼できるか否かを判断する。

【００５７】

ＷＥＢブラウザ２０１には、パブリックＣＡ署名証明書の信頼性を検証するためのパブリックＣＡ証明書が予めインストールされている。ＷＥＢブラウザ２０１には、ユーザ署名証明書の信頼性を検証するためのプライベートＣＡ証明書をユーザがインポートすることができる。ＷＥＢブラウザ２０１は、これらのＣＡ証明書を用いた検証により、サーバ証明書が信頼できるか否かを判断する。パブリックＣＡ署名証明書およびユーザ署名証明書は、対応するＣＡ証明書をＷＥＢブラウザ２０１が有していれば、信頼できると判断されるが、プリインストール証明書は、基本的には、信頼できないと判断される。

【００５８】

ＷＥＢブラウザ２０１は、ＷＥＢサーバ部Ｍ１０から送信されたサーバ証明書を信頼できないと判断すると、その旨を通知する通知ページをブラウザ画面に表示する。

【００５９】

図４は、通知ページの一例を示す図である。通知ページＰ１は、サーバ証明書が信頼できない旨のメッセージＭＳ１と、２つの指示受付ボタンＢ１およびＢ２とを含んでいる。指示受付ボタンＢ１は、ユーザからＳＳＬハンドシェイクの継続指示を受け付けるためのボタンである。指示受付ボタンＢ２は、ユーザからＳＳＬハンドシェイクの中断指示を受け付けるためのボタンである。ユーザが指示受付ボタンＢ１を操作すると、ＷＥＢブラウザ２０１は、ＷＥＢサーバ部Ｍ１０から送信されたサーバ証明書を用いてＳＳＬハンドシ

ェイクを継続する。一方、ユーザが指示受付ボタンＢ２を操作すると、ＷＥＢブラウザ２０１は、ＳＳＬハンドシェイクを中断し、ブラウザ画面に、ＳＳＬハンドシェイクの開始前に表示されていたＷＥＢページを表示する。

【００６０】

ＳＳＬハンドシェイクが終了して、ＳＳＬ通信が確立されると、ＷＥＢブラウザ２０１は、ユーザが指定したＵＲＬによって特定されるページデータを要求するＨＴＴＰリクエストをＳＳＬ通信にてＷＥＢサーバ部Ｍ１０に送信する（ステップＳ８０）。ＨＴＴＰリクエストには、ＵＲＬの<path>部分が記述される。

【００６１】

ＷＥＢサーバ部Ｍ１０の受信部Ｍ１１がＨＴＴＰリクエストを受信すると、ＷＥＢサーバ部Ｍ１０は、ＨＴＴＰレスポンスに格納して送信すべきページデータ（以下では、送信ページデータとも呼ぶ）を選択する送信ページデータ選択処理を実行する（ステップＳ９０）。送信ページデータ選択処理の詳細については後述する。

【００６２】

送信ページデータが選択されると、ＷＥＢサーバ部Ｍ１０の送信部Ｍ１２は、選択されたページデータが格納されたＨＴＴＰレスポンスをＳＳＬ通信にてＷＥＢブラウザ２０１に対して送信する（ステップＳ１００）。ＷＥＢブラウザ２０１は、受信したＨＴＴＰレスポンスに格納されたページデータを用いて、ＷＥＢページをブラウザ画面に表示する（ステップＳ１１０）。

【００６３】

一方、ユーザが<scheme>を「http」としたＵＲＬを指定した場合には、ＳＳＬ通信確立処理（図２（ｂ））を行うことなく、図２（ｂ）に示すステップＳ８０～Ｓ１００の処理が行われる。すなわち、ＷＥＢブラウザ２０１は、ユーザが指定したＵＲＬによって特定されるページデータを要求するＨＴＴＰリクエストを非暗号化通信にてＷＥＢサーバ部Ｍ１０に送信する（ステップＳ８０）。そして、ＨＴＴＰリクエストを受信したＷＥＢサーバ部Ｍ１０は、送信ページデータ選択処理を実行する（ステップＳ９０）。そして、ＷＥＢサーバ部Ｍ１０の送信部Ｍ１２は、選択されたページデータが格納されたＨＴＴＰレスポンスを非暗号化通信にてＷＥＢブラウザ２０１に対して送信する（ステップＳ１００）。ＷＥＢブラウザ２０１は、受信したＨＴＴＰレスポンスに格納されたページデータを用いて、ＷＥＢページをブラウザ画面に表示する（ステップＳ１１０）。

【００６４】

次に、上述した送信ページデータ選択処理（ステップＳ９０）について説明する。図５は、送信ページデータ選択処理の処理ステップを示すフローチャートである。送信ページデータ選択処理は、ＷＥＢサーバ部Ｍ１０の受信部Ｍ１１がＨＴＴＰリクエストを受信すると開始される。まず、図５に示すように、ＷＥＢサーバ部Ｍ１０は、受信されたＨＴＴＰリクエストが要求するページデータ（以下では、要求ページデータとも呼ぶ）を認識し（ステップＳ９０４）、要求ページデータが特定ＷＥＢページのページデータ（以下では、特定ページデータとも呼ぶ）であるか否かを判断する（ステップＳ９０６）。

【００６５】

特定ページデータは、個人情報などのセキュリティの確保が求められる特定情報を含み得るＷＥＢページである。本実施例における特定ＷＥＢページは、上述した外部プリントサービスに用いる特定情報をプリンタ１００に登録するためのユーザインターフェースを提供するページ（以下では、特定情報登録ページとも呼ぶ）である。

【００６６】

図６は、特定情報登録ページの一例を示す図である。特定情報登録ページＰ２は、特定情報（具体的には、アカウント名、メールアドレス、パスワード）を入力するための入力ボックスＩＢ１～ＩＢ３を含んでいる。特定情報が既に登録されている場合には、特定情報登録ページＰ２のページデータは特定情報を含む。

【００６７】

要求ページデータが特定ページデータである場合には（図５：ステップＳ９０６：ＹＥ

Ｓ）、ＷＥＢサーバ部Ｍ１０の受信プロトコル判断部Ｍ１３は、受信されたＨＴＴＰリクエストがＳＳＬ通信にて受信されたか否かを判断する（ステップＳ９０８）。具体的には、受信プロトコル判断部Ｍ１３は、ＨＴＴＰリクエストの宛先ポート番号を取得する。宛先ポート番号は、ＨＴＴＰリクエストを格納したＴＣＰパケットのヘッダに記述されている。受信プロトコル判断部Ｍ１３は、取得した宛先ポート番号が例えば「４４３」である場合には、ＨＴＴＰリクエストはＳＳＬ通信にて受信されたと判断する。受信プロトコル判断部Ｍ１３は、取得した宛先ポート番号が「４４３」でない場合（例えば、「８０」である場合）には、ＨＴＴＰリクエストはＳＳＬ通信にて受信されていない（非暗号化通信にて受信された）と判断する。

【００６８】

ＨＴＴＰリクエストはＳＳＬ通信にて受信された場合には（ステップＳ９０８：ＹＥＳ）、ＷＥＢサーバ部Ｍ１０は、要求ページデータである特定ページデータを送信ページデータとして選択する（ステップＳ９１２）。ＨＴＴＰリクエストはＳＳＬ通信にて受信されていない場合には（ステップＳ９０８：ＮＯ）、ＷＥＢサーバ部Ｍ１０は、要求ページデータである特定ページデータに代えて、警告ページのページデータを送信ページデータとして選択する（ステップＳ９１０）。

【００６９】

図７は、警告ページの一例を示す図である。警告ページＰ３は、リクエスト再送用リンク項目ＬＴ１と、メッセージＭＳ２とを有している。リクエスト再送用リンク項目ＬＴ１は、ＷＥＢブラウザ２０１に、ＳＳＬ通信を用いて、特定ページデータを要求するＨＴＴＰリクエストを再送させるためのＵＲＬ（以下では、再送ＵＲＬとも呼ぶ）に対応付けられている。具体的には、ＵＲＬの<scheme>は、「https」である。このＵＲＬの<host>は、プリンタ１００のＩＰアドレスである。このＵＲＬの<path>は、特定ページデータを特定するリソース名である。ＷＥＢサーバ部Ｍ１０は、プリンタ１００に設定されているＩＰアドレスを取得し、再送ＵＲＬを生成して、リクエスト再送用リンク項目ＬＴ１およびメッセージＭＳ２とを含む警告ページデータを予め作成しておく。メッセージＭＳ２は、リクエスト再送用リンク項目ＬＴ１を操作することにより、セキュリティが確保されたＳＳＬ通信を用いて、特定ページデータを要求するＨＴＴＰリクエストを再送することを、ユーザに促すメッセージである。警告ページＰ３のページデータに含まれる、リクエスト再送用リンク項目ＬＴ１のデータは、ＷＥＢブラウザ２０１（クライアント２００）に、特定ページデータを要求するＨＴＴＰリクエストをＳＳＬ通信にて再送させる表示情報であると言える。

【００７０】

一方、要求ページデータが特定ページデータでない場合には（図５：ステップＳ９０６：ＮＯ）、ＨＴＴＰリクエストがＳＳＬ通信にて受信されたか否かに拘わらず、ＷＥＢサーバ部Ｍ１０は、要求ページデータを送信ページデータとして選択する（ステップＳ９１２）。ステップＳ９１０またはステップＳ９１２の後、送信ページデータ選択処理は終了される。

【００７１】

以上説明したプリンタ１００のＷＥＢサーバ部Ｍ１０に対して、クライアント２００のＷＥＢブラウザ２０１を用いてアクセスした場合におけるブラウザ画面の表示内容について説明する。

【００７２】

図８は、特定ＷＥＢページとは異なるＷＥＢページの一例を示す図である。このＷＥＢページＰ４のページデータは、セキュリティを確保するべき特定情報を含み得ないページデータである。ＷＥＢページＰ４は、特定ページデータ（特定ＷＥＢページである特定情報登録ページＰ２（図６）のページデータ）を特定する相対パス形式のＵＲＬと対応付けられたリンク項目ＬＴ２を有している。ＷＥＢページＰ４は、特定ＷＥＢページではないので、ＷＥＢブラウザ２０１は、ＷＥＢページＰ４のページデータを、ＳＳＬ通信を用いているか否かに拘わらず、取得することができる。

【００７３】
ＷＥＢブラウザ２０１が、ＷＥＢページＰ４のページデータをＳＳＬ通信にて取得してＷＥＢページＰ４をブラウザ画面に表示している場合に、ユーザがＷＥＢページＰ４のリンク項目ＬＴ２を選択すると、ＷＥＢブラウザ２０１は、特定ページデータを要求するＨＴＴＰリクエストをＳＳＬ通信にてＷＥＢサーバ部Ｍ１０に送信する。この場合には、ＷＥＢブラウザ２０１は、ＳＳＬ通信にて特定ページデータを取得して、特定情報登録ページＰ２（図６）をブラウザ画面に表示することができる。
【００７４】
一方、ＷＥＢブラウザ２０１が、ＷＥＢページＰ４のページデータを非暗号化通信にて取得してＷＥＢページＰ４をブラウザ画面に表示している場合に、ユーザがＷＥＢページＰ４のリンク項目ＬＴ２を選択すると、ＷＥＢブラウザ２０１は、特定ページデータを要求するＨＴＴＰリクエストを非暗号化通信にてＷＥＢサーバ部Ｍ１０に送信する。この場合には、ＷＥＢブラウザ２０１は、非暗号化通信にて、警告ページＰ３（図７）のページデータを取得して、警告ページＰ３をブラウザ画面に表示することになる。ユーザは、警告ページＰ３のリクエスト再送用リンク項目ＬＴ１を選択することにより、ＷＥＢブラウザ２０１に、セキュリティが確保されたＳＳＬ通信にて特定ページデータを取得させることができる。すなわち、非暗号化通信にて特定ページデータを要求するＨＴＴＰリクエストがＷＥＢサーバ部Ｍ１０に送信された場合であっても、最終的には、特定ページデータは、ＳＳＬ通信にて送信される。
【００７５】
以上の説明から解るように本実施例におけるプリンタ１００によれば、ＷＥＢブラウザ２０１が、非暗号化通信にて、特定ページデータを要求した場合には、特定ページデータとは異なるデータである警告ページＰ３のページデータを送信する。すなわち、プリンタ１００は、非暗号化通信でのデータ要求とＳＳＬ通信でのデータ要求との両方を受け付けるにも拘わらず、非暗号化通信にて特定ページデータを送信することないので、特定ページデータに含まれ得る特定情報（例えば、個人情報）に対するセキュリティを向上することができる。
【００７６】
上記プリンタ１００は、プリインストール証明書格納領域１３１に格納されたプリインストール証明書を用いてＳＳＬ通信確立処理を行って通信を確立し得る。従って、ユーザインストール証明書格納領域１４２にユーザインストール証明書が格納されていなくても、特定ページデータ（特定情報）を送信することが可能となる。この結果、ユーザの負担を軽減することができる。また、ユーザインストール証明書格納領域１４２にユーザインストール証明書が格納されている場合には、これを優先して選択するので、ユーザの意図に沿った電子証明書を用いて、特定ページデータ（特定情報）を送信することが可能となる。
【００７７】
上記プリンタ１００は、ＳＳＬ通信確立処理（図２（ｂ））よりも前（具体的には、プリンタ１００の起動時）に、サーバ証明書の選択を実行し、その選択結果を示す情報を、選択結果格納領域１２１に格納する。従って、ＳＳＬ通信確立処理を、選択結果を示す情報に基づくサーバ証明書を用いて速やかに実行できる。
【００７８】
上記プリンタ１００は、上述した証明書選択処理を行うので、サーバ証明書の信頼性の違いや、ユーザの意図を考慮して適切なサーバ証明書を自動的に選択することができる。この結果、ユーザの負担を軽減することができる。
【００７９】
プリンタ１００は、受信したＨＴＴＰリクエストの宛先ポート番号を用いて、ＨＴＴＰリクエストがＳＳＬ通信にて受信されたか否かを容易に判断することができる。
【００８０】
上記実施例において、プリンタ１００は、特許請求の範囲における通信装置の一例であ

る。ユーザインストール証明書格納領域１４２は、特許請求の範囲における証明書格納部、第１証明書格納部の一例である。プリインストール証明書格納領域１３１は、特許請求の範囲における証明書格納部、第２証明書格納の一例である。選択結果格納領域１２１は、特許請求の範囲における選択結果格納部の一例である。

【００８１】

Ｂ．第２実施例：

【００８２】

第２実施例におけるプリンタの構成および動作について、第１実施例と異なる点について説明する。第２実施例におけるプリンタの、以下に説明する点以外の構成および動作は、第１実施例におけるプリンタ１００と同一である。

【００８３】

Ｂ－１．第２実施例におけるプリンタの構成

図１において破線で示すように、第２実施例におけるプリンタの証明書管理部Ｍ２０は、第１実施例におけるプリンタ１００の証明書管理部Ｍ２０の構成に加えて、証明書生成部Ｍ２３と証明書更新部Ｍ２４とを備えている。また、第２実施例におけるプリンタのＲＡＭ１２０は、第１実施例におけるプリンタ１００のＲＡＭ１２０の構成に加えて、自動生成証明書格納領域１２２を有している。第２実施例におけるプリンタのマスクＲＯＭ１３０は、プリインストール証明書格納領域１３１を有していない。すなわち、第２実施例におけるプリンタには、プリインストール証明書が格納されていない。

【００８４】

Ｂ－２．第２実施例における証明書選択処理

図９は、第２実施例における証明書選択処理の処理ステップを示すフローチャートである。第２実施例における証明書選択処理が、第１実施例における証明書選択処理（図３）と異なる点は、第１実施例における証明書選択処理のステップＳ５０６に代えて、ステップＳ５０６ａとステップＳ５０７ａ（図９）を備える点である。他のステップの内容は、第１実施例における証明書選択処理（図３）における同名のステップと同一である。

【００８５】

ステップＳ５０６ａでは、証明書生成部Ｍ２３は、サーバ証明書を自動生成して、ＲＡＭ１２０の自動生成証明書格納領域１２２に格納する。以下では、自動生成されたサーバ証明書を自動生成サーバ証明書とも呼ぶ。証明書生成部Ｍ２３が自動生成するサーバ証明書は、第１実施例におけるプリインストール証明書と同等のサーバ証明書である。ただし、証明書生成部Ｍ２３が自動生成するサーバ証明書は、有効期限がプリインストール証明書と比較して短い（例えば、１０日）。

【００８６】

ステップＳ５０７ａでは、証明書選択部Ｍ２１は、ステップＳ５０６ａにて自動生成されたサーバ証明書を使用するサーバ証明書として選択する。

【００８７】

Ｂ－３．証明書更新処理

図１０は、証明書更新処理の処理ステップを示すフローチャートである。証明書更新処理は、上述した証明書生成部Ｍ２３によって自動生成サーバ証明書を更新する処理である。証明書更新処理は、証明書更新部Ｍ２４によって、所定間隔（例えば、１２時間）で定期的に実行される。

【００８８】

証明書更新処理が開始されると、証明書更新部Ｍ２４は、自動生成サーバ証明書の有効期限を取得する（ステップＳ１０１０）。証明書更新部Ｍ２４は、取得した有効期限の残期間、すなわち、現在から有効期限までの期間が、所定期間（例えば、１日）以下であるか否かを判断する（ステップＳ１０２０）。証明書更新部Ｍ２４は、残期間が所定期間以下であると判断すると（ステップＳ１０２０：ＹＥＳ）、ステップＳ５６０ａ（図９）の処理のごとくサーバ証明書を新たに自動生成し、これを自動生成証明書格納領域１２２（ＲＡＭ１２０）に格納された既存の自動生成サーバ証明書に上書きすることで、自動生成

サーバ証明書を更新する（ステップＳ３０）。その後、証明書更新処理を終了する。このとき、サーバ証明書と関連付けられる秘密鍵も同時に更新される。証明書更新部Ｍ２４は、残期間が所定期間よりも長いと判断すると（ステップＳ１０２０：ＮＯ）、証明書更新処理を終了する。

【００８９】

上記実施例において、自動生成証明書格納領域１２２は、特許請求の範囲における証明書格納部、第２証明書格納部の一例である。

【００９０】

第２実施例におけるプリンタによれば、ユーザインストール証明書がユーザインストール証明書格納領域１４２に格納されていない場合に、サーバ証明書を自動的に生成するので、サーバ証明書がないために、ＳＳＬ通信が行えない事態を避けることができる。

【００９１】

さらに、自動生成されたサーバ証明書の自動更新を行うので、自動生成された電子証明書の有効期限が切れたために、ＳＳＬ通信が行えない事態を避けることができる。例えば、長時間に亘ってプリンタ１００の電源が投入されている場合などに有効である。

【００９２】

さらに、プリインストール証明書が格納されないので、プリンタ１００の不揮発性の記憶領域の必要容量、例えば、マスクＲＯＭ１３０の必要容量を抑制することができる。

【００９３】

Ｃ．変形例：

なお、上記実施例における構成要素の中の、独立クレームでクレームされた要素以外の要素は、付加的な要素であり、適宜省略可能である。また、この発明は上記の実施例や実施形態に限られるものではなく、その要旨を逸脱しない範囲において種々の態様において実施することが可能であり、例えば次のような変形も可能である。

【００９４】

（１）上記実施例におけるプリンタ１００のＷＥＢサーバ部Ｍ１０は、いわゆるＨＴＴＰ通信とＨＴＴＰＳ通信とに対応しているが、これに限らず、セキュリティレベルの異なる他の２種類のプロトコルによりデータ要求を受け付けることができる場合であれば、本発明を適用することができる。例えば、セキュリティレベルの異なる２種類のプロトコルの組み合わせとしては、ｆｔｐ（File Transfer Protocol）とｆｔｐｓ（File Transfer Protocol over SSL）の組み合わせ、ＳＮＭＰｖ１（Simple Network Management Protocol version 1）とＳＮＭＰｖ３の組み合わせ、ｔｅｌｎｅｔと、ｔｅｌｎｅｔ／ＳＳＨ（Secure SHell）の組み合わせなどがある。

【００９５】

（２）上記実施例におけるＳＳＬ通信は、電子証明書を用いて接続処理を経て確立される暗号化通信であるが、これに代えて、電子証明書を用いることなく、通信を行う双方の装置に共通鍵を予め格納させておき、その共通鍵を用いて行う暗号化通信が採用されても良い。

【００９６】

（３）上記実施例のプリンタ１００では、信頼性の異なる複数種類のサーバ証明書を格納可能であるが、１種類のサーバ証明書のみが格納可能であっても良い。

【００９７】

（４）上記実施例のプリンタ１００では、証明書選択処理をプリンタ１００の起動時に実行しているが、ＳＳＬ通信要求を受信してから証明書選択処理を実行しても良い。

【００９８】

（５）上記実施例のプリンタ１００では、受信プロトコル判断部Ｍ１３は、ＨＴＴＰリクエストとともに送信される情報である、ＨＴＴＰリクエストを格納するＴＣＰパケットのヘッダに記述された宛先ポート番号を用いて、ＨＴＴＰリクエストがＳＳＬ通信にて受信されたか否かを判断している。これに代えて、ＨＴＴＰリクエストに含まれる情報、例えば、ＨＴＴＰリクエストのリファラ（referrer）欄に記述されたＵＲＬの<scheme>を用い

て判断しても良い。

【００９９】

（６）上記実施例では、ＷＥＢサーバ部Ｍ１０の機能を有する通信装置としてプリンタが採用されているが、これに代えて、他の通信装置が採用されても良い。他の通信装置としては、スキャナ、ファクシミリ、複数の機能（印刷、スキャナ等）を有する複合機などの画像処理装置を採用可能である。あるいは、他の通信装置としては、パーソナルコンピュータ、ルータ、スイッチなどを採用可能である。

【０１００】

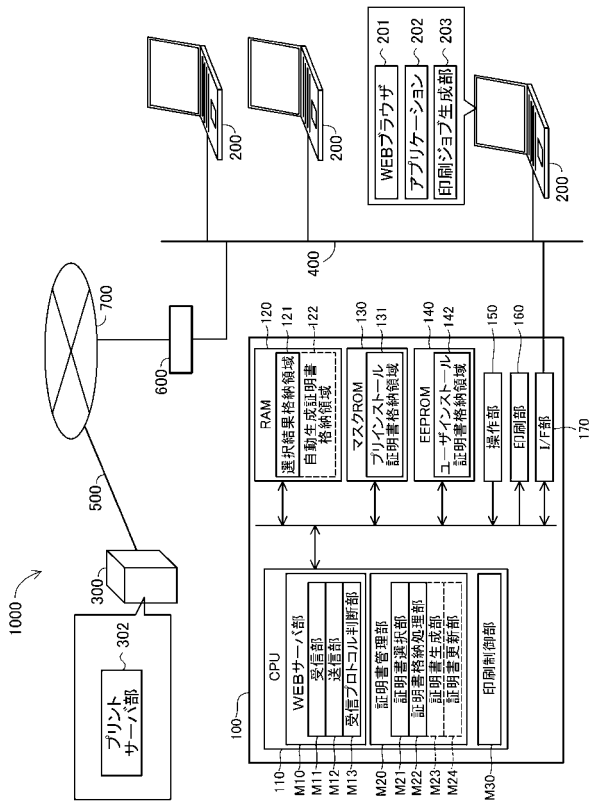
（７）上記実施例において、ハードウェアによって実現されていた構成の一部をソフトウェアに置き換えるようにしてもよく、逆に、ソフトウェアによって実現されていた構成の一部をハードウェアに置き換えるようにしてもよい。

【符号の説明】

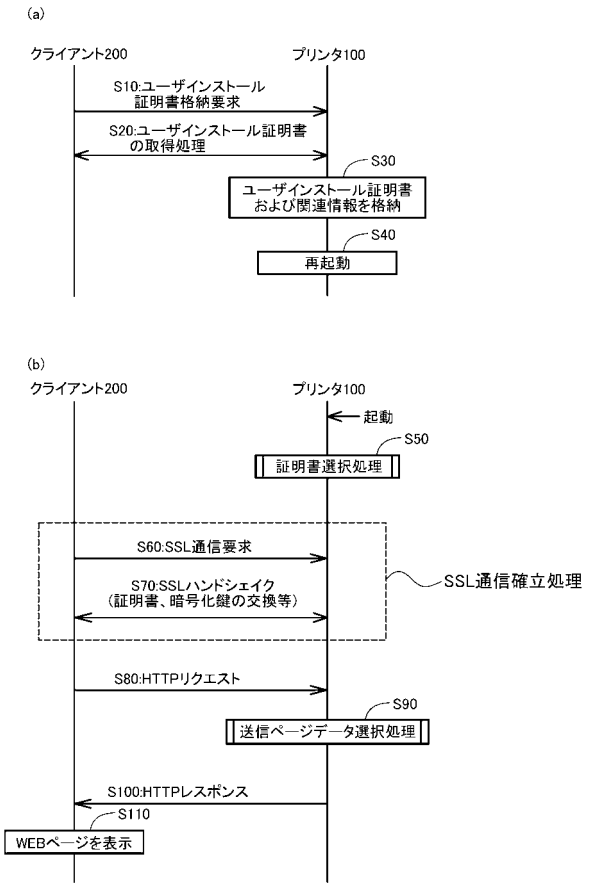
【０１０１】

１００...プリンタ、１１０...ＣＰＵ、１２０...ＲＡＭ、１３０...マスクＲＯＭ、１５０...操作部、１６０...印刷部、２００...クライアント、２０１...ＷＥＢブラウザ、２０２...アプリケーション、２０３...印刷ジョブ生成部、３００...サーバ、Ｍ１０...ＷＥＢサーバ部、Ｍ２０...証明書管理部、Ｍ３０...印刷制御部

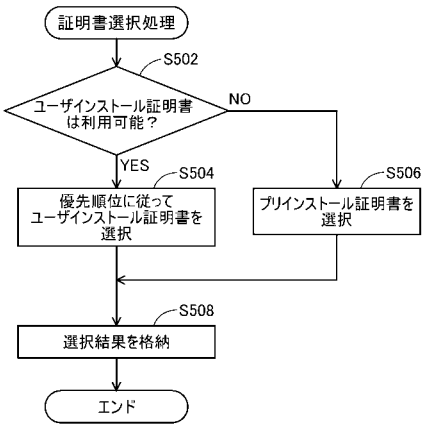
【図１】



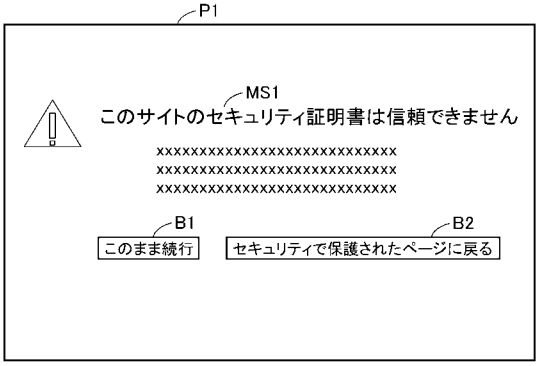
【図２】



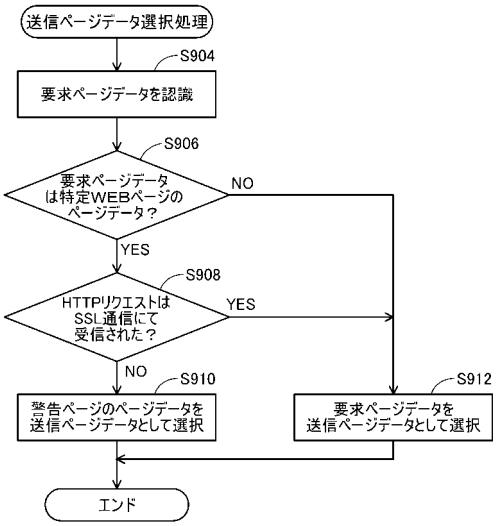
【図３】



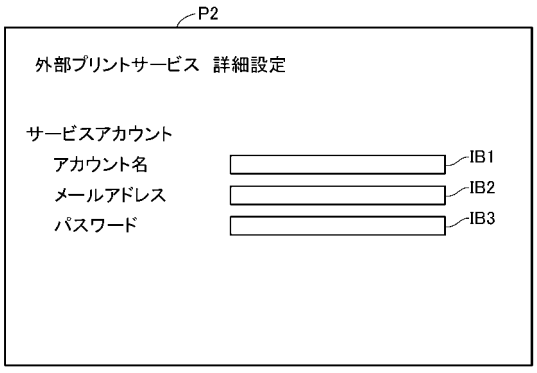
【図４】



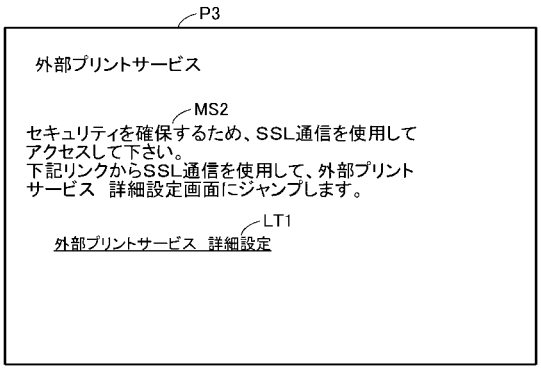
【図５】



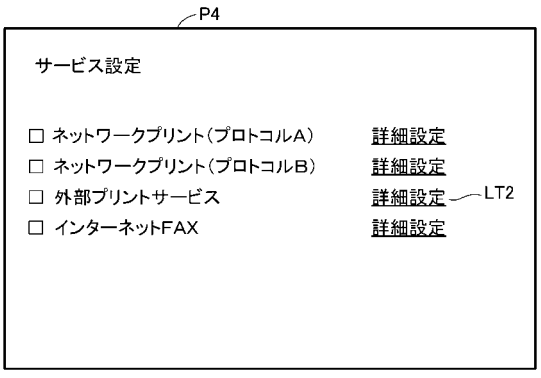
【図６】



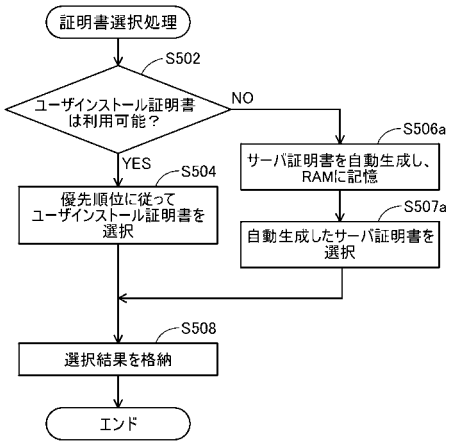
【図７】



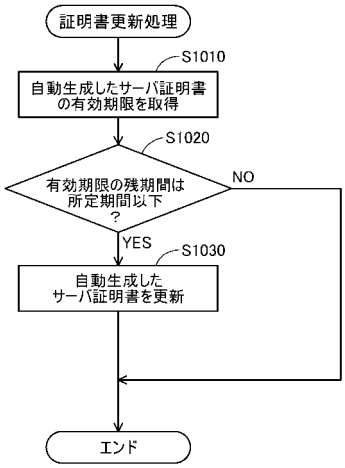
【図８】



【図９】


証明書選択処理
S502
ユーザインストール証明書は利用可能？
NO
YES
S504
優先順位に従ってユーザインストール証明書を選択
S506a
サーバ証明書を自動生成し、RAMに記憶
S507a
自動生成したサーバ証明書を選択
S508
選択結果を格納
エンド

【図１０】


証明書更新処理
S1010
自動生成したサーバ証明書の有効期限を取得
S1020
有効期限の残期間は所定期間以下？
NO
YES
S1030
自動生成したサーバ証明書を更新
エンド

フロントページの続き

(51)Int.Cl.			FI		
H04N	***1/00***	***(2006.01)***	H04N	1/00	107Z
H04N	***1/44***	***(2006.01)***	H04N	1/44	

(72)発明者　矢田　裕紀
愛知県名古屋市瑞穂区苗代町１５番１号　ブラザー工業株式会社内

審査官　平井　誠

(56)参考文献　特開２００７－２１３３９７（ＪＰ，Ａ）
特開２００６－１６５６７８（ＪＰ，Ａ）
特開２００９－２００５６５（ＪＰ，Ａ）
特開２００２－２１５８２６（ＪＰ，Ａ）
特開２００２－２０７６３６（ＪＰ，Ａ）
特開２００８－０９０４５８（ＪＰ，Ａ）
特開２００５－１３０４５７（ＪＰ，Ａ）
特開２００５－１３０４５９（ＪＰ，Ａ）
特開２００６－０１４１８２（ＪＰ，Ａ）
特開２００７－１８１１３９（ＪＰ，Ａ）
米国特許出願公開第２０１２／０２３３７０２（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１