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

特許第4597551号
(P4597551)

(45)発行日　平成22年12月15日(2010.12.15)　(24)登録日　平成22年10月1日(2010.10.1)

(51)Int.Cl.		F I		
G06F 11/00	(2006.01)	G06F	9/06	630A
G06F 21/22	(2006.01)	G06F	9/06	660G
G06F 13/00	(2006.01)	G06F	13/00	530B
H04L 9/32	(2006.01)	H04L	9/00	673A

請求項の数 19　(全 38 頁)

(21)出願番号　特願2004-58270(P2004-58270)
(22)出願日　平成16年3月2日(2004.3.2)
(65)公開番号　特開2004-318838(P2004-318838A)
(43)公開日　平成16年11月11日(2004.11.11)
審査請求日　平成18年11月9日(2006.11.9)
(31)優先権主張番号　特願2003-90827(P2003-90827)
(32)優先日　平成15年3月28日(2003.3.28)
(33)優先権主張国　日本国(JP)
(31)優先権主張番号　特願2003-90886(P2003-90886)
(32)優先日　平成15年3月28日(2003.3.28)
(33)優先権主張国　日本国(JP)

(73)特許権者　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(74)代理人　100123881
弁理士　大澤　豊
(74)代理人　100080931
弁理士　大澤　敬
(72)発明者　奈須　政巳
東京都大田区中馬込１丁目３番６号　株式会社リコー内

審査官　稲垣　良一

最終頁に続く

(54)【発明の名称】ソフトウェア更新装置、ソフトウェア更新システム、ソフトウェア更新方法及びプログラム

(57)【特許請求の範囲】

【請求項１】

ネットワークを介して被更新装置と通信可能なソフトウェア更新装置であって、

前記被更新装置のソフトウェアを更新する場合に更新用認証情報を生成し、これを暗号化された第１の通信経路で前記被更新装置に送信して記憶するよう要求する認証情報設定手段と、

前記被更新装置に前記更新用認証情報を送信し、該認証情報による認証処理を要求する認証要求手段と、

該認証処理が成功した場合に更新用ソフトウェアを前記第１の通信経路よりも処理負荷の小さい第２の通信経路で前記被更新装置に送信する送信手段と、

前記被更新装置との通信に基づき、前記被更新装置においてソフトウェアの前記更新用ソフトウェアへの更新が成功したと判断した場合に、前記更新用認証情報に上書きさせるための消去用情報を生成し、これを前記第１の通信経路で前記被更新装置に送信して前記更新用認証情報に上書きして記憶するよう要求する認証情報消去手段とを設けたことを特徴とするソフトウェア更新装置。

【請求項２】

請求項１記載のソフトウェア更新装置であって、

前記被更新装置のソフトウェアの更新を、外部からのソフトウェア更新要求に応じて行い、その結果を該更新要求の要求元に返す手段を設けたことを特徴とするソフトウェア更新装置。

【請求項３】
請求項１又は２記載のソフトウェア更新装置であって、
前記被更新装置から起動した旨を示す起動通知を受け付ける手段と、
前記更新用ソフトウェアの送信後に前記被更新装置から前記起動通知を受け付けた場合に該被更新装置からソフトウェアのバージョン情報を取得し、送信した更新用ソフトウェアのバージョン情報と比較して更新の成否を確認する手段とを設けたことを特徴とするソフトウェア更新装置。
【請求項４】
請求項１乃至３のいずれか一項記載のソフトウェア更新装置であって、
前記第１の通信経路はＳＳＬによる通信を行う通信経路であり、
前記第２の通信経路はＦＴＰによる通信を行う通信経路であることを特徴とするソフトウェア更新装置。
【請求項５】
請求項１乃至３のいずれか一項記載のソフトウェア更新装置であって、
前記第１の通信経路は、送信すべきデータを暗号化して送信する通信経路であり、
前記第２の通信経路は、送信すべきデータを暗号化しないで送信する通信経路であることを特徴とするソフトウェア更新装置。
【請求項６】
ネットワークを介して互いに通信可能なソフトウェア更新装置と被更新装置とによって構成されるソフトウェア更新システムであって、
前記ソフトウェア更新装置に、
前記被更新装置のソフトウェアを更新する場合に更新用認証情報を生成し、これを暗号化された第１の通信経路で前記被更新装置に送信して記憶するよう要求する認証情報設定手段と、
前記被更新装置に前記更新用認証情報を送信し、該認証情報による認証処理を要求する認証要求手段と、
該認証処理が成功した場合に更新用ソフトウェアを前記第１の通信経路よりも処理負荷の小さい第２の通信経路で前記被更新装置に送信する送信手段と、
前記被更新装置との通信に基づき、前記被更新装置においてソフトウェアの前記更新用ソフトウェアへの更新が成功したと判断した場合に、前記更新用認証情報に上書きさせるための消去用情報を生成し、これを前記第１の通信経路で前記被更新装置に送信して前記更新用認証情報に上書きして記憶するよう要求する認証情報消去手段とを設け、
前記被更新装置に、
前記更新用認証情報を記憶するよう要求された場合にこれを記憶する記憶手段と、
前記認証処理を要求された場合に、受信した更新用認証情報と前記記憶手段に記憶している更新用認証情報とを用いて認証処理を行って結果を返す認証手段と、
該認証処理が成功した場合に前記更新用ソフトウェアを受信し、自機のソフトウェアを該更新用ソフトウェアに更新する更新手段と、
前記更新装置と通信して、該更新装置に前記更新手段によるソフトウェアの更新が成功したことを確認させる手段と、
前記消去用情報を記憶するよう要求された場合にこれを前記更新用認証情報に上書きして記憶する手段とを設けたことを特徴とするソフトウェア更新システム。
【請求項７】
請求項６記載のソフトウェア更新システムであって、
前記被更新装置に、
前記ソフトウェアの更新が成功したことを確認させる手段として、
前記更新手段によるソフトウェアの更新後に自機を再起動する手段と、
起動時に前記ソフトウェア更新装置にその旨を示す起動通知を送信する手段と、
前記ソフトウェア更新装置からの要求に応じて該装置にソフトウェアのバージョン情報を送信する手段とを設け、

前記ソフトウェア更新装置に、
前記更新用ソフトウェアの送信後に前記被更新装置から前記起動通知を受け付けた場合に該被更新装置に対してソフトウェアのバージョン情報の送信を要求して該バージョン情報を取得し、送信した更新用ソフトウェアのバージョン情報と比較して更新の成否を確認する手段を設けたことを特徴とするソフトウェア更新システム。
【請求項８】
請求項６又は７記載のソフトウェア更新システムであって、
前記第１の通信経路はＳＳＬによる通信を行う通信経路であり、
前記第２の通信経路はＦＴＰによる通信を行う通信経路であることを特徴とするソフトウェア更新システム。
【請求項９】
請求項６又は７記載のソフトウェア更新システムであって、
前記第１の通信経路は、送信すべきデータを暗号化して送信する通信経路であり、
前記第２の通信経路は、送信すべきデータを暗号化しないで送信する通信経路であることを特徴とするソフトウェア更新システム。
【請求項１０】
ソフトウェア更新装置によって、ネットワークを介して通信可能な被更新装置のソフトウェアを更新するソフトウェア更新方法であって、
前記被更新装置のソフトウェアを更新する場合に更新用認証情報を生成し、これを暗号化された第１の通信経路で前記被更新装置に送信して記憶させ、
前記被更新装置に前記更新用認証情報を送信して該認証情報による認証処理を行わせ、
該認証処理が成功した場合に更新用ソフトウェアを前記第１の通信経路よりも処理負荷の小さい第２の通信経路で前記被更新装置に送信してソフトウェアの更新を行わせ、
前記被更新装置との通信に基づき、前記被更新装置においてソフトウェアの前記更新用ソフトウェアへの更新が成功したと判断した場合に、前記更新用認証情報に上書きさせるための消去用情報を生成し、これを前記第１の通信経路で前記被更新装置に送信して前記更新用認証情報に上書きして記憶させることを特徴とするソフトウェア更新方法。
【請求項１１】
請求項１０記載のソフトウェア更新方法であって、
前記被更新装置のソフトウェアの更新を、外部からのソフトウェア更新要求に応じて行い、その結果を該更新要求の要求元に返すことを特徴とするソフトウェア更新方法。
【請求項１２】
請求項１０又は１１記載のソフトウェア更新方法であって、
前記被更新装置から起動した旨を示す起動通知を受け付け、
前記更新用ソフトウェアの送信後に前記被更新装置から前記起動通知を受け付けた場合に該被更新装置からソフトウェアのバージョン情報を取得し、送信した更新用ソフトウェアのバージョン情報と比較して更新の成否を確認することを特徴とするソフトウェア更新方法。
【請求項１３】
請求項１０乃至１２のいずれか一項記載のソフトウェア更新方法であって、
前記第１の通信経路はＳＳＬによる通信を行う通信経路であり、
前記第２の通信経路はＦＴＰによる通信を行う通信経路であることを特徴とするソフトウェア更新方法。
【請求項１４】
請求項１０乃至１２のいずれか一項記載のソフトウェア更新方法であって、
前記第１の通信経路は、送信すべきデータを暗号化して送信する通信経路であり、
前記第２の通信経路は、送信すべきデータを暗号化しないで送信する通信経路であることを特徴とするソフトウェア更新方法。
【請求項１５】
ネットワークを介して被更新装置と通信可能なソフトウェア更新装置を制御するコンピ

ュータを、
前記被更新装置のソフトウェアを更新する場合に更新用認証情報を生成し、これを暗号化された第１の通信経路で前記被更新装置に送信して記憶するよう要求する認証情報設定手段と、
前記被更新装置に前記更新用認証情報を送信し、該認証情報による認証処理を要求する認証要求手段と、
該認証処理が成功した場合に更新用ソフトウェアを前記第１の通信経路よりも処理負荷の小さい第２の通信経路で前記被更新装置に送信する送信手段と、
前記被更新装置との通信に基づき、前記被更新装置においてソフトウェアの前記更新用ソフトウェアへの更新が成功したと判断した場合に、前記更新用認証情報に上書きさせるための消去用情報を生成し、これを前記第１の通信経路で前記被更新装置に送信して前記更新用認証情報に上書きして記憶するよう要求する認証情報消去手段として機能させるためのプログラム。
【請求項１６】
請求項１５記載のプログラムであって、
前記コンピュータを、前記被更新装置のソフトウェアの更新を外部からのソフトウェア更新要求に応じて行い、その結果を該更新要求の要求元に返す手段として機能させるためのプログラムをさらに含むことを特徴とするプログラム。
【請求項１７】
請求項１５又は１６記載のプログラムであって、
前記コンピュータを、
前記被更新装置から起動した旨を示す起動通知を受け付ける手段と、
前記更新用ソフトウェアの送信後に前記被更新装置から前記起動通知を受け付けた場合に該被更新装置からソフトウェアのバージョン情報を取得し、送信した更新用ソフトウェアのバージョン情報と比較して更新の成否を確認する手段として機能させるためのプログラムをさらに含むことを特徴とするプログラム。
【請求項１８】
請求項１５乃至１７のいずれか一項記載のプログラムであって、
前記第１の通信経路はＳＳＬによる通信を行う通信経路であり、
前記第２の通信経路はＦＴＰによる通信を行う通信経路であることを特徴とするプログラム。
【請求項１９】
請求項１５乃至１７のいずれか一項記載のプログラムであって、
前記第１の通信経路は、送信すべきデータを暗号化して送信する通信経路であり、
前記第２の通信経路は、送信すべきデータを暗号化しないで送信する通信経路であることを特徴とするプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、ネットワークを介して通信可能な被更新装置のソフトウェアを更新するソフトウェア更新装置、このようなソフトウェア更新装置と被更新装置とによって構成されるソフトウェア更新システム、上記のソフトウェア更新装置によるソフトウェア更新方法、コンピュータを上記のソフトウェア更新装置として機能させるためのプログラムに関する。そして、更新すべきソフトウェアとしては、例えばファームウェアやアプリケーションプログラム等が考えられる。
【背景技術】
【０００２】
従来から、プリンタ，ＦＡＸ装置，コピー機，スキャナ，デジタル複合機等の画像処理装置において、ハードウェアの基本的な制御を行うためのソフトウェアであるファームウェアを更新可能とすることが行われている。そして、特許文献１には、サービスセンタが

画像形成装置からファームウェアのバージョン情報を取得し、バージョンが古く、更新が必要だと判断した場合に通信コントロール装置を介して画像形成装置にファームウェアを送信してファームウェアの更新を行わせる画像形成装置管理システムが記載されている。

【特許文献１】特開２００２－２８８０６６号公報

【０００３】

ところで、特許文献１に記載の画像形成装置管理システムは、基本的にサービスセンタと通信コントロール装置との間の通信は公衆回線（ＰＳＴＮ）や専用回線、通信コントロール装置と画像形成装置との間の通信はＲＳ－４８５規格の通信経路を用いて行うものである。

これに対し、近年では、汎用性や拡張性を重視し、管理装置と被管理装置との間の通信を、インターネットやローカルエリアネットワーク（ＬＡＮ）等のネットワークを介して行う管理システムが提案されている。そして、このような管理システムにおいても、特許文献１の場合と同様に、管理装置から被管理装置にファームウェアを送信してファームウェアの更新を行わせることが考えられる。

【０００４】

この場合の処理として考えられるのは、例えば図２６のシーケンス図に示す処理である。なお、この場合においては、管理装置はファームウェア更新装置（ファーム更新装置）、被管理装置はファームウェア（以下単に「ファーム」ともいう）の被更新装置であると考えられる。

図２６に示す処理においては、ファーム更新装置９１と被更新装置９２とはＦＴＰ（File Transfer Protocol）を用いて通信を行うが、予めファーム更新装置９１にＦＴＰのためのＩＤとパスワードを設定しておき、これらをファーム更新装置９１と被更新装置９２の双方に記憶させておくものとする。

【０００５】

この処理において、まずファーム更新装置９１が、一定時間毎あるいは所定のイベントが発生した場合等に、バージョン情報取得処理を実行し、被更新装置９２にＩＤとパスワードを送信してＦＴＰによる接続を要求する。ＩＤとパスワードはＦＴＰの規格に従ったものであり、接続を要求された被更新装置９２はこれらによってファーム更新装置９１を認証することができる。そして、このＩＤとパスワードを記憶しているものと比較し、一致すれば認証成功として接続を確立する（Ｓ１１）。ＩＤ又はパスワードが一致しなかった場合には接続は確立されず、エラーとなって処理は終了する。

接続が確立されると、ファーム更新装置９１は被更新装置９２にファームウェアのバージョン情報を送信するよう要求し、被更新装置９２がこれに応答してファームのバージョン情報を送信する（Ｓ１２）。その後、ファーム更新装置９１は被更新装置９２との接続を切断する（Ｓ１３）。以上がバージョン情報取得処理である。

【０００６】

次に、ファーム更新装置９１は取得したファームのバージョン情報をもとに更新の要否を判断する。既に最新のバージョンのファームが被更新装置９２にインストールされていれば、更新は不要である。ここで更新不要と判断すれば処理を終了し、その後トリガが発生した場合に再度バージョン情報取得処理を行うことになる。しかし、更新が必要と判断すれば（Ｓ１４）、次のファーム送信処理を実行する。

この処理では、まずステップＳ１１の場合と同様に被更新装置９２にＩＤとパスワードを送信し、接続を確立する（Ｓ１５）。そして、更新用のファームを被更新装置９２に送信する（Ｓ１６）。被更新装置９２側では、これを受信すると、ファームの更新処理を行い（Ｓ１７）、更新が完了すると自身をリセットし、再起動して新たなファームを有効にする（Ｓ１８）。また、被更新装置９２のリセットにより、ＦＴＰ接続は切断される。以上がファーム送信処理である。

以上の処理によって、必要な場合に被更新装置９２のファームを更新することができる。そして、再度バージョン情報取得処理やファーム送信処理を行う場合も、シーケンス図の続きに同じステップ番号で示したように、同じパスワードを用いて同様な処理を行う。

【発明の開示】
【発明が解決しようとする課題】
【０００７】
しかし、ＦＴＰによる通信は、データを暗号化しないため、ＩＤやパスワードも平文のままネットワーク上を転送されることになる。従って、図２７に示すように、ファーム更新装置９１と被更新装置９２との間の通信経路をパケットモニタ９３によってモニタリングすれば、転送されるデータパケットからＩＤやパスワードを取り出すことができてしまう。そして、これを悪用すれば、第３者がファーム更新装置９１になりすまして被更新装置９２にアクセスし、ファームを不正なものに更新させることも可能になってしまう。
従って、図２６に示したようにＦＴＰによって送信したパスワードを何度も繰り返して用いることは、安全面で問題があると言える。
以上のような点は、更新対象のソフトウェアがファームウェアでなく、それ以外の例えばアプリケーションプログラムであっても、同様に問題となる。
【０００８】
なお、特許文献１に記載のようにＰＳＴＮ，専用回線，ＲＳ－４８５のような通信経路を用いた場合には、独自の通信プロトコルを用いて通信することになるため、各装置をハード的に解析し、プロトコルを知得しなければ通信をモニタリングすることができない。従って、モニタリングが困難であるので、このような安全面の問題は発生せず、そのためこの問題を解決する手段についても特に記載されていない。
しかし、ＴＣＰ／ＩＰ（Transmission Control Protocol/Internet Protocol）等のインターネットの標準技術を利用してソフトウェア更新システムを構築しようとする場合には、このような安全面の問題の解決は重要な課題となる。
【０００９】
ところで、上記の問題を解消するためには、通信内容を暗号化する通信プロトコルとして例えばＳＳＬ（Secure Socket Layer）と呼ばれるプロトコルが開発されており、広く用いられている。このプロトコルを用いて通信を行うことにより、公開鍵暗号方式と共通鍵暗号方式とを組み合わせ、通信相手の認証を行うと共に、情報の暗号化により改竄及び盗聴の防止を図ることができる。
このようなＳＳＬによる通信を行えば、ファーム更新装置９１と被更新装置９２とが安全に共通鍵を交換することができ、通信を安全に行うことができる。しかしながら、ＳＳＬのように暗号化処理を含む通信方式は、認証やデータ転送に係る処理負荷が、ＦＴＰのように暗号化を行わない通信方式よりも大きくなってしまう。
特に、ソフトウェアのように大きなサイズのデータを送信する場合には、この影響が大きい。またもちろん、ＦＴＰとＳＳＬ以外のプロトコルを使用する場合でも、処理負荷の大小の問題は同様に存在する。
【００１０】
この発明は、これらの問題を解決し、ネットワークを介して通信可能な被更新装置のソフトウェアをソフトウェア更新装置によって更新する場合において、高い安全性を確保しながら更新処理の負荷を低減することを目的とする。
【課題を解決するための手段】
【００１１】
上記の目的を達成するため、この発明は、ネットワークを介して被更新装置と通信可能なソフトウェア更新装置において、上記被更新装置のソフトウェアを更新する場合に更新用認証情報を生成し、これを暗号化された第１の通信経路で上記被更新装置に送信して記憶するよう要求する認証情報設定手段と、上記被更新装置に上記更新用認証情報を送信し、その認証情報による認証処理を要求する認証要求手段と、その認証処理が成功した場合に更新用ソフトウェアを上記第１の通信経路よりも処理負荷の小さい第２の通信経路で上記被更新装置に送信する送信手段と、上記被更新装置との通信に基づき、上記被更新装置においてソフトウェアの上記更新用ソフトウェアへの更新が成功したと判断した場合に、上記更新用認証情報に上書きさせるための消去用情報を生成し、これを上記第１の通信経

路で上記被更新装置に送信して上記更新用認証情報に上書きして記憶するよう要求する認証情報消去手段とを設けたものである。

【００１２】

このようなソフトウェア更新装置において、上記被更新装置のソフトウェアの更新を、外部からのソフトウェア更新要求に応じて行い、その結果をその更新要求の要求元に返す手段を設けるとよい。

【００１３】

さらに、上記被更新装置から起動した旨を示す起動通知を受け付ける手段と、上記更新用ソフトウェアの送信後に上記被更新装置から上記起動通知を受け付けた場合にその被更新装置からソフトウェアのバージョン情報を取得し、送信した更新用ソフトウェアのバージョン情報と比較して更新の成否を確認する手段とを設けるとよい。

さらにまた、上記第１の通信経路をＳＳＬによる通信を行う通信経路とし、上記第２の通信経路をＦＴＰによる通信を行う通信経路とするとよい。

あるいは、上記第１の通信経路を、送信すべきデータを暗号化して送信する通信経路とし、上記第２の通信経路を、送信すべきデータを暗号化しないで送信する通信経路としてもよい。

【００１４】

また、この発明のソフトウェア更新システムは、ネットワークを介して互いに通信可能なソフトウェア更新装置と被更新装置とによって構成されるソフトウェア更新システムにおいて、上記ソフトウェア更新装置に、上記被更新装置のソフトウェアを更新する場合に更新用認証情報を生成し、これを暗号化された第１の通信経路で上記被更新装置に送信して記憶するよう要求する認証情報設定手段と、上記被更新装置に上記更新用認証情報を送信し、その認証情報による認証処理を要求する認証要求手段と、その認証処理が成功した場合に更新用ソフトウェアを上記第１の通信経路よりも処理負荷の小さい第２の通信経路で上記被更新装置に送信する送信手段と、上記被更新装置との通信に基づき、上記被更新装置においてソフトウェアの上記更新用ソフトウェアへの更新が成功したと判断した場合に、上記更新用認証情報に上書きさせるための消去用情報を生成し、これを上記第１の通信経路で上記被更新装置に送信して上記更新用認証情報に上書きして記憶するよう要求する認証情報消去手段とを設け、上記被更新装置に、上記更新用認証情報を記憶するよう要求された場合にこれを記憶する記憶手段と、上記認証処理を要求された場合に、受信した更新用認証情報と上記記憶手段に記憶している更新用認証情報とを用いて認証処理を行って結果を返す認証手段と、その認証処理が成功した場合に上記更新用ソフトウェアを受信し、自機のソフトウェアをその更新用ソフトウェアに更新する更新手段と、上記更新装置と通信して、その更新装置に上記更新手段によるソフトウェアの更新が成功したことを確認させる手段と、上記消去用情報を記憶するよう要求された場合にこれを上記更新用認証情報に上書きして記憶する手段とを設けたものである。

【００１６】

このようなソフトウェア更新システムにおいて、上記被更新装置に、上記ソフトウェアの更新が成功したことを確認させる手段として、上記更新手段によるソフトウェアの更新後に自機を再起動する手段と、起動時に上記ソフトウェア更新装置にその旨を示す起動通知を送信する手段と、上記ソフトウェア更新装置からの要求に応じてその装置にソフトウェアのバージョン情報を送信する手段とを設け、上記ソフトウェア更新装置に、上記更新用ソフトウェアの送信後に上記被更新装置から上記起動通知を受け付けた場合にその被更新装置に対してソフトウェアのバージョン情報の送信を要求してそのバージョン情報を取得し、送信した更新用ソフトウェアのバージョン情報と比較して更新の成否を確認する手段を設けるとよい。

さらにまた、上記第１の通信経路をＳＳＬによる通信を行う通信経路とし、上記第２の通信経路をＦＴＰによる通信を行う通信経路とするとよい。

あるいは、上記第１の通信経路を、送信すべきデータを暗号化して送信する通信経路とし、上記第２の通信経路を、送信すべきデータを暗号化しないで送信する通信経路として

もよい。

【００１７】

また、この発明のソフトウェア更新方法は、ソフトウェア更新装置によって、ネットワークを介して通信可能な被更新装置のソフトウェアを更新するソフトウェア更新方法において、上記被更新装置のソフトウェアを更新する場合に更新用認証情報を生成し、これを暗号化された第１の通信経路で上記被更新装置に送信して記憶させ、上記被更新装置に上記更新用認証情報を送信してその認証情報による認証処理を行わせ、その認証処理が成功した場合に更新用ソフトウェアを上記第１の通信経路よりも処理負荷の小さい第２の通信経路で上記被更新装置に送信してソフトウェアの更新を行わせ、上記被更新装置との通信に基づき、上記被更新装置においてソフトウェアの上記更新用ソフトウェアへの更新が成功したと判断した場合に、上記更新用認証情報に上書きさせるための消去用情報を生成し、これを上記第１の通信経路で上記被更新装置に送信して上記更新用認証情報に上書きして記憶させるようにしたものである。

【００１８】

このようなソフトウェア更新方法において、上記被更新装置のソフトウェアの更新を、外部からのソフトウェア更新要求に応じて行い、その結果をその更新要求の要求元に返すようにするとよい。

【００１９】

さらに、上記被更新装置から起動した旨を示す起動通知を受け付け、上記更新用ソフトウェアの送信後に上記被更新装置から上記起動通知を受け付けた場合にその被更新装置からソフトウェアのバージョン情報を取得し、送信した更新用ソフトウェアのバージョン情報と比較して更新の成否を確認するようにするとよい。

さらにまた、上記第１の通信経路がＳＳＬによる通信を行う通信経路であり、上記第２の通信経路がＦＴＰによる通信を行う通信経路であるとよい。

あるいは、上記第１の通信経路を、送信すべきデータを暗号化して送信する通信経路とし、上記第２の通信経路を、送信すべきデータを暗号化しないで送信する通信経路としてもよい。

【００２０】

また、この発明のプログラムは、ネットワークを介して被更新装置と通信可能なソフトウェア更新装置を制御するコンピュータを、上記被更新装置のソフトウェアを更新する場合に更新用認証情報を生成し、これを暗号化された第１の通信経路で上記被更新装置に送信して記憶するよう要求する認証情報設定手段と、上記被更新装置に上記更新用認証情報を送信し、その認証情報による認証処理を要求する認証要求手段と、その認証処理が成功した場合に更新用ソフトウェアを上記第１の通信経路よりも処理負荷の小さい第２の通信経路で上記被更新装置に送信する送信手段と、上記被更新装置との通信に基づき、上記被更新装置においてソフトウェアの上記更新用ソフトウェアへの更新が成功したと判断した場合に、上記更新用認証情報に上書きさせるための消去用情報を生成し、これを上記第１の通信経路で上記被更新装置に送信して上記更新用認証情報に上書きして記憶するよう要求する認証情報消去手段として機能させるためのプログラムである。

【００２１】

このようなプログラムにおいて、上記コンピュータを、上記被更新装置のソフトウェアの更新を外部からのソフトウェア更新要求に応じて行い、その結果をその更新要求の要求元に返す手段として機能させるためのプログラムをさらに含めるとよい。

【００２２】

また、上記コンピュータを、上記被更新装置から起動した旨を示す起動通知を受け付ける手段と、上記更新用ソフトウェアの送信後に上記被更新装置から上記起動通知を受け付けた場合にその被更新装置からソフトウェアのバージョン情報を取得し、送信した更新用ソフトウェアのバージョン情報と比較して更新の成否を確認する手段として機能させるためのプログラムをさらに含めるとよい。

さらに、上記第１の通信経路をＳＳＬによる通信を行う通信経路とし、上記第２の通信

経路をＦＴＰによる通信を行う通信経路とするとよい。
あるいは、上記第１の通信経路を、送信すべきデータを暗号化して送信する通信経路とし、上記第２の通信経路を、送信すべきデータを暗号化しないで送信する通信経路としてもよい。
【発明の効果】
【００２３】
以上のようなこの発明のソフトウェア更新装置、ソフトウェア更新システム、ソフトウェア更新方法によれば、ネットワークを介して通信可能な被更新装置のソフトウェアをソフトウェア更新装置によって更新する場合において、高い安全性を確保しながら更新処理の負荷を低減することができる。
また、この発明のプログラムによれば、コンピュータにソフトウェア更新装置を制御させてこのようなソフトウェア更新装置の特徴を実現し、同様な効果を得ることができる。
【発明を実施するための最良の形態】
【００２４】
以下、この発明の好ましい実施の形態を図面を参照して説明する。
まず、この発明によるソフトウェア更新装置及びソフトウェア更新システムの構成例について説明する。図１は、そのソフトウェア更新システムを含む遠隔管理システムの構成の一例を示す概念図であり、この図において仲介装置１０１がソフトウェア更新装置、被管理装置１０が被更新装置である。管理装置１０２をソフトウェア更新装置としたり、この場合に仲介装置１０１を被更新装置としたりすることもできるが、ここでは、仲介装置１０１がソフトウェア更新装置、被管理装置１０が被更新装置である例について説明する。また、ここでは更新対象のソフトウェアがファームウェアである場合を例として説明するが、これがアプリケーションプログラム等の他のソフトウェアでもよいことはもちろんである。
【００２５】
このソフトウェア更新システムは、プリンタ，ＦＡＸ装置，デジタル複写機，スキャナ装置，デジタル複合機等の画像処理装置や、ネットワーク家電，自動販売機，医療機器，電源装置，空調システム，ガス・水道・電気等の計量システム，汎用コンピュータ，自動車，航空機等に通信機能を持たせた通信装置を被管理装置１０とする遠隔管理システムの一部として構成される。そして、必要な場合に仲介装置１０１から被管理装置１０にファームウェアを送信し、被管理装置１０のファームウェアを更新させる機能を有する。
また、上記の遠隔管理システムは、被管理装置１０とＬＡＮ（ローカルエリアネットワーク）によって接続された遠隔管理仲介装置である仲介装置１０１、更に仲介装置１０１とインタネット１０３（公衆回線等の他のネットワークでもよい）を介して接続されるサーバ装置として機能する管理装置１０２を備え、当該管理装置１０２が、仲介装置１０１を介して各被管理装置１０を集中的に遠隔管理できるようにしたものである。当該仲介装置１０１及び被管理装置１０は、その利用環境に応じて多様な階層構造を成す。
【００２６】
例えば、図１に示す設置環境Ａでは、管理装置１０２とＨＴＴＰによる直接的なコネクションを確立できる仲介装置１０１ａが、被管理装置１０ａ及び１０ｂを従える単純な階層構造になっているが、同図に示す設置環境Ｂでは、４台の被管理装置１０を設置する為、１台の仲介装置１０１を設置しただけでは負荷が大きくなる。その為、管理装置１０２とＨＴＴＰによる直接的なコネクションを確立できる仲介装置１０１ｂが、被管理装置１０ｃ及び１０ｄだけでなく、他の仲介装置１０１ｃを従え、この仲介装置１０１ｃが被管理装置１０ｅ及び１０ｆを更に従えるという階層構造を形成している。この場合、被管理装置１０ｅ及び１０ｆを遠隔管理するために管理装置１０２から発せられた情報は、仲介装置１０１ｂとその下位のノードである仲介装置１０１ｃとを経由して、被管理装置１０ｅ又は１０ｆに到達することになる。
【００２７】
また、設置環境Ｃのように、被管理装置１０に仲介装置１０１の機能を併せ持たせた仲

介機能付被管理装置１１ａ，１１ｂを、別途仲介装置を介さずにインタネット１０３によって管理装置１０２に接続するようにしてもよい。
図示はしていないが、仲介機能付被管理装置１１の下位にさらに被管理装置１０を接続することもできる。
なお、各設置環境には、セキュリティ面を考慮し、ファイアウォール１０４を設置する。

【００２８】
このような遠隔管理システムにおいて、仲介装置１０１は、これに接続された被管理装置１０の制御管理のためのアプリケーションプログラムを実装している。
管理装置１０２は、各仲介装置１０１の制御管理、更にはこの仲介装置１０１を介した被管理装置１０の制御管理を行うためのアプリケーションプログラムを実装している。そして、被管理装置１０も含め、この遠隔管理システムにおけるこれら各ノードは、ＲＰＣ（Remote Procedure Call）により、相互の実装するアプリケーションプログラムのメソッドに対する処理の依頼である「要求」を送信し、この依頼された処理の結果である「応答」を取得することができるようになっている。

【００２９】
すなわち、仲介装置１０１又はこれと接続された被管理装置１０では、管理装置１０２への要求を生成してこれを管理装置１０２へ引き渡し、この要求に対する応答を取得できる一方で、管理装置１０２は、上記仲介装置１０１側への要求を生成してこれを仲介装置１０１側へ引き渡し、この要求に対する応答を取得できるようになっている。この要求には、仲介装置１０１に被管理装置１０に対して各種要求を送信させ、被管理装置１０からの応答を仲介装置１０１を介して取得することも含まれる。
なお、ＲＰＣを実現するために、ＳＯＡＰ（Simple Object Access Protocol：ソープ），ＨＴＴＰ（HyperText Transfer Protocol），ＦＴＰ,ＣＯＭ（Component Object Model），ＣＯＲＢＡ（Common Object Request Broker Architecture）等の既知のプロトコル（通信規格），技術，仕様などを利用することができる。

【００３０】
この送受信のデータ送受モデルを図２の概念図に示す。
（Ａ）は、被管理装置１０で管理装置１０２に対する要求が発生したケースである。このケースでは、被管理装置１０が被管理装置側要求ａを生成し、これを仲介装置１０１を経由して受け取った管理装置１０２がこの要求に対する応答ａを返すというモデルになる。同図に示す仲介装置１０１は複数であるケースも想定できる（上記図１に示す設置環境Ｂ）。なお、（Ａ）では、応答ａだけでなく応答遅延通知ａ′を返信するケースが表記されている。これは、管理装置１０２が、仲介装置１０１を経由して被管理装置側要求を受け取って、当該要求に対する応答を即座に返せないと判断したときには、応答遅延通知を通知して一旦接続状態を切断し、次回の接続の際に上記要求に対する応答を改めて引き渡す構成としているためである。

【００３１】
（Ｂ）は、管理装置１０２で被管理装置１０に対する要求が発生したケースである。このケースでは、管理装置１０２が管理装置側要求ｂを生成し、これを仲介装置１０１を経由して受け取った被管理装置１０が、当該要求に対する応答ｂを返すというモデルになっている。なお、（Ｂ）のケースでも、応答を即座に返せないときに応答遅延通知ｂ′を返すことは（Ａ）のケースと同様である。

【００３２】
次に、図１に示す管理装置１０２の物理的構成について説明すると、当該管理装置１０２は、不図示のＣＰＵ、ＲＯＭ、ＲＡＭ、不揮発性メモリ、ネットワークインタフェースカード（以下ＮＩＣという）等を備えている。
また、図１に示す仲介装置１０１の物理的構成は、図３に示す通りである。
すなわち、ＣＰＵ５２，ＳＤＲＡＭ５３，フラッシュメモリ５４，ＲＴＣ（リアルタイムクロック）５５，Op-Port（操作部接続ポート）５６，ＰＨＹ（物理メディアインタフ

ェース）５７，モデム５８，ＨＤＤ制御部５９，拡張Ｉ／Ｆ（インターフェース）６０，ＲＳ２３２Ｉ／Ｆ６１，ＲＳ４８５Ｉ／Ｆ６２，ＨＤＤ（ハードディスクドライブ）６３等を備えている。そして、当該仲介装置１５はＰＨＹ５７を介してＬＡＮと接続される。また、そのＬＡＮを介して被管理装置１０と接続されるものである。ＲＳ２３２Ｉ／Ｆ６１及びＲＳ４８５Ｉ／Ｆ６２を介しても被管理装置１０と接続可能であるが、ここではこのＩ／Ｆは使用しないものとする。

【００３３】

なお、仲介機能付被管理装置１１については、仲介装置１０１の機能を実現するためにこれらのユニットを単に被管理装置１０に付加しても良いが、被管理装置１０に備えるＣＰＵ，ＲＯＭ，ＲＡＭ等のハードウェア資源を利用し、ＣＰＵに適当なアプリケーションやプログラムモジュールを実行させることによって仲介装置１０１の機能を実現することもできる。

【００３４】

図４は、仲介装置１０１のソフトウェア構成の一例を示すブロック図である。この図に示すように、仲介装置１０１のソフトウェアは、アプリケーション層７０，サービス層８０，プロトコル層９０の３層からなっている。そして、これらのソフトウェアを構成するプログラムはＨＤＤ６３やＳＤＲＡＭ５３、あるいはフラッシュメモリ５４上に記憶され、必要に応じて読み出されてＣＰＵ５２によって実行される。そしてＣＰＵ５２は、これらのプログラムを必要に応じて実行し、装置の制御を行うことにより、各機能（認証情報設定手段，認証要求手段，送信手段，その他の手段としての機能）を実現することができる。

【００３５】

このソフトウェアにおいて、アプリケーション層７０には、デバイスコントロールメソッド群７１とＮＲＳ（ニュー・リモート・サービス）アプリケーションメソッド群７２とを有する。

そして、デバイスコントロールメソッド群７１は、管理対象情報設定，機器設定，ソフトウェアアップデート，ポーリング設定変更，ログ出力，起動処理の各メソッドを備え、この実施形態の特徴に係るファームウェア更新処理を始め、被管理装置の情報管理や通信の設定等を行うためのプログラムである。

ＮＲＳアプリケーションメソッド群７２は、ログ収集，ソフトウェアダウンロード，機器コマンド実行，機器設定変更，サプライ通知，異常通知，デバイス起動／導入，デバイス生死確認の各メソッドを備え、被管理装置１０からの種々の通知や要求に対応したり、管理装置１０２からの要求に従って被管理装置１０に動作を行わせたりするためのプログラムである。

【００３６】

次に、サービス層８０には、セキュリティサービス８１，対接続機器通信サービス８２，対管理装置通信サービス８３，スケジューラサービス８４とを備えている。

そして、セキュリティサービス８１は、内部情報などの外部への不正流出を予防、妨害するなどのジョブを生成・実行するモジュールである。

対接続機器通信サービス８２は、仲介装置１０１に接続されたネットワーク接続機器との間で情報の授受を実現するため、情報取得の対象となる機器の検索、対象機器との接続管理、ファイル送受信、パラメータ管理、ＡＰＬ管理などのジョブを生成・実行するモジュールである。

対管理装置通信サービス８３は、管理装置１０２との間でコマンド受信，ファイル送受信，情報要求，情報送信（情報通知）などのジョブを生成・実行するモジュールである。

スケジューラサービス８４は、所定の設定時間情報に基づき、リモートコントロールアプリを展開するモジュールである。

【００３７】

次のプロトコル層９０には、情報の送受信対象に応じたプロトコルを用いて情報の授受をおこなうジョブを生成・実行するための各メソッドを備える。即ち、ＬＡＮを介したネ

ットワーク接続機器の通信環境に広く対応可能なように、ＳＯＡＰ（Simple Object Access Protocol）や、その下位プロトコルとして用いられるＨＴＴＰ，ＨＴＴＰＳ（Hypertext Transfer Protocol Security），ＦＴＰなどを制御可能なメソッドを有している。

【００３８】

以下、図１に示した遠隔管理システムのより具体的な例として、画像処理装置を被管理装置とした画像処理装置遠隔管理システムについて説明する。この遠隔管理システムは、画像処理装置を被更新装置とした、この発明によるソフトウェア更新システムの実施形態を含むものである。図５は、その画像処理装置遠隔管理システムの構成の一例を示す概念図であるが、被管理装置１０を画像処理装置１００に、仲介機能付被管理装置１１を仲介機能付画像処理装置１１０に変更した点が図１と相違するのみであるので、システムの全体構成についての説明は省略する。なお、ソフトウェア更新システムは、この発明のソフトウェア更新装置の実施形態である仲介装置１０１と被更新装置となる画像処理装置１００のみで構成することができ、管理装置１０２やファイアウォール１０４等の他の構成要素は必須ではない。

【００３９】

そして、画像処理装置１００は、コピー、ファクシミリ、スキャナ等の機能及び外部装置と通信を行う機能を備えたデジタル複合機であり、それらの機能に係るサービスを提供するためのアプリケーションプログラムを実装しているものである。また、仲介機能付画像処理装置１１０は、画像処理装置１００に仲介装置１０１の機能を併せ持たせたものである。

【００４０】

このような画像処理装置１００の物理的構成について図６を用いて説明する。

図６は、画像処理装置１００内の物理的構成の一例を示すブロック図である。同図に示すように、画像処理装置１００は、コントローラボード２００、ＨＤＤ（ハードディスクドライブ）２０１、ＮＶ－ＲＡＭ（不揮発性ＲＡＭ）２０２、ＰＩ（パーソナルインタフェース）ボード２０３、ＰＨＹ２０４、操作パネル２０５、プロッタ／スキャナエンジンボード２０６、電源ユニット２０７、フィニッシャ２０８、ＡＤＦ（自動原稿給送装置）２０９、給紙バンク２１０、その他周辺機２１１を備えている。

【００４１】

ここで、コントローラボード２００は、制御手段に該当し、ＣＰＵ，ＲＯＭ，ＲＡＭ等を備え、ＰＣＩ－ＢＵＳ（Peripheral Components Interconnect-Bus）２１２を介して各機能を制御している。また、ＨＤＤ２０１は、記憶手段に該当する。また、ＮＶ－ＲＡＭ２０２は、記憶手段に該当し、不揮発性メモリであって、例えば、フラッシュメモリ等が該当する。

【００４２】

また、ＰＩボード２０３とＰＨＹ２０４は、通信手段に該当し、外部との通信を行うためのものであって、例えば、通信ボード等が該当する。ＰＩボード２０３はＲＳ４８５規格に準拠したインタフェースを備え、ラインアダプタを介して公衆回線に接続している。ＰＨＹ２０４は、ＬＡＮを介して外部装置と通信を行うためのインタフェースであり、ＩＥＥＥ（Institute of Electrical and Electronic Engineers）８０２．１１ｂ規格（無線ＬＡＮ対応），ＩＥＥＥ１３９４規格，ＩＥＥＥ８０２．３規格（イーサネット（登録商標）対応）に準拠したインタフェースをそれぞれ設け、複数の通信手段としている。

また、操作パネル２０５は、操作部及び表示部に該当するユーザインタフェースである。

【００４３】

ここで、同図中のＥＮＧＲＤＹは、エンジン側の各種初期設定が完了して、コントローラボード２００とコマンドの送受信の準備ができたことをコントローラボード２００側に通知するための信号線である。また、ＰＷＲＣＴＬは、エンジンへの電源供給をコントローラボード２００側から制御するための信号線である。これら信号線の動作に関しては後述する。

【００４４】
次に、画像処理装置１００におけるソフトウェア構成を図７を用いて説明する。
図７は、画像処理装置１００のソフトウェア構成の一例を示すブロック図である。画像処理装置１００のソフトウェア構成は、最上位のアプリケーションモジュール（アプリ）層、その下位のサービスモジュール層からなる。そして、これらのソフトウェアを構成するプログラムはＨＤＤ２０１やコントローラボード２００上のＲＡＭに記憶され、必要に応じて読み出されてコントローラボード２００上のＣＰＵによって実行される。そしてＣＰＵは、これらのプログラムを必要に応じて実行することにより、各機能（記憶手段，認証手段，更新手段，その他の手段としての機能）を実現することができる。
【００４５】
特に、アプリケーションモジュール層のソフトウェアは、ＣＰＵをハードウェア資源を動作させて所定の機能を実現させる複数のアプリケーション制御手段として機能させるためのプログラムによって構成され、サービスモジュール層のソフトウェアは、ＣＰＵを、ハードウェア資源と各アプリケーション制御手段との間に介在し、複数のアプリケーション制御手段からのハードウェア資源に対する動作要求の受付，その動作要求の調停，およびその動作要求に基づく動作の実行制御を行うサービス制御手段として機能させるためのプログラムによって構成される。
またＯＳ３２０は、ＵＮＩＸ（登録商標）などのオペレーティングシステムであり、サービスモジュール層及びアプリケーションモジュール層の各プログラムをそれぞれプロセスとして並列実行する。
【００４６】
サービスモジュール層には、オペレーションコントロールサービス（ＯＣＳ）３００、エンジンコントロールサービス（ＥＣＳ）３０１、メモリコントロールサービス（ＭＣＳ）３０２、ネットワークコントロールサービス（ＮＣＳ）３０３、ファクスコントロールサービス（ＦＣＳ）３０４、カスタマーサポートシステム（ＣＳＳ）３０５、システムコントロールサービス（ＳＣＳ）３０６、システムリソースマネージャ（ＳＲＭ）３０７、イメージメモリハンドラ（ＩＭＨ）３０８、デリバリーコントロールサービス（ＤＣＳ）３１６、ユーザコントロールサービス（ＵＣＳ）３１７、データエンクリプションセキュリティサービス（ＤＥＳＳ）３１８、サーティフィカットコントロールサービス（ＣＣＳ）３１９を実装している。更に、アプリケーションモジュール層には、コピーアプリ３０９、ファクスアプリ３１０、プリンタアプリ３１１、スキャナアプリ３１２、ネットファイルアプリ３１３、ウェブアプリ３１４、ＮＲＳ（ニューリモートサービス）アプリ３１５を実装している。
【００４７】
これらを更に詳述する。
ＯＣＳ３００は、操作パネル２０５を制御するモジュールである。
ＥＣＳ３０１は、ハードウェアリソース等のエンジンを制御するモジュールである。
ＭＣＳ３０２は、メモリ制御をするモジュールであり、例えば、画像メモリの取得及び開放、ＨＤＤ２０１の利用等を行う。
ＮＣＳ３０３は、ネットワークとアプリケーションモジュール層の各アプリケーションプログラムとの仲介処理を行わせるモジュールである。
ＦＣＳ３０４は、ファクシミリ送受信、ファクシミリ読み取り、ファクシミリ受信印刷等を行うモジュールである。
【００４８】
ＣＳＳ３０５は、公衆回線を介してデータを送受信する際のデータの変換等をするモジュールであり、また公衆回線を介した遠隔管理に関する機能をまとめたモジュールである。
ＳＣＳ３０６は、コマンドの内容に応じたアプリケーションモジュール層の各アプリケーションプログラムの起動管理及び終了管理を行うモジュールである。
ＳＲＭ３０７は、システムの制御及びリソースの管理を行うモジュールである。

ＩＭＨ３０８は、一時的に画像データを入れておくメモリを管理するモジュールである。

【００４９】

ＤＣＳ３１６は、ＨＤＤ２０１やコントローラボード２００上のメモリに記憶している（する）画像ファイル等をＳＭＴＰ（Simple Mail Transfer Protocol）やＦＴＰ（File Transfer Protocol）を用いて送受信するモジュールである。

ＵＣＳ３１７は、ユーザが登録した宛先情報や宛名情報等のユーザ情報を管理するモジュールである。

ＤＥＳＳ３１８は、ＰＫＩやＳＳＬを利用した各ユニットあるいは外部装置の認証や、通信の暗号化を行うモジュールである。

ＣＣＳ３１９は、この画像処理装置１００に入力された認証情報について認証処理を行うモジュールである。

【００５０】

コピーアプリ３０９は、コピーサービスを実現するためのアプリケーションプログラムである。

ファクスアプリ３１０は、ファクスサービスを実現するためのアプリケーションプログラムである。

プリンタアプリ３１１は、プリンタサービスを実現するためのアプリケーションプログラムである。

【００５１】

スキャナアプリ３１２は、スキャナサービスを実現するためのアプリケーションプログラムである。

ネットファイルアプリ３１３は、ネットファイルサービスを実現するためのアプリケーションプログラムである。

ウェブアプリ３１４は、ウェブサービスを実現するためのアプリケーションプログラムである。

ＮＲＳアプリ３１５は、ネットワークを介してデータを送受信する際のデータの変換や、ネットワークを介した遠隔管理に関する機能（管理装置１０２との通信に係わる機能を含む）を実現するためのアプリケーションプログラムである。そして、外部装置からネットワーク経由で受信したデータを、各アプリにおける処理に適したデータ構造体に変換する機能も有する。

なお、説明の都合上、以下の説明において、ＣＰＵが以上のような各プログラムに従って動作することによって実行する処理について、それらのプログラムが処理を実行するものとして説明する。

【００５２】

ここで、上述したＥＮＧＲＤＹ信号とＰＷＲＣＴＬ信号との動作を図８を用いて説明する。

図８の（Ａ）は機器の立ち上がり時のＥＮＧＲＤＹ信号とＰＷＲＣＴＬ信号の動作の一例を示している。ＡＣ－ＰＯＷＥＲのＡＣ電源をＯＮにすると電源供給が開始され、これと同時にＥＮＧＲＤＹ信号はＨｉｇｈになる。この状態ではエンジン側との通信はできない。なぜなら、エンジン側の初期設定が完了していないからである。そして、一定期間経過後にエンジン側の初期設定が完了し、ＥＮＧＲＤＹ信号がＬｏｗになった段階でエンジン側との通信が可能となる。

【００５３】

次に、同図（Ｂ）は省エネモードに移行した時のＥＮＧＲＤＹ信号とＰＷＲＣＴＬ信号の動作の一例を示している。省エネモードに移行するため、コントローラボード２００によりＰＷＲＣＴＬ信号をＯＦＦにする。これと同時に電源供給もおちる。これに伴って、ＥＮＧＲＤＹ信号は、Ｈｉｇｈとなり省エネモードに移行する。次に、省エネモードから復帰する場合を同図（Ｃ）に示す。

【００５４】

同図（Ｃ）は、省エネモードから復帰する時のＥＮＧＲＤＹ信号とＰＷＲＣＴＬ信号の動作の一例を示している。上記（Ｂ）の省エネモードから復帰する際には、コントローラボード２００によりＰＷＲＣＴＬ信号をＯＮにする。これと同時に電源供給もされる。しかし、上記の（Ａ）で示したように、エンジン側の初期設定が完了するまで、ＥＮＧＲＤＹ信号はＨｉｇｈの状態であり、初期設定が完了するとエンジン側との通信が可能となり、Ｌｏｗとなる。

【００５５】

次に、上述した画像処理装置１００のソフトウェアの構成に含まれるＮＲＳアプリ３１５の内部構成を図９を用いて更に説明する。

図９は、ＮＲＳアプリの構成の一例を示す機能ブロック図である。同図に示すように、ＮＲＳアプリ３１５は、アプリケーションモジュール層とＮＣＳ３０３との間で処理をおこなっている。ウェブサーバ機能部５００は、外部から受信した要求に関する応答処理を行う。ここでの要求は、例えば、構造化言語であるＸＭＬ（Extensible Markup Language）形式で記載された、ＳＯＡＰ（Simple Object Access Protocol）によるＳＯＡＰリクエストであることが考えられる。ウェブクライアント機能部５０１は、外部への要求を発行する処理を行う。ｌｉｂｘｍｌ５０２は、ＸＭＬ形式で記載されたデータを処理するライブラリであり、ｌｉｂｓｏａｐ５０３は、ＳＯＡＰを処理するライブラリである。また、ｌｉｂｇｗｗｗ５０４は、ＨＴＴＰを処理するライブラリであり、ｌｉｂｇｗ＿ｎｃｓ５０５は、ＮＣＳ３０３との間の処理をするライブラリである。

【００５６】

上記のＳＯＡＰリクエストは、ＰＨＹ２０４によって受信され、ＳＯＡＰヘッダとＳＯＡＰボディを含むＳＯＡＰドキュメントがＨＴＴＰメッセージの形でＮＣＳ３０３を介してＮＲＳアプリ３１５に渡される。そして、ＮＲＳアプリ３１５において、ｌｉｂｓｏａｐ５０３を用いてＳＯＡＰドキュメントからＳＯＡＰボディを取り出し、ｌｉｂｘｍｌ５０２を用いてＳＯＡＰボディを解釈してＤＯＭ（Document Object Model）ツリーを生成し、ウェブサーバ機能部５００がこれを各アプリにおける処理に適したデータ構造体に変換した上でＳＯＡＰボディに含まれるコマンドに対応したアプリに渡す。

データ構造体については、例えばアプリのプログラムがＣ言語で記載されている場合にはＣ言語の構造体データであり、この構造体データを引数としてアプリのプログラムをコールすることによってアプリにデータを渡すことができる。

【００５７】

上述した構成を踏まえて、図５の画像処理装置遠隔管理システム内で行われるデータ送受信の際の通信シーケンスの一例について図１０を用いて説明する。図１０は、管理装置、仲介装置、及び画像処理装置間で行われるデータ送受信の際の通信シーケンスの一例を示す図である。

この例においては、まず、仲介装置１０１は、管理装置１０２に対してポーリング（送信要求があるかどうかの問い合わせ）を行う（Ｓ６０１）。つまり、自己の識別情報である識別子を付加したポーリング用のＳＯＡＰドキュメントを生成し、ＨＴＴＰメッセージとして管理装置１０２へ送信する。図５に示したように、仲介装置１０１と管理装置１０２との間にはファイアウォール１０４を設けているため、管理装置１０２から仲介装置１０１に向けて通信セッションを張る（通信を要求して通信経路を確立する）ことができないので、管理装置１０２から仲介装置１０１（あるいは仲介装置１０１を介して画像処理装置１００）に要求を送信したい場合でも、このように仲介装置１０１からのポーリングを待つ必要があるのである。

【００５８】

管理装置１０２は、仲介装置１０１から上記ＨＴＴＰメッセージを受信すると、課金カウンタ取得要求を示すＳＯＡＰドキュメントを生成し、該当する仲介装置１０１（受信したＳＯＡＰメッセージの送信元）へ、ポーリングに対する応答のＨＴＴＰメッセージとして送信する（Ｓ６０２）。このとき、受信したＨＴＴＰメッセージ内のＳＯＡＰドキュメントに付加された識別子に基づいて該当する仲介装置１０１を認識する。このように、フ

ァイアウォール１０４の内側からの通信（ＨＴＴＰリクエスト）に対する応答（ＨＴＴＰレスポンス）であれば、ファイアウォールの外側から内側に対してデータを送信することができる。

【００５９】

仲介装置１０１は、管理装置１０２から上記ＨＴＴＰメッセージを受信すると、そのＨＴＴＰメッセージに基づいて課金カウンタ取得要求を示すＳＯＡＰドキュメントを生成し、やはりＨＴＴＰメッセージとして自己に接続されている画像処理装置１００のＮＲＳアプリ３１５へ送信する（Ｓ６０３）。

ＮＲＳアプリ３１５は、仲介装置１０１からＨＴＴＰメッセージとして受信したＳＯＡＰドキュメントに記述されている課金カウンタ取得要求をＳＣＳ３０６へ通知する（Ｓ６０４）。

ＳＣＳ３０６は、ＮＲＳアプリ３１５から課金カウンタ取得要求の通知を受けると、ＮＶ－ＲＡＭ２０２に格納されている課金カウンタのデータを読み取る（Ｓ６０５）。そして、その読み取った課金カウンタのデータ（応答データ）をＮＲＳアプリ３１５へ引き渡す（Ｓ６０６）。

【００６０】

ＮＲＳアプリ３１５は、ＳＣＳ３０６から課金カウンタのデータを受け取る（取得する）と、その内容を示す課金カウンタ用のＳＯＡＰドキュメントを生成し、ＨＴＴＰメッセージとして仲介装置１０１へ送信する（Ｓ６０７）。

仲介装置１０１は、ＮＲＳアプリ３１５から課金カウンタ用のＳＯＡＰドキュメントを受信すると、そのＳＯＡＰドキュメントをＨＴＴＰメッセージとして管理装置１０２へ送信する（Ｓ６０８）。

このように、上記通信シーケンスにより、データの送受信が行われる。

【００６１】

次に、上記図１０と異なり、画像処理装置１００から仲介装置１０１を経て管理装置１０２へデータを送信する場合の通信シーケンスの一例について図１１を用いて説明する。

図１１は、画像処理装置から管理装置１０２へデータを送信する場合の通信シーケンスの一例を示す図である。

この例においては、まず、ＯＣＳ３００は、ユーザコールキーが押下された旨をＳＣＳ３０６へ通知する（Ｓ７０１）。

ＳＣＳ３０６は、ＯＣＳ３００からユーザコールキーが押下された旨の通知を受けると、ユーザコール要求をＮＲＳアプリ３１５へ通知する（Ｓ７０２）。

【００６２】

ＮＲＳアプリ３１５は、ＳＣＳ３０６からユーザコール要求の通知を受けると、ユーザコールを知らせるユーザコール情報であるユーザコール用のＳＯＡＰドキュメントを生成し、ＨＴＴＰメッセージとして仲介装置１０１へ送信する（Ｓ７０３）。

仲介装置１０１は、ＮＲＳアプリ３１５からユーザコール用のＳＯＡＰドキュメントを受信すると、そのＳＯＡＰドキュメントに自己の識別情報である識別子を付加し、そのＳＯＡＰドキュメントをやはりＨＴＴＰメッセージとして管理装置１０２に対して送信し、ユーザコールを行う。つまり、自己の識別子を付加したユーザコール用のＳＯＡＰドキュメントを管理装置１０２へ通報する（Ｓ７０４）。この場合には、ファイアウォール１０４の内側から外側に向けての送信であるので、仲介装置１０１が自ら管理装置１０２に向けてセッションを張ってデータを送信することができる。

ここで、ステップＳ７０４の処理後のパターンを以下の（Ａ）から（Ｃ）に分けて説明する。

【００６３】

まず、（Ａ）において、管理装置１０２は、ユーザ先の仲介装置１０１からユーザコール用のＳＯＡＰドキュメントをＨＴＴＰメッセージとして受信し、その受信が正常に終了した場合には、その旨（ユーザコールが成功した旨）のコール結果を、正常に終了しなかった（異常に終了した）場合には、その旨（ユーザコールが失敗した旨）のコール結果を

示すＳＯＡＰドキュメント生成し、ＨＴＴＰメッセージによる応答として通報元の仲介装置１０１へ送信する（Ｓ７０５）。
仲介装置１０１は、管理装置１０２からコール結果を示すＳＯＡＰドキュメントを受信すると、そのＳＯＡＰドキュメントを、やはりＨＴＴＰメッセージとしてユーザコールキーが押下された画像処理装置１００のＮＲＳアプリ３１５へ送信する（Ｓ７０６）。
【００６４】
ＮＲＳアプリ３１５は、仲介装置１０１からコール結果を示すＳＯＡＰドキュメントを受信すると、そのＳＯＡＰドキュメントが示すコール結果を解釈（判定）し、ＳＣＳ３０６へ通知する（Ｓ７０７）。
ＳＣＳ３０６は、コール結果を受け取ると、それをＯＣＳ３００へ引き渡す。
ＯＣＳ３００は、ＳＣＳ３０６からコール結果を受け取ると、その内容つまりユーザコールが成功したか失敗したかを示すメッセージを操作パネル２０５上の文字表示器に表示する（Ｓ７０８）。
【００６５】
次に（Ｂ）において、仲介装置１０１は、規定時間（予め設定された所定時間）が経っても管理装置１０２から応答がないと判断した場合には、ユーザコールが失敗した旨のコール結果を示すＳＯＡＰドキュメントを生成し、ＨＴＴＰメッセージとしてＮＲＳアプリ３１５へ送信する（Ｓ７０９）。
ＮＲＳアプリ３１５は、失敗した旨のコール結果を示すＳＯＡＰドキュメントを受信すると、そのＳＯＡＰドキュメントに記述されている失敗した旨のコール結果を解釈し、ＳＣＳ３０６へ通知する（Ｓ７１０）。
ＳＣＳ３０６は、ＮＲＳアプリ３１５からコール結果を受け取ると、それをＯＣＳ３００へ引き渡す。
ＯＣＳ３００は、ＳＣＳ３０６からコール結果を受け取ると、その内容つまりユーザコールが失敗した旨を示すメッセージを操作パネル２０５上の文字表示器に表示する（Ｓ７１１）。
【００６６】
次に（Ｃ）において、ＮＲＳアプリ３１５は、規定時間が経っても仲介装置１０１から応答がないと判断した場合には、ユーザコールが失敗した旨のコール結果をＳＣＳ３０６へ通知する（Ｓ７１２）。
ＳＣＳ３０６は、ＮＲＳアプリ３１５からコール結果を受け取ると、それをＯＣＳ３００へ引き渡す。
ＯＣＳ３００は、ＳＣＳ３０６からコール結果を受け取ると、その内容つまりユーザコールが失敗した旨を示すメッセージを操作パネル２０５上の文字表示器に表示する（Ｓ７１３）。
【００６７】
なお、ここでは管理装置１０２からファイアウォール１０４を越えて仲介装置１０１（あるいは仲介装置１０１を介して画像処理装置１００）にデータを送信するために、仲介装置１０１からのＨＴＴＰリクエストに対するレスポンスという形で送信を行う例について説明したが、ファイアウォール１０４を越える手段はこれに限られるものではなく、例えば、ＳＭＴＰ（Simple Mail Transfer Protocol）を利用して、送信したいデータを記載あるいは添付したメールを管理装置１０２から仲介装置１０１に送信することも考えられる。ただし、信頼性の面ではＨＴＴＰが優れている。
【００６８】
ここで、このような基本的な機能を有する図５に示した画像処理装置遠隔管理システムにおいて実行する、画像処理装置１００のファームウェア更新処理の参考例について説明する。
背景技術の項で図２６に示した処理の安全性を向上させる手段としては、通信を暗号化するほか、図１２に示すようなパスワードリストを用いることも考えられ、この参考例は、このパスワードリストを使用した処理である。また、ファーム更新装置９１と対応する

装置は仲介装置１０１、被更新装置９２と対応する装置は画像処理装置１００とする。
そして、ここで使用するパスワードリストは、仲介装置１０１に設定されたＩＤと対応するパスワードを多数生成し、順序をつけたものである。このようなパスワードリストは、メモリカード等に記憶させて書留郵便のようなネットワーク以外の安全な経路で仲介装置１０１と画像処理装置１００の管理者に送付し、それぞれの管理者が装置の記憶手段に記憶させておく。そして、仲介装置１０１から画像処理装置１００に認証を要求する際には未使用のパスワードの中から先頭のものを選んで使用するようにし、使用したものは使用済みとして、次に認証を要求する際には次のパスワードを用いるようにするのである。

【００６９】

このようなパスワードリストを用いる場合の図２６と対応する処理は、例えば図１３のシーケンス図に示すようになる。
図１３に示す処理においても、仲介装置１０１と画像処理装置１００とはＦＴＰ（File Transfer Protocol）を用いて通信を行う。
この処理においても、所定のイベントが発生した場合等に仲介装置１０１が画像処理装置１００にＩＤとパスワードを送信してＦＴＰによる接続を要求するが、その前にパスワードリストを参照して使用するパスワードを決定する（Ｓ４１）。ここでは、まだパスワードは１つも使用されておらず、先頭のパスワードＡを選択するものとする。

【００７０】

そしてその後、仲介装置１０１は図２６のステップＳ１１乃至Ｓ１３の場合と同様にバージョン情報取得処理を行って画像処理装置１００のファームのバージョン情報を取得する（Ｓ４２～Ｓ４４）が、この際に用いるパスワードはステップＳ１１で選択したパスワードＡである。そして、画像処理装置１００も同じパスワードリストを記憶しているので、これを参照して先頭のパスワードＡと比較することにより、認証処理を行うことができる。
バージョン情報取得処理が終了すると、仲介装置１０１はパスワード更新処理を開始し、ＨＴＴＰ（Hyper Text Transfer Protocol）を用いて画像処理装置１００にパスワード更新要求を送信する（Ｓ４５）。そして、この要求に従って、画像処理装置１００はパスワードリストのうちの使用したパスワード（パスワードＡ）を使用済に設定し（Ｓ４６）、これが成功すると更新ＯＫ通知を返す（Ｓ４７）。

【００７１】

仲介装置１０１は、この通知を受け取ると、画像処理装置１００と同じように、使用したパスワードを使用済に設定する（Ｓ４８）。以上がパスワード更新処理であり、この処理によって、仲介装置１０１と画像処理装置１００の双方で、一度ＦＴＰで転送したパスワードを使用済みとし、まだ使用していない次の安全なパスワード（パスワードＢ）を使用するように設定することができる。ただし、続けてファーム送信処理を行う場合には、ファーム送信処理の終了まではバージョン情報取得処理で用いたパスワードをそのまま使用するものとする。

【００７２】

次に、仲介装置１０１はステップＳ４３で取得したファームのバージョン情報をもとに更新の要否を判断する。ここで更新不要と判断すれば処理を終了し、また必要が生じた場合にバージョン情報取得処理を行うことになる。しかし、更新が必要と判断すれば（Ｓ４９）、次のファーム送信処理を実行する（Ｓ５０～Ｓ５３）。この処理は、図２６に示したファーム送信処理とほぼ同様であり、認証処理に用いるパスワードがパスワードリストに含まれるパスワードＡである点が異なるのみである。

【００７３】

以上の処理によって、必要な場合に画像処理装置１００のファームを更新することができる。そして、再度バージョン情報取得処理やファーム送信処理を行う場合は、再度パスワードリストを参照して使用するパスワードを決定する（Ｓ５４）が、ここでは、パスワードＡが使用済みになっているので、次のパスワードＢを選択することになる。
そして、ステップＳ５５～Ｓ５７で、ステップＳ４２～Ｓ４４の場合と同様に、バージ

ョン情報取得処理を行うが、ここで認証に使用するパスワードはパスワードＢとなる。
以下、同様にして、パスワードをパスワードＣ，Ｄ，・・・と順次変更して処理を繰り返すことになる。

【００７４】

このようにパスワードリストを用いるようにすれば、一度ＦＴＰを用いて転送したパスワードはファームウェア更新処理後には使用されることがなく、常に秘密の保たれたパスワードを使用して認証処理を行うことができるので、なりすまし等の不正アクセスを防止してセキュリティの向上を図ることができる。
しかしながら、この参考例で用いたパスワードリストは、多数のパスワードを含むため、データ量が多くなり、これを記憶する領域を用意するとメモリのコストアップにつながる。また、パスワードを装置に記憶させた状態にすることになるため、装置にアクセスした第３者にリストごとパスワードを盗まれる可能性も否定できない。また、初めにパスワードリストを郵便等によって送付し、管理者が手動で記憶させる必要があるので、労力がかかるという問題もあった。さらに、処理にエラーが生じて装置間で使用するパスワードのＮｏ．が異なる事態が発生すると、認証処理が正常に行えないという問題もあった。また、パスワードリストに含まれるパスワードの数は有限であるので、全部使用してしまった後は、再度新たなリストを配布して記憶させるか、多少の危険を承知で使用済みのパスワードを再利用する必要があるという問題もあった。

【００７５】

ところで、図５に示した画像処理装置遠隔管理システムにおいて、仲介装置１０１と画像処理装置１００との間の通信を、必要に応じてＳＳＬを用いた認証を行ってから行うようにすることができる。そこで次に、この認証を行う場合の通信手順について、認証処理の部分に焦点を当てて説明する。この認証には、互いが互いを認証する相互認証と、一方が他方を認証する片方向認証とが考えられるが、まず相互認証の場合について説明する。
図１４は、仲介装置１０１と画像処理装置１００とがＳＳＬによる相互認証を行う際に各装置において実行する処理のフローチャートを、その処理に用いる情報と共に示す図である。

【００７６】

図１４に示すように、ＳＳＬによる相互認証を行う際には、まず仲介装置１０１側にルート鍵証明書，私有鍵Ａ，公開鍵証明書Ａを記憶させておく必要がある。私有鍵Ａは、認証局（ＣＡ：certificate authority）が仲介装置１０１に対して発行した私有鍵である。そして、公開鍵証明書Ａは、その私有鍵と対応する公開鍵にＣＡがデジタル署名を付してデジタル証明書としたものである。また、ルート鍵証明書は、ＣＡが付したデジタル署名の正当性を確認するための鍵であるルート鍵に、デジタル署名を付してデジタル証明書としたものである。なお、公開鍵は、対応する私有鍵を用いて暗号化された文書を復号化するための鍵本体と、その公開鍵の発行者（ＣＡ），発行相手，有効期限等の情報を含む書誌情報とによって構成されるものとする。

【００７７】

また、画像処理装置１００側には、ルート鍵証明書，私有鍵Ｂ，公開鍵証明書Ｂを記憶させておく必要がある。私有鍵Ｂ及び公開鍵証明書Ｂは、ＣＡが画像処理装置１００に対して発行した私有鍵及び公開鍵証明書である。ここでは仲介装置１０１と画像処理装置１００に対して同じＣＡが同じルート私有鍵を用いて証明書を発行しているものとし、この場合にはルート鍵証明書は仲介装置１０１と画像処理装置１００で共通となる。

【００７８】

フローチャートの説明に入る。なお、図１４において、２本のフローチャート間の矢印は、データの転送を示し、送信側は矢印の根元のステップで転送処理を行い、受信側はその情報を受信すると矢印の先端のステップの処理を行うものとする。また、各ステップの処理が正常に完了しなかった場合には、その時点で認証失敗の応答を返して処理を中断するものとする。相手から認証失敗の応答を受けた場合、処理がタイムアウトした場合等も同様である。また、それぞれの処理は、仲介装置１０１と画像処理装置１００とがそれぞ

れ備えるＣＰＵが所要の制御プログラムに従った処理を行うことにより実現されるものである。

【００７９】

仲介装置１０１は、画像処理装置１００に接続を要求する場合、図１４の左側に示すフローチャートの処理を開始する。そして、ステップＳ２１で画像処理装置１００に対して接続要求を送信する。

一方画像処理装置１００は、この接続要求を受信すると、図１４の右側に示すフローチャートの処理を開始する。そして、ステップＳ３１で第１の乱数を生成し、これを私有鍵Ｂを用いて暗号化する。そして、ステップＳ３２でその暗号化した第１の乱数と公開鍵証明書Ｂとを仲介装置１０１に送信する。

【００８０】

仲介装置１０１側では、これを受信すると、ステップＳ２２でルート鍵証明書を用いて公開鍵証明書Ｂの正当性を確認する。これには、公開鍵に含まれる書誌情報を参照して画像処理装置１００が適当な通信相手であることを確認する処理を含む。

そして確認ができると、ステップＳ２３で、受信した公開鍵証明書Ｂに含まれる公開鍵Ｂを用いて第１の乱数を復号化する。ここで復号化が成功すれば、第１の乱数は確かに公開鍵証明書Ｂの発行対象である画像処理装置１００から受信したものだと確認できる。そして、画像処理装置１００を正当な通信相手として認証する。

【００８１】

その後、ステップＳ２４でこれとは別に第２の乱数及び第３の乱数を生成する。そして、ステップＳ２５で第２の乱数を私有鍵Ａを用いて暗号化し、第３の乱数を公開鍵Ｂを用いて暗号化し、ステップＳ２６でこれらを公開鍵証明書Ａと共に画像処理装置１００に送信する。第３の乱数の暗号化は、画像処理装置１００以外の装置に乱数を知られないようにするために行うものである。

【００８２】

画像処理装置１００側では、これを受信すると、ステップＳ３３でルート鍵証明書を用いて公開鍵証明書Ａの正当性を確認する。これにも、ステップＳ２２の場合と同様、仲介装置１０１が適当な通信相手であることを確認する処理を含む。そして確認ができると、ステップＳ３４で、受信した公開鍵証明書Ａに含まれる公開鍵Ａを用いて第２の乱数を復号化する。ここで復号化が成功すれば、第２の乱数は確かに公開鍵証明書Ａの発行対象である仲介装置１０１から受信したものだと確認できる。そして、画像処理装置１００を正当な通信相手として認証する。

【００８３】

その後、ステップＳ３５で私有鍵Ｂを用いて第３の乱数を復号化する。ここまでの処理で、サーバ側とクライアント側に共通の第１乃至第３の乱数が共有されたことになる。そして、少なくとも第３の乱数は、生成した仲介装置１０１と、私有鍵Ｂを持つ画像処理装置１００以外の装置が知ることはない。ここまでの処理が成功すると、ステップＳ３６で仲介装置１０１に対して認証成功の応答を返す。

【００８４】

仲介装置１０１側では、これを受信すると、ステップＳ２７で第１乃至第３の乱数から共通鍵を生成し、以後の通信の暗号化に用いるものとして認証処理を終了する。画像処理装置１００側でも、ステップＳ３７で同様の処理を行って終了する。そして、以上の処理によって互いに通信を確立し、以後はステップＳ２７又はＳ３７で生成した共通鍵を用い、共通鍵暗号方式でデータを暗号化して通信を行う。

【００８５】

通信の際にこのようなＳＳＬによる相互認証を行えば、仲介装置１０１と画像処理装置１００とが互いに相手を認証した上で安全に共通鍵を交換することができ、通信を確かな相手と安全に行うことができる。以下の説明において、これらのいずれかの装置が通信相手に対してＳＳＬの接続要求を行う場合には、その要求に応じて図１４に示したような相互認証処理を行い、認証が成功した場合に通信を確立するものとする。ただし、図１４に

は仲介装置１０１から画像処理装置１００に対して接続を要求する場合の処理を示しているので、画像処理装置１００から仲介装置１０１に接続を要求する場合には、画像処理装置１００が図１４の仲介装置１０１に相当する処理を、仲介装置１０１が図１４の画像処理装置１００に相当する処理を行うことになる。

【００８６】

なお、片方向認証を採用し、例えば画像処理装置１００が仲介装置１０１を認証するのみでよいのであれば、図１４に示した認証処理において、第１及び第３の乱数の暗号化を省略することができる。この場合には、画像処理装置１００側にはルート鍵証明書のみを記憶させておけばよい。そして、認証処理は、図１５に示すように簡略化することができる。すなわち、仲介装置１０１側のステップＳ２２及びＳ２３の処理は不要となり、画像処理装置１００側のステップＳ３５の処理も不要となる。

逆に、仲介装置１０１が画像処理装置１００を認証するようにする場合、第２の乱数の暗号化を省略することができる。この場合には、仲介装置１０１側にはルート鍵証明書のみを記憶させておけばよい。そして、認証処理は、図１６に示すように簡略化することができる。すなわち、仲介装置１０１側のステップＳ２３及びＳ２４の処理は不要になる。

【００８７】

次に、図５に示した画像処理装置遠隔管理システムにおけるこの実施形態の特徴に関連する動作である、画像処理装置１００のファームウェア更新処理およびそのために必要な構成について説明する。この処理は、図１７のシーケンス図に示す処理であり、この発明のソフトウェア更新方法に係る処理であって、管理装置１０２，仲介装置１０１，画像処理装置１００の各ＣＰＵが、所要の制御プログラムを実行することによって行うものである。なお、仲介装置１０１がこの発明のソフトウェア更新装置として機能し、画像処理装置１００が被更新装置となる。そして、これらの装置によってこの発明のソフトウェア更新システムが実現され、管理装置１０２はこのソフトウェア更新システムにファームウェア更新要求を行う外部装置に該当する。

なお、図１７に示す処理を行うに先立って、仲介装置１０１には予め更新用ファームウェアを記憶させておくものとする。この記憶は、管理装置１０２その他の装置から転送して行ってもよいし、記録媒体に記録したものを仲介装置１０１に読み込ませることによって行ってもよい。その他の適当な方法を採ることもできる。

【００８８】

図５に示した画像処理装置遠隔管理システムにおいて、管理装置１０２は、所定時間毎あるいは管理装置１０２のオペレータから指示があった場合等、所定のイベントが発生した場合に、仲介装置１０１に対してファームウェア更新要求を送信する（Ｓ１０１）。図示は省略したが、この送信は、図１０を用いて説明したように仲介装置１０１からのポーリングに対する応答として行うようにすることができる。

仲介装置１０１は、この要求を受けると、画像処理装置１００のファーム更新に係る処理を開始するが、初めにワンタイムパスワード共有処理を行う（Ｓ１０２）。

【００８９】

この処理において、まずステップＳ１０２で仲介装置１０１がファーム更新時の認証処理に用いるための更新用認証情報としてワンタイムパスワードを乱数などにより生成し、これを記憶する。そして、画像処理装置１００に対してＳＳＬによる接続要求を行う（Ｓ１０３）。この接続が確立すると、画像処理装置１００にワンタイムパスワードを送信し、これを記憶するよう要求する（Ｓ１０４）。この要求は、ＳＯＡＰによるＲＰＣとして行うようにすることができる。

【００９０】

画像処理装置１００は、この要求に応じて受信したワンタイムパスワードを記憶手段に記憶し（Ｓ１０５）、以後ＦＴＰ接続の際の認証処理において、仲介装置１０１のＩＤと対応するパスワードとして用いるものとする。認証はＳＳＬの接続要求の際に完了しているので、ここではワンタイムパスワードを認証処理に用いることはない。そして、図示は省略したが、この記憶の終了後、画像処理装置１００はその旨の応答を仲介装置１０１に

返し、仲介装置１０１はこの応答を受け取るとＳＳＬの接続を切断する（Ｓ１０６）。ステップＳ１０３乃至Ｓ１０６の通信は、ＨＴＴＰＳを用いて行われる。

【００９１】

以上の処理がワンタイムパスワード共有処理であり、この処理において、仲介装置１０１のＣＰＵ５２が認証情報設定手段として機能する。そしてこの処理によって、仲介装置１０１と画像処理装置１００は、暗号化された通信経路を用いて安全にワンタイムパスワードを共有することができる。ここで用いたＳＳＬによる通信経路が、第１の通信経路である。なお、「通信経路」とは、物理的な伝送経路よりむしろ通信に使用するプロトコル（通信方式）によって定められるものである。従って、物理的な伝送経路が同一であっても通信プロトコルが異なれば「通信経路」は異なることになるし、逆にインターネットを介した通信のように物理的な伝送経路が状況に応じて変化する場合であっても、通信を行う装置と通信に使用するプロトコルが定まれば、「通信経路」は特定される。

【００９２】

ワンタイムパスワード共有処理が終了すると、仲介装置１０１は次にバージョン情報取得処理を行う。

この処理は、従来の技術の項で図２６に示した処理のステップＳ１１乃至Ｓ１３とほぼ同様なものであるが、仲介装置１０１がステップＳ１０７でＦＴＰによる接続を要求する際に画像処理装置１００に送信するパスワードは、ステップＳ１０４で送信したものと同じワンタイムパスワードである。そして、画像処理装置１００はステップＳ１０５で記憶したワンタイムパスワードを用いて認証処理を行う。これらが一致すれば認証成功として接続を確立し（Ｓ１０７）、一致しなかった場合には接続は確立されず、エラーとなって処理は終了する。この処理において、仲介装置１０１のＣＰＵ５２が認証要求手段として機能し、画像処理装置１００のＣＰＵが認証手段として機能する。

【００９３】

接続が確立されると、画像処理装置１００は仲介装置１０１からの要求に応じてファームのバージョン情報を送信する（Ｓ１０８）。仲介装置１０１はこのバージョン情報を取得し、その後、画像処理装置１００との接続を切断する（Ｓ１０９）。以上がバージョン情報取得処理である。

次のステップＳ１１０の処理及びその後のファーム送信処理も、ワンタイムパスワードを用いることを除き、図２６に示した処理のステップＳ１４乃至Ｓ１８とほぼ同様なものである。

【００９４】

すなわち、仲介装置１０１はステップＳ１０８で取得したファームのバージョン情報をもとに更新の要否を判断し、更新が必要と判断すれば（Ｓ１１０）、次のファーム送信処理を実行する。更新が不要と判断した場合には、管理装置１０２に対してファーム更新要求に対する応答としてその旨を通知するようにするとよい。

そして、ファーム送信処理では、仲介装置１０１はまずステップＳ１０７の場合と同様に画像処理装置１００にＩＤとワンタイムパスワードを送信し、画像処理装置１００が認証処理を行って、成功すればＦＴＰによる接続を確立する（Ｓ１１１）。そして、仲介装置１０１が更新用ファームウェアを画像処理装置１００に送信する（Ｓ１１２）。この処理において、仲介装置１０１のＣＰＵ５２が送信手段として機能する。

【００９５】

画像処理装置１００側では、これを受信すると、自機のファームウェアを受信した更新用ファームウェアに更新する（Ｓ１１３）。この処理においては、画像処理装置１００のＣＰＵが更新手段として機能する。そして、更新が完了すると自身をリセットし、再起動して新たなファームを有効にする（Ｓ１１４）。また、画像処理装置１００のリセットにより、ＦＴＰ接続は切断される。以上がファーム送信処理である。

ここで用いたＦＴＰによる通信経路が、第２の通信経路である。ＦＴＰの場合には、通信内容の暗号化を行わないので、処理負荷はＳＳＬを用いた第１の通信経路よりもはるかに小さい。

【００９６】
画像処理装置１００は、再起動が完了した時に、起動した旨を示す起動通知として電源ＯＮ通知を仲介装置１０１に対して送信するようにするとよい（Ｓ１１５）。このようにすれば、仲介装置１０１側で画像処理装置１００においてファームウェアの更新が終了したことを把握できるので、適切なタイミングで更新が成功したか否かの判断を行うことができる。また、電源ＯＮ通知は、ＳＯＡＰドキュメントとして記載し、ＨＴＴＰを用いて送信することができる。
【００９７】
そして、仲介装置１０１は、この電源ＯＮ通知を受信すると、ステップＳ１０７～Ｓ１０９の場合と同様にバージョン情報取得処理を行い、画像処理装置１００との間でＦＴＰによる通信を確立し、画像処理装置１００からファームのバージョン情報を取得する（Ｓ１１６～Ｓ１１８）。そして、このバージョン情報がステップＳ１１２で送信した更新用ファームウェアのものと一致していれば、ファームの更新が成功したと判断し（Ｓ１１９）、次のワンタイムパスワード消去処理を行う。一致していなければ、更新失敗と判断し、再度ファーム送信処理を行うか、あるいは管理装置１０２に対してファーム更新要求に対する応答として更新が失敗した旨を通知する。
なお、更新失敗と判断した場合であっても、画像処理装置１００との間でＳＳＬを用いた通信（ワンタイムパスワードを安全に送信可能な経路での通信）が可能であることが確認できた場合には、ワンタイムパスワード消去処理を行うようにしてもよい。
【００９８】
次のワンタイムパスワード消去処理においては、仲介装置１０１はワンタイムパスワード共有処理の場合と同様に画像処理装置１００に対してＳＳＬによる接続要求を行う（Ｓ１２０）。そして、この接続が確立すると、画像処理装置１００に消去用パスワードを送信し、これを記憶するよう要求する（Ｓ１２１）。この要求は、いわばワンタイムパスワードの無効化要求であり、この処理において、仲介装置１０１のＣＰＵ５２が認証情報無効化手段として機能する。なお、消去用パスワードは、送信毎に作成するランダムなものであってもよいし、固定のパスワードでもよい。ＦＴＰによって送信しておらず、その後もＦＴＰでは送信しないパスワードを用いればよい。また、この要求を行う際に、自身で記憶しているワンタイムパスワードも消去するようにしてもよい。
なお、ワンタイムパスワードの無効化要求は、記憶しているワンタイムパスワードを消去する要求であればよいのであるが、上述のようにパスワードの記憶（上書き）要求を用いるようにすれば、ワンタイムパスワードの共有の場合と処理を共通化し、プログラムのコンパクト化を図ると共に開発効率を向上させることができる。
【００９９】
画像処理装置１００は、この要求に応じてワンタイムパスワードを受信した消去用パスワードで上書きし（Ｓ１２２）、以後ステップＳ１０５で記憶したワンタイムパスワードはＦＴＰ接続の際の認証処理に用いないようにする。認証はＳＳＬの接続要求の際に完了しているので、ここで消去用パスワードを認証処理に用いることはない。この記憶の終了後、仲介装置１０１はＳＳＬの接続を切断する（Ｓ１２３）。
以上の処理がワンタイムパスワード消去処理であり、この処理によって、画像処理装置１００に記憶させたワンタイムパスワードを無効化することができる。
このワンタイムパスワード消去処理が終了すると、仲介装置１０１は、管理装置１０２に対してファーム更新要求に対する応答として更新が成功した旨を通知する（Ｓ１２４）。
以上の処理を行うことにより、ネットワークを介して通信可能な被更新装置のファームウェアをソフトウェア更新装置によって更新することができる。
【０１００】
この処理をフローチャートで示したものが図１８乃至図２０である。これらの図を用いて上述の処理についての説明を補足する。これらの図において、２本のフローチャート間の矢印は、データの転送を示し、送信側は矢印の根元のステップで転送処理を行い、受信

側はその情報を受信すると矢印の先端のステップの処理を行うものとする。
仲介装置１０１は、管理装置１０２からファーム更新要求を受け取ると、図１８の左側に示すフローチャートの処理を開始する。そして、ステップＳ２０１でワンタイムパスワードを生成して記憶し、ステップＳ２０２で画像処理装置１００に対してＳＳＬによる接続要求を行う。
【０１０１】
画像処理装置１００は、この要求を受け取ると図１８の右側に示すフローチャートの処理を開始する。そして、ステップＳ３０１で仲介装置１０１側とＳＳＬによる接続処理を行う。仲介装置１０１側のステップＳ２０２と画像処理装置１００側のステップＳ３０１で行う処理が、図１４に示した相互認証処理である。
認証が成功すると、画像処理装置１００は図１４のステップＳ３６のように認証成功の応答を返す。すると、仲介装置１０１はステップＳ２０３で画像処理装置１００にステップＳ２０１で生成したワンタイムパスワードを送信し、記憶するよう要求する。画像処理装置１００はこれを受け取ると、ステップＳ３０２で記憶し、記憶完了の応答を返す。仲介装置１０１は、この応答があるとステップＳ２０４で画像処理装置１００に切断要求を送ってＳＳＬによる接続を切断する。この要求を受けた仲介装置１０１もステップＳ３０３で接続を切断する。ここまでの処理がワンタイムパスワード共有処理である。
【０１０２】
次に、仲介装置１０１は、ステップＳ２０５で画像処理装置１００に対してＦＴＰの接続要求を行う。すると、画像処理装置１００はステップＳ３０４で認証のためのＩＤとパスワードを要求するので、仲介装置１０１はこれに応じてステップＳ２０６でＩＤとステップＳ２０１で生成したワンタイムパスワードを送信する。
画像処理装置１００はこのＩＤとパスワードを用いて認証処理を行い、これらが記憶しているものと一致すれば認証成功としてその旨の応答を返す。そして、これを受けた仲介装置１０１は、ステップＳ２０７で画像処理装置１００に対してバージョン情報取得要求を送信してファームのバージョン情報を求める。画像処理装置１００はこれに応じてステップＳ３０６で仲介装置１０１にバージョン情報を送信し、仲介装置１０１はこれを取得するとステップＳ２０８でＦＴＰ接続を切断する。ここまでの処理がバージョン情報取得処理である。
なお、ステップＳ３０５で認証が失敗した場合には、ステップＳ３０７に進んでエラー処理を行うが、この処理としては、仲介装置１０１に認証失敗を通知して再度接続要求を待つ状態に移行することが考えられる。
図示は省略したが、ステップＳ３０１等でＳＳＬによる相互認証が失敗した場合にも、同様な処理を行うようにするとよい。
【０１０３】
一方仲介装置１０１は、ステップＳ２０８の次にステップＳ２０９に進み、ステップＳ２０７で取得したバージョン情報が最新バージョンのものか否かをもとに、画像処理装置１００のファームを更新する必要があるか否か判断する。そして、更新する必要があれば、ステップＳ２１０に進んでファーム送信処理を行う。
この場合、仲介装置１０１はステップＳ２１０でステップＳ２０５及びＳ２０６と同様な処理を、画像処理装置１００はステップＳ３０８でステップＳ３０４及びＳ３０５と同様な処理を行ってＦＴＰ接続を確立する。ここで用いるパスワードも、ステップＳ２０６の場合と同じワンタイムパスワードである。
【０１０４】
接続が確立すると、仲介装置１０１はステップＳ２１１で画像処理装置１００に更新用ファームウェアを送信し、画像処理装置１００はステップＳ３０９でこれを受信すると、ステップＳ３１０で自機のファームウェアをその更新用ファームウェアに更新する。このとき、他のジョブが実行中であったり、予約されていたりした場合には、それが完了するまでは更新せずに待機するようにしてもよい。ファームウェアの更新が完了すると、画像処理装置１００はステップＳ３１１で自身をリセットし、再起動して新たなファームを有

効にする。また、画像処理装置１００のリセットにより、ＦＴＰ接続は切断される。以上がファーム送信処理である。

【０１０５】

続いて、画像処理装置１００の再起動が完了すると、画像処理装置１００は起動したことを示す電源ＯＮ通知を仲介装置１０１に送信する。すると、仲介装置１０１はこれに応じてステップＳ２１２で画像処理装置１００に対してＦＴＰによる通信を要求し、以下ステップＳ２１４までで、ステップＳ２０５～Ｓ２０８と同様な処理を行って画像処理装置１００からファームのバージョン情報を取得する。画像処理装置側でも、ステップＳ３１３及びＳ３１４で、ステップＳ３０４乃至Ｓ３０７の場合と同様な処理を行ってファームのバージョン情報を送信する。

【０１０６】

そして、仲介装置１０１はステップＳ２１５で、ステップＳ２１３で取得したバージョン情報と、ステップＳ２１１で送信した更新用ファームウェアのバージョン情報を比較し、一致していれば更新成功と判断して図２０のステップＳ２１７に進む。一致していなければ、更新失敗と判断してステップＳ２１６に進み、エラー処理を行う。このエラー処理としては、再度Ｓ２１０からのファーム送信処理を行って画像処理装置１００のファームウェアの更新を試みたり、あるいはファーム更新要求の送信元である管理装置１０２に対して、更新が失敗した旨の応答を返したりするとよい。後者の場合には、処理を終了し、再度のファーム更新要求を待つことになる。

【０１０７】

ステップＳ２１５の判断がＹＥＳであり、図２０のステップＳ２１７に進むと、ワンタイムパスワード無効化処理を開始し、仲介装置１０１はステップＳ２０２の場合と同様に画像処理装置１００に対してＳＳＬによる接続処理を行い、画像処理装置１００側のステップＳ３１５の処理と併せて相互認証を行う。そして、画像処理装置１００側から認証成功の応答が返されると、仲介装置１０１はステップＳ２１８で画像処理装置１００に対して消去用パスワードを送信し、これを記憶するよう要求する。画像処理装置１００はこれを受け取ると、ステップＳ３１６で記憶していたワンタイムパスワードに消去用パスワードを上書き記憶し、記憶完了の応答を返す。仲介装置１０１は、この応答があるとステップＳ２１９で画像処理装置１００に切断要求を送ってＳＳＬによる接続を切断する。この要求を受けた仲介装置１０１もステップＳ３１７で接続を切断する。ここまでの処理がワンタイムパスワード無効化処理である。

なお、この処理において、記憶しているワンタイムパスワードを消去できるのであれば必ずしも上書きをしなくてもよいことは、上述した通りである。

【０１０８】

この処理は、消去用パスワードを必ずしも毎回生成する必要がない点を除けば、ワンタイムパスワード共有処理と同様なものである。しかし、このような処理によって、画像処理装置１００がＦＴＰの認証処理に用いるパスワードを別のパスワードに変更すれば、漏洩の危険性がある元のワンタイムパスワードを無効化でき、第３者によるなりすましを防止できる。また、消去用パスワードはＦＴＰでは転送せず、例えばＳＳＬを用いた安全な通信経路で転送するようにすれば、これが漏洩することもない。

【０１０９】

ワンタイムパスワード無効化処理の後、仲介装置１０１はステップＳ２２０で管理装置１０２にファームウェア更新についての結果を通知し、処理を終了する。

なお、ステップＳ２０９でファームの更新が不要と判断した場合には、そのまま図２０のステップＳ２１７に進んでワンタイムパスワード無効化処理を行い、ステップＳ２２０で管理装置１０２に結果を通知して終了する。画像処理装置１００側の処理は、基本的に仲介装置１０１からのトリガに応じて行うので、ステップＳ２１０やステップＳ２１２での要求がなければ、画像処理装置１００は図１９に示した部分の処理は行わない。

【０１１０】

以上説明したような処理を行うことにより、ネットワークを介して通信可能な被更新装

置のファームウェアをソフトウェア更新装置によって更新する場合において、高い安全性を確保しながらコンパクトなプログラムによって更新処理を行うことができる。更新の対象がファームウェア以外のソフトウェアでも同様であることは、上述した通りである。

すなわち、まずソフトウェアの更新に必須のバージョン情報取得処理及びソフトウェア送信処理は処理負荷の小さいＦＴＰによって行うようにしているので、プログラムをコンパクトにまとめることができる。ソフトウェア自体は、パスワード等の認証情報や被管理装置の利用者情報等に比べて機密性の高いデータではないので、ＦＴＰなどの暗号化を行わない通信で問題なく、むしろ処理負荷を低減してプログラムをコンパクトにする要求が強いのである。また、ソフトウェアは、パスワード等の認証情報に比べてサイズが大きいため、これを処理負荷の小さい通信経路で送信するようにすることにより、処理負荷を大きく低減することができる。

【０１１１】

一方で、不正なソフトウェアを受信しないようにするためには、通信相手の認証が重要となるが、ＦＴＰでの認証処理に使用するパスワードは、使用する直前に生成して、通信内容を暗号化するＳＳＬを用いて仲介装置１０１と画像処理装置１００とが共有するようにしている。従って、このパスワードが第３者に漏洩することはなく、第３者が仲介装置１０１になりすまして別の装置から画像処理装置１００に不正なソフトウェアを送信し、これに更新させてしまうといった事態を防止できる。

また、ＦＴＰでの認証処理に使用したパスワードを、ソフトウェアの更新成功を確認した後にただちに無効化してしまうようにすれば、第３者がＦＴＰによる通信をモニタリングしてワンタイムパスワードを不正に取得したとしても、後日そのパスワードを用いて接続される可能性はなく、不正なアクセスを防止することができる。

【０１１２】

また、ソフトウェア更新後に画像処理装置１００が再起動した時点でソフトウェアのバージョン情報を確認するようにすれば、仲介装置１０１側で更新の成否を容易に知ることができる。そして、失敗していた場合に速やかに再更新等の対応を行うことができる。画像処理装置１００が再起動時に電源ＯＮ通知を仲介装置１０１に送信するようにすれば、容易にこの確認のタイミングを計ることができる。

さらにまた、仲介装置１０１が外部からの要求に応じて画像処理装置１００にソフトウェアを更新させ、その結果を応答として返すようにすれば、各画像処理装置１００におけるソフトウェアの更新状況を管理装置１０２等によって管理することができる。

【０１１３】

また、特にファームウェアの更新を考慮した場合には、ファームウェアはハードウェアの基本的な制御を行うためのソフトウェアを含むため、ファームウェア自身に更新機能を設けた場合、更新に失敗すると装置が全く動作しなくなる恐れがある。そこで、このような事態を避けるため、更新処理用の更新プログラムを別途用意し、これ以外の部分のみのファームウェアを更新することが行われている。そして、このようにした場合、ファームウェア更新時以外の通常動作時に使用しない更新プログラムのために大きな記憶容量を使用することは、コスト面等を考慮すると妥当でない。従って、更新プログラムはできるだけ容量が小さいものが好ましいという要求がある。そこで、以上説明したような更新処理を行うようにすることにより、更新に直接必要な処理を、例えばＦＴＰのようにコンパクトなプログラムを用いて実現できるので、更新プログラムの容量を低減し、このような要求を満たすことができる。

【０１１４】

また、ファームウェアの場合、更新に失敗した場合に備えて、被更新装置にはファームウェア自体の他にファームウェア更新処理用の更新プログラムを備えることは上述の通りであるが、上述の処理において、ファームウェアの更新に失敗した場合にはワンタイムパスワードを無効化しないようにしておけば、更新に失敗したとしても、ＳＳＬを使用しないバージョン情報取得処理からやり直すことができるので、画像処理装置１００における更新プログラムとして用意するのは、バージョン情報取得処理及びファームウェア送信処

理のためのプログラムのみでよい。従って、パスワードの受け渡しにＳＳＬを使用して安全性を向上させながら、この処理に必要な部分を更新プログラムに含める必要がなく、更新プログラムをコンパクトにすることができる。

【０１１５】

なお、ワンタイムパスワードの無効化について、上述した処理では、これを消去用パスワードの上書きによって行うようにすることにより、ワンタイムパスワードの共有の場合と処理を共通化し、プログラムのコンパクト化を図っている。

しかし、消去用パスワードの上書き要求に代えて、単に記憶しているワンタイムパスワードを認証処理に用いないようにする要求を行い、画像処理装置がこれに応じてワンタイムパスワードによる認証処理を行わない旨の設定を行うようにしてもよい。このようにする場合、要求自体を秘匿する必要はないので、必ずしもＳＳＬによる通信を行う必要はない。画像処理装置１００から消去用パスワードが盗まれる危険性を考慮するのであれば、このような設定が有効になる。

【０１１６】

〔変形例〕

以下、上述した実施形態に適用できる種々の変形例について説明する。

以上説明した実施形態においては、仲介装置１０１が管理装置１０２からファーム更新要求を受けた場合にファームの更新処理を開始し、この際に仲介装置１０１がワンタイムパスワードを生成する例について説明した。しかし、この発明に係るファームの更新処理は、これに限られるものではない。

【０１１７】

まず、第１の変形例として、ワンタイムパスワードの生成を画像処理装置１００側で行うようにしてもよい。この場合、図１７のステップＳ１０１乃至Ｓ１０６の処理に代えて、図２１に示す処理を行う。

すなわち、仲介装置１０１がステップＳ１０１でファーム更新要求を受けると、画像処理装置１００のファーム更新に係る処理を開始するが、初めに画像処理装置１００に対してワンタイムパスワード生成要求を送信する（Ｓ４０１）。この要求自体は特に秘匿する必要はないので、ＳＯＡＰドキュメントとしてＨＴＴＰによって送信することができる。

【０１１８】

そして、画像処理装置１００はこれに応じてワンタイムパスワードを生成し、これを記憶する（Ｓ４０２）。そしてこのワンタイムパスワードを、以後ＦＴＰ接続の際の認証処理において、ワンタイムパスワード生成要求の送信元である仲介装置１０１のＩＤと対応するパスワードとして用いるものとする。

その後、画像処理装置１００は仲介装置１０１に対してＳＳＬによる接続要求を行う（Ｓ４０３）。この接続が確立すると、仲介装置１０１にワンタイムパスワードを送信し、これを記憶するよう要求する（Ｓ４０４）。この要求は、ＳＯＡＰによるＲＰＣとしてなされる。

【０１１９】

仲介装置１０１は、この要求に応じて受信したワンタイムパスワードを記憶手段に記憶し（Ｓ４０５）、以後ＦＴＰ接続の際の認証処理において、このワンタイムパスワードを送信するものとする。そして、図示は省略したが、この記憶の終了後、仲介装置１０１はその旨の応答を画像処理装置１００に返し、画像処理装置１００はこの応答を受け取るとＳＳＬの接続を切断する（Ｓ４０６）。ステップＳ４０３乃至Ｓ４０６の通信は、ＨＴＴＰＳを用いて行われる。

そして、ステップＳ４０２乃至Ｓ４０６の処理において、画像処理装置１００のＣＰＵが認証情報設定手段として機能する。

このような処理によっても、図１７に示した処理の場合と同様に、仲介装置１０１と画像処理装置１００が暗号化された通信経路を用いて安全にワンタイムパスワードを共有することができる。従って、図１７に示した処理を行う場合と同様な効果を得ることができる。

【０１２０】
　また、第２の変形例として、画像処理装置１００が、操作パネル２０５等から直接ファームウェアの更新指示を受け付けることができるようにしてもよい。この場合、図１７のステップＳ１０１乃至Ｓ１０６の処理に代えて、図２２に示す処理を行う。
　すなわち、画像処理装置１００がファームウェアの更新指示を受け付けた場合（Ｓ４１１）、画像処理装置１００のファーム更新に係る処理を開始し、仲介装置１０１に対してワンタイムパスワード生成要求を送信するようにする（Ｓ４１２）。そして仲介装置１０１は、この要求を受け取ると、図１７に示した処理で管理装置１０２からファーム更新要求を受け取った場合と同様に、ワンタイムパスワード共有処理を行う。すなわち、ステップＳ４１３～Ｓ４１７では、図１７のステップＳ１０２～Ｓ１０６と同様な処理を行う。
【０１２１】
　このようにすれば、画像処理装置１００が直接ファームウェアの更新指示を受け付けた場合でも、管理装置１０２からファーム更新要求があった場合と同様に画像処理装置１００のファームウェアを更新することができる。
　なお、この変形例では管理装置１０２からのファーム更新要求はないが、管理装置１０２が特定できるのであれば、ステップＳ１２４の更新結果通知は行うようにするとよい。このようにすれば、管理装置１０２は自身以外からの指示によるファームの更新状況も把握でき、適切な管理を行うことができる。
　また、仲介装置１０１がOp-Port５６に接続する操作部から直接ファームウェアの更新指示を受け付け、これに応じて画像処理装置１００のファーム更新に係る処理（ワンタイムパスワード共有処理以降の処理）を開始できるようにしてもよい。
【０１２２】
　第３の変形例としては、第１の変形例と第２の変形例を組み合わせることが考えられる。すなわち、画像処理装置１００が、直接ファームウェアの更新指示を受け付け、さらにワンタイムパスワードの生成を画像処理装置１００側で行うようにするのである。
　この場合、図１７のステップＳ１０１乃至Ｓ１０６の処理に代えて、図２３に示す処理を行う。
【０１２３】
　この処理は、ステップＳ４１１の処理は図２２の場合と同様であり、ステップＳ４０２～Ｓ４０６の処理は図２１の場合と同様であるので、詳細な説明は省略するが、この場合には、仲介装置１０１は、ステップＳ４０４でワンタイムパスワードの記憶要求があった時点で画像処理装置１００のファーム更新に係る処理が開始されたものと認識し、以後の処理を行うものとする。
　この変形例の効果は、第１の変形例の効果と第２の変形例の効果を合わせたものになる。
【０１２４】
　第４の変形例としては、ワンタイムパスワード消去処理において、消去用パスワードの記憶要求を画像処理装置１００側から行うようにすることができる。この場合、図１７のステップＳ１２０乃至Ｓ１２３の処理に代えて、図２４に示す処理を行う。
　すなわち、画像処理装置１００がまず図２２のステップＳ４１２の場合と同様に仲介装置１０１に対してＳＳＬによる接続要求を行う（Ｓ４２１）。そして、この接続が確立すると、仲介装置１０１に消去用パスワードを送信し、これを記憶するよう要求する（Ｓ４２２）。この要求は、いわばワンタイムパスワードの無効化要求であり、この処理において、画像処理装置１００のＣＰＵが認証情報無効化手段として機能する。
【０１２５】
　仲介装置１０１は、この要求に応じてワンタイムパスワードを受信した消去用パスワードで上書きし（Ｓ４２３）、それまで記憶していたワンタイムパスワードは以後ＦＴＰ接続の際に送信しないようにする。一方、画像処理装置１００自身も、記憶しているワンタイムパスワードを消去用パスワードで上書きし（Ｓ４２４）、それまで記憶していたワンタイムパスワードは以後ＦＴＰ接続の際の認証処理に用いないようにする。これらの記憶

の終了後、画像処理装置１００はＳＳＬの接続を切断する（Ｓ４２５）。
この変形例は、上述した実施形態及び各変形例に適用できるが、第１及び第３の変形例のように、画像処理装置１００側でワンタイムパスワードを生成する場合に適用すると、ＳＳＬによるパスワードの送信処理を画像処理装置１００側に統一できてプログラムの簡略化に効果的である。
なお、この変形例を適用する場合、仲介装置１０１が、図１７のステップＳ１１９でファームの更新が成功したと判断した場合に画像処理装置１０１に対してその旨を通知するようにし、画像処理装置１０１がその通知を受け取った場合に図２４に示す処理を開始するようにするとよい。

【０１２６】
また、以上の実施形態及び各変形例においては、被更新装置の例として通信機能を備えた画像処理装置について主に説明したが、この発明はこれに限られるものではなく、通信機能を備えたネットワーク家電，自動販売機，医療機器，電源装置，空調システム，ガス・水道・電気等の計量システム等や、ネットワークに接続可能な汎用コンピュータ，自動車，航空機等も含め、通信機能を備えた各種電子装置に適用可能である。

【０１２７】
例えば、図１に示した遠隔管理システムにおいて、これらの各装置を被管理装置（被更新装置）とし、図２５に示すような遠隔管理システム及び証明書設定システムを構成することが考えられる。この図においては、仲介装置１０１を別途設ける被管理装置の例としてテレビ受像機１２ａや冷蔵庫１２ｂのようなネットワーク家電、医療機器１２ｃ，自動販売機１２ｄ，計量システム１２ｅ，空調システム１２ｆを挙げている。そして、仲介装置１０１の機能を併せ持つ被管理装置の例として、自動車１３ａや航空機１３ｂを挙げている。また、自動車１３ａや航空機１３ｂのように広範囲を移動する装置においては、ファイアウォール（ＦＷ）１０４の機能も併せ持つようにすることが好ましい。
このような遠隔管理システムにおいて被管理装置となる各装置のソフトウェアを更新する場合にも、この発明はもちろん適用可能である。

【０１２８】
また、ソフトウェア更新装置についても、図１、図３及び図２５等に示した仲介装置に限られるものではなく、ソフトウェア更新の専用装置であったり、あるいは管理装置１０２であってもよい。
さらに、この発明のソフトウェア更新システムは、必ずしも遠隔管理システムに含まれるものとは限らず、また、被更新装置，ソフトウェア更新装置，管理装置の構成及びこれらの接続形式は、以上の実施形態に限られるものではない。これらの各装置の間の通信も、有線，無線を問わず、ネットワークを構築可能な各種通信回線（通信経路）を用いて行うことができる。

【０１２９】
また、通信経路について、第１の通信経路としてＳＳＬによる通信経路、第２の通信経路としてＦＴＰによる通信経路を用いた例について説明したが、これに限られるものではなく、第１の通信経路が送信すべきデータを暗号化して送信するものであり、第２の通信経路が第１の通信経路よりも処理負荷の小さいものであれば、他のプロトコルを使用した通信経路（通信方式）であっても構わない。このとき、第２の通信経路を、送信すべきデータを暗号化しないで送信する通信経路とすることにより、処理負荷を低減することが考えられる。また、更新装置が被更新装置に更新用認証情報を送信して認証を要求する際の通信経路が、更新用ソフトウェアの転送に使用する第２の通信経路と異なるもの、例えば認証用の独自プロトコルによる通信経路であってもよい。
さらに、以上説明した変形を適宜組み合わせて適用してよいことも、もちろんである。

【０１３０】
また、この発明によるプログラムは、ネットワークを介して被更新装置と通信可能なソフトウェア更新装置を制御するコンピュータに、上述した各機能（認証情報設定手段，認証要求手段，送信手段，その他の手段としての機能）を実現させるためのプログラムであ

り、このようなプログラムをコンピュータに実行させることにより、上述したような効果を得ることができる。

【０１３１】

このようなプログラムは、はじめからコンピュータに備えるＲＯＭあるいはＨＤＤ等の記憶手段に格納しておいてもよいが、記録媒体であるＣＤ－ＲＯＭあるいはフレキシブルディスク，ＳＲＡＭ，ＥＥＰＲＯＭ，メモリカード等の不揮発性記録媒体（メモリ）に記録して提供することもできる。そのメモリに記録されたプログラムをコンピュータにインストールしてＣＰＵに実行させるか、ＣＰＵにそのメモリからこのプログラムを読み出して実行させることにより、上述した各手順を実行させることができる。

さらに、ネットワークに接続され、プログラムを記録した記録媒体を備える外部機器あるいはプログラムを記憶手段に記憶した外部機器からダウンロードして実行させることも可能である。

【産業上の利用可能性】

【０１３２】

以上説明してきたように、この発明のソフトウェア更新装置、ソフトウェア更新システム、ソフトウェア更新方法、またはプログラムによれば、ネットワークを介して通信可能な被更新装置のソフトウェアをソフトウェア更新装置によって更新する場合において、高い安全性を確保しながら更新処理の負荷を低減することができる。

従って、この発明を適用することにより、例えばユーザに販売した通信装置のソフトウェアを安全かつ容易に更新可能とするようなシステムを提供することができる。

【図面の簡単な説明】

【０１３３】

【図１】この発明によるソフトウェア更新システムを含む遠隔管理システムの構成例を示す概念図である。

【図２】その遠隔管理システムにおけるデータ送受モデルを示す概念図である。

【図３】その遠隔管理システムを構成する仲介装置のハードウェア構成例を示すブロック図である。

【図４】その仲介装置のソフトウェア構成例を示すブロック図である。

【図５】画像処理装置を被更新装置としたこの発明によるソフトウェア更新システムを含む、画像処理装置遠隔管理システムの構成例を示す概念図である。

【図６】その画像処理装置遠隔管理システムを構成する画像処理装置のハードウェア構成例を示すブロック図である。

【図７】その画像処理装置のソフトウェア構成例を示すブロック図である。

【図８】その画像処理装置におけるＥＮＧＲＤＹ信号とＰＷＲＣＴＬ信号について説明するための図である。

【図９】その画像処理装置におけるウェブサービスアプリの構成例を示す機能ブロック図である。

【図１０】図３に示した画像処理装置遠隔管理システム内で行われるデータ送受信の際の通信シーケンスの一例を示す図である。

【０１３４】

【図１１】図３に示した画像処理装置から管理装置１０２へデータを送信する場合の通信シーケンスの一例を示す図である。

【図１２】図３に示した仲介装置によって画像処理装置のファームウェアを更新する処理の参考例に用いるパスワードリストの例を示す図である。

【図１３】その参考例のファームウェア更新処理を示すシーケンス図である。

【図１４】図３に示した仲介装置と画像処理装置との間でＳＳＬを用いた相互認証を行う際の処理例を示す図である。

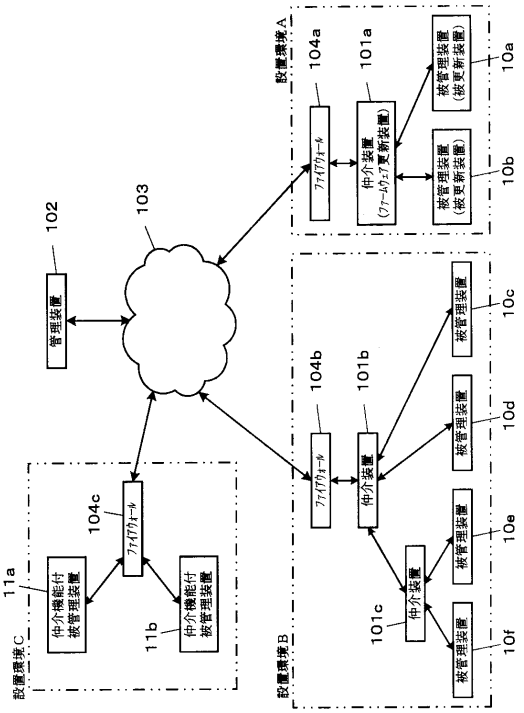
【図１５】同じく片方向認証を行う際の処理例を示す図である。

【図１６】その別の例を示す図である。

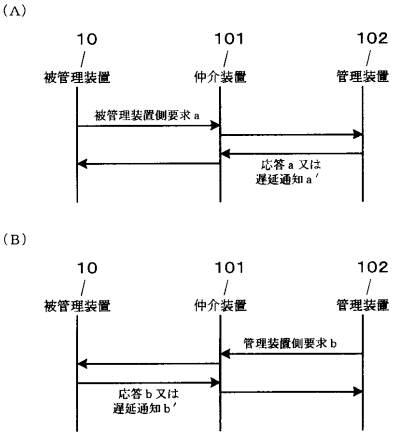
【図１７】図３に示した仲介装置によって画像処理装置のファームウェアを更新する際の

処理例を示すシーケンス図である。
【図１８】図３に示した仲介装置によって画像処理装置のファームウェアを更新する際の処理例の一部を示すフローチャートである。
【図１９】図１８の続きの処理を示すフローチャートである。
【図２０】図１９の続きの処理を示すフローチャートである。
【０１３５】
【図２１】図１７に示した処理の第１の変形例において図１７の処理と入れ替える部分の処理例を示すシーケンス図である。
【図２２】同じく第２の変形例において図１７の処理と入れ替える部分の処理例を示すシーケンス図である。
【図２３】同じく第３の変形例において図１７の処理と入れ替える部分の処理例を示すシーケンス図である。
【図２４】同じく第４の変形例において図１７の処理と入れ替える部分の処理例を示すシーケンス図である。
【図２５】図１に示した遠隔管理システムの別の構成例を示す図である。
【図２６】従来のファームウェア更新システムにおけるファームウェア更新処理の例を示すシーケンス図である。
【図２７】図２６に示した処理の危険性について説明するための図である。
【符号の説明】
【０１３６】
１０：被管理装置　　１１：仲介機能付被管理装置
５２：ＣＰＵ　　５３：ＳＤＲＡＭ
５４：フラッシュメモリ　　５５：ＲＴＣ
５６：0p-Port　　５７：ＰＨＹ
５８：モデム　　５９：ＨＤＤ制御部
６３：ＨＤＤ　　７０：アプリケーション層
８０：サービス層　　９０：プロトコル層
１００：画像処理装置　　１０１：仲介装置
１０２：管理装置　　１０３：インタネット
１０４：ファイアウォール　１０５：端末装置
１１０：仲介機能付画像処理装置
２００：コントローラボード　２０１：ＨＤＤ
２０２：ＮＶ－ＲＡＭ　　２０３：ＰＩボード
２０４：ＰＨＹ　　２０５：操作パネル
２０６：プロッタ／スキャナエンジンボード
２０７：電源ユニット　　２１２：ＰＣＩ－ＢＵＳ
３００：ＯＣＳ　　３０１：ＥＣＳ
３０２：ＭＣＳ　　３０３：ＮＣＳ
３０４：ＦＣＳ　　３０５：ＣＳＳ
３０６：ＳＣＳ　　３０７：ＳＲＭ
３０８：ＩＭＨ　　３０９：コピーアプリ
３１０：ファクスアプリ　３１１：プリンタアプリ
３１２：スキャナアプリ
３１３：ネットファイルアプリ　３１４：ウェブアプリ
３１５：ＮＲＳアプリ　　３１６：ＤＣＳ
３１７：ＵＣＳ　　３１８：ＤＥＳＳ
３１９：ＣＣＳ

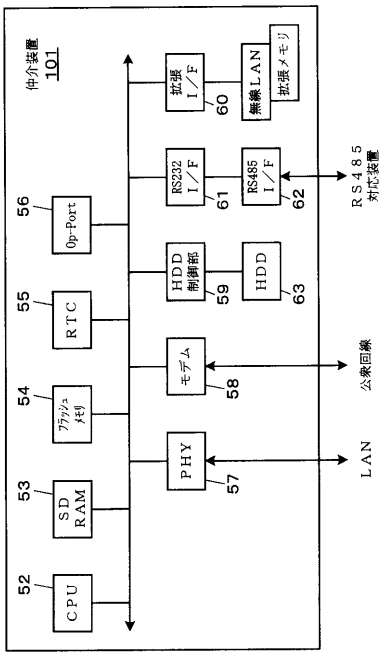
【図１】


設置環境A
設置環境B
設置環境C
管理装置
102
103
ファイアウォール
104a
104b
104c
仲介装置
101a
101b
101c
仲介装置
(ファームウェア更新装置)
被管理装置
(被更新装置)
10a
10b
10c
10d
10e
10f
11a
11b
仲介機能付
被管理装置

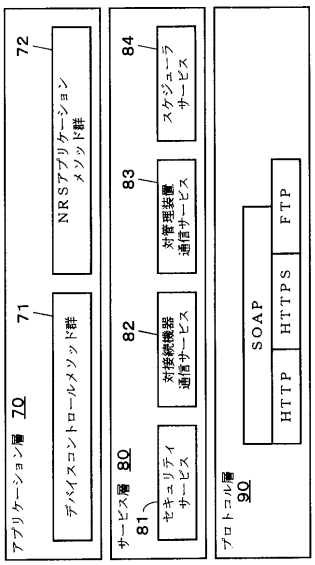
【図２】


(A)
10
101
102
被管理装置
仲介装置
管理装置
被管理装置側要求 a
応答 a 又は
遅延通知 a'
(B)
10
101
102
被管理装置
仲介装置
管理装置
管理装置側要求 b
応答 b 又は
遅延通知 b'

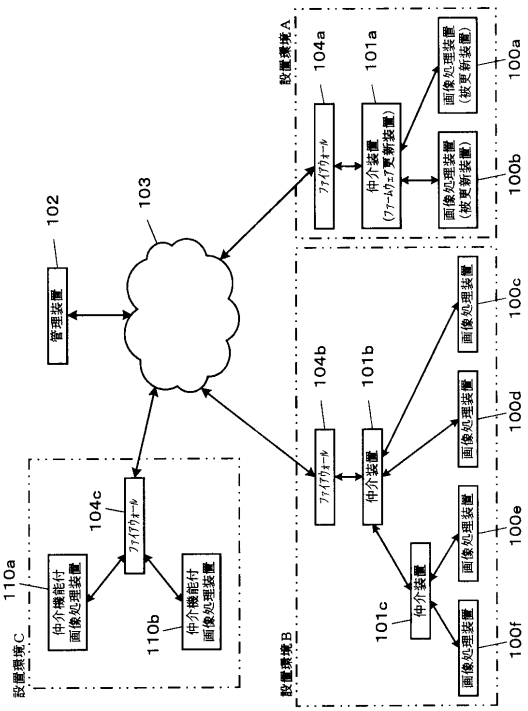
【図３】


仲介装置
101
CPU
52
SD
RAM
53
フラッシュ
メモリ
54
RTC
55
Op-Port
56
PHY
57
モデム
58
HDD
制御部
59
拡張
I／F
60
RS232
I／F
61
RS485
I／F
62
HDD
63
無線LAN
拡張メモリ
RS485
対応装置
公衆回線
LAN

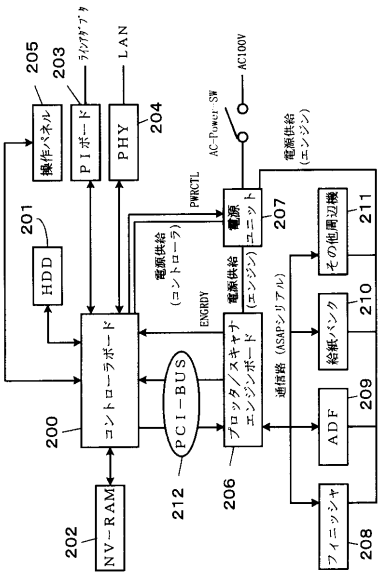
【図４】


アプリケーション層 70
71
デバイスコントロールメソッド群
72
NRSアプリケーション
メソッド群
サービス層 80
81
セキュリティ
サービス
82
対接続機器
通信サービス
83
対管理装置
通信サービス
84
スケジューラ
サービス
プロトコル層
90
SOAP
HTTP
HTTPS
FTP

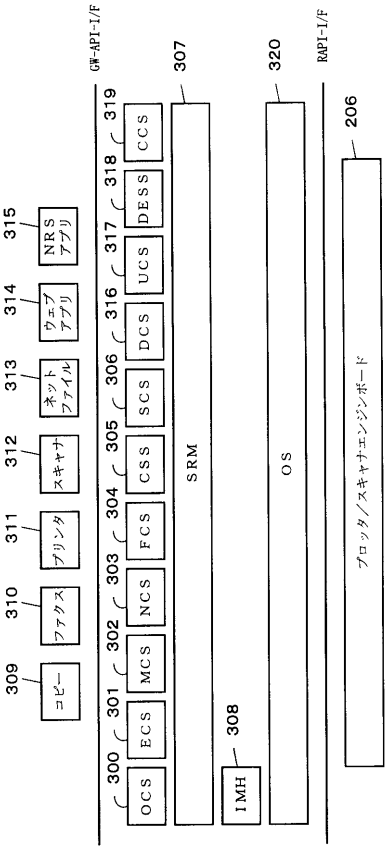
【図５】


設置環境A
設置環境B
設置環境C
管理装置
102
103
ファイアウォール
104a
104b
104c
仲介装置
101a
101b
101c
仲介装置
(ファームウェア更新装置)
画像処理装置
(版更新装置)
100a
100b
100c
100d
100e
100f
110a
110b
仲介機能付
画像処理装置

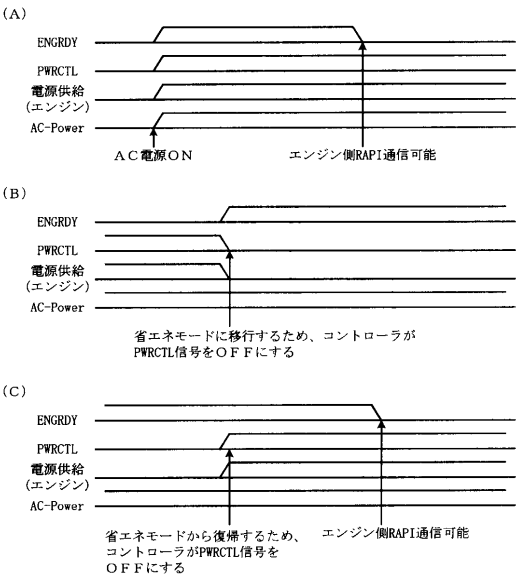
【図６】


操作パネル
205
203
PHY
204
LAN
AC100V
AC-Power SW
電源
ユニット
207
電源供給
(エンジン)
HDD
201
PWRCTL
電源供給
(コントローラ)
ENGRDY
コントローラボード
200
PCI-BUS
212
プロッタ/スキャナ
エンジンボード
206
通信路 (ASAPシリアル)
その他周辺機
211
給紙バンク
210
ADF
209
フィニッシャ
208
NV-RAM
202

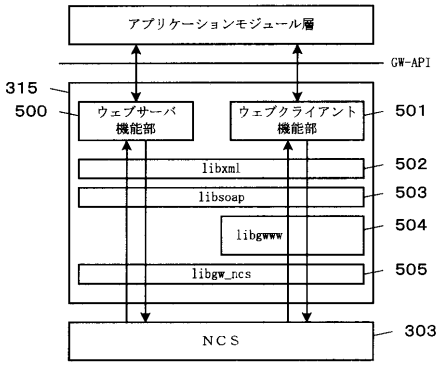
【図７】


GW-API-I/F
RAPI-I/F
307
320
206
SRM
OS
プロッタ/スキャナエンジンボード
IMH
308
OCS
ECS
MCS
NCS
FCS
CSS
SCS
DCS
UCS
DESS
CCS
300
301
302
303
304
305
306
316
317
318
319
コピー
ファクス
プリンタ
スキャナ
ネットファイル
ウェブアプリ
NRSアプリ
309
310
311
312
313
314
315

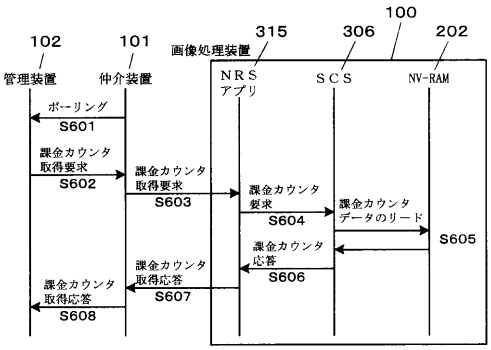
【図８】


(A)
ENGRDY
PWRCTL
電源供給
(エンジン)
AC-Power
AC電源ON
エンジン側RAPI通信可能
(B)
ENGRDY
PWRCTL
電源供給
(エンジン)
AC-Power
省エネモードに移行するため、コントローラが
PWRCTL信号をOFFにする
(C)
ENGRDY
PWRCTL
電源供給
(エンジン)
AC-Power
省エネモードから復帰するため、
コントローラがPWRCTL信号を
OFFにする
エンジン側RAPI通信可能

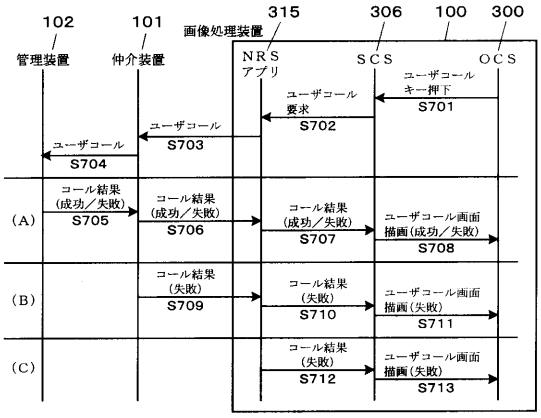
【図９】



【図１０】



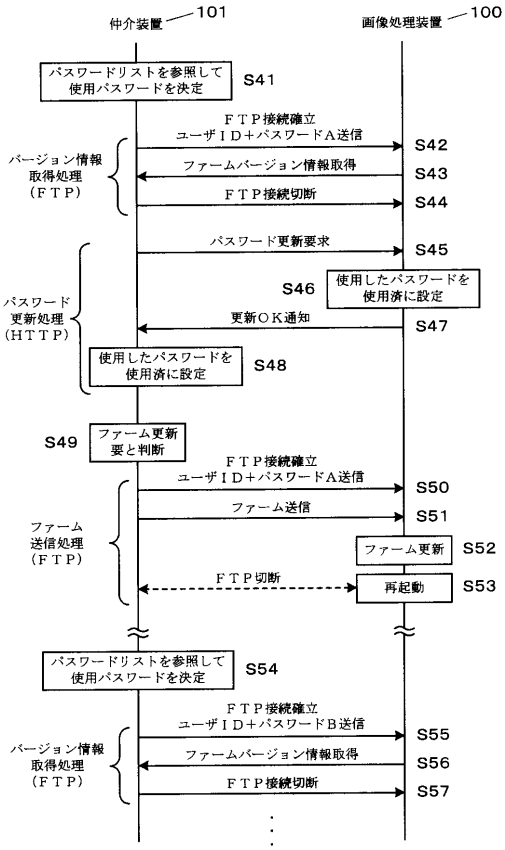
【図１１】



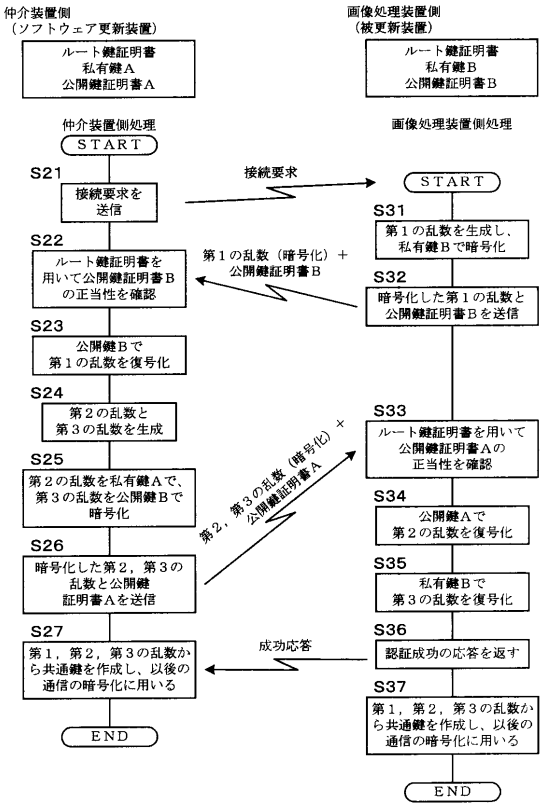
【図１２】

No.	使用済み／未使用	パスワード
A	使用済み	adfghjuhgk
B	使用済み	hj75fgukja
C	未使用	5rhjdebha
⋮	⋮	⋮
X	未使用	rtgfc6qkqa
Y	未使用	6q3fgdysa

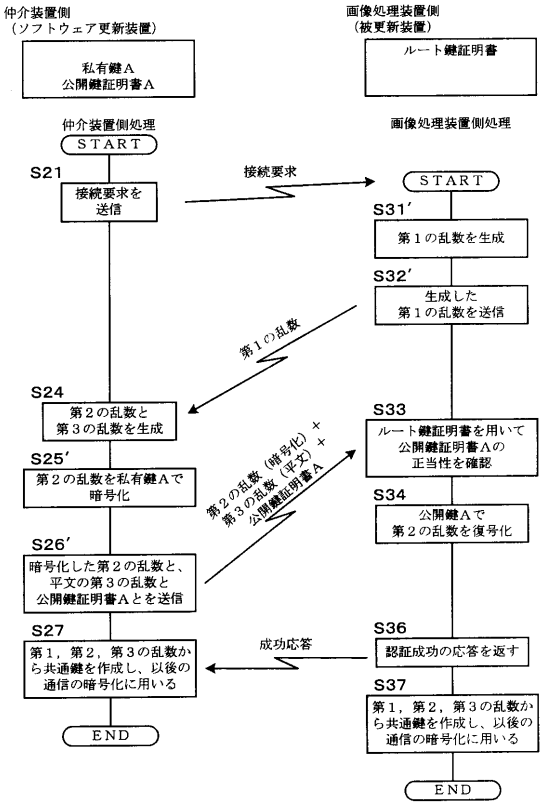
【図１３】



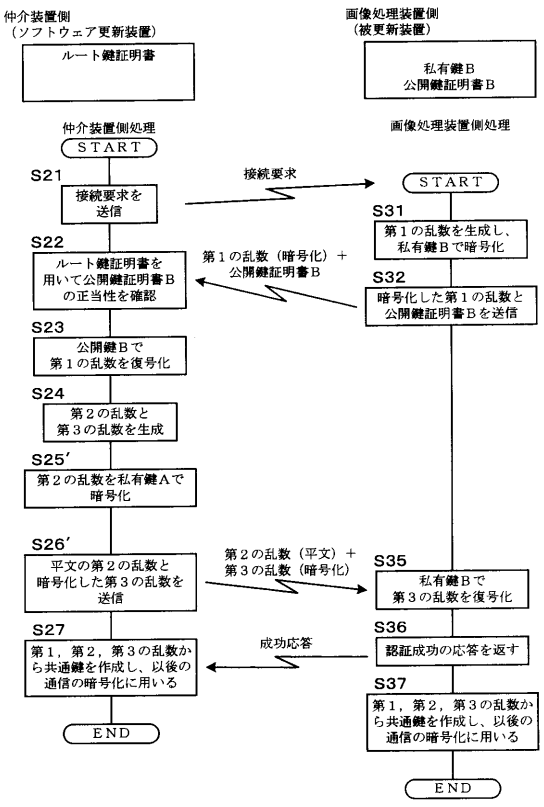
【図１４】



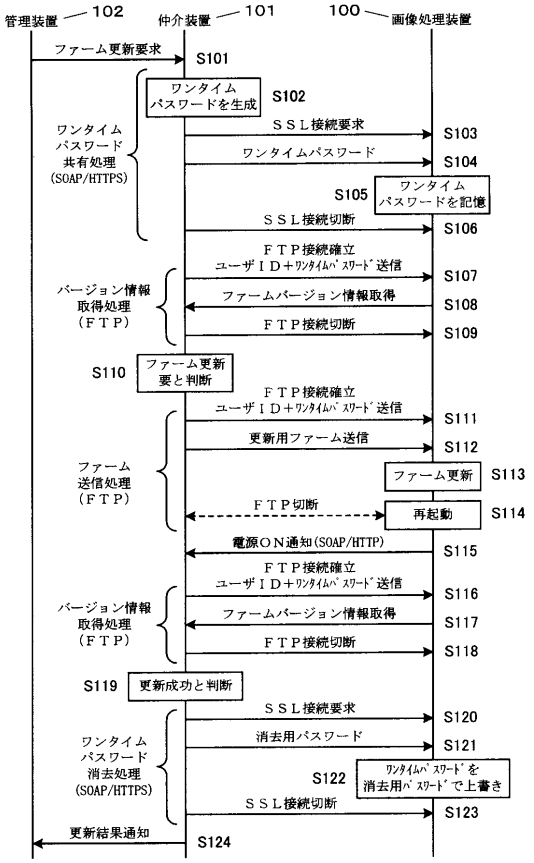
【図１５】



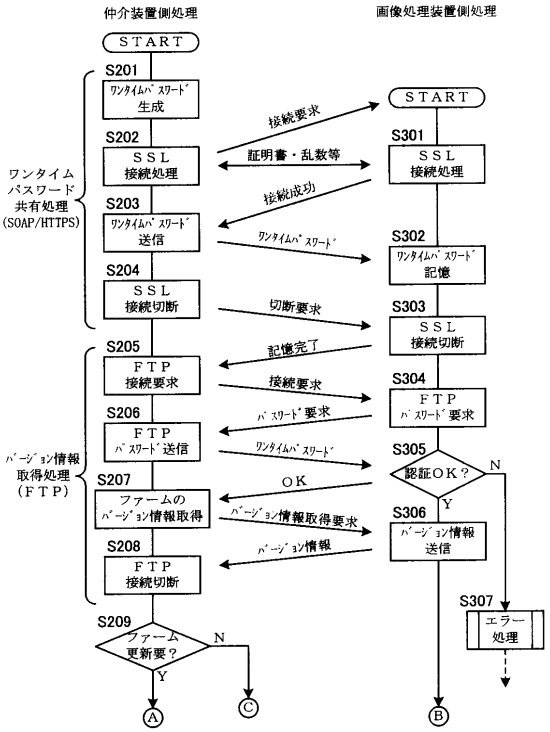
【図１６】



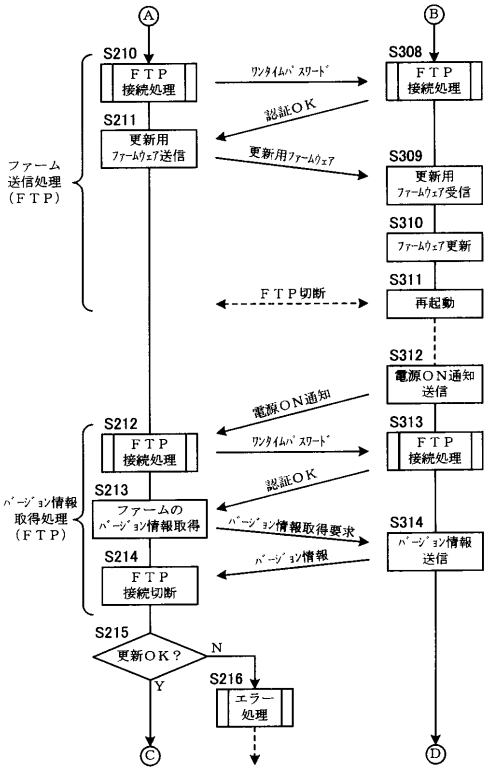
【図１７】



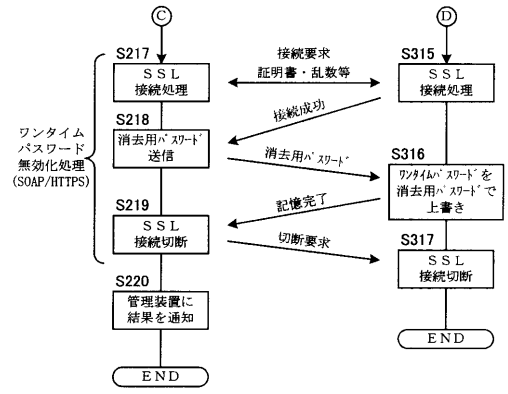
【図１８】



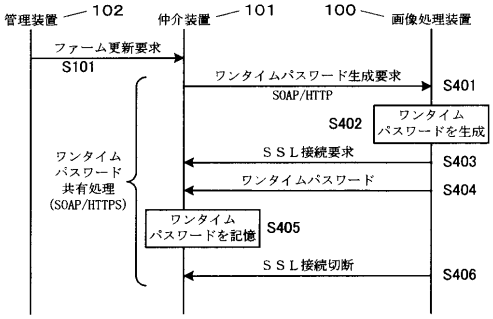
【図１９】



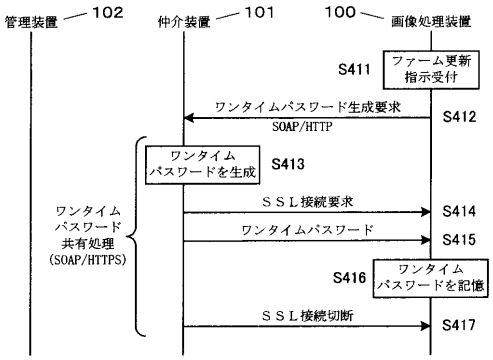
【図２０】



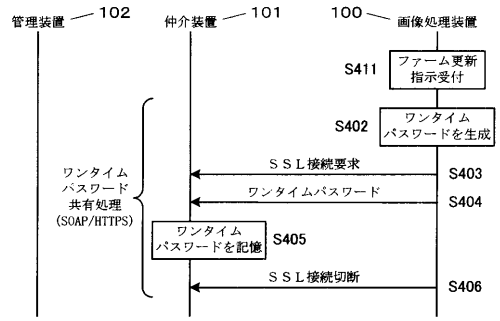
【図２１】



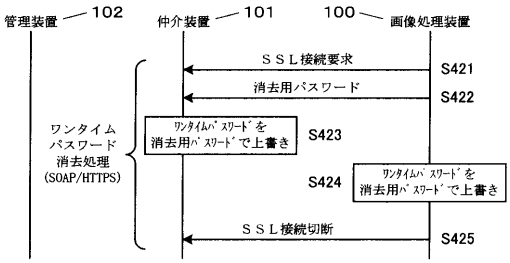
【図２２】



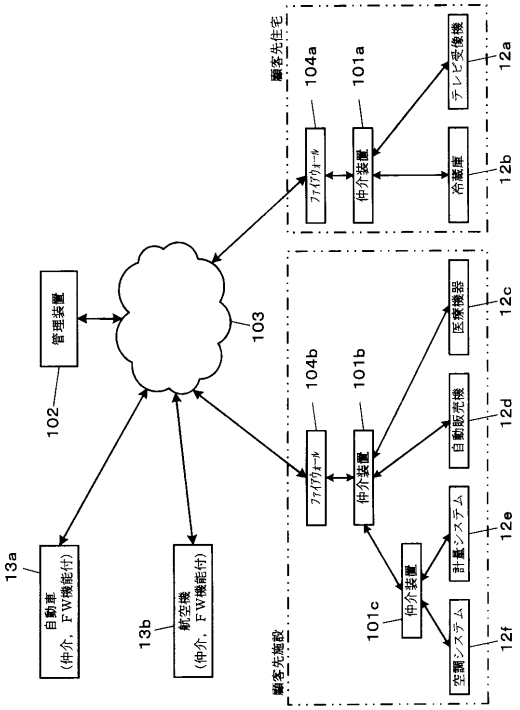
【図２３】



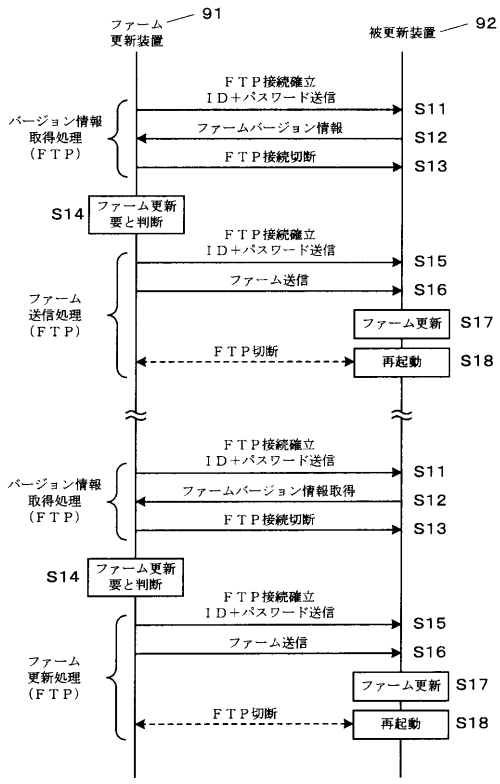
【図２４】



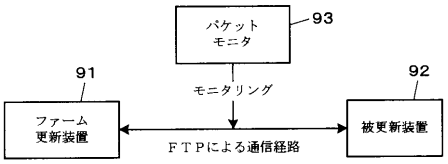
【図２５】



【図２６】



【図２７】



フロントページの続き

(56)参考文献 特開平１０－１４５３５４（ＪＰ，Ａ）
特開２００１－７５９６５（ＪＰ，Ａ）
特開２００２－４１２９５（ＪＰ，Ａ）
特開２００４－５５８５（ＪＰ，Ａ）
特開２００２－７３５５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ １１／００
Ｇ０６Ｆ ２１／２２
Ｇ０６Ｆ １３／００
Ｇ０６Ｆ ９／４４５