

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2012-169894

(P2012-169894A)

(43) 公開日 平成24年9月6日(2012.9.6)

(51) Int.Cl.	F I	テーマコード (参考)
H O 4 L 9/08 (2006.01)	H O 4 L 9/00 6 O 1 B	5 J 1 O 4
H O 4 L 9/14 (2006.01)	H O 4 L 9/00 6 4 1	

審査請求 未請求 請求項の数 6 O L (全 15 頁)

(21) 出願番号	特願2011-29518 (P2011-29518)	(71) 出願人	000001007
(22) 出願日	平成23年2月15日 (2011.2.15)		キヤノン株式会社
			東京都大田区下丸子3丁目30番2号
		(74) 代理人	100114775
			弁理士 高岡 亮一
		(72) 発明者	浅原 英雄
			東京都大田区下丸子3丁目30番2号 キ
			ヤノン株式会社内
		Fターム(参考)	5J104 AA16 AA34 EA01 EA04 EA08
			EA18 JA03 NA02 NA24 NA37
			PA07

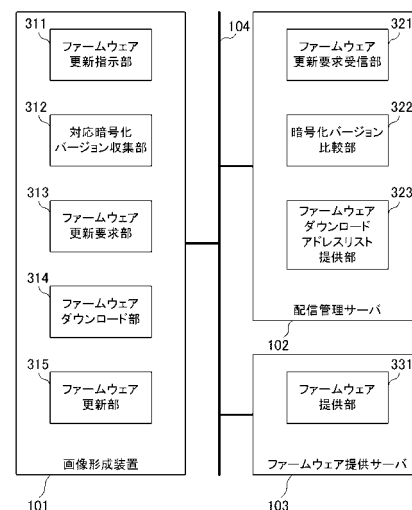
(54) 【発明の名称】 ネットワークシステム、プログラムセット配信サーバ、プログラムセット配信方法、配信サーバの制御方法およびコンピュータプログラム

(57) 【要約】

【課題】新暗号化方式方式に対応していない画像形成装置が新暗号化方式で暗号化されている更新対象のプログラムセットを復号・更新できるようにするネットワークシステムを提供する。

【解決手段】配信管理サーバ102が、画像形成装置101が要求する要求ファームの暗号化方式に画像形成装置101が対応済みかを判断し、画像形成装置101が上記暗号化方式に対応済みでない場合に、第2の通信経路よりセキュリティレベルの高い第1の通信経路を確立する。そして、ファームウェア提供サーバ103が、画像形成装置101に対して、画像形成装置101が上記暗号化方式に対応するために適用する復号モジュールを第1の通信経路により配信し、要求ファームを第2の通信経路により配信する。

【選択図】図2



【特許請求の範囲】**【請求項 1】**

画像形成装置と、前記画像形成装置に対して暗号化されたプログラムセットを配信する配信サーバとを備えるネットワークシステムであって、

前記配信サーバは、

前記画像形成装置が前記プログラムセットの暗号化方式に対応済みか否かを判断する判断手段と、

前記画像形成装置が前記プログラムセットの暗号化方式に対応済みでない場合に、第 2 の通信経路よりセキュリティレベルの高い第 1 の通信経路を確立する通信経路確立手段と、

前記画像形成装置に対して、前記画像形成装置が前記暗号化方式に対応するために適用するプログラムを前記第 1 の通信経路により配信し、前記暗号化方式で暗号化された前記プログラムセットを前記第 2 の通信経路により配信する配信手段とを備える

ことを特徴とするネットワークシステム。

【請求項 2】

前記配信手段は、前記暗号化方式に対応するために適用するプログラムを、前記暗号化方式で暗号化された前記プログラムセットの配信に先立って前記画像形成装置に対して送信し、前記画像形成装置が前記プログラムを適用した後に、前記暗号化方式で暗号化された前記プログラムセットを前記画像形成装置に対して配信する

ことを特徴とする請求項 1 に記載のネットワークシステム。

【請求項 3】

画像形成装置と、前記画像形成装置に対して暗号化されたプログラムセットを配信する配信サーバとを備えるシステムにおけるプログラムセット配信方法であって、

前記配信サーバが、前記画像形成装置が前記プログラムセットの暗号化方式に対応済みか否かを判断する工程と、

前記配信サーバが、前記画像形成装置が前記プログラムセットの暗号化方式に対応済みでない場合に、第 2 の通信経路よりセキュリティレベルの高い第 1 の通信経路を確立する工程と、

前記配信サーバが、前記画像形成装置に対して、前記画像形成装置が前記暗号化方式に対応するために適用するプログラムを前記第 1 の通信経路により配信し、前記暗号化方式で暗号化された前記プログラムセットを前記第 2 の通信経路により配信する工程とを有する

ことを特徴とするプログラムセット配信方法。

【請求項 4】

画像形成装置に対して暗号化されたプログラムセットを配信する配信サーバであって、前記画像形成装置が前記プログラムセットの暗号化方式に対応済みでない場合に、前記画像形成装置に対して、前記画像形成装置が前記暗号化方式に対応するために適用するプログラムを、前記暗号化方式で暗号化された前記プログラムセットの配信に先立って、第 2 の通信経路よりセキュリティレベルの高い第 1 の通信経路により配信する手段と、

前記画像形成装置が前記プログラムを適用した後に、前記暗号化方式で暗号化された前記プログラムセットを、前記第 2 の通信経路により前記画像形成装置に対して配信する手段とを備える

ことを特徴とする配信サーバ。

【請求項 5】

画像形成装置に対して暗号化されたプログラムセットを配信する配信サーバの制御方法であって、

前記画像形成装置が前記プログラムセットの暗号化方式に対応済みでない場合に、前記画像形成装置に対して、前記画像形成装置が前記暗号化方式に対応するために適用するプログラムを、前記暗号化方式で暗号化された前記プログラムセットの配信に先立って、第 2 の通信経路よりセキュリティレベルの高い第 1 の通信経路により配信する工程と、

10

20

30

40

50

前記画像形成装置が前記プログラムを適用した後に、前記暗号化方式で暗号化された前記プログラムセットを、前記第2の通信経路により前記画像形成装置に対して配信する工程とを有する

ことを特徴とする配信サーバの制御方法。

【請求項6】

請求項5に記載の配信サーバの制御方法をコンピュータに実行させることを特徴とするコンピュータプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、ネットワークシステム、プログラムセット配信サーバ、プログラムセット配信方法、配信サーバの制御方法およびコンピュータプログラムに関する。

【背景技術】

【0002】

画像形成装置に対して更新対象の新しいファームウェアを配信する配信サーバが提案されている。ファームウェアは、様々な技術や知的財産を含むので、第三者に見られてはならない。従って、配信サーバが、ファームウェアを暗号化してから画像形成装置に対して配信し、画像処理装置上で動作しているファームウェアが含む復号化機能がこのファームウェアを復号化し、更新することが考えられる。

【0003】

暗号化データの解読技術の進歩に伴って、ファームウェアの暗号化方式が変更される場合がある。その場合に、新しい暗号化方式に対応したファームウェアをセキュアに画像形成装置に配信する方法がない。従って、現在は、一度市場に出した製品に対して、ファームウェアの暗号化方式を変更することはしないようにしている。また、やむを得ずにファームウェアの暗号化方式を差し替える必要がある場合には、画像形成装置が配置されている全ての場所にサービスマンが出向いて、手動でファームウェアを更新しなければならなかった。

【0004】

特許文献1は、新旧2つの暗号方式識別情報を保持するセンタ装置が通信端末から暗号化識別情報を受信し、受信した暗号化識別情報を新旧2つの暗号方式識別情報のいずれか

による復号・照合を通じて最新暗号方式識別情報へ更新するシステム装置を開示する。

【先行技術文献】

【特許文献】

【0005】

【特許文献1】特開2001-127749号公報

【発明の概要】

【発明が解決しようとする課題】

【0006】

サービスマンが手動でファームウェアを更新する方法では、画像形成装置が配置されている全ての場所へメンテナンスに行く必要がある。従って、この方法では膨大な人的時間的コストが必要となる。また、この方法によってファームウェアを更新する前提として、更新するファームウェアは、変更前の暗号化方式で暗号化されている必要がある。すなわち、変更後の暗号化方式が変更前の暗号化方式で守られた状態であるため、仮に外部に流出してしまうと変更後の暗号化方式のセキュリティが損なわれるリスクがあった。

【0007】

また、特許文献1が開示する技術を画像形成装置へのファームウェアすなわちプログラムセットの配信に適用した場合、以下のような問題がある。すなわち、ユーザが更新したいファームウェアが、画像形成装置が保持する復号化機能で復号化できない新暗号化方式で暗号化されているときは、ファームウェアを更新できない。

【0008】

10

20

30

40

50

本発明は、新暗号化方式方式に対応していない画像形成装置が当該新暗号化方式で暗号化されている更新対象のプログラムセットを復号・更新できるようにするネットワークシステムの提供を目的とする。

【課題を解決するための手段】

【０００９】

本発明の一実施形態のネットワークシステムは、画像形成装置と、前記画像形成装置に対して暗号化されたプログラムセットを配信する配信サーバとを備えるネットワークシステムである。前記配信サーバは、前記画像形成装置が前記プログラムセットの暗号化方式に対応済みか否かを判断する判断手段と、前記画像形成装置が前記プログラムセットの暗号化方式に対応済みでない場合に、第２の通信経路よりセキュリティレベルの高い第１の通信経路を確立する通信経路確立手段と、前記画像形成装置に対して、前記画像形成装置が前記暗号化方式に対応するために適用するプログラムを前記第１の通信経路により配信し、前記暗号化方式で暗号化された前記プログラムセットを前記第２の通信経路により配信する配信手段とを備える。

10

【発明の効果】

【００１０】

本発明のネットワークシステムによれば、新暗号化方式方式に対応していない画像形成装置が当該新暗号化方式で暗号化されている更新対象のプログラムセットを復号・更新できるようになる。従って、例えば、ユーザが更新したいファームウェアが、画像処理装置が保持する復号化機能で復号化できない暗号化方式で暗号化されている場合であっても、ファームウェア更新することが可能である。

20

【図面の簡単な説明】

【００１１】

【図１】本実施形態のネットワークシステムの構成例を示す図である。

【図２】実施例１のネットワークシステムの機能を説明する図である。

【図３】ファームウェア更新要求の例を示す図である。

【図４】ファームウェアダウンロードアドレスリストの例を示す図である。

【図５】ファームウェアリストの例を示す図である。

【図６】復号モジュールリストの例を示す図である。

【図７】ファームウェア更新要求の送信処理例を説明するフローチャートである。

30

【図８】ファームウェアダウンロードアドレスリストの生成処理例を説明するフローチャートである。

【図９】ファームウェアの更新処理の例を説明するフローチャートである。

【発明を実施するための形態】

【００１２】

図１は、本実施形態のネットワークシステムの構成例を示す図である。このネットワークシステムは、画像形成装置１０１と、配信管理サーバ１０２と、ファームウェア提供サーバ１０３とを備える。画像形成装置１０１乃至ファームウェア提供サーバ１０３は、互いにネットワーク１０４を介して通信可能である。ネットワーク１０４は、例えばインターネットである。本実施形態のプログラムセット配信方法は、図１に示すネットワークシステムが備える各装置の機能によって実現される。

40

【００１３】

画像形成装置１０１は、外部装置または所定のインタフェースを介して入力された印刷データを対象に印刷処理を実行する情報処理装置である。画像形成装置１０１は、例えばプリンタである。画像形成装置１０１は、画像形成装置１０１の機能を実現するためのソフトウェアであるファームウェアを備える。ファームウェアは、プログラムセット（１つ以上のソフトウェアのセット）である。本実施形態では、ファームウェアは、ファームウェアを更新するためのソフトウェアと、暗号化されたファームウェアを復号化するためのソフトウェアとを含む。以下の説明では、暗号化されたファームウェアを復号化するためのソフトウェアを、復号モジュールと記述する。復号モジュールは、ファームウェアを構

50

成する他のソフトウェアと比較してサイズが小さい。また、ファームウェアを更新するためのソフトウェアを、更新用ソフトウェアと記述する。

【0014】

画像形成装置101は、CPU110、不揮発性メモリ111、揮発性メモリ112、補助記憶装置113、ディスプレイ114、入力装置115、ネットワーク通信装置116を備える。

【0015】

CPU110は、画像形成装置101全体を制御する。具体的には、CPU110は、画像形成装置101の機能を実現するコンピュータプログラムを実行したり、内部バス120を介して接続された各装置の制御を実行したりする。

10

【0016】

不揮発性メモリ111は、ROM(Read Only Memory)を有する。不揮発性メモリ111は、画像形成装置101の起動処理において初期段階に必要なプログラムやデータを予め格納している。揮発性メモリ112は、RAM(Random Access Memory)を有する。揮発性メモリ112は、プログラム、データの一時的な格納場所として用いられる。

【0017】

補助記憶装置113は、ハードディスクやRAMドライブ等の大容量記憶装置から構成され、大容量データの保管、プログラムの実行コードの保持を行う。補助記憶装置113は、揮発性メモリ112と比較して、長時間保持する必要があるデータを記憶する。具体的には、補助記憶装置113は、画像形成装置101上で動作するファームウェアを保持する。ディスプレイ114は、画像形成装置101を操作するユーザに情報を通知する表示装置である。

20

【0018】

入力装置115は、ユーザの選択指示を受付け、内部バス120を介して、CPU110が実行するプログラムに伝達する装置である。ネットワーク通信装置116は、画像形成装置101と外部装置との間の通信を媒介する。すなわち、ネットワーク通信装置116は、CPU110の指示に従い、ネットワーク104を介して外部装置と通信する。

【0019】

配信管理サーバ102は、ファームウェア提供サーバ103から画像形成装置101に対するファームウェアの配信を管理するサーバである。ファームウェア提供サーバ103は、画像形成装置101に対して暗号化されたファームウェアをネットワーク104を介して提供するサーバである。

30

【0020】

すなわち、配信管理サーバ102とファームウェア提供サーバ103とは、画像形成装置102に対して暗号化されたプログラムセットを配信する配信サーバとして機能する。このために、ファームウェア提供サーバ103は、画像形成装置101上で動作するファームウェアを、ダウンロード可能な状態で保持する。

【0021】

ファームウェア提供サーバ103は、HTTPSに準じたセキュアな通信経路(第1の通信経路)とHTTPに準じた通常の通信経路(第2の通信経路)とを確立し、確立した通信経路を用いて画像形成装置101にファームウェアを配信する。HTTPは、Hypertext Transfer Protocolの略称である。HTTPSは、Hypertext Transfer Protocol Securityの略称である。HTTPSとHTTPとを比較すると、HTTPSの方が多少速度は劣り、また、ファームウェア提供サーバ103をレンタルするためのコストも高い。一方、HTTPSは、HTTPよりセキュリティレベルが高い(セキュアである)。

40

【0022】

図1には、1台のファームウェア提供サーバ103が示されているが、本実施形態のネットワークシステムは、複数のファームウェア提供サーバにアクセスを分散させる仕組みを有する。これにより、世界各国に素早く安定してファームウェアを提供することができ

50

る。

【 0 0 2 3 】

図 2 は、実施例 1 のネットワークシステムの機能を説明する図である。画像形成装置 1 0 1 は、ファームウェア更新指示部 3 1 1、対応暗号化バージョン収集部 3 1 2、ファームウェア更新要求部 3 1 3、ファームウェアダウンロード部 3 1 4、ファームウェア更新部 3 1 5 を備える。

【 0 0 2 4 】

ファームウェア更新指示部 3 1 1 は、ユーザ操作に従って入力装置 1 1 5 (図 1) が入力する入力情報に基づいて、ファームウェア更新指示を行う。ファームウェア更新指示は、ファームウェアを更新する指示である。対応暗号化バージョン収集部 3 1 2 は、画像形成装置 1 0 1 上で現在動作しているファームウェアが復号可能であるファームウェアまたはソフトウェアの暗号化方式のバージョンを取得する。以下では、画像形成装置 1 0 1 上で現在動作しているファームウェアを、現行ファームと記述する。また、現行ファームが復号可能であるファームウェアまたはソフトウェアの暗号化方式を、現行ファーム対応暗号化方式と記述する。

【 0 0 2 5 】

本実施形態では、補助記憶装置 1 1 3 が、ファームウェアとともに現行ファーム対応暗号化方式のバージョンを記憶している。従って、対応暗号化バージョン収集部 3 1 2 は、補助記憶装置 1 1 3 から現行ファーム対応暗号化方式のバージョンを読み出して取得する。以下では、現行ファーム対応暗号化方式のバージョンを、対応暗号化バージョンとも記述する。

【 0 0 2 6 】

ファームウェア更新要求部 3 1 3 は、ファームウェア更新指示部 3 1 1 からファームウェア更新指示を受ける。そして、ファームウェア更新要求部 3 1 3 は、配信管理サーバ 1 0 2 に対してファームウェア更新要求を行う。ファームウェア更新要求は、新たに更新して適用したいファームウェアの配信を求める要求である。

【 0 0 2 7 】

図 3 は、ファームウェア更新要求部が行うファームウェア更新要求の例を示す図である。ファームウェア更新要求 4 0 1 は、XML 形式のデータを有する。ファームウェア更新要求部 3 1 3 は、ファームウェア更新要求のタグの中に、機種識別子、デバイス識別子、要求ファームウェアバージョン、対応暗号化バージョンを設定する。

【 0 0 2 8 】

機種識別子は、画像形成装置の機種を一意に識別する識別情報である。この例では、画像形成装置 1 0 1 の機種識別子は、機種 A である。デバイス識別子は、画像形成装置自身を一意に識別する識別情報である。この例では、画像形成装置 1 0 1 のデバイス識別子は、XXX00001 である。

【 0 0 2 9 】

要求ファームウェアバージョンは、画像形成装置 1 0 1 が配信を要求するファームウェアのバージョンである。画像形成装置 1 0 1 は、配信を受けたファームウェアで、画像形成装置 1 0 1 上で動作しているファームウェアを置き換えて更新する。バージョンは機種別に固有であるものとする。この例では、要求ファームウェアバージョンは、03.00 である。従って、ファームウェア更新要求 4 0 1 は、配信管理サーバ 1 0 2 に対して、03.00 というバージョンのファームウェアの配信を求めることを示す。ファームウェア更新要求部 3 1 3 は、対応暗号化バージョン収集部 3 1 2 から対応暗号化バージョンを取得し、ファームウェア更新要求 4 0 1 に設定する。この例では、ファームウェア更新要求 4 0 1 に、01.00 という対応暗号化バージョンが設定されている。従って、画像形成装置 1 0 1 が、01.00 という対応暗号化バージョンの暗号化方式で暗号化されたファームウェアまたはソフトウェアに対応していること、すなわちこのファームウェアまたはソフトウェアを復号可能であることがわかる。

【 0 0 3 0 】

図 2 に戻って、ファームウェアダウンロード部 3 1 4 は、配信管理サーバ 1 0 2 からファームウェアダウンロードアドレスリストをネットワーク 1 0 4 を介して取得する。ファームウェアダウンロードアドレスリストは、画像形成装置 1 0 1 に対して配信するファームウェアのダウンロードアドレスのリストである。そして、ファームウェアダウンロード部 3 1 4 は、取得したファームウェアダウンロードアドレスリストが含むダウンロードアドレスに基づいて、ファームウェアをダウンロードする。

【 0 0 3 1 】

図 4 は、ファームウェアダウンロードアドレスリストの例を示す図である。ファームウェアダウンロードアドレスリスト 7 0 1 は、XML 形式のデータを有する。図 4 に示す例では、画像形成装置 1 0 1 がダウンロード対象とするファームウェア（以下、ダウンロード対象ファームと記述）が、復号モジュールと、メインコントローラと、プリンタエンジンコントローラとを含むものとする。

10

【 0 0 3 2 】

ここで、配信管理サーバ 1 0 2 は、対応暗号化バージョンがファームウェア更新要求が要求するファームウェアの被暗号化バージョンと合致しない場合に、以下の処理を実行する。配信管理サーバ 1 0 2 は、ファームウェア更新要求が要求するファームウェア（要求ファーム）の暗号化方式に対応する復号モジュールのダウンロードアドレスをファームウェアダウンロードアドレスリストに設定する。ファームウェアダウンロードアドレスリスト 7 0 1 が含む復号モジュールは、当該ダウンロード対象ファームが含む、復号モジュール以外のソフトウェア（この例ではメインコントローラとプリンタエンジンコントローラ）を復号できる。すなわち、当該復号モジュールは、画像形成装置 1 0 1 が要求ファームの暗号化方式に対応するために適用するプログラムである。

20

【 0 0 3 3 】

この例では、ファームウェアダウンロードアドレスタグの下に、復号モジュールタグ、メインコントローラタグ、プリンタエンジンコントローラタグが設定されている。復号モジュールタグの下に、復号モジュールのダウンロードアドレスが設定されている。メインコントローラタグの下に、メインコントローラのダウンロードアドレスが設定されている。プリンタエンジンコントローラタグの下に、プリンタエンジンコントローラのダウンロードアドレスが設定されている。ファームウェア提供サーバ 1 0 3 がこれらのダウンロードアドレスを管理している。

30

【 0 0 3 4 】

復号モジュールのダウンロードアドレスは、HTTPS のアドレスである。つまり、画像形成装置 1 0 1 がファームウェア提供サーバ 1 0 3 から復号モジュールをダウンロードする時には、セキュアな通信経路（第 1 の通信経路）が確立されている。これにより、ファームウェア提供サーバ 1 0 3 から復号モジュールをダウンロードする際のセキュリティが保たれる。メインコントローラのダウンロードアドレス、プリンタエンジンコントローラのダウンロードアドレスは、HTTP のアドレスである。つまり、画像形成装置 1 0 1 は、ファームウェア提供サーバ 1 0 3 からメインコントローラとプリンタエンジンコントローラとをダウンロードする時には、通常の通信経路（第 2 の通信経路）でダウンロードする。

40

【 0 0 3 5 】

図 2 に戻って、ファームウェア更新部 3 1 5 は、ファームウェアダウンロード部 3 1 4 によってダウンロードされたファームウェアを用いて、画像形成装置 1 0 1 上で現在動作するファームウェア（現行ファーム）を更新する。

【 0 0 3 6 】

ダウンロードされたファームウェアが復号モジュールを含む場合、ファームウェア更新部 3 1 5 は、まず、現行ファームを用いて、復号モジュールの更新処理を行う。具体的には、ファームウェア更新部 3 1 5 が、現行ファームが含む復号モジュールを用いて、ダウンロードされたファームウェアが含む復号モジュールを復号する。ファームウェア更新部 3 1 5 が、復号した復号モジュールで当該現行ファームが含む復号モジュールを更新する

50

。これにより、更新された復号モジュールが動作できる状態になる。次に、ファームウェア更新部 315 は、更新された復号モジュールを用いて、ダウンロードされたファームウェアが含む、復号モジュール以外のソフトウェア（例えば、プリンタドライバコントローラ）を復号する。そして、ファームウェア更新部 315 は、復号した当該ソフトウェアで、現行ファームに含まれるソフトウェアを更新する。

【0037】

配信管理サーバ 102 は、ファームウェア更新要求受信部 321、暗号化バージョン比較部 322、ファームウェアダウンロードアドレスリスト提供部 323 を備える。ファームウェア更新要求受信部 321 は、画像形成装置 101 のファームウェア更新要求部 313 からファームウェア更新要求を受信する。

10

【0038】

暗号化バージョン比較部 322 は、画像形成装置 101 が要求ファームを復号可能であるかを判断する。すなわち、暗号化バージョン比較部 322 は、画像形成装置 101 が要求ファームの暗号化方式に対応済みか否かを判断する判断手段として機能する。

【0039】

暗号化バージョン比較部 322 は、ファームウェア更新要求が含む対応暗号化バージョンと、要求ファームの暗号化方式のバージョンとが合致するかを判断し、該判断結果に基づいて、ダウンロード対象ファームを復号可能であるかを判断する。要求ファームの暗号化方式のバージョンを、以下では被暗号化バージョンと記述する。被暗号化バージョンは、予め記憶手段に記憶されたファームウェアリストに含まれる。

20

【0040】

図 5 は、ファームウェアリストの例を示す図である。ファームウェアリスト 501 は、識別番号と、機種識別子と、ファームウェアバージョンと、被暗号化バージョンとを含む。識別番号は、ファームウェア提供サーバが提供可能なファームウェアを一意に識別する識別情報である。機種識別子は、図 3 を参照して説明した機種識別子と同義である。

【0041】

ファームウェアバージョンは、ファームウェア提供サーバ 103 が提供可能なファームウェアのバージョンである。被暗号化バージョンは、ファームウェア提供サーバ 103 が提供可能なファームウェアの暗号化方式のバージョンである。

【0042】

図 2 に戻って、暗号化バージョン比較部 322 は、例えば、図 3 に示すファームウェア更新要求 401 が含む要求ファームウェアバージョンと機種識別子とを取得する。この例では、暗号化バージョン比較部 322 は、03 . 00 という要求ファームウェアバージョンと、機種 A という機種識別子を取得する。次に、暗号化バージョン比較部 322 は、図 5 に示すファームウェアリスト 501 のエントリ（一行分のデータ）のうち、機種識別子が機種 A であり、ファームウェアバージョンが 03 . 00 であるエントリを探索する。この例では、暗号化バージョン比較部 322 は、識別番号が 5 番のエントリを探索結果として取得する。この、識別番号 5 番のエントリに対応するファームウェアが要求ファームである。

30

【0043】

次に、暗号化バージョン比較部 322 は、取得したエントリが含む被暗号化バージョンすなわち要求ファームの被暗号化バージョンを取得する。この例では、暗号化バージョン比較部 322 は、被暗号化バージョンとして 03 . 00 を取得する。また、暗号化バージョン比較部 322 は、ファームウェア更新要求 401 が含む対応暗号化バージョンを取得する。この例では、暗号化バージョン比較部 322 は、対応暗号化バージョンとして、01 . 00 を取得する。そして、暗号化バージョン比較部 322 は、取得した対応暗号化バージョンと被暗号化バージョンとが合致するかを判断する。

40

【0044】

対応暗号化バージョンと被暗号化バージョンとが合致する場合、暗号化バージョン比較部 322 は、画像形成装置 101 が要求ファームを復号可能であると判断する。対応暗号

50

化バージョンと被暗号化バージョンとが合致しない場合、暗号化バージョン比較部 3 2 2 は、画像形成装置 1 0 1 が要求ファームを復号可能でないと判断する。この例では、被暗号化バージョンは 0 3 . 0 0 であり、対応暗号化バージョンは、0 1 . 0 0 であるので、被暗号化バージョンと対応暗号化バージョンとは合致しない。従って、暗号化バージョン比較部 3 2 2 は、画像形成装置 1 0 1 が要求ファームを復号可能でないと判断する。

【 0 0 4 5 】

図 2 に戻って、ファームウェアダウンロードアドレスリスト提供部（以下、提供部）3 2 3 は、ファームウェアダウンロードアドレスリストを生成する。暗号化バージョン比較部 3 2 2 が、画像形成装置 1 0 1 が要求ファームを復号可能であると判断した場合、提供部 3 2 3 は、要求ファームをダウンロード対象ファームとする。そして、提供部 3 2 3 は、当該ダウンロード対象ファーム（要求ファーム）のダウンロードアドレスのリストをファームウェアダウンロードアドレスリストとして作成する。

10

【 0 0 4 6 】

暗号化バージョン比較部 3 2 2 が、画像形成装置 1 0 1 が要求ファームを復号可能でないと判断した場合、提供部 3 2 3 は、所定の記憶手段に予め記憶された復号モジュールリストを参照して、以下の処理を実行する。提供部 3 2 3 は、画像形成装置 1 0 1 が復号可能であって、かつ、要求ファームの暗号化方式に対応する復号モジュールを選択し、選択した復号モジュールと要求ファームとをダウンロード対象ファームとする。そして、提供部 3 2 3 は、当該ダウンロード対象ファーム（復号モジュールと要求ファーム）のダウンロードアドレスのリストを、ファームウェアダウンロードアドレスリストとして作成する。

20

【 0 0 4 7 】

図 6 は、復号モジュールリストの例を示す図である。復号モジュールリスト 6 0 1 は、識別番号、機種識別子、対応暗号化バージョン、被暗号化バージョンとを含む。識別番号は、ファームウェア提供サーバ 1 0 3 が提供する復号モジュールを一意に識別する識別情報である。機種識別子は、図 3 を参照して説明した機種識別子と同義である。対応暗号化バージョンは、復号モジュールが対応している暗号化方式のバージョン、すなわち、復号モジュールが復号可能であるファームウェアまたはソフトウェアの暗号化方式のバージョンである。被暗号化バージョンは、復号モジュール自身の暗号化方式のバージョンである。

30

【 0 0 4 8 】

図 3 乃至 6 を参照して、提供部 3 2 3 の処理の例について具体的に説明する。図 5 に示すファームウェアリスト 5 0 1 の識別番号 5 に対応するファームウェアが要求ファームであるものとする。当該要求ファームの被暗号化バージョン " 0 3 . 0 0 " と図 3 のファームウェア更新要求 4 0 1 が含む対応暗号化バージョン " 0 1 . 0 0 " とが合致しないので、暗号化バージョン比較部 3 2 2 が、画像形成装置 1 0 1 が要求ファームを復号可能でないと判断する。

【 0 0 4 9 】

提供部 3 2 3 は、図 6 に示す復号モジュールリストのエントリのうち、対応暗号化バージョンが上記要求ファームの被暗号化バージョン " 0 3 . 0 0 " と合致し、被暗号化バージョンが対応暗号化バージョン " 0 1 . 0 0 " と合致するエントリを探索する。この例では、提供部 3 2 3 は、識別番号が 2 のエントリを探索結果として取得し、取得したエントリに対応する復号モジュールのダウンロードアドレスを、ファームウェアダウンロードアドレスリストへの設定対象として決定する。

40

【 0 0 5 0 】

例えば、要求ファームがメインコントローラとプリンタエンジンコントローラとを含む場合を想定する。提供部 3 2 3 は、当該コントローラのダウンロードアドレスと復号モジュールのダウンロードアドレスとをファームウェア提供サーバ 1 0 3 から取得し、取得したダウンロードアドレスをファームウェアダウンロードアドレスリスト 7 0 1（図 4 を参照）に設定する。このために、提供部 3 2 3 は、当該コントローラと復号モジュールとを

50

ファームウェア提供サーバ 103 のファームウェア提供部 331 に通知し、ファームウェア提供部 331 からコントローラと復号モジュールのダウンロードアドレスの割り当てを受ける。また、提供部 323 は、ファームウェアダウンロードアドレスリストを画像形成装置 101 のファームウェアダウンロード部 314 に対してネットワーク 104 を介して提供する。

【0051】

図 2 に戻って、ファームウェア提供サーバ 103 は、ファームウェア提供部 331 を備える。ファームウェア提供部 331 は、配信管理サーバ 102 の提供部 323 から要求ファーム、復号モジュールの通知を受けると、要求ファーム、復号モジュールにダウンロードアドレスを割り当ててダウンロード可能な状態にする。そして、このダウンロードアドレスを提供部 323 に通知する。

10

【0052】

ファームウェア提供部 331 は、復号モジュールに対しては HTTPS のアドレスを割り当てる。また、ファームウェア提供部 331 は、要求ファームに対しては HTTP のアドレスを割り当てる。つまり、ダウンロード対象ファームが復号モジュールと要求ファームとを含む場合、ファームウェア提供部 331 は、ダウンロード対象ファームが含むファームウェアのうち、復号モジュール以外のファームウェアに対して HTTP のアドレスを割り当てる。

【0053】

すなわち、配信管理サーバ 102 の提供部 323 とファームウェア提供サーバ 103 のファームウェア提供部 331 とは、以下の処理を行う通信経路確立手段として機能する。この通信経路確立手段は、画像形成装置 101 が要求ファームの暗号化方式に対応済みでない場合に、復号モジュールのダウンロードアドレスとして HTTPS のアドレスを割り当てる。つまり、この通信経路確立手段は、HTTP のアドレスによる通信経路（第 2 の通信経路）よりセキュリティレベルの高い第 1 の通信経路を確立する。

20

【0054】

図 7 は、ファームウェア更新要求の送信処理例を説明するフローチャートである。まず、入力装置 115 が、ユーザの操作に従って、ファームウェア更新要求を受け付け（ステップ S1）、受け付けたファームウェア更新要求をファームウェア更新指示部 311 に送信する。

30

【0055】

次に、対応暗号化バージョン収集部 312 が、対応暗号化バージョンを収集する（ステップ S2）。そして、ファームウェア更新要求部 313 が、ステップ S2 において収集された対応暗号化バージョンを含むファームウェア更新要求 401 を、ネットワーク 104 を介して配信管理サーバ 102 に送信する（ステップ S3）。

【0056】

図 8 は、ファームウェアダウンロードアドレスリストの生成処理例を説明するフローチャートである。配信管理サーバ 102 のファームウェア更新要求受信部 321 が、画像形成装置 101 のファームウェア更新要求部 313 から、ファームウェア更新要求 401 を受信する（ステップ S11）。続いて、暗号化バージョン比較部 322 が、ファームウェア更新要求 401 から、画像形成装置 101 の対応暗号化バージョンを取得する（ステップ S12）。

40

【0057】

次に、暗号化バージョン比較部 322 が、ファームウェア更新要求 401 から機種識別子と要求ファームウェアバージョンとを取得する。そして、暗号化バージョン比較部 322 が、ファームウェアリスト 501 を参照して、上記取得した機種識別子と要求ファームウェアバージョンに対応するファームウェア（要求ファーム）を選択し、その被暗号化バージョンを取得する（ステップ S13）。

【0058】

次に、暗号化バージョン比較部 322 が、ステップ S12 において取得した対応暗号化

50

バージョンとステップ S 1 3 において取得した被暗号化バージョンとが合致するかを判断する（ステップ S 1 4）。

【 0 0 5 9 】

暗号化バージョン比較部 3 2 2 が、対応暗号化バージョンと被暗号化バージョンとが合致すると判断した場合は、ステップ S 1 7 に進む。暗号化バージョン比較部 3 2 2 が、対応暗号化バージョンと被暗号化バージョンとが合致しないと判断した場合は、ステップ S 1 5 に進む。

【 0 0 6 0 】

暗号化バージョン比較部 3 2 2 が、被暗号化バージョンがステップ S 1 2 において取得された対応暗号化バージョンに合致し、対応暗号化バージョンがステップ S 1 3 において取得された被暗号化バージョンに合致する復号モジュールを選択する（ステップ S 1 5）。これにより、選択された復号モジュールと要求ファームとを含むファームウェアがダウンロード対象ファームとして決定される。

【 0 0 6 1 】

次に、暗号化バージョン比較部 3 2 2 が、ステップ S 1 5 において選択された復号モジュールのダウンロードアドレスをファームウェア提供サーバ 1 0 3 から取得して、ファームウェアダウンロードアドレスリストに設定する（ステップ S 1 6）。また、暗号化バージョン比較部 3 2 2 が、要求ファームのダウンロードアドレスをファームウェア提供サーバ 1 0 3 から取得して、ファームウェアダウンロードアドレスリストに設定する（ステップ S 1 7）。

【 0 0 6 2 】

図 9 は、画像形成装置におけるファームウェアの更新処理の例を説明するフローチャートである。画像形成装置 1 0 1 のファームウェアダウンロード部 3 1 4 が、配信管理サーバ 1 0 2 の提供部 3 2 3 から、ネットワーク 1 0 4 を介して、ファームウェアダウンロードアドレスリストを受信する（ステップ S 2 1）。

【 0 0 6 3 】

次に、ファームウェアダウンロード部 3 1 4 が、ステップ S 2 1 において受信したファームウェアダウンロードアドレスリストに設定されたダウンロードアドレスからダウンロード対象ファームをダウンロードする（ステップ S 2 2）。これにより、ファームウェア提供サーバ 1 0 3 から画像形成装置 1 0 1 に対してダウンロード対象ファームが配信される。

【 0 0 6 4 】

ステップ S 2 2 の処理において、ファームウェア提供サーバ 1 0 3 のファームウェア提供部 3 3 1 は、以下の処理を実行する配信手段として機能する。ファームウェア提供部 3 3 1 は、画像形成装置 1 0 1 に対して、復号モジュールを第 1 の通信経路（H T T P S による通信経路）により配信し、要求ファームを第 2 の通信経路（H T T P による通信経路）により配信する。

【 0 0 6 5 】

次に、ファームウェア更新部 3 1 5 が、ダウンロード対象ファームが復号モジュールを含むかを判断する（ステップ S 2 3）。ダウンロード対象ファームが復号モジュールを含まない場合は、ダウンロード対象ファームが要求ファームのみを含む。また、ダウンロード対象ファームが復号モジュールを含まないことは、配信管理サーバ 1 0 2 の提供部 3 2 3 が復号モジュールを選択しなかったこと、つまり、画像形成装置 1 0 1 が要求ファームを復号可能であることを意味する。

【 0 0 6 6 】

ダウンロード対象ファームが復号モジュールを含まない場合は、ステップ S 2 5 に進み、ファームウェア更新部 3 1 5 が、要求ファームを更新する。具体的には、ファームウェア更新部 3 1 5 が、現行ファームが含む復号モジュールで要求ファームを復号する。そして、ファームウェア更新部 3 1 5 が、現行ファームが含む更新用ソフトウェアを用いて、復号された要求ファームで現行ファームを更新する。

10

20

30

40

50

【 0 0 6 7 】

ダウンロード対象ファームが復号モジュールを含む場合は、ダウンロード対象ファームが、復号モジュールと要求ファームとを含む。ダウンロード対象ファームが復号モジュールを含むことは、配信管理サーバ 1 0 2 の提供部 3 2 3 が復号モジュールを選択したこと、つまり、画像形成装置 1 0 1 が要求ファームを復号可能でないことを意味する。ダウンロード対象ファームが復号モジュールを含む場合は、処理がステップ S 2 4 に進む。

【 0 0 6 8 】

ステップ S 2 4 において、ファームウェア更新部 3 1 5 が、復号モジュールの更新処理を実行する（ステップ S 2 4）。具体的には、ファームウェア更新部 3 1 5 は、ダウンロード対象ファームが含む復号モジュールを、現行ファームが含む復号モジュールを用いて復号する。そして、ファームウェア更新部 3 1 5 が、現行ファームが含む更新用ソフトウェアを用いて、上記復号された復号モジュールで現行ファームが含む復号モジュールを更新する。

10

【 0 0 6 9 】

次に、ファームウェア更新部 3 1 5 が、要求ファームを更新する（ステップ S 2 5）。具体的には、ファームウェア更新部 3 1 5 が、上記ステップ S 2 4 において更新された復号モジュールを用いて、ダウンロード対象ファームが含む要求ファームを復号する。そして、ファームウェア更新部 3 1 5 が、復号された要求ファームで、現行ファームを更新する。

【 0 0 7 0 】

なお、実施例 1 において、配信管理サーバ 1 0 2 は、画像形成装置 1 0 1 に対するファームウェアの配信管理を実行するが、配信管理サーバ 1 0 2 が、他のデータも含んで配信管理（例えば、アプリケーションを配信管理）するようにしてもよい。また、ファームウェア提供サーバ 1 0 3 が、複数のサーバから構成されるようにしてもよいし、世界で 1 つのユニークなサーバであってもよい。また、配信管理サーバ 1 0 2 が、配信管理サーバ 1 0 2 と同じサーバで動作するようにしてもよい。また、ネットワーク 1 0 4 は、企業内 LAN や WAN のように、ある程度閉じられたネットワークであってもよい。

20

【 0 0 7 1 】

また、例えば、復号モジュールが、ファームウェアに含まれるソフトウェアとして動作するのではなく、独立して実行可能であるソフトウェアであってもよい。復号モジュールが独立して実行可能である場合、ファームウェア提供サーバ 1 0 3 のファームウェア提供部 3 3 1 は、復号モジュール単体と、要求ファームとを、画像形成装置 1 0 1 に対して送信する。

30

【 0 0 7 2 】

復号モジュールと要求ファームとをダウンロードした画像形成装置 1 0 1 は、以下の処理を実行する。画像形成装置 1 0 1 は、当該復号モジュールを復号した上で更新し、更新した復号モジュールを用いて、要求ファームを復号する。

【 0 0 7 3 】

ファームウェア提供部 3 3 1 が、復号モジュールを、要求ファームの配信に先立って画像形成装置 1 0 1 に対して送信するようにしてもよい。そして、ファームウェア提供部 3 3 1 が、画像形成装置 1 0 1 が復号モジュールを適用した後に、要求ファームを画像形成装置 1 0 1 に対して配信するようにしてもよい。

40

【 0 0 7 4 】

次に、実施例 2 のネットワークシステムについて説明する。実施例 2 では、配信管理サーバ 1 0 2 が、画像形成装置 1 0 1 の対応暗号化バージョンと現行ファームのバージョンとの対応情報（以下、バージョン対応情報と記述）を、予め記憶手段に記憶している。

【 0 0 7 5 】

ファームウェア更新要求部 3 1 3 は、ファームウェア更新要求に、対応暗号化バージョンの代わりに現行ファームのバージョンを設定し、このファームウェア更新要求を配信管理サーバ 1 0 2 に対して送信する。

50

【 0 0 7 6 】

配信管理サーバ 1 0 2 の暗号化バージョン比較部 3 2 2 が、バージョン対応情報を参照して、画像形成装置 1 0 1 から受信したファームウェア更新要求が含む現行ファームのバージョンに対応する対応暗号化バージョンを取得する。そして、暗号化バージョン比較部 3 2 2 は、取得した対応暗号化バージョンと要求ファームの被暗号化バージョンとが合致するかを判断し、該判断結果に基づいて、ダウンロード対象ファームを復号可能であるかを判断する。

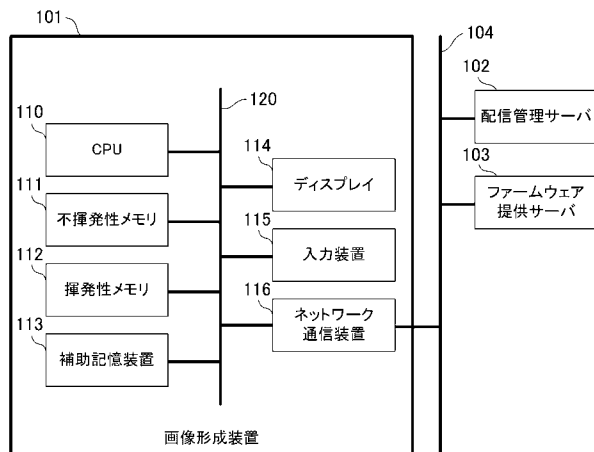
【 0 0 7 7 】

(その他の実施例)

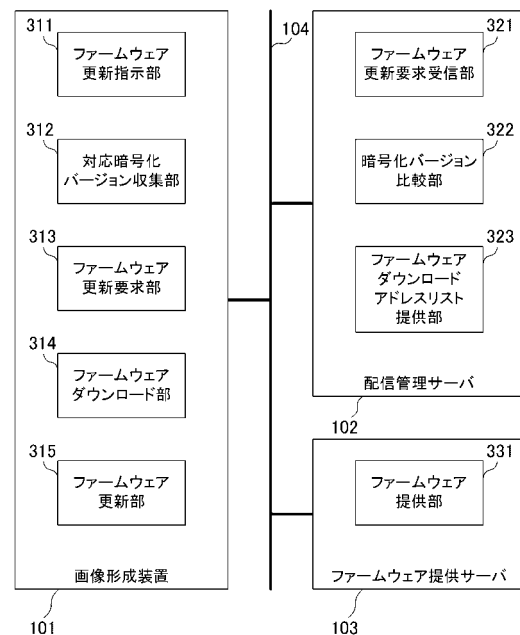
また、本発明は、以下の処理を実行することによっても実現される。即ち、上述した実施形態の機能を実現するソフトウェア（プログラム）を、ネットワーク又は各種記憶媒体を介してシステム或いは装置に供給し、そのシステム或いは装置のコンピュータ（または CPU や MPU 等）がプログラムを読み出して実行する処理である。この場合、そのプログラム、及び該プログラムを記憶した記憶媒体は本発明を構成することになる。

10

【 図 1 】



【 図 2 】



【図 3】

401

```
<?xml version="1.0" encoding="UTF-8">
<ファームウェア更新要求>
  <機種識別子>
    機種A
  </機種識別子>
  <デバイス識別子>
    XXX00001
  </デバイス識別子>
  <要求ファームウェアバージョン>
    03.00
  </要求ファームウェアバージョン>
  <対応暗号化バージョン>
    01.00
  </対応暗号化バージョン>
</ファームウェア更新要求>
```

【図 5】

501

識別番号	機種識別子	ファームウェアバージョン	被暗号化バージョン
1	機種A	01.00	01.00
2	機種A	01.01	01.00
3	機種A	01.02	01.00
4	機種A	02.00	02.00
5	機種A	03.00	03.00
6	機種B	01.00	01.00

【図 4】

701

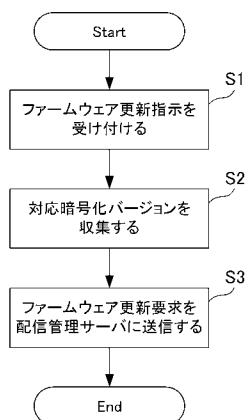
```
<?xml version="1.0" encoding="UTF-8">
<ファームウェアダウンロードアドレス>
  <復号化モジュール>
    https://firmware-upload.com/decrypt/ahiehrgeruoga8g
  </復号化モジュール>
  <メインコントローラ>
    http://firmware-upload.com/awoetgaiugoireagh5w5
  </メインコントローラ>
  <プリンタエンジンコントローラ>
    http://firmware-upload.com/oaergaergoujaeroljiergj
  </プリンタエンジンコントローラ>
</ファームウェアダウンロードアドレス>
```

【図 6】

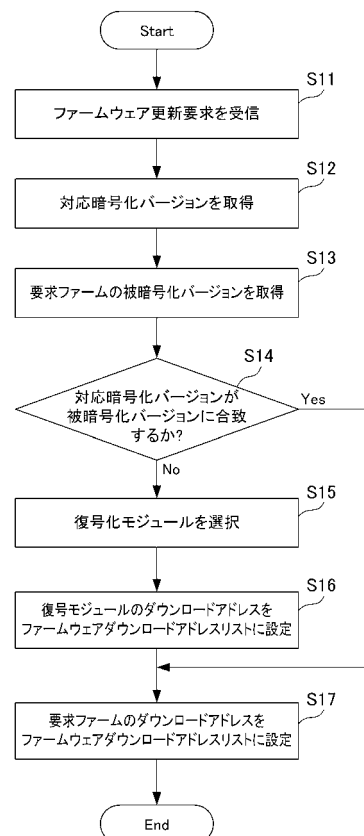
601

識別番号	機種識別子	対応暗号化バージョン	被暗号化バージョン
1	機種A	02.00	01.00
2	機種A	03.00	01.00
3	機種A	03.00	02.00
4	機種B	02.00	01.00

【図 7】



【図 8】



【 図 9 】

