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

特許第4974848号
(P4974848)

(45)発行日　平成24年7月11日(2012.7.11)　(24)登録日　平成24年4月20日(2012.4.20)

(51)Int.Cl.　　F I
G06F 13/00 (2006.01)　　G06F 13/00　353B
H04L 12/28 (2006.01)　　H04L 12/28　200M
G06F 21/20 (2006.01)　　G06F 21/20　144C

請求項の数 7　(全 19 頁)

(21)出願番号　特願2007-281835 (P2007-281835)
(22)出願日　平成19年10月30日 (2007.10.30)
(65)公開番号　特開2009-110261 (P2009-110261A)
(43)公開日　平成21年5月21日 (2009.5.21)
審査請求日　平成22年10月27日 (2010.10.27)

(73)特許権者　000001007
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　100126240
弁理士　阿部　琢磨
(74)代理人　100124442
弁理士　黒岩　創吾
(72)発明者　大橋　俊夫
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

審査官　寺谷　大亮

最終頁に続く

(54)【発明の名称】ネットワーク管理装置、ネットワーク管理方法、ならびにネットワーク管理方法を実行するプログラム

(57)【特許請求の範囲】
【請求項１】
通信の際に鍵情報を必要とするバージョンのＳＮＭＰ（Ｓｉｍｐｌｅ　Ｎｅｔｗｏｒｋ　Ｍａｎａｇｅｍｅｎｔ　Ｐｒｏｔｏｃｏｌ）を用いて周辺装置と通信するネットワーク管理装置であって、
前記周辺装置から複数種類の機器固有情報を取得する手段と、
前記バージョンのＳＮＭＰで通信する前に、複数の候補として、前記複数種類の機器固有情報のそれぞれを用いて鍵情報を生成する手段と、
前記周辺装置のＳＮＭＰエンジンＩＤを取得する取得手段と、
前記ＳＮＭＰエンジンＩＤがいずれの種類の機器固有情報に対応するものかを判断する判断手段と、
前記ＳＮＭＰエンジンＩＤを保持し、前記生成された複数の候補の中の、前記判断手段により前記ＳＮＭＰエンジンＩＤに対応すると判断された種類の機器固有情報に対応する鍵情報を用いて前記バージョンのＳＮＭＰで通信を行う通信手段と、
を有することを特徴とするネットワーク管理装置。
【請求項２】
前記複数種類の機器固有情報にはＭＡＣアドレス及びＩＰアドレスが含まれることを特徴とする請求項１に記載のネットワーク管理装置。
【請求項３】
前記ＳＮＭＰエンジンＩＤが前記ＩＰアドレスに対応するものであると前記判断手段が

判断し、かつ周辺装置に対して前記ＩＰアドレスを変更する要求が送信された場合に、保持している前記鍵情報の候補を更新する手段を有することを特徴とする請求項２に記載のネットワーク管理装置。

【請求項４】

周辺装置に設定されている設定情報を更新する指示を受け付ける手段と、

前記受け付けられた指示が、ＩＰアドレスの変更を指示するものであるか否かを判定する判定手段と、

ＳＮＭＰエンジンＩＤが機器固有情報としてのＩＰアドレスに対応する場合に、前記判定手段がＩＰアドレスの変更を指示するものであると前記判定手段が判定した場合は、変更前のＩＰアドレスを用いて生成された鍵情報を用いて前記バージョンのＳＮＭＰによる通信を行うことでＩＰアドレスの設定処理を実行し、変更後のＩＰアドレスを用いて鍵情報を再生成する手段とを有し、

前記判定手段がＩＰアドレスの変更を指示するものではないと判定した場合は、変更前のＩＰアドレスを用いて生成された鍵情報を用いて前記バージョンのＳＮＭＰによる通信を行うことで設定処理を実行した後に、鍵情報の再生成は行われないことを特徴とする請求項１に記載のネットワーク管理装置。

【請求項５】

前記判断手段は、ベンダー定義領域の領域に基づき判断を行うことを特徴とする請求項１乃至４のいずれか１項に記載のネットワーク管理装置。

【請求項６】

通信の際に鍵情報を必要とするバージョンのＳＮＭＰ（Ｓｉｍｐｌｅ　Ｎｅｔｗｏｒｋ　Ｍａｎａｇｅｍｅｎｔ　Ｐｒｏｔｏｃｏｌ）を用いて周辺装置と通信するネットワーク管理装置における方法であって、

前記周辺装置から複数種類の機器固有情報を取得する工程と、

前記バージョンのＳＮＭＰで通信する前に、複数の候補として、前記複数種類の機器固有情報のそれぞれを用いて鍵情報を生成する工程と、

前記周辺装置のＳＮＭＰエンジンＩＤを取得する取得工程と、

前記ＳＮＭＰエンジンＩＤがいずれの種類の機器固有情報に対応するものかを判断する判断工程と、

前記ＳＮＭＰエンジンＩＤを保持し、前記生成された複数の候補の中の、前記判断工程で前記ＳＮＭＰエンジンＩＤに対応すると判断された種類の機器固有情報に対応する鍵情報を用いて前記バージョンのＳＮＭＰで通信を行う通信工程と、

を有することを特徴とする方法。

【請求項７】

請求項１乃至５のいずれか１項に記載の手段としてコンピュータを機能させるための制御プログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、ネットワークデバイスを管理する方法、該方法を適用可能な装置、制御プログラム等に関するものである。

【背景技術】

【０００２】

ネットワーク管理プロトコルとして、ＳＮＭＰ（Ｓｉｍｐｌｅ　Ｎｅｔｗｏｒｋ　Ｍａｎａｇｅｍｅｎｔ　Ｐｒｏｔｏｃｏｌ）が近年注目されている。ＳＮＭＰには、例えばＳＮＭＰｖ１とＳＮＭＰｖ３の２つのバージョンが存在する。特にＳＮＭＰｖ３は、通信時の認証や暗号化などのセキュリティ機能が強化されている。そのため、セキュリティに関心の高い昨今では、プリンタなどのネットワークデバイスや、それらを管理するユーティリティソフトのＳＮＭＰｖ３対応が進んでいる。

【０００３】

ＳＮＭＰｖ３では、送受信する装置間でＳＮＭＰエンジンによって認証・暗号化通信を行う。ＳＮＭＰエンジンは、ユニークなＳＮＭＰエンジンＩＤと呼ばれる識別子によって識別され、ＳＮＭＰメッセージの認証・暗号化やネットワーク上への送受信などを行う。ＳＮＭＰｖ３の認証・暗号化仕様については、ＲＦＣ３４１４で定義されているユーザベース・セキュリティ・モデル（ＳＮＭＰｖ３ＵＳＭ）を用いるのが一般的である。ＳＮＭＰｖ３ＵＳＭでは、まずメッセージ送信前に周辺装置からＳＮＭＰエンジンＩＤを取得する。そして、取得したＳＮＭＰエンジンＩＤとパスワードを用いて認証・暗号化用の秘密鍵を生成し、認証・暗号化通信を行う。

【０００４】

しかし、ＳＮＭＰｖ３に限らず、認証・暗号化通信においては、毎回通信時にパラメータを取得して認証・暗号化用の鍵を生成すると、通信処理時間が長くなってしまうという問題がある。

【０００５】

そこで従来は、認証・暗号化通信において、毎回通信時にパラメータを取得して鍵を生成するのではなく、初回通信時に取得した鍵やパラメータをキャッシュして次回以降の通信で利用する方式が提案されていた（特開２０００－２７８２５８号公報、特開２００５－０８５０９０号公報）。

【０００６】

この方法は、鍵やパラメータがいつ取得及び生成しても変化しない場合に有効である。よって、この方法に拠れば、セキュリティを保ちながら通信処理時間を短縮することができる。

【非特許文献１】ＲＦＣ３４１４，”Ｕｓｅｒ－Ｂａｓｅｄ Ｓｅｃｕｒｉｔｙ Ｍｏｄｅｌ（ＵＳＭ） ｆｏｒ Ｖｅｒｓｉｏｎ ３ ｏｆ ｔｈｅ Ｓｉｍｐｌｅ Ｎｅｔｗｏｒｋ Ｍａｎａｇｅｍｅｎｔ Ｐｒｏｔｏｃｏｌ（ＳＮＭＰｖ３）”

【特許文献１】特開２０００－２７８２５８号公報

【特許文献２】特開２００５－０８５０９０号公報

【発明の開示】

【発明が解決しようとする課題】

【０００７】

しかし、ＳＮＭＰｖ３ＵＳＭにおいて通信時に取得する必要があるＳＮＭＰエンジンＩＤは、固有値であるＭＡＣアドレスだけではなく、動的に変化する可能性のあるＩＰアドレスや文字列・バイト列、ベンダー定義値なども取り得る。ＲＦＣ３４１４にもその旨定義されている。このため、その時々のエンジンＩＤにどの種別の値がセットされているかは取得するまで分からない。ＳＮＭＰエンジンＩＤに使われている種別によっては毎回取得するたびに同じ値が入っている保証もない。また、認証・暗号化に利用する鍵は、取得したＳＮＭＰエンジンＩＤより生成される。よって、従来技術のように初回通信時にキャッシュしたＳＮＭＰエンジンＩＤや鍵情報を次回通信時に利用することはできない。そのため、毎回通信時にＳＮＭＰエンジンＩＤを取得し、鍵生成する必要がある。このため、通信時間のスループットが長くなってしまっていた。

【課題を解決するための手段】

【０００８】

上記課題を解決するために、本発明におけるネットワーク管理装置は、通信の際に鍵情報を必要とするバージョンのＳＮＭＰ（Ｓｉｍｐｌｅ ＮｅｔｗｏｒｋＭａｎａｇｅｍｅｎｔ Ｐｒｏｔｏｃｏｌ）を用いて周辺装置と通信するネットワーク管理装置であって、前記周辺装置から複数種類の機器固有情報を取得する手段と、前記バージョンのＳＮＭＰで通信する前に、複数の候補として、前記複数種類の機器固有情報のそれぞれを用いて鍵情報を生成する手段と、前記周辺装置のＳＮＭＰエンジンＩＤを取得する取得手段と、前記ＳＮＭＰエンジンＩＤがいずれの種類の機器固有情報に対応するものかを判断する判断手段と、前記ＳＮＭＰエンジンＩＤを保持し、前記生成された複数の候補の中の、前記判断手段により前記ＳＮＭＰエンジンＩＤに対応すると判断された種類の機器固有情報に対

応する鍵情報を用いて前記バージョンのＳＮＭＰで通信を行う通信手段と、を有することを特徴とする。

【発明の効果】

【０００９】

本発明の一つの側面によれば、ネットワーク管理プロトコルにおける認証又は暗号化通信の前に、事前にＳＮＭＰエンジンＩＤの可能性がある値を取得した段階で鍵候補を生成しておくことで、通信時の鍵生成処理を削減することができるという有利な効果がある。

【００１０】

また、本発明の別の側面によれば、ＳＮＭＰエンジンＩＤの取得回数も削減するので、通信処理時間を短縮することができる。

【発明を実施するための最良の形態】

【００１１】

以下、本発明を実施するための形態の一例について、図面を参照して説明する。

【００１２】

＜＜システム構成＞＞

図１は、本発明における一実施形に係るネットワーク管理システムの全体構成を示す図である。図１において、ネットワーク管理システムはネットワーク１００により互いに接続されたコンピュータ１０１と画像処理装置１０２（被管理装置）から構成される。ネットワーク管理装置はネットワーク上に２台以上存在しても良い。

【００１３】

ネットワーク１００は、ＴＣＰ／ＩＰネットワークが構築可能で、ネットワーク経由で通信機器を監視・制御するＳＮＭＰプロトコルが利用可能であればよい。例えば、ＬＡＮなどが挙げられる。

【００１４】

コンピュータ１０１および画像処理装置１０２については、ハードウェア構成とソフトウェア構成に分けて説明する。画像処理装置は、画像処理を行う装置である。例えば、画像処理装置１０２は、プリンタ、ファクシミリ、スキャナ、及びこれらの複合機等が考えられる。図では、プリンタである場合の一例を示す。画像処理装置１０２は、本発明のネットワークデバイスの一例である。１０５はクライアントコンピュータであり、コンピュータ１０１内の管理ユーティリティ３０３と通信して各種情報をウェブブラウザで表示できる。

【００１５】

画像処理装置１０２は本発明の周辺装置の一例である。

【００１６】

＜コンピュータ１０１のハードウェア構成＞

図２に、コンピュータ１０１のハードウェア構成を示す。２０９は入力手段の一例であるキーボードや、マウスを制御する部分である。ＤＣ２０８は、表示手段の一例であるディスプレイを制御するコントローラである。

【００１７】

コンピュータ１０１は汎用コンピュータにより構成される。システムバス２００は、コンピュータを構成する各要素を接続する役割を持つ。ＣＰＵ（中央演算装置）２０１は、コンピュータ全体の制御および演算処理等を行う。ＲＡＭ（ランダムアクセスメモリ）２０２は、様々な処理ごとに各々のプログラムおよびデータがロードされ、実行される領域である。ＲＯＭ（読み出し専用メモリ）２０３は、システム起動プログラム等の記憶領域である。ＤＫＣ（外部記憶装置制御部）２０４は、ＨＤ（ハードディスク）２０７などの外部記憶装置の制御を行う。ＨＤ２０７は、プログラムおよびデータを記憶させておき、実行時必要に応じて参照またはＲＡＭへロードする。

【００１８】

コンピュータ１０１は、ＣＰＵが基本Ｉ／Ｏプログラムおよびｏｓを実行している状態で動作する。基本Ｉ／ＯプログラムはＲＯＭに書き込まれており、ＯＳはＨＤに書き込ま

れている。そしてコンピュータ部の電源がＯＮされたときに、基本Ｉ／Ｏプログラム中のイニシャルプログラムロード機能により、ＨＤからＯＳがＲＡＭに書き込まれ、ＯＳの動作が開始される。ネットワークＩ／Ｆ２０５は、ネットワークへ接続しネットワーク通信を行う。入出力Ｉ／Ｆ２０６は、キーボードやディスプレイなどに接続され、データの入出力を行う。１０５のクライアントコンピュータも基本的には同じ構成である。

【００１９】

＜コンピュータ１０１のソフトウェア構成＞

続いて、図３に、ネットワーク管理装置の一例であるコンピュータ１０１のソフトウェア構成を示す。コンピュータ１０１は、基本Ｉ／ＯプログラムおよびＯＳが実行状態にあることが前提で、Ｗｅｂサーバサービス、ＤＢサーバサービス、管理ユーティリティ３０３から構成される。これらのソフトウェアはプログラムとして図２のＨＤ２０７に書き込まれている。図３に記載のソフトウェア３０１、３０２、３０３、３１０，３１１，３１３，３１２は、図２のＣＰＵ２０１を用いてＲＡＭ２０２に書き込まれ実行される。

【００２０】

Ｗｅｂサーバサービス３０１は、クライアントコンピュータのＷｅｂブラウザからＨＴＴＰによるＧＥＴリクエストを受け取ると、ＨＤ２０７に保存されたＷｅｂページデータを返信するサービスを提供する。Ｗｅｂサーバサービスによって、外部からネットワーク経由でコンピュータ１０１へ接続することができる。なお、外部からコンピュータ１０１の管理ユーティリティ３０３へ接続する必要がない場合、Ｗｅｂサーバサービスは無くてもよい。

【００２１】

ＤＢサーバサービス３０２は、管理ユーティリティ３０３の利用するデータを格納し、格納されたデータを取得するサービスを提供する。ＤＢサーバサービスはコンピュータ１０１内でなく、ネットワークで接続された他のコンピュータ上に構成されていてもよい。管理ユーティリティ３０３内で独自にデータの格納・取得を行う場合は、ＤＢサーバサービスは無くてもよい。

【００２２】

管理ユーティリティ３０３は、ネットワーク接続された画像処理装置１０２と通信を行う。管理ユーティリティ３０３のユーザインタフェースとしてはウェブブラウザが利用できる。そして、画像処理装置１０２の設定の変更や状態監視などを行うソフトウェアである。この状態監視は、一定期間ごとであっても良い。管理ユーティリティ３０３は、探索モジュール３１０、デバイス情報設定モジュール３１１、認証情報管理モジュール３１３などの各機能モジュールと、ＳＮＭＰエンティティ３１２から構成される。なお、本実施例ではＳＮＭＰｖ３通信を行うモジュールの例としてデバイス情報設定モジュールを挙げているが、ＳＮＭＰ通信を行うモジュールであれば他機能のモジュールでもよい。探索モジュール３１０は、ネットワーク接続された画像処理装置を探索する機能を持つ。デバイス情報設定モジュール３１１は、既に探索済みのネットワーク接続された画像処理装置１０２などの設定情報をネットワーク経由で変更する機能を持つ。図１の複数の画像処理装置とＳＮＭＰｖ３で通信する場合、後述の認証情報管理モジュールが保存した認証情報を使用して通信を行う。認証情報管理モジュール３１３は、既に探索済みのネットワーク接続された画像処理装置について、ユーザが入力したＳＮＭＰｖ３パスワードを保存する機能を持つ。ＳＮＭＰエンティティ３１２は、コマンド送信アプリケーションとＳＮＭＰエンジンから構成され、ＳＮＭＰプロトコルにおける管理機能を実現する。コマンド送信アプリケーション３２０は、画像処理装置１０２を含むネットワーク機器の管理情報の取得・設定機能を持つ。ＳＮＭＰエンジン３２１は、ユニークなＳＮＭＰエンジンＩＤによって識別され、ＳＮＭＰメッセージの認証・暗号化やネットワーク上への送受信などを行う。１０５のクライアントコンピュータも基本的には同じ構成を持っていてもよい。ただし、ウェブブラウザのみが搭載されていても良い。

【００２３】

＜画像処理装置のハードウェア構成＞

図４に、画像処理装置の例として、ＭＦＰ（Ｍｕｌｔｉｆｕｎｃｔｉｏｎ Ｐｒｉｎｔｅｒ、多機能プリンタ）のハードウェア構成を示す。前述のとおり、画像処理装置にはＭＦＰ以外のものも含む（単機能プリンタ、ＦＡＸなど）。
画像処理装置１０２は、操作部、プリンタ、スキャナ、制御ユニットから構成される。制御ユニット（Ｃｏｎｔｒｏｌｌｅｒ Ｕｎｉｔ）４００は、ネットワークに接続され、コンピュータ１０１との間で通信を行う。操作部４０１、プリンタ４０２、スキャナ４０３は制御ユニットに接続され制御される。なお、画像処理装置には上記スキャナを有さないものも含まれる。

【００２４】

制御ユニットは、ＣＰＵ、ＲＡＭ、操作部Ｉ／Ｆ、ネットワークＩ／Ｆ、ＲＯＭ、ＨＤＤ、イメージバスＩ／Ｆ、システムバス、画像バス、ラスタイメージプロセッサ、デバイスＩ／Ｆ、スキャナ画像処理部、プリンタ画像処理部から構成される。なお、上記構成のうち、スキャナおよびスキャナ画像処理部はなくてもよい。ＣＰＵ４１０は、制御ユニット全体を制御するコントローラである。ＲＡＭ４１１は、ＣＰＵ４１０が動作するために使用するシステムワークメモリである。また、ＲＡＭは、画像データを一時記憶するための画像メモリでもある。操作部Ｉ／Ｆ４１２は、操作部との間のインタフェースをつかさどり、操作部に表示すべき画像データを操作部に対して出力する。また、使用者が操作部を介して入力した情報を、ＣＰＵに伝える役割を果たす。ネットワークＩ／Ｆ４１３は、ネットワークとの接続と、ネットワークへの情報の入出力をつかさどる。ＲＯＭ４１４はブートＲＯＭであり、システムのブートプログラムが格納されている。ＨＤＤ４１５は、ハードディスクドライブであり、システムソフトウェア、画像データを格納する。イメージバスＩ／Ｆ４１６は、システムバス４１７と画像データを高速で転送する画像バス４１８とを接続し、データ構造を変換するバスブリッジである。画像バス４１８は、ＰＣＩバスまたはＩＥＥＥ１３９４で構成される。ラスタイメージプロセッサ（ＲＩＰ）４１９は、ネットワークから送信されたＰＤＬコマンドをビットマップイメージに展開する。デバイスＩ／Ｆ部４２０は、画像入出力デバイスであるプリンタ４０２やスキャナ４０３と制御ユニットとを接続し、画像データの同期系／非同期系の変換を行う。スキャナ画像処理部４２１は、入力画像データに対し補正、加工、編集を行う。プリンタ画像処理部４２２は、プリント出力画像データに対して、プリンタの性能に応じた補正、解像度変換等を行う。

【００２５】

＜画像処理装置のソフトウェア構成＞

続いて、図５に、画像処理装置のソフトウェア構成を示す。画像処理装置はＳＮＭＰエンティティとＭＩＢから構成される。これらのソフトウェアはプログラムとしてＨＤＤ１５に記憶されている。ＣＰＵ４１０により、これらのソフトウェアはＲＡＭ４１１に書き込まれ実行される。ＳＮＭＰエンティティ５００は、ＳＮＭＰエンジンとコマンド応答アプリケーションから構成され、ＳＮＭＰプロトコルにおける管理機能を実現する。ＳＮＭＰエンジン５１０は、ユニークなＳＮＭＰエンジンＩＤによって識別され、ＳＮＭＰメッセージの認証・暗号化やネットワーク上への送受信などを行う。コマンド応答アプリケーション５１１は、コンピュータ１０１から受信した画像処理装置の管理情報取得・設定要求コマンドに対して、ＭＩＢオブジェクトにアクセスする。そして、アクセスしたＭＩＢオブジェクトをコンピュータ１０１に対して応答する機能を持つ。ＭＩＢオブジェクト５０１は、管理情報構造（ＳＭＩ）などで定義された、画像処理装置の管理情報を定義するオブジェクトである。例えば、プリンタステータス、エラー、プリンタの識別子、ジョブの情報、給紙排紙トレーの構成情報等、多彩な情報をオブジェクトとして定義できる。

【００２６】

ネットワークＩ／Ｆ部にＳＮＭＰエンティティを実装してもよい。

【００２７】

＜＜コンピュータ１０１の動作＞＞

次に、コンピュータ１０１の動作に関して説明する。コンピュータ１０１の動作は大き

く分けて、画像処理装置の探索、認証情報の登録、画像処理装置の設定変更の動作からなる。

【００２８】

＜探索時の動作＞

まず、コンピュータ１０１の管理ユーティリティ３０３が、探索モジュールを利用してネットワーク上から管理対象とする画像処理装置１０２を探索する。探索モジュールは任意のプロトコルで、ネットワーク接続された画像処理装置のＩＰアドレスとＭＡＣアドレスを取得するコマンドをブロードキャストアドレスで送信する。プロトコルは、管理対象とする画像処理装置のＩＰアドレスとＭＡＣアドレスが取得できれば、ＳＮＭＰｖ１でもＳＮＭＰｖ３でもＳＬＰ（Ｓｅｒｖｉｃｅ　Ｌｏｃａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）でも何でもよい。

【００２９】

ＳＮＭＰｖ３の場合は、探索モジュールがＳＮＭＰエンティティのコマンド送信アプリケーションを使って、ＳＮＭＰエンジンＩＤを取得するコマンドをブロードキャスト送信する。するとコマンド送信アプリケーションがＳＮＭＰエンジンを使って認証なし・暗号化なしのＳｅｃｕｒｉｔｙ　Ｌｅｖｅｌでパケットを送信する。画像処理装置側のＳＮＭＰエンジン５１０は、ＳＮＭＰエンジン５１０がＳＮＭＰエンジンＩＤ取得要求のパケットを受信する。すると、ＳＮＭＰエンジン５１０は、パケットの応答としてＳＮＭＰエンジンＩＤを送信する。コンピュータ１０１側のＳＮＭＰエンジンが応答を受信した場合、その応答を送信した画像処理装置１０２が、ネットワーク上の管理対象デバイスとなる。その後は管理対象の画像処理装置１０２に任意のプロトコルでＭＡＣアドレス取得コマンドを送信してＭＡＣアドレスを取得する。

【００３０】

＜認証情報登録時の動作＞

探索によってコンピュータ１０１の管理対象となった画像処理装置のうち、ＳＮＭＰｖ３対応のものについては通信時に認証情報が必要になる。そこで、図６の認証情報登録画面で、ユーザに認証情報を入力してもらう。すなわち、管理ユーティリティ３０３の図６の画面をクライアントコンピュータ１０５のディスプレイに表示する。そして、クライアントコンピュータ１０５のキーボードやマウスにより入力された認証情報を取得する。

【００３１】

図６は、クライアントコンピュータ１０５からコンピュータ１０１の管理ユーティリティ３０３にＷｅｂブラウザでアクセスした際に、クライアントコンピュータ１０５のディスプレイに表示した認証情報登録画面の例を示す。図６の例では、ＳＮＭＰｖ３対応の画像処理装置がリストアップされ、各画像処理装置について認証情報を入力しコンピュータ１０１に登録できるようになっている。６００はＷｅｂブラウザのＵＩである。６０１はＳＮＭＰｖ３対応の画像処理装置の名称である。図１の１０２乃至１０４に対応する。６０２はＳＮＭＰｖ３対応の画像処理装置のＩＰアドレスである。６０３はＳＮＭＰｖ３の認証情報であるユーザ名の入力欄である。６０４は同様にＳＮＭＰｖ３の認証情報である認証パスワード、６０５は認証に用いるハッシュアルゴリズム、６０６は暗号化パスワード、６０７はコンテキスト名の入力欄である。更新ボタン６０８を押すと、各欄に入力された認証情報をクライアントコンピュータ１０５からコンピュータ１０１に対して送信する。そして、コンピュータ１０１がその認証情報をＤＢサーバサービス３０２に保存する。キャンセルボタン６０９を押すと認証情報の登録をクライアントコンピュータ１０５はキャンセルする。なお、認証情報のパラメータについては、必ずしも６０３から６０７までの全項目を入力させる必要はない。場合に応じてコンテキスト名は入力させずにシステムで固定の値を使用する、等のカスタマイズを行ってもよい。もちろん、本例のように個々の画像処理装置ごとに認証情報を管理せずに、管理している画像処理装置すべてに同じ認証情報を登録し、クライアントコンピュータ１０５からコンピュータ１０１へ送信してもよい。図７に、図６で更新ボタンが押された際の、コンピュータ１０１における認証情報登録の処理の流れを示す。図６の画面は前述のとおりクライアントコンピュータ１０５

上に表示される。クライアントコンピュータ１０５のマウスやキーボードを使って、更新指示が入力される。この指示は更新６０８がユーザにより押下されることに応答して、クライアントコンピュータ１０５からコンピュータ１０１へ送信される。この際送信されるのは、図６の画面を介した全ての入力である。これらの入力は、コンピュータ１０１の管理ユーティリティ３０３により受信され、処理される。この情報の受信により、図７の処理を管理ユーティリティ３０３が開始する。

【００３２】

Ｓ７００で、既に画像処理装置の探索が行われたかを確認する。未探索の場合は、認証情報は保存する必要が無いので処理を終了する。探索済みの場合、Ｓ７０１で探索済みの画像処理装置の情報をＤＢサーバサービス３０２から取得する。そしてＳ７０２で画像処理装置がＳＮＭＰｖ３対応デバイスかを判定する。

【００３３】

画像処理装置１０２がＳＮＭＰｖ３対応デバイスでないと判定された場合、認証情報を保存する必要がないので処理を終了する。ＳＮＭＰｖ３対応デバイスと判定された場合は、Ｓ７０３で、ユーザが入力した認証情報をＤＢへ保存する。なお、保存された認証情報は、ＳＮＭＰｖ３で画像処理装置１０２と通信を行う際に使用される。Ｓ７０４で、保存された認証情報が、以前保存された認証情報から変更されているかを判定する。認証情報が変更されたと判定された場合、Ｓ７０５で認証情報と画像処理装置情報を元にＳＮＭＰｖ３通信用の鍵候補を生成する。そしてＳ７０６で生成した鍵候補をＤＢに保存する。Ｓ７０２からＳ７０６までを、管理対象となっているすべてのＳＮＭＰｖ３対応の画像処理装置１０２に関して行う。認証情報が変更されていないと判定された場合は、その画像処理装置に関する認証情報の登録処理を終了する。

【００３４】

Ｓ７０５で説明した鍵候補の生成方法の詳細例を図８に示す。まず、画像処理装置１０２等のＩＰアドレスとＭＡＣアドレスから、ＳＮＭＰエンジンＩＤ候補８０１を生成する。ＳＮＭＰエンジンＩＤ候補はＲＦＣ３４１１に記載されたＳＮＭＰエンジンＩＤの定義を元に生成する。先頭ビット８０２は”１”がＳＮＭＰｖ３形式を表す。企業番号８０３は４バイトの企業番号を入力する。種別８０４は識別データ８０５の種別を表す１バイトデータである。”１”がＩＰｖ４アドレス、”２”がＩＰｖ６アドレス、”３”がＭＡＣアドレスを表す。識別データ８０５には、画像処理装置情報の内、種別８０４に相当する情報が入る。そして、パスワード８００とＳＮＭＰエンジンＩＤ候補８０２を元に、ＳＮＭＰｖ３ＵＳＭで定義されたローカル秘密鍵生成方式を使って鍵候補８０６を生成する。

【００３５】

＜画像処理装置１０２の設定変更時の動作＞

管理ユーティリティ３０３は、画像処理装置１０２の探索および正しい認証情報の保存が終わると、画像処理装置１０２とＳＮＭＰｖ３プロトコルによる通信が可能になる。ＳＮＭＰｖ３通信の例として、今回は画像処理装置１０２の設定変更処理を挙げて説明する。図９に、管理ユーティリティ３０３が画像処理装置１０２の設定を変更する際の処理の流れを示す。

【００３６】

Ｓ９００で設定項目入力画面を表示し、画像処理装置１０２の変更する設定項目をユーザに入力させる。クライアントコンピュータ１０５からコンピュータ１０１の管理ユーティリティ３０３にＷｅｂブラウザでアクセスして表示した設定項目入力画面の例を図１０に示す。１０００はデバイス情報の設定項目欄、１００１は通信設定の設定項目欄である。各項目のチェックボックスを選択してテキストボックスに変更する値を設定し、更新ボタン１００２を押すと設定が変更される。すなわち、図１０の各フィールドに入力された内容が、クライアントコンピュータ１０５からコンピュータ１０１へと送信される。その後、すぐに図９の処理が開始する。キャンセルボタン１００３を押すと設定変更をキャンセルする。図９は管理ユーティリティ３０３の処理である。図１０では、デバイス名、設置場所、管理社名、管理者連絡先、管理者コメント、サービス担当者名、サービス担当者

連絡先、サービス担当者コメントを入力可能である。また、フレームタイプ、ＤＨＣＰやＢＯＯＴＰ、ＲＡＲＰ，サブネットマスク、ゲートウェイアドレス、ＬＰＤ印刷、や各種サーバのアドレスや名前が入力可能である。ここで、特に重要な情報はＩＰアドレスである。この情報は個別の設定画面にて別途入力でき、他の情報と同様に、３０３から画像処理装置１０２に対して指示に応じて送信される。

【００３７】

設定変更項目の入力後、Ｓ９０１でＤＢ３０２から画像処理装置１０２の情報を取得する。ここで取得する情報はＩＰアドレスなど、管理ユーティリティ３０３が画像処理装置１０２と通信を行うのに必要な情報である。そして、Ｓ９０２で画像処理装置１０２がＳＮＭＰｖ３対応デバイスかどうかを判定する。もしＳＮＭＰｖ３対応デバイスでないと判定されれば、Ｓ９０４でＳＮＭＰｖ３以外の通信可能なプロトコルを使って画像処理装置１０２の設定を変更して終了する。

【００３８】

もし画像処理装置１０２がＳＮＭＰｖ３対応デバイスと判定された場合は、Ｓ９０３で画像処理装置１０２の設定を行う。Ｓ９０３のＳＮＭＰｖ３による設定変更処理の流れを、さらに細かく図１１に示す。

【００３９】

まず、Ｓ１１００で、画像処理装置１０２のＳＮＭＰエンジンと通信を行うためのＳＮＭＰエンジンＩＤを取得する。ＳＮＭＰｖ３ＵＳＭでは、ＮｏＡｕｔｈ／ＮｏＰｒｉｖのセキュリティレベルでＳＮＭＰリクエストメッセージを送信することでＳＮＭＰエンジンＩＤを取得できる。なお、その際にはｍｓｇＡｕｔｈｏｒｉｔａｔｉｖｅ ＥｎｇｉｎｅＩＤ・ｍｓｇＵｓｅｒＮａｍｅの長さを０にし、ｖａｒＢｉｎｄＬｉｓｔを空にする必要がある。そして、Ｓ１１０１とＳ１１０２で取得したＳＮＭＰエンジンＩＤの種別がＭＡＣアドレスもしくはＩＰアドレスかどうかを判定する。もしＳＮＭＰエンジンＩＤがＭＡＣアドレスと判定されれば、Ｓ１１０７に進み、Ｓ７０６で生成した鍵候補のうち、ＭＡＣアドレスを元に生成した鍵候補をＤＢ３０２から取得する。もしＳＮＭＰエンジンＩＤがＩＰアドレスと判定されれば、Ｓ１１０８に進み、同様にＩＰアドレスを元に生成した鍵候補をＤＢから取得する。ＭＡＣアドレスやＩＰアドレスは、基本的に通信中に変動しない。（ＩＰアドレスは外部から変更される場合があるが、通信中に変更された場合は画像処理装置１０２と通信不可となるので、再探索が必要となる。）そこでＳ１１０９で、取得したＳＮＭＰエンジンＩＤと鍵候補を利用して、画像処理装置１０２の設定変更を行うリクエストすべての送信を行う。これにより、リクエスト送信時に毎回ＳＮＭＰエンジンＩＤの取得と鍵生成を行う必要が無くなり、通信処理時間を短縮することができる。もしＳＮＭＰエンジンＩＤがＭＡＣアドレスでもＩＰアドレスでもない場合は、ＳＮＭＰエンジンＩＤは変動する可能性があるので、毎回リクエスト送信時にＳＮＭＰエンジンＩＤの取得と鍵生成を行う。Ｓ１１０３でＳＮＭＰエンジンＩＤを取得し、Ｓ１１０４でエンジンＩＤが更新されているかを判定する。もしＳＮＭＰエンジンＩＤが更新されていると判定されれば、Ｓ１１０５でＤＢから取得した認証情報とＳＮＭＰエンジンＩＤを利用して鍵を生成してからＳ１１０６へ進む。ＳＮＭＰエンジンＩＤが更新されていないと判定されれば、そのままＳ１１０６へ進む。そしてＳ１１０６でＳＮＭＰエンジンＩＤと鍵を利用してリクエストを送信する。

【００４０】

なお、本実施例では、ＭＡＣアドレスおよびＩＰアドレスを画像処理装置１０２固有の変動しない値として扱ったが、ＳＮＭＰエンジンＩＤの種別が文字列やバイト列の場合でも、同様に機器固有情報として扱ってもよい。また、ＩＰアドレスを変動する情報とし、ＭＡＣアドレスを変動しない機器固有情報として扱うことも可能である。

【００４１】

次に、ＳＮＭＰエンジンＩＤがＩＰアドレスで、かつコンピュータ１０１がＳＮＭＰｖ３で通信中にＩＰアドレスを変更する場合について説明する。

【００４２】

なお、システム構成は最初の実施形態と同様である。また、探索および認証情報登録時のコンピュータ１０１の動作についても、最初の実施形態と同様の処理をする。

【００４３】

＜画像処理装置１０２の設定変更時の動作＞

コンピュータ１０１による画像処理装置１０２の設定変更時の動作についても、図９までは最初の実施形態と同様である。最初の実施形態と異なる部分を説明する。ここでは、図９におけるＳ９０３の内容について図１２で説明する。

【００４４】

図１２は、コンピュータ１０１上の管理ユーティリティ３０３がＳＮＭＰｖ３プロトコルで画像処理装置１０２の設定を変更する際の詳細な処理の流れを示す。下記は３０３での処理である。Ｓ１１００からＳ１１０９については、図１１と同じなので説明を省略する。Ｓ１２００は、ＳＮＭＰエンジンＩＤがＩＰアドレスの場合に、リクエストを送信した後の処理になり、送信されたリクエストがＩＰアドレスを変更する内容かどうかを判定する。もし送信リクエストがＩＰアドレスを変更する内容と判定された場合、Ｓ１２０１で、変更後のＩＰアドレスを使ってＳＮＭＰエンジンＩＤを更新する。そして、Ｓ１２０２で更新後のＳＮＭＰエンジンＩＤとＤＢ３０２から取得した認証情報を使って鍵候補を再生成する。次回以降の送信リクエストからは、変更後のＩＰアドレスと、更新したＳＮＭＰエンジンＩＤと鍵候補を使って、送信を行う。これにより、コンピュータ１０１が送信リクエストの途中で、画像処理装置１０２のＩＰアドレスを自ら変更した場合も、残りの送信リクエストが正しく画像処理装置１０２のＳＮＭＰエンジンに送信される。もし送信リクエストがＩＰアドレスを変更する内容ではないと判定された場合は、Ｓ１１０３に進む。Ｓ１１０３以降は図１１と同様の処理になるので、説明は省略する。鍵候補を生成して、Ｓ１２００で旧い鍵と取り替えるタイミングは、ＩＰアドレスの設定変更を確実に確認してからにするとよい。すなわち、仮の鍵候補として用意し、変更を確認してから旧い鍵候補を消去するようにすると良い。

【００４５】

一番先に説明した実施形態では、画像処理装置１０２の探索後、認証情報登録時に鍵候補を生成し、ＳＮＭＰｖ３通信の初回通信時にＳＮＭＰエンジンＩＤの取得と鍵候補から利用する鍵の選択をおこなった。本実施形態では、認証情報登録時にＳＮＭＰエンジンＩＤを事前取得し、鍵を生成してキャッシュしておく方法を説明する。

【００４６】

なお、システム構成ならびに、探索時のコンピュータ１０１の動作については、最初の実施形態と同様のため省略する。

【００４７】

＜認証情報登録時の動作＞

図１３は、コンピュータ１０１における認証情報登録の処理の流れを示す。なおＳ７００からＳ７０５は、最初の実施形態の図７と同じなので省略する。ユーザ入力された認証情報が更新されると、Ｓ１３００で画像処理装置１０２のＳＮＭＰエンジンのＳＮＭＰエンジンＩＤを取得する。ＳＮＭＰエンジンＩＤの取得方法は最初の実施形態のＳ１１００と同様である。そして、Ｓ１３０１で取得したＳＮＭＰエンジンＩＤがＭＡＣアドレスもしくはＩＰアドレスかどうかを判定する。もしＳＮＭＰエンジンＩＤがＭＡＣアドレスかＩＰアドレスであると判定されれば、Ｓ１３０２においてＳＮＭＰｖ３通信で認証・暗号化に利用する鍵を生成する。鍵の生成方法は最初の実施形態の図８と同様である。そしてＳ１３０３で、生成した鍵をＤＢ３０２に保存する。

【００４８】

＜画像処理装置１０２の設定変更時の動作＞

画像処理装置１０２の設定変更時におけるコンピュータ１０１の動作は最初の実施形態と同様である。また、ＳＮＭＰｖ３での通信までは最初の実施形態と同様である。最初に説明した実施例と異なる部分を中心に説明する。図９におけるＳ９０３の内容について、図１４で説明する。

【００４９】
図１４は、コンピュータ１０１によるＳＮＭＰｖ３での画像処理装置１０２の設定変更処理を示す。Ｓ１４００で、既に認証情報登録時にＳＮＭＰエンジンＩＤと鍵がＤＢ３０２に保存されているかどうかを判定する。もしＤＢにＳＮＭＰエンジンＩＤと鍵が保存されていると判定されれば、Ｓ１１０３からＳ１１０６でＳＮＭＰエンジンＩＤを取得し、エンジンＩＤが更新されていれば鍵を生成する。そしてＳＮＭＰエンジンＩＤと鍵を使ってＳＮＭＰｖ３でリクエスト送信を行う。これを全送信リクエストについて繰り返す。一方、もしＤＢにＳＮＭＰエンジンＩＤと鍵が保存されていないと判定された場合は、Ｓ１４０１でＳＮＭＰエンジンＩＤを、Ｓ１４０２で鍵をＤＢから取得する。そして、取得したＳＮＭＰエンジンＩＤと鍵を利用して、Ｓ１４０３でＳＮＭＰｖ３による認証・暗号化通信で全リクエストを送信する。
【００５０】
その他の実施例を説明する。最初の実施例では、コンピュータ１０１が画像処理装置１０２を探索してから、認証情報の登録を行い、その上で画像処理装置１０２の設定変更を行った。本実施例では、画像処理装置１０２を探索し、認証情報登録時に鍵候補を生成した後でＩＰアドレスが変更された場合に鍵候補を更新する方法について説明する。
【００５１】
なお、システム構成ならびに、認証情報登録、設定変更時のコンピュータ１０１の動作については、最初の実施例と同様のため省略する。本実施例では、画像処理装置探索時の、コンピュータ１０１の動作についてのみ図１５にて説明する。
【００５２】
まずＳ１５００で、ネットワーク上の画像処理装置１０２の探索を行う。探索方法は最初の実施形態で説明したとおりである。次にＳ１５０１で、探索された画像処理装置１０２が新規に探索されたデバイスかどうかを判定する。もし新規に探索されたと判定された場合は、Ｓ１５０３に進む。既に探索されたことのあるデバイスと判定された場合は、Ｓ１５０２でＩＰアドレスが以前の探索結果から変更されていないかを判定する。ＩＰアドレスの変更が無いと判定されれば、鍵候補の再生成の必要は無いので、そのまま処理を終了する。もしＩＰアドレスが変更されていると判定された場合は、Ｓ１５０３へ進む。そしてＳ１５０３では認証情報が登録されているかを判定する。もし認証情報が登録されていると判定されれば、Ｓ１５０４で鍵候補を再生成し、Ｓ１５０５で再生成した鍵をＤＢ３０２へ保存する。以上の処理で、画像処理装置１０２が探索され、認証情報登録時に鍵候補が生成された後でＩＰアドレスが変更されても、再探索時に鍵候補が自動で再生成される。以上は３０３での処理である。
【００５３】
最後の実施例について説明する。最初の実施形態では、ＳＮＭＰエンジンＩＤの種別がＭＡＣアドレスもしくはＩＰアドレスの場合に、ＳＮＭＰエンジンＩＤと事前生成した鍵候補をキャッシュして使用した。本実施例では、ＳＮＭＰエンジンＩＤ種別のベンダー定義可能領域を利用して通信処理の高速化を図る例を示す。
【００５４】
図８におけるＳＮＭＰエンジンＩＤ８０１において、種別８０４はＲＦＣ３４１１で定義されている。ＲＦＣ３４１１では、種別値が１２８から２５５まではベンダー定義可能と定義されている。そこで、本実施例では図１７に示すように、画像処理装置１０２とコンピュータ１０１が利用するＳＮＭＰエンジンＩＤの種別におけるベンダー定義領域を、固定値領域と変動値領域で分割する。これにより、コンピュータ１０１と画像処理装置１０２がＳＮＭＰｖ３プロトコルで通信する際に、毎回ＳＮＭＰエンジンＩＤを取得する必要があるかどうかを画像処理装置１０２からコンピュータ１０１に通知する。
【００５５】
次に、コンピュータ１０１によるＳＮＭＰｖ３での画像処理装置１０２の設定変更の流れを図１６に示す。なお、画像処理装置１０２ならびにコンピュータ１０１が図１７のＳＮＭＰエンジンＩＤ設定を利用していることと、予め探索と認証情報登録が完了している

ことが前提となる。

【００５６】

まずＳ１６００で、ＳＮＭＰエンジンＩＤを取得する。エンジンＩＤの取得方法は最初の実施形態のＳ１１００と同様である。そしてＳ１６０１で、取得したＳＮＭＰエンジンＩＤの種別がベンダー定義領域かを判定する。もしベンダー定義領域でないと判定されれば、Ｓ１６０３からＳ１６０６で、毎回リクエスト送信時にＳＮＭＰエンジンＩＤを取得し、エンジンＩＤが更新されていれば鍵生成を行う。そしてＳＮＭＰエンジンＩＤと鍵を使ってＳＮＭＰｖ３でリクエストを送信する。もしベンダー定義領域と判定されたら、Ｓ１６０２でエンジンＩＤの種別が固定値を示す領域かどうかを判定する。もし固定値であると判定されれば、Ｓ１６０７で一回鍵を生成したら、あとは生成した鍵とＳＮＭＰエンジンＩＤを利用してＳ１６０８でリクエストの送信を行う。一方、もしＳＮＭＰエンジンＩＤの種別が変動値と判定されれば、Ｓ１６０３からＳ１６０６で、毎回リクエスト送信時にＳＮＭＰエンジンＩＤを取得し、エンジンＩＤ更新時には鍵生成を行い、リクエストを送信する。以上のように、ＳＮＭＰエンジンＩＤの種別フィールドにおけるベンダー定義領域を利用して、ＳＮＭＰエンジンＩＤを毎回通信ごとに取得する必要があるかどうかを判別する。それによって、ＳＮＭＰエンジンＩＤの取得と鍵生成の回数を削減することができ、通信処理時間を短縮することができる。すなわち、ベンダー定義領域において、エンジンＩＤをどの領域に固定値を格納し、どの領域に固定値でない値を格納するかを予め定めておく、そして、エンジンＩＤがどの領域から取得されるかで固定値か固定値でないかを決定するものとする。

【００５７】

以上説明したように、通信の際に鍵を必要とするバージョンのＳＮＭＰ（Ｓｉｍｐｌｅ Ｎｅｔｗｏｒｋ Ｍａｎａｇｅｍｅｎｔ Ｐｒｏｔｏｃｏｌ）を用いて周辺装置と通信するコンピュータ１０１が開示された。

【００５８】

周辺装置の一例である画像処理装置１０２乃至１０４から機器固有情報の一例である機器固有情報を取得する管理ユーティリティ３０３が開示された。ＳＮＭＰエンジンＩＤとして、ＭＡＣアドレスやＩＰアドレスなどがあげられる。

【００５９】

ＳＮＭＰＶ３による通信の前に、機器固有情報から鍵情報の一例である図８に示す情報を生成する。そして、管理ユーティリティ３０３は、画像処理装置１０２０を識別するＳＮＭＰエンジンＩＤを取得する。さらに、管理ユーティリティ３０３は、ＳＮＭＰエンジンＩＤが前記機器固有情報に対応するものかを判断する。例えば、ＳＮＭＰエンジンＩＤがＩＰアドレスはＭＡＣアドレスそのものであるかを判定する。又は、ＳＮＭＰエンジンＩＤが、それらのアドレスに対して所定のエンコード処理をしたものかどうかを判定する。

【００６０】

さらに、ＳＮＭＰエンジンＩＤが機器固有情報に対応するものであると管理ユーティリティ３０３が判断した場合に、前記ＳＮＭＰエンジンＩＤを保持する。そして、管理ユーティリティ３０３は、生成した鍵情報を用いてＳＮＭＰで通信を行う。これらの処理はネットワーク管理装置の一例であるコンピュータ１０１で実行される。

【００６１】

ＳＮＭＰエンジンＩＤが機器固有情報に対応するものであると管理ユーティリティ３０３が判断し、かつ周辺装置に対して前記機器固有情報を変更する要求が送信された場合に、保持している前記鍵候補を管理ユーティリティ３０３は更新する。

【００６２】

管理ユーティリティ３０３が取得したＳＮＭＰエンジンＩＤが変動値か固定値かを判断する。

【００６３】

管理ユーティリティ３０３は、ＳＮＭＰエンジンＩＤが固定値の場合に、通信セッショ

ン完了までＳＮＭＰエンジンＩＤを保持し、そのＳＮＭＰエンジンＩＤを用いて鍵情報を生成し、鍵情報を利用してＳＮＭＰで通信を行うようにしてもよい。

【００６４】

管理ユーティリティ３０３は、画像処理装置１０２に設定されている設定情報を更新する指示を受け付ける。

【００６５】

管理ユーティリティ３０３は、受け付けられた指示が、ＩＰアドレスの変更を指示するものであるか否かを判定する。

【００６６】

ＳＮＭＰエンジンＩＤがＩＰアドレスである場合、管理プログラムがＩＰアドレスの変更を指示するものであると判定した場合は、次の処理をする。すなわち管理ユーティリティ３０３は、変更前のＩＰアドレスを用いて生成された鍵候補を用いてＳＮＭＰによるＩＰアドレスの設定処理を実行する。さらに、管理ユーティリティ３０３は、変更後のＩＰアドレスを用いて鍵候補を再生成する。一方、管理ユーティリティ３０３がＩＰアドレスの変更を指示するものではないと判定した場合は、次の処理をする。すなわち、管理ユーティリティ３０３は、変更前の鍵候補でＳＮＭＰによる設定処理を実行して鍵候補を再生成しないようにする。

【００６７】

本実施形態における各図に示す処理が、外部からインストールされるプログラムによって、コンピュータ１０１などにより遂行される。そして、その場合、ＣＤ－ＲＯＭやフラッシュメモリやＦＤ等の記憶媒体により、あるいはネットワークを介して外部の記憶媒体から、プログラムを含む情報群をホストコンピュータに供給される場合でも本発明は適用されるものである。

【００６８】

以上のように、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体を、システムあるいは装置に供給し、又は、外部サーバ（図示省略）からダウンロードすることで、そのシステムあるいは装置のコンピュータ（またはＣＰＵやＭＰＵ）が記憶媒体に格納されたプログラムコードを読出し実行することによっても、本発明の目的が達成されることは言うまでもない。

【００６９】

この場合、記憶媒体から読み出されたプログラムコード自体が本発明の新規な機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。プログラムコードを供給するための記憶媒体としては、たとえば、フロッピィーディスク、ハードディスク、光ディスク、光磁気ディスク、ＤＶＤ、ＣＤ－ＲＯＭ、磁気テープ、不揮発性のメモリカード、ＲＯＭ、ＥＥＰＲＯＭ等を用いることができる。

【００７０】

また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているＯＳ（オペレーティングシステム）等が実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。さらに、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵ等が実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【図面の簡単な説明】

【００７１】

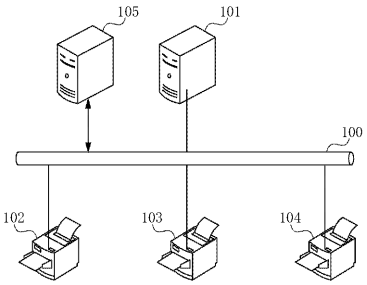
【図１】本実施形態のシステム構成の一例を示す図である。

【図２】図１のコンピュータ１０１ハードウェア構成の一例を示す図である。

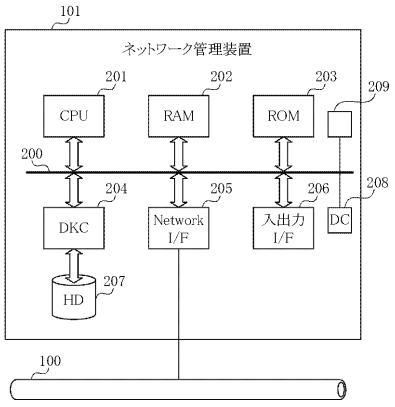
【図３】図１のコンピュータ１０１のソフトウェア構成の一例を示す図である。

【図４】図１の画像処理装置１０２のハードウェア構成の一例を示す図である。
【図５】画像処理装置１０２のソフトウェア構成の一例を示す図である。
【図６】認証情報入力画面の一例を示す図である。
【図７】認証情報登録フローチャートの一例を示す図である。
【図８】鍵生成方法の一例を示す図である。
【図９】画像処理装置１０２の設定変更フローチャートの一例を示す図である。
【図１０】設定項目入力画面の一例を示す図である。
【図１１】画像処理装置１０２の設定変更詳細フローチャートの一例を示す図である。
【図１２】画像処理装置１０２の設定変更詳細フローチャートの一例を示す図である。
【図１３】認証情報登録の処理の流れの一例を示す図である。
【図１４】画像処理装置１０２の設定変更詳細フローチャートの一例を示す図である。
【図１５】探索時フローチャートの一例を示す図である。
【図１６】画像処理装置１０２の設定変更詳細フローチャートの一例を示す図である。
【図１７】ＳＮＭＰエンジンＩＤ種別分類表の一例を示す図である。

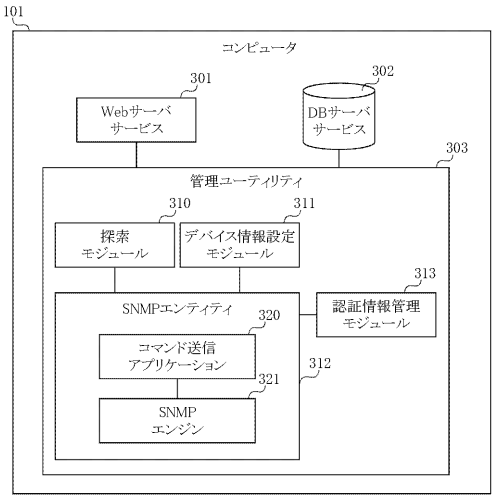
【図１】



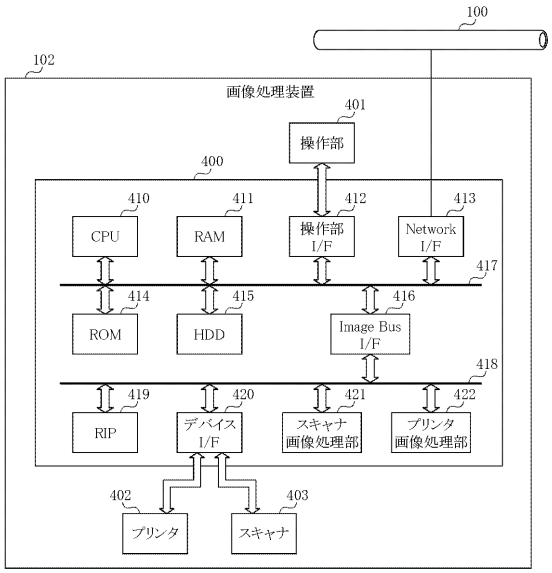
【図２】



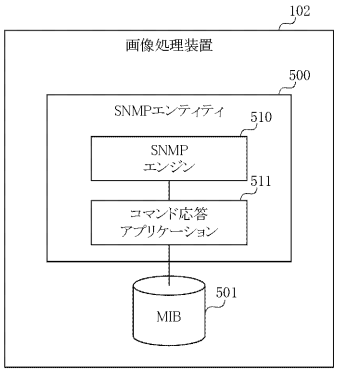
【図３】


101
コンピュータ
301
Webサーバ
サービス
302
DBサーバ
サービス
303
管理ユーティリティ
310
探索
モジュール
311
デバイス情報設定
モジュール
313
認証情報管理
モジュール
SNMPエンティティ
320
コマンド送信
アプリケーション
321
SNMP
エンジン
312

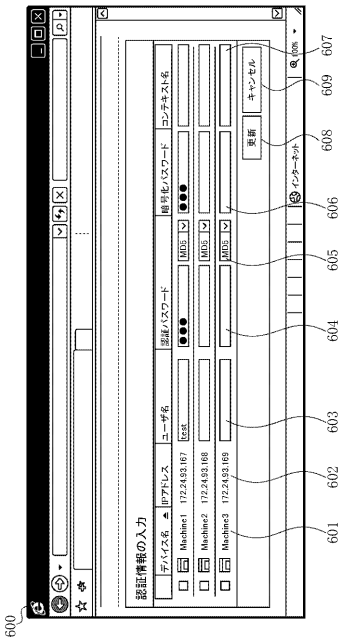
【図４】


100
102
画像処理装置
401
操作部
400
410
CPU
411
RAM
412
操作部
I/F
413
Network
I/F
417
414
ROM
415
HDD
416
Image Bus
I/F
418
419
RIP
420
デバイス
I/F
421
スキャナ
画像処理部
422
プリンタ
画像処理部
402
プリンタ
403
スキャナ

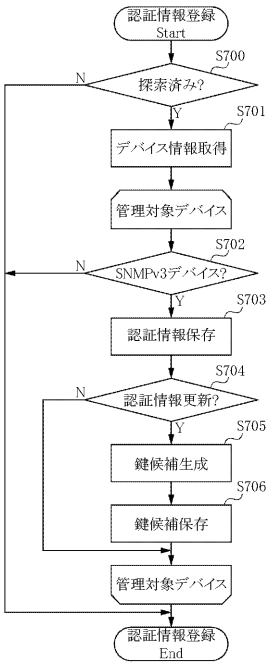
【図５】


102
画像処理装置
500
SNMPエンティティ
510
SNMP
エンジン
511
コマンド応答
アプリケーション
501
MIB

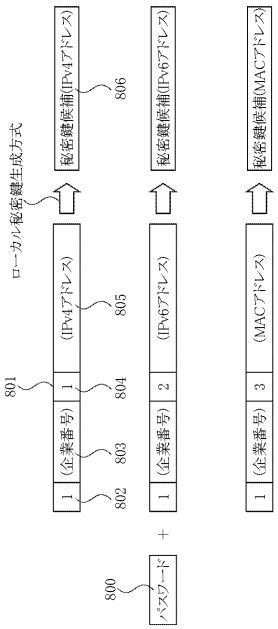
【図６】


600
認証情報の入力
デバイス名
IPアドレス
ユーザ名
接続パスワード
暗号化パスワード
コンテキスト名
Machine1
Machine2
Machine3
172.24.93.167
172.24.93.168
172.24.93.169
test
MD5
キャンセル
更新
インターネット
100%
601
602
603
604
605
606
607
608
609

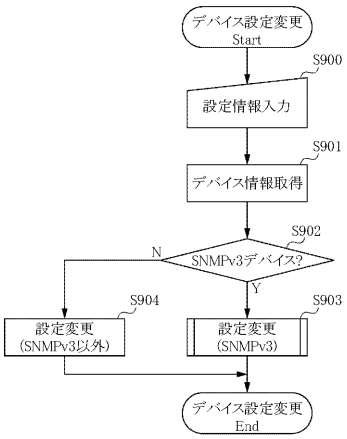
【図７】


認証情報登録
Start
S700
探索済み?
N
Y
S701
デバイス情報取得
管理対象デバイス
S702
SNMPv3デバイス?
N
Y
S703
認証情報保存
S704
認証情報更新?
N
Y
S705
鍵候補生成
S706
鍵候補保存
管理対象デバイス
認証情報登録
End

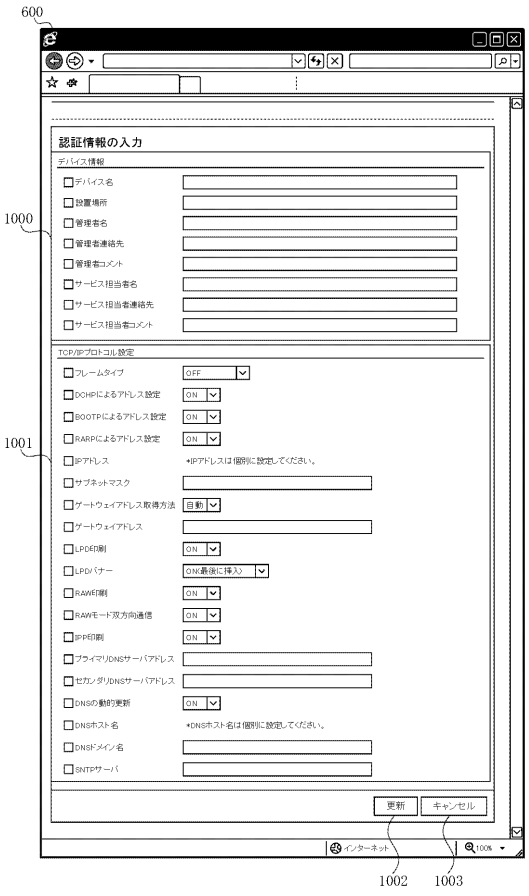
【図８】


ローカル秘密鍵生成方式
秘密鍵候補(IPv4アドレス)
806
秘密鍵候補(IPv6アドレス)
秘密鍵候補(MACアドレス)
801
1
(企業番号)
803
(IPv4アドレス)
805
1
804
2
(IPv6アドレス)
3
(MACアドレス)
1
802
1
(企業番号)
1
(企業番号)
+
800
パスワード

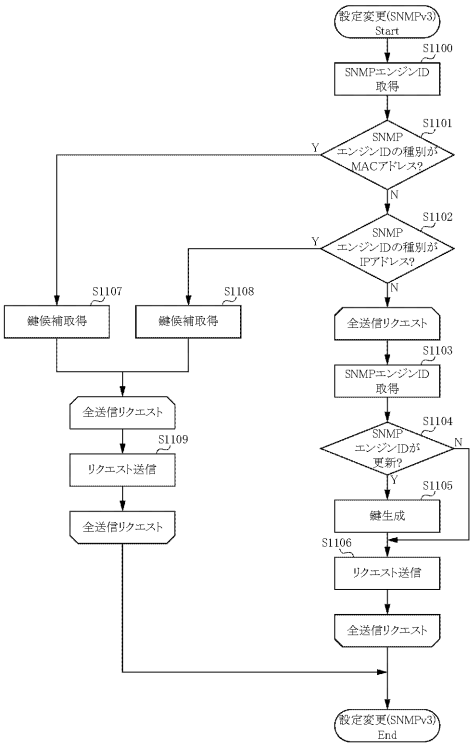
【図９】


デバイス設定変更
Start
S900
設定情報入力
S901
デバイス情報取得
S902
SNMPv3デバイス?
N
Y
S904
設定変更
(SNMPv3以外)
S903
設定変更
(SNMPv3)
デバイス設定変更
End

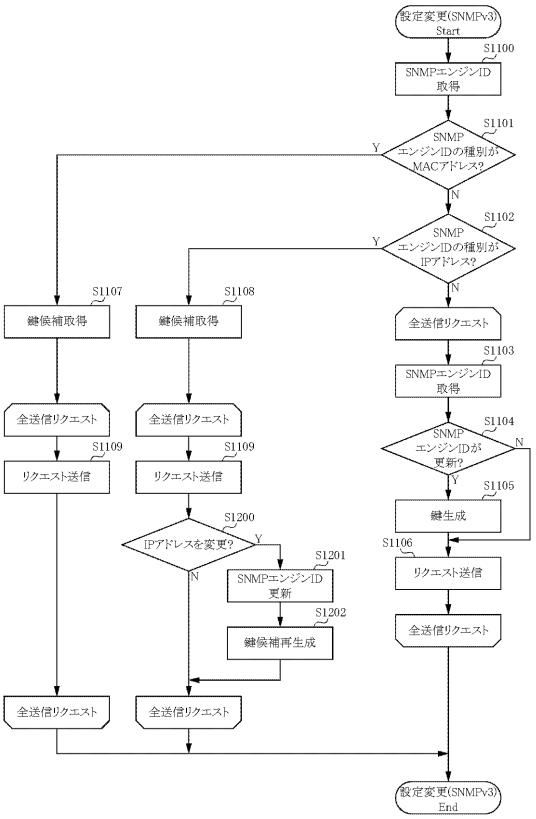
【図１０】


600
認証情報の入力
デバイス情報
デバイス名
設置場所
管理者名
管理者連絡先
管理者コメント
サービス担当者名
サービス担当者連絡先
サービス担当者コメント
1000
TCP/IPプロトコル設定
フレームタイプ
DCHPによるアドレス設定
BOOTPによるアドレス設定
RARPによるアドレス設定
IPアドレス
*IPアドレスは個別に設定してください。
サブネットマスク
ゲートウェイアドレス取得方法
ゲートウェイアドレス
LPD印刷
LPDバナー
RAW印刷
RAWモード双方向通信
IPP印刷
プライマリDNSサーバアドレス
セカンダリDNSサーバアドレス
DNSの動的更新
DNSホスト名
*DNSホスト名は個別に設定してください。
DNSドメイン名
SNTPサーバ
1001
更新
キャンセル
インターネット
100%
1002
1003

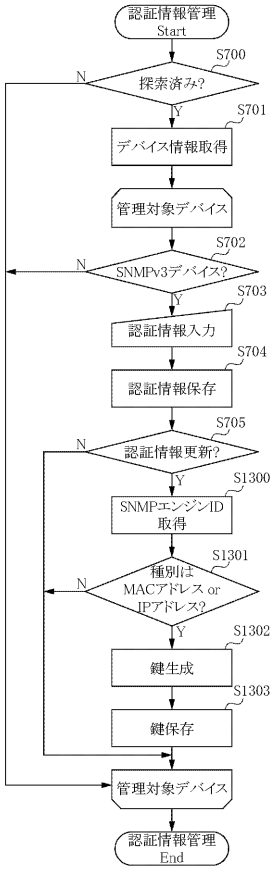
【図１１】



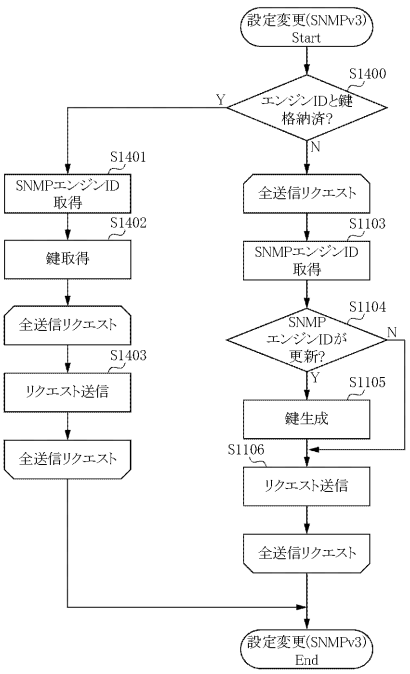
【図１２】



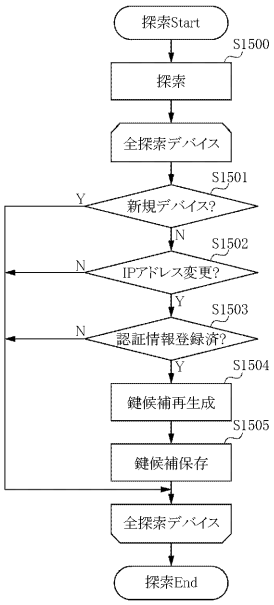
【図１３】



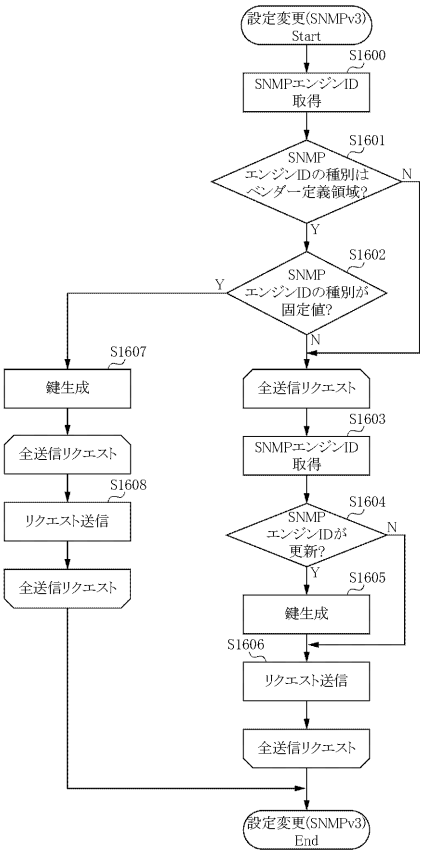
【図１４】



【図１５】



【図１６】



【図１７】

種別	RFC3411定義	本実施例	
0	未使用	未使用	
1	IPv4アドレス	IPv4アドレス	
2	IPv6アドレス	IPv6アドレス	
3	MACアドレス	MACアドレス	
4	文字列	文字列	
5	バイト列	バイト列	
6-127	予約	予約	
128	ベンダー定義可能	変動値	Location
・・・			マシン名
191			HostName
192		固定値	製品名
・・・			NIC製品名
255			製品Version

フロントページの続き

(56)参考文献 特開２００６－２５２０２３（ＪＰ，Ａ）
特表２００３－５１０９６５（ＪＰ，Ａ）
特開２００５－２０４２９３（ＪＰ，Ａ）
特開２００９－０６５２８８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　１３／００
Ｇ０６Ｆ　２１／２０
Ｈ０４Ｌ　　９／００
Ｈ０４Ｌ　１２／２８