

(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2019-121908

(P2019-121908A)

(43) 公開日 令和1年7月22日(2019.7.22)

(51) Int.Cl.	F I	テーマコード (参考)
HO4L 12/28 (2006.01)	HO4L 12/28 200M	5B042
GO6F 3/12 (2006.01)	GO6F 3/12 303	5B089
GO6F 11/07 (2006.01)	GO6F 3/12 323	5J104
HO4L 12/70 (2013.01)	GO6F 11/07 193	5K030
HO4L 9/32 (2006.01)	HO4L 12/70 100Z	5K033

審査請求 未請求 請求項の数 12 O L (全 14 頁) 最終頁に続く

(21) 出願番号 特願2018-306 (P2018-306)
 (22) 出願日 平成30年1月4日 (2018.1.4)

(71) 出願人 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 100114775
 弁理士 高岡 亮一
 (74) 代理人 100121511
 弁理士 小田 直
 (72) 発明者 平井 正仁
 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) 5B042 JJ02 KK02
 5B089 GA11 GA16 GA21 GB02 HB06
 JA35 JB14 JB15 KA13 KB01
 KB04 KH30 MB01

最終頁に続く

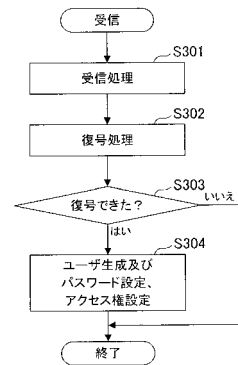
(54) 【発明の名称】 管理装置、管理装置の制御方法、及びプログラム

(57) 【要約】

【課題】書き込み権限が制限された初期状態であっても非管理装置の再起動を行うことができる管理装置を提供する。

【解決手段】管理装置が管理する秘密鍵のペアとなる公開鍵を保持するネットワークデバイスを管理する管理装置である。管理装置は、ネットワークデバイスに対する再起動の指示が必要な場合に、所定のデバイス管理プロトコルで再起動のために必要となる権限を持つユーザーに係るユーザーデータを作成する作成手段と、ユーザーデータに対して、秘密鍵を用いた暗号化処理を実行する暗号化手段と、暗号化処理に応じて作成された暗号データを用いて、ネットワークデバイスにユーザーデータの登録を要求する要求手段と、ネットワークデバイスで暗号データの復号処理により得られたユーザーデータの登録が行われたことに応じて、所定のデバイス管理プロトコルで再起動の指示をネットワークデバイスに対して送信する送信手段と、を有する。

【選択図】 図11



【特許請求の範囲】**【請求項 1】**

管理装置が管理する秘密鍵のペアとなる公開鍵を保持するネットワークデバイスを管理する管理装置であって、

前記ネットワークデバイスに対する再起動の指示が必要な場合に、所定のデバイス管理プロトコルで再起動のために必要となる権限を持つユーザーに係るユーザーデータを作成する作成手段と、

前記ユーザーデータに対して、前記秘密鍵を用いた暗号化処理を実行する暗号化手段と

、
前記暗号化処理に応じて作成された暗号データを用いて、前記ネットワークデバイスに前記ユーザーデータの登録を要求する要求手段と、

前記ネットワークデバイスで前記暗号データの復号処理により得られた前記ユーザーデータの登録が行われたことに応じて、前記所定のデバイス管理プロトコルで再起動の指示を前記ネットワークデバイスに対して送信する送信手段と、

を有する

ことを特徴とする管理装置。

【請求項 2】

前記作成手段は、前記ネットワークデバイスが前記所定のデバイス管理プロトコルが無効、かつ、初期ユーザーのみ登録されている際に、前記ユーザーデータを作成する

ことを特徴とする請求項 1 に記載の管理装置。

【請求項 3】

前記再起動のために作成された前記ユーザーデータを、再起動後に自動削除するか否かを問合せる第 1 問合せ手段

をさらに有する

ことを特徴とする請求項 1 または 2 に記載の管理装置。

【請求項 4】

前記第 1 問合せ手段の問合せにより、前記ユーザーデータを自動削除することが指示されている場合には、再起動後に、前記再起動のために作成された前記ユーザーデータの削除処理を実行する削除手段

をさらに有する

ことを特徴とする請求項 3 に記載の管理装置。

【請求項 5】

前記削除手段は、前記第 1 問合せ手段の問合せにより、前記ユーザーデータを自動削除しないことが指示されている場合には、初期ユーザーデータを削除する

ことを特徴とする請求項 4 に記載の管理装置。

【請求項 6】

再起動後に前記所定のデバイス管理プロトコルを無効化するか否かを問合せる第 2 問合せ手段

をさらに有する

ことを特徴とする請求項 1 ~ 5 のいずれか 1 項に記載の管理装置。

【請求項 7】

前記第 2 問合せ手段の問合せにより、前記所定のデバイス管理プロトコルを無効化することが指示された場合には、再起動後に、前記所定のデバイス管理プロトコルを無効化する無効化手段

をさらに有する

ことを特徴とする請求項 6 に記載の管理装置。

【請求項 8】

前記作成手段は、前記ネットワークデバイスから取得したユーザーデータに前記管理装置に保持された既定のユーザーデータが存在する場合、前記ユーザーデータを作成しないことを特徴とする請求項 1 ~ 7 のいずれか 1 項に記載の管理装置。

10

20

30

40

50

【請求項 9】

前記ユーザーデータは、再起動に必要なアクセス権のみが設定されることを特徴とする請求項 1 ~ 8 のいずれか 1 項に記載の管理装置。

【請求項 10】

前記所定のデバイス管理プロトコルは、SNMPv3 であることを特徴とする請求項 1 ~ 9 のいずれか 1 項に記載の管理装置。

【請求項 11】

管理装置が管理する秘密鍵のペアとなる公開鍵を保持するネットワークデバイスを管理する管理装置の制御方法であって、

前記ネットワークデバイスに対する再起動の指示が必要な場合に、所定のデバイス管理プロトコルで再起動のために必要となる権限を持つユーザーに係るユーザーデータを作成する作成工程と、

前記ユーザーデータに対して、前記秘密鍵を用いた暗号化処理を実行する暗号化工程と、

前記暗号化処理に応じて作成された暗号データを用いて、前記ネットワークデバイスに前記ユーザーデータの登録を要求する要求工程と、

前記ネットワークデバイスで前記暗号データの復号処理により得られた前記ユーザーデータの登録が行われたことに応じて、前記所定のデバイス管理プロトコルで再起動の指示を前記ネットワークデバイスに対して送信する送信工程と、

を有する

ことを特徴とする装置の制御方法。

【請求項 12】

請求項 1 乃至 10 のいずれか 1 項に記載の装置の各手段としてコンピューターを機能させるためのプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、管理装置、管理装置の制御方法、及びプログラムに関し、特にネットワーク機器を管理するためのプロトコル SNMPv3 に関する。

【背景技術】

【0002】

管理装置からネットワークを介して印刷装置などの被管理装置を管理するためのプロトコルである SNMPv3 の仕様において、管理装置は被管理装置に対して、初期ユーザーから別のユーザーを作成することが可能である。また、特許文献 1 には、SNMPv3 で機器管理を行うユーザー情報の被管理装置への登録について開示がある。SNMPv3 の初期ユーザーの推定が容易な場合には、第三者によって、初期ユーザーから別のユーザーとパスワードが生成され、初期ユーザーを削除されると、正規の管理者が被管理装置にアクセスできなくなるという危惧がある。そのため、被管理装置における初期状態として、SNMPv3 を無効もしくは書き込みができないようにしている場合がある。

【先行技術文献】

【特許文献】

【0003】

【特許文献 1】特開 2015 - 76071 号公報

【発明の概要】

【発明が解決しようとする課題】

【0004】

ここで、管理装置が SNMPv3 で被管理装置に対して再起動を行うなどといった遠隔操作を行うためには、書き込み権限が必要な場合がある。しかしながら、被管理装置の初期状態で SNMPv3 が無効または SNMPv3 での書き込みができない（書き込み権限を制限している）場合、管理装置から SNMPv3 で被管理装置に対して再起動を実現で

10

20

30

40

50

きない。つまり、初期状態においては、管理装置から被管理装置に対してSNMPv3を用いた操作については、利便性が悪くなる。

【0005】

本発明は、上記課題を鑑みて、書き込み権限が制限された初期状態であっても非管理装置の再起動を行うことができる管理装置を提供することを目的とする。

【課題を解決するための手段】

【0006】

上記の課題を解決するために、本発明の管理装置は、管理装置が管理する秘密鍵のペアとなる公開鍵を保持するネットワークデバイスを管理する管理装置であって、前記ネットワークデバイスに対する再起動の指示が必要な場合に、所定のデバイス管理プロトコルで再起動のために必要となる権限を持つユーザーに係るユーザーデータを作成する作成手段と、前記ユーザーデータに対して、前記秘密鍵を用いた暗号化処理を実行する暗号化手段と、前記暗号化処理に応じて作成された暗号データを用いて、前記ネットワークデバイスに前記ユーザーデータの登録を要求する要求手段と、前記ネットワークデバイスで前記暗号データの復号処理により得られた前記ユーザーデータの登録が行われたことに応じて、前記所定のデバイス管理プロトコルで再起動の指示を前記ネットワークデバイスに対して送信する送信手段と、を有することを特徴とする。

【発明の効果】

【0007】

本発明によれば、書き込み権限が制限された初期状態であっても非管理装置の再起動を行うことができる管理装置を提供することができる。

【図面の簡単な説明】

【0008】

【図1】ハードウェア構成を示す図である。

【図2】ソフトウェア構成を示す図である。

【図3】設定に関するユーザーインターフェースを示す図である。

【図4】SNMPv3メッセージの構成を示す図である。

【図5】再起動を行う際の前処理に関するフローチャートである。

【図6】第1実施形態に係る再起動を行う際のフローチャートである。

【図7】第2実施形態に係る再起動を行う際のフローチャートである。

【図8】第2実施形態に係る再起動を行う際のフローチャートである。

【図9】第3実施形態に係る再起動を行う際のフローチャートである。

【図10】第3実施形態に係る再起動を行う際のフローチャートである。

【図11】被管理装置における再起動ユーザー生成のフローチャートである。

【発明を実施するための形態】

【0009】

以下、本発明を実施するための最良の形態について図面などを参照して説明する。

【0010】

(第1実施形態)

図1は、ハードウェア構成を示す図である。管理装置101は、ネットワークに接続可能な印刷装置などの被管理装置(ネットワークデバイス)102とネットワーク103を介して通信を行う。そして、被管理装置102から情報を取得し、被管理装置102に対して情報を書き込み、再起動する等の操作を行う。管理装置101は、内部にCPU111、メモリ112、HDD113、入力装置114、出力装置115、ネットワークインターフェース116を有し、それぞれがバス117で接続されている。CPU111は、HDD113に保存されたプログラム及びデータをメモリ112にロードし、メモリ112にロードされたプログラムの実行を行う。入力装置114は、ユーザーに入力された情報を取得する。また、出力装置115は、プログラムの操作に必要な情報の表示を行う。ネットワークインターフェース116は、ネットワーク103を介して被管理装置102との信号の送受信を行う。被管理装置102は、内部にCPU121、メモリ122、H

10

20

30

40

50

DD123、ネットワークインターフェース124を有し、それぞれがバス125で接続されている。CPU121は、HDD123に保存されたプログラム及びデータをメモリ122にロードし、メモリ122にロードされたプログラムの実行を行う。ネットワークインターフェース124は、ネットワーク103を介して管理装置102との信号の送受信を行う。

【0011】

図2は、本実施形態に係るソフトウェアの構成図である。ユーザー制御部201、暗号処理部202、再起動処理部203、送受信部204、UI制御部205は、管理装置101のCPU111で実行されるプログラムを構成する各機能モジュールである。格納部206は、メモリ112もしくはHDD113に格納されるデータ格納領域である。ユーザー制御部201は、被管理装置102に対するSNMPv3のユーザーの生成及び削除命令の生成を行う。SNMPv3は、ネットワークに接続可能な印刷装置等の被管理装置102を管理するための所定のデバイス管理プロトコルである。暗号処理部202は、SNMPv3のユーザー名及びパスワードの暗号化を行う。

10

【0012】

再起動処理部203は、被管理装置102に対する再起動命令の生成を行う。再起動命令については、後述の図4において詳細を説明する。送受信部204は、ユーザー制御部201で生成されたユーザー生成及び削除命令、再起動処理部203で生成された再起動命令の送信を行う。また、被管理装置102からの応答メッセージの処理を行う。UI制御部205は、出力装置115で表示された画面表示に基づくユーザー操作による入力装置114からの入力情報を制御する。

20

【0013】

ユーザー制御部211、復号処理部212、再起動処理部213、送受信部214は、被管理装置102のCPU121で実行されるプログラムを構成する各機能モジュールである。格納部216は、メモリ122もしくはHDD123に格納されるデータ格納領域である。ユーザー制御部211は、格納部216に保存された表AのSNMPv3のユーザー管理テーブルに対して、ユーザー追加、削除を行う。例えば、ユーザー管理テーブルには、初期状態でInitialという名称の初期ユーザーが定義されており、この初期ユーザーとその初期ユーザーの認証情報(パスワード)を用いて別のユーザーを複製することが可能である。また、ユーザー管理テーブルの各ユーザーに対しては、MIBと呼ばれる機器管理情報の集合の部分集合へのアクセス権を設定することが可能である。つまり、管理装置101からSNMPv3を用いて機器の再起動を行うには、書込権限が必要だが、被管理装置102の初期状態ではSNMPv3が無効であり、書込権限がない。そのため、再起動を行うことができない。そのため、本実施形態では、例えば、初期ユーザーは、再起動ユーザーを生成に関連する処理のみを行うMIBの値にのみへのアクセス権が設定されているものとする。また、後述の再起動専用ユーザーは、再起動を行うためのMIBにのみアクセス権が設定されるものとする。なお、本実施形態では、初期状態においてはSNMPv3が無効であるとする。そして、再起動処理後にSNMPv3を無効にするか否かを予め設定し、再起動処理後に無効化する処理を行ってもよい。

30

【表1】

40

表A

番号	ユーザ名	auth	priv
1	initial	aaaaaaaa	bbbbbbbb
2	administrator	cccccccc	dddddddd
3	admin	eeeeeeee	fffffff

【0014】

50

復号処理部 2 1 2 は、管理装置 1 0 1 から受信した暗号化された情報を復号する処理を行う。再起動処理部 2 1 3 は、管理装置 1 0 1 から受信した再起動命令により、被管理装置 1 0 2 の再起動処理を行う。送受信部 2 1 4 は、管理装置 1 0 1 から受信した情報の通信処理を行い、管理装置 1 0 1 に対して返信処理を行う。

【 0 0 1 5 】

図 3 は、設定に関するユーザーインターフェースを示す図である。図 3 (A) は、管理装置 1 0 1 が被管理装置 1 0 2 に対して再起動を行う処理の前の設定をユーザーに行わせるための設定画面 3 0 1 a である。チェックボックス 3 1 1 a は、再起動実行時再起動専用ユーザーを生成するか否かを判断するための値を取得するためのユーザーインターフェースである。チェックボックス 3 2 1 a は、再起動後に再起動専用ユーザーを自動削除するか否かを判断するための値を取得するためのユーザーインターフェースである。チェックボックス 3 2 1 a は、チェックボックス 3 1 1 a が非選択状態の場合には、選択不可能な状態となる。チェックボックス 3 2 1 a は、チェックボックス 3 1 1 a が選択状態の場合に選択可能な状態となる。

10

【 0 0 1 6 】

図 4 は、管理装置 1 0 1 が被管理装置 1 0 2 に対して送信する SNMP v 3 メッセージのデータ構造を示す図である。SNMP バージョン 4 0 1 は、SNMP のバージョン情報であり、本実施形態では、SNMP v 3 を採用するので、バージョン 3 を示す数値の 3 が入る。ヘッダ情報 4 0 2 には、SNMP v 3 メッセージを一意に識別する ID、受信可能な最大サイズ、メッセージフラグ、セキュリティモデル情報が含まれる。メッセージフラグは、メッセージにおける認証と暗号化の有無に応じて、それぞれ有の場合には 1、無の場合には 0 が入る。

20

【 0 0 1 7 】

再起動ユーザーの生成メッセージの場合、オブジェクト名 4 0 9 は、例えば、Add Username であり、オブジェクト値 4 1 0 は、生成する再起動ユーザー名と対応するパスワードを含む暗号化されたデータである。PDU タイプ 4 0 6 は、値を設定することを示す値 Set Request (0 x A 3) となる。また、再起動ユーザーの削除メッセージの場合、オブジェクト名 4 0 9 は、例えば、Delete Username、オブジェクト値 4 1 0 は、削除する名前の文字列が記載される。PDU タイプ 4 0 6 は、値を設定することを示す値 Set Request (0 x A 3) となる。

30

【 0 0 1 8 】

SNMP v 3 の表 A ユーザー管理テーブルにあるユーザーリスト取得メッセージの場合、オブジェクト名 4 0 9 は、Get User List である。PDU タイプ 4 0 6 は、複数の値を順次取得することを示す値 Get Next Request (0 x A 1) または Get Bulk Request (0 x A 5) となる。また、その要求に対する被管理装置 1 0 2 からの応答のメッセージにおいては、PDU タイプ 4 0 6 は、値を返すことを示す値 Get Response (0 x A 2) となる。なお、要求のメッセージにおける PDU タイプ 4 0 6 は、値を取得することを示す値 Get Next Request (0 x A 1) の場合には、表 A ユーザー管理テーブルから複数の値の取得が終わるまで、要求と応答の処理が繰り返し行われる。

40

【 0 0 1 9 】

再起動実行のメッセージの場合、オブジェクト名 4 0 9 は、prt General Reset、オブジェクト値 4 1 0 は、power Cycle Reset (4) といった値がセットされる。PDU タイプ 4 0 6 は、値を設定することを示す値 Set Request (0 x A 3) となる。また、セキュリティパラメータ 4 0 3 には、再起動専用ユーザー及びパスワードを使って生成されたセキュリティパラメータを含み、そのセキュリティパラメータについては、SNMP v 3 のセキュリティモデルに従う。セキュリティモデルについては、例えば RFC 3 4 1 4 に定義されたユーザーベースセキュリティモデルがあり、本発明ではユーザーベースセキュリティモデルを採用しているものとする。なお、初期状態において、被管理装置が初期ユーザーを有するので、例えば、Initial という名

50

前の初期ユーザーとそれに対応する既定パスワードにより生成されたセキュリティパラメータとなる。再起動を行う処理の場合には、再起動専用ユーザー及びパスワードや管理専用のユーザー及びパスワードが生成されたセキュリティパラメータ403となる。また、データ構造には、エンジン種別を示すエンジンID404、コンテキスト名405、リクエストID407、エラーを示すエラー情報408が含まれる。

【0020】

図5は、管理装置101が被管理装置102に対して再起動を行う処理の前の設定処理のフローチャートを示す図である。ステップS101において、UI制御部205が301aの再起動動作に関する設定画面を出力装置115に表示する。ステップS102において、入力装置114がユーザー操作によりOKボタン303aが押下されたことを検知し、OKボタン303aが押下されていれば、ステップS103に移行し、OKボタン303aが押下されていない場合はステップS101の画面表示に戻る。ステップS103において、UI制御部205は、チェックボックス311a及びチェックボックス321aの選択状態を取得し、その選択状態に応じた値を格納部206に保存する。例えば、チェックボックス311aが選択状態の場合には、再起動実行時再起動専用ユーザーを生成することを意味する値1であり、チェックボックス311aが非選択状態の場合には、再起動実行時に再起動専用ユーザーを生成しないことを意味する値0である。また、チェックボックス321aが選択状態の場合には、再起動実行後に再起動専用ユーザーを削除することを意味する値1であり、チェックボックス321aが非選択状態の場合には、再起動実行後に再起動専用ユーザーを削除しないことを意味する値0である。

10

20

【0021】

図6は、管理装置101が被管理装置102に対して再起動の指示が必要な場合のフローチャートである。管理装置101が被管理装置102に対する再起動の処理が開始されると、まず、ステップS201において、ユーザー制御部201は、格納部206に保存された再起動実行時再起動専用ユーザーを生成するか否かを示す値を取り出す。そして、再起動専用ユーザーを生成するか否かを判定する。ステップS201で、再起動専用ユーザーを生成すると判定された場合、ステップS202に移行し、再起動専用ユーザーを生成しないと判定された場合、ステップS205に移行する。

【0022】

次に、ステップS202において、ユーザー制御部201は、再起動専用のユーザー名とパスワード(ユーザーデータ)を生成し、格納部206に保存する。その際、ユーザー名とパスワードの生成は、一定の生成ルールに基づいて生成される。なお、本実施形態では、再起動専用のユーザー名とパスワードはユーザーが参照する手段はなく、他の管理装置101と被管理装置102からも参照できないものとする。

30

【0023】

次に、ステップS203において、暗号処理部202は、格納部206に保存された再起動専用のユーザー名とパスワードと予め格納部206に保存された管理装置101の秘密鍵を取り出す。さらに、ステップS203において、暗号処理部202は、秘密鍵によりユーザー名とパスワードの暗号化処理を行う。

【0024】

次に、ステップS204において、送受信部204は、前記暗号化されたデータ(暗号データ)を含む再起動ユーザー生成命令を生成し、被管理装置102に送信する処理を行う。被管理装置102の送受信部214は、再起動ユーザー生成命令を受信し、再起動ユーザー生成を行う。次に、ステップS205において、再起動処理部203は、格納部206に保存された再起動専用ユーザーとパスワードの取得を試みる。ステップS206において、再起動処理部203は、再起動専用ユーザーとパスワードの取得ができたか否かを判定し、取得できた場合、ステップS208に移行し、取得できない場合、ステップS207に移行する。

40

【0025】

次に、ステップS207において、再起動処理部203は、管理装置101に保持され

50

た既定のユーザーとパスワードを取得する。なお、管理装置 101 に保持された既定のユーザーとパスワードを用いる場合には、予め被管理装置 102 に同じユーザーとパスワードが存在しないと被管理装置 102 に対して再起動を行うことができない。次に、ステップ S 208 において、再起動処理部 203 は、ステップ S 05 またはステップ S 207 で取得したユーザーとパスワードを含む再起動命令を生成する。そして、送受信部 204 は、被管理装置 102 に対して再起動命令を送信する。被管理装置 102 の送受信部 214 は、再起動命令を受信し、被管理装置 102 の再起動処理部 213 が再起動処理を行う。なお、再起動処理後に SNMP v 3 を無効にするか否かを判断するための設定を予め行い、その設定に従って再起動処理後に SNMP v 3 を無効にするか否かを判定して、無効にする場合には、SNMP v 3 を無効化する処理を行ってもよい。

10

【0026】

次に、ステップ S 209 において、ユーザー制御部 201 は、格納部 206 に保存された再起動専用ユーザーを削除するか否かの値を問い合わせ取り出し、再起動専用ユーザーを削除するか否かを判定する。ステップ S 209 で、再起動専用ユーザーを削除処理を行い削除すると判定された場合、ステップ S 210 に移行し、再起動専用ユーザーを削除しないと判定された場合、処理を終了する。

【0027】

次に、ステップ S 210 において、ユーザー制御部 201 は、格納部 206 に保存された再起動専用ユーザー及びパスワードを取り出し、ユーザー削除命令を生成する。さらに、送受信部 204 は、被管理装置 102 に対して前記ユーザー削除命令を送信する。被管理装置 102 の送受信部 214 は、ユーザー削除命令を受信し、ユーザー制御部 211 が格納部 216 に保存された表 A のユーザー管理テーブルとユーザー及びパスワードが一致するユーザーを削除する。また、ユーザー制御部 201 は、格納部 206 に保存された再起動専用ユーザー及びパスワードを削除する。

20

【0028】

図 11 は、被管理装置 102 において、管理装置 101 から受信した再起動ユーザー生成命令に基づく再起動ユーザー生成のフローチャートである。まず、ステップ S 301 において、送受信部 214 が管理装置 101 から再起動ユーザー生成命令を含むパケットを受信し、再起動ユーザー命令を取り出し、復号処理部 212 に再起動ユーザー生成命令を渡す。次に、ステップ S 302 において、復号処理部 212 は、再起動ユーザー命令に含まれる暗号化されたデータを公開鍵を用いて復号する。ここで、公開鍵とは、管理装置 101 が管理する秘密鍵のペアとなる公開鍵であって、被管理装置（ネットワークデバイス）102 が保持している。次に、ステップ S 303 において、復号処理部 212 は、復号できたか否かを判定し、復号できたと判定した場合、ステップ S 304 に移行し、復号できないと判定した場合、処理は終了となる。次に、ステップ S 304 において、ユーザー制御部 211 が、復号されたユーザー情報を取り出し、格納部 216 に保存された表 A のユーザー管理テーブルにユーザー情報を追加する。

30

【0029】

以上、本実施形態によれば、書き込み権限が制限された初期状態の被管理装置 102 に対する遠隔操作で管理装置から再起動を行うことが可能となる。

40

【0030】**(第2実施形態)**

以下、第2実施形態について図面を用いて説明する。本実施形態では、既にユーザーが存在する場合を考慮している点が第1実施形態と異なる。第1実施形態と異なる管理装置 101 が被管理装置 102 に対して再起動を行う際の処理について、図7及び8を用いて説明する。

【0031】

図7及び8は、管理装置 101 が被管理装置 102 に対して再起動を行う際のフローチャートを示す図である。まず、ステップ S 211 において、管理装置 101 のユーザー制御部 201 は、SNMP v 3 のユーザーリストの取得要求を生成する。なお、ユーザーリ

50

ストは、表 A ユーザー管理テーブルに存在するユーザー名の一覧である。さらに、送受信部 204 は、ユーザーリスト情報の取得要求を被管理装置 102 に送信し、被管理装置 102 は、格納部 216 に保存された表 A ユーザー管理テーブルに有するユーザーリストを返信する。次に、ステップ S 212 において、ユーザー制御部 201 は、ユーザーリストを取得できたか否かを判定し、取得できなかったと判定した場合、ステップ S 207 に移行する。一方、ステップ S 212 において、ユーザーリストを取得できたと判定した場合、ステップ S 213 に移行する。

【0032】

次に、ステップ S 213 において、ユーザー制御部 201 は、ユーザーリストに再起動専用ユーザーが存在するか否かを確認する。そして、ステップ S 213 で、再起動専用ユーザーが存在しないと判定された場合、ステップ S 215 に移行する。一方、ステップ S 213 で、再起動専用ユーザーが存在すると判定された場合、ステップ S 214 に移行する。次に、ステップ S 214 において、ユーザー制御部 201 は、再起動専用ユーザーの情報を管理装置 101 の格納部 206 から取り出す。格納部 206 に再起動専用ユーザーが存在しない場合には、再起動専用ユーザー情報を生成する。そして、ステップ S 214 の処理の後、ステップ S 208 に移行し、再起動専用ユーザー情報を用いて、被管理装置 102 に対する再起動処理が行われる。

【0033】

次に、ステップ S 215 において、ユーザー制御部 201 は、ユーザーリストに初期ユーザーのみが存在するか否かを確認する。そして、ステップ S 215 で、初期ユーザーのみが存在すると判定された場合、ステップ S 201 に移行する。つまり、被管理装置 102 における初期状態として、SNMPv3 が無効であり、初期ユーザーのみが登録されている場合、ステップ S 201 に移行する。一方、ステップ S 215 で、初期ユーザー以外にも存在すると判定された場合、ステップ S 216 に移行する。次に、ステップ S 216 において、ユーザー制御部 201 は、初期ユーザー以外のユーザー情報である管理者ユーザー情報を管理装置 101 の格納部 206 から取り出す。ステップ S 216 の処理の後、ステップ S 208 に移行し、管理者ユーザー情報を用いて、被管理装置 102 に対する再起動処理が行われる。なお、ステップ S 201 からステップ S 210 の処理は、第 1 実施形態と同様であるため詳細な説明を省略する。

【0034】

以上、本実施形態によれば、既に初期ユーザー以外のユーザーが存在する場合でも、被管理装置 102 に対する遠隔操作で管理装置から再起動を行うことが可能となる。

【0035】

(第 3 実施形態)

以下、第 3 実施形態について図面を用いて説明する。特に、第 1 実施形態、第 2 実施形態と異なる図 3、図 9 及び 10 についての説明を行う。図 3 (B) は、管理装置 101 が被管理装置 102 に対して再起動を行う処理の前の設定をユーザーに行わせるための設定画面 301b である。チェックボックス 311b は、再起動実行時再起動専用ユーザーを生成するか否かを判定するための値を取得するために利用するユーザインターフェースである。チェックボックス 321b は、再起動実行後にユーザーを削除するか否かを判定するための値を取得するために利用するユーザインターフェースである。

【0036】

チェックボックス 321b は、チェックボックス 311b が非選択状態の場合には、選択不可能な状態となる。チェックボックス 321b は、チェックボックス 311b が選択された状態の場合に選択可能な状態となる。ラジオボタン 331b は、再起動専用ユーザーを削除するか否かを判定するための値を取得するために利用するユーザインターフェースである。ラジオボタン 332b は、初期ユーザーを削除するか否かを判定するための値を取得するために利用するユーザインターフェースである。ラジオボタン 331b とラジオボタン 332b は、チェックボックス 321b が選択された状態の場合にのみ、選択可能な状態となる。また、チェックボックス 321b が選択された状態の場合には、ラジオ

10

20

30

40

50

ボタン 3 3 1 b かラジオボタン 3 3 2 b のどちらか一方だけが選択された状態となる。

【 0 0 3 7 】

本実施形態では、図 5 のステップ S 1 0 3 において、UI 制御部 2 0 5 は、チェックボックス 3 1 1 b、ラジオボタン 3 2 1 b、ラジオボタン 3 3 2 b の選択状態を取得し、その選択状態に応じた値を格納部 2 0 6 に保存する。例えば、チェックボックス 3 1 1 b が選択状態の場合には、再起動実行時再起動専用ユーザーを生成することを意味する値 1 であり、チェックボックス 3 1 1 b が非選択状態の場合には、再起動実行時に再起動専用ユーザーを生成しないことを意味する値 0 である。また、ラジオボタン 3 2 1 b が選択状態の場合には、再起動実行後に再起動専用ユーザーを削除することを意味する値 1 であり、ラジオボタン 3 2 1 b が非選択状態の場合には、再起動実行後に再起動専用ユーザーを削除しないことを意味する値 0 である。また、ラジオボタン 3 2 2 b が選択状態の場合には、再起動実行後に初期ユーザーを削除することを意味する値 1 であり、ラジオボタン 3 2 2 b が非選択状態の場合には、再起動実行後に初期ユーザーを削除しないことを意味する値 0 である。

10

【 0 0 3 8 】

図 9 及び 1 0 は、管理装置 1 0 1 が被管理装置 1 0 2 に対して再起動を行う際のフローチャートである。図 9 及び 1 0 は、第 2 実施形態の図 7 及び 8 に示すフローチャートにおけるステップ S 2 0 1 からステップ S 2 0 8 までと、ステップ S 2 1 1 からステップ S 2 1 6 までとは同様であるため、その詳細な説明を省略する。そして、ステップ S 2 2 1 において、ユーザー制御部 2 0 1 は、格納部 2 1 6 から、再起動専用ユーザーを削除するか否かの情報を取得し、再起動専用ユーザーを削除するか否かを判定する。ステップ S 2 2 1 で、再起動専用ユーザーを削除すると判定した場合、ステップ S 2 1 2 に移行する。次に、ステップ S 2 1 2 において、ユーザー制御部 2 0 1 は、格納部 2 0 6 に保存された再起動専用ユーザー及びパスワードを取り出し、ユーザー削除命令を生成する。さらに、送受信部 2 0 4 は、被管理装置 1 0 2 に対して前記ユーザー削除命令を送信する。

20

【 0 0 3 9 】

一方、ステップ S 2 2 1 で、再起動専用ユーザーを削除しないと判定した場合、ステップ S 2 2 3 に移行する。次に、ステップ S 2 2 3 において、ユーザー制御部 2 0 1 は、格納部 2 1 6 から、初期ユーザーを削除するか否かの情報を取得し、初期ユーザーを削除するか否かを判定する。そして、ステップ S 2 2 3 で、初期ユーザーを削除すると判定した場合、ステップ S 2 2 4 に移行する。一方、ステップ S 2 2 3 で、初期ユーザーを削除しないと判定した場合、処理が終了に移行する。次に、ステップ S 2 2 4 において、ユーザー制御部 2 0 1 は、初期ユーザー名を含むユーザー削除命令を生成し、送受信部 2 0 4 は、ユーザー削除命令を被管理装置 1 0 2 に送信する。被管理装置 1 0 2 の送受信部 2 1 4 は、初期ユーザー情報削除命令を受信し、ユーザー制御部 2 1 1 は、表 A のユーザー管理テーブルから初期ユーザー情報（初期ユーザーデータ）を削除する。

30

【 0 0 4 0 】

以上、本実施形態によれば、不要なユーザーを削除しつつ、被管理装置 1 0 2 に対する遠隔操作で管理装置から再起動を行うことが可能となる。

【 0 0 4 1 】

40

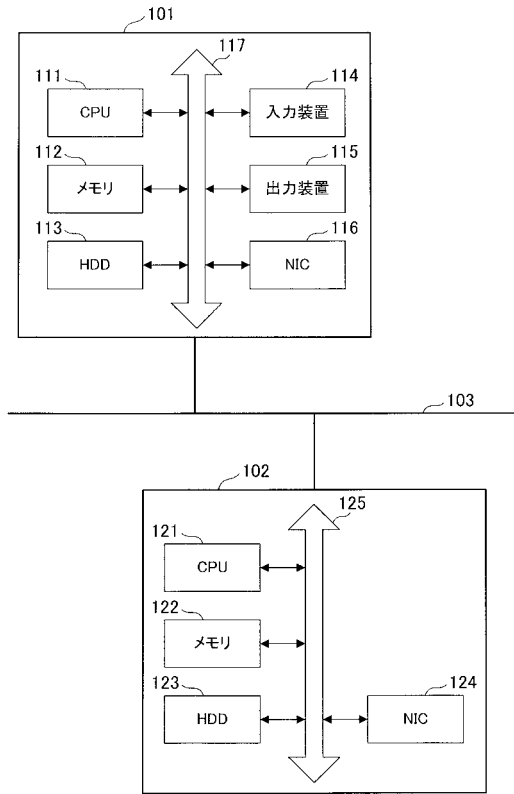
（その他の実施例）

本発明は、上述の実施形態の 1 以上の機能を実現するプログラムを、ネットワーク又は記憶媒体を介してシステム又は装置に供給し、そのシステム又は装置のコンピューターにおける 1 つ以上のプロセッサがプログラムを読み出し実行する処理でも実現可能である。また、1 以上の機能を実現する回路（例えば、ASIC）によっても実現可能である。

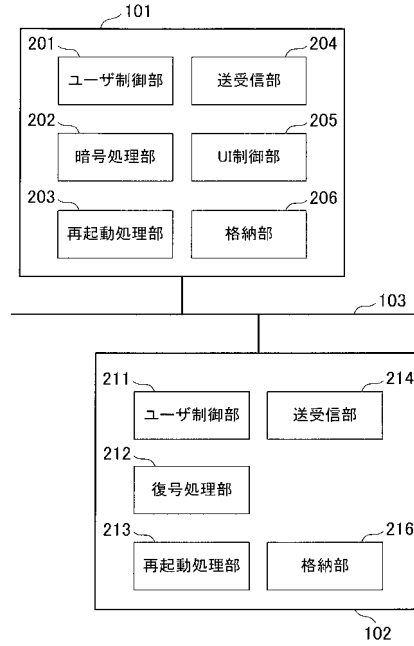
【 0 0 4 2 】

また、本発明の好ましい実施形態について説明したが、本発明は、これらの実施形態に限定されず、その要旨の範囲内で種々の変形および変更が可能である。

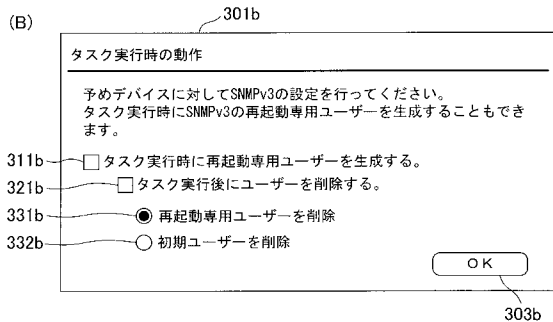
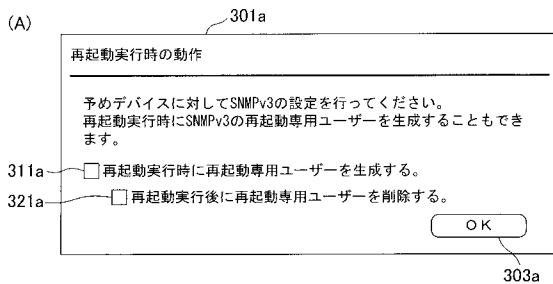
【 図 1 】



【 図 2 】



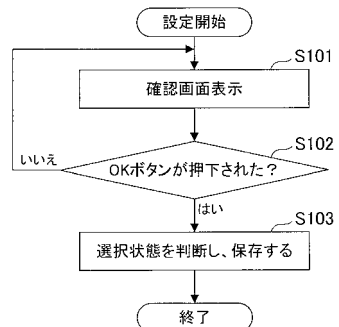
【 図 3 】



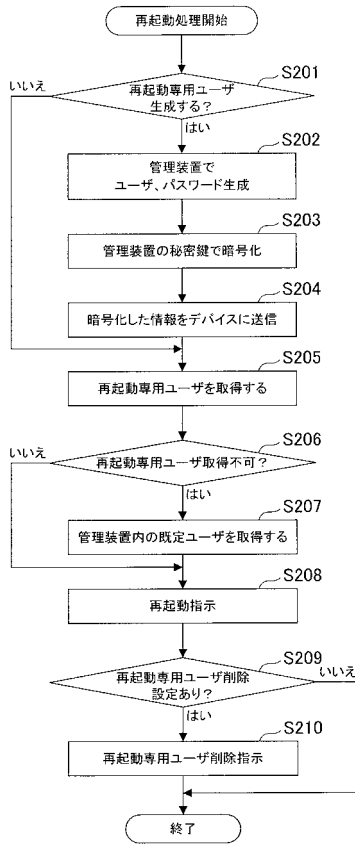
【 図 4 】

SNMPバージョン(3)	401
ヘッダ	402
セキュリティパラメータ	403
エンジンID	404
コンテキスト名	405
PDUタイプ	406
リクエストID	407
エラー情報	408
オブジェクト名	409
オブジェクト値	410

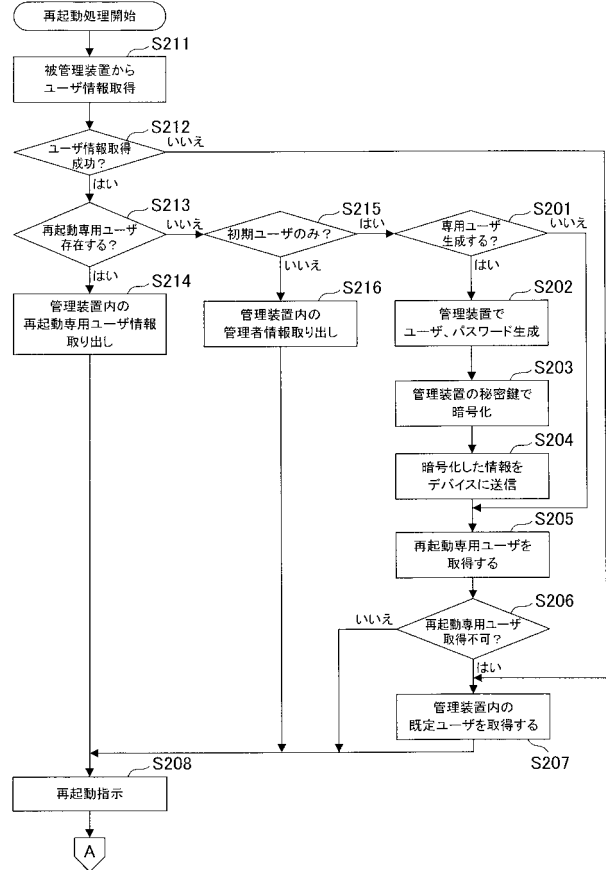
【 図 5 】



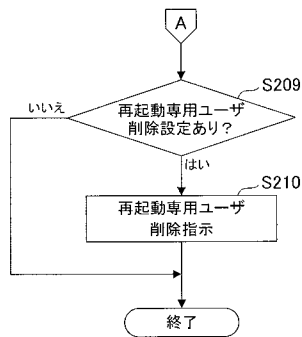
【 図 6 】



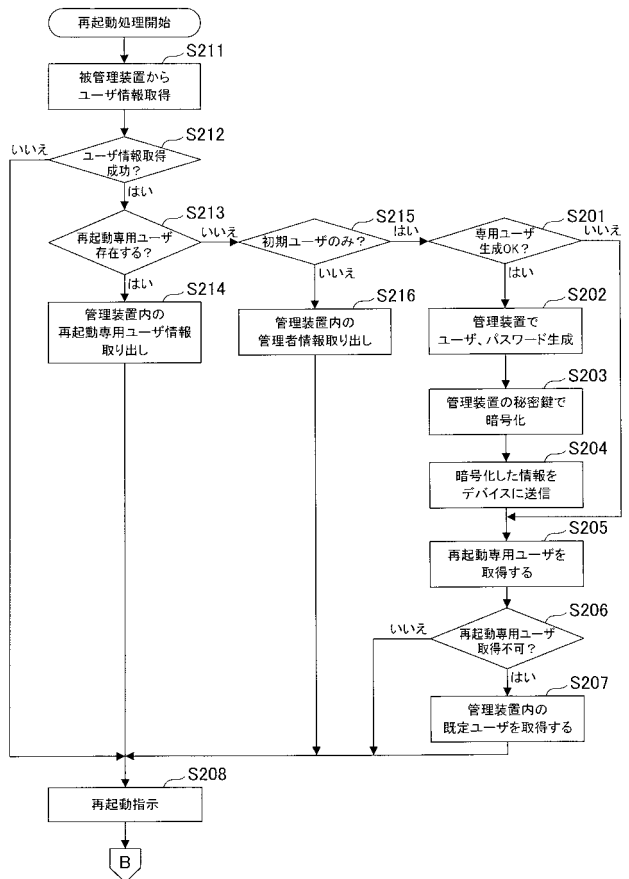
【 図 7 】



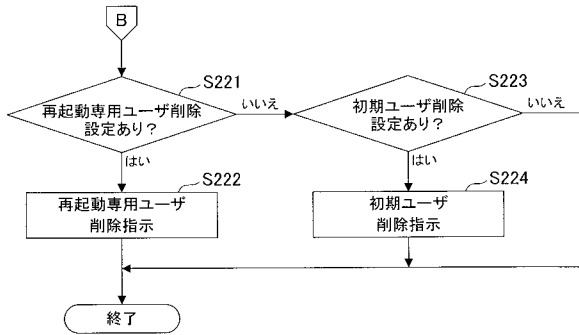
【 図 8 】



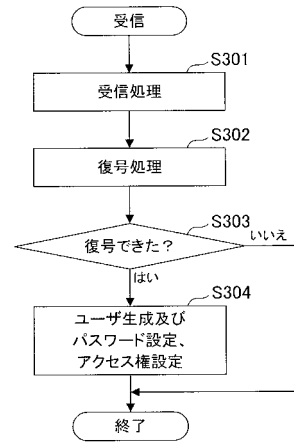
【 図 9 】



【図10】



【図11】



フロントページの続き

(51)Int.Cl.	F I			テーマコード(参考)		
G 0 9 C 1/00 (2006.01)	H 0 4 L	9/00	6 7 5 B			
G 0 6 F 13/00 (2006.01)	G 0 9 C	1/00	6 4 0 E			
	G 0 6 F	13/00	3 5 3 B			

Fターム(参考) 5J104 AA07 AA16 EA17 JA21 KA01 KA05 MA02 NA02 NA05 NA37
NA38
5K030 GA16 HC01 HC13 HD06 JA10 MC09 MD04
5K033 CB08 CC01 DA01 DA05 DB16 DB18 DB20 EA07 EC01