(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2017-183930
(P2017-183930A)
(43)公開日　平成29年10月5日(2017.10.5)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/32	(2006.01)	H04L	9/00	675B	5J104
H04L	9/14	(2006.01)	H04L	9/00	641	
H04L	9/08	(2006.01)	H04L	9/00	601F	
G06F	21/44	(2013.01)	G06F	21/44		

審査請求 未請求　請求項の数 8　ＯＬ　（全 12 頁）

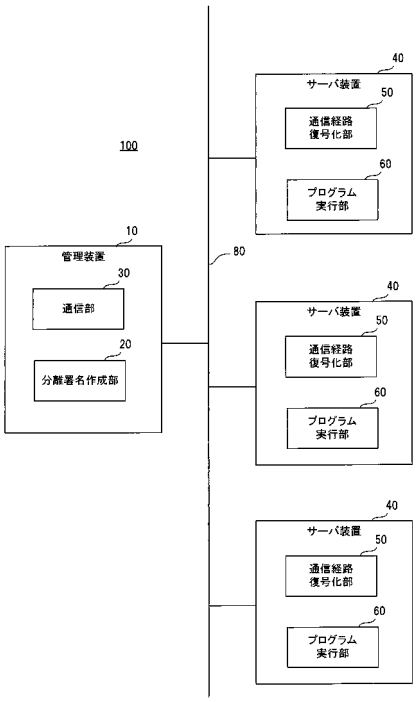
(21)出願番号　特願2016-66497(P2016-66497)
(22)出願日　平成28年3月29日(2016.3.29)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　110002044
特許業務法人ブライタス
(72)発明者　大津　裕史
東京都港区芝五丁目７番１号　日本電気株式会社内

Ｆターム(参考)　5J104 AA09 AA16 AA32 EA04 EA19 JA21 NA02 NA37 NA38 PA07

(54)【発明の名称】サーバ管理システム、サーバ装置、サーバ管理方法、及びプログラム

(57)【要約】
【課題】通信経路のセキュリティの確保を図ると同時に、プログラムの実行権限の設定を容易に行なえ得る、サーバ管理システム、サーバ装置、サーバ管理方法、及びプログラムを提供する。
【解決手段】サーバ管理システム１００は、管理装置１０とサーバ装置４０とを備えている。管理装置１０は、サーバ装置において実行されるプログラム毎に、暗号化された分離署名を作成する分離署名作成部２０と、暗号化した通信経路を介して分離署名をサーバ装置４０に送信する通信部３０とを備えている。サーバ装置４０は、管理装置１０が、暗号化した通信経路を介して、分離署名を送信してきた場合に、第１の公開鍵を用いて、通信経路の復号化を実行する通信経路復号化部５０と、通信経路の復号化が成功した場合に、第２の公開鍵を用いて、分離署名の検証を実行し、検証が成功した場合に、分離署名が対応するプログラムを実行するプログラム実行部６０とを備えている。
【選択図】図１



【特許請求の範囲】
【請求項１】
管理装置と、管理対象となるサーバ装置とを備え、
前記管理装置は、
前記サーバ装置において実行されるプログラム毎に、暗号化された分離署名を作成する、分離署名作成部と、
暗号化した通信経路を介して、前記分離署名を、前記サーバ装置に送信する、通信部と、
を備え、
前記サーバ装置は、
前記管理装置が、暗号化した通信経路を介して、前記分離署名を送信してきた場合に、第１の公開鍵を用いて、前記通信経路の復号化を実行する、通信経路復号化部と、
前記通信経路の復号化が成功した場合に、第２の公開鍵を用いて、前記分離署名の検証を実行し、前記検証が成功した場合に、前記分離署名が対応するプログラムを実行する、プログラム実行部と、
を備えている、
ことを特徴とする、サーバ管理システム。
【請求項２】
前記管理装置において、前記通信部が、アカウントを提示して、前記分離署名を、前記サーバ装置に送信し、
前記サーバ装置において、前記プログラム実行部が、前記分離署名が対応するプログラムについて前記アカウントでの実行が許可されているかどうかを判定し、許可されている場合に、前記分離署名が対応するプログラムを実行する、
請求項１に記載のサーバ管理システム。
【請求項３】
プログラム毎に暗号化された分離署名を作成する管理装置から、暗号化した通信経路を介して、前記分離署名が送信されてきた場合に、第１の公開鍵を用いて、前記通信経路の復号化を実行する、通信経路復号化部と、
前記通信経路の復号化が成功した場合に、第２の公開鍵を用いて、前記分離署名の検証を実行し、前記検証が成功した場合に、前記分離署名が対応するプログラムを実行する、プログラム実行部と、
を備えている、
ことを特徴とする、サーバ装置。
【請求項４】
前記管理装置から、アカウントを提示して、前記分離署名が送信されてきた場合に、
前記プログラム実行部が、前記分離署名が対応するプログラムについて前記アカウントでの実行が許可されているかどうかを判定し、許可されている場合に、前記分離署名が対応するプログラムを実行する、
請求項３に記載のサーバ装置。
【請求項５】
管理装置と、管理対象となるサーバ装置とを用いた、サーバ管理方法であって、
（ａ）前記管理装置によって、前記サーバ装置において実行されるプログラム毎に、暗号化された分離署名を作成する、ステップと、
（ｂ）前記管理装置によって、暗号化した通信経路を介して、前記分離署名を、前記サーバ装置に送信する、ステップと、
（ｃ）前記サーバ装置によって、前記管理装置が、暗号化した通信経路を介して、前記分離署名を送信してきた場合に、第１の公開鍵を用いて、前記通信経路の復号化を実行する、ステップと、
（ｄ）前記通信経路の復号化が成功した場合に、第２の公開鍵を用いて、前記分離署名の検証を実行し、前記検証が成功した場合に、前記分離署名が対応するプログラムを実行する、ステップと、

を有することを特徴とする、サーバ管理方法。
【請求項６】
前記（ｂ）のステップにおいて、アカウントを提示して、前記分離署名を、前記サーバ装置に送信し、
前記（ｄ）のステップにおいて、前記分離署名が対応するプログラムについて前記アカウントでの実行が許可されているかどうかを判定し、許可されている場合に、前記分離署名が対応するプログラムを実行する、
請求項５に記載のサーバ管理方法。
【請求項７】
コンピュータに、
（ａ）プログラム毎に暗号化された分離署名を作成する管理装置から、暗号化した通信経路を介して、前記分離署名が送信されてきた場合に、第１の公開鍵を用いて、前記通信経路の復号化を実行する、ステップと、
（ｂ）前記通信経路の復号化が成功した場合に、第２の公開鍵を用いて、前記分離署名の検証を実行し、前記検証が成功した場合に、前記分離署名が対応するプログラムを実行する、ステップと、
を実行させるプログラム。
【請求項８】
前記管理装置から、アカウントを提示して、前記分離署名が送信されてきた場合に、
前記（ｂ）のステップにおいて、前記分離署名が対応するプログラムについて前記アカウントでの実行が許可されているかどうかを判定し、許可されている場合に、前記分離署名が対応するプログラムを実行する、
請求項７に記載のプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、管理装置によって複数のサーバ装置を管理するためのサーバ管理システム及びサーバ管理方法に関し、更には、管理対象となるサーバ装置及びこれを実現するためのプログラムに関する。
【背景技術】
【０００２】
近年、クラウドコンピューティングの利用が増加している。クラウドコンピューティングによれば、ユーザは、インターネットの向こう側から各種サービスを受けることができるので、自身においてサービスに必要な設備を用意する必要がなく、接続環境のみを用意すれば良い。
【０００３】
そして、このクラウドコンピューティングでは、遠隔からサーバ装置を管理する必要があり、この遠隔からのサーバ装置の管理技術が重要となる（例えば、特許文献１参照。）。具体的には、特許文献１は、遠隔地からの依頼に応じてプログラムを起動するシステムを開示している。特許文献１に開示されたシステムは、ユーザ側のコンピュータと、プログラムを実行するコンピュータとで構成されている。
【０００４】
そして、特許文献１に開示されたシステムにおいて、後者のコンピュータは、まず、プログラムのＵＲＬ、ユーザの識別情報、及びアクセス権限情報が設定されたリストを入手する。次に、後者のコンピュータは、前者のコンピュータから送信された署名及び公開鍵証明書を用いて、署名検証とユーザの同定とを実行する。そして、署名検証とユーザの同定とが成功すると、後者のコンピュータは、入手したリストから、ＵＲＬとアクセス権限情報とを読み出して、プログラムを実行する。このように、特許文献１に開示されたシステムによれば、不正なアクセスを排除しつつ、ユーザが要求するプログラムを実行できるので、遠隔からサーバ装置を適切に管理できると考えられる。

【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特開２００６－５８９９４号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
しかしながら、特許文献１に開示されたシステムでは、モジュール本体に、署名、ＵＲＬ、及びアクセス権限情報を付与する必要があり、管理に必要となる設定作業が面倒であるという問題がある。また、特許文献１に開示されたシステムでは、プログラムの実行を指示するユーザ側のコンピュータとプログラムを実行するコンピュータとの通信経路のセキュリティが確保できていないという問題もある。
【０００７】
本発明の目的の一例は、上記問題を解消し、通信経路のセキュリティの確保を図ると同時に、プログラムの実行権限の設定を容易に行なえ得る、サーバ管理システム、サーバ装置、サーバ管理方法、及びプログラムを提供することにある。
【課題を解決するための手段】
【０００８】
上記目的を達成するため、本発明の一側面におけるサーバ管理システムは、
管理装置と、管理対象となるサーバ装置とを備え、
前記管理装置は、
前記サーバ装置において実行されるプログラム毎に、暗号化された分離署名を作成する、分離署名作成部と、
暗号化した通信経路を介して、前記分離署名を、前記サーバ装置に送信する、通信部と、
を備え、
前記サーバ装置は、
前記管理装置が、暗号化した通信経路を介して、前記分離署名を送信してきた場合に、第１の公開鍵を用いて、前記通信経路の復号化を実行する、通信経路復号化部と、
前記通信経路の復号化が成功した場合に、第２の公開鍵を用いて、前記分離署名の検証を実行し、前記検証が成功した場合に、前記分離署名が対応するプログラムを実行する、プログラム実行部と、
を備えている、
ことを特徴とする。
【０００９】
上記目的を達成するため、本発明の一側面におけるサーバ装置は、
プログラム毎に暗号化された分離署名を作成する管理装置から、暗号化した通信経路を介して、前記分離署名が送信されてきた場合に、第１の公開鍵を用いて、前記通信経路の復号化を実行する、通信経路復号化部と、
前記通信経路の復号化が成功した場合に、第２の公開鍵を用いて、前記分離署名の検証を実行し、前記検証が成功した場合に、前記分離署名が対応するプログラムを実行する、プログラム実行部と、
を備えている、
ことを特徴とする。
【００１０】
また、上記目的を達成するため、本発明の一側面におけるサーバ管理方法は、
管理装置と、管理対象となるサーバ装置とを用いた、サーバ管理方法であって、
（ａ）前記管理装置によって、前記サーバ装置において実行されるプログラム毎に、暗号化された分離署名を作成する、ステップと、
（ｂ）前記管理装置によって、暗号化した通信経路を介して、前記分離署名を、前記サーバ装置に送信する、ステップと、

（ｃ）前記サーバ装置によって、前記管理装置が、暗号化した通信経路を介して、前記分離署名を送信してきた場合に、第１の公開鍵を用いて、前記通信経路の復号化を実行する、ステップと、
（ｄ）前記通信経路の復号化が成功した場合に、第２の公開鍵を用いて、前記分離署名の検証を実行し、前記検証が成功した場合に、前記分離署名が対応するプログラムを実行する、ステップと、
を有することを特徴とする。
【００１１】
更に、上記目的を達成するため、本発明の一側面におけるプログラムは、
コンピュータに、
（ａ）プログラム毎に暗号化された分離署名を作成する管理装置から、暗号化した通信経路を介して、前記分離署名が送信されてきた場合に、第１の公開鍵を用いて、前記通信経路の復号化を実行する、ステップと、
（ｂ）前記通信経路の復号化が成功した場合に、第２の公開鍵を用いて、前記分離署名の検証を実行し、前記検証が成功した場合に、前記分離署名が対応するプログラムを実行する、ステップと、
を実行させることを特徴とする。
【発明の効果】
【００１２】
以上のように、本発明によれば、通信経路のセキュリティの確保を図ると同時に、プログラムの実行権限の設定を容易に行なうことができる。
【図面の簡単な説明】
【００１３】
【図１】図１は、本発明の実施の形態におけるサーバ装置及びサーバ管理システムの概略構成を示すブロック図である。
【図２】図２は、本発明の実施の形態におけるサーバ装置及びサーバ管理システムの具体的構成を示すブロック図である。
【図３】図３は、本発明の実施の形態における管理装置の動作を示すフロー図である。
【図４】図４は、本発明の実施の形態におけるサーバ装置の動作を示すフロー図である。
【図５】図５は、本発明の実施の形態における管理装置及びサーバ装置を実現するコンピュータの一例を示すブロック図である。
【発明を実施するための形態】
【００１４】
（実施の形態）
以下、本発明の実施の形態における、サーバ装置、サーバ管理システム、及びプログラムについて、図１～図４を参照しながら説明する。
【００１５】
［装置構成］
最初に、図１を用いて、本実施の形態におけるサーバ装置及びサーバ管理システムの概略構成について説明する。図１は、本発明の実施の形態におけるサーバ装置及びサーバ管理システムの概略構成を示すブロック図である。
【００１６】
図１に示すように、本実施の形態におけるサーバ管理システム１００は、管理装置１０と、管理対象となるサーバ装置４０とを備えている。本実施の形態では、管理装置１０は、ネットワーク８０を介してサーバ装置４０に接続されている。また、管理装置１０の管理対象となるサーバ装置４０は複数台である。
【００１７】
また、図１に示すように、管理装置１０は、分離署名作成部２０と、通信部３０とを備えている。分離署名作成部２０は、サーバ装置４０において実行されるプログラム毎に、暗号化された分離署名を作成する。通信部３０は、暗号化した通信経路を介して、分離署

名を、サーバ装置４０に送信する。

【００１８】

更に、図１に示すように、サーバ装置４０は、通信経路復号化部５０と、プログラム実行部６０とを備えている。通信経路復号化部５０は、管理装置１０が、暗号化した通信経路を介して、分離署名を送信してきた場合に、第１の公開鍵を用いて、通信経路の復号化を実行する。プログラム実行部６０は、通信経路の復号化が成功した場合に、第２の公開鍵を用いて、分離署名の検証を実行し、検証が成功した場合に、分離署名が対応するプログラムを実行する。

【００１９】

このように、本実施の形態では、管理装置から分離署名が送られてきたことを条件にプログラムが実行されるので、プログラム自体に権限情報等を付与することなく、プログラムの実行権限の設定を容易なものとできる。また、分離署名は、通信経路が複合化されない限り送信されないので、通信経路のセキュリティも同時に確保される。

【００２０】

続いて、図２を用いて、本実施の形態におけるサーバ装置及びサーバ管理システムの構成をより具体的に説明する。図２は、本発明の実施の形態におけるサーバ装置及びサーバ管理システムの具体的構成を示すブロック図である。なお、図２においては、説明のため、単一のサーバ装置のみが図示されている。

【００２１】

まず、本実施の形態では、サーバ装置４０において実行が予定されているプログラムに対しては、事前に、第三者によって検証が行なわれている。そして、図２に示すように、検証によって合格とされたプログラムが、実行モジュール７０として、サーバ装置４０に配置される。

【００２２】

図２に示すように、管理装置１０において、分離署名作成部２０は、実行モジュール７０毎に、ＰＧＰ（Pretty Good Privacy）を用いて分離署名２２を作成する。更に、分離署名作成部２０は、作成した分離署名２２を、管理装置１０に配置されているＰＧＰ秘密鍵２１を使用して暗号化する。

【００２３】

通信部３０は、本実施の形態では、ＳＳＨ（Secure SHell）を利用して、サーバ装置４０との間でデータ通信を実行する。具体的には、通信部３０は、ＳＳＨ公開鍵５１を作成し、これをサーバ装置４０に送信して、サーバ装置４０との間にセッションを確立する。その後、通信部３０は、送信対象となるデータをＳＳＨ秘密鍵にて暗号し、暗号化後のデータをサーバ装置４０に送信する。これにより、通信経路の暗号化が図られることになる。例えば、送信対象となるデータが分離署名２２の場合は、通信部３０は、ＳＳＨ秘密鍵３１を用いて暗号化した分離署名２２を、サーバ装置４０に送信する。

【００２４】

また、図２に示すように、サーバ装置４０において、通信経路復号化部５０は、ＳＳＨ公開鍵５１を受け取り、管理装置１０との間でセッションを確立すると、管理装置１０から送信されてきたデータをＳＳＨ公開鍵５１によって復号化し、復号化したデータをプログラム実行部６０に入力する。これにより、通信経路の復号化が図られることになる。

【００２５】

プログラム実行部６０は、本実施の形態では、モジュールディスパッチャで構築されており、各実行モジュール７０の実行指示はプログラム実行部６０でしか行なえないようになっている。また、プログラム実行部６０には、予め、ＰＧＰ公開鍵６１が配置されている。

【００２６】

プログラム実行部６０は、管理装置１０から、通信部３０と通信経路復号化部５０とで確立されたＳＳＨを介して、実行モジュール７０の実行指示と分離署名２２とが送信されてくると、ＰＧＰ公開鍵６１を使用して、分離署名２２の検証を実行する。そして、プロ

グラム実行部６０は、分離署名２２の検証が正常である場合は、実行モジュール７０は署名済みであり、且つ改竄されていないので、この実行モジュール７０を実行する。

【００２７】

［装置動作］

次に、本発明の実施の形態におけるサーバ管理システム１００の動作を図３及び図４を用いて説明する。以下の説明においては、適宜図１及び図２を参酌する。また、本実施の形態では、サーバ管理システム１００を動作させることによって、サーバ管理方法が実施される。よって、本実施の形態におけるサーバ管理方法の説明は、以下のサーバ管理システム１００の動作説明に代える。

【００２８】

最初に、管理装置１０の動作について図３を用いて説明する。図３は、本発明の実施の形態における管理装置の動作を示すフロー図である。また、前提として、管理装置１０において、分離署名作成部２０は、実行モジュール７０毎に分離署名２２を作成し、作成した分離署名２２を、ＰＧＰ秘密鍵２１を使用して暗号化しているとする。

【００２９】

図３に示すように、最初に、通信部３０は、外部から実行モジュール７０の実行が指示されると、指示された実行モジュールを配置しているサーバ装置４０との間でセッションを確立する（ステップＡ１）。具体的には、通信部３０は、ＳＳＨ公開鍵５１を作成し、これをサーバ装置４０に送信する。そして、サーバ装置４０が、ＳＳＨ公開鍵５１で暗号化されたセッション鍵を作成し、これを管理装置１０に送信すると、セッションが確立される。

【００３０】

次に、分離署名作成部２０が、通信部３０に対して、実行が指示された実行モジュールの分離署名を送信するように指示すると、通信部３０は、ＳＳＨ秘密鍵３１によって実行指示と分離署名とを暗号化し、これをサーバ装置４０に送信する（ステップＡ２）。

【００３１】

ステップＡ２の実行により、管理装置１０での処理は一旦終了する。なお、ステップＡ１及びＡ２は、実行モジュール７０の実行が指示される度に実行される。

【００３２】

続いて、サーバ装置４０の動作について図４を用いて説明する。図４は、本発明の実施の形態におけるサーバ装置の動作を示すフロー図である。

【００３３】

図４に示すように、最初に、通信経路復号化部５０は、管理装置１０から送信されてきたＳＳＨ公開鍵５１を受け取り、管理装置１０との間でセッションを確立する（ステップＢ１）。

【００３４】

次に、通信経路復号化部５０は、管理装置１０から送信されてきた、実行モジュール７０の実行指示と分離署名とを受信し、これらをＳＳＨ公開鍵によって復号化する（ステップＢ２）。

【００３５】

次に、通信経路復号化部５０は、ステップＢ２による復号化が成功しているかどうかを判定する（ステップＢ３）。ステップＢ３の判定の結果、復号化が成功していない場合は、通信経路復号化部５０は、後述のステップＢ７を実行する。

【００３６】

一方、ステップＢ３の判定の結果、復号化が成功している場合は、通信経路復号化部５０は、プログラム実行部６０を起動する。これにより、プログラム実行部６０は、ＰＧＰ公開鍵６１を用いて、ステップＢ２で受信した分離署名を検証する（ステップＢ４）。

【００３７】

次に、プログラム実行部６０は、分離署名の検証が成功したかどうかを判定する（ステップＢ５）。ステップＢ６の判定の結果、検証が成功している場合は、プログラム実行部

６０は、実行モジュールを実行する（ステップＢ６）。一方、ステップＢ６の判定の結果、検証が成功していない場合は、プログラム実行部６０は、そのことを通信経路復号化部５０に通知する。これにより、通信経路復号化部５０は、ステップＢ７を実行する。

【００３８】

ステップＢ７では、通信経路復号化部５０は、管理装置１０に対して、実行モジュールを実行できない旨のメッセージを送信する。

【００３９】

ステップＢ６又はＢ７の実行により、サーバ装置４０での処理は一旦終了する。なお、ステップＢ１～Ｂ７は、管理装置１０から実行モジュール７０の実行が指示される度に実行される。

【００４０】

［実施の形態における効果］

以上のように、本実施の形態では、管理装置１０から、ＳＳＨを介して実行モジュール７０の実行指示を受け付けられるのは、モジュールディスパッチャであるプログラム実行部６０のみである。サーバ装置４０において、特権で動くことができるのも、プログラム実行部６０のみである。つまり、本実施の形態では、プログラム実行部６０以外が実行モジュール７０を直接実行することはできず、また、実行モジュール７０自体が単独で特権を取得することもできないようになっている。更に、本実施の形態では、管理装置１０とサーバ装置４０との間のセキュリティはＳＳＨによって確保されている。

【００４１】

このため、本実施の形態では、特権が必要な運用がセキュアに自動化されるので、管理装置１０のオペレータは、各サーバ装置４０の特権の取得方法を網羅しておく必要がなく、事前に実行モジュールの検証を行なうだけで良い。更に、実行モジュールが、上位層から自動実行される場合、つまり人による判断が介在しない場合においても、特権作業でありながら安全に実行できる。

【００４２】

また、実行モジュール７０の改造、追加、削除等を行うために、実行モジュールを用意することができ、この場合は、機能の拡張及び調整が、容易、且つ安全なものとなる。更に、本実施の形態は、管理装置１０の管理対象となるサーバ装置４０の数が多くなればなるほど、その仕様が標準化されているほど、大きな効果を発揮する。

【００４３】

以上の効果が得られるので、本実施の形態におけるサーバ管理システム１００は、例えば、分散配置されたデータセンタの集中管理に有用である。また、サーバ管理システム１００は、オフィス等に配置された各種機器、例えば、複合機、自動販売機等を管理する場合にも有用である。

【００４４】

［変形例］

また、本実施の形態では、管理装置１０において、通信部３０は、アカウントを提示して、分離署名２２を、サーバ装置４０に送信することができる。この場合、サーバ装置４０において、プログラム実行部６０は、分離署名が対応する実行モジュール７０について、提示されたアカウントでの実行が許可されているかどうかを判定する。そして、プログラム実行部６０は、提示されたアカウントでの実行が許可されている場合にのみ、分離署名が対応するプログラムを実行する。このような態様とした場合は、アカウントによる権限管理を行なうことが可能となる。

【００４５】

［プログラム］

本実施の形態における第１のプログラムは、コンピュータに、図３に示すステップＡ１及びＡ２を実行させるプログラムであれば良い。このプログラムをコンピュータにインストールし、実行することによって、本実施の形態における管理装置１０を実現することができる。この場合、コンピュータのＣＰＵ（Central Processing Unit）は、分離署名作

成部２０及び通信部３０として機能し、処理を行なう。
【００４６】
また、本実施の形態における第１のプログラムは、複数のコンピュータによって構築されたコンピュータシステムによって実行されても良い。この場合は、例えば、各コンピュータが、それぞれ、分離署名作成部２０及び通信部３０のいずれかとして機能する。
【００４７】
本実施の形態における第２のプログラムは、コンピュータに、図４に示すステップＢ１～Ｂ７を実行させるプログラムであれば良い。このプログラムをコンピュータにインストールし、実行することによって、本実施の形態におけるサーバ装置４０を実現することができる。この場合、コンピュータのＣＰＵ（Central Processing Unit）は、通信経路復号化部５０及びプログラム実行部７０として機能し、処理を行なう。
【００４８】
また、本実施の形態における第２のプログラムも、複数のコンピュータによって構築されたコンピュータシステムによって実行されても良い。この場合は、例えば、各コンピュータが、それぞれ、信経路復号化部５０及びプログラム実行部７０のいずれかとして機能する。
【００４９】
［物理構成］
ここで、本実施の形態における第１のプログラムを実行することによって、管理装置１０を実現するコンピュータ、及び第２のプログラムを実行することによって、サーバ装置４０を実現するコンピュータについて図５を用いて説明する。図５は、本発明の実施の形態における管理装置及びサーバ装置を実現するコンピュータの一例を示すブロック図である。
【００５０】
図５に示すように、コンピュータ１１０は、ＣＰＵ１１１と、メインメモリ１１２と、記憶装置１１３と、入力インターフェイス１１４と、表示コントローラ１１５と、データリーダ／ライタ１１６と、通信インターフェイス１１７とを備える。これらの各部は、バス１２１を介して、互いにデータ通信可能に接続される。
【００５１】
ＣＰＵ１１１は、記憶装置１１３に格納された、本実施の形態におけるプログラム（コード）をメインメモリ１１２に展開し、これらを所定順序で実行することにより、各種の演算を実施する。メインメモリ１１２は、典型的には、ＤＲＡＭ（Dynamic Random Access Memory）等の揮発性の記憶装置である。また、本実施の形態におけるプログラムは、コンピュータ読み取り可能な記録媒体１２０に格納された状態で提供される。なお、本実施の形態におけるプログラムは、通信インターフェイス１１７を介して接続されたインターネット上で流通するものであっても良い。
【００５２】
また、記憶装置１１３の具体例としては、ハードディスクドライブの他、フラッシュメモリ等の半導体記憶装置が挙げられる。入力インターフェイス１１４は、ＣＰＵ１１１と、キーボード及びマウスといった入力機器１１８との間のデータ伝送を仲介する。表示コントローラ１１５は、ディスプレイ装置１１９と接続され、ディスプレイ装置１１９での表示を制御する。
【００５３】
データリーダ／ライタ１１６は、ＣＰＵ１１１と記録媒体１２０との間のデータ伝送を仲介し、記録媒体１２０からのプログラムの読み出し、及びコンピュータ１１０における処理結果の記録媒体１２０への書き込みを実行する。通信インターフェイス１１７は、ＣＰＵ１１１と、他のコンピュータとの間のデータ伝送を仲介する。
【００５４】
また、記録媒体１２０の具体例としては、ＣＦ（Compact Flash（登録商標））及びＳＤ（Secure Digital）等の汎用的な半導体記憶デバイス、フレキシブルディスク（Flexib

le Disk）等の磁気記憶媒体、又はＣＤ－ＲＯＭ（Compact Disk Read Only Memory）などの光学記憶媒体が挙げられる。

【産業上の利用可能性】

【００５５】

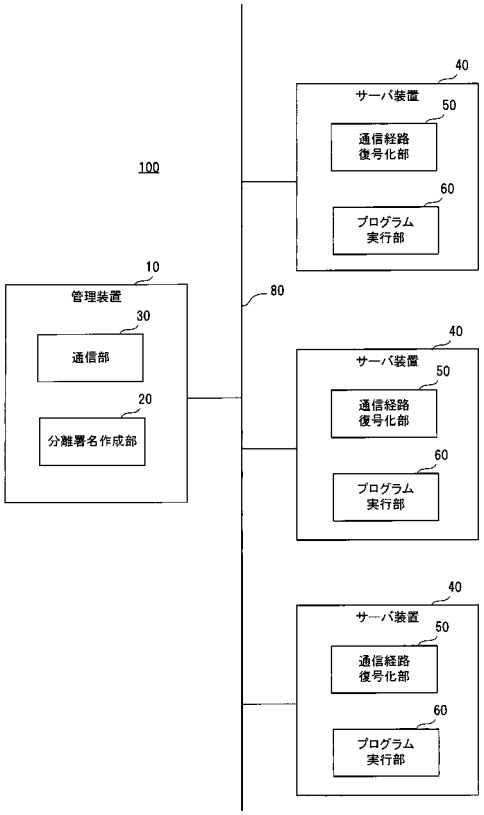
以上のように、本発明によれば、通信経路のセキュリティの確保を図ると同時に、プログラムの実行権限の設定を容易に行なうことができる。本発明は、遠隔からのアプリケーションプログラムの実行が必要な分野において有用である。

【符号の説明】

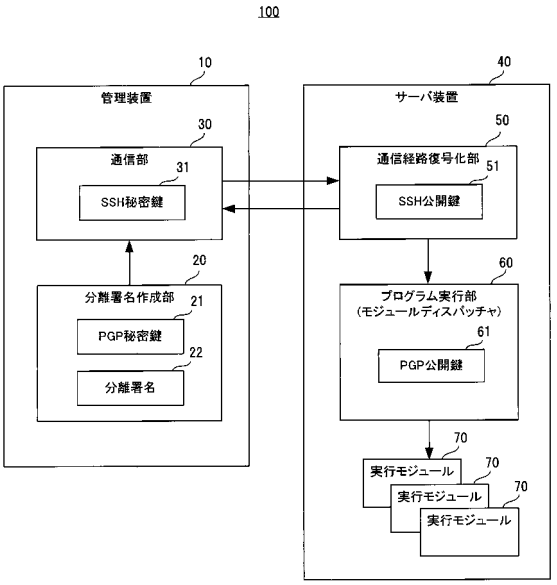
【００５６】

１０　管理装置
２０　分離署名作成部
２１　ＰＧＰ秘密鍵
２２　分離署名
３０　通信部
３１　ＳＳＨ秘密鍵
４０　サーバ装置
５０　通信経路復号化部
５１　ＳＳＨ公開鍵
６０　プログラム実行部
６１　ＰＧＰ公開鍵
７０　実行モジュール
１００　サーバ管理システム
１１０　コンピュータ
１１１　ＣＰＵ
１１２　メインメモリ
１１３　記憶装置
１１４　入力インターフェイス
１１５　表示コントローラ
１１６　データリーダ／ライタ
１１７　通信インターフェイス
１１８　入力機器
１１９　ディスプレイ装置
１２０　記録媒体
１２１　バス

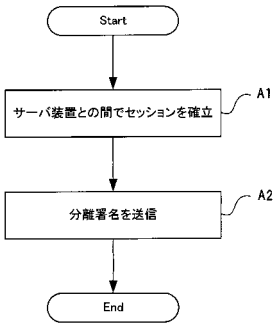
【図１】


100
10
管理装置
30
通信部
20
分離署名作成部
80
40
サーバ装置
50
通信経路
復号化部
60
プログラム
実行部
40
サーバ装置
50
通信経路
復号化部
60
プログラム
実行部
40
サーバ装置
50
通信経路
復号化部
60
プログラム
実行部

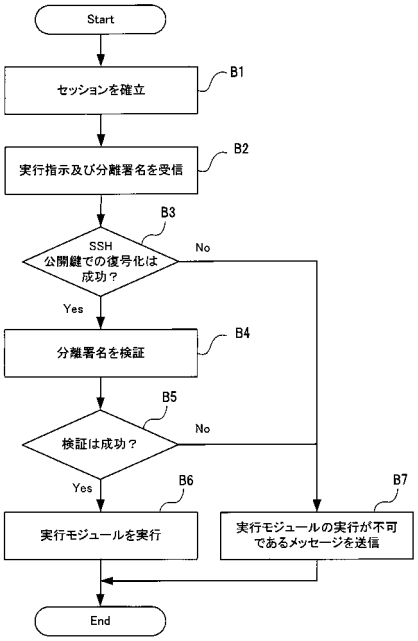
【図２】


100
10
管理装置
30
通信部
31
SSH秘密鍵
20
分離署名作成部
21
PGP秘密鍵
22
分離署名
40
サーバ装置
50
通信経路復号化部
51
SSH公開鍵
60
プログラム実行部
(モジュールディスパッチャ)
61
PGP公開鍵
70
実行モジュール
70
実行モジュール
70
実行モジュール

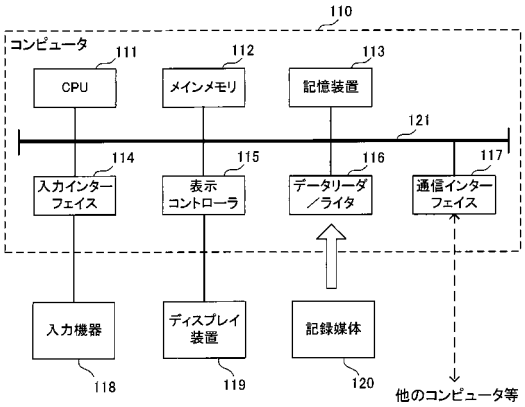
【図３】


Start
サーバ装置との間でセッションを確立
A1
分離署名を送信
A2
End

【図４】


Start
セッションを確立
B1
実行指示及び分離署名を受信
B2
B3
SSH
公開鍵での復号化は
成功？
No
Yes
分離署名を検証
B4
B5
検証は成功？
No
Yes
B6
実行モジュールを実行
B7
実行モジュールの実行が不可
であるメッセージを送信
End

【図５】


110
コンピュータ
111
CPU
112
メインメモリ
113
記憶装置
121
114
入力インターフェイス
115
表示コントローラ
116
データリーダ／ライタ
117
通信インターフェイス
入力機器
118
ディスプレイ装置
119
記録媒体
120
他のコンピュータ等