(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2007-179357
(P2007-179357A)
(43)公開日　平成19年7月12日(2007.7.12)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/22	(2006.01)	G06F	9/06	660E	5B017
G06F 21/24	(2006.01)	G06F	12/14	530C	5B076
					5B276

審査請求 未請求　請求項の数 1　OL　（全 7 頁）

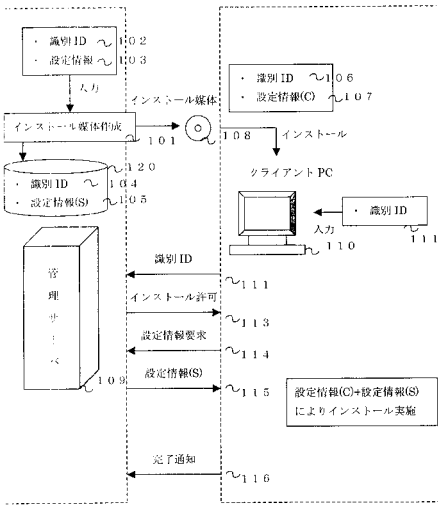
(21)出願番号　特願2005-377725 (P2005-377725)
(22)出願日　平成17年12月28日 (2005.12.28)

(71)出願人　000233055
日立ソフトウエアエンジニアリング株式会社
神奈川県横浜市鶴見区末広町一丁目１番４３
(74)代理人　100088720
弁理士　小川　眞一
(72)発明者　白澤　勇治
東京都品川区東品川４丁目１２番７号　日立ソフトウエアエンジニアリング株式会社内

Fターム(参考)　5B017 AA03　BB10　CA15
5B076 AA06　FB01
5B276 FB01

(54)【発明の名称】コンピュータプログラムのインストール方法

(57)【要約】
【課題】　インストール媒体の解析による設定データの流出防止と、不正ユーザのコンピュータ内に正規ユーザと同じインストール済み環境が構築されるのを防止すること。
【解決手段】　管理サーバにおいて前記設定情報をセキュリティ上の保護対象とする第１の設定情報と保護対象としない第２の設定情報に分割し、その第２の設定情報とインストール媒体の識別ＩＤとを埋め込んだインストール媒体を作成すると共に、前記第２の設定情報は管理サーバのデータベースに格納するステップと、前記管理サーバにおいて、ユーザコンピュータから受信した識別ＩＤが前記データベースに格納されている識別ＩＤと一致するか否かによってユーザ認証を行い、一致した場合のみ第１の設定情報を読出し、配信要求元のユーザコンピュータに配信するステップとを備える。
【選択図】　図１



【特許請求の範囲】
【請求項１】
保守管理などに使用する設定情報を埋め込んだインストール媒体によりコンピュータプログラムをインストール対象のコンピュータにインストールする方法において、
管理サーバにおいて前記設定情報をセキュリティ上の保護対象とする第１の設定情報と保護対象としない第２の設定情報に分割し、その第２の設定情報とインストール媒体の識別ＩＤとを埋め込んだインストール媒体を作成すると共に、前記第２の設定情報は管理サーバのデータベースに格納する第１のステップと、
前記インストール媒体によるインストール対象のユーザコンピュータにおけるインストール実行時に前記識別ＩＤに一致する識別ＩＤがユーザにより入力された場合にのみ、入力された識別ＩＤを前記管理サーバに送信する第２のステップと、
前記管理サーバにおいて、前記ユーザコンピュータから受信した識別ＩＤが前記データベースに格納されている識別ＩＤと一致するか否かによってユーザ認証を行い、一致した場合のみインストール許可通知を識別ＩＤ送信元のユーザコンピュータに返信する第３のステップと、
インストール許可通知を受けたユーザコンピュータにおいて、前記第１の設定情報の配信要求を前記管理サーバに送信する第４のステップと、
管理サーバにおいて前記データベースに格納された前記第１の設定情報を読出し、配信要求元のユーザコンピュータに配信する第５のステップと、
ユーザコンピュータにおいて管理サーバから受信した第１の設定情報と前記第２の設定情報が埋め込まれたコンピュータプログラムのインストールを実行する第６のステップとを備えることを特徴とするコンピュータプログラムのインストール方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、コンピュータプログラムのインストール方法に係り、特に、インストール媒体に記録された情報の解析によって正規ユーザではない第３者に、正規ユーザのみに提供する情報が漏洩しないようにインストールすることができるコンピュータプログラムのインストール方法に関するものである。
【背景技術】
【０００２】
従来、コンピュータにインストールするプログラムやデータなどの安全性を確保する技術として、例えば、下記特許文献１～３に記載のものが知られている。
コンピュータにプログラムをインストールする場合に、著作権保護の目的でインストールそのものに制限をかけることがある（例えば、特許文献１参照）。
また、プログラムの不正利用防止を目的として、インストールするコンピュータに固有の情報をキーにして実行を制御する方法がある（例えば、特許文献２参照）。
同様に、不正利用を目的として同じ識別コードをクライアントプログラムとサーバプログラムに埋め込み、識別コードの一致を確認することにより実行を制御する方法がある（例えば、特許文献３参照）。
【０００３】
【特許文献１】特開２００４－２３４６６８
【特許文献２】特開２００２－３１２０５２
【特許文献３】特開２００３－５８５９
【発明の開示】
【発明が解決しようとする課題】
【０００４】
ところで、ユーザに配布されるコンピュータプログラムのインストール媒体には当該プログラムの利便性や保守管理などを考慮した初期データが埋め込まれている場合がある。この初期データには、作成元外部の第３者に知られても問題のない情報と、作成元外部の

第３者に知られることが好ましくない情報とに分類される。
作成元外部の第３者に知られても問題のない情報の例として、インストールするプログラムのショートカットをデスクトップ上に作成するか否かを指定しているような情報がある。
これに対して、作成元外部の第３者に知られることが好ましくない初期データの例として、通信を行うプログラムなどで設定する必要のある管理サーバのホスト名やポート番号、インストール時に使用するＩＤとパスワードの組など、構築対象のシステムに関するセキュリティポリシーに関する情報がある。

【０００５】

しかしながら、上記従来技術においては、インストールそれ自体の実行を制御することはできるが、インストール媒体そのものに埋め込まれた情報の解析や改ざんを行うことができる。このため、インストール媒体に記録された情報の解析により、作成元外部の第３者に知られることが好ましくない情報が知られてしまうと、不正ユーザのコンピュータ内に管理サーバへのアクセス環境を不正に構築することが可能になり、情報漏洩の危険性が大きくなるという問題がある。
すなわち、インストール媒体そのものに埋め込まれた情報の解析により管理サーバのホスト名やポート番号、ＩＤとパスワードの組などの初期データが不正ユーザに知られてしまうと、そのホスト名やポート番号、ＩＤとパスワードの組などのデータを不正に使用して管理サーバ内で管理しているデータを不正に入手し、不正ユーザのコンピュータ内に管理サーバへのアクセス環境を不正に構築することが可能になる。その結果、管理サーバ内で管理している初期データ等の情報漏洩の危険性が高くなる。
また、プログラムの実行を管理サーバ経由で許可するような初期データが組み込まれていたとしても、その初期データの改ざんにより、管理サーバを迂回してプログラムを不正に実行することも可能になり、好ましくない。

【０００６】

本発明の目的は、コンピュータプログラムのインストール媒体に保守管理などの設定データを埋め込んで配布する形態において、インストール媒体の解析による設定データの流出防止と、不正ユーザのコンピュータ内に正規ユーザと同じインストール済み環境が構築されるのを防止することができるコンピュータプログラムのインストール方法を提供することにある。

【課題を解決するための手段】

【０００７】

上記目的を達成するために、本発明は、保守管理などに使用する設定情報を埋め込んだインストール媒体によりコンピュータプログラムをインストール対象のコンピュータにインストールする方法において、
管理サーバにおいて前記設定情報をセキュリティ上の保護対象とする第１の設定情報と保護対象としない第２の設定情報に分割し、その第２の設定情報とインストール媒体の識別ＩＤとを埋め込んだインストール媒体を作成すると共に、前記第２の設定情報は管理サーバのデータベースに格納する第１のステップと、
前記インストール媒体によるインストール対象のユーザコンピュータにおけるインストール実行時に前記識別ＩＤに一致する識別ＩＤがユーザにより入力された場合にのみ、入力された識別ＩＤを前記管理サーバに送信する第２のステップと、
前記管理サーバにおいて、前記ユーザコンピュータから受信した識別ＩＤが前記データベースに格納されている識別ＩＤと一致するか否かによってユーザ認証を行い、一致した場合のみインストール許可通知を識別ＩＤ送信元のユーザコンピュータに返信する第３のステップと、
インストール許可通知を受けたユーザコンピュータにおいて、前記第１の設定情報の配信要求を前記管理サーバに送信する第４のステップと、
管理サーバにおいて前記データベースに格納された前記第１の設定情報を読出し、配信要求元のユーザコンピュータに配信する第５のステップと、

ユーザコンピュータにおいて管理サーバから受信した第１の設定情報と前記第２の設定情報が埋め込まれたコンピュータプログラムのインストールを実行する第６のステップとを備えることを特徴とするコンピュータプログラムのインストール方法。

【発明の効果】

【０００８】

本発明によれば、管理サーバで作成するインストール媒体には、セキュリティで保護対象となる第１の設定情報は埋め込まれず、インストール媒体の識別ＩＤとインストールするプログラムのショートカットなどのセキュリティ上の保護対象にしない第２の設定情報のみが埋め込まれてユーザに配布される。

このため、インストール媒体が盗難等により紛失した場合でも、インストール媒体を不正に入手した第三者が、インストール媒体自体の情報を解析したとしてもセキュリティで保護対象となる第１の設定情報を知ることは不可能となる。

また、正規の識別ＩＤを入手しない限り、セキュリティで保護対象となる第１の設定情報を管理サーバから取得してインストールを完了させることはできなくなる。

この結果、インストール媒体を不正に入手した第三者が、正規ユーザと同一の環境を不正ユーザのコンピュータ内に構築し、管理サーバで管理している機密情報を不正取得したり、管理サーバを攻撃するといった二次的なセキュリティ脅威をなくすことができる。

また、ユーザコンピュータから送信された識別ＩＤを基にユーザコンピュータに配信する第１の設定情報を変更できるため、第１の設定情報を更新する必要が生じた場合でも、個別にインストール媒体を作成するよりも、効率良く管理することが可能になる。

【発明を実施するための最良の形態】

【０００９】

以下、本発明を実施する場合の一形態を、図面を参照して具体的に説明する。

図１は、本発明を実施する際の一形態を示すブロック図である。

インストール媒体１０８を作成し管理を行う管理サーバ１０９と、実際にインストールを行うクライアントＰＣ１１０で構成される。

管理サーバ１０９は、インストール媒体１０８の作成時に設定した識別ＩＤ１０２とインストール時に必要な設定情報１０３のうち、特にセキュリティ上で保護すべき設定情報（Ｓ）を格納するデータベース１２０を有している。

管理サーバ１０９でインストール媒体１０８を作成する際、設定情報１０３の他に識別ＩＤ１０２の入力をインストール媒体作成者に要求する。管理サーバ１０９は、入力された識別ＩＤ１０２を含むインストール媒体１０８を作成すると同時に、管理サーバ１０９のデータベース１２０にも前記識別ＩＤ１０２と同じ識別ＩＤ１０４を格納しておき、実際のインストールにおいてユーザ認証を行う際に使用する。

また、セキュリティ上で保護すべき設定情報（Ｓ）については、インストール媒体１０８に含ませず、管理サーバ１０９のデータベース１２０に格納しておく。

クライアントＰＣ１１０にインストールを行う場合は、識別ＩＤ１０６（識別ＩＤ１０２と同じ）と一部の設定情報（Ｃ）１０７が格納されたインストール媒体１０８を用意し、インストールを開始する。

ここで、設定情報（Ｃ）とは、インストールするプログラムのショートカットアイコンなどの保護対象としない情報である。また設定情報（Ｓ）とは、セキュリティで保護対象とする管理サーバ名やポート番号などの情報である。

【００１０】

インストール時には識別ＩＤ１１１（識別ＩＤ１０６と同じ）の入力が求められるため、インストール媒体１０８に含まれる識別ＩＤ１０６と同じ識別ＩＤを入力する。

クライアントＰＣ１１０は、インストール媒体１０８に含まれる識別ＩＤ１０６と入力された識別ＩＤ１１１が一致した場合のみ、管理サーバ１０９と通信を行い、管理サーバ１０９に対し、入力された識別ＩＤ１１１を送信する。

管理サーバ１０９では、データベース１２０に格納している識別ＩＤ１０４とクライアントＰＣ１１０から受信した識別ＩＤ１１１とを比較し、一致した場合はインストール許

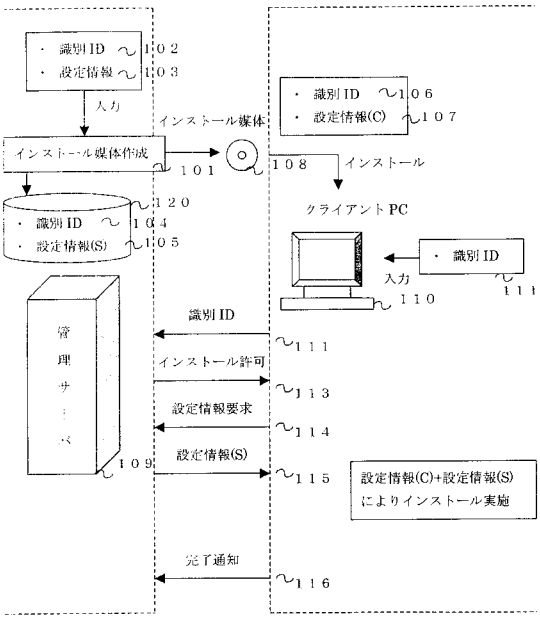
可１１３をクライアントＰＣ１１０に通知する。
インストールが許可されたクライアントＰＣ１１０は、管理サーバ１０９のデータベース１２０に格納されているセキュリティで保護すべき設定情報（Ｓ）１０５を取得するため、管理サーバ１０９に設定情報取得要求１１４を送信する。
管理サーバ１０９は、インストールを許可したクライアントＰＣ１１０から要求された設定情報（Ｓ）１１５をクライアントＰＣ１１０に配信する。
クライアントＰＣ１１０は、管理サーバ１０９から取得した設定情報（Ｓ）１１５と、インストール媒体１０８に含まれる設定情報（Ｃ）１０７を合わせて、クライアントＰＣ１１０でインストールを実行する。
クライアントＰＣ１１０は、インストールが完了した際は、管理サーバ１０９にインストール完了通知１１６を送信する。
【００１１】
図２は、管理サーバ側で動作するプログラムの一例を示すフローチャートである。
管理サーバ１０９では、クライアントＰＣ１１０から送信された識別ＩＤ１１１を受信する（ステップ２０１）。そして、受信した識別ＩＤ１１１とデータベース１２０に保存されている識別ＩＤ１０４を比較し（ステップ２０２）、不一致ならば、クライアントＰＣ１１０の要求を無視する（ステップ２０３）。
【００１２】
しかし、一致している場合には、インストールの許可をクライアントＰＣ１１０に通知する（ステップ２０４）。
次に、設定情報（Ｓ）の要求待ちとし（ステップ２０５）、クライアントＰＣ１１０から送信された設定情報要求を受信したならば（ステップ２０６）、データベース１２０に保存されている設定情報（Ｓ）１０５を読出し、クライアントＰＣ１１０に送信する（ステップ２０７）。
この後、インストール完了通知の受信待ちとなり（ステップ２０８）、インストール完了通知を受信したならば、処理を終了する（ステップ２０９）。
【００１３】
図３は、クライアントＰＣ側で動作するプログラムの一例を示すフローチャートである。
クライアントＰＣ１１０において、管理サーバ１０９の管理者から配布されたインストール媒体１０８によりインストール開始すると（ステップ３０１）、識別ＩＤの入力をユーザに要求する（ステップ３０２）。
ユーザ入力またはトークンにより取得した識別ＩＤ１１１とインストール媒体１０８に埋め込まれた識別ＩＤ１０６を比較し、不一致ならばエラーメッセージ表示してインストールを中断する（ステップ３０４）。
【００１４】
しかし、一致していた場合には、識別ＩＤ１１１を管理サーバ１０９に送信する（ステップ３０５）。
この後、管理サーバ１０９における認証の結果待ちとなり（ステップ３０６）、認証成功の結果を受信したならば、設定情報（Ｓ）１０５の配信を管理サーバ１０９に要求する（ステップ３０８）。
そして、設定情報（Ｓ）１０５を受信したならば、インストール媒体１０８に埋め込まれている設定情報（Ｃ）１０７と管理サーバ１０９から受信した設定情報（Ｓ）を使用してインストールを行う（ステップ３０９）。そして、インストール完了通知を管理サーバ１０９に送信し（ステップ３１０）、インストール完了とする（ステップ３１１）。
【図面の簡単な説明】
【００１５】
【図１】本発明を実施する一形態を示すブロック図である。
【図２】管理サーバ側で動作するプログラムの一例を示すフローチャートである。
【図３】クライアントＰＣ側で動作するプログラムの一例を示すフローチャートである。

【符号の説明】

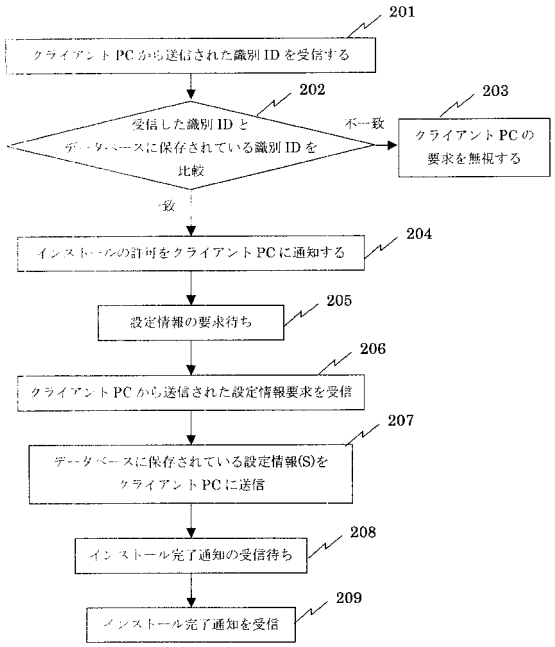
【００１６】

１０４　データベースに格納された識別ＩＤ
１０５　データベースに格納された設定情報（Ｓ）
１０６　インストール媒体に埋め込まれた識別ＩＤ
１０７　インストール媒体に埋め込まれた設定情報（Ｃ）
１０８　管理サーバで作成したインストール媒体
１０９　管理サーバ
１１０　クライアントコンピュータ
１２０　データベース

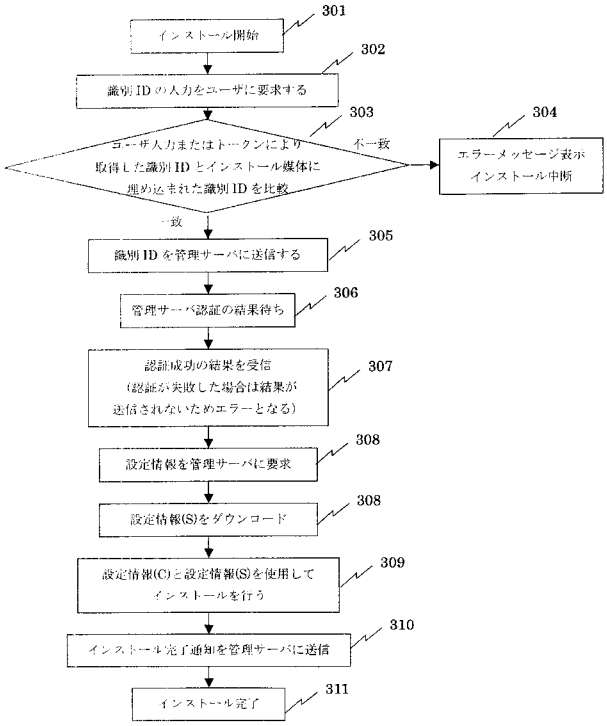
【図１】



【図２】



【図３】


301
インストール開始
302
識別IDの入力をユーザに要求する
303
ユーザ入力またはトークンにより
取得した識別IDとインストール媒体に
埋め込まれた識別IDを比較
不一致
304
エラーメッセージ表示
インストール中断
一致
305
識別IDを管理サーバに送信する
306
管理サーバ認証の結果待ち
307
認証成功の結果を受信
(認証が失敗した場合は結果が
送信されないためエラーとなる)
308
設定情報を管理サーバに要求
308
設定情報(S)をダウンコード
309
設定情報(C)と設定情報(S)を使用して
インストールを行う
310
インストール完了通知を管理サーバに送信
311
インストール完了