

【公報種別】特許法第 17 条の 2 の規定による補正の掲載
 【部門区分】第 6 部門第 3 区分
 【発行日】平成 18 年 9 月 7 日 (2006.9.7)

【公開番号】特開 2000-215168 (P2000-215168A)

【公開日】平成 12 年 8 月 4 日 (2000.8.4)

【出願番号】特願 平 11-214030

【国際特許分類】

G 0 6 F 21/20 (2006.01)

G 0 9 C 1/00 (2006.01)

H 0 4 L 9/32 (2006.01)

【F I】

G 0 6 F 15/00 3 3 0 B

G 0 9 C 1/00 6 6 0 E

H 0 4 L 9/00 6 7 3 A

H 0 4 L 9/00 6 7 5 A

【手続補正書】

【提出日】平成 18 年 7 月 25 日 (2006.7.25)

【手続補正 1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項 1】 1 つ以上のサービス・ホスト・コンピュータに対して接続されているアドミニストレーション・サーバ・コンピュータから前記 1 つ以上のサービス・ホスト・コンピュータ上に存在する複数の異なるサービスのアドミニストレーションへのアクセスを保護する方法であって、サービス・マネージャが前記アドミニストレーション・サーバ・コンピュータ上に存在する方法において、

選択されたユーザ識別子及び対応するプライベート・キーワードを提供する工程と、前記ユーザ識別子は前記複数の異なるサービスのうちの少なくとも 1 つへのアドミニストレイティブ・アクセスを有するユーザを識別するために設けられていることと、

前記サービス・マネージャのコントロール下において、前記選択されたユーザ識別子及び対応するプライベート・キーワードを永続ストレージ領域内に格納された複数のユーザ識別子及びプライベート・キーワードと比較することにより、ユーザを認証する工程と、

前記ユーザ識別子に関連するユーザがアドミニストレイティブ・アクセスを有するサービスのリストを導出する工程と、

前記導出したサービスのリストに含まれる前記複数のサービスのうちの選択された 1 つを管理するリクエストがあった際、前記永続ストレージ領域内の前記選択されたユーザ識別子に関連するアクセス・コントロール・データを調べることにより、前記選択されたユーザ識別子に関連するユーザが前記選択されたサービスへのアクセスを許可されていることを、前記選択されたサービスに関連するサービス・ホスト・コンピュータにおいてベリファイする工程と、

前記サービス・ホスト・コンピュータ上の 1 つ以上のマネジメント・ファイルをアドミニストレーション・サーバへ転送し、これによって、前記サービス・マネージャを使用したマネジメント・ファイルの操作を促進する工程とを含む方法。

【請求項 2】 前記アドミニストレーション・サーバ・コンピュータは、ブラウザ・プログラムの実行に適したアドミニストレーション・クライアント・コンピュータに対し

て接続されており、前記選択されたユーザ識別子及び対応するプライベート・キーワードは、前記アドミニストレーション・クライアント・コンピュータ及びアドミニストレーション・サーバ・コンピュータの間の通信コネクションを通じて提供され、前記アドミニストレーション・サーバ・コンピュータ、前記アドミニストレーション・クライアント・コンピュータ及び前記1つ以上のサービス・ホスト・コンピュータの間の通信接続はインターネット・プロトコルを使用する請求項1に記載の方法。

【請求項3】 前記選択されたユーザ識別子及び対応するプライベート・キーワードを提供する工程は、前記アドミニストレーション・クライアント・コンピュータを通じて前記サービス・マネージャへログオンする工程を更に含む請求項1 または2に記載の方法。

【請求項4】 前記ユーザを認証する工程は、前記ユーザ識別子及び対応するプライベート・キーワードを前記永続ストレージ領域へ伝達するために、ライトウェイト・ディレクトリ・アクセス・プロトコルを使用する工程を含む請求項1 から請求項3のいずれかに記載の方法。

【請求項5】 前記各ユーザ識別子是对応するユーザ・プロフィールを有し、前記ユーザ・プロフィールは特定のサービス・マネージャ・ユーザに対応するグローバル・ユーザ・アイデンティティを表す請求項1 から請求項4のいずれかに記載の方法。

【請求項6】 前記サービスのリストを導出する工程は、前記永続ストレージ領域を検索する工程を更に含み、前記永続ストレージ領域はユーザ・プロフィール・データベースを有し、前記ユーザ・プロフィール・データベースはユーザ・アクセス・レベル、許可可能なサービスのリスト及びパスワードをユーザ毎に含む請求項1 から請求項5のいずれかに記載の方法。

【請求項7】 前記選択されたユーザ識別子に関連するユーザが前記サービスのリストから選択されたサービスへのアクセスを許可されていることを、前記サービス・ホスト・コンピュータにおいてベリファイする工程は、コモン・ゲートウェイ・インターフェースを使用することによって、前記選択されたユーザ識別子及び対応するプライベート・キーワードをホスト・サーバ・コンピュータへ伝達する工程を更に含む請求項1 から請求項6のいずれかに記載の方法。

【請求項8】 前記サービス・ホスト・コンピュータは認証及びアクセス・コントロール・セグメントを有する請求項1 から請求項7のいずれかに記載の方法。

【請求項9】 前記選択されたユーザ識別子及び対応するプライベート・キーワードは使用を目的として前記1つ以上のサービス・ホスト・コンピュータへ自動的に伝達される請求項1 から請求項8のいずれかに記載の方法。

【請求項10】 前記サービスのリストを、前記アドミニストレーション・クライアント・コンピュータ上に表示されたユーザ・インターフェース内で表示する工程を更に含む請求項1に記載の方法。

【請求項11】 ホスト・サーバ・コンピュータ上のサービスの位置を決定するために、前記マネジメント・コンソール・プログラムによってサービス・ロケータを作成する工程を更に含む請求項1に記載の方法。

【請求項12】 前記ホスト・サーバ上の1つ以上のマネジメント・ファイルをアドミニストレーション・サーバへ転送する工程は、前記アドミニストレーション・サーバ・コンピュータ上のコモン・ゲートウェイ・インターフェースを開始し、これによって、前記1つ以上のマネジメント・ファイル及び複数のオペレーティング・システム・コマンドの転送を可能にする工程を更に含む請求項1 から請求項8のいずれかに記載の方法。

【請求項13】 アドミニストレーション・サーバ・コンピュータから1つ以上のサービス・ホスト・コンピュータ上に存在するサービスのアドミニストレーションを保護するシステムであって、前記アドミニストレーション・サーバ・コンピュータが、ブラウザ型プログラムを有するアドミニストレーション・クライアントと、前記1つ以上のサービス・ホスト・コンピュータとに対してインターネット・プロトコルを使用して接続されているシステムにおいて、

ユーザ特権に関連するデータを格納するためのユーザ・プロフィール・データ・リポジトリと、前記データはユーザ・アクセス・レベル、サービスのリスト及びパスワードをユーザ毎に含むことと、

ユーザ識別子及び対応するキーワードを受信し、かつ前記ユーザ識別子及び対応するキーワードを前記ユーザ・プロフィール・データ・リポジトリへ送信するために、前記アドミニストレーション・サーバ・コンピュータ上に存在する通信インターフェースのサービス・マネージャ・サブコンポーネントと、

前記1つ以上のサービス・ホスト上へ配置することに適したコンポーネント・コンフィギュレーション・ディレクトリと、前記コンポーネント・コンフィギュレーション・ディレクトリは前記複数のサービスに関連したマネジメント・モジュールを格納するためのコンポーネント・コンフィギュレーション・ファイルを含み、前記マネジメント・モジュールは前記複数のサービスを管理するために使用するマネジメント・データを含むことと、

前記ユーザ・プロフィール・データ・リポジトリ内に格納されたユーザ特権に関連するデータを調べることによってバリフィケーションを行うべく、前記ユーザ識別子及び対応するキーワードを受信し、かつ前記ユーザ識別子及び対応するキーワードを前記複数のサービス・ホスト・コンピュータへ送信するために、前記アドミニストレーション・サーバ・コンピュータ上に存在する前記通信インターフェースのサービス・ホスト・サブコンポーネントとを含むシステム。

【請求項14】 1つ以上のサービス・ホスト・コンピュータと、アドミニストレーション・クライアント・コンピュータとへ接続されたアドミニストレーション・サーバ・コンピュータから前記1つ以上のサービス・ホスト・コンピュータ上に存在する複数の異なるサービスのアドミニストレーションへのアクセスを保護するシステムであって、サービス・マネージャが前記アドミニストレーション・サーバ・コンピュータ上に存在するシステムにおいて、

選択されたユーザ識別子及び対応するプライベート・キーワードを前記サービス・マネージャへ提供するために使用可能な前記アドミニストレーション・クライアント・コンピュータ及びアドミニストレーション・サーバ・コンピュータの間の通信コネクションと、前記ユーザ識別子は前記複数のサービスのうちの少なくとも1つに対するアドミニストレイティブ・アクセスを有するユーザを識別するために設けられていることと、

前記サービス・マネージャのコントロール下において、前記選択されたユーザ識別子及び対応するプライベート・キーワードを永続ストレージ領域内に格納された複数のユーザ識別子及びプライベート・キーワードと比較することにより、ユーザを認証するために形成されたオーセンティケータと、

前記ユーザ識別子に関連するユーザがアドミニストレイティブ・アクセスを有するサービスのリストを導出するためのアクセス・コントロール・メカニズムと、

前記導出したサービスのリストに含まれる前記複数のサービスのうちの選択された1つへアクセスすることを前記選択されたユーザ識別子に関連するユーザが許可されていることをバリファイするためのサービス・ホスト・バリファイヤと、前記バリファイヤは前記選択されたサービスに関連するサービス・ホスト・コンピュータ上に存在し、かつ前記永続ストレージ領域内の前記選択されたユーザ識別子に関連するアクセス・コントロール・データを使用することと、

前記サービス・ホスト・コンピュータ上の1つ以上のマネジメント・ファイルを前記アドミニストレーション・サーバ・コンピュータへ転送し、これによって、前記サービス・マネージャを使用したマネジメント・ファイルの操作を促進するためのデータ転送コンポーネントと

を含むシステム。

【請求項15】 1つ以上のサービス・ホスト・コンピュータへ接続されたアドミニストレーション・サーバ・コンピュータから前記1つ以上のサービス・ホスト・コンピュータ上に存在する複数の異なるサービスのアドミニストレーションへのアクセスを保護す

るためにコンピュータによって実行されるコンピュータ・プログラミング命令を格納するために設けられたコンピュータ読み取り可能媒体であって、サービス・マネージャが前記アドミニストレーション・サーバ・コンピュータ上に存在するコンピュータ読み取り可能媒体において、

選択されたユーザ識別子及び対応するプライベート・キーワードを提供するためのコンピュータ・プログラミング命令と、前記ユーザ識別子は前記複数の異なるサービスのうちの少なくとも1つへのアドミニストレイティブ・アクセスを有するユーザを識別するために設けられていることと、

前記サービス・マネージャのコントロール下において、前記選択されたユーザ識別子及び対応するプライベート・キーワードを永続ストレージ領域内に格納された複数のユーザ識別子及びプライベート・キーワードと比較することにより、ユーザを認証するためのコンピュータ・プログラミング命令と、

前記ユーザ識別子に関連するユーザがアドミニストレイティブ・アクセスを有するサービスのリストを導出するためのコンピュータ・プログラミング命令と、

前記導出したサービスのリストに含まれる前記複数のサービスのうちの選択された1つを管理するリクエストがあったとき、前記永続ストレージ領域内の前記選択されたユーザ識別子に関連するアクセス・コントロール・データを調べることにより、前記選択されたユーザ識別子に関連するユーザが前記選択されたサービスへのアクセスを許可されていることを、前記選択されたサービスに関連するサービス・ホスト・コンピュータにおいてベリファイするためのコンピュータ・プログラミング命令と、

前記サービス・ホスト・コンピュータ上の1つ以上のマネジメント・ファイルをアドミニストレーション・サーバへ転送し、これによって、前記サービス・マネージャを使用したマネジメント・ファイルの操作を促進するためのコンピュータ・プログラミング命令を含むコンピュータ読み取り可能媒体。

【請求項16】 前記選択されたユーザ識別子及び対応するプライベート・キーワードを提供するためのコンピュータ・プログラミング命令、前記アドミニストレーション・クライアント・コンピュータを通じて前記サービス・マネージャへログオンするするためのコンピュータ・プログラミング命令を更に含む請求項15に記載のコンピュータ読み取り可能媒体。

【請求項17】 前記ユーザを認証するためのコンピュータ・プログラミング命令は、前記ユーザ識別子及び対応するプライベート・キーワードを前記永続ストレージ領域へ伝達するために、ライトウェイト・ディレクトリ・アクセス・プロトコルを使用するためのコンピュータ・プログラミング命令を含む請求項15または請求項16に記載の方法。

【請求項18】 前記サービスのリストを導出するためのコンピュータ・プログラミング命令は、前記永続ストレージ領域を検索するためのコンピュータ・プログラミング命令を更に含み、前記永続ストレージ領域はユーザ・プロフィール・データベースを有し、前記ユーザ・プロフィール・データベースはユーザ・アクセス・レベル、許可可能なサービスのリスト及びパスワードをユーザ毎に含む請求項15から請求項17のいずれかに記載の方法。

【請求項19】 前記選択されたユーザ識別子に関連するユーザが前記サービスのリストから選択されたサービスへのアクセスを許可されていることを、前記サービス・ホスト・コンピュータにおいてベリファイするためのコンピュータ・プログラミング命令は、コモン・ゲートウェイ・インターフェースを使用することによって、前記選択されたユーザ識別子及び対応するプライベート・キーワードをホスト・サーバ・コンピュータへ伝達するためのコンピュータ・プログラミング命令を更に含む請求項15から請求項18のいずれかに記載の方法。

【請求項20】 前記サービスのリストを、前記アドミニストレーション・クライアント・コンピュータ上に表示されたユーザ・インターフェース内で表示するためのコンピュータ・プログラミング命令を更に含む請求項15に記載の方法。

【請求項21】 ホスト・サーバ・コンピュータ上のサービスの位置を決定するため

に、前記マネジメント・コンソール・プログラムによってサービス・ロケータを作成するためのコンピュータ・プログラミング命令を更に含む請求項 15 に記載の方法。

【請求項 22】 前記ホスト・サーバ上の 1 つ以上のマネジメント・ファイルをアドミニストレーション・サーバへ転送するためのコンピュータ・プログラミング命令は、前記アドミニストレーション・サーバ・コンピュータ上のコモン・ゲートウェイ・インターフェースを開始し、これによって、前記 1 つ以上のマネジメント・ファイル及び複数のオペレーティング・システム・コマンドの転送を可能にするためのコンピュータ・プログラミング命令を更に含む請求項 15 から請求項 19 のいずれかに記載の方法。