

【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 17 年 11 月 17 日 (2005.11.17)

【公開番号】特開 2005-149528 (P2005-149528A)
 【公開日】平成 17 年 6 月 9 日 (2005.6.9)
 【年通号数】公開・登録公報 2005-022
 【出願番号】特願 2004-378761 (P2004-378761)
 【国際特許分類第 7 版】

G 0 6 F 15/00

G 0 6 K 17/00

【F I】

G 0 6 F 15/00 3 3 0 B

G 0 6 F 15/00 3 3 0 G

G 0 6 K 17/00 T

【手続補正書】

【提出日】平成 17 年 10 月 3 日 (2005.10.3)

【手続補正 1】

【補正対象書類名】明細書

【補正対象項目名】発明の名称

【補正方法】変更

【補正の内容】

【発明の名称】可搬媒体を用いた認証方法

【手続補正 2】

【補正対象書類名】特許請求の範囲

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項 1】

可搬媒体を用いた認証方法であって、

第 1 のコンピュータが第 1 の認証情報を受付け、

前記第 1 の認証情報と可搬媒体とを用いて、前記第 1 のコンピュータで認証し、

前記認証に応じて、前記第 1 のコンピュータが、前記可搬媒体に格納された第 2 の認証情報を取得し、該第 2 の認証情報を用いて第 2 のコンピュータへの認証処理を行う

ことを特徴とする可搬媒体を用いた認証方法。

【請求項 2】

請求項 1 に記載の可搬媒体を用いた認証方法であって、

前記第 2 のコンピュータへの認証処理は、前記第 2 のコンピュータへのログイン処理である

ことを特徴とする可搬媒体を用いた認証方法。

【請求項 3】

請求項 1 に記載の可搬媒体を用いた認証方法であって、

前記第 2 のコンピュータは、第 1 のコンピュータに対し業務を提供するサーバであり、

前記サーバへの認証処理により認証された場合に、前記サーバが前記第 1 のコンピュータからの業務処理を受け付ける

ことを特徴とする可搬媒体を用いた認証方法。

【請求項 4】

請求項 3 に記載の可搬媒体を用いた認証方法であって、

前記可搬媒体が前記第1のコンピュータからはずされた場合に、業務処理が終了することを特徴とする可搬媒体を用いた認証方法。

【請求項5】

請求項3又は4に記載の可搬媒体を用いた認証方法であって、前記サーバへの認証処理は、前記サーバへのログイン処理であることを特徴とする可搬媒体を用いた認証方法。

【請求項6】

可搬媒体を用いた認証方法であって、第1のコンピュータが第1の認証情報を受付け、前記第1の認証情報と可搬媒体とを用いて、前記第1のコンピュータで認証し、前記認証に応じて、前記第1のコンピュータが、前記可搬媒体に格納された第2の認証情報を取得し、該第2の認証情報を用いて第2のコンピュータの、オペレーティングシステム又はアプリケーションの少なくとも1への認証処理を行うことを特徴とする可搬媒体を用いた認証方法。

【請求項7】

請求項6記載の可搬媒体を用いた認証方法であって、前記オペレーティングシステム又は前記アプリケーションの少なくとも1への認証処理により認証された場合に、前記オペレーティングシステム又は前記アプリケーションの少なくとも1が、前記第1のコンピュータからの処理要求を受け付けることを特徴とする可搬媒体を用いた認証方法。

【請求項8】

請求項7記載の可搬媒体を用いた認証方法であって、前記可搬媒体が前記第1のコンピュータからはずされた場合に、前記オペレーティングシステム又は前記アプリケーションの少なくとも1の、前記第1のコンピュータに対する処理が終了することを特徴とする可搬媒体を用いた認証方法。

【請求項9】

請求項7又は8に記載の可搬媒体を用いた認証方法であって、前記オペレーティングシステム又は前記アプリケーションの少なくとも1への前記認証処理は、前記オペレーティングシステム又は前記アプリケーションの少なくとも1へのログイン処理であることを特徴とする可搬媒体を用いた認証方法。

【請求項10】

請求項1乃至9のいずれか1に記載の可搬媒体を用いた認証方法であって、前記可搬媒体がICカードであることを特徴とする可搬媒体を用いた認証方法。

【請求項11】

請求項1乃至10のいずれか1に記載の可搬媒体を用いた認証方法であって、前記第1の認証情報が生物的な情報であることを特徴とする可搬媒体を用いた認証方法。

【請求項12】

請求項11に記載の可搬媒体を用いた認証方法であって、前記生物的な情報が指紋であることを特徴とする可搬媒体を用いた認証方法。

【請求項13】

請求項1乃至12のいずれか1に記載の可搬媒体を用いた認証方法であって、前記第2の認証情報が電子証明書であることを特徴とする可搬媒体を用いた認証方法。

【請求項14】

請求項1乃至13のいずれか1に記載の可搬媒体を用いた認証方法であって、前記第1の認証情報と前記可搬媒体とを用いた前記認証の処理が所定回数失敗した場合に、前記第2の認証情報を無効にすることを特徴とする可搬媒体を用いた認証方法。

【請求項15】

請求項1乃至13のいずれか1に記載の可搬媒体を用いた認証方法であって、前記第1の認証情報と前記可搬媒体とを用いた前記認証の処理が所定回数失敗した場合に、前記可搬媒体内の情報を使用不可能な状態にすることを特徴とする可搬媒体を用いた認証方法。

【手続補正3】

【補正対象書類名】明細書

【補正対象項目名】0011

【補正方法】変更

【補正の内容】

【0011】

本発明によれば、可搬媒体に格納された認証情報を利用した認証が実施可能となる。

【手続補正4】

【補正対象書類名】明細書

【補正対象項目名】0024

【補正方法】変更

【補正の内容】

【0024】

認証クライアント22は、画面制御部7210、可搬媒体制御部7220、情報入出力制御部7230から構成される。画面制御部7210は、可搬媒体の利用時や申請時に必要な認証情報入力画面7211、可搬媒体発行申請画面7212及び可搬媒体再利用要求画面7213、ユーザの業務要求時に必要なユーザ認証画面7212などを管理する。また、可搬媒体制御部7220では、可搬媒体の無効化機能7221、可搬媒体の無効化解除機能7222、可搬媒体への情報書き込み機能7223、パスワード管理機能7224などを含む。情報入出力制御部7230は、ユーザからの入力情報の受け付け機能7231、生物的情報による認証装置701とのインタフェース7232、ユーザへの情報表示機能7233を備える。クライアントの中に、前記認証クライアント22と可搬媒体読み取り装置705がある。

本発明によれば、企業情報システムで可搬媒体を利用したシングルログインを実現できる。先願発明(特願平9-76954)で提案した強固なユーザ認証及びアクセス制御の基盤を利用し、さらに、クライアント側に可搬媒体利用の画面制御手段、生物学情報による認証手段を設けることによりユーザを厳密に認証できる。アクセス可否判定の結果、不当なユーザに対しては可搬媒体を無効にするので高度なセキュリティが保証されている。ユーザは可搬媒体を用いない従来の認証処理も利用できるが、可搬媒体の利用申請や無効となった可搬媒体を再度利用可能にする処理も可能である。可搬媒体の利用と業務を連携させれば、ユーザの業務運用の簡易化や特定の業務向けに運用のカスタマイズ化もできる。