(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4709992号
(P4709992)
(45)発行日　平成23年6月29日(2011.6.29)　(24)登録日　平成23年4月1日(2011.4.1)

(51)Int.Cl.　　F I
*G06F 21/20 (2006.01)*　　G06F 15/00 330E
*H04L 9/32 (2006.01)*　　H04L 9/00 673A

請求項の数 19　(全 24 頁)

(21)出願番号　特願2007-162408 (P2007-162408)
(22)出願日　平成19年6月20日 (2007.6.20)
(65)公開番号　特開2008-97575 (P2008-97575A)
(43)公開日　平成20年4月24日 (2008.4.24)
審査請求日　平成19年6月21日 (2007.6.21)
(31)優先権主張番号　11/581319
(32)優先日　平成18年10月16日 (2006.10.16)
(33)優先権主張国　米国 (US)

(73)特許権者　505205731
レノボ・シンガポール・プライベート・リミテッド
シンガポール　５５６７４１、ニュウテックパーク、＃０２－０１、ローロンチュアン　１５１
(73)特許権者　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国１０５０４　ニューヨーク州　アーモンク　ニュー　オーチャード　ロード

最終頁に続く

(54)【発明の名称】認証パスワードの格納方法、生成方法、ユーザの認証方法、およびコンピュータ

(57)【特許請求の範囲】
【請求項１】
ＡＳＣＩＩコードで構成されたウィンドウズ（登録商標）の認証パスワードをコンピュータが格納する方法であって、
前記コンピュータが乱数を生成するステップと、
前記ウィンドウズ（登録商標）のＧＩＮＡ（Graphic Identification and Authentication）が前記コンピュータに前記認証パスワードとユーザ・アカウントを受け取る機能を実現させるステップと、
前記ＧＩＮＡが前記コンピュータに、前記認証パスワードをＵＮＩＣＯＤＥデータに変換する機能を実現させるステップと、
前記コンピュータが前記ＵＮＩＣＯＤＥデータを前記乱数でソルティングするステップと、
前記ＧＩＮＡが前記コンピュータに、前記ソルティングしたＵＮＩＣＯＤＥデータがＵＮＩＣＯＤＥ文字に対応しないコード番号を含む場合に該コード番号を変更してＵＮＩＣＯＤＥ文字だけで構成されたＵＮＩＣＯＤＥデータを生成する機能を実現させるステップと、
前記コンピュータが前記ソルティングしたＵＮＩＣＯＤＥデータをハッシュするステップと、
前記コンピュータが前記ユーザ・アカウントと前記ハッシュしたＵＮＩＣＯＤＥデータを前記ウィンドウズ（登録商標）のＳＡＭ（Security Account Manager）データベースに

格納するステップと
を有する格納方法。
【請求項２】
前記ＵＮＩＣＯＤＥデータを生成する機能を実現させるステップが、前記ＧＩＮＡが前記コンピュータに、コード番号と該コード番号に対応する文字を含むマッピング用の変換テーブルを使用し、前記ソルティングしたＵＮＩＣＯＤＥデータの中に、前記変換テーブルに存在しない文字のコード番号が含まれる場合、前記ソルティングしたＵＮＩＣＯＤＥデータを前記変換テーブルに存在するコード番号のいずれかの文字に変換する機能を実現させるステップを含む請求項１記載の格納方法。
【請求項３】
前記ＵＮＩＣＯＤＥデータを生成する機能を実現させるステップが、前記ＧＩＮＡが前記コンピュータに、前記変換テーブルに存在しない文字のコード番号を一ずつ増減して前記変換テーブルに存在するコード番号のいずれかの文字に変換する機能を実現させるステップを含む請求項２記載の格納方法。
【請求項４】
前記乱数が、リード／ライト保護された不揮発性メモリに格納される請求項１から請求項３のいずれかに記載の格納方法。
【請求項５】
前記乱数が、ＢＩＯＳだけがアクセス可能な不揮発性メモリに格納される請求項１から請求項３のいずれかに記載の格納方法。
【請求項６】
前記乱数を、ＴＰＭ（Trusted Platform Module）が生成する請求項１から請求項３のいずれかに記載の格納方法。
【請求項７】
ＡＳＣＩＩコードで構成された認証パスワードとユーザ・アカウントでユーザを認証するウィンドウズ（登録商標）が搭載されたコンピュータであって、
ユーザ・アカウントと前記認証パスワードを受け取る手段と、
前記認証パスワードをＵＮＩＣＯＤＥデータに変換する手段と、
前記ＵＮＩＣＯＤＥデータを乱数でソルティングする手段と、
前記ソルティングしたＵＮＩＣＯＤＥデータがＵＮＩＣＯＤＥ文字に対応しないコード番号を含む場合に該コード番号を変更してＵＮＩＣＯＤＥ文字だけで構成されたＵＮＩＣＯＤＥデータを生成する手段と、
前記ソルティングしたＵＮＩＣＯＤＥデータをハッシュする手段と、
前記ハッシュしたＵＮＩＣＯＤＥデータを前記ユーザ・アカウントに関連づけて格納する手段と
を有するコンピュータ。
【請求項８】
前記格納する手段が、前記ウィンドウズ（登録商標）のＳＡＭ（Security Account Manager）データベースを含んで構成されている請求項７記載のコンピュータ。
【請求項９】
前記ＵＮＩＣＯＥデータを生成する手段が、前記ウィンドウズ（登録商標）のＧＩＮＡ（Graphic Identification and Authentication）を含んで構成されている請求項７または請求項８に記載のコンピュータ。
【請求項１０】
ＡＳＣＩＩコードで構成されたウィンドウズ（登録商標）の認証パスワードをコンピュータが格納する方法であって、
前記コンピュータが乱数を生成するステップと、
前記コンピュータが前記認証パスワードとユーザ・アカウントを受け取るステップと、
前記コンピュータが前記認証パスワードをＵＮＩＣＯＤＥデータに変換するステップと、

前記コンピュータが前記ＵＮＩＣＯＤＥデータを前記乱数でソルティングするステップと、
前記コンピュータが、前記ソルティングしたＵＮＩＣＯＤＥデータがＵＮＩＣＯＤＥ文字に対応しないコード番号を含む場合に該コード番号を変更してＵＮＩＣＯＤＥ文字だけで構成されたＵＮＩＣＯＤＥデータを生成するステップと、
前記コンピュータが前記ソルティングしたＵＮＩＣＯＤＥデータをハッシュするステップと、
前記コンピュータが前記ユーザ・アカウントと前記ハッシュしたＵＮＩＣＯＤＥデータを前記コンピュータのデータベースに格納するステップと
を有する格納方法。

【請求項１１】
前記ＵＮＩＣＯＤＥデータに変換するステップと前記ソルティングするステップがＴＰＭ（Trusted Platform Module）の内部で行われる請求項１０記載の格納方法。

【請求項１２】
前記ＵＮＩＣＯＤＥデータに変換するステップと前記ソルティングするステップをＢＩＯＳが前記コンピュータに実現させる請求項１０に記載の格納方法。

【請求項１３】
ウィンドウズ（登録商標）が動作するコンピュータに入力されたユーザ・アカウントとＡＳＣＩＩコードで構成された認証パスワードにより前記コンピュータが複数のユーザを認証する方法であって、
前記コンピュータが各ユーザのユーザ・アカウントに対応した乱数の一覧を記憶するステップと、
前記コンピュータが前記ウィンドウズ（登録商標）のＳＡＭ（Security Account Manager）データベースに前記ユーザの認証パスワードに関連するデータを記憶するステップと、
前記ウィンドウズ（登録商標）のＧＩＮＡ（Graphic Identification and Authentication）が前記コンピュータに前記ユーザ・アカウントと前記認証パスワードを受け取る機能を実現させるステップと、
前記コンピュータが、前記受け取ったユーザ・アカウントに対応した乱数を前記乱数の一覧から獲得し、前記受け取った認証パスワードを前記獲得した乱数でソルティングしたＵＮＩＣＯＤＥデータに変換するステップと、
前記ＧＩＮＡが前記コンピュータに、前記ソルティングしたＵＮＩＣＯＤＥデータがＵＮＩＣＯＤＥ文字に対応しないコード番号を含む場合に該コード番号を変更してＵＮＩＣＯＤＥ文字だけで構成されたＵＮＩＣＯＤＥデータを生成する機能を実現させるステップと、
前記コンピュータが前記ソルティングしたＵＮＩＣＯＤＥデータをハッシュするステップと、
前記ウィンドウズ（登録商標）の認証パッケージが前記コンピュータに、前記ハッシュしたＵＮＩＣＯＤＥデータを前記ＳＡＭデータベースに格納された前記ユーザの認証パスワードに関連するデータと比較する機能を実現させるステップと
を有する認証方法。

【請求項１４】
ユーザ・アカウントとＡＳＣＩＩコードで構成された認証パスワードで複数のユーザを認証するウィンドウズ（登録商標）が搭載されたコンピュータであって、
各ユーザ・アカウントに対応した乱数の一覧を格納する手段と、
各ユーザ・アカウントに対応した前記認証パスワードに関連するデータを格納する手段と、
ユーザ・アカウントと認証パスワードを受け取る手段と、
前記受け取ったユーザ・アカウントに対応した乱数を前記乱数の一覧から獲得し、前記受け取った認証パスワードを前記獲得した乱数でソルティングしたＵＮＩＣＯＤＥデータ

に変換する手段と、
前記ソルティングしたＵＮＩＣＯＤＥデータがＵＮＩＣＯＤＥ文字に含まれないコード番号を含む場合に該コード番号を変更してＵＮＩＣＯＤＥ文字だけで構成されたＵＮＩＣＯＤＥデータを生成する手段と、
前記ソルティングしたＵＮＩＣＯＤＥデータをハッシュする手段と、
前記ハッシュしたＵＮＩＣＯＤＥデータと前記認証パスワードに関連するデータを格納する手段に格納された前記認証パスワードに関連するデータを比較する手段と
を有するコンピュータ。
【請求項１５】
前記認証パスワードに関連するデータを格納する手段が、ウィンドウズ（登録商標）のＳＡＭ（Security Account Manager）データベースを含む請求項１４記載のコンピュータ。
【請求項１６】
前記ＵＮＩＣＯＤＥデータを生成する手段が、前記ウィンドウズ（登録商標）のＧＩＮＡ（Graphic Identification and Authentication）を含む請求項１４記載のコンピュータ。
【請求項１７】
ウィンドウズ（登録商標）が動作するコンピュータに入力されたユーザ・アカウントとＡＳＣＩＩコードで構成された認証パスワードにより前記コンピュータが複数のユーザを認証する方法であって、
前記コンピュータが各ユーザのユーザ・アカウントに対応した乱数の一覧を記憶するステップと、
前記コンピュータが前記ウィンドウズ（登録商標）のＳＡＭ（Security Account Manager）データベースに前記ユーザの認証パスワードに関連するデータを記憶するステップと、
前記コンピュータが前記ユーザ・アカウントと前記認証パスワードを受け取るステップと、
前記コンピュータが前記受け取った認証パスワードをＵＮＩＣＯＤＥデータに変換するステップと、
前記コンピュータが前記受け取ったユーザ・アカウントに対応した乱数を前記乱数の一覧から獲得するステップと、
前記コンピュータが前記ＵＮＩＣＯＤＥデータを前記獲得した乱数でソルティングするステップと、
前記コンピュータが、前記ソルティングしたＵＮＩＣＯＤデータがＵＮＩＣＯＤＥ文字に対応しないコード番号を含む場合に該コード番号を変更してＵＮＩＣＯＤＥ文字だけで構成されたＵＮＩＣＯＤＥデータを生成するステップと、
前記コンピュータが前記ソルティングしたＵＮＩＣＯＤＥデータをハッシュするステップと、
前記コンピュータが、前記ハッシュしたＵＮＩＣＯＤＥデータを前記ＳＡＭデータベースに格納された前記ユーザの認証パスワードに関連するデータと比較するステップと
を有する認証方法。
【請求項１８】
ウィンドウズ（登録商標）で動作するコンピュータに前記ウィンドウズ（登録商標）の認証パスワードを格納するための格納データを前記コンピュータが生成する方法であって、
前記コンピュータがユーザ・アカウントとＡＳＣＩＩコードで生成された認証パスワードを受け取るステップと、
前記コンピュータが乱数を生成するステップと、
前記コンピュータが前記認証パスワードをＵＮＩＣＯＤＥデータに変換するステップと、

前記コンピュータが前記認証パスワードを前記乱数でソルティングしてＵＮＩＣＯＤＥデータに変換するステップと、
前記コンピュータが前記ソルティングしたＵＮＩＣＯＤＥデータがＵＮＩＣＯＤＥ文字に対応しないコード番号を含む場合に該コード番号を変更してＵＮＩＣＯＤＥ文字だけで構成されたＵＮＩＣＯＤＥデータを生成するステップと、
前記コンピュータが前記ソルティングしたＵＮＩＣＯＤＥデータをハッシュするステップと
を有する格納データの生成方法。
【請求項１９】
前記ウィンドウズ（登録商標）がＮＴ、２０００、ＸＰのいずれかである請求項１８記載の生成方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ウィンドウズ（登録商標）が動作するコンピュータに格納された認証パスワードに対する攻撃への防御を強化する技術に関し、さらには、ウィンドウズ（登録商標）の基本モジュールに変更を加えないで防御を強化する技術に関する。
【背景技術】
【０００２】
パーソナル・コンピュータ（以下ＰＣという）においては、米国マイクロソフト社のウィンドウズ（登録商標）ＮＴ／２０００／ＸＰなどのようにマルチユーザに対応したオペレーティング・システム（以後ＯＳという）が一般的に使われている。ＰＣの電源を入れ、ＢＩＯＳ（Basic Input/Output System）による各デバイスの初期化の後にＯＳが起動すると、ユーザが認証情報であるユーザ・アカウント（以後ユーザＩＤという。）および認証パスワードを入力してＯＳにログオンする。
【０００３】
図１４は、ウィンドウズ（登録商標）における従来のユーザのログオンの仕組みを示す概念図である。ウィンドウズ（登録商標）が起動すると、ウィンドウズ（登録商標）で通常作業を行なっている時に表示される画面であるアプリケーション・デスクトップ１００１、スクリーン・セーバーを表示するスクリーン・セーバー・デスクトップ１００３、ログオン画面の表示を行うＷｉｎＬｏｇｏｎデスクトップ１００５の３つのデスクトップ画面が作成される。ディスプレイに表示されるデスクトップ画面は常にそのうちの一つだけである。ＷｉｎＬｏｇｏｎ１００５は、ウィンドウズ（登録商標）の中でログオン・セッションの管理、およびディスプレイに表示するデスクトップ画面の切り替えなどを行うコンポーネントである。
【０００４】
ウィンドウズ（登録商標）が起動されたときに表示されるユーザＩＤおよびパスワードの入力を要求する画面は、ＷｉｎＬｏｇｏｎデスクトップ１００５である。ユーザＩＤおよびパスワードの入力のダイアログを表示するのはウィンドウズ（登録商標）のＧＩＮＡ（Graphic Identification and Authentication）１００９と呼ばれるコンポーネントである。ＧＩＮＡによって表示されたダイアログ１０１１に対して、ユーザがユーザＩＤおよび認証パスワードを入力すると、入力されたユーザＩＤおよび認証パスワードはＧＩＮＡ１００９からＬＳＡ（Local Security Authority、ローカル セキュリティ認証）１０１３と呼ばれるコンポーネントに渡される。ＬＳＡは、ローカル コンピュータ上のユーザのログオンおよび認証を処理するエージェントとして機能する。その際、ＧＩＮＡ１００９からＬＳＡ１０１３にユーザＩＤおよび認証パスワードを渡すために、LogonUserおよびLsaLogonUserという２通りのＡＰＩ（Application Program Interface）が使用できる。LogonUserは、ＡＳＣＩＩコードで記述された半角英数文字のユーザＩＤおよび認証パスワードのみ入力が可能であるのに対して、LsaLogonUserはＵＮＩＣＯＤＥで記述されたユーザＩＤおよび認証パスワードのみ入力が可能である。通常はLogonUserの方が使用

され、ユーザは半角英数文字のユーザＩＤおよび認証パスワードを入力する。

【０００５】

ＬＳＡ１０１３はパスワードをハッシュし、ユーザＩＤおよびハッシュされた認証パスワードをＡＰ（Authentication Package、認証パッケージ）１０１５に渡す。ここでいう「ハッシュする」とは、暗号技術的ハッシュ関数（cryptographic hash function）と呼ばれる一方向性関数によって、データを変換することをいう。ＳＡＭ（Security Account Manager）１０１７と呼ばれるコンポーネントは、ユーザ・アカウント・データベース１０１９を維持する。このデータベースの中には、ユーザＩＤおよびハッシュされたパスワードが格納される。ＡＰ１０１５は、ＬＳＡ１０１３から受け取ったユーザＩＤおよび認証パスワードをデータベース１０１９の中から検索し、当該ユーザＩＤおよび認証パスワードを入力したユーザが正当なユーザであるかどうかを認証する。認証が成功すれば、ＷｉｎＬｏｇｏｎ１００７はディスプレイに表示されるデスクトップ画面をアプリケーション・デスクトップ１００１に切り替える。なお、ユーザ・アカウント・データベースは、ウィンドウズ（登録商標）が起動していない時にはウィンドウズ（登録商標）のシステム・ファイルとして磁気ディスクに保存され、ウィンドウズ（登録商標）が起動するとレジストリの中にコピーされて使用される。

【０００６】

以上で示したユーザ認証の仕組みは、ウィンドウズ（登録商標）の標準的な仕様として定められ、さらに開発者向けにユーザ認証をカスタマイズする仕組みが公開されている。サード・パーティがウィンドウズ（登録商標）のユーザ認証をカスタマイズする必要がある場合、独自のＧＩＮＡを作成してウィンドウズ（登録商標）のコンポーネントとして登録することが普通である。独自のＧＩＮＡを作成し、該ＧＩＮＡからＬＳＡにユーザＩＤおよび認証パスワードを渡すことにより、ユーザ認証にかかるそれ以外のコンポーネントを変更することなく、カスタマイズされた独自のユーザ認証を実現することができる。他にも、ユーザ認証の仕組みをサード・パーティで作成するために独自のＡＰを作成する方法も開発者向けに公開されているが、ＧＩＮＡを作成するのに比べて多大な手間がかかるため、この方法が実際の製品で使われることは少ない。

【０００７】

なお、ウィンドウズ（登録商標）のユーザ認証に関する技術として、以下のような文献がある。特許文献１は米国マイクロソフト社による出願であり、ユーザ認証情報（クレデンシャル）を、サーバ上のそれと同期させる技術を開示する。特許文献２は、ＤＯＳネットワーク・ロギング・セッションによってユーザがログオンした後、カスタム・ビルト・ログイン・スクリーンによってログオン画面を置換する技術を開示する。

【特許文献１】特開２００５－３０３９９３号公報

【特許文献２】特開２０００－４７９８３号公報

【発明の開示】

【発明が解決しようとする課題】

【０００８】

前述のように、ウィンドウズ（登録商標）にログオンしようとするユーザは、ＡＳＣＩＩコードで記述された半角英数文字のユーザＩＤおよび認証パスワードを入力することが普通である。パスワードは、各々のユーザのみが覚えることができ、他のユーザには入力できない文字列であることが望ましい。しかし、通常は意味のある英単語や数字などを組み合わせたパスワードが使われることが多い。そのため、従来のユーザＩＤおよび認証パスワードは辞書攻撃を受けやすい。辞書攻撃は、パスワードの割り出しや暗号の解読に最もよく使われる攻撃手法の一つであり、辞書にある単語に数字などを任意に組み合わせて生成したパスワードを片っ端から入力して試行するものである。１文字ずつ組み合わせて認証パスワードを生成するのに比べて、辞書を利用して単語を組み合わせてパスワードを生成すれば、試行する回数が少なくて済むのでより短時間でパスワードを割り出すことができる。そのためのアルゴリズムやツール、および単語が使用頻度順に並べ替えられた辞書などは、インターネットなどを通じて簡単に入手できる。

【０００９】
図１５は、ユーザ・アカウント・データベース１０１９に対する辞書攻撃の方法を示す概念図である。ウィンドウズ（登録商標）が起動していない時にはユーザ・アカウント・データベース１０１９は、システム・ファイルの中の一つとして保存されている。しかも、そのファイル名および磁気ディスク内の位置は公開されている。そのため当該コンピュータで、たとえばＬｉｎｕｘ（登録商標）などのような別のＯＳをインストールしたり、フロッピー（登録商標）・ディスクや光学ディスクなどから起動したりするなどして、当該認証パスワードを認証するウィンドウズ（登録商標）とは別のＯＳを起動することにより、データベース１０１９のファイルをコピーすることができる。このデータベース１０１９は、暗号化されていないユーザＩＤ１１０９およびハッシュされた認証パスワード１１１１を含み、しかもそのデータ構造は開発者向けに公開されている。さらに、認証パスワードをハッシュするハッシュ関数１１０７（たとえばＬＭハッシュ、ＮＴハッシュなど)の仕様も開発者向けに公開されている。

【００１０】
インターネット上などで公開されている辞書攻撃によるパスワード割り出しツール１１０１は、やはりインターネット上などで公開されている辞書１１０３からアトランダムにピックアップした単語を組み合わせて、多くのパスワード１１０５を生成する。そして生成されたパスワード１１０５を、既知のハッシュ関数１１０７によって片っ端からハッシュし、データベース１０１９に含まれるパスワード１１１１と一致するかどうかを調べる。このようにして、コピーされたデータベース１０１９のファイルから、辞書攻撃によってパスワードを割り出すことが容易にできてしまう。

【００１１】
パスワードを辞書攻撃によって割り出されにくくするために、辞書に掲載されているような意味のある単語を認証パスワードとして使用しないこと、記号や数字などをランダムに組み合わせた文字列を認証パスワードとして使うこと、認証パスワードの文字数を長くすること、認証パスワードを定期的に変更することなどのような対策が推奨されている。しかし、そのような認証パスワードは人間にとって覚えにくく、利便性に欠ける。ユーザがウィンドウズ（登録商標）にログオンする際に入力する認証パスワードは、利便性の面からＡＳＣＩＩコードで記述された半角英数文字で意味のある単語を組み合わせて構成する傾向がある。その一方で、パスワードに替わるユーザの認証方法として、たとえば指紋、静脈、虹彩などのような生体情報、あるいはスマート・カードやトークンなどのような媒体に保存された電子情報が使われることも多くなっている。しかし、それらの生体情報および電子情報を利用した認証には、専用の入力装置などが必要であり、その分がコストに反映されたＰＣは高価になる。

【００１２】
また、マイクロソフト社自身はこの問題に対する解決法として、システム・キー・ユーティリティ（Syskey）と呼ばれる、ウィンドウズ（登録商標）が動作していない間にユーザ・アカウント・データベースを暗号化して保存する機能を提供している。暗号化された該データベースから、ユーザＩＤおよびハッシュされた認証パスワードなどを取得することは困難である。該データベースを暗号化するための鍵は、文字列による認証パスワード、もしくはフロッピー（登録商標）・ディスクなどの記憶媒体として保存し、ウィンドウズ（登録商標）の起動時に入力することができる。しかし、この方法ではＰＣ１台に対して当該鍵が１つしか提供されない。このため、特にマルチユーザでウィンドウズ（登録商標）を使用する場合には、鍵であるパスワードもしくは記憶媒体をユーザ間で共有する必要があるので、不便である。

【００１３】
そこで本発明の目的は、コンピュータにＡＳＣＩＩコードで入力されて格納されるウィンドウズ（登録商標）の認証パスワードに対する攻撃への防御を強化した認証パスワードの格納方法および認証方法を提供することにある。さらに本発明の目的は、そのような格納方法または認証方法を実現するコンピュータを提供することにある。さらに本発明の目

的は、ウィンドウズ（登録商標）の認証パスワードを格納するための格納データをコンピュータが生成する方法を提供することにある。

【課題を解決するための手段】

【００１４】

本発明の第１の態様は、ＡＳＣＩＩコードで構成されたウィンドウズ（登録商標）の認証パスワードをコンピュータが格納する方法を提供する。ウィンドウズ（登録商標）のＧＩＮＡがＡＳＣＩＩコードで構成された認証パスワードを受け取り、受け取った認証パスワードを乱数でソルティングされたＵＮＩＣＯＤＥデータに変換する。ＵＮＩＣＯＤＥデータはさらにウィンドウズ（登録商標）のＬＳＡ（Local Security Authority）によりハッシュされて、ＳＡＭ（Security Account Manager）が維持するユーザ・アカウント・データベースに格納される。その結果従来のＡＳＣＩＩコードをハッシュしてユーザ・アカウント・データベースに格納するよりも、ハッシュする前にＵＮＩＣＯＤＥデータに変換してバイト数を増大させた部分と、システムにユニークなユーザごとの乱数でソルティングした部分により、辞書攻撃に対する防御を強化することができる。

【００１５】

ＧＩＮＡはＵＮＩＣＯＤＥデータを生成する際に、ＡＳＣＩＩコードを第１のＵＮＩＣＯＤＥデータに変換し、変換された第１のＵＮＩＣＯＤＥデータを乱数を利用してソルティングして第２のＵＮＩＣＯＤＥデータを生成する。ソルトとは、通常はＤＥＳ、ＭＤ５などのような暗号化に使われる関数で平文を暗号化する際に使われる補助的な情報のことをいう。しかしながらここでいうソルティングは、第１のＵＮＩＣＯＤＥを、乱数を使用して加工して同一桁数のデータを生成することをいう。ソルティングされた第１のＵＮＩＣＯＤＥデータは、第１のＵＮＩＣＯＤＥデータ以外のＵＮＩＣＯＤＥの文字だけで構成されたＵＮＩＣＯＤＥデータまたはＵＮＩＣＯＤＥに含まれない文字を含むデータになる。本発明においては、ＧＩＮＡはＵＮＩＣＯＤＥに含まれない文字を含むデータをＵＮＩＣＯＤＥデータに変換する機能も備えている。

【００１６】

ＧＩＮＡは、第１のＵＮＩＣＯＤＥデータをソルティングしたデータがＵＮＩＣＯＤＥに含まれない文字を含む場合は、コード番号とコード番号に対応する文字を含むマッピング用の変換テーブルを使用してＵＮＩＣＯＤＥの文字だけで構成された第２のＵＮＩＣＯＤＥデータに変換する。このとき、ソルティングしたデータに含まれる変換テーブル上に存在しない文字を、変換テーブルに存在するコード番号の最も近い文字に置き換えることもできる。これにより、ソルティングされた第１のＵＮＩＣＯＤＥデータは、すべてＵＮＩＣＯＤＥに実在する文字で構成された第２のＵＮＩＣＯＤＥデータになるので、ウィンドウズ（登録商標）が保証する範囲で認証パッケージに入力することができる。

【００１７】

ＵＮＩＣＯＤＥは全世界で使われる多くの言語を一つの体系にまとめた文字コードであるので、乱数でソルティングされたＵＮＩＣＯＤＥ形式の認証パスワードは、複数の言語の文字が混在したものとなり、辞書に掲載されている単語に等しい文字列が使われる可能性が極めて低くなる。そのため、ユーザ・アカウント・データベースを攻撃者に取得されても、辞書攻撃によって攻撃者に認証パスワードを割り出される危険性は低減される。ユーザにＵＮＩＣＯＤＥデータの認証パスワードを入力させる場合には、たとえば漢字などを使って意味のある文字列を構成する傾向になり、辞書攻撃に対する耐性が低下することが考えられるが、本発明では、ユーザが認証パスワードにＡＳＣＩＩコードを使用できるのでそのような問題がなく、また、ユーザが通常使い慣れている文字形式の認証パスワードを使用できるので利便性が低下することがない。なお、本発明における方法はＧＩＮＡをカスタマイズしたり追加したりすれば、認証パッケージ、ＳＡＭ、およびユーザ・アカウント・データベースなどの基本モジュールはそのまま利用して実施できる。もちろん専用の入力装置などは不要である。

【００１８】

認証パスワードのソルティングに使われる乱数は、ユーザが入力するユーザＩＤに関連

づけられ、リード／ライト保護された不揮発性メモリ、もしくはＢＩＯＳだけがアクセス可能な不揮発性メモリに格納される。さらに、ＴＰＭ（Trusted Platform Module）内部に乱数を格納することもできる。これらのことによって、格納された乱数が、ユーザ認証にかかるウィンドウズ（登録商標）とは違うＯＳなどから取得されにくくなるので、攻撃者にパスワードを割り出される危険性はさらに低減される。

【００１９】

本発明の第２の態様は、ＡＳＣＩＩコードで構成された認証パスワードとユーザ・アカウントをウィンドウズ（登録商標）に入力して複数のユーザを認証する方法を提供する。コンピュータにはm各ユーザのユーザ・アカウントに対応した乱数の一覧が格納されている。格納場所は第３者が容易にアクセスできないセキュアな記憶場所を選定することが望ましい。また、ウィンドウズ（登録商標）のＳＡＭ（Security Account Manager）が維持するユーザ・アカウント・データベースにユーザの認証パスワードに関連するデータが格納されている。認証パスワードに関連するデータとは、認証パスワードを暗号化したデータである。

【００２０】

ウィンドウズ（登録商標）のＧＩＮＡは、ユーザ・アカウントとＡＳＣＩＩコードで構成された認証パスワードを受け取る。ＧＩＮＡは受け取った認証パスワードをユーザ・アカウントに対応する乱数でソルティングされたＵＮＩＣＯＤＥデータに変換する。変換されたＵＮＩＣＯＤＥデータはＬＳＡによりハッシュされる。認証パッケージは、ハッシュされたＵＮＩＣＯＤＥデータを受け取り、ＳＡＭ（Security Account Manager）が維持するユーザ・アカウント・データベースに格納された当該ユーザの認証パスワードに関連するデータと比較することによってユーザ認証を行う。ユーザ・アカウント・データベースには、ＡＳＣＩＩコードから各ユーザのユーザ・アカウントに対応する乱数でソルティングされたＵＮＩＣＯＤＥデータがさらにハッシュされた認証パスワードに関連するデータが格納されている。

【００２１】

以上で述べてきた本発明の各々の態様における特徴は、ＡＳＣＩＩコードで構成された認証パスワードをソルティングされたＵＮＩＣＯＤＥデータへ変換する作業をすべてＧＩＮＡが行っている。本発明の他の態様では、ＧＩＮＡ以外のモジュールがＡＳＣＩＩコードで構成された認証パスワードをＵＮＩＣＯＤＥデータへ変換し、これをソルティングしたデータをＧＩＮＡに渡す。ソルティングされたデータがすべてＵＮＩＣＯＤＥの文字から構成されていれば、ＧＩＮＡはそのデータをＵＮＩＣＯＤＥデータとする。ソルティングされたデータにＵＮＩＣＯＤＥ以外の文字が含まれている場合は、ＵＮＩＣＯＤＥだけの文字で構成されたＵＮＩＣＯＤＥデータを生成する。ＵＮＩＣＯＤＥデータはハッシュされ、ユーザ・アカウント・データ・ベースに格納される。あらかじめハッシュされたＵＮＩＣＯＤＥデータが対応するユーザ・アカウントとともにユーザ・アカウント・データ・ベースに格納されている場合は、ＧＩＮＡからＡＳＣＩＩの認証パスワードが入力されたときに生成されたハッシュされたＵＮＩＣＯＤＥデータと、ユーザ・アカウント・データ・ベースに格納されたハッシュされたＵＮＩＣＯＤＥデータを比較して、ウィンドウズ（登録商標）の認証パッケージが認証処理を行うことができる。また、本発明の他の態様は、認証パスワードの格納方法およびユーザの認証方法を実現するコンピュータを提供する。さらに本発明の他の態様は、ウィンドウズ（登録商標）の認証パスワードを格納するための格納データをコンピュータが生成する方法を提供する。

【発明の効果】

【００２２】

本発明によって、コンピュータにＡＳＣＩＩコードで入力されて格納されるウィンドウズ（登録商標）の認証パスワードに対する攻撃への防御を強化した認証パスワードの格納方法および認証方法を提供することができた。さらに、そのような格納方法または認証方法を実現するコンピュータを提供することができた。さらに、ウィンドウズ（登録商標）の認証パスワードを格納するための格納データをコンピュータが生成する方法を提供する

ことができた。

【発明を実施するための最良の形態】

【００２３】

図１は、本発明の第１の実施の形態にかかるＰＣ１０のシステム構成を示す概略ブロック図である。ＰＣ１０の筐体内部には、図１に示す各種のデバイスが搭載されている。ＣＰＵ１１は、ＰＣ１０の中枢機能を担う演算処理装置で、ＯＳ、ＢＩＯＳ、デバイス・ドライバ、あるいはアプリケーション・プログラムなどを実行する。本実施の形態は、現時点においては、ウィンドウズ（登録商標）ＮＴ、２０００、ＸＰのいずれかに適用され、９８以前のウィンドウズ（登録商標）には適用されない。本実施の形態にかかるＣＰＵ１１は、ＳＭＩ（System Management Interrupt）入力ピン（ＳＭＩ＃）がアサートされることによって、システム管理用の動作モードであるＳＭＭ（System Management Mode）で動作することが可能である。ＳＭＭでは、特別に割り当てられたメモリ空間において、米国インテル社製のＣＰＵに存在する割り込み制御ハンドラであるＳＭＩハンドラが実行される。ＳＭＭは主にサスペンド、レジューム、電源管理およびセキュリティ関連の操作などに利用される特権実行モードである。

【００２４】

ＣＰＵ１１は、システム・バスとしてのＦＳＢ(Front Side Bus)１３、ＣＰＵ１１と周辺機器との間の通信を行うためのＰＣＩ(Peripheral Component Interconnect)バス１５、ＩＳＡバスに代わるインターフェイスであるＬＰＣ(Low Pin Count)バス１７という３段階のバスを介して各デバイスに接続されて信号の送受を行っている。ＦＳＢ１３とＰＣＩバス１５は、メモリ／ＰＣＩチップと呼ばれるＣＰＵブリッジ１９によって連絡されている。ＣＰＵブリッジ１９は、メイン・メモリ２１へのアクセス動作を制御するためのメモリ・コントローラ機能や、ＦＳＢ１３とＰＣＩバス１５との間のデータ転送速度の差を吸収するためのデータ・バッファ機能などを含んだ構成となっている。メイン・メモリ２１は、ＣＰＵ１１が実行するプログラムの読み込み領域、処理データを書き込む作業領域として利用される書き込み可能メモリである。同時にメイン・メモリ２１はＳＭＭで動作するＣＰＵ１１が独占的に使用できるＳＭＲＡＭ（System Management RAM）としての領域を含む。ビデオ・カード２３は、ビデオ・チップ（図示せず）およびＶＲＡＭ（図示せず）を有し、ＣＰＵ２１からの描画命令を受けて描画すべきイメージを生成しＶＲＡＭに書き込み、ＶＲＡＭから読み出されたイメージを描画データとしてディスプレイ２５に送る。

【００２５】

ＰＣＩバス１５には、Ｉ／Ｏブリッジ２７、ＣａｒｄＢｕｓコントローラ２９、ｍｉｎｉＰＣＩスロット３３、Ｅｔｈｅｒｎｅｔ（登録商標）コントローラ３５がそれぞれ接続されている。ＣａｒｄＢｕｓコントローラ２９は、ＰＣＩバス１５とＰＣカード（図示せず）とのデータ転送を制御するコントローラである。ＣａｒｄＢｕｓコントローラ２９にはＣａｒｄＢｕｓスロット３１が接続され、ＣａｒｄＢｕｓスロット３１にはＰＣカード（図示せず）が装着される。ｍｉｎｉＰＣＩスロット３３には、例えば無線ＬＡＮモジュールが内蔵されたｍｉｎｉＰＣＩカード（図示せず）が装着される。Ｅｔｈｅｒｎｅｔ（登録商標）コントローラ３５は、ＰＣ１０を有線ＬＡＮに接続するためのコントローラである。

【００２６】

Ｉ／Ｏブリッジ２７は、ＰＣＩバス１５とＬＰＣバス１７とのブリッジ機能を備えている。また、Ｉ／Ｏブリッジ２７は、ＩＤＥ(Integrated Device Electronics)インターフェイス機能を備えており、ハード・ディスク・ドライブ(ＨＤＤ)３９および光学ドライブ４１（ＣＤドライブ，ＤＶＤドライブ等）が接続される。また、Ｉ／Ｏブリッジ２７にはＵＳＢコネクタ３７が接続されている。ＵＳＢコネクタ３７にはＵＳＢに対応した各種周辺機器（図示せず）が接続される。ＬＰＣバス１７には、エンベデッド・コントローラ４３、ＢＩＯＳフラッシュＲＯＭ４７、ＴＰＭ（Trusted Platform Module）５７、Ｉ／Ｏコントローラ５１が接続されている。Ｉ／Ｏコントローラ５１にはＩ／Ｏコネクタ５３を

介してキーボード５５を初めとする入出力機器（図示せず）が接続されている。ＢＩＯＳフラッシュＲＯＭ４７およびＴＰＭ（Trusted Platform Module）５７については後述する。

【００２７】

エンベデッド・コントローラ４３は、８～１６ビットのＣＰＵ、ＲＯＭ、ＲＡＭなどで構成されたマイクロ・コンピュータであり、さらに複数チャネルのＡ／Ｄ入力端子、Ｄ／Ａ出力端子、およびデジタル入出力端子を備えている。エンベデッド・コントローラ４３には、それらの入出力端子を介して冷却ファン（図示せず）、温度センサ（図示せず）および電源装置４５などが接続されており、ＰＣ内部の動作環境の管理にかかるプログラムをＣＰＵ１１とは独立して動作させることができる。

【００２８】

なお、図１は本実施の形態を説明するために、本実施の形態に関連する主要なハードウェアの構成および接続関係を簡素化して記載したに過ぎないものである。ここまでの説明で言及した以外にも、ＰＣ１０を構成するには多くのデバイスが使われる。しかしそれらは当業者には周知であるので、ここでは詳しく言及しない。もちろん、図で記載した複数のブロックを１個の集積回路もしくは装置としたり、逆に１個のブロックを複数の集積回路もしくは装置に分割して構成したりすることも、当業者が任意に選択することができる範囲においては本発明の範囲に含まれる。

【００２９】

図２は、本発明の実施の形態にかかるＰＣ１０のセキュリティを強化するモジュールであるＴＰＭ（Trusted Platform Module）５７の内部構成を示す図である。ＴＰＭ５７は、ＴＣＧ（Trusted Computing Group）によって策定された仕様書に基づいて製造されてＰＣに搭載される。ＴＰＭ５７は、Ｉ／Ｏ１０１を介して、ＬＰＣバス１７とのデータの交換を行う。不揮発性ＲＡＭ１０３には、プラットフォームおよびユーザの認証に使用される鍵などが記憶され、本実施の形態では後述するソルト値データベースもここに記憶される。ＰＣＲ（Platform Configuration Resister）１０５は、プラットフォーム状態情報（ソフトウェアの計測値）を保持するレジスタである。ＡＩＫ（Attestation Identity Key、認証識別キー）１０７はプラットフォーム認証に利用され、ＴＰＭ５７内部のデータにデジタル署名を付加するために利用される。

【００３０】

プラットフォームおよびユーザの認証などに使用される各種プログラムは、ＲＯＭ１０９に記憶され、プロセッサおよび揮発性ＲＡＭを含む実行エンジン１１１で実行される。ＴＰＭ５７は他に、乱数を発生する乱数発生器１１３、暗号化に使われる一方向性関数である暗号技術的ハッシュ関数（cryptographic hash function）を実行するハッシュ関数エンジン１１５、暗号鍵生成器１１７で生成された暗号鍵に電子的に署名するＰＫＩエンジン１１９、意図されない場所でＰＣ１０が使われることを防止するＯｐｔ－Ｉｎ１２１も備える。本実施の形態では、後述するパスワード管理用プログラムもＲＯＭ１０９に記憶される。また、不揮発性ＲＡＭ１０３に記憶された内容は、実行エンジン１１１からのみ参照でき、ＣＰＵ１１から直接アクセスされることはない。

【００３１】

図３は、ＴＳＳ（TCG Software Stack）の概念図である。ＴＰＭ５７はハードウェアとしてＰＣ１０と関連づけられ、ＰＣ１０の中でハードウェア的に信頼できる環境を構築すると同時に、ドライバを介してアプリケーション・ソフトウェアからＴＰＭ５７の機能を使用することも可能である。アプリケーション・ソフトウェアがＴＰＭ５７を使用するためのソフトウェア・スタックとして、ＴＳＳがＴＣＧによって定義されている。ソフトウェア・アプリケーション層２０１、ソフトウェア・インフラストラクチャ（ミドルウェア）層２０３、ハードウェア層２０５という３つの階層を定義すると、ハードウェア層２０５に属するＴＰＭ５７は、ＢＩＯＳフラッシュＲＯＭ４７に記憶されてＰＣ１０の電源を入れると最初に起動するＢｏｏｔ　ＢＩＯＳ２０７から直接操作されることができる。また、やはりＢＩＯＳフラッシュＲＯＭ４７に記憶されてシステムの設定を行うＰＣ　ＢＩ

ＯＳ２０９から、ＴＰＭ／ＴＳＳ　ＢＩＯＳ　ＡＰＩ２１１を介して操作されることもできる。

【００３２】

ウィンドウズ（登録商標）に対しては、ソフトウェア・インフラストラクチャ層２０３に、ＴＰＭ５７に対応したデバイス・ドライバ２１３、デバイス・ドライバ２１３を利用するためのライブラリ２１５が提供される。同時に、デバイス・ドライバ２１３およびライブラリ２１５の上で動作するアプリケーションであり、インターネット・エクスプローラ（登録商標）およびＯｕｔｌｏｏｋ（登録商標）などのような一般的なアプリケーション・ソフトウェア２２９にユーザ認証、暗号化、電子証明書の保護などの機能を提供するクライアント・セキュリティ・ソリューション２１７も提供される。クライアント・セキュリティ・ソリューション２１７は、標準的なソフトウェア・スタックであるＴＳＳ２１９、ＴＰＭの設定などを行う管理ツール２２１、および暗号の標準ＡＰＩであるマイクロソフト社のＣｒｙｐｔｏ　ＡＰＩ２２３、ＲＳＡセキュリティ社のＰＫＣＳ＃１１　２２７、その他のＣＳＰ（Crypto Service Provider）２２７などが含まれる。アプリケーション・ソフトウェア２２９は、それらのＡＰＩを利用することにより、ユーザ認証および暗号化にかかる処理をＴＰＭ５７に渡して実行させることができる。もちろんこれらの処理はプラットフォームおよびユーザが正しく認証された状態で行われるので、ＰＣ１０で本来動作するウィンドウズ（登録商標）とは別のＯＳを起動しても、これらの処理を実行することはできない。

【００３３】

図４は、本実施の形態におけるユーザのログオンの仕組みを示す概念図である。ＰＣ１０の電源を投入すると、まずＢＩＯＳフラッシュＲＯＭ４７に記憶されたＢｏｏｔ　ＢＩＯＳ２０７およびＰＣ　ＢＩＯＳ２０９がＣＰＵ１１に読み出されて実行され、ＰＣ１０に搭載されたハードウェアのセルフテストおよび初期設定が行われる。その後でＨＤＤ３９にインストールされたウィンドウズ（登録商標）がＣＰＵ１１に読み出されて実行される。ウィンドウズ（登録商標）が起動されると、ウィンドウズ（登録商標）で通常作業を行なっている時に表示される画面であるアプリケーション・デスクトップ３０１、スクリーン・セーバーを表示するスクリーン・セーバー・デスクトップ３０３、およびログオン画面の表示を行うＷｉｎＬｏｇｏｎデスクトップ３０５の３つのデスクトップ画面が作成される。ＷｉｎＬｏｇｏｎ３０７は、それらの中からＷｉｎＬｏｇｏｎデスクトップ３０５をディスプレイ２５に表示する。

【００３４】

ＷｉｎＬｏｇｏｎデスクトップ３０５上には、ユーザＩＤおよび認証パスワード（以後、単にパスワードという。）の入力のダイアログ３０９がプライベートＧＩＮＡ３１１によって表示される。プライベートＧＩＮＡ３１１は、本実施の形態のためにカスタマイズされ、ウィンドウズ（登録商標）のコンポーネントとして登録されたＧＩＮＡである。ダイアログ３０９で、ユーザがキーボード５５を介してユーザＩＤおよびパスワードを入力すると、入力されたユーザＩＤおよびパスワードはプライベートＧＩＮＡ３１１から、ＴＳＳ２１９およびデバイス・ドライバ２１３を介してＴＰＭ５７内の実行エンジン１１１に渡される。実行エンジン１１１では、ＲＯＭ１０９から読み出されたパスワード管理用プログラムによって後述する処理が実行される。さらにプライベートＧＩＮＡ３１１は、ＡＳＣＩＩコードからＵＮＩＣＯＤＥへ文字列を変換するための変換テーブル３１６も備える。変換テーブル３１６は、ＵＮＩＣＯＤＥの文字配列テーブルを含む。

【００３５】

図５は、ＴＰＭ５７内の不揮発性ＲＡＭ１０３に記憶されたソルト値データベース３１５のデータ構成を示す図である。ユーザＩＤ３５１に対応するソルト値３５５が保存されている。図６は、本実施の形態におけるパスワードの登録時の動作を表すフローチャートである。あるユーザが正常にログオンしている状態で、パスワードの変更の処理が呼び出されると（ブロック４０１）、ＷｉｎＬｏｇｏｎ３０７がディスプレイ２５に表示する画面をＷｉｎＬｏｇｏｎデスクトップ３０５に切り替え、プライベートＧＩＮＡ３１１が該

デスクトップ画面上に、変更後のパスワードを入力するためのダイアログ３０９を表示する（ブロック４０３）。ユーザがダイアログ３０９に対して変更後のパスワードをＡＳＣＩＩコードである半角英数文字で入力すると（ブロック４０５）、プライベートＧＩＮＡ３１１はＴＰＭ５７を呼び出し、ログオン中のユーザのユーザＩＤをＴＰＭ５７に渡す（ブロック４０７）。

【００３６】

ユーザＩＤを受け取ったＴＰＭ５７は、ＴＰＭ５７内部のＲＯＭ１０９に記憶されたパスワード管理用プログラムを実行エンジン１１１に呼び出し（ブロック４０９）、乱数発生器１１３で乱数を生成し（ブロック４１１）、生成された乱数をソルト値とする。ユーザＩＤおよびそれに対応するソルト値が、ＴＰＭ５７内部の不揮発性ＲＡＭ１０３にソルト値データベース３１５として保存される（ブロック４１３）。ソルト値がプライベートＧＩＮＡ３１１に渡される。ここまでの段階で、パスワードはＡＳＣＩＩコードで記述された半角英数文字である。そこで、プライベートＧＩＮＡ３１１がパスワードをＵＮＩＣＯＤＥデータにフォーマット変換（ブロック４１５）する。ＵＮＩＣＯＤＥは２ないし４バイトで構成され、１バイトのＡＳＣＩＩコードに比べて桁数が多い分だけ辞書攻撃に対する耐性が強化されたことになる。さらにＵＮＩＣＯＤＥデータはＴＰＭ５７から渡されたソルト値を使用してソルティングされ、ＵＮＩＣＯＤＥ文字だけで構成されたパスワードが生成する（ブロック４１６）。ＵＮＩＣＯＤＥデータをソルティングしたデータは、必ずしもＵＮＩＣＯＤＥの文字だけで構成されるとは限らないので、これを全てＵＮＩＣＯＤＥの文字だけで構成されるように再フォーマット変換を行う（ブロック４１７）。フォーマット変換、ソルティング、および再フォーマット変換の手法は次に述べる。

【００３７】

図７は、本実施の形態におけるパスワードのソルティングについて示す概念図である。パスワードのソルティングは、パスワードとソルト値とを特定の関数に入力することによって行う。たとえば（入力パスワード）ＸＯＲ（ソルト値）＝（ソルティング済パスワード）などのような単純な論理関数を使用してもよい。ＸＯＲを使用する場合、ソルト値は入力パスワードと同じ桁数である必要がある。あるいは、暗号技術的ハッシュ関数などのような一方向性関数を使用してもよい。ＡＳＣＩＩコードで記述された半角英数文字によるパスワードをＵＮＩＣＯＤＥデータに変換すると、ビット数が倍になる。たとえばソルティングする前のパスワードを半角英数文字の「abc」とすると、この文字列はＡＳＣＩＩコードでは図７の（Ａ）に示すように「61 62 63」で表現されるのに対し、ＵＮＩＣＯＤＥでは図７の（Ｂ）に示すように「0061 0062 0063」と表現される。

【００３８】

図７の（Ｂ）に示したＵＮＩＣＯＤＥデータにフォーマット変換されたパスワードに対して、ＴＰＭ５７から渡された同じ桁数のソルト値を図７の（Ｃ）に示すようにたとえば「1234 5678 9ABC」とすると、（パスワード）ＸＯＲ（ソルト値）＝（ソルティング済パスワード）によって得られるソルティング済パスワードは図７の（Ｄ）に示すように「1255 561A 9ADF」となる。これを、変換テーブル３１６を利用してＵＮＩＣＯＤＥの文字配列（ＵＴＦ－１６）に当てはめると、「1255」「561A」「9ADF」はいずれもＵＮＩＣＯＤＥの文字配列に存在する文字となる。しかし、「1255」はエチオピア語の音節を表す文字（Ethiopic Syllable QHE)、「561A」および「9ADF」は主に中国語で使われる漢字（CJK Unified Ideographs）である。つまり、異なる言語の文字が混在する意味のない文字列となるので、特に辞書攻撃に使用される使用頻度順の辞書にはこのような文字列が載ることはない。従って、図７の（Ｄ）に示すようなソルティング済のパスワードを、辞書攻撃によって割り出すことは極めて困難である。

【００３９】

ソルティングされたＵＮＩＣＯＤＥデータの中に、変換テーブル３１６に含まれるＵＮＩＣＯＤＥの文字配列テーブルに存在しない文字が含まれたら、これを全てＵＮＩＣＯＤＥの文字配列テーブルに存在する文字だけで構成されるように再フォーマット変換を行う。具体的には、ＵＮＩＣＯＤＥの文字配列テーブルに存在しない文字のコード番号を一つ

ずつ増大させたり減少させたりして、ＵＮＩＣＯＤＥの文字配列テーブルに存在するいずれかのコード番号の文字で置き換える。たとえば、図７の（Ｅ）に示すように、コード番号「037F」に対応する文字はＵＮＩＣＯＤＥの文字配列テーブルの中には存在しないが、この場合はコード番号を一つずつ加算して、初めてＵＮＩＣＯＤＥの文字配列テーブルに存在する文字に該当したときのコード番号である「0384」（ギリシャ語のTONOSと呼ばれる記号）に置き換えることができる。これとは逆にコード番号を一つずつ減算してゆく方法や、加算方向および減算方向において文字配列テーブルに存在しない文字のコード番号に最も近い文字配列テーブル上のコード番号の文字に置き換える方法を採用してもよい。

【００４０】

図４および図６に戻って、ここまでの処理でユーザＩＤとソルティングされたＵＮＩＣＯＤＥデータとが、プライベートＧＩＮＡ３１１からLsaLogonUserを介してＬＳＡ３１７に渡される。LsaLogonUserが受け付けるパスワードはＵＮＩＣＯＤＥデータで記述されたものであることがマイクロソフト社の仕様によって定められているが、前述のようにＵＮＩＣＯＤＥデータがソルティングされたデータはすべてＵＮＩＣＯＤＥ上で実在する文字で構成されるので、問題なくＬＳＡ３１７に入力することができる。ＬＳＡ３１７は、ローカル コンピュータ上のユーザのパスワード変更処理を開始し（ブロック４１９）、ソルティングされたＵＮＩＣＯＤＥデータのパスワードをハッシュし、ユーザＩＤおよびハッシュされた変更後のパスワードをＡＰ３１９に渡す（ブロック４２１）。ＡＰ３１９は、ＬＳＡから受け取ったユーザＩＤおよび変更後のパスワードをＳＡＭ３２１を介してデータベース３２３に記録する（ブロック４２３）。変更後のパスワードの記録が完了すれば（ブロック４２５）、ＷｉｎＬｏｇｏｎ３０７はディスプレイ２５に表示されるデスクトップ画面をＷｉｎＬｏｇｏｎデスクトップ３０５からアプリケーション・デスクトップ画面３０１に切り替える。

【００４１】

図８は、本実施の形態におけるユーザの認証時の動作を表すフローチャートである。ＰＣ１０の電源を投入し（ブロック５０１）、ウィンドウズ（登録商標）が起動すると（ブロック５０３）、ＷｉｎＬｏｇｏｎ３０７がディスプレイ２５にＷｉｎＬｏｇｏｎデスクトップ３０５画面を表示し、プライベートＧＩＮＡ３１１が該デスクトップ画面上にユーザＩＤおよびパスワードの入力のダイアログ３０９を表示する（ブロック５０５）。ユーザがダイアログ３０９に対してユーザＩＤおよびパスワードをＡＳＣＩＩコードである半角英数文字で入力すると（ブロック５０７）、プライベートＧＩＮＡ３１１はＴＰＭ５７を呼び出し、入力されたユーザＩＤをＴＰＭ５７に渡す（ブロック５０９）。

【００４２】

ユーザＩＤを受け取ったＴＰＭ５７は、ＴＰＭ５７内部のＲＯＭ１０９に記憶されたパスワード管理用プログラムを実行エンジン１１１に呼び出し（ブロック５１１）、ソルト値データベース３１５から入力されたユーザＩＤに対応するソルト値を呼び出す（ブロック５１３）。呼び出されたソルト値はプライベートＧＩＮＡ３１１に渡される。そこで、プライベートＧＩＮＡ３１１がパスワードをＵＮＩＣＯＤＥデータにフォーマット変換し（ブロック５１５）、ＴＰＭ５７から渡されたソルト値を使用してソルティングし（ブロック５１６）、さらにソルティングされたデータを全てＵＮＩＣＯＤＥの文字だけで構成されるように再フォーマット変換を行う（ブロック５１７）。フォーマット変換、ソルティング、および再フォーマット変換の手法は、図６および図７で説明したパスワードの登録の場合と同一であるので、説明を省略する。

【００４３】

以上の処理で、ユーザＩＤとソルティングされたＵＮＩＣＯＤＥデータから生成されたＵＮＩＣＯＤＥのパスワードとが、プライベートＧＩＮＡ３１１からLsaLogonUserを介してＬＳＡ３１７に渡される。ＬＳＡは、ローカル コンピュータ上のユーザのパスワード変更処理を開始し（ブロック５１９）、パスワードをハッシュする。ユーザＩＤおよびハッシュされた変更後のパスワードは、ＬＳＡ３１７からＡＰ３１９に渡される（ブロック５２１）。ＡＰ３１９は、ＬＳＡから受け取ったユーザＩＤに対応するパスワードをＳＡ

Ｍ３２１を介してデータベース３２３の中から検索し、呼び出す（ブロック５２３）。ＡＰ３１９は、ＬＳＡから受け取ったパスワードと、データベース３２３から呼び出したパスワードとを比較し（ブロック５２５）、両者が一致すれば正当なユーザであると判断して、ユーザの認証を完了する（ブロック５２７）。ＷｉｎＬｏｇｏｎ３０７はディスプレイ２５に表示されるデスクトップ画面をＷｉｎＬｏｇｏｎデスクトップ３０５からアプリケーション・デスクトップ画面３０１に切り替える。ブロック５２５で比較されたパスワードが一致しなければ、ブロック５０７のユーザＩＤおよびパスワードの入力からやり直しとなる。

【００４４】

以上の説明からわかるように、本実施の形態ではウィンドウズ（登録商標）のユーザのログオンにかかる処理は、ＧＩＮＡをカスタマイズしてプライベートＧＩＮＡ３１１として構成する点を除いては変更されていない。また、ＴＰＭ５７を利用することにより、パスワードのソルティングに必要なソルト値を攻撃者に取得できないようにすることができる。そして、これによってデータベース３２３に記憶されるパスワードは、前述のように辞書攻撃によって割り出されにくいものとなる。もちろん、ユーザが入力するパスワードは、ＡＳＣＩＩコードで記述された半角英数文字による従来のもののままでよい。

【００４５】

図９は、本発明の第２の実施の形態にかかるＰＣ１０’のシステム構成を示す概略ブロック図である。ＰＣ１０’の構成は、第１の実施の形態にかかるＰＣ１０と比べて、相違点は１箇所だけである。それは、ＰＣ１０に装備されていたＴＰＭ５７が存在しておらず、ＰＣ１０になかったＮＶＲＡＭ４９がＬＰＣバス１７に接続されている点である。ＮＶＲＡＭ４９は、ＰＣ１０の電源を切っても消失しないようにバッテリーでバックアップされた不揮発性（Non-Volatile）ＲＡＭであるが、詳しくは後述する。この点以外のブロックについては、ＰＣ１０’の構成はＰＣ１０と同一であるので、参照番号も同一として、説明を省略する。

【００４６】

図１０は、本発明の第２の実施の形態でＢＩＯＳフラッシュＲＯＭ４７、ＮＶＲＡＭ４９、およびメイン・メモリ２１の内部構成について示す図である。図１０（Ａ）に示すＢＩＯＳフラッシュＲＯＭ４７は、不揮発性で記憶内容を電気的に書き替え可能なメモリであり、システムの起動および管理に使われる基本プログラムであるシステムＢＩＯＳ（SSO Shell Bios）６０１、電源および温度などの動作環境を管理するソフトウェアである各種ユーティリティ６０３、ＰＣ１０の起動時にハードウェアのテストを行うソフトウェアであるＰＯＳＴ（Power-On Self Test）６０５、本発明にかかるパスワード強化システム６０７、乱数を発生する乱数発生器６０９，ＣＰＵ１１をＳＭＭで動作させるＳＭＩハンドラ６１１、ＨＤＤ３９にアクセスするＩＮＴ１３Ｈハンドラ６１３などが記憶されている。乱数発生器６０９は、ソフトウェアとして実装されても、ハードウェアとして実装されてもよい。

【００４７】

図１０（Ｂ）に示すＮＶＲＡＭ４９は、ＰＣ１０の電源を切っても消失しないように電池でバックアップされたＲＡＭである。また、ＮＶＲＡＭ４９はリード／ライト保護が可能である。リード／ライト保護された状態では、ＮＶＲＡＭ４９は外部からの読み書きが不可能である。ＮＶＲＡＭ４９は、ＰＣ１０のデバイス・コントローラの設定情報６１５、および各ユーザのソルト値データ６１７を記憶している。設定情報６１５の内容としては、主にディスク装置の起動順序やドライブ番号、各周辺機器の接続方法やデータ転送に関するパラメータなどがある。ソルト値データ６１７は、図５で説明した第１の実施の形態と同じく、ユーザＩＤ３５１に対応するパスワード３５３、ソルト値３５５が保存されている。また、このソルト値データ６１７はシステムＢＩＯＳ６０１からのみアクセスが可能であり、ウィンドウズ（登録商標）およびその他のＯＳから記憶された内容を参照することは不可能である。ソルト値データ６１７の記憶域には、ユーザが入力したユーザＩＤとパスワード、および当該ユーザに対応するソルト値とを一時的に記憶する一時記憶域

６１８を含む。

【００４８】

図１０（Ｃ）に示すメイン・メモリ２１には、ＰＣシステムの通常の動作で使用されるユーザ領域６２１の他に、ＳＭＲＡＭ（System Management RAM）６１９としての領域が確保されている。システムＢＩＯＳ６０１からＳＭＩハンドラ６１１が呼び出されることによってＣＰＵ１１がＳＭＭに入ると、ＣＰＵ１１はシングル・タスクでの動作となり、すべての割り込みは無効とされる。さらに、ＳＭＲＡＭ領域６１９はＳＭＭで動作するＣＰＵ１１のみが独占的に使用可能となる。従って、ＣＰＵ１１がＳＭＭで動作している間、システムＢＩＯＳ６０１の制御下で動作している単一のタスク以外のプログラムが動作することもなく、また当該プログラム以外のプロセスからＳＭＲＡＭ領域６１９にアクセスされることもない。

【００４９】

図１１は、本実施の形態におけるユーザのログオンの仕組みを示す概念図である。ＰＣ１０の電源を投入すると、まずＢＩＯＳフラッシュＲＯＭ４７に記憶されたシステムＢＩＯＳ６０１がＣＰＵ１１に読み出されて実行され、ＰＣ１０に搭載されたハードウェアのセルフテストおよび初期設定が行われる。その後で、システムＢＩＯＳ６０１による制御のままで、ユーザＩＤおよびパスワードの入力のプロンプト７０１がパスワード強化システム６０７によって表示される。入力されたユーザＩＤ７０３およびパスワード７０５は、ソルト値データ６１７の記憶域の一時記憶域６１８に記憶される。さらに、該ユーザＩＤおよびパスワードに対して、後述する処理がパスワード強化システム６０７によって実行され、その結果として得られたソルト値７０７（詳細は後述）も一時記憶域６１８に記憶される。

【００５０】

システムＢＩＯＳ６０１による制御が完了したら、ＨＤＤ３９にインストールされたウィンドウズ（登録商標）がＣＰＵ１１に読み出されて実行される。ウィンドウズ（登録商標）が起動されると、ウィンドウズ（登録商標）で通常作業を行なっている時に表示される画面であるアプリケーション・デスクトップ３０１、スクリーン・セーバーを表示するスクリーン・セーバー・デスクトップ３０３、ログオン画面の表示を行うＷｉｎＬｏｇｏｎデスクトップ３０５、以上３つのデスクトップ画面が作成される。ＷｉｎＬｏｇｏｎ３０７は、それらの中からＷｉｎＬｏｇｏｎデスクトップ３０５をディスプレイ２５に表示する。ＷｉｎＬｏｇｏｎデスクトップ３０５上には、ログオン中の表示のダイアログ３０９’がプライベートＧＩＮＡ３１１’によって表示される。プライベートＧＩＮＡ３１１’は、本実施の形態のためにカスタマイズされ、ウィンドウズ（登録商標）のコンポーネントとして登録されたＧＩＮＡである。その間にプライベートＧＩＮＡ３１１’は、物理メモリレジスタ・ドライバ７０９を介して一時記憶域６１８に記憶されたユーザＩＤ、パスワードおよびソルト値を読み出し、ログオンにかかる以後の処理を行う。

【００５１】

物理メモリレジスタ・ドライバ７０９は、システムＢＩＯＳ６０１とウィンドウズ（登録商標）の間で情報交換を行うモジュールであり、ウィンドウズ（登録商標）のシステム・ファイル内にカーネルモード・ドライバとしてインストールされる。ウィンドウズ（登録商標）が管理しているメイン・メモリ２１の論理アドレスをシステムＢＩＯＳ６０１で解釈することは不可能であるが、物理メモリレジスタ・ドライバ７０９はメイン・メモリ２１上の特定の物理アドレスをキープし、ＳＭＩハンドラ６１１を呼び出し、Ｉ／Ｏ命令を使用してＣＰＵ１１のレジスタ経由でＳＭＩを発行することにより、ＣＰＵ１１のレジスタで指定される該物理アドレスをシステムＢＩＯＳ６０１に伝達することができる。制御を得たシステムＢＩＯＳ６０１は、伝達された該物理アドレスに、要求されたデータを格納してからＣＰＵ１１のＳＭＭでの動作を終了する。これによって、ウィンドウズ（登録商標）に当該データを渡すことができる。ここでいうメイン・メモリ２１の物理アドレスは、ＳＭＲＡＭ６１９領域内であっても、ユーザ領域６２１内であってもよい。なお、ここで説明した以外のブロックは、図４で説明した第１の実施の形態と同一であるので、

参照番号も同一とし、説明を省略する。

【００５２】

図１２は、本実施の形態におけるパスワードの登録時の動作を表すフローチャートである。あるユーザが正常にログオンしている状態で、パスワードの変更の処理が呼び出されると（ブロック８０１）、ＷｉｎＬｏｇｏｎ３０７がディスプレイ２５に表示する画面をＷｉｎＬｏｇｏｎデスクトップ３０５に切り替え、プライベートＧＩＮＡ３１１’が該デスクトップ画面上にユーザの変更後のパスワードの入力のダイアログ３０９を表示する（ブロック８０３）。ユーザがダイアログ３０９に対して変更後のパスワードを半角英数文字で入力すると（ブロック８０５）、プライベートＧＩＮＡ３１１’はＳＭＩハンドラ６１１を呼び出し、ＣＰＵ１１をＳＭＭで動作させる。ログオン中のユーザのユーザＩＤは、一時記憶域６１８に記憶される（ブロック８０７）。

【００５３】

ＳＭＭに入り、システムＢＩＯＳ６０１の制御で動作するＣＰＵ１１は、ＢＩＯＳフラッシュＲＯＭ４７に記憶されたパスワード強化システム６０７を呼び出す（ブロック８０９）。パスワード強化システム６０７は、ユーザＩＤをＳＭＲＡＭ６１９から受け取り、乱数発生器６０９で乱数を生成し（ブロック８１１）、生成された乱数をソルト値とする。ユーザＩＤおよびそれに対応するソルト値が、ＮＶＲＡＭ４９にソルト値データ６１７として保存される（ブロック８１３）。変更後のパスワードとソルト値は一時記憶域６１８に記憶され（ブロック８１４）、ＣＰＵ１１のＳＭＭでの動作は終了する。再びウィンドウズ（登録商標）の制御でプライベートＧＩＮＡ３１１’がパスワードをＵＮＩＣＯＤＥデータにフォーマット変換し（ブロック８１５）、物理メモリレジスタ・ドライバ７０９を介して一時記憶域６１８にソルト値を照会して受け取る（ブロック８１６）。そこで、プライベートＧＩＮＡ３１１が一時記憶域６１８に照会して受け取ったソルト値を使用してパスワードをソルティングし（ブロック８１７）、さらにソルティングされたデータを全てＵＮＩＣＯＤＥの文字だけで構成されるように再フォーマット変換を行う（ブロック８１８）。フォーマット変換、ソルティング、および再フォーマット変換の手法は、図６および図７で説明した説明した第１の実施の形態と同一であるので、説明を省略する。

【００５４】

以上の処理で、ユーザＩＤとソルティングされたＵＮＩＣＯＤＥデータから生成されたＵＮＩＣＯＤＥのパスワードとが、プライベートＧＩＮＡ３１１’からLsaLogonUserを介してＬＳＡ３１７に渡される。以後は図６で説明した第１の実施の形態と同様に、ＬＳＡ３１７は、ローカル コンピュータ上のユーザのパスワード変更処理を開始し（ブロック８１９）し、パスワードをハッシュし、ユーザＩＤおよびハッシュされた変更後のパスワードをＡＰ３１９に渡す（ブロック８２１）。ＡＰ３１９は、ＬＳＡから受け取ったユーザＩＤおよび変更後のパスワードをＳＡＭ３２１を介してデータベース３２３に記録する（ブロック８２３）。変更後のパスワードの記録が完了すれば（ブロック８２５）、ＷｉｎＬｏｇｏｎ３０７はディスプレイ２５に表示されるデスクトップ画面をＷｉｎＬｏｇｏｎデスクトップ３０５からアプリケーション・デスクトップ画面３０１に切り替える。

【００５５】

図１３は、本実施の形態におけるユーザの認証時の動作を表すフローチャートである。ＰＣ１０の電源を投入すると（ブロック９０１）、ウィンドウズ（登録商標）が起動される前にシステムＢＩＯＳ６０１の制御で、ＢＩＯＳフラッシュＲＯＭ４７に記憶されたパスワード強化システム６０７が実行され（ブロック９０３）、ユーザＩＤおよびパスワードの入力のプロンプト７０１が表示される（ブロック９０５）。ユーザがプロンプト７０１に対してユーザＩＤおよびパスワードを半角英数文字で入力すると（ブロック９０７）、パスワード強化システム６０７がソルト値データ６１７から入力されたユーザＩＤに対応するソルト値を呼び出す（ブロック９０９）。入力されたユーザＩＤ、パスワード、およびソルト値は、ソルト値データ６１７の記憶域の一時記憶域６１８に記憶される（ブロック９１１）。

【００５６】

ＨＤＤ３９にインストールされたウィンドウズ（登録商標）がＣＰＵ１１に読み出されて起動されると（ブロック９１３）、ＷｉｎＬｏｇｏｎ３０７がディスプレイ２５にＷｉｎＬｏｇｏｎデスクトップ３０５画面を表示し、プライベートＧＩＮＡ３１１’が該デスクトップ画面上にログオン中の表示のダイアログ３０９’を表示する（ブロック９１５）。その間にプライベートＧＩＮＡ３１１’は、物理メモリレジスタ・ドライバ７０９を介して一時記憶域６１８に記憶されたユーザＩＤ、パスワードおよびソルト値を照会して読み出す（ブロック９１６）。この段階でパスワードは、ＡＳＣＩＩコードで記述された半角英数文字である。ユーザＩＤ、パスワード、およびソルト値を受け取ったプライベートＧＩＮＡ３１１’は、パスワードをＵＮＩＣＯＤＥデータにフォーマット変換し（ブロック９１７）、さらに受け取ったソルト値を使用してＵＮＩＣＯＤＥデータをソルティングし（ブロック９１８）、さらにソルティングされたデータを全てＵＮＩＣＯＤＥの文字だけで構成されるように再フォーマット変換を行う（ブロック９１９）。フォーマット変換、ソルティング、および再フォーマット変換の手法は、図６および図７で説明した第１の実施の形態と同一であるので説明を省略する。

【００５７】

以上の処理で、ユーザＩＤとソルティングされたＵＮＩＣＯＤＥデータから生成されたＵＮＩＣＯＤＥのパスワードとが、プライベートＧＩＮＡ３１１’からLsaLogonUserを介してＡＰ３１９に渡される。ＬＳＡは、ローカル コンピュータ上のユーザのパスワード変更処理を開始し（ブロック９２１）、ソルティングされたＵＮＩＣＯＤＥのパスワードをハッシュし、ユーザＩＤおよびハッシュされた変更後のパスワードをＡＰ３１９に渡す（ブロック９２３）。ＡＰ３１９は、ＬＳＡから受け取ったユーザＩＤに対応するパスワードをＳＡＭ３２１を介してデータベース３２３の中から検索し、呼び出す（ブロック９２５）。ＡＰ３１９はＬＳＡから受け取ったパスワードと、データベース３２３から呼び出されたパスワードとを比較し（ブロック９２７）、両者が一致すれば正当なユーザであると判断して、ユーザの認証が正常に完了する（ブロック９２９）。ＷｉｎＬｏｇｏｎ３０７はディスプレイ２５に表示されるデスクトップ画面をＷｉｎＬｏｇｏｎデスクトップ３０５からアプリケーション・デスクトップ画面３０１に切り替える。ブロック５２５で比較されたパスワードが一致しなければ、ＰＣ１０は強制終了され（ブロック９３１）、ブロック９０１からやり直しとなる。

【００５８】

以上の説明からわかるように、本実施の形態では、ＰＣ１０’が一般的に備えるＢＩＯＳフラッシュＲＯＭ４７およびＮＶＲＡＭ４９を利用することにより、ＴＰＭ５７などのような特別なハードウェアを必要とせずに、パスワードのソルティングに必要なソルト値を攻撃者に取得できないようにすることができる。ソフトウェアについても、ウィンドウズ（登録商標）に対してＧＩＮＡをカスタマイズしてプライベートＧＩＮＡ３１１’として構成し、物理メモリレジスタ・ドライバ７０９をインストールすることを除いては変更する必要はない。もちろん、データベース３２３に記憶されるパスワードが辞書攻撃によって割り出されにくい点、そしてユーザが入力するパスワードは従来のままでよい点は、第１の実施の形態と同じである。

【００５９】

なお、ここまでで述べた第１および第２の実施の形態では、プライベートＧＩＮＡがＴＰＭもしくはＢＩＯＳからソルト値を受け取ってパスワードのＵＮＩＣＯＤＥデータへのフォーマット変換および変換されたＵＮＩＣＯＤＥデータのソルティング、およびソルティングされたＵＮＩＣＯＤＥデータからＵＮＩＣＯＤＥデータの生成を行っている。しかし、ＴＰＭ内部もしくはシステムＢＩＯＳ上での処理でパスワードをソルティングするステップまでを行って、プライベートＧＩＮＡがソルティングされたＵＮＩＣＯＤＥデータのパスワードを受け取り、それ以後の処理を行うという実施の形態も考えられる。そして、プライベートＧＩＮＡが、ソルティングされたＵＮＩＣＯＤＥデータがＵＮＩＣＯＤＥでない文字を含む場合には、図７で説明した方法でＵＮＩＣＯＤＥデータを生成する。

【００６０】

さらにＢＩＯＳからソルト値を受け取る第２の実施の形態では、パスワードをＰＣの起動直後に起動されるシステムＢＩＯＳによって表示されるプロンプトから入力するのではなく、第１の実施の形態と同様にウィンドウズ（登録商標）が起動してからプライベートＧＩＮＡによって表示されるダイアログから入力するという実施の形態も考えられる。さらに、システムＢＩＯＳによって表示されるプロンプトと、プライベートＧＩＮＡによって表示されるダイアログとで各々別個のパスワードを入力するという実施の形態も考えられる。

【００６１】

これまで本発明について図面に示した特定の実施の形態をもって説明してきたが、本発明は図面に示した実施の形態に限定されるものではなく、本発明の効果を奏する限り、これまで知られたいかなる構成であっても採用することができることは言うまでもないことである。

【産業上の利用可能性】

【００６２】

ウィンドウズ（登録商標）をＯＳとするコンピュータに対して利用可能である。

【図面の簡単な説明】

【００６３】

【図１】第１の実施の形態にかかるＰＣの概略ブロック図である。

【図２】ＴＰＭ（Trusted Platform Module）の内部構成を示す図である。

【図３】ＴＳＳ（TCG Software Stack）の概念図である。

【図４】第１の実施の形態におけるユーザのログオンの仕組みを示す概念図である。

【図５】ソルト値データベースのデータ構成を示す図である。

【図６】第１の形態におけるパスワードの登録時の動作を表すフローチャートである。

【図７】パスワードのソルティングについて示す概念図である。

【図８】第１の形態におけるユーザの認証時の動作を表すフローチャートである。

【図９】第２の実施の形態にかかるＰＣの概略ブロック図である。

【図１０】第２の実施の形態でＢＩＯＳフラッシュＲＯＭ、ＮＶＲＡＭ、およびメイン・メモリの内部構成について示す図である。

【図１１】第２の実施の形態におけるユーザのログオンの仕組みを示す概念図である。

【図１２】第２の形態におけるパスワードの登録時の動作を表すフローチャートである。

【図１３】第２の形態におけるユーザの認証時の動作を表すフローチャートである。

【図１４】従来のユーザのログオンの仕組みを示す概念図である。

【図１５】ユーザ・アカウント・データベースに対する辞書攻撃の方法を示す図である。

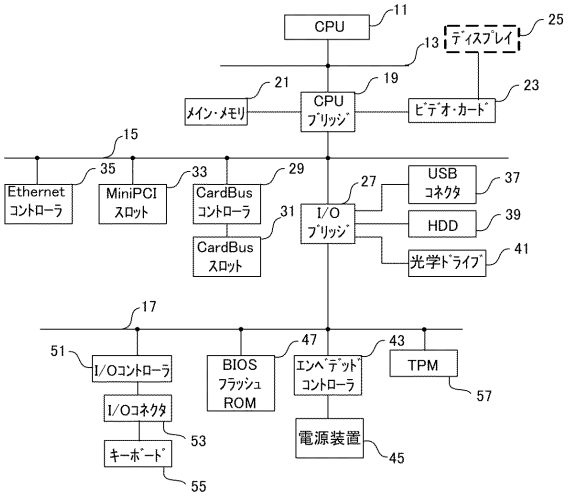
【符号の説明】

【００６４】

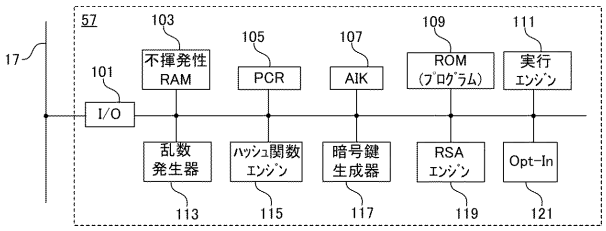
１０，１０’　ＰＣ
１１　ＣＰＵ
２１　メイン・メモリ
４７　ＢＩＯＳフラッシュＲＯＭ
４９　ＮＶＲＡＭ
５７　ＴＰＭ（Trusted Platform Module）
１０３　不揮発性ＲＡＭ（ＴＰＭ内）
１０９　ＲＯＭ（ＴＰＭ内）
１１１　実行エンジン（ＴＰＭ内）
１１３　乱数発生器（ＴＰＭ内）
３０５　ＷｉｎＬｏｇｏｎデスクトップ
３０７　ＷｉｎＬｏｇｏｎ
３１１，３１１’　プライベートＧＩＮＡ（Graphic Identification and Authentication）
３１５　ソルト値データベース

３１６　変換テーブル
３１７　ＬＳＡ（Local Security Authority、ローカル セキュリティ認証）
３１９　ＡＰ（Authentication Package、認証パッケージ）
３２１　ＳＡＭ（Security Account Manager）
３２３　データベース
６０１　システムＢＩＯＳ
６０７　パスワード強化システム
６０９　乱数発生器
６１１　ＳＭＩハンドラ
６１７　ソルト値データ
６１８　一時記憶域
７０９　物理メモリレジスタ・ドライバ

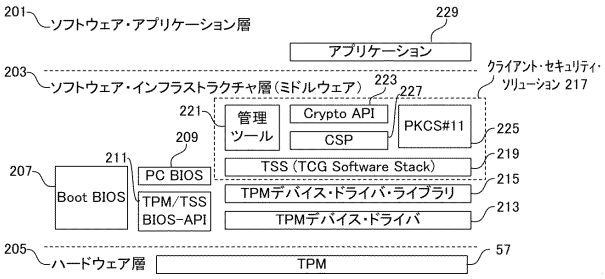
【図１】



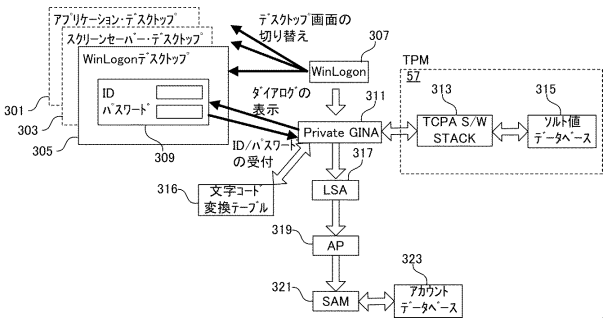

【図２】



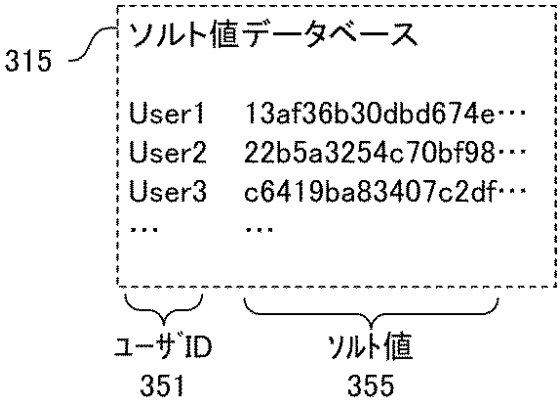

【図３】



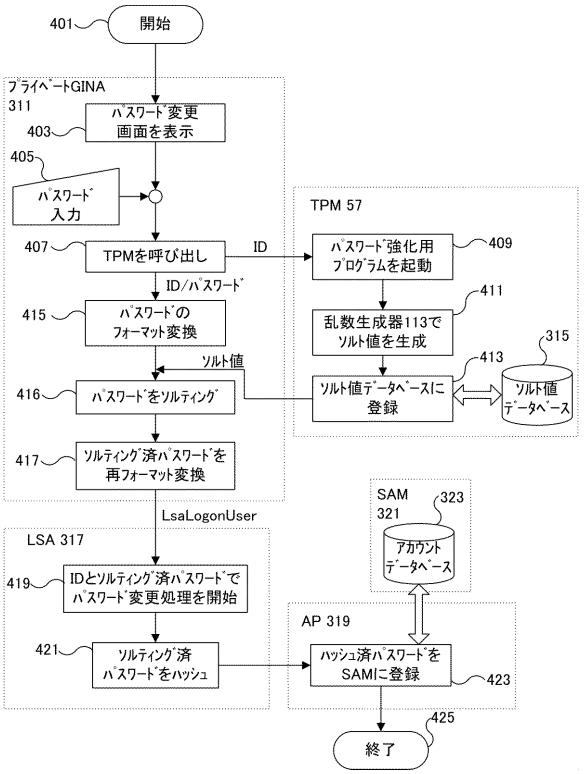

【図４】



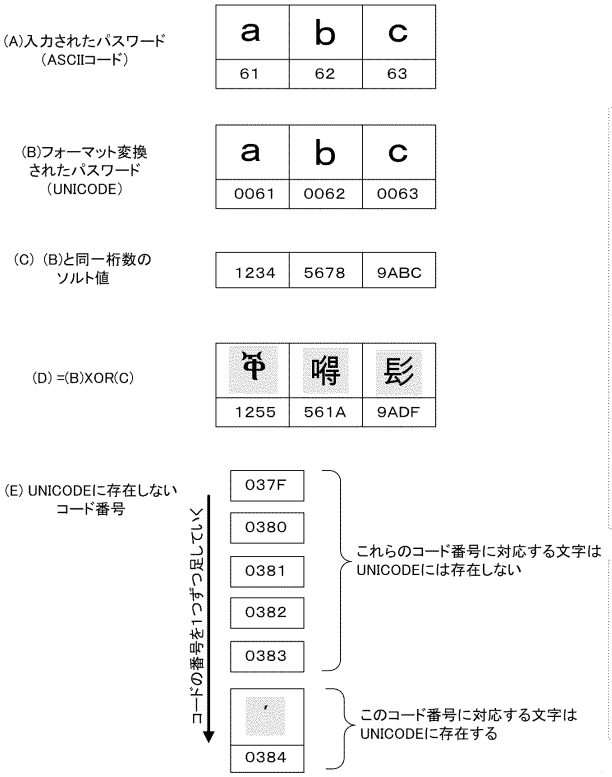
【図５】


315
ソルト値データベース
User1 13af36b30dbd674e…
User2 22b5a3254c70bf98…
User3 c6419ba83407c2df…
… …
ユーザID
351
ソルト値
355

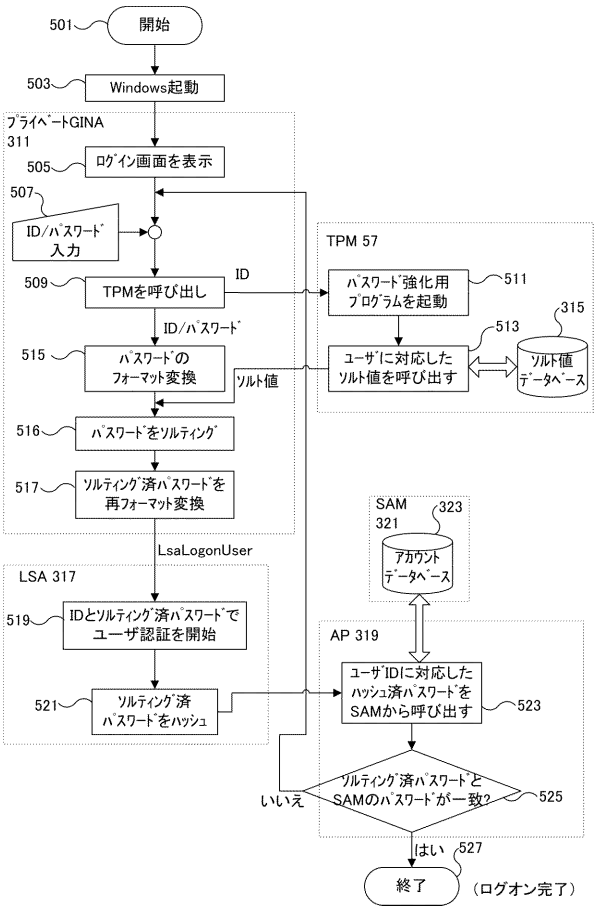
【図６】


401 開始
プライベートGINA
311
403 パスワード変更画面を表示
405 パスワード入力
407 TPMを呼び出し
ID
ID/パスワード
415 パスワードのフォーマット変換
ソルト値
416 パスワードをソルティング
417 ソルティング済パスワードを再フォーマット変換
LsaLogonUser
LSA 317
419 IDとソルティング済パスワードでパスワード変更処理を開始
421 ソルティング済パスワードをハッシュ
TPM 57
409 パスワード強化用プログラムを起動
411 乱数生成器113でソルト値を生成
413 ソルト値データベースに登録
315 ソルト値データベース
SAM
321
323 アカウントデータベース
AP 319
423 ハッシュ済パスワードをSAMに登録
425 終了

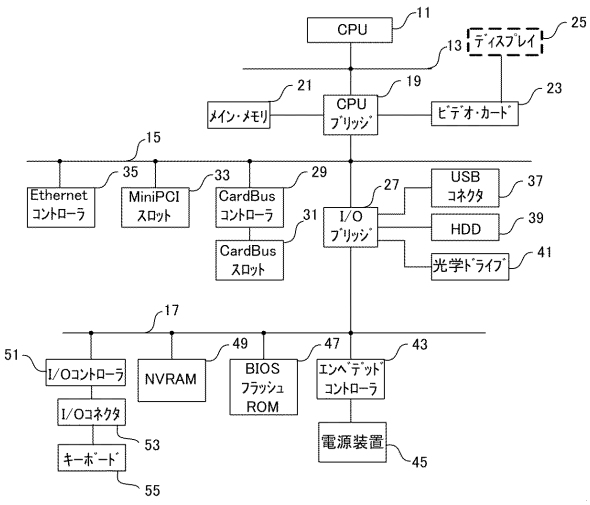
【図７】


(A)入力されたパスワード（ASCIIコード）
a b c
61 62 63
(B)フォーマット変換されたパスワード（UNICODE）
a b c
0061 0062 0063
(C) (B)と同一桁数のソルト値
1234 5678 9ABC
(D) =(B)XOR(C)
1255 561A 9ADF
(E) UNICODEに存在しないコード番号
037F
0380
0381
0382
0383
これらのコード番号に対応する文字はUNICODEには存在しない
コードの番号を1つずつ足していく
0384
このコード番号に対応する文字はUNICODEに存在する

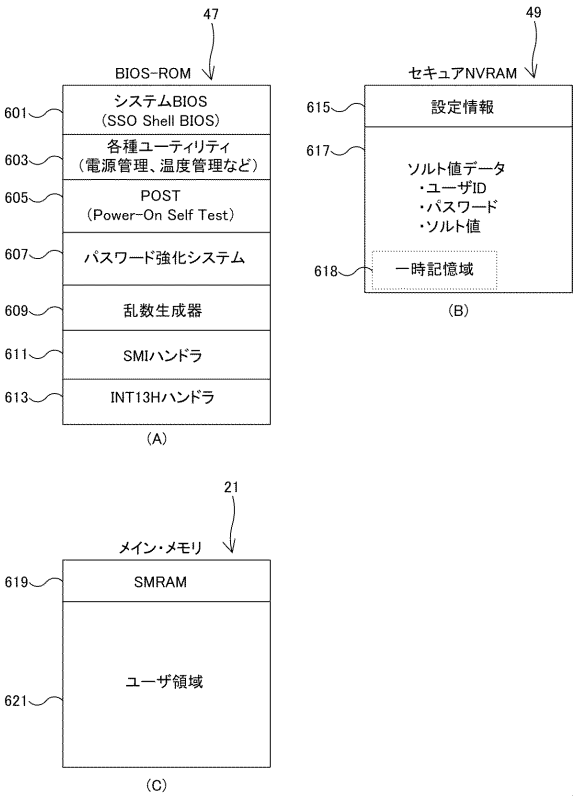
【図８】


501 開始
503 Windows起動
プライベートGINA
311
505 ログイン画面を表示
507 ID/パスワード入力
509 TPMを呼び出し
ID
ID/パスワード
515 パスワードのフォーマット変換
ソルト値
516 パスワードをソルティング
517 ソルティング済パスワードを再フォーマット変換
LsaLogonUser
LSA 317
519 IDとソルティング済パスワードでユーザ認証を開始
521 ソルティング済パスワードをハッシュ
TPM 57
511 パスワード強化用プログラムを起動
513 ユーザに対応したソルト値を呼び出す
315 ソルト値データベース
SAM
321
323 アカウントデータベース
AP 319
523 ユーザIDに対応したハッシュ済パスワードをSAMから呼び出す
525 ソルティング済パスワードとSAMのパスワードが一致?
いいえ
はい
527 終了
（ログオン完了）

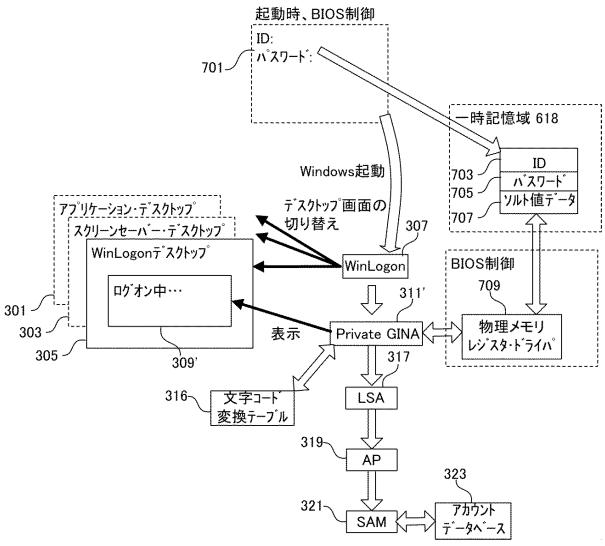
【図９】



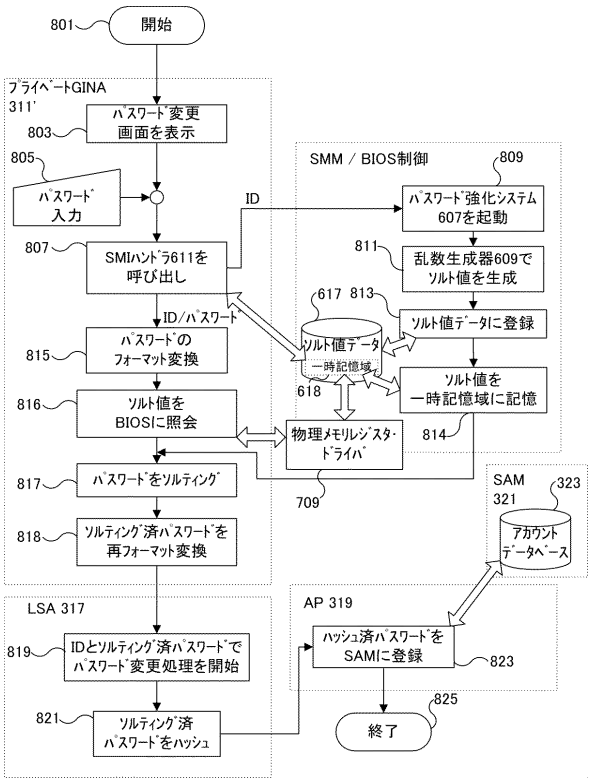

【図１０】



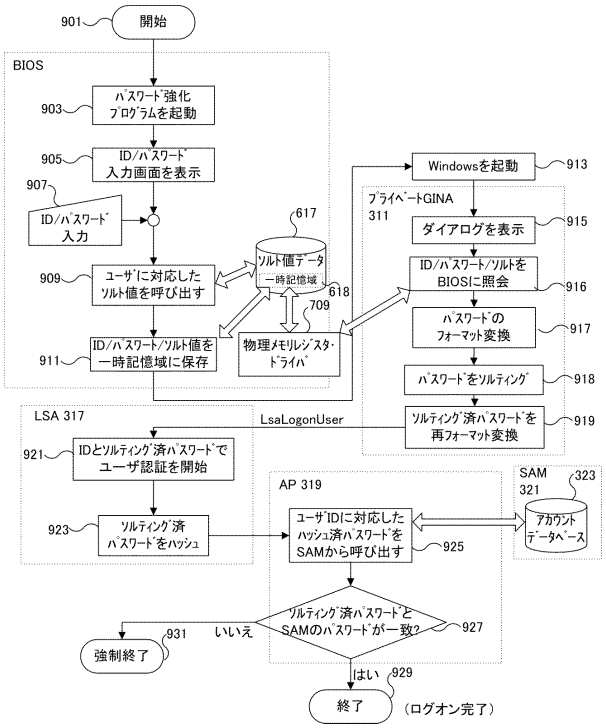

【図１１】



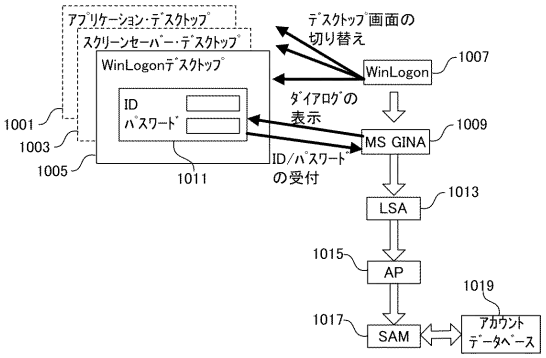

【図１２】



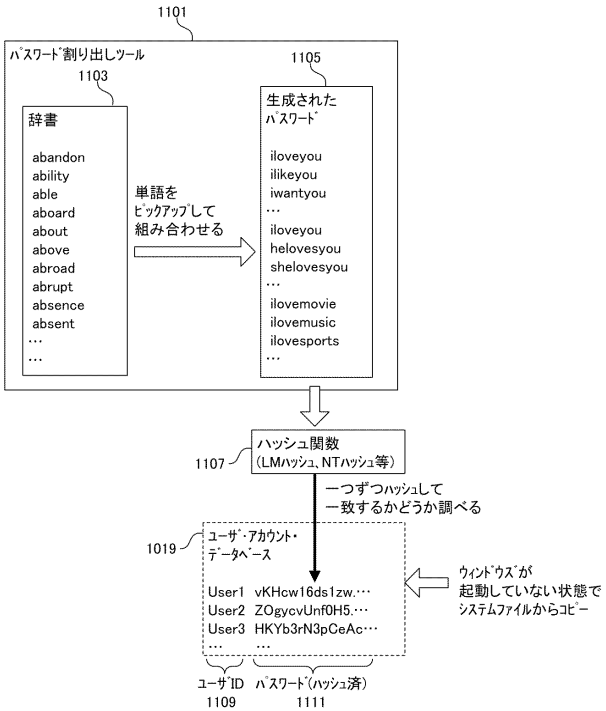
【図１３】


901
開始
BIOS
903
ﾊﾟｽﾜｰﾄﾞ強化
ﾌﾟﾛｸﾞﾗﾑを起動
905
ID/ﾊﾟｽﾜｰﾄﾞ
入力画面を表示
907
ID/ﾊﾟｽﾜｰﾄﾞ
入力
909
ﾕｰｻﾞに対応した
ｿﾙﾄ値を呼び出す
911
ID/ﾊﾟｽﾜｰﾄﾞ/ｿﾙﾄ値を
一時記憶域に保存
617
ｿﾙﾄ値ﾃﾞｰﾀ
一時記憶域
618
709
物理ﾒﾓﾘﾚｼﾞｽﾀ･
ﾄﾞﾗｲﾊﾞ
Windowsを起動
913
ﾌﾟﾗｲﾍﾞｰﾄGINA
311
915
ﾀﾞｲｱﾛｸﾞを表示
916
ID/ﾊﾟｽﾜｰﾄﾞ/ｿﾙﾄを
BIOSに照会
917
ﾊﾟｽﾜｰﾄﾞの
ﾌｫｰﾏｯﾄ変換
918
ﾊﾟｽﾜｰﾄﾞをｿﾙﾃｨﾝｸﾞ
919
ｿﾙﾃｨﾝｸﾞ済ﾊﾟｽﾜｰﾄﾞを
再ﾌｫｰﾏｯﾄ変換
LSA 317
LsaLogonUser
921
IDとｿﾙﾃｨﾝｸﾞ済ﾊﾟｽﾜｰﾄﾞで
ﾕｰｻﾞ認証を開始
923
ｿﾙﾃｨﾝｸﾞ済
ﾊﾟｽﾜｰﾄﾞをﾊｯｼｭ
AP 319
ﾕｰｻﾞIDに対応した
ﾊｯｼｭ済ﾊﾟｽﾜｰﾄﾞを
SAMから呼び出す
925
SAM
321
323
ｱｶｳﾝﾄ
ﾃﾞｰﾀﾍﾞｰｽ
ｿﾙﾃｨﾝｸﾞ済ﾊﾟｽﾜｰﾄﾞと
SAMのﾊﾟｽﾜｰﾄﾞが一致?
927
いいえ
931
強制終了
はい
929
終了
（ログオン完了）

【図１４】


ｱﾌﾟﾘｹｰｼｮﾝ･ﾃﾞｽｸﾄｯﾌﾟ
ｽｸﾘｰﾝｾｰﾊﾞｰ･ﾃﾞｽｸﾄｯﾌﾟ
WinLogonﾃﾞｽｸﾄｯﾌﾟ
ID
ﾊﾟｽﾜｰﾄﾞ
1001
1003
1005
1011
ﾃﾞｽｸﾄｯﾌﾟ画面の
切り替え
ﾀﾞｲｱﾛｸﾞの
表示
ID/ﾊﾟｽﾜｰﾄﾞ
の受付
WinLogon
1007
MS GINA
1009
LSA
1013
AP
1015
SAM
1017
ｱｶｳﾝﾄ
ﾃﾞｰﾀﾍﾞｰｽ
1019

【図１５】


1101
ﾊﾟｽﾜｰﾄﾞ割り出しﾂｰﾙ
1103
辞書
abandon
ability
able
aboard
about
above
abroad
abrupt
absence
absent
…
単語を
ﾋﾟｯｸｱｯﾌﾟして
組み合わせる
1105
生成された
ﾊﾟｽﾜｰﾄﾞ
iloveyou
ilikeyou
iwantyou
…
iloveyou
helovesyou
shelovesyou
…
ilovemovie
ilovemusic
ilovesports
…
ﾊｯｼｭ関数
(LMﾊｯｼｭ、NTﾊｯｼｭ等)
1107
一つずつﾊｯｼｭして
一致するかどうか調べる
1019
ﾕｰｻﾞ･ｱｶｳﾝﾄ･
ﾃﾞｰﾀﾍﾞｰｽ
User1 vKHcw16ds1zw.…
User2 ZOgycvUnf0H5.…
User3 HKYb3rN3pCeAc…
… …
ｳｨﾝﾄﾞｳｽﾞが
起動していない状態で
ｼｽﾃﾑﾌｧｲﾙからｺﾋﾟｰ
ﾕｰｻﾞID
1109
ﾊﾟｽﾜｰﾄﾞ(ﾊｯｼｭ済)
1111

フロントページの続き

(74)代理人 100106699
弁理士 渡部 弘道
(74)代理人 100077584
弁理士 守谷 一雄
(72)発明者 河野 誠一
神奈川県大和市下鶴間１６２３番地１４ レノボ・ジャパン株式会社 基礎研究所内
(72)発明者 杉山 祐二
神奈川県大和市下鶴間１６２３番地１４ 日本アイ・ビー・エム株式会社 大和事業所内
(72)発明者 デビッド・キャロル・チャレナー
アメリカ合衆国２７６１５ ノースカロライナ州ローリー ハンティング・リッジ・ロード ７１３
(72)発明者 フィリップ・リー・チャイルズ
アメリカ合衆国２７６０４ ノースカロライナ州ローリー ヒザーフィールド・ウェイ ４９０１
(72)発明者 ノーマン・アーサー・ディオン二世
アメリカ合衆国２７６０４ ノースカロライナ州キャリー ウェスト・ゲレル・センター １１３

審査官 市川 武宜

(56)参考文献 特開２００５－１２９０３２（ＪＰ，Ａ）
米国特許出願公開第２００３／０１７７３６４（ＵＳ，Ａ１）
国際公開第２００４／０２５４８８（WO，Ａ１）
特表２００５－５０９９３８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／２０
Ｈ０４Ｌ ９／３２