(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2008-171389
(P2008-171389A)
(43)公開日　平成20年7月24日(2008.7.24)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330B	5B017
G06F 21/22	(2006.01)	G06F	9/06	660E	5B276
G06F 1/00	(2006.01)	G06F	1/00	370E	5B285
G06F 21/24	(2006.01)	G06F	12/14	560D	

審査請求 有　請求項の数 18　ＯＬ　（全 24 頁）

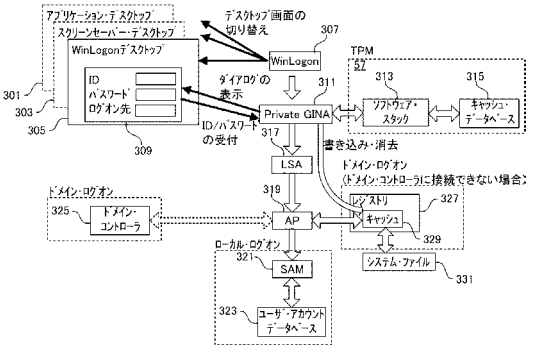
(21)出願番号　特願2007-257116 (P2007-257116)
(22)出願日　平成19年10月1日 (2007.10.1)
(31)優先権主張番号　11/621,288
(32)優先日　平成19年1月9日 (2007.1.9)
(33)優先権主張国　米国 (US)

(71)出願人　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
(71)出願人　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】ドメイン・ログオンの方法、およびコンピュータ

(57)【要約】
【課題】レジストリのキャッシュを利用したドメイン・ログオンを可能にしつつ、悪意のあるユーザにパスワードなどを取得される危険性を小さくする。
【解決手段】ウィンドウズ（登録商標）の一部であるＧＩＮＡがセキュアな記憶領域からユーザ識別情報に対応した加工されたパスワード情報を読み出し、レジストリに書き込む。そして、ドメイン・ログオンに係る認証が完了した後に、レジストリに書き込まれたパスワード情報は消去される。このことにより、当該ユーザのパスワード情報はレジストリに残らず、システム・ファイルとして保存されることもなくなる。
【選択図】図４



【特許請求の範囲】
【請求項１】
ドメイン・コントローラと、ウィンドウズ（登録商標）をオペレーティング・システムとして動作するクライアント・コンピュータとを含むネットワーク環境において、前記クライアント・コンピュータにおいてユーザがドメイン・ログオンをする方法であって、
前記ネットワーク環境にユーザ識別情報と該ユーザ識別情報に対応したドメイン・パスワード情報を格納したセキュアな記憶領域を提供するステップと、
前記ウィンドウズ（登録商標）の第１のモジュールがユーザの入力するユーザ識別情報およびドメイン・パスワードを受け取るステップと、
前記セキュアな記憶領域に格納され前記ユーザ識別情報に対応したドメイン・パスワード情報を前記コンピュータが前記ウィンドウズ（登録商標）のレジストリに書き込むステップと、
前記受け取ったドメイン・パスワードと前記レジストリに書き込まれたドメイン・パスワード情報に基づいて前記ウインドウズ（登録商標）の第２のモジュールがドメイン・ログオンに係る認証を行うステップと、
前記認証を行うステップの後に前記第１のモジュールが前記ドメイン・パスワード情報を前記レジストリから消去するステップと
を有するドメイン・ログオンの方法。
【請求項２】
前記セキュアな記憶領域が前記ネットワーク環境または前記クライアント・コンピュータの内部に提供される請求項１記載のドメイン・ログオンの方法。
【請求項３】
前記セキュアな記憶領域が前記クライアント・コンピュータのＴＰＭ（Trusted Platform Module）の内部に提供される請求項２記載のドメイン・ログオンの方法。
【請求項４】
前記セキュアな記憶領域が前記クライアント・コンピュータのＢＩＯＳからのみ参照可能な不揮発性メモリの内部に提供される請求項２記載のドメイン・ログオンの方法。
【請求項５】
前記セキュアな記憶領域が記憶している前記ユーザ識別情報および該ユーザ識別情報に対応したドメイン・パスワード情報が、前記クライアント・コンピュータにおいて過去にドメイン・ログオンに成功したユーザのユーザ識別情報および該ユーザ識別情報に対応したドメイン・パスワード情報を含む請求項１記載のドメイン・ログオンの方法。
【請求項６】
前記ドメイン・パスワード情報を前記レジストリから消去するステップが、前記ユーザが入力したドメイン・パスワードから生成したドメイン・パスワード情報を前記セキュアな記憶領域に書き込むステップを含む請求項１記載のドメイン・ログオンの方法。
【請求項７】
前記ドメイン・パスワード情報を前記レジストリから消去するステップが、前記認証されたユーザがログオフされるタイミングに実行される請求項１記載のドメイン・ログオンの方法。
【請求項８】
前記ドメイン・パスワード情報を前記レジストリから消去するステップが、前記認証を完了したタイミングに実行される請求項１記載のドメイン・ログオンの方法。
【請求項９】
前記第１のモジュールがＧＩＮＡ（Graphical Identification and Authentication）で、前記第２のモジュールがＡＰ（Authentication Package）である請求項１記載のドメイン・ログオンの方法。
【請求項１０】
ドメイン・コントローラと、ウィンドウズ（登録商標）をオペレーティング・システムとして動作するクライアント・コンピュータとを含むネットワーク環境において、前記ク

ライアント・コンピュータにおいてユーザがドメイン・ログオンをする方法であって、
前記ネットワーク環境にユーザ識別情報と該ユーザ識別情報に対応したドメイン・パスワード情報を格納したセキュアな記憶領域を提供するステップと、
前記ウィンドウズ（登録商標）の第１のモジュールが前記ユーザの入力するユーザ識別情報およびドメイン・パスワードを受け取るステップと、
前記セキュアな記憶領域に格納され前記ユーザ識別情報に対応したドメイン・パスワード情報を前記コンピュータが前記ウィンドウズ（登録商標）のレジストリに書き込むステップと、
前記ウインドウズ（登録商標）の第２のモジュールが前記ドメイン・コントローラに対して接続を試行するステップと、
前記第２のモジュールが、前記ドメイン・コントローラに対して接続が成功したときには前記ドメイン・コントローラに対して前記ユーザ識別情報および前記ドメイン・パスワードを照会することによってドメイン・ログオンに係る認証を行い、前記ドメイン・コントローラに対して接続が失敗したときには前記受け取ったドメイン・パスワードと前記レジストリに書き込まれたドメイン・パスワード情報に基づいてドメイン・ログオンに係る認証を行うステップと、
前記認証を行うステップの後に前記第１のモジュールが前記ドメイン・パスワード情報を前記レジストリから消去するステップと
を有するドメイン・ログオンの方法。
【請求項１１】
ウィンドウズ（登録商標）をオペレーティング・システムとして動作し、ドメイン・コントローラを含むネットワーク環境に接続可能なコンピュータであって、
ユーザ識別情報と該ユーザ識別情報に対応したドメイン・パスワード情報を格納したセキュアな記憶手段と、
ユーザがユーザ識別情報とドメイン・パスワードを入力する入力手段と、
前記セキュアな記憶手段に格納され前記ユーザ識別情報に対応したドメイン・パスワード情報を前記ウィンドウズ（登録商標）のレジストリに書き込む書き込み手段と、
入力された前記ドメイン・パスワードと前記レジストリに書き込まれたドメイン・パスワード情報に基づいてドメイン・ログオンに係る認証をする認証手段と、
前記ドメイン・ログオンに係る認証が行われた後に前記ドメイン・パスワード情報を前記レジストリから消去する消去手段と
を有するコンピュータ。
【請求項１２】
前記セキュアな記憶手段が、ＴＰＭ（Trusted Platform Module）を含む請求項１１記載のコンピュータ。
【請求項１３】
前記セキュアな記憶手段がＢＩＯＳからのみ参照可能な不揮発性メモリを含む請求項１１記載のコンピュータ。
【請求項１４】
前記書き込み手段がＧＩＮＡ（Graphical Identification and Authentication）を含む請求項１１記載のコンピュータ。
【請求項１５】
前記消去手段がＧＩＮＡ（Graphical Identification and Authentication）を含む請求項１１記載のコンピュータ。
【請求項１６】
ウィンドウズ（登録商標）をオペレーティング・システムとして動作し、ドメイン・コントローラを含むネットワーク環境に接続可能なコンピュータであって、
ユーザ識別情報と該ユーザ識別情報に対応したドメイン・パスワード情報を格納したセキュアな記憶手段と、
ユーザがユーザ識別情報とドメイン・パスワードを入力する入力手段と、

前記セキュアな記憶手段に格納され前記ユーザ識別情報に対応したドメイン・パスワード情報を前記ウィンドウズ（登録商標）のレジストリに書き込む書き込み手段と、
前記ドメイン・コントローラに対して接続を試行する接続手段と、
前記接続手段が、前記ドメイン・コントローラに対して接続が成功したときには前記ドメイン・コントローラに対して前記ユーザ識別情報および前記ドメイン・パスワードを照会することによってドメイン・ログオンに係る認証を行い、前記ドメイン・コントローラに対して接続が失敗したときには入力された前記ドメイン・パスワードと前記レジストリに書き込まれたドメイン・パスワード情報に基づいてドメイン・ログオンに係る認証を行う認証手段と、
前記ドメイン・ログオンに係る認証が行われた後に前記ドメイン・パスワード情報を前記レジストリから消去する消去手段と
を有するコンピュータ。

【請求項１７】
ウィンドウズ（登録商標）をオペレーティング・システムとして動作し、コントローラを含むネットワーク環境に接続可能コンピュータであって、
プロセッサと、
ユーザ識別情報と該ユーザ識別情報に対応したドメイン・パスワード情報を格納したセキュアな記憶装置と、
プログラムを格納した記憶媒体とを有し、
前記プログラムは前記プロセッサに
ユーザの入力するユーザ識別情報とドメイン・パスワードを受け取るステップと、
前記セキュアな記憶装置に格納され前記ユーザ識別情報に対応したドメイン・パスワード情報を前記ウィンドウズ（登録商標）のレジストリに書き込むステップと、
前記受け取ったドメイン・パスワードと前記レジストリに書き込まれたドメイン・パスワード情報に基づいてドメイン・ログオンに係る認証を行うステップと、
前記認証をするステップの後に前記ドメイン・パスワード情報を前記レジストリから消去するステップとを実行させる
コンピュータ。

【請求項１８】
ウィンドウズ（登録商標）をオペレーティング・システムとして動作し、ドメイン・コントローラを含むネットワーク環境に接続可能コンピュータであって、
プロセッサと、
ユーザ識別情報と該ユーザ識別情報に対応したドメイン・パスワード情報を格納したセキュアな記憶装置と、
プログラムを格納した記憶媒体とを有し、
前記プログラムは前記プロセッサに
ユーザの入力するユーザ識別情報およびドメイン・パスワードを受け取るステップと、
前記セキュアな記憶装置に格納され前記ユーザ識別情報に対応したドメイン・パスワード情報を前記ウィンドウズ（登録商標）のレジストリに書き込むステップと、
前記ドメイン・コントローラに対して接続を試行するステップと、
前記ドメイン・コントローラに対して接続が成功したときには前記ドメイン・コントローラに対して前記ユーザ識別情報および前記ドメイン・パスワードを照会することによってドメイン・ログオンに係る認証を行うステップと、
前記ドメイン・コントローラに対して接続が失敗したときには前記受け取ったドメイン・パスワードと前記レジストリに書き込まれたドメイン・パスワード情報に基づいてドメイン・ログオンに係る認証を行うステップと、
前記認証を行うステップの後に前記ドメイン・パスワード情報を前記レジストリから消去するステップとを実行させる
コンピュータ。

【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）の制御によって動作しドメインに参加するコンピュータにおいてユーザを認証する技術に関し、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ドメイン認証に伴うセキュリティ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（以後単にパスワードという。）を入力してＯＳにログオンする。その際、当該ＰＣに登録されたユーザＩＤおよびパスワードを入力してログオンすることができる。これをローカル・ログオンという。
【０００３】
一方、ウィンドウズ（登録商標）・シリーズのＯＳによって動作する複数のＰＣを、イーサネット（Ethernet、登録商標）などによって相互に接続することにより、容易にＬＡＮ（Local Area Network）もしくはＷＡＮ（Wide Area Network）を構築できる。その際、論理的に一つのグループとして扱われる複数のＰＣやプリンタなどのコンピュータ資源を総称して、ドメインという。一つのドメインの中では、ユーザＩＤおよびセキュリティ・ポリシーは、基本的に１台のコンピュータによって管理される。このコンピュータをドメイン・コントローラという。ドメイン・コントローラは、ユーザの認証、ユーザ・アカウントの追加や削除、セキュリティ設定の変更などを統括して行うことができる。なお、ドメイン・コントローラが一つのドメインの中で複数存在する場合もある。その場合は、主に使用される一つのドメイン・コントローラをプライマリ・ドメイン・コントローラとし、その他をバックアップ用のバックアップ・ドメイン・コントローラとすることができる。ここでいうドメインは、ウィンドウズ（登録商標）のバージョン、あるいはＬＡＮもしくはＷＡＮの規模などによって、ＮＴドメインである場合もあれば、アクティブ・ディレクトリ（Active Directory）・ドメインである場合もあるが、ここではそれらを総称してドメインということにする。
【０００４】
ドメインに参加しているコンピュータでは、ローカル・ログオンに代えて当該ドメインのドメイン・コントローラに登録されたユーザＩＤおよびパスワードを入力してログオンすることもできる。これをドメイン・ログオンという。ローカル・ログオンはユーザＩＤおよびパスワードを登録した当該ＰＣで行うのに対し、ドメイン・ログオンは当該ドメインに参加している全てのＰＣで、ドメイン・コントローラに登録されたユーザＩＤおよびパスワードを利用してログオンできる。ドメイン・ログオンした場合は、当該ドメインで共有されるコンピュータ資源を使用できる。さらに、当該ドメインと信頼関係を結んだ他のドメインのコンピュータ資源を共用することもできる。
【０００５】
図１３は、ドメインに属するＰＣでの、従来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。ＷｉｎＬｏｇｏｎ１００７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。

【０００６】

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（Graphical 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、パスワード、およびログオン先を入力すると、入力されたユーザＩＤおよびパスワードはＧＩＮＡ１００９からＬＳＡ（Local Security Authority、ローカル セキュリティ機関）１０１３と呼ばれるコンポーネントに渡される。ＬＳＡは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。なお、ログオン先は当該ＰＣ自身と、ＰＣが属するドメインとを選択できる。ログオン先としてＰＣ自身を選択すればローカル・ログオン、ドメインを選択すればドメイン・ログオンとなる。

【０００７】

ＬＳＡ１０１３は、ユーザが入力したユーザＩＤ、パスワードおよびログオン先をＡＰ（Authentication Package、認証パッケージ）１０１５に渡す。ＡＰ１０１５は、ユーザより指定されたログオン先に応じてユーザの認証を行う。ローカル・ログオンであれば、ＡＰ１０１５はＬＳＡ１０１３から受け取ったパスワードをウィンドウズ（登録商標）のＳＡＭ（Security Accounts Manager）１０１７と呼ばれるコンポーネントが保持するユーザ・アカウント・データベース１０１９の中から検索したパスワードと比較し、当該ユーザＩＤおよび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。

【０００８】

ドメイン・ログオンである場合、ＡＰ１０１５はＰＣが属するドメインのドメイン・コントローラ１０２１にアクセスし、ＬＳＡ１０１３から受け取ったユーザＩＤおよびパスワードをドメイン・コントローラ１０２１に対して照会する。その際、ＰＣとドメイン・コントローラ１０２１との間では、ＬＭ認証、ＮＴＬＭ認証、ＮＴＬＭｖ２認証などのような方式で相互に認証が行われる。その場合、ＰＣからのユーザＩＤなどを含むリクエストを受け取ったドメイン・コントローラ１０２１は、ＰＣに対してチャレンジと呼ばれる文字列を返送する。チャレンジを受け取ったＰＣは、パスワードによってチャレンジを暗号化した文字列（レスポンス）をドメイン・コントローラ１０２１に返送する。ドメイン・コントローラ１０２１は、このレスポンスから、当該ユーザＩＤおよびパスワードが正当なものであるかどうかを認証し、認証された結果はドメイン・コントローラ１０２１からＰＣへ返信される。この方式によれば、パスワードを直接ネットワークを介して送信しなくても、ドメイン・コントローラ１０２１に対してユーザＩＤおよびパスワードの正当性を照会し、認証を行うことができる。

【０００９】

ローカル・ログオンおよびドメイン・ログオンのどちらであっても、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。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ており、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。

【００１０】
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１】特開２００５－３０３９９３号公報
【発明の開示】
【発明が解決しようとする課題】
【００１１】
ウィンドウズ（登録商標）の動作環境下では、ドメイン・ログオンに成功したユーザのログオン情報は、当該ＰＣのレジストリ１０２３内のキャッシュ１０２５という場所に保存される。ここでいうログオン情報は、ユーザＩＤ、パスワード、ログオンした日時、ドメイン名、および当該ＰＣのホスト名などが含まれる。当該ＰＣがドメイン・コントローラ１０２１に接続できない場合、キャッシュ１０２５に保存されたログオン情報を利用すれば、ドメイン・コントローラ１０２１に接続できる場合と同じユーザＩＤおよびパスワードを利用してログオンできる。たとえば、普段オフィス内でＬＡＮに接続されてドメインに属しているノートブック型ＰＣ（以後ノートＰＣという）は、ＬＡＮから切り離されてオフィス外に持ち出されて使用される場合には、オフィス内に存在するドメイン・コントローラ１０２１に接続できない。また、無線ＬＡＮに接続されるＰＣで、該無線ＬＡＮの電波状態が悪化してドメイン・コントローラ１０２１に接続できなくなる場合もある。それらのような場合でも、キャッシュ１０２５に保存されたログオン情報を利用してドメイン・ログオンすれば、ドメインに登録されたアカウントで当該ノートＰＣにログオンでき、ドメイン・コントローラ１０２１に接続できる場合と同一の操作環境、たとえばデスクトップ画面の配置やスタート・メニューの構成、あるいはソフトウェアの設定などを再現して使用できる。なお、キャッシュ１０２５に保存されるログオン情報は、過去に成功した各ユーザのドメイン・ログオンについて、特定の回数分だけ保存される。保存回数は、０回～５０回の範囲で設定を変更することが可能である。デフォルトでは、過去１０回の成功したドメイン・ログオンについて保存される。
【００１２】
しかし、キャッシュ１０２５に保存されたログオン情報は、ある程度以上の操作権限を与えられたユーザであれば誰でも取得することができる。前述のように、ドメイン・ログオンであれば当該ドメインに参加している全てのＰＣで登録されているユーザＩＤおよびパスワードでログオンできるため、当該ＰＣも当該ドメインに属する複数のユーザによって使用されている可能性が高い。従って、キャッシュ１０２５にアクセスする権限を与えられたユーザであれば、当該ＰＣに最近ドメイン・ログオンしたユーザ全てのログオン情報を取得することができる。即ち、悪意のあるユーザがログオンすれば、別のユーザのユーザＩＤおよびハッシュされたパスワードにアクセスすることができてしまうので、ユーザＩＤおよびパスワードを盗まれる危険性がある。さらに、キャッシュ１０２５に保存されたパスワードがたとえソルティングされハッシュされていても、辞書攻撃などの方法でハッシュされる前のパスワードを割り出される危険性がある。辞書攻撃によってパスワードを割り出すツール（パスワード・クラッキング・ツール）、およびそれに使用される使用頻度順の辞書などは、インターネットなどを通じて誰でも簡単に入手できる。
【００１３】
また、ウィンドウズ（登録商標）を起動している間はレジストリ１０２３内のキャッシュ１０２５に保存されているログオン情報は、ウィンドウズ（登録商標）がログオフの状態になるときには、磁気ディスク装置のシステム・ファイル１０２７の中に保存され、次回のログオンのときに再びレジストリのキャッシュに保存された情報として利用できるようになっている。しかも、ログオン情報が保存されるファイル名および磁気ディスク内でのアドレス、さらにファイル内部のデータ構造やハッシュ関数のアルゴリズムなどは開発者向けに公開されている。そのため、当該ＰＣ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

クなどから別のＯＳを起動したりするなどして、システム・ファイル１０２７の中からキャッシュ１０２５に保存されていたログオン情報をコピーすることができる。このファイルからも、暗号化されていないユーザＩＤおよびハッシュされたパスワードを読み出すことができる。特にＰＣ本体またはＰＣから抜き取られた磁気ディスク装置が盗難にあった場合、そのような手段でドメインに属する複数のユーザのユーザＩＤおよびパスワードが読み出される危険性がある。

【００１４】

前述のように、キャッシュ１０２５に保存されるログオン情報は、過去に成功したドメイン・ログオンについて、０回～５０回の範囲で保存する回数の設定を変更することが可能である。より具体的には、レジストリ・キーのHKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\Current Version\Winlogonの、CachedLogonsCountとして保存されている値が、過去に成功したドメイン・ログオンについてログオン情報を保存する回数である。この値を「０」に設定すれば、キャッシュ１０２５にはログオン情報は一切保存されないことになるので、ログオン情報に含まれるパスワードが盗まれる危険性は少なくなる。しかし、そうすると今度はキャッシュ１０２５を利用したドメイン・ログオンが不可能になり、ドメイン・コントローラ１０２１に接続できない環境では、当該ノートＰＣにログオンするにはローカル・ログオンする以外にない。これでは、ドメイン・ログオンが可能な場合の操作環境を再現できないので、利便性に欠ける。

【００１５】

そこで本発明の目的は、ウィンドウズ（登録商標）で利用できるドメイン・ログオンの利便性を維持し、かつ、ウィンドウズ（登録商標）の基本モジュールに変更を加えたり特別なハードウェアを用意したりすることなく、より安全にドメイン・ログオンをする方法およびドメイン・パスワードを格納する方法を提供することにある。さらに本発明の目的は、レジストリのキャッシュを利用したドメイン・ログオンを可能にしつつ、キャッシュに格納された情報を通じて悪意のあるユーザにパスワードなどのログオン情報を取得される危険性の少ないドメイン・ログオンの方法、およびドメイン・パスワード情報の格納方法を提供することにある。さらに本発明の目的は、そのような認証方法または格納方法を実現するコンピュータを提供することにある。

【課題を解決するための手段】

【００１６】

本発明の一つの態様は、ドメイン・コントローラと、ウィンドウズ（登録商標）をオペレーティング・システムとして動作するクライアント・コンピュータとを含むネットワーク環境において、クライアント・コンピュータのドメイン・ログオンの方法を提供する。ネットワーク環境には、ユーザ識別情報と該ユーザ識別情報に対応したドメイン・パスワード情報を格納したセキュアな記憶領域が存在する。セキュアな記憶領域は、セキュアなチャネルで接続されたクライアント・コンピュータの外部装置に設けてもクライアント・コンピュータの内部に設けてもよい。ドメイン・パスワード情報は、ドメイン・パスワードがソルティングされたりハッシュ関数で暗号化されたりしてドメイン・パスワード自体とは異なるが、両者の照合を可能にするドメイン・パスワードと関連ある情報である。

【００１７】

ウィンドウズ（登録商標）の第１のモジュールが、ユーザ識別情報（ユーザＩＤ）とドメイン・パスワードをユーザから受け取る。第１のモジュールはＧＩＮＡとすることができる。さらに、コンピュータは、ユーザ識別情報に対応したドメイン・パスワード情報をセキュアな記憶領域から読み出し、レジストリに書き込む。この書き込みは、ＧＩＮＡまたはその他のコンポーネントが行うことができる。ウィンドウズ（登録商標）の第２のモジュールがユーザから受け取ったドメイン・パスワードと、レジストリに書き込まれたドメイン・パスワード情報とを比較することによってドメイン・ログオンに係る認証が行われる。

【００１８】

第２のモジュールは、ＡＰとすることができる。ＡＰはドメイン認証のためにドメイン

・コントローラにアクセスできないときはレジストリのキャッシュに格納されたパスワード情報とユーザから受け取ったドメイン・パスワードで認証することになっているが、この認証に必要な情報はセキュアな記憶領域から読み出されているので、認証作業に支障は生じない。認証が完了した後に第１のモジュールはレジストリに書き込まれたドメイン・パスワード情報を消去する。このことにより、当該ユーザのパスワードはレジストリに残らず、かつ従来とは異なりウィンドウズ（登録商標）をログオフする際にシステム・ファイルとして保存されることもなくなるので、悪意のあるユーザに取得される危険性は小さくなる。しかも、クライアント・コンピュータがドメイン・コントローラにアクセスできない場合であっても、ＡＰがレジストリを参照してユーザを認証することによりドメイン・ログオンが可能である。

【００１９】

セキュアな記憶領域としては、クライアント・コンピュータ内部のＴＰＭ（Trusted Platform Module）内部のメモリ、または、ＢＩＯＳからのみ参照可能な不揮発性メモリを利用することができる。また、セキュアな記憶領域が記憶しているユーザ識別情報と該ユーザ識別情報に対応したドメイン・パスワード情報は、このクライアント・コンピュータにおいて過去にドメイン・ログオンに成功したユーザのユーザ識別情報およびパスワードである。このことにより、通常ウィンドウズ（登録商標）で行われている認証手順と同様に、過去にドメイン・ログオンに成功したユーザは、クライアント・コンピュータがドメイン・コントローラに接続できない場合であってもドメイン・ログオンを行うことが可能となる。さらに、レジストリに書き込まれたパスワードを消去するタイミングに合わせて、ドメイン・ログオンに成功したドメイン・パスワードから生成されたドメイン・パスワード情報をセキュアな記憶領域に書き込むことにより、ドメイン・ログオンが成功するたびに該ユーザのユーザ識別情報およびドメイン・パスワード情報を保存してゆくことができる。

【００２０】

その結果、ウィンドウズ（登録商標）の認証アルゴリズムが更新されたような場合であっても、セキュアな記憶領域の情報は常に最新の認証アルゴリズムに基づいたドメイン・パスワード情報に置き換えられるので、その後の認証に支障をきたすことがなくなる。レジストリに書き込まれたパスワードを、ドメイン・ログオンの認証が完了した直後のタイミングで消去すると、それ以後ドメイン・パスワード情報がレジストリから盗まれる可能性がなくなるのでパスワード・クラッキングに対する耐性が最も高くなる。また、またユーザがログオフされるタイミングで消去するようにすれば、当該ユーザがログオンしている間は、当該ユーザのもとでドメイン認証が必要なさまざまなアプリケーション・プログラムを利用できるようになり、しかも、ログオフ後のパスワード攻撃に対する耐性が強化される。

【００２１】

また、クライアント・コンピュータがドメイン・ログオンをする際、クライアント・コンピュータはまずドメイン・コントローラへの接続を試行し、接続が成功した場合は、ドメイン・コントローラに対してユーザ識別情報とユーザから受け取ったドメイン・パスワードとを照合してドメイン・ログオンに係る認証を行うようにする。接続が失敗した場合は、レジストリに書き込まれたドメイン・パスワード情報を参照してドメイン・ログオンに係る認証を行う。そして、ドメイン・コントローラに接続が成功した場合も、接続が失敗した場合も、ドメイン・ログオンに成功したドメイン・パスワードから生成したドメイン・パスワード情報をセキュアな記憶領域に書き込み、レジストリに書き込まれたドメイン・パスワード情報をレジストリから消去する。このことにより、次回以降のドメイン・ログオンの際にドメイン・コントローラにアクセスできなくても、今回ドメイン・ログオンに成功したのと同じユーザ識別情報とパスワードでドメイン・ログオンが可能になる。

【００２２】

別の捉え方では、本発明はウィンドウズ（登録商標）をオペレーティング・システムとして動作し、ドメイン・コントローラを含むネットワーク環境に接続可能なクライアント

・コンピュータを提供する。このコンピュータは、ドメイン・ログオンの方法として説明した各々のステップを実行する手段を持つ。さらに別の捉え方では、本発明に係るコンピュータはプロセッサと、セキュアな記憶装置と、ドメイン・ログオンの方法として説明した各々のステップをプロセッサで実行するプログラムを記憶した記憶媒体とを持つ。

【発明の効果】

【００２３】

本発明により、ウィンドウズ（登録商標）で利用できるドメイン・ログオンの利便性を維持し、かつ、ウィンドウズ（登録商標）の基本モジュールに変更を加えたり特別なハードウェアを用意したりすることなく、より安全にドメイン・ログオンをする方法およびドメイン・パスワードを格納する方法を提供することができた。さらに本発明により、レジストリのキャッシュを利用したドメイン・ログオンを可能にしつつ、キャッシュに格納された情報を通じて悪意のあるユーザにパスワードなどのログオン情報を取得される危険性の少ないドメイン・ログオンの方法、およびドメイン・パスワード情報の格納方法を提供することができた。さらに本発明により、そのような認証方法または格納方法を実現するコンピュータ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】

【００２４】

図１は、本発明の第１の実施の形態にかかるクライアント・コンピュータである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。

【００２５】

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、ＣＰＵ１１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。

【００２６】

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、イーサネット（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。イーサネット（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。

【００２７】

Ｉ／Ｏブリッジ２７は、ＰＣＩバス１５とＬＰＣバス１７との間のブリッジとしての機能を備えている。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。

【００２８】

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。

【００２９】

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。

【００３０】

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キャッシュ・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。

【００３１】

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。本実施の形態では、後述するログオン情報管理用プログラムもＲＯＭ１０９に記憶される。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ＲＳＡ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。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。

【００３２】

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（TCG Software Stack）がＴＣＧによって定義されている。図３は、ＴＳＳ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の中で信頼できるプラットフォーム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。ＴＳＳでは、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つの階層が定義されている。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。また、ＢＩＯＳフラッシュＲＯＭ４７に記憶されてシステムの設定を行うＰＣ　ＢＩＯＳ２０９から、ＴＰＭ／ＴＳＳ　ＢＩＯＳ　ＡＰＩ２１１を介しても操作される。

【００３３】

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＃１１　２２５、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。

【００３４】

図４は、本発明の第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。クライアントであるＰＣ１０は、ドメインのメンバーとしてドメイン・コントローラとともにネットワーク環境を構成するように設定されているものとする。ドメイン・コントローラには、管理者によりドメインに参加することが許可された複数のユーザの認証情報が登録されている。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。

【００３５】

ＷｉｎＬｏｇｏｎデスクトップ３０５上には、ユーザＩＤ、パスワード、およびログオン先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。ＰＣ

１０は、ネットワークの管理者によってあらかじめドメインのメンバーとして登録されているので、ダイアログ３０９はユーザがローカル・ログオンとドメイン・ログオンを選択できるように表示される。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を介してローカル・ログオンまたはドメイン・ログオンのいずれかのユーザＩＤおよびパスワードを入力すると、入力されたユーザＩＤはプライベートＧＩＮＡ３１１から、ソフトウェア・スタック３１３に含まれる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。キャッシュ・データベース３１５は不揮発性ＲＡＭ１０３上にあり、過去に成功したドメイン・ログオンについてのログオン情報が保存される。ログオン情報には、ユーザがＰＣ１０に入力するパスワードがソルティングされた後でハッシュされた情報を含む。実行エンジン１１１では、ＲＯＭ１０９から読み出されたログオン情報管理用プログラムによって後述する処理が実行される。プライベートＧＩＮＡ３１１以外のプログラムから、このログオン情報管理用プログラムにアクセスすることはできない。また、ログオン情報管理用プログラム以外のプログラムから、キャッシュ・データベース３１５の内容を参照することもできない。

【００３６】

ＬＳＡ３１７、ＡＰ３１９、ＳＡＭ３２１、ユーザ・アカウント・データベース３２３、ドメイン・コントローラ３２５、レジストリ３２７、キャッシュ３２９、システム・ファイル３３１は、全て図１３で示した従来技術のものと同一であるので、説明を省略する。ただし、本実施の形態ではウィンドウズ（登録商標）が起動されてユーザの認証を開始する時点では、キャッシュ３２９にはいずれのユーザのログオン情報も保存しないことによって安全性を高めている。そして、ユーザの認証を行う際に、ログオンしようとしているユーザ１人の認証に必要なログオン情報のみが、プライベートＧＩＮＡ３１１によってキャッシュ３２９に書き込まれる。ウインドウズ（登録商標）では、ドメイン・コントローラに接続できない場合には、キャッシュ３２９に当該ユーザのログオン情報が存在しないとドメイン・ログオンを行うことができないので、本実施の形態ではＡＰ３１９が認証作業を行う前にログオンを開始したユーザだけのログオン情報をキャッシュ３２９に書き込むことにしている。

【００３７】

図５～６は、本発明の第１の実施の形態におけるユーザのログオンの手順を表すフローチャートである。ユーザのログオンには、ドメインに参加しないローカル・ログオンとドメインに参加するドメイン・ログオンを含んでいる。図５～６は、図面の錯綜を回避するため、ここでは２つの図に分けて記載する。ＰＣ１０の電源を投入し（ブロック４０１）、ウィンドウズ（登録商標）が起動すると（ブロック４０３）、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、パスワード、およびログオン先の入力のダイアログ３０９を表示する（ブロック４０５）。ユーザがダイアログ３０９に対してユーザＩＤ、パスワード、およびログオン先を入力すると（ブロック４０７）、プライベートＧＩＮＡ３１１はまずログオン先を判断する（ブロック４０９）。ローカル・ログオンであれば、後述するブロック４１１～４１５の処理は行わず、ブロック４１７に進む。

【００３８】

ブロック４０９でドメイン・ログオンである場合、ユーザが入力したユーザＩＤをＴＰＭ５７に渡す（ブロック４１１）。ユーザＩＤを受け取ったＴＰＭ５７は、ＴＰＭ５７内部のＲＯＭ１０９に記憶されたログオン情報管理用プログラムを実行エンジン１１１に呼び出し、キャッシュ・データベース３１５に入力されたユーザＩＤに対応するログオン情報を呼び出す（ブロック４１３）。もし、キャッシュ・データベース３１５内に入力されたユーザＩＤに対応するログオン情報が存在すれば、当該ログオン情報を受け取ったプライベートＧＩＮＡ３１１が、当該情報を当該ＰＣのレジストリ３２７内のキャッシュ３２

９に書き込む（ブロック４１５）。キャッシュ・データベース３１５内に入力されたユーザＩＤに対応するログオン情報が存在しなければ、キャッシュ３２９には何も書き込まれない。

【００３９】

以上の処理が完了したら、プライベートＧＩＮＡ３１１はＡＰＩ関数の一つであるWlxLoggedOutSASを呼び出すことにより、ユーザが入力したユーザＩＤ、パスワード、およびログオン先をＬＳＡ３１７に渡す（ブロック４１７）。ＬＳＡ３１７が受け取ったユーザＩＤ、パスワード、およびログオン先は、さらにＡＰ３１９に渡され、従来技術と同一のユーザの認証の処理が行われる（ブロック４１９）。ＡＰ３１９はログオン先を判断し（ブロック４２１）、ローカル・ログオンの場合は、ＡＰ３１９はＳＡＭ３２１が持つユーザ・アカウント・データベース３２３を参照する（ブロック４２３）。ドメイン・ログオンの場合は、まずドメイン・コントローラ３２５に接続を試み（ブロック４２５）、接続できたら当該ドメイン・コントローラに対して、ユーザが入力したパスワードが正当なものであるかどうかを照会する（ブロック４２７）。ウインドウズ（登録商標）では、ドメイン・ログオンの場合においてドメイン・コントローラ３２５に接続できなければ、キャッシュ３２９を参照する（ブロック４２９）ようになっている。入力されたユーザＩＤに対応するログオン情報がＴＰＭ５７内のキャッシュ・データベース３１５に存在していれば、ブロック４１３～４１５で対応するログオン情報がキャッシュ３２９に書き込まれているので、ＡＰ３１９はこのログオン情報をキャッシュ３２９で参照して認証することができる。従って、ドメイン・コントローラ３２５に接続できなくても、キャッシュ３２９の情報によってドメイン・ログオンを行うことが可能である。なお、ブロック４１３で入力されたユーザＩＤに対応するログオン情報がキャッシュ・データベース３１５に存在しなければ、キャッシュ３２９には何も書き込まれないので、ドメイン・コントローラ３２５に接続できない限りドメイン・ログオンはできないことになる。

【００４０】

ユーザの認証が成功したら（ブロック４３１）、ドメイン・コントローラ３２５に接続できたか否かにかかわらず、今回のドメイン・ログオンに係る認証が成功したことに伴う新たなログオン情報をＡＰ３１９がキャッシュ３２９に書き込む（ブロック４３３）。ここで書き込まれる新たなログオン情報には、今回ドメイン・ログオンに成功したユーザＩＤおよびパスワード、ログオンした日時などが含まれる。その際、ブロック４１５で書き込まれた過去のログオン情報は、この時点では上書きしてもよいし、残してもよい。また、ローカル・ログオンの場合は、ログオン情報をキャッシュ３２９に書き込む必要がない。

【００４１】

ブロック４３３に続いて、プライベートＧＩＮＡ３１１は再びログオン先を判断する（ブロック４３５）。ローカル・ログオンであれば、後述するブロック４３７～４４１の処理は行わず、ブロック４４３に進む。ブロック４３５でドメイン・ログオンである場合、プライベートＧＩＮＡ３１１はキャッシュ３２９に書き込まれた新たなログオン情報を読み取り（ブロック４３７）、ＴＰＭ５７内部のログオン情報管理用プログラムを呼び出し、読み取った新たなログオン情報をキャッシュ・データベース３１５に記録する（ブロック４３９）。この結果、ＴＰＭ内部でのログオン情報の処理方法が更新された場合でも対応することができるようになる。そして、プライベートＧＩＮＡ３１１がキャッシュ３２９から、ブロック４１５で書き込まれた過去のログオン情報と、ブロック４３３で書き込まれた新たなログオン情報を消去する（ブロック４４１）。これでユーザの認証は完了し（ブロック４４３）、プライベートＧＩＮＡ３１１はＡＰＩ関数の一つであるWlxActivateUserShellでアプリケーション・デスクトップ３０１を呼び出して、ユーザは通常の作業を行うことができる。なお、ブロック４３１で認証が失敗したら、ブロック４０７の入力に戻る。

【００４２】

ここで、現在ログオンしているユーザがレジストリ３２７にアクセスし、キャッシュ３

２９の内容を読み取ろうとしても、キャッシュ３２９の内容はブロック４４１の処理によって既に消去されているため、ログオン情報を読み取ることができない。もちろん、現在ログオンしているユーザの操作によってＴＰＭ５７内部に存在するキャッシュ・データベース３１５にアクセスしてその内容を読み取ることもできない。従って、当該ドメインにログオンできるユーザにも、もちろんそれ以外の第三者にも、キャッシュ３２９を介してログオン情報を取得されることはない。しかし、本実施の形態においては、ユーザがドメイン・ログオンする際に入力したログオン情報はキャッシュ・データベース３１５に記録されていて、プライベートＧＩＮＡ３１１がユーザ認証を行うたびに該当するユーザのログオン情報だけをキャッシュ３２９に書き込むので、ドメイン・コントローラ３２５に接続できない環境においても従来技術と全く同じようにドメイン・ログオンが可能である。また、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について、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変更点はない。

【００４３】

図７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。

【００４４】

図８は、本発明の第２の実施の形態に供される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８（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）５０１、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５０３、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）５０５、本発明にかかるログオン情報管理システム５０７、ＣＰＵ１１をＳＭＭで動作させるＳＭＩハンドラ５０９、磁気ディスク装置３９にアクセスするＩＮＴ１３Ｈハンドラ５１１などが記憶されている。

【００４５】

図８（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５１３、およびキャッシュ・データベース５１５を記憶している。設定情報５１３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。キャッシュ・データベース５１５は、ユーザＩＤおよびそれに対応するログオン情報を収納する。キャッシュ・データベース５１５は、システムＢＩＯＳ５０１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。

【００４６】

図８（Ｃ）に示すメイン・メモリ２１には、ＰＣの通常の動作で使用されるユーザ領域５１９の他に、ＳＭＲＡＭ（System Management RAM）５１７としての領域が確保されている。システムＢＩＯＳ５０１からＳＭＩハンドラ５０９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５１７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

ＢＩＯＳ５０１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５１７にアクセスされることもない。

【００４７】

図９は、本発明の第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。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ＢＩＯＳ５０１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、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。

【００４８】

ＷｉｎＬｏｇｏｎデスクトップ３０５上には、ユーザＩＤ、パスワード、およびログオン先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はプライベートＧＩＮＡ３１１’から、物理メモリレジスタ・ドライバ６０１を介して、システムＢＩＯＳ５０１で動作するログオン情報管理システム５０７に渡される。物理メモリレジスタ・ドライバ６０１は、システムＢＩＯＳ５０１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ＢＩＯＳ５０１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６０１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５０９を呼び出し、Ｉ／Ｏ命令を使用してＣＰＵ１１のレジスタ経由でＳＭＩを発行し、ＣＰＵ１１のレジスタで指定される該物理アドレスをシステムＢＩＯＳ５０１に伝達することができる。

【００４９】

ログオン情報管理システム５０７は、渡されたユーザＩＤに対応するログオン情報をキャッシュ・データベース５１５から読み出す。システムＢＩＯＳ５０１は、読み出されたログオン情報を伝達された該物理アドレスに格納してから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、ＳＭＲＡＭ５１７領域内であっても、ユーザ領域５１９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。

【００５０】

図１０～１１は、本発明の第２の実施の形態におけるユーザのログオンの手順を表すフローチャートである。図１０～１１は、図面の錯綜を回避するため、ここでは２つの図に分けて記載する。ＰＣ１０’の電源を投入し（ブロック７０１）、ウィンドウズ（登録商標）が起動すると（ブロック７０３）、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、パスワード、およびログオン先の入力のダイアログ３０９を表示する（ブロック７０５）。ユーザがダイアログ３０９に対してユーザＩＤ、パスワード、およびログオン先を入力すると（ブロック７０７）、プライベートＧＩＮＡ３１１’はまずログオン先を判断する（ブロック７０９）。ローカル・ログオンであれば、後述するブロック７１１～７１５の処理は行わず、ブロック７１７に進む。

【００５１】
ブロック７０９でドメイン・ログオンである場合、ユーザが入力したユーザＩＤを物理メモリレジスタ・ドライバ６０１に渡す（ブロック７１１）。ここでＣＰＵ１１はＳＭＭに入り、システムＢＩＯＳ５０１の制御下でログオン情報管理システム５０７が動作し、ユーザＩＤを受け取る（ブロック７１３）。ログオン情報管理システム５０７は、入力されたユーザＩＤに対応するログオン情報をＮＶＲＡＭ４９内のキャッシュ・データベース５１５から読み出し、メイン・メモリ２１上の指定されたアドレスに書き込む（ブロック７１３）。ここでＳＭＭが終了してウィンドウズ（登録商標）の制御下に戻り、制御が渡されたプライベートＧＩＮＡ３１１’はログオン情報を受け取ることができる。もし、キャッシュ・データベース３１５内に入力されたユーザＩＤに対応するログオン情報が存在すれば、当該ログオン情報を受け取ったプライベートＧＩＮＡ３１１’が、当該情報を当該ＰＣのレジストリ３２７内のキャッシュ３２９に書き込む（ブロック７１５）。キャッシュ・データベース３１５内に入力されたユーザＩＤに対応するログオン情報が存在しなければ、キャッシュ３２９には何も書き込まれない。

【００５２】
以上の処理が完了したら、プライベートＧＩＮＡ３１１’はＡＰＩ関数の一つであるWlxLoggedOutSASを呼び出すことにより、ユーザが入力したユーザＩＤ、パスワード、およびログオン先をＬＳＡ３１７に渡す（ブロック７１７）。ＬＳＡ３１７が受け取ったユーザＩＤ、パスワード、およびログオン先は、さらにＡＰ３１９に渡され、従来技術と同一のユーザの認証の処理が行われる（ブロック７１９）。ＡＰ３１９はログオン先を判断し（ブロック７２１）、ローカル・ログオンの場合は、ＡＰ３１９はＳＡＭ３２１が持つユーザ・アカウント・データベース３２３を参照する（ブロック７２３）。ドメイン・ログオンの場合は、まずドメイン・コントローラ３２５に接続を試み（ブロック７２５）、接続できたら当該ドメイン・コントローラに対して、ユーザが入力したパスワードが正当なものであるかどうかを照会する（ブロック７２７）。ドメイン・ログオンの場合でドメイン・コントローラ３２５に接続できなければ、キャッシュ３２９を参照する（ブロック７２９）。入力されたユーザＩＤに対応するログオン情報がＴＰＭ５７内のキャッシュ・データベース３１５に存在していれば、ブロック７１３～７１５で対応するログオン情報がキャッシュ３２９に書かれているので、ＡＰ３１９はこのログオン情報をキャッシュ３２９で参照することができる。従って、ドメイン・コントローラ３２５に接続できなくても、キャッシュ３２９の情報によってドメイン・ログオンを行うことが可能である。なお、ブロック７１３で入力されたユーザＩＤに対応するログオン情報が存在しなければ、キャッシュ３２９には何も書き込まれないので、ドメイン・コントローラ３２５に接続できなければドメイン・ログオンはできない。

【００５３】
ユーザの認証が成功したら（ブロック７３１）、ドメイン・コントローラ３２５に接続できたか否かにかかわらず、今回のドメイン・ログオンに係る認証が成功したことに伴う新たなログオン情報をＡＰ３１９がキャッシュ３２９に書き込む（ブロック７３３）。ここで書き込まれる新たなログオン情報には、今回ドメイン・ログオンに成功したユーザＩＤおよびパスワード、ログオンした日時などが含まれる。その際、ブロック７１５で書き込まれた過去のログオン情報は、上書きしてもよいし、残してもよい。また、ローカル・ログオンの場合は、ログオン情報をキャッシュ３２９に書き込むこと自体がない。

【００５４】
プライベートＧＩＮＡ３１１’は、再びログオン先を判断する（ブロック７３５）。ローカル・ログオンであれば、後述するブロック７３７～７４１の処理は行わず、ブロック７４３に進む。ブロック７３５でドメイン・ログオンである場合、プライベートＧＩＮＡ３１１’はキャッシュ３２９に書き込まれた新たなログオン情報を読み取り（ブロック７３７）、読み取った新たなログオン情報をブロック７１１と同じように物理メモリレジスタ・ドライバ６０１を介してログオン情報管理システム５０７に渡し（ブロック７３８）、ＮＶＲＡＭ４９内のキャッシュ・データベース５１５に記録させる（ブロック７３９）

。そして、プライベートＧＩＮＡ３１１’がキャッシュ３２９から、ブロック７１５で書き込まれた過去のログオン情報と、ブロック７３３で書き込まれた新たなログオン情報を消去する（ブロック７４１）。これでユーザの認証は完了し（ブロック７４３）、プライベートＧＩＮＡ３１１’はＡＰＩ関数の一つであるWlxActivateUserShellでアプリケーション・デスクトップ３０１を呼び出して、ユーザは通常の作業を行うことができる。なお、ブロック７３１で認証が失敗したら、ブロック７０７の入力に戻る。

【００５５】

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、ユーザの操作によってキャッシュ・データベース５１５にアクセスしてその内容を読み取ることを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６０１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、キャッシュ３２９の内容が消去されるため、当該ドメインにログオンできるユーザにも、もちろんそれ以外の第三者にも、キャッシュ３２９を介してログオン情報を取得されることはない点は、第１の実施の形態と同じである。

【００５６】

図１２は、ドメイン・ログオンにおけるログオン情報のレジストリ３２７への書き込みおよび消去のタイミングを示す概念図である。同図では、各々のブロックが実行される時系列の順に昇順で参照番号を付与している。図１２（Ａ）は、第１および第２の実施の形態でのタイミングを示している。左から順に、ウィンドウズ（登録商標）の状態およびユーザの操作、プライベートＧＩＮＡ３１１または３１１’の動作、およびキャッシュ３２９の状態を示す。ウィンドウズ（登録商標）が起動され（ブロック８０１）、ディスプレイ２５にＷｉｎＬｏｇｏｎデスクトップ３０５が表示されると（ブロック８０２）、ユーザが入力したユーザＩＤ、パスワード、およびログオン先を受け付けたプライベートＧＩＮＡ３１１または３１１’は、キャッシュ・データベース３１５または５１５から当該ユーザのログオン情報を呼び出して、キャッシュ３２９に当該ログオン情報を書き込む（ブロック８０３）。そしてプライベートＧＩＮＡ３１１または３１１’は、ＡＰＩ関数WlxLoggedOutSASを呼び出すことにより、ドメイン・ログオンを開始する（ブロック８０４）。

【００５７】

キャッシュ３２９に存在するログオン情報によってドメイン・ログオンに係る当該ユーザの認証が完了したら（ブロック８０５）、プライベートＧＩＮＡ３１１または３１１’はキャッシュ３２９から全てのログオン情報を消去する（ブロック８０６）。そしてプライベートＧＩＮＡ３１１または３１１’は、ＡＰＩ関数WlxActivateUserShellでアプリケーション・デスクトップ３０１を呼び出す（ブロック８０７～８０８）。これで、ユーザはＰＣ１０またはＰＣ１０‘においてドメインのネットワーク資源を利用しながら作業を行うことができる。ユーザが作業をしている間は、キャッシュ３２９にはいかなるユーザのログオン情報も残っていないので、パスワード攻撃に対する耐性が強化されたことになる。ユーザが作業を終了し、ログオフの操作をしたら（ブロック８０９）、プライベートＧＩＮＡ３１１または３１１’はＡＰＩ関数WlxIsLogoffOKを呼び出し、ログオフの動作を行う（ブロック８１０）。ユーザがログオフした後で当該ＰＣ１０または１０’の電源を切っても、キャッシュ３２９にはログオン情報が存在していないのでＰＣ１０またはＰＣ１０’やそれらに搭載されている磁気ディスク装置が盗まれても、システム・ファイルからログオン情報を読み取ることは不可能である。

【００５８】

図１２（Ａ）で説明した第１および第２の実施の形態では、ログオン情報はユーザの認証が成功した直後のブロック８０６で消去されるので、ブロック８０３～８０６の間だけしかキャッシュ３２９に存在しない。ログオンしているユーザが自らの操作でキャッシュ

３２９からログオン情報を読み取ることができるのはブロック８０８～８０９の間であるが、その時点ではブロック８０６で示した処理が既に完了し、キャッシュ３２９から全てのログオン情報は消去されている。このことは、万一ログオンしているユーザがキャッシュ３２９からログオン情報を読み取ろうとしても、不可能であるということを意味する。また、ログオン情報がキャッシュ３２９に存在しないことによってＯＳおよびアプリケーションの動作に不具合を生ずる場面は少ない。

【００５９】

しかし、一部の電子メール・クライアントなどのアプリケーションで、キャッシュ３２９に書き込まれた現在ログオンしているユーザに関するログオン情報を参照して使用するものがある。たとえば、ＳＳＰＩ（Security Support Provider Interface）を利用して、アプリケーションがクライアント－サーバ間の通信を行うときに、クライアントおよびサーバそれぞれの正当性を確認し、通信されるデータの機密性と完全性を保証するために、キャッシュ３２９に記録されたログオン情報を利用して認証を行う場合がある。そのような場合、現在ログオンしているユーザのログオン情報がキャッシュ３２９に記録されていないと、認証を必要とするアプリケーションが動作しないことになる。

【００６０】

この問題を、ログオン情報の消去をユーザの認証が成功した直後ではなく、ユーザがログオフする時に行うようにすることで解決する方法がある。図１２（Ｂ）は、ログオン情報を消去するタイミングをそのように変更した、第１および第２の実施の形態の変型について示している。この実施の形態の変型は、ログオン情報を消去するタイミングを変更することを除いては、第１および第２の実施の形態と全く同じであるので、ハードウェアおよびソフトウェアの構成、およびアルゴリズムなどについての説明を省略する。また、図１２（Ｂ）の構成は図１２（Ａ）と同じである。ウィンドウズ（登録商標）が起動され（ブロック８５１）、ディスプレイ２５にＷｉｎＬｏｇｏｎデスクトップ３０５が表示されると（ブロック８５２）、ユーザが入力したユーザＩＤ、パスワード、およびログオン先を受け付けたプライベートＧＩＮＡ３１１または３１１’は、キャッシュ・データベース３１５または５１５から当該ユーザのログオン情報を呼び出して、キャッシュ３２９に当該ログオン情報を書き込む（ブロック８５３）。そしてプライベートＧＩＮＡ３１１または３１１’は、ＡＰＩ関数WlxLoggedOutSASを呼び出すことにより、ドメイン・ログオンを開始する（ブロック８５４）。

【００６１】

キャッシュ３２９に存在するログオン情報によってドメイン・ログオンに係る当該ユーザの認証が完了したら（ブロック８５５）、プライベートＧＩＮＡ３１１または３１１’は、ＡＰＩ関数WlxActivateUserShellでアプリケーション・デスクトップ３０１を呼び出す（ブロック８５６～８５７）。これで、ユーザは作業を行うことができる。ユーザが作業を終了し、ログオフの操作をしたら（ブロック８５８）、プライベートＧＩＮＡ３１１または３１１’はキャッシュ３２９から全てのログオン情報を消去する（ブロック８５９）。そしてプライベートＧＩＮＡ３１１または３１１’はＡＰＩ関数WlxIsLogoffOKを呼び出し、ログオフの作業を行う（ブロック８６０）。ユーザをログオフした後で当該ＰＣ１０または１０’の電源を切っても、その時点でキャッシュ３２９に存在していないログオン情報が、システム・ファイルとして保存されることがないので、当該システム・ファイルからログオン情報を読み取ることは不可能である。

【００６２】

この実施の形態の変型によると、ログオン情報は当該ログオン情報に関連するユーザがログオフする直後のブロック８５９で消去されるので、キャッシュ３２９にはブロック８５３～８５９の間だけログオン情報が存在する。それに対して、ログオンしているユーザが自らの操作でキャッシュ３２９から情報を読み取ることができるのはブロック８５７～８５８の間であるので、該ユーザは自らの操作でログオン情報を読み取ることができることになる。しかし、ブロック８５３でキャッシュ３２９に書き込まれるログオン情報は、ログオンしているユーザ自身のログオン情報だけである。その他のユーザのログオン情報

は、ユーザの操作によってアクセスできないキャッシュ・データベース３１５または５１５の中にだけ存在し、キャッシュ３２９には書き込まれない。つまり、ログオンしているユーザがキャッシュ３２９から読み取ることができる情報は、既知である自分自身のユーザＩＤおよびパスワードだけであり、その他のユーザのログオン情報を取得することはできない。もちろん、現在ログオンしているユーザのログオン情報が、当該ドメインにログオンできる他のユーザにも、それら以外の第三者にも、キャッシュ３２９を介して取得されることはない。その一方で、ログオンしているユーザ自身のログオン情報はキャッシュ３２９に存在するので、ＳＳＰＩを利用して認証を行う必要のあるアプリケーションが動作しなくなることはない。

【００６３】

前述の通り、従来技術でキャッシュに保存されるログオン情報は、過去に成功したドメイン・ログオンについて、０回～５０回の範囲で設定された回数だけ保存される。これはウィンドウズ（登録商標）の仕様として決められていることであるので、これ以外の条件でログオン情報の保存を設定することはできない。しかし本実施の形態ではログオン情報をウィンドウズ（登録商標）の仕様に基づいてキャッシュに保存する必要がないので、ログオン情報の保存条件を自由に設定することができる。たとえば、過去に成功したドメイン・ログオンについて、ＴＰＭ５７またはＮＶＲＡＭ４９の記憶容量の許す限り、５１回以上何回分でも保存する回数を設定することが可能である。また、回数以外の条件を設定することもできる。たとえば「過去１ヶ月以内に成功したドメイン・ログオン」などのように、日時によって保存するログオン情報の条件を設定してもよい。また、複数の条件を組み合わせて設定することもできる。もちろん、保存する条件を変えても、ログオン情報は全てユーザが自らの操作で読み取ることができないＴＰＭ５７またはＮＶＲＡＭ４９の中に保存されるので、安全性が損なわれることはない。

【００６４】

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】

【００６５】

ウィンドウズ（登録商標）をＯＳとし、ドメインに参加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】

【００６６】

【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】第１の実施の形態におけるユーザのログオンの動作を表すフローチャートである。

【図６】図５の続きである。

【図７】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８】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９】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。

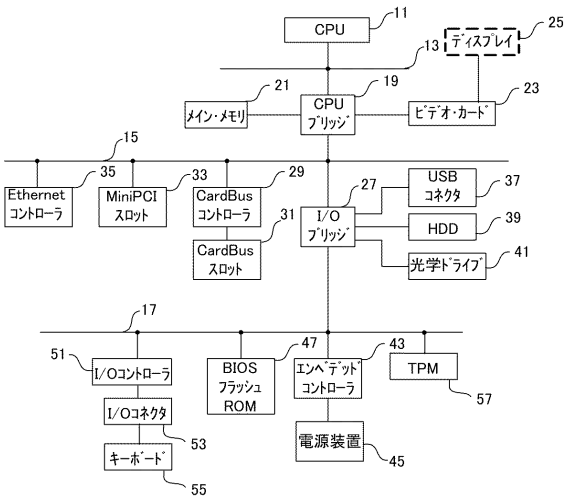
【図１０】第２の実施の形態におけるユーザのログオンの動作を表すフローチャートである。

【図１１】図１０の続きである。

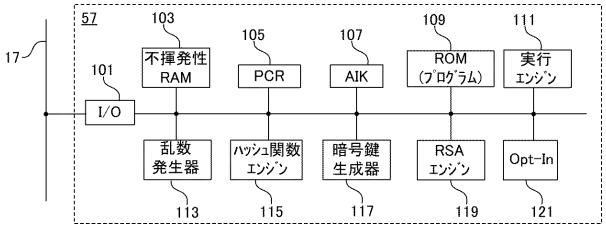
【図１２】ドメイン・ログオンにおけるログオン情報のレジストリへの書き込みおよび消去のタイミングを示す概念図である。

【図１３】ドメインに属するＰＣでの、従来のログオンの仕組みを示す概念図である。
【符号の説明】
【００６７】
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）
３１１，３１１’　プライベートＧＩＮＡ（Graphical Identification and Authentication）
３１５　キャッシュ・データベース
３２５　ドメイン・コントローラ
３２７　レジストリ
３２９　キャッシュ
５０１　システムＢＩＯＳ
５０７　ログオン情報管理システム
５１５　キャッシュ・データベース
６０１　物理メモリレジスタ・ドライバ

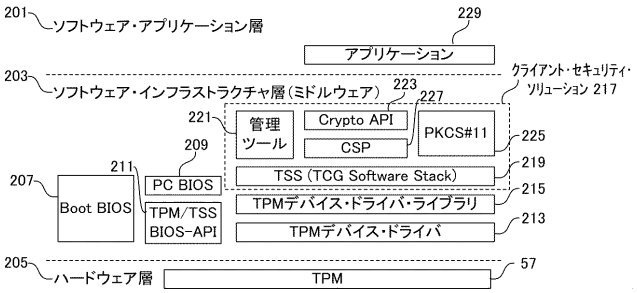
【図１】



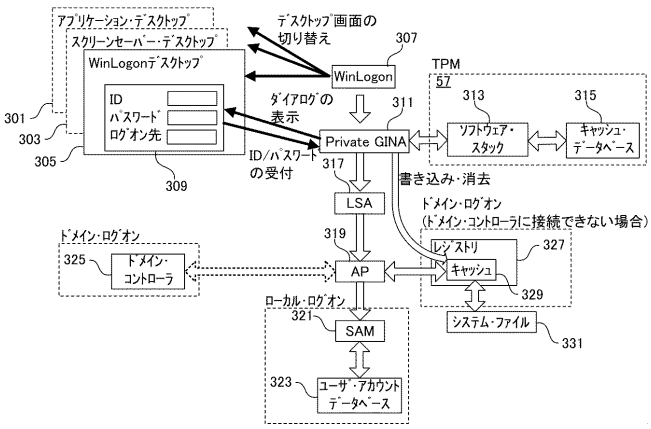
【図２】



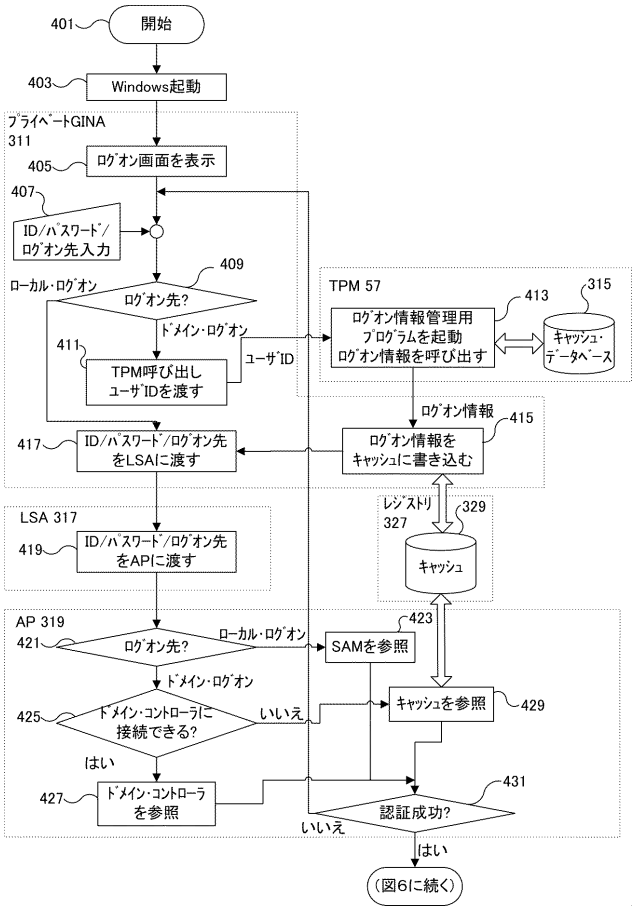
【図３】



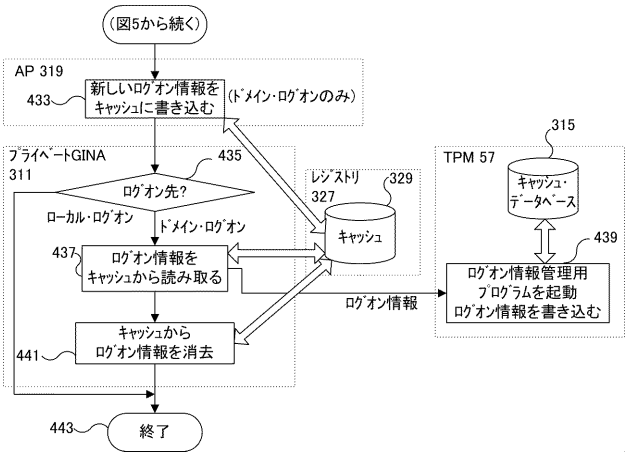
【図４】



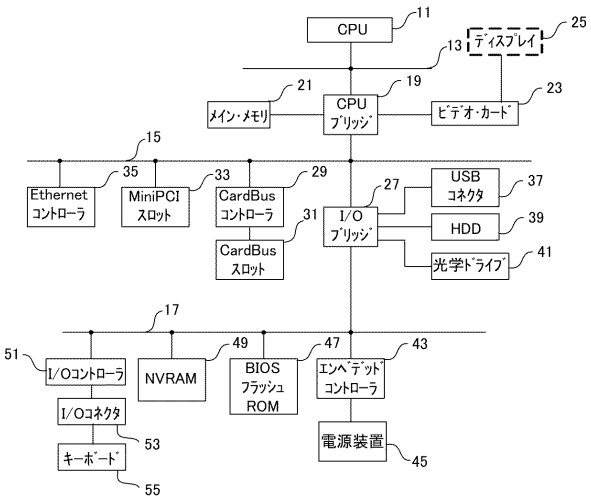
【図５】


401 開始
403 Windows起動
プライベートGINA 311
405 ログオン画面を表示
407 ID/パスワード/ログオン先入力
409 ローカル・ログオン / ログオン先? / ドメイン・ログオン
411 TPM呼び出し ユーザIDを渡す
ユーザID
TPM 57
413 ログオン情報管理用プログラムを起動 ログオン情報を呼び出す
315 キャッシュ・データベース
ログオン情報
415 ログオン情報をキャッシュに書き込む
417 ID/パスワード/ログオン先をLSAに渡す
レジストリ 327
329 キャッシュ
LSA 317
419 ID/パスワード/ログオン先をAPに渡す
AP 319
421 ログオン先? / ローカル・ログオン / ドメイン・ログオン
423 SAMを参照
425 ドメイン・コントローラに接続できる? / いいえ / はい
キャッシュを参照 429
427 ドメイン・コントローラを参照
431 認証成功? / いいえ / はい
(図6に続く)

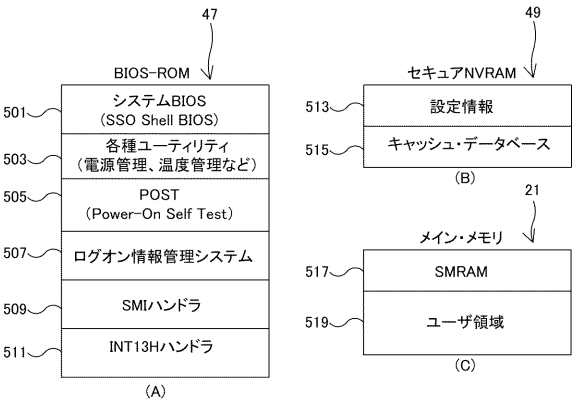
【図６】


(図5から続く)
AP 319
433 新しいログオン情報をキャッシュに書き込む (ドメイン・ログオンのみ)
プライベートGINA 311
435 ログオン先? / ローカル・ログオン / ドメイン・ログオン
437 ログオン情報をキャッシュから読み取る
441 キャッシュからログオン情報を消去
443 終了
レジストリ 327
329 キャッシュ
ログオン情報
TPM 57
315 キャッシュ・データベース
439 ログオン情報管理用プログラムを起動 ログオン情報を書き込む

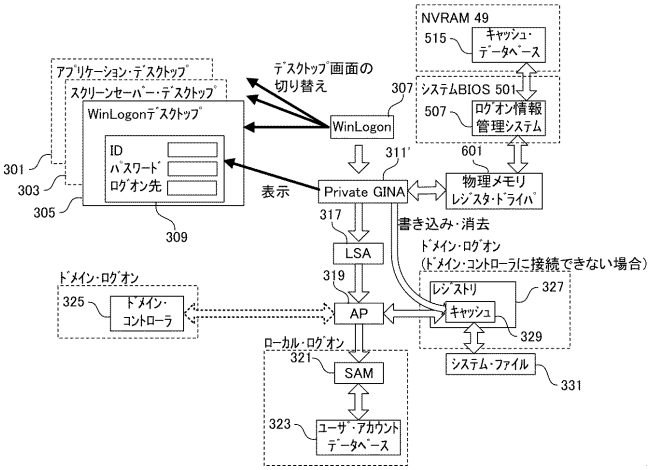
【図７】


CPU 11
ディスプレイ 25
13
メイン・メモリ 21
CPUブリッジ 19
ビデオ・カード 23
15
Ethernetコントローラ 35
MiniPCIスロット 33
CardBusコントローラ 29
CardBusスロット 31
I/Oブリッジ 27
USBコネクタ 37
HDD 39
光学ドライブ 41
17
51 I/Oコントローラ
NVRAM 49
BIOSフラッシュROM 47
エンベデッドコントローラ 43
I/Oコネクタ
キーボード 53 55
電源装置 45

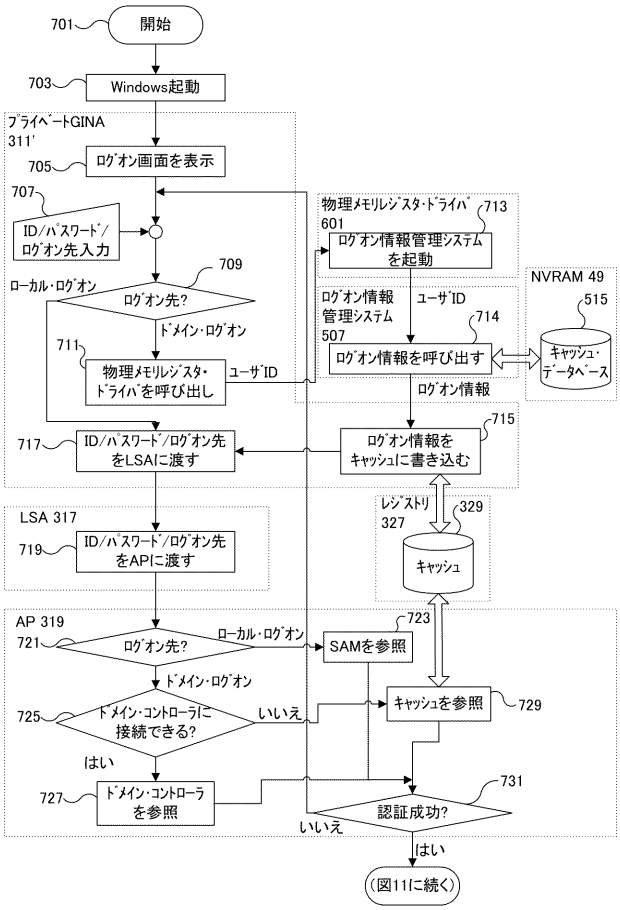
【図８】


47
BIOS-ROM
501 システムBIOS (SSO Shell BIOS)
503 各種ユーティリティ (電源管理、温度管理など)
505 POST (Power-On Self Test)
507 ログオン情報管理システム
509 SMIハンドラ
511 INT13Hハンドラ
(A)
49
セキュアNVRAM
513 設定情報
515 キャッシュ・データベース
(B)
21
メイン・メモリ
517 SMRAM
519 ユーザ領域
(C)

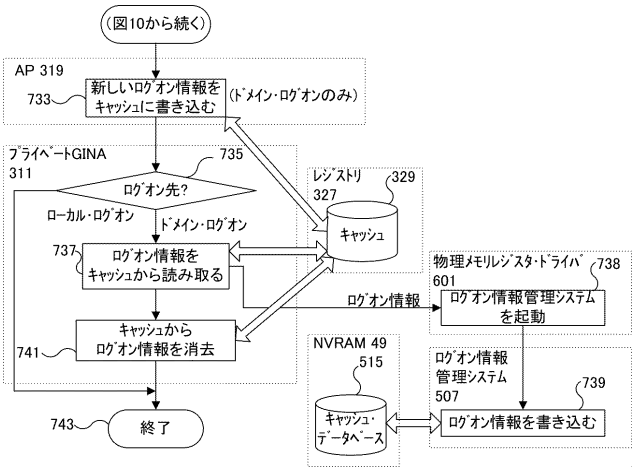
【図９】


NVRAM 49
515 キャッシュ・データベース
システムBIOS 501
507 ログオン情報管理システム
601
物理メモリ レジスタ・ドライバ
アプリケーション・デスクトップ
スクリーンセーバー・デスクトップ
WinLogonデスクトップ
ID
パスワード
ログオン先
301 303 305 309
デスクトップ画面の切り替え
307 WinLogon
311'
Private GINA
表示
317
書き込み・消去
LSA
319
AP
ドメイン・ログオン
325 ドメイン・コントローラ
ドメイン・ログオン (ドメイン・コントローラに接続できない場合)
レジストリ 327
キャッシュ 329
システム・ファイル 331
ローカル・ログオン
321 SAM
323 ユーザ・アカウント データベース

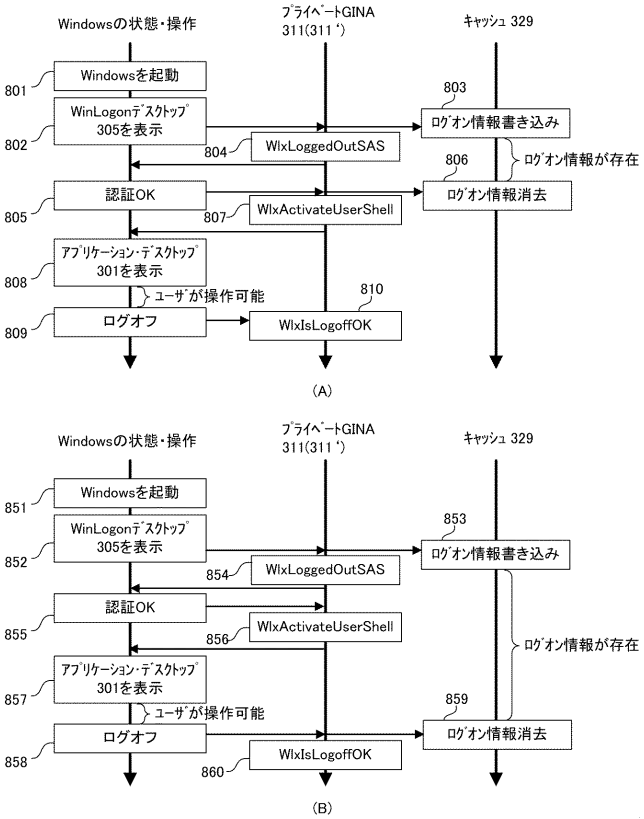
【図１０】



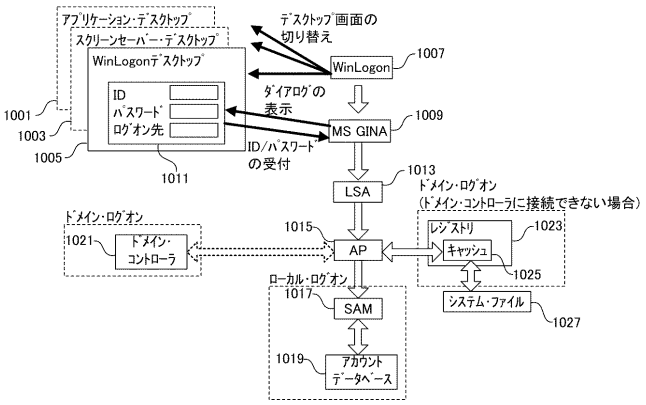
【図１１】



【図１２】



【図１３】



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 井上 忠宣
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 東京基礎研究所内
(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

Ｆターム(参考) 5B017 AA03 BA08
5B276 FB05
5B285 AA01 BA08 CA02 CA41 CA47 CB02 CB53 CB56 CB63 CB72
CB85 CB94