(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3658189号
(P3658189)
(45)発行日　平成17年6月8日(2005.6.8)　(24)登録日　平成17年3月18日(2005.3.18)

| (51)Int.Cl.[7] | F I | | |
|---|---|---|---|
| G06F 1/00 | G06F | 1/00 | 370E |
| G06F 3/08 | G06F | 3/08 | C |
| G06F 15/00 | G06F | 15/00 | 330G |
| G06K 19/10 | G06K | 19/00 | R |

請求項の数 5　(全 7 頁)

(21)出願番号　特願平10-155119
(22)出願日　平成10年4月20日(1998.4.20)
(65)公開番号　特開平11-305867
(43)公開日　平成11年11月5日(1999.11.5)
審査請求日　平成14年3月13日(2002.3.13)

(73)特許権者　597115082
システムニーズ株式会社
東京都港区芝２丁目３番３号
(74)代理人　100093104
弁理士　船津　暢宏
(74)代理人　100092772
弁理士　阪本　清孝
(72)発明者　中山　恵介
東京都港区芝浦４－９－２１

審査官　田中　友章

(56)参考文献　特開平０２－２３４２６０（ＪＰ，Ａ）
特開平０５－０６２０２８（ＪＰ，Ａ）
特開平０５－３１３７７２（ＪＰ，Ａ）
最終頁に続く

(54)【発明の名称】コンピュータ装置におけるなりすまし防止方法

(57)【特許請求の範囲】

【請求項１】

コンピュータ装置において、

当該コンピュータ装置に接続するＩＣカード装置にＩＣカードが挿入されていることが検出されると、前記ＩＣカードに記憶されているユーザＩＤ、パスワードを読み込み、当該読み込んだユーザＩＤ、パスワードを用いてログイン処理を行い、

ログインが成功した場合、スクリーンセーバで処理をロックされた場合の当該ロックを解除するためにアクセスカウンタ又はタイムスタンプを当該コンピュータ装置内及び前記ＩＣカードに記憶し、コンピュータ装置を操作可能な状態とし、

設定された時間内に何らかの操作がなされなければ、前記ＩＣカード装置にＩＣカードが挿入されているかをチェックし、ＩＣカードが挿入されていることが検出されなければ、スクリーンセーバで処理をロックすることを特徴とするコンピュータ装置におけるなりすまし防止方法。

【請求項２】

スクリーンセーバで処理をロックした状態で、前記ＩＣカード装置にＩＣカードが挿入されているかをチェックし、ＩＣカードが挿入されていることが検出されると、当該ＩＣカードからユーザＩＤ及びアクセスカウンタ又はタイムスタンプを読み込み、コンピュータ装置内に記憶したユーザＩＤ及びアクセスカウンタ又はタイムスタンプとを照合し、照合結果が正しければ、前記処理のロック前のコンピュータ装置が操作可能な状態に戻ることを特徴とする請求項１記載のコンピュータ装置におけるなりすまし防止方法。

【請求項３】
コンピュータ装置において、
当該コンピュータ装置に接続するＩＣカード装置にＩＣカードが挿入されていることが検出されると、ＩＣカードの製造元チェックなどのセキュリティチェックを行い、当該チェックが正常であれば、前記ＩＣカードに記憶されているユーザＩＤ、パスワードを読み込み、当該読み込んだユーザＩＤ、パスワードを用いてログイン処理を行い、
ログインが成功した場合、スクリーンセーバで処理をロックされた場合の当該ロックを解除するためにアクセスカウンタ又はタイムスタンプを当該コンピュータ装置内及び前記ＩＣカードに記憶し、コンピュータ装置を操作可能な状態とし、
設定された時間内に何らかの操作がなされなければ、前記ＩＣカード装置にＩＣカードが挿入されているかをチェックし、ＩＣカードが挿入されていることが検出されなければ、スクリーンセーバで処理をロックすることを特徴とするコンピュータ装置におけるなりすまし防止方法。
【請求項４】
スクリーンセーバで処理をロックした状態で、前記ＩＣカード装置にＩＣカードが挿入されているかをチェックし、ＩＣカードが挿入されていることが検出されると、ＩＣカードの製造元チェックなどのセキュリティチェックを行い、当該チェックが正常であれば、当該ＩＣカードからユーザＩＤ及びアクセスカウンタ又はタイムスタンプを読み込み、コンピュータ装置内に記憶したユーザＩＤ及びアクセスカウンタ又はタイムスタンプとを照合し、照合結果が正しければ、前記処理のロック前のコンピュータ装置が操作可能な状態に戻ることを特徴とする請求項３記載のコンピュータ装置におけるなりすまし防止方法。
【請求項５】
コンピュータ装置において、ＩＣカードに記憶されたユーザＩＤ及びアクセスカウンタ又はタイムスタンプと前記コンピュータ装置内に記憶されたユーザＩＤ及びアクセスカウンタ又はタイムスタンプとを照合し、照合結果が正しければ、生物個体を識別するバイオメトリックスによる認証を行い、正規ユーザと認証されれば、処理のロック前のコンピュータ装置が操作可能な状態に戻ることを特徴とする請求項２又は４記載のコンピュータ装置におけるなりすまし防止方法。
【発明の詳細な説明】
【０００１】
【発明に属する技術分野】
この発明は、コンピュータを使用する際に正規の権限者でない人によるログインやログイン後のなりすましを防止するセキュリティシステムに関する。
【０００２】
【従来の技術】
一般的なオペレーティングシステムレベルが提供するコンピュータセキュリティは、主にユーザ管理とそのユーザ（グループ）が使用できる資源アクセス制限管理によるものである。ユーザ認証方法の多くは、ユーザＩＤとそのユーザを結びつけるためのパスワード入力による照合チェックで行うものである。また、ログイン後におけるなりすましを防止する機能は一般的なオペレーティングシステムレベルでは提供されていない。
【０００３】
設定した時間内に操作が何もされない場合に画面（スクリーン）を変えて全ての処理をロックさせる機能をもつスクリーンセーバソフトウェアは、設定されたパスワードを入力しなければ再開できないという機能を持つものも存在するが、ログインしたユーザとは無関係で動作している。
【０００４】
【発明が解決しようとする課題】
しかしながら、セキュリティを考える場合にはパスワードによるユーザ認証やスクリーンセーバによる方法を用いても次のような問題があった。
（ア）パスワードが盗まれたり漏洩した場合に、不正使用されて正規のユーザが被害を被

ることや不正のユーザに不正利益を与えること。
（イ）パスワードの代わりに物理的複製が可能な磁気カードなどの記録媒体を使用してユーザ認証をする場合に、不正使用されて正規のユーザが被害を被ることや不正のユーザに不正利益を与えること。
（ウ）パスワード管理についてはユーザの記憶に依存しなければならなく、メモしていたり付箋に記入しモニタに貼ってあったりなどしていてセキュリティの意味をなしていない。
（エ）パスワードを一定期間で変更する方法でセキュリティを高める場合において、変更や配布作業時間やコスト負担が発生すること。また、配布先での管理が徹底できていないこと。
（オ）セキュリティを保つために、１度ログインしてから席を離れる場合やコンピュータを使用しない場合にはその都度ログアウトしなければならないが、習慣上誰も実行されていないこと。
（カ）外注やアルバイトなどに対して臨時のコンピュータアクセスを許可場合に、登録や設定作業の負担があったり時間がかかり不便であること。さらに、臨時作業が終了した場合にユーザ削除やパスワード変更などの負担も発生すること。
（キ）特定のコンピュータを特定のユーザだけが使用できるように制限する場合において、パスワード管理では不正にアクセスされること。
【０００５】
そこで、本発明は、ログインに関するユーザ認証でユーザの唯一性を保証しログイン後のログインユーザの操作継続性を保証することで不正アクセスを防止することを目的とする。さらに、セキュリティ管理を容易にし工数およびコストを削減すること、ユーザの操作性を容易にすることも可能とする。
【０００６】
【課題を解決するための手段および発明の効果】
【０００７】
この発明に係わる手段は、ログイン時にユーザの唯一性が保証された認証方法による処理とログアウトするまでの一定時間経過後のユーザ認証処理で構成し、その処理結果の整合性によりログイン時からの同一ユーザの操作継続性を保証することで「なりすまし」の防止機能を実現する（図１）。
【０００８】
ログイン時にユーザの唯一性を保証する認証方法には、ユーザＩＤやパスワードなどの入力をキーボードからではなく（図２）、ＩＣカードから読み込んでログインができる機能とする。（図３）これは、ＩＣカードの持つカードアクセス制御やデータ暗号化の高度なセキュリティ機能で物理的な複製や不正なデータ読み書きを困難としているからである。したがって、ＩＣカードの厳密な発行管理だけでユーザの唯一性が保証されることになり、正規ユーザ以外の不正ユーザのアクセスを防止することができるのである。ただし、ＩＣカードではユーザ本人であるかは所有管理の問題となるが、指紋認証や音声認識などの生物個体を識別するバイオメトリックスによる認証方法と組み合わせると厳密なユーザの唯一性を保証できる。
また、ユーザは記憶に頼るパスワード管理やキーボード入力から開放されることになる。さらに、特定コンピュータと特定ユーザの関係を厳密に制限できるようになる。例えば、経理用コンピュータには経理課だけのユーザＩＤを持った人しか使用できないなど。
【０００９】
ログアウトするまでの一定時間経過後のユーザ認証処理には、一定時間経過後に起動するスクリーンセーバの処理ロックを解除するのにＩＣカード認証を採用する。ログイン時からの同一ユーザによる処理継続性を保証するには、同一ユーザであること、ログアウトがされていないこと、ＩＣカードが差し替えられていないことが保証される必要がある。そこで、ログイン時のＩＣカードから読み込んだ情報をコンピュータ内部に記録しておき、さらにアクセスカウンタやタイムスタンプなどをＩＣカードおよびコンピュータ内部に記

録しておく。次にスクリーンセーバのロック解除時にＩＣカードから読み込まれる情報がコンピュータの内部に記録されたものと一致する場合に限り同一ＩＣカードでログアウトされていないことが保証されることになる。したがって、ＩＣカードによるユーザの唯一性と同一ユーザによる操作継続性が保証されることになり、なりすましを防止することができる。また、操作性においては、処理中断時にログアウトせずに、ＴＣカードを抜くだけで可能となり再開にはＩＣカードを挿すだけで済むことになる。

【００１０】

ＩＣカードの発行方法において、個々のユーザ単位でなくアクセス権限で分けられる職能単位のグループでユーザを作成しグループのメンバー数の発行をすることもできる。こうすることによって、人事異動時のユーザ毎の設定変更や外注・アルバイトへの臨時アクセス権発行の場合には、職能別に発行したＩＣカードの配布だけで済み、設定変更や発行業務が削減することができる。

【００１１】

【発明の実施の形態】

この発明の一実施形態におけるハードウェア構成（図４）、セキュリティ管理者処理フロー（図５）および操作者処理フロー（図６）を示す。

【００１２】

セキュリティ管理者は、ＩＣカード１をＩＣカード装置２に挿入し、ユーザＩＤ（Ｄ１）、ドメイン名（Ｄ２）、ユーザパスワード（Ｄ３）などのデータをキーボードより入力し、ＩＣカードに書き込む（図５）。ユーザにこのＩＣカードが配布されるが、パスワードは公開されない。

【００１３】

コンピュータの電源オンや再起動を行う前にＩＣカード１をＩＣカード装置２に挿入する。（Ｓ１）

【００１４】

コンピュータの電源オンや再起動によりオペレーティングシステムがロード（Ｓ２）され、ログインプログラムが起動する（Ｓ３）。その際にＩＣカード１がＩＣカード装置２に挿入されているかのチェックを行う（Ｓ４）。もし挿入されていない場合にはＩＣカード挿入指示画面が表示され確認入力を待つ（Ｓ５）。ＩＣカードを検出するまで無限ループで待機する。

【００１５】

ＩＣカード１が検出されると、ＩＣカードの製造元チェックを行う（Ｓ６）。

【００１６】

製造元チェックが正常であれば、ＩＣカード１に記録されているユーザＩＤ（Ｄ１）、ドメイン名（Ｄ２）、パスワード（Ｄ３）などを読み込む。（Ｓ７）

【００１７】

ログインプログラムに、上記処理（Ｓ７）で読み込んだユーザＩＤ（Ｄ１）、ドメイン名（Ｄ２）、ユーザパスワード（Ｄ３）を引き渡し、ログインプログラムを続行する。

【００１８】

ログインが成功した場合には、乱数により発生させたアクセスカウンタ（Ｄ４）をコンピュータ３（Ｓ８）およびＩＣカード１に記録する（Ｓ９）。アクセスカウンタ（Ｄ４）には、乱数でなくタイムスタンプでもよい。

【００１９】

ログアウトされるまで、以下の処理を繰り返す。（Ｓ１０）

【００２０】

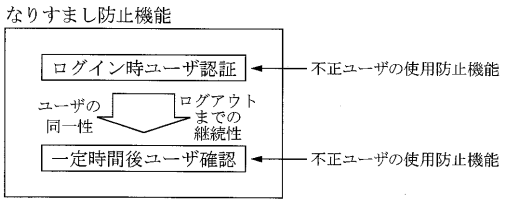
コンピュータの操作をする。（Ｓ１１）

【００２１】

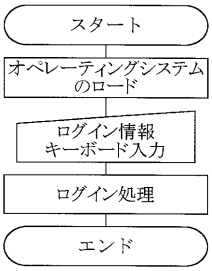
設定された時間内に何らかの操作がされなければ（Ｓ１２）、ＩＣカード１がＩＣカード装置２に挿入されているかをチェックする（Ｓ１３）。もし、検出された場合にはＩＣカードの製造元チェックを行い（Ｓ１４）、検出されない場合にはスクリーンセーバで処理

をロックする（Ｓ１７）。
【００２２】
製造元チェックが正常な場合には、ＩＣカード１から同様にしてユーザＩＤ（Ｄ１）およびアクセスカウンタ（Ｄ４）を読み込む（Ｓ１５）。もし、正常でない場合には、エラー処理をしたあと上記の処理（Ｓ１３）に戻る。
【００２３】
処理（Ｓ８）でコンピュータに記録したユーザＩＤ（Ｄ５）、アクセスカウンタ（Ｄ６）と処理（Ｓ１５）で読み込んだユーザＩＤ（Ｄ１）、アクセスカウンタ（Ｄ４）を照合する（Ｓ１６）。
【００２４】
照合した結果が正しければ、上記の処理（Ｓ１０）の前に戻る。もし、正しくなければ、スクリーンセーバで処理をロックして（Ｓ１７）、上記の処理（Ｓ１３）の前に戻る。
【００２５】
上記の処理（Ｓ１０）の前に戻る。
【図面の簡単な説明】
【図１】「なりしまし」防止機能の構成
【図２】一般的なログインの方法（キーボード入力）
【図３】ＩＣカード自動読込みによるログインの方法
【図４】ハードウェア構成
【図５】セキュリティ管理者によるＩＣカード発行処理フロー
【図６】コンピュータ操作での処理フロー
【図７】ＩＣカードの記録内容とコンピュータ内部の記録内容
【符号の説明】
１…　ＩＣカード
２…　ＩＣカード装置（Ｒ／Ｗ）
３…　コンピュータ

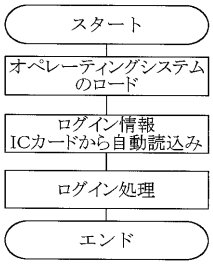
【図１】



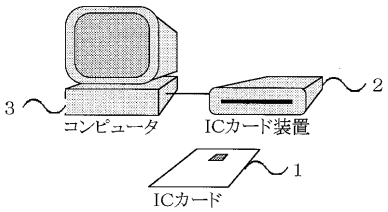

【図２】



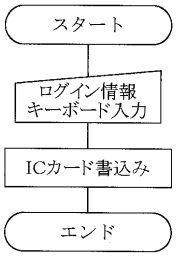

【図３】



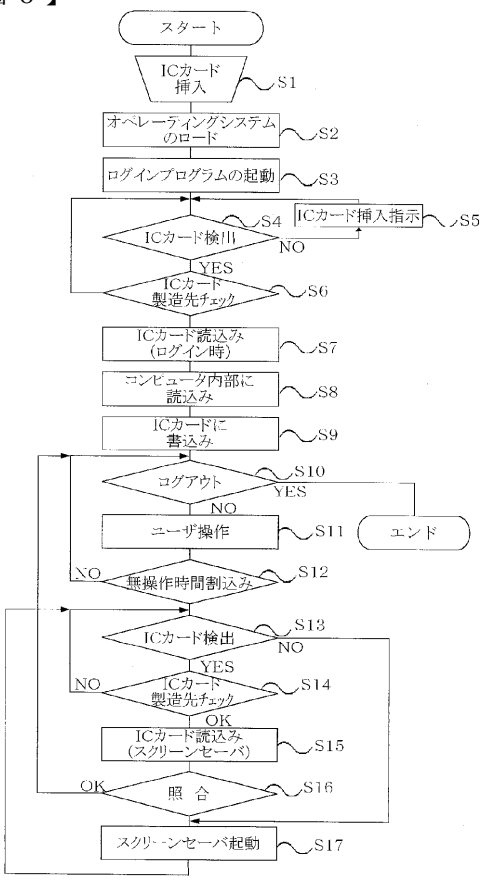

【図４】



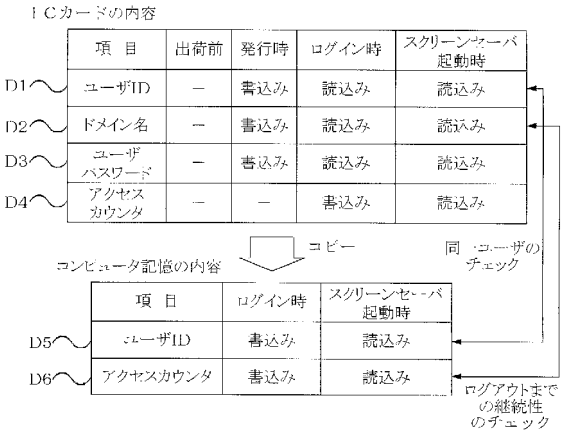

【図５】




【図６】




【図７】



フロントページの続き

(58)調査した分野(Int.Cl.[7], ＤＢ名)

G06F 1/00 370
G06F 3/08
G06F 15/00 330
G06K 19/10