【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19年6月21日(2007.6.21)

【公表番号】特表2003-521758(P2003-521758A)
【公表日】平成15年7月15日(2003.7.15)
【出願番号】特願2000-615873(P2000-615873)
【国際特許分類】
Ｇ０６Ｋ　19/073　(2006.01)
Ｇ０６Ｆ　12/14　(2006.01)
Ｇ０６Ｋ　19/00　(2006.01)
【ＦＩ】
Ｇ０６Ｋ　19/00　Ｐ
Ｇ０６Ｆ　12/14　３２０Ｃ
Ｇ０６Ｆ　12/14　３２０Ｅ
Ｇ０６Ｋ　19/00　Ｑ

【手続補正書】
【提出日】平成19年5月7日(2007.5.7)
【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】　ユーザプロファイルをネットワークとスタンドアロンコンピューティングデバイスとの間で物理的に転送し、前記ネットワークまたはスタンドアロンコンピューティングデバイスのうちの１つに自動的にログオンし、前記ログオンしたネットワークまたはスタンドアロンコンピューティングデバイスを、前記ユーザプロファイルにしたがってユーザ基本設定及びユーザが選択したオペレーティングシステムの特性で自動的に構成するアセンブリであって、該アセンブリは、
物理鍵と通信するインタフェースと、前記ユーザプロファイルを安全に保持する安全なメモリとを有する可搬型プロファイルストレージデバイスと、
前記物理鍵がパスコード起動され、前記インタフェースと連結される場合に、前記メモリ内の前記ユーザプロファイルに交互にアクセスできるようにし、前記インタフェースから取り外された場合に、前記ユーザプロファイルにアクセスできないようにする、前記ユーザに関連する取り外し可能なパスコード起動物理鍵と
を備え、
前記可搬型プロファイルストレージデバイスは、コンピューティングデバイスと連結すると、前記ユーザプロファイルを前記コンピューティングデバイスにアクセス可能にし、前記物理鍵は、前記インタフェースと連結し、ユーザパスコードは前記物理鍵を起動し、
前記物理鍵はまず、前記ユーザを認証し、次いで前記可搬型プロファイルストレージデバイスを認証し、次いで前記ユーザを前記コンピューティングデバイスに自動的にログオンさせ、次いで前記コンピューティングデバイスを、前記ユーザプロファイルからの前記ユーザ基本設定及び前記ユーザが選択したオペレーティングシステムの特性で自動的に構成する
ことを特徴とするアセンブリ。
【請求項２】　前記デバイスは、前記ユーザプロファイルがアクセス可能にされた場合にアクセス可能にされるユーザのデータを、安全に記憶することを特徴とする請求項１に記載のアセンブリ。

【請求項３】　前記可搬型プロファイルストレージデバイスは公開暗号鍵を記憶し、前記物理鍵は対応する秘密復号鍵を記憶し、前記公開鍵と前記秘密鍵が関連付けられていることを確認すると、前記安全なメモリ内の前記ユーザプロファイルへのアクセスが可能になり、前記ユーザパスコードは前記物理鍵を起動することを特徴とする請求項１に記載のアセンブリ。

【請求項４】　ユーザと関連付けられたパスコードを記憶する記憶カードと、

ＰＣＭＣＩＡカードのフォームファクタで構成され、前記記憶カードと通信するためのインタフェース、およびユーザのプロファイルを記憶するメモリを有するＰＣＭＣＩＡデバイスとを備えたプロファイルキャリアであって、

パスコード確認によって前記記憶カードでユーザを認証すると、前記ＰＣＭＣＩＡデバイスのメモリ内の前記ユーザプロファイルへのアクセスを前記アセンブリが許可することを特徴とするプロファイルキャリア。

【請求項５】　前記記憶カードはスマートカードを備えたことを特徴とする請求項４に記載のプロファイルキャリア。

【請求項６】　前記メモリはフラッシュメモリを備えたことを特徴とする請求項４に記載のプロファイルキャリア。

【請求項７】　前記ＰＣＭＣＩＡデバイスはデータファイルも記憶することを特徴とする請求項４に記載のプロファイルキャリア。

【請求項８】　前記ＰＣＭＣＩＡデバイスは公開鍵を記憶し、前記記憶カードはそれに対応する秘密鍵を記憶し、前記公開鍵と前記秘密鍵が関連付けられていることが確認されると、前記ＰＣＭＣＩＡデバイスのメモリ内の前記ユーザプロファイルへのアクセスを前記アセンブリが許可することを特徴とする請求項４に記載のプロファイルキャリア。

【請求項９】　パスコード、および秘密／公開鍵ペアの秘密鍵を記憶するスマートカードと、

ＰＣＭＣＩＡカードのフォームファクタで構成され、前記スマートカードと通信するためのインタフェースと、ユーザデータおよび前記秘密／公開鍵ペアの公開鍵を記憶するフラッシュメモリとを有するＰＣＭＣＩＡデバイスとを備え、

ユーザが入力したパスコードを記憶パスコードを用いて確認した後で、前記秘密鍵の使用を許可するようにスマートカードが構成され、

さらに、前記秘密鍵を使用して、前記ＰＣＭＣＩＡデバイスのメモリに記憶されている前記公開鍵を認証するように前記スマートカードが構成され、

前記スマートカードで前記公開鍵の認証に成功すると、前記メモリに記憶されているユーザデータへのアクセスを許可するように前記ＰＣＭＣＩＡデバイスが構成されることを特徴とするアセンブリ。

【請求項１０】　前記ＰＣＭＣＩＡデバイスは、コンピュータの構成に使用するユーザプロファイルも記憶することを特徴とする請求項９に記載のアセンブリ。

【請求項１１】　ＰＣＭＣＩＡカードのフォームファクタで構成され、記憶カードから情報を読み出すように構成されたカードリーダと、

前記カードリーダ中に常駐し、ユーザデータを記憶するデータメモリと、

記憶カードからのアクセスを可能にする情報を受け取った前記カードリーダに応答して、前記データメモリ中のユーザデータへのアクセスを可能にする、カードリーダ内に常駐するコントローラと

を備えたことを特徴とするデバイス。

【請求項１２】　前記データメモリはフラッシュメモリを備えたことを特徴とする請求項１１に記載のデバイス。

【請求項１３】　前記データメモリは、コンピュータの構成に使用されるユーザプロファイルを記憶することを特徴とする請求項１１に記載のデバイス。

【請求項１４】　請求項１１に記載のデバイスと、

前記カードリーダにインタフェースすること、および前記カードリーダから取り外すことが交互にできる記憶カードとを備えたことを特徴とするアセンブリ。

【請求項１５】　ＰＣＭＣＩＡデバイスリーダを有するコンピュータと、
前記コンピュータがデバイスにあるユーザデータにアクセスすることができるように、前記ＰＣＭＣＩＡデバイスリーダを介して前記コンピュータとインタフェースされる請求項１４に記載のアセンブリと
を備えたことを特徴とするコンピュータシステム。
【請求項１６】　フラッシュメモリを備えたことを特徴とするＰＣＭＣＩＡスマートカードリーダ。
【請求項１７】　請求項１６に記載のＰＣＭＣＩＡスマートカードリーダと、
前記スマートカードリーダにインタフェースすること、および前記スマートカードリーダから取り外すことが交互にできるスマートカードと
を備えたことを特徴とするアセンブリ。
【請求項１８】　ＰＣＭＣＩＡデバイスリーダを有するコンピュータと、
前記ＰＣＭＣＩＡデバイスリーダを介して前記コンピュータとインタフェースされる請求項１７に記載のアセンブリと
を備えたことを特徴とするコンピュータシステム。
【請求項１９】　可搬型スマートカードで安全保護されたメモリアセンブリ内のユーザ証明、ユーザ基本設定、及びユーザが選択したオペレーティングシステムの特徴を記憶するコンピュータシステムであって、ユーザを、様々なネットワーク及びスタンドアロンコンピューティングデバイスに自動的にログオンさせ、前記ログオンしたネットワークまたはスタンドアロンコンピューティングデバイスのうちの１つを、前記ユーザ基本設定及びユーザが選択したオペレーティングシステムの特性で自動的に構成する前記コンピュータシステムは、
可搬型デバイスリーダを有するコンピュータと、
前記コンピュータ中の前記可搬型デバイスリーダと互換的にインタフェースするためのスマートカードで安全保護されたメモリアセンブリであって、ユーザプロファイルと、存在し、パスコードによって起動された場合は前記ユーザプロファイルにアクセスを交互に可能にし、取り外された場合は前記ユーザプロファイルへのアクセスを不可能にするパスコードで保護された取り外し可能なスマートカードを有する前記スマートカードで安全保護されたメモリアセンブリと
を備え、
前記スマートカードはまず、前記ユーザを認証し、次いで前記ユーザプロファイルを認証し、次いで前記ユーザを前記コンピュータに自動的にログオンさせ、次いで前記コンピュータを、前記ユーザプロファイルからの前記ユーザ基本設定及び前記ユーザが選択したオペレーティングシステムの特性で自動的に構成する
ことを特徴とするコンピュータシステム。
【請求項２０】　前記データメモリはフラッシュメモリを備えたことを特徴とする請求項１９に記載のコンピュータシステム。
【請求項２１】　前記スマートカードはパスコードを記憶し、ユーザデータへのアクセスを可能にする条件として、前記コンピュータに入力されるユーザ提供のパスコードを認証するように前記スマートカードが構成されることを特徴とする請求項１９に記載のコンピュータシステム。
【請求項２２】　前記スマートカードは第１の鍵を記憶し、
前記データメモリは、第１の鍵と関連付けられた第２の鍵を記憶し、
ユーザデータへのアクセスを可能にする条件として、前記第１の鍵を使用してデータメモリからの前記第２の鍵を認証するように前記スマートカードが構成されることを特徴とする請求項１９に記載のコンピュータシステム。
【請求項２３】　前記スマートカードは、パスコード、および公開／秘密鍵ペアの秘密鍵を記憶し、
前記データメモリは、公開／秘密鍵ペアの公開鍵を記憶し、
前記秘密鍵へのアクセスを可能にする条件として、前記コンピュータに入力されるユー

ザ提供のパスコードを認証し、かつユーザデータへのアクセスを可能にする条件として、前記秘密鍵を使用してデータメモリからの前記公開鍵を認証するように前記スマートカードが構成されることを特徴とする請求項１９に記載のコンピュータシステム。

【請求項２４】　ＰＣＭＣＩＡデバイスリーダを有するコンピュータと、

前記コンピュータ内のＰＣＭＣＩＡデバイスリーダと互換的にインタフェースするためにＰＣＭＣＩＡカードのフォームファクタを有する、コンピュータの構成用のユーザプロファイルを移植するための可搬型プロファイルキャリアであって、

（ａ）ユーザと関連付けられた記憶カードと、

（ｂ）前記記憶カードと通信するためのインタフェース、およびユーザプロファイルを記憶するデータメモリを有し、前記記憶カードが記憶カードリーダのデータメモリにあるユーザデータへのアクセスを可能にする記憶カードリーダとを備えるプロファイルキャリアとを備えたコンピュータシステムであって、

前記プロファイルキャリアは前記ＰＣＭＣＩＡデバイスリーダを介して前記コンピュータとインタフェースされると、前記コンピュータを構成するためにユーザプロファイルへのアクセスが可能になることを特徴とするコンピュータシステム。

【請求項２５】　前記データメモリはフラッシュメモリを有することを特徴とする請求項２４に記載のコンピュータシステム。

【請求項２６】　前記記憶カードはスマートカードを有することを特徴とする請求項２４に記載のコンピュータシステム。

【請求項２７】　前記スマートカードはパスコードを記憶し、ユーザプロファイルへのアクセスを可能にする条件として、前記コンピュータに入力されたユーザ提供のパスコードを認証するように前記スマートカードが構成されることを特徴とする請求項２６に記載のコンピュータシステム。

【請求項２８】　前記スマートカードは第１の鍵を記憶し、

前記記憶カードリーダは前記第１の鍵と関連付けられた第２の鍵を記憶し、

ユーザプロファイルへのアクセスを可能にする条件として、前記第１の鍵を使用して、前記記憶カードリーダから渡された前記第２の鍵を認証するように前記スマートカードが構成されることを特徴とする請求項２６に記載のコンピュータシステム。

【請求項２９】　前記スマートカードは、パスコード、および公開／秘密鍵ペアの秘密鍵を記憶し、

前記記憶カードリーダは前記公開／秘密鍵ペアの公開鍵を記憶し、

前記秘密鍵へのアクセスを可能にする条件として、前記コンピュータに入力されたユーザ提供のパスコードを認証し、かつユーザプロファイルへのアクセスを可能にする条件として、前記秘密鍵を使用して、前記記憶カードリーダから渡された公開鍵を認証するように前記スマートカードが構成されることを特徴とする請求項２６に記載のコンピュータシステム。

【請求項３０】　カードで安全保護されたプロファイルキャリアのデータメモリにユーザプロファイルを記憶し、該カードで安全保護されたプロファイルキャリアは、データメモリを備えたＰＣＭＣＩＡカードのフォームファクタによるリーダ構成要素と、前記リーダ構成要素とインタフェースされると、前記データメモリ内のユーザプロファイルへのアクセスを選択的に可能にするカード構成要素とを有すること、

前記カード構成要素を前記リーダ構成要素とインタフェースさせて、カードで安全保護されたプロファイルキャリアを形成すること、

カードで安全保護されたプロファイルキャリアをコンピュータとインタフェースさせること、および

コンピュータの構成に使用するユーザプロファイルを前記データメモリから読み出すこと

を含むことを特徴とするコンピュータにユーザプロファイルを移植する方法。

【請求項３１】　カードで安全保護されたプロファイルキャリアを別の第２コンピュータとインタフェースさせ、前記第２コンピュータの構成に使用するユーザプロファイル

を前記データメモリから読み出すことをさらに含むことを特徴とする請求項３０に記載の方法。

【請求項３２】　ユーザデータをカードリーダに記憶すること、

前記カードリーダに記憶されたユーザデータへのアクセスを可能にするアクセスクリデンシャルを記憶カードに記憶すること、

前記記憶カードを前記カードリーダとインタフェースさせること、および

前記記憶カードから前記アクセスクリデンシャルを読み出して、ユーザデータへのアクセスを可能にすることを含むことを特徴とする方法。

【請求項３３】　カードリーダ中に取り付けられたメモリにユーザデータを記憶すること、

リーダ常駐の鍵を前記カードリーダのメモリに記憶すること、

リーダ常駐鍵に対応するカード常駐鍵をＩＣ（集積回路）カードに記憶すること、

パスコードを前記ＩＣカードに記憶すること、

前記ＩＣカードを前記カードリーダとインタフェースさせること、

ユーザが入力したパスコードを受け取ること、

前記ＩＣカードに記憶したパスコードを使用してユーザ入力のパスコードを確認した後、前記カード常駐鍵の使用を許可すること、

前記リーダ常駐鍵を前記カードリーダから前記ＩＣカードに渡すこと、

前記カード常駐鍵を使用してＩＣカード部で前記リーダ常駐鍵を認証すること、および

前記リーダ常駐鍵の認証に成功すると、前記カードリーダのメモリに記憶されたユーザデータへのアクセスを許可することを含むことを特徴とする方法。

【請求項３４】　ＰＣＭＣＩＡデバイスリーダを備えたコンピュータと、前記コンピュータ中の前記ＰＣＭＣＩＡデバイスリーダと互換的にインタフェースするためのＰＣＭＣＩＡカードのフォームファクタを有するスマートカードで安全保護されたプロファイルキャリアとを有するシステムにおいて、前記スマートカードで安全保護されたプロファイルキャリアは、ユーザプロファイルを記憶するメモリ、および取り外し可能スマートカードを有し、プロファイルキャリアに常駐するコンピュータ可読媒体は、

ユーザ提供のパスコードをコンピュータから受け取ること、

プロファイルキャリアに記憶されたパスコードを用いてユーザ提供のパスコードを認証すること、

ユーザ提供のパスコードの認証に成功すると、プロファイルキャリアにある秘密鍵へのアクセスを可能にすること、

秘密鍵を使用して、メモリと関連付けられた公開鍵を認証すること、および

公開鍵の認証に成功すると、メモリ中のユーザプロファイルへのアクセスを可能にすることを含む実行可能命令を有することを特徴とするシステム。

【請求項３５】　ＰＣＭＣＩＡデバイスリーダを備えたコンピュータと、前記コンピュータ内の前記ＰＣＭＣＩＡデバイスリーダと互換的にインタフェースするためのＰＣＭＣＩＡカードのフォームファクタを有するスマートカードで安全保護されたプロファイルキャリアとを有するシステムにおいて、前記スマートカードで安全保護されたプロファイルキャリアは、ユーザプロファイルを記憶するメモリ、および取り外し可能スマートカードを有し、スマートカード部のコンピュータ可読媒体は、

ユーザ提供のパスコードをコンピュータから受け取ること、

スマートカードに記憶されたパスコードを用いて、ユーザ提供のパスコードを認証すること、

ユーザ提供のパスコードの認証に成功すると、スマートカードにある秘密鍵へのアクセスを可能にすること、

メモリから公開鍵を受け取ること、

秘密鍵を使用して公開鍵を認証すること、および

公開鍵の認証に成功すると、プロファイルキャリアのメモリ中のユーザプロファイルへのアクセスを可能にすることを含む実行可能命令を有することを特徴とするシステム。

【請求項３６】　前記スマートカードで安全保護されたメモリアセンブリは、前記ユーザプロファイルを記憶するＵＳＢ準拠のメモリを備えることを特徴とする請求項１９に記載のコンピュータシステム。

【請求項３７】　前記メモリは公開鍵を記憶し、前記物理鍵は対応する秘密鍵を記憶し、前記メモリ内に記憶された前記ユーザプロファイルへのアクセスは、前記物理鍵が前記メモリと連結し、前記公開鍵及び前記秘密鍵の関連が確認され、前記正しいパスコードが入力された場合に、可能になることを特徴とする請求項３６に記載のアセンブリ。

【請求項３８】　前記メモリはパブリック領域及びプライベート領域を有し、前記プライベート領域は、データファイルをさらに記憶することを特徴とする請求項３６に記載のアセンブリ。

【請求項３９】　前記データファイルは、前記ユーザプロファイル及びその他のデータファイルを含むことを特徴とする請求項３８に記載のアセンブリ。

【請求項４０】　コンピューティングネットワークとスタンドアロンコンピューティングデバイスとの間でコンピューティングデバイスユーザのプロファイルを物理的に転送する、アセンブリ上の個人情報キャリアであって、該個人情報キャリアは、

データファイルを記憶する取外し可能な手段と、

前記コンピューティングネットワーク及び前記スタンドアロンコンピューティングデバイスを通信的に連結し、及び非連結にする、前記取外し可能な手段上のインタフェースと、

前記取外し可能な手段に通信的に接続した場合に、前記取外し可能な手段上のデータファイルへの、パスコードで保護されたアクセスを可能にするもう１つの取外し可能な手段と

を備え、

前記取外し可能な手段はフラッシュメモリを含み、前記データファイルは、前記コンピューティングネットワーク及び前記スタンドアロンコンピューティングデバイスを構成するユーザプロファイルを含み、

前記もう１つの取外し可能な手段はまず、前記ユーザを認証し、次いで前記取外し可能な手段を認証し、次いで前記ユーザを前記コンピューティングデバイスに自動的にログオンさせ、次いで前記コンピューティングデバイスを、前記ユーザプロファイルからのユーザ基本設定及びユーザが選択したオペレーティングシステムの特性で自動的に構成することを特徴とする個人情報キャリア。

【請求項４１】　前記もう１つの取外し可能な手段はパスコードを記憶し、前記取外し可能な手段内に記憶された前記データファイルへのアクセスは、前記もう１つの取外し可能な手段上に記憶されたパスコードについて、ユーザが供給するパスコードを確認すると可能になることを特徴とする請求項４０に記載のアセンブリ。

【請求項４２】　前記取外し可能な手段は公開鍵を記憶し、前記もう１つの取外し可能な手段は対応する秘密鍵を記憶し、前記取外し可能な手段内に記憶されたデータファイルへのアクセスは、前記公開鍵と前記秘密鍵が関連することを確認すると可能になることを特徴とする請求項４０に記載のアセンブリ。

【請求項４３】　コンピューティングデバイス間でコンピューティングデバイスユーザのプロファイルを物理的に転送する安全な装置であって、該安全な装置は、

前記プロファイルを記憶し、暗号鍵ペアの公開鍵を記憶する記憶領域と、

前記コンピューティングデバイスのうちの１つと通信的に連結する第１のインタフェースと、

第２のインタフェースと

を備える第１の可搬型ストレージデバイスと、

前記暗号鍵ペアの秘密鍵を記憶する記憶領域と、

前記ユーザからのパスコードを確認する認証装置と

を備える前記第２のインタフェースと連結することができる第２の可搬型ストレージデバイスと

を備え、
前記安全な装置は、前記安全な装置に通信的に連結されている前記コンピューティングデバイスと、前記公開鍵に関連する前記秘密鍵と、前記ユーザから受け取った前記パスコードを確認する前記認証装置とに応答して、前記プロファイルを前記コンピューティングデバイスにアップロードし、
前記第２の可搬型ストレージデバイスは前記ユーザを認証し、次いで前記第１の可搬型ストレージデバイスを認証し、次いで前記ユーザを前記コンピューティングデバイスのうちの１つに自動的にログオンさせ、次いで前記ログオンしたコンピューティングデバイスを、前記プロファイルからのユーザ基本設定及びユーザが選択したオペレーティングシステムの特性で自動的に構成する
ことを特徴とする安全な装置。
【請求項４４】　前記コンピューティングデバイスに連結された取外し可能なデバイスが、前記第２の可搬型ストレージデバイス連結された前記第１の可搬型ストレージデバイスであるかどうかを検出する、前記コンピューティングデバイスのうちの１つに含まれるドライバをさらに備えることを特徴とする請求項４３に記載の安全な装置。
【請求項４５】　前記安全な装置が前記コンピューティングデバイスに連結され、前記第２の可搬型ストレージデバイスが前記第１の可搬型ストレージデバイスに連結されることを確認し、前記ユーザを自動的にログオンさせる、前記コンピューティングデバイスのうちの１つに含まれるログオンモジュールをさらに備えることを特徴とする請求項４３に記載の安全な装置。