(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6258205号
(P6258205)
(45)発行日　平成30年1月10日(2018.1.10)　(24)登録日　平成29年12月15日(2017.12.15)

(51)Int.Cl.　F I
G06F 21/32 (2013.01)　G06F 21/32

請求項の数 26　(全 34 頁)

(21)出願番号	特願2014-533527 (P2014-533527)
(86)(22)出願日	平成24年8月6日 (2012.8.6)
(65)公表番号	特表2014-535090 (P2014-535090A)
(43)公表日	平成26年12月25日 (2014.12.25)
(86)国際出願番号	PCT/US2012/049760
(87)国際公開番号	WO2013/048621
(87)国際公開日	平成25年4月4日 (2013.4.4)
審査請求日	平成27年8月5日 (2015.8.5)
審判番号	不服2016-8607 (P2016-8607/J1)
審判請求日	平成28年6月9日 (2016.6.9)
(31)優先権主張番号	13/247,652
(32)優先日	平成23年9月28日 (2011.9.28)
(33)優先権主張国	米国 (US)

早期審査対象出願

(73)特許権者　502208397
グーグル　エルエルシー
アメリカ合衆国　カリフォルニア州　９４０４３　マウンテン　ビュー　アンフィシアター　パークウェイ　１６００
(74)代理人　110001195
特許業務法人深見特許事務所
(72)発明者　松岡　良倫
アメリカ合衆国、カリフォルニア州　９５０１４、クパチーノ、スタンダール　レーン　８２１

最終頁に続く

(54)【発明の名称】顔認識に基づくコンピューティング・デバイスへのログイン

(57)【特許請求の範囲】
【請求項１】
第１のユーザをコンピューティング・デバイスにログインさせる方法であって、
前記コンピューティング・デバイスに動作可能に結合されたカメラを介して前記第１のユーザの第１の画像を受信すること、
前記受信した第１の画像に基づいて前記第１のユーザの身元を判別すること、
前記第１のユーザの前記判別された身元が第１の所定の身元と一致する場合に、少なくとも前記第１のユーザの前記身元が前記第１の所定の身元と一致することに基づいて、前記第１のユーザを前記コンピューティング・デバイスにログインさせること、
前記コンピューティング・デバイスに動作可能に結合されたカメラを介して第２のユーザの顔の第２の画像を受信すること、
前記受信した第２の画像に基づいて前記第２のユーザの身元を判別すること、
前記第１のユーザが前記カメラの検出エリア内に存在し、前記第１のユーザのログイン中に、前記第２のユーザの前記判別された身元が第２の所定の身元と一致する場合に、前記第１のユーザ及び前記第２のユーザに対して、前記第１のユーザを前記コンピューティング・デバイスからログアウトさせ及び前記第２のユーザを前記コンピューティング・デバイスにログインさせることを確認する指示を発行すること、を含み、
前記指示は、さらに、前記第２のユーザを前記コンピューティング・デバイスにログインさせるための条件として前記第２のユーザに英数字情報を提供するよう指示することなく、当該第２のユーザにジェスチュアを提供するよう指示し、

前記指示に応じて、前記コンピューティング・デバイスのタッチ・センシティブ・エリア内で所定のジェスチュアと一致するジェスチュアを受信すること、及び、
受信した前記ジェスチュアに応じて、前記第１のユーザを前記コンピューティング・デバイスからログアウトさせ及び前記第２のユーザを前記コンピューティング・デバイスにログインさせること、
を含む、方法。
【請求項２】
前記カメラが前記コンピューティング・デバイスと物理的に統合されている、請求項１に記載の方法。
【請求項３】
前記第１のユーザの前記判別された身元が前記第１の所定の身元と一致する場合に、前記ユーザからの英数字入力を要求することなく、前記第１のユーザを前記コンピューティング・デバイスにログインさせる、請求項１又は２に記載の方法。
【請求項４】
前記第１のユーザを前記コンピューティング・デバイスにログインさせることは、前記第１のユーザが前記第１のユーザに関連する第１のリソースであって、前記第１のユーザにとって個人的なドキュメントを含む前記第１のリソースにアクセスすることを許可するが、前記第１のユーザが第２のユーザに関連する第２のリソースにアクセスすることを禁止することを含み、
前記第２のユーザを前記コンピューティング・デバイスにログインさせることは、前記第２のユーザが前記第２のユーザに関連する第２のリソースであって、前記第２のユーザにとって個人的なドキュメントを含む前記第２のリソースにアクセスすることを許可するが、前記第２のユーザが前記第１のユーザに関連する前記第１のリソースにアクセスすることを禁止することを含む、
請求項１～３のいずれか１項に記載の方法。
【請求項５】
前記第２のユーザの前記判別された身元が前記第２の所定の身元と一致しない場合に、前記第２のユーザを前記コンピューティング・デバイスにログインさせるための条件として前記第２のユーザに第１の所定の英数字情報と一致する第１の英数字情報を入力するように要求することをさらに含む、
請求項４に記載の方法。
【請求項６】
前記第１の所定の英数字情報が前記第１のユーザに関連するユーザ名を含む、請求項５に記載の方法。
【請求項７】
前記カメラを介して前記第１のユーザの複数の２次元画像を受信することであって、前記複数の２次元画像は、前記ユーザの顔に対して複数の異なる視点から撮られており、組み合わされて前記ユーザの顔に関する３次元情報を提供するものである、前記第１のユーザの前記複数の２次元画像を受信すること、及び、
受信した前記複数の２次元画像によって提供される、前記ユーザの顔に関する前記３次元情報に基づいて前記第１のユーザの前記身元を判別すること、
をさらに含む、請求項１～６のいずれか１項に記載の方法。
【請求項８】
前記カメラを介して前記第１のユーザの複数の画像を受信することであって、前記複数の画像は組み合わされて前記ユーザの顔面のジェスチュアを定義するものである、前記第１のユーザの複数の画像を受信すること、
受信した前記複数の画像に基づいて及び前記顔面のジェスチュアに基づいて、前記第１のユーザの前記身元を判別すること、及び、
前記判別された身元が前記第１の所定の身元と一致する場合に、前記第１のユーザを前記コンピューティング・デバイスにログインさせること、

をさらに含む、請求項１～７のいずれか１項に記載の方法。
【請求項９】
前記コンピューティング・デバイスが電話を含む、請求項１～８のいずれか１項に記載の方法。
【請求項１０】
前記受信した画像に基づいて前記第１のユーザの前記身元を判別することは、前記ユーザの前記画像における前記ユーザの目、鼻、頬骨及び顎のうちの少なくとも一つの相対位置、サイズ若しくは形状又はこれらの組み合わせのうちの１つまたは複数に基づいて前記第１のユーザの前記身元を判別することを含む、請求項１～９のいずれか１項に記載の方法。
【請求項１１】
前記第１のユーザを前記コンピューティング・デバイスにログインさせた後、
前記第２のユーザの前記判別された身元が、前記第１のユーザの前記身元に一致する前記第１の所定の身元と一致しない場合に、前記第１のユーザを前記コンピューティング・デバイスからログアウトさせることをさらに含む、請求項１～１０のいずれか１項に記載の方法。
【請求項１２】
コンピュータ可読媒体に保存されたコンピュータプログラムであって、実行されたときに、
コンピューティング・デバイスに動作可能に結合されたカメラを介して第１のユーザの第１の画像を受信すること、
前記受信した第１の画像に基づいて前記第１のユーザの身元を判別すること、
前記第１のユーザの前記判別された身元が第１の所定の身元と一致する場合に、少なくとも前記第１のユーザの前記身元が前記第１の所定の身元と一致することに基づいて、前記第１のユーザを前記コンピューティング・デバイスにログインさせること、
前記コンピューティング・デバイスに動作可能に結合されたカメラを介して第２のユーザの顔の第２の画像を受信すること、
前記受信した第２の画像に基づいて前記第２のユーザの身元を判別すること、
前記第１のユーザが前記カメラの検出エリア内に存在し、前記第１のユーザのログイン中に、前記第２のユーザの前記判別された身元が第２の所定の身元と一致する場合に、前記第１のユーザ及び前記第２のユーザに対して、前記第１のユーザを前記コンピューティング・デバイスからログアウトさせ及び前記第２のユーザを前記コンピューティング・デバイスにログインさせることを確認する指示を発行すること、
前記指示は、さらに、前記第２のユーザを前記コンピューティング・デバイスにログインさせるための条件として前記第２のユーザに英数字情報を提供するよう指示することなく、当該第２のユーザにジェスチュアを提供するよう指示し、
前記指示に応じて、前記コンピューティング・デバイスのタッチ・センシティブ・エリア内で所定のジェスチュアと一致するジェスチュアを受信すること、及び、
受信した前記ジェスチュアに応じて、前記第１のユーザを前記コンピューティング・デバイスからログアウトさせ及び前記第２のユーザを前記コンピューティング・デバイスにログインさせること、
をコンピュータ・システムに実行させる命令を含む、
コンピュータプログラム。
【請求項１３】
前記第１のユーザの前記判別された身元が前記第１の所定の身元と一致する場合に、前記ユーザからの英数字入力を要求することなく、前記第１のユーザを前記コンピューティング・デバイスにログインさせる、請求項１２に記載のコンピュータプログラム。
【請求項１４】
前記第１のユーザを前記コンピューティング・デバイスにログインさせることは、前記第１のユーザが前記第１のユーザに関連する第１のリソースであって、前記第１のユーザ

にとって個人的なドキュメントを含む前記第１のリソースにアクセスすることを許可するが、前記第１のユーザが第２のユーザに関連する第２のリソースにアクセスすることを禁止することを含み、
前記第２のユーザを前記コンピューティング・デバイスにログインさせることは、前記第２のユーザが前記第２のユーザに関連する第２のリソースであって、前記第２のユーザにとって個人的なドキュメントを含む前記第２のリソースにアクセスすることを許可し、前記第２のユーザが前記第１のユーザに関連する前記第１のリソースにアクセスすることを禁止することを含む、
請求項１２又は１３に記載のコンピュータプログラム。
【請求項１５】
前記命令は、実行されたときに、
前記第２のユーザの前記判別された身元が前記第２の所定の身元と一致しない場合に、第１の所定の英数字情報と一致する第１の英数字情報と、第２の所定の英数字情報と一致する第２の英数字情報とを入力するよう前記第２のユーザに指示すること、及び、前記第１の英数字情報が前記第１の所定の英数字情報に一致し且つ前記第２の英数字情報が前記第２の所定の英数字情報に一致した場合に前記第２のユーザを前記コンピューティング・デバイスにログインさせること、をコンピュータ・システムにさらに実行させ、
前記第２のユーザの前記判別された身元が前記第２の所定の身元と一致する場合、前記第１のユーザを前記コンピューティング・デバイスからログアウトさせ及び前記第２のユーザを前記コンピューティング・デバイスにログインさせることを確認する前記指示は、さらに、前記第２の所定の英数字情報と一致する前記第２の英数字情報を入力し、前記第１の所定の英数字情報と一致する前記第１の英数字情報を入力しないよう前記第２のユーザに指示することを含む、
請求項１２～１４のいずれか１項に記載のコンピュータプログラム。
【請求項１６】
前記命令は、実行されたときに、
前記カメラを介して前記第１のユーザの複数の２次元画像を受信することであって、前記複数の２次元画像は、前記ユーザの顔に対して複数の異なる視点から撮られており、組み合わされて前記ユーザの顔に関する３次元情報を提供するものである、前記第１のユーザの前記複数の２次元画像を受信すること、及び、
受信した前記複数の２次元画像によって提供される、前記ユーザの顔に関する前記３次元情報に基づいて前記第１のユーザの前記身元を判別すること、
を前記コンピュータ・システムにさらに実行させる、
請求項１２～１５のいずれか１項に記載のコンピュータプログラム。
【請求項１７】
前記命令は、実行されたときに、
前記カメラを介して前記第１のユーザの複数の画像を受信することであって、前記複数の画像は組み合わされて前記ユーザの顔面のジェスチュアを定義するものである、前記第１のユーザの複数の画像を受信すること、
受信した前記複数の画像に基づいて及び前記顔面のジェスチュアに基づいて、前記第１のユーザの前記身元を判別すること、及び、
前記判別された身元が前記第１の所定の身元と一致する場合に、前記第１のユーザを前記コンピューティング・デバイスにログインさせること、
を前記コンピュータ・システムにさらに実行させる、
請求項１２～１６のいずれか１項に記載のコンピュータプログラム。
【請求項１８】
第１のユーザの第１の画像及び第２のユーザの第２の画像を受信するように構成されたカメラと、
受信した前記第１の画像に基づいて前記第１のユーザの身元を判別すると共に、受信した前記第２の画像に基づいて前記第２のユーザの身元を判別するように構成されたユーザ

認識部と、
ログイン制御部と、
を含み、
前記ログイン制御部は、
前記第１のユーザの前記判別された身元が第１の所定の身元と一致する場合に、少なくとも前記第１のユーザの前記身元が前記所定の身元と一致することに基づいて、前記第１のユーザをコンピューティング・デバイスにログインさせ、
前記第１のユーザが前記カメラの検出エリア内に存在し、前記第１のユーザのログイン中に、前記第２のユーザの前記判別された身元が第２の所定の身元と一致する場合に、前記第１のユーザ及び前記第２のユーザに対して、前記第１のユーザを前記コンピューティング・デバイスからログアウトさせ及び前記第２のユーザを前記コンピューティング・デバイスにログインさせることを確認する指示を発行し、
前記指示は、さらに、前記第２のユーザを前記コンピューティング・デバイスにログインさせるための条件として前記第２のユーザに英数字情報を提供するよう指示することなく、当該第２のユーザにジェスチュアを提供するよう指示し、
前記指示に応じて、前記コンピューティング・デバイスのタッチ・センシティブ・エリア内で所定のジェスチュアと一致するジェスチュアを受信し、及び、
受信した前記ジェスチュアに応じて、前記第１のユーザを前記コンピューティング・デバイスからログアウトさせ、前記第２のユーザを前記コンピューティング・デバイスにログインさせる、
ように構成されている、
コンピューティング・デバイス。
【請求項１９】
前記カメラが前記コンピューティング・デバイスと物理的に統合されている、請求項１８に記載のコンピューティング・デバイス。
【請求項２０】
前記カメラは、前記第１のユーザの複数の２次元画像を受信するように構成され、前記複数の２次元画像は、前記ユーザの顔に対して複数の異なる視点から撮られており、組み合わされて前記ユーザの顔に関する３次元情報を提供するものであり、
前記ユーザ認識部は、受信した前記複数の２次元画像によって提供される、前記ユーザの顔に関する前記３次元情報に基づいて、前記第１のユーザの前記身元を判別するように構成されている、
請求項１８又は１９に記載のコンピューティング・デバイス。
【請求項２１】
前記ログイン制御部は、
前記第２のユーザの前記判別された身元が前記第２の所定の身元と一致しない場合、第１の所定の英数字情報と一致する第１の英数字情報と、第２の所定の英数字情報と一致する第２の英数字情報とを入力するよう前記第２のユーザに要求し、前記ユーザによって入力された前記第１の英数字情報が前記第１の所定の英数字情報と一致し且つ前記第２の英数字情報が前記第２の所定の英数字情報と一致する場合に、前記第２のユーザを前記コンピューティング・デバイスにログインさせるようにさらに構成され、
前記第２のユーザの前記判別された身元が前記第２の所定の身元と一致する場合、前記第１のユーザを前記コンピューティング・デバイスからログアウトさせること及び前記第２のユーザを前記コンピューティング・デバイスにログインさせることを確認する指示は、さらに、前記第２の所定の英数字情報と一致する第２の英数字情報を入力するよう前記第２のユーザに指示するが、前記第１の所定の英数字情報と一致する第１の英数字情報を入力するよう前記第２のユーザに指示しないことを含む、
請求項１８～２０のいずれか１項に記載のコンピューティング・デバイス。
【請求項２２】
前記第１のユーザを前記コンピューティング・デバイスにログインさせることは、前記

第１のユーザが前記第１のユーザに関連する第１のリソースであって、前記第１のユーザにとって個人的なドキュメントを含む前記第１のリソースにアクセスすることを許可するが、前記第１のユーザが第２のユーザに関連する第２のリソースにアクセスすることを禁止することを含み、

前記第２のユーザを前記コンピューティング・デバイスにログインさせることは、前記第２のユーザが前記第２のユーザに関連する第２のリソースであって、前記第２のユーザにとって個人的なドキュメントを含む前記第２のリソースにアクセスすることを許可するが、前記第２のユーザが前記第１のユーザに関連する前記第１のリソースにアクセスすることを禁止することを含む、

請求項１８～２１のいずれか１項に記載のコンピューティング・デバイス。

【請求項２３】

前記ログイン制御部は、前記第２のユーザの前記判別された身元が前記第２の所定の身元と一致しない場合に、前記第２のユーザを前記コンピューティング・デバイスにログインさせるための条件として第１の所定の英数字情報と一致する第１の英数字情報を入力するよう前記第２のユーザに要求するようにさらに構成される、

請求項１８～２２のいずれか１項に記載のコンピューティング・デバイス。

【請求項２４】

前記第１の所定の英数字情報が前記第１のユーザに関連するユーザ名を含む、請求項２３に記載のコンピューティング・デバイス。

【請求項２５】

前記カメラは、前記第１のユーザの複数の画像であって、組み合わされて前記ユーザの顔面のジェスチュアを定義する前記複数の画像を受信するようにさらに構成され、

前記ユーザ認識部は、受信した前記複数の画像に基づいて及び前記顔面のジェスチュアに基づいて、前記第１のユーザの前記身元を判別するようにさらに構成され、

前記ログイン制御部は、前記判別された身元が前記第１の所定の身元と一致する場合に、前記第１のユーザを前記コンピューティング・デバイスにログインさせるようにさらに構成される、

請求項１８～２４のいずれか１項に記載のコンピューティング・デバイス。

【請求項２６】

電話をさらに含む、請求項１８～２５のいずれか１項に記載のコンピューティング・デバイス。

【発明の詳細な説明】

【技術分野】

【０００１】

関連出願の相互参照

本出願は、２０１１年９月２８日に出願され、「LOGIN TO A COMPUTING DEVICE BASED ON FACIAL RECOGNITION」という名称の米国特許出願第１３／２４７６５２号に対する優先権を主張し、その継続であり、同特許出願は参照によりその全体が本明細書に組み込まれる。

【０００２】

この説明は、コンピュータに対するユーザの認証に関し、特に、顔認識（facial recognition）に基づくコンピューティング・デバイスへのログインに関する。

【背景技術】

【０００３】

コンピュータ・セキュリティでは、ログインまたはログオン（ロギングインまたはロギングオンならびにサインインまたはサインオンとも呼ばれる）は、一般に、それによりコンピュータ・システムへの個別アクセスがユーザによって提供されたセキュリティ証明書を使用したユーザの識別によって制御されるプロセスである。ユーザは、システムにログインしてコンピュータ・システムのリソースにアクセスすることができ、その後、アクセスがもはや不要になったときにログアウトまたはログオフする（ログアウト／ログオフを

実行する）ことができる。ログアウトは、一般に、前にログインした後にコンピュータ・システムのリソースへのアクセスを遮断することである。

【発明の概要】

【発明が解決しようとする課題】

【０００４】

伝統的に、コンピュータまたはコンピューティング・デバイスは、無許可使用または不注意な使用を防止するために、ロックするかまたはその他の方法で保護することができる。一般に、ユーザは、コンピュータをアンロックするために、何らかの積極的アクションを実行する（たとえば、パスワードを入力する、キーの組み合わせをタイプする、マウスを移動させる、画面上で指をスワイプするなど）必要がある。

【課題を解決するための手段】

【０００５】

第１の一般的な態様では、第１のユーザをコンピューティング・デバイスにログインさせる方法は、コンピューティング・デバイスに動作可能に結合されたカメラを介して第１のユーザの画像を受信することと、受信画像に基づいて第１のユーザの身元（identity）を判別することを含む。判別された身元が所定の身元と一致する場合に、少なくとも第１のユーザの身元が所定の身元と一致することに基づいて、第１のユーザをコンピューティング・デバイスにログインさせる。

【０００６】

他の一般的な態様では、第１のユーザをコンピューティング・デバイスにログインさせるためのシステムは、有形のコンピュータ可読媒体に保存され、命令を含む、コンピュータ・プログラム・プロダクトを含むことができる。この命令は、実行されたときに、コンピューティング・デバイスに動作可能に結合されたカメラを介して第１のユーザの画像を受信することと、受信画像に基づいて第１のユーザの身元を判別することと、判別された身元が所定の身元と一致する場合に、少なくとも第１のユーザの身元が所定の身元と一致することに基づいて、第１のユーザをコンピューティング・デバイスにログインさせることをコンピュータ・システムに実行させることができる。

【０００７】

他の一般的な態様では、コンピューティング・デバイスは、第１のユーザの画像を受信するために構成されたカメラと、受信画像に基づいて第１のユーザの身元を判別するために構成されたユーザ認識部（user recognizer）と、判別された身元が所定の身元と一致する場合に、少なくとも第１のユーザの身元が所定の身元と一致することに基づいて、第１のユーザをコンピューティング・デバイスにログインさせるように構成されたログイン制御部（login manager）とを含むことができる。

【０００８】

実現例は以下の特徴のうちの１つまたは複数を含むことができる。たとえば、カメラはコンピューティング・デバイスと物理的に統合することができる。コンピューティング・デバイスは電話を含むことができる。

【０００９】

第１のユーザをコンピューティング・デバイスにログインさせることは、第１のユーザが第１のユーザに関連する第１のリソースにアクセスすることを許可するが、第１のユーザが第２のユーザに関連する第２のリソースにアクセスすることを禁止することを含むことができ、この方法は、第１のユーザをコンピューティング・デバイスからログアウトさせることと、コンピューティング・デバイスに動作可能に結合されたカメラを介して第２のユーザの第２の画像を受信することと、受信した第２の画像に基づいて第２のユーザの身元を判別することをさらに含むことができる。次に、第２のユーザの判別された身元が所定の身元と一致する場合に、少なくとも第２のユーザの身元が所定の身元と一致することに基づいて、第２のユーザをコンピューティング・デバイスにログインさせることができ、第２のユーザをコンピューティング・デバイスにログインさせることは、第２のユーザが第２のユーザに関連する第２のリソースにアクセスすることを許可するが、第２のユ

ーザが第１のユーザに関連する第１のリソースにアクセスすることを禁止することを含む。

【００１０】

判別された身元が所定の身元と一致する場合に、第１のユーザから英数字入力を要求せずに、第１のユーザをコンピューティング・デバイスにログインさせることができる。

【００１１】

判別された身元が所定の身元と一致しない場合、第１の所定の英数字情報と一致する第１の英数字情報と、第２の所定の英数字情報と一致する第２の英数字情報とを入力するよう第１のユーザに要求することができ、第１のユーザによって入力された第１の英数字情報が第１の所定の英数字情報と一致する場合であって、第２の英数字情報が第２の所定の英数字情報と一致する場合に、第１のユーザをコンピューティング・デバイスにログオンさせることができる。判別された身元が所定の身元と一致する場合に、第２の所定の英数字情報と一致する第２の英数字情報を入力するよう第１のユーザに要求することができるが、第１のユーザは、第１の所定の英数字情報と一致する第１の英数字情報を入力するよう要求されないであろう。第２の英数字情報が第２の所定の英数字情報と一致する場合に、第１のユーザをコンピューティング・デバイスにログオンさせることができる。第１の所定の英数字情報は第１のユーザに関連するユーザ名を含むことができ、第２の所定の英数字情報は第１のユーザに関連するパスワードを含むことができる。

【００１２】

カメラを介して第１のユーザの複数の画像を受信することができ、この複数の画像はユーザの顔に対して複数の異なる視点から撮られ、複数の受信画像に基づいて第１のユーザの身元を判別する。

【００１３】

カメラを介して第１のユーザの複数の画像を受信することができ、この複数の画像はユーザの顔面のジェスチュア（facial gesture）を含み、複数の受信画像に基づき、さらに顔面のジェスチュアに基づいて、第１のユーザの身元を判別することができ、判別された身元が所定の身元と一致する場合に、第１のユーザをコンピューティング・デバイスにログインさせることができる。

【００１４】

受信画像に基づいて第１のユーザの身元を判別することは、ユーザの画像内のユーザの目、鼻、頬骨、あるいは顎、またはこれらの組み合わせの相対位置、サイズ、あるいは形状、またはこれらの組み合わせのうちの１つまたは複数に基づいて第１のユーザの身元を判別することを含むことができる。

【００１５】

判別された身元が所定の身元と一致しない場合、第１のユーザは、第１のユーザをコンピューティング・デバイスにログオンさせるための条件として第１の所定の英数字情報と一致する第１の英数字情報を入力するよう要求される。次に、判別された身元が所定の身元と一致する場合、コンピューティング・デバイスのタッチ・センシティブ・エリア（touch sensitive area）内で１つまたは複数のジェスチュアを受信することができる。タッチ・センシティブ・エリア内で受信したジェスチュア（複数も可）はメモリ内に保存された１つまたは複数の所定のデバイス・ジェスチュア（device gesture）と比較することができ、受信したジェスチュア（複数も可）が所定のジェスチュア（複数も可）と一致する場合に、第１のユーザをコンピューティング・デバイスにログオンさせるための条件として英数字情報を入力するよう第１のユーザに要求せずに、第１のユーザをコンピューティング・デバイスにログオンさせることができる。

【００１６】

この方法は、第１のユーザをコンピューティング・デバイスにログインさせた後に、カメラを介して第２のユーザの画像を受信することと、第２のユーザの受信画像に基づいて第２のユーザの身元を判別することと、第２のユーザの判別された身元が第１のユーザの身元によって一致した所定の身元と一致しない場合に、第１のユーザをコンピューティン

グ・デバイスからログアウトさせることをさらに含むことができる。第２のユーザの判別された身元が所定の身元と一致する場合に、少なくとも第２のユーザの身元が所定の身元と一致することに基づいて、第２のユーザをコンピューティング・デバイスにログインさせることができる。

【００１７】

カメラは第１のユーザの複数の画像を受信するように構成することができ、この複数の画像はユーザの顔に対して複数の異なる視点から撮られ、ユーザ認識部は、複数の受信画像に基づいて第１のユーザの身元を判別するように構成することができる。

【００１８】

１つまたは複数の実現例の詳細は添付図面および以下の説明に明記されている。その他の特徴は、その説明および図面ならびに特許請求の範囲から明らかになるであろう。

【図面の簡単な説明】

【００１９】

【図１】開示されている主題によるシステムの実現例のブロック図である。

【図２】開示されている主題による装置の実現例のブロック図である。

【図３】開示されている主題によるシステムの実現例のブロック図である。

【図４】開示されている主題によるシステムの実現例のブロック図である。

【図５Ａ】開示されている主題によるシステムの実現例のブロック図である。

【図５Ｂ】開示されている主題によるシステムの実現例のブロック図である。

【図５Ｃ】開示されている主題によるシステムの実現例のブロック図である。

【図６】開示されている主題によるシステムの実現例のブロック図である。

【図７】開示されている主題による技法の実現例の流れ図である。

【図８】本明細書に記載されている技法を実現するために使用できるコンピュータ・デバイスおよびモバイル・コンピュータ・デバイスの一例を示す図である。

【発明を実施するための形態】

【００２０】

様々な図面における同様の参照記号は同様の要素を示している。

【００２１】

図１は、開示されている主題によるシステム１００の実現例のブロック図である。一実現例では、システム１００はコンピューティング・デバイス１０２とサーバ１０４とを含むことができる。コンピューティング・デバイス１０２は、デスクトップ・コンピュータ、ラップトップ・コンピュータ、タブレット・コンピュータ、ネットブック・コンピュータ、スマートフォンなどを含むことができる。このコンピューティング・デバイス１０２は、ユーザ１９０によって使用することができ、ネットワークによりサーバ１０４と通信することができる。コンピューティング・デバイス１０２は、ユーザの存在を検出し、顔認識技術に基づいてユーザの身元を判別するために使用できるカメラ１０６を含むことができる。次に、ユーザの身元は、コンピューティング・デバイス１０２にログインする許可を受けているかまたはコンピューティング・デバイス１０２のリソースを使用する許可を受けているユーザに関する保存情報と比較することができる。判別された身元と保存情報との一致が見つかると、識別されたユーザは、コンピューティング・デバイスにログインすることができるかまたはコンピューティング・デバイス１０２のリソースを使用することを許可される。

【００２２】

様々な実現例では、コンピューティング・デバイス１０２はプロセッサ１１５とメモリ１１４とを含むことができる。いくつかの実現例では、プロセッサ１１５は、様々なソフトウェア、ファームウェア、またはその組み合わせを実行することができる。たとえば、一実現例では、プロセッサ１１５は、ログイン制御部１１２、ユーザ認識部１０８、あるいはログイン・ユーザインターフェース１１０、またはこれらの組み合わせを実行することができる。このような実現例では、実行されたソフトウェアの各部分はメモリ１１４内に保存することができる。

【００２３】
例示的な一実現例では、ユーザ（たとえば、ユーザ１９０）がコンピューティング・デバイス１０２に近い場合、カメラ１０６はユーザのデジタル画像を取得することができる。カメラ１０６はコンピューティング・デバイス１０２と統合され、それに動作可能に接続される場合もあれば、カメラ１０６はコンピューティング・デバイス１０２から分離され、（たとえば、コンピューティング・デバイスとの有線または無線接続により）それに動作可能に接続される場合もある。プロセッサ１１５またはプロセッサ１１５上で実行されているユーザ認識部１０８は、ユーザのデジタル画像を分析して、コンピューティング・デバイス１０２に近いユーザの身元を判別することができる。たとえば、ユーザ認識部１０８は、ユーザのデジタル画像を分析して、ユーザの目のサイズ、ユーザの両目の間の距離、ユーザの鼻のサイズおよび形状、ユーザの目と鼻の相対位置などの情報を判別することができる。この情報は、コンピューティング・デバイスまたはそのリソースを使用する許可を受けているユーザに関する保存情報と比較することができ、一致が見つかった場合、プロセッサ１１５またはプロセッサ上で実行されているログイン制御部１１２は、ユーザをコンピューティング・デバイスにログインさせるかまたはユーザがコンピューティング・デバイス１０２のリソースを使用することを許可することができる。

【００２４】
一実現例では、コンピューティング・デバイス１０２は、数人の異なるユーザによって共用されるデスクトップ・コンピューティング・デバイスまたはノートブック・コンピューティング・デバイスにすることができる。コンピューティング・デバイス１０２は、コンピューティング・デバイス内に統合することができるカメラ１０６を含むことができる。たとえば、カメラは、コンピューティング・デバイス１０２のディスプレイ部分のベゼル内に統合することができ、顔が表示装置の正面に位置するユーザに面するように表示装置に対して垂直に向けることができる。

【００２５】
カメラ１０６は、その視野内の物体の画像を記録することができる。カメラ１０６は、定期的に、たとえば、一定の速度で、またはカメラの正面のゾーン内の動きに応じて、たとえば、ユーザがカメラの正面の位置に移動したことに応じて、またはユーザからの明示的な入力、たとえば、ユーザがコンピューティング・デバイス１０２のキーボードのキーに触れたことに応じて、画像を記録するように構成することができる。一実現例では、カメラ１０６は、カメラの正面のゾーン内で動きが検出されないときに低速で画像を記録し、ゾーン内で動きが検出されたときにより高速で画像を記録するように構成することができる。これにより、カメラは、コンピューティング・デバイスを使用するべくデバイスの正面に着座するユーザまたはコンピューティング・デバイスから歩き去るユーザに対して迅速に応答するが、ユーザがコンピューティング・デバイス１０２の正面に座っている間は高速でコンピューティング・リソースを消費するのを回避することができる。いくつかの実現例では、カメラ１０６によって記録された画像はその画像が記録されてから閾値量の時間（たとえば、５分）が経過した後に廃棄することができるか、あるいは、カメラによって記録された画像はコンピューティング・デバイスがシャットダウンされるかまたは低電力状態になったときに廃棄することができるか、またはその両方を行うことができる。

【００２６】
カメラ１０６によって記録された画像は、ユーザ認識部１０８によって受信し分析して、その画像が記録されたユーザの身元を判別することができる。様々な実現例では、ユーザ認識部１０８は、画像について顔認識を実行することができる。たとえば、ユーザ認識部１０８は、カメラ１０６によって検出され、ユーザ認識部１０８によって分析されたユーザ１９０の顔の特徴を、可能性のあるユーザのグループの顔の特徴と比較することができる。この比較は、ユーザを識別するために使用できるその他の顔の特徴の比較を含むことができる。

【００２７】

様々な顔認識技法を使用することができる。たとえば、カメラの視野内のその他の特徴から顔を区別し、その顔の様々な特徴を測定する技法を使用することができる。どの顔にも、多数の区別可能な標識点（landmark）と、顔の特徴を構成する種々の山と谷がある。これらの標識点を使用して、顔上の複数の節点を定義することができ、これは、ユーザの両目の間の距離、ユーザの鼻の幅、ユーザの眼窩の深さ、ユーザの頬骨の形状、ユーザの下顎の輪郭の長さに関する情報を含むことができる。ユーザの顔の節点は、ユーザの顔を現すフェースプリント（faceprint）として知られる数値コードを作成するために、ユーザの顔の１つまたは複数の画像から判別することができる。

【００２８】

また、顔認識は、ユーザの顔の３次元画像に基づくかまたはユーザの顔に関する３次元情報を共に提供できる複数の２次元画像に基づいて実行することもできる。３次元顔認識では、顔の示差的特徴、たとえば、眼窩、鼻、および下顎の曲線など、固定された組織および骨が最も明らかな場所を使用して、ユーザを識別し、ユーザのフェースプリントを生成する。ユーザのフェースプリントは、ユーザの顔面上の特徴を表す１組の数字などの定量化可能なデータを含むことができる。

【００２９】

ユーザを識別するために、ユーザの顔に対して異なる複数の視点の複数の２次元画像も取得して使用することができる。これは、実際にはコンピューティング・デバイス１０２の正面に存在しないユーザの写真を掲げることなどにより顔認識技術を欺そうという試みを未然に防ぐこともできる。

【００３０】

ユーザの１つまたは複数の画像に基づいてユーザの身元が判別された後、たとえば、ユーザの顔について生成された定量化可能なフェースプリントにより判別された後、ユーザ認識部１０８はユーザの身元を１つまたは複数の所定の身元と比較することができる。判別された身元と所定の身元との一致が見つかった場合、ログイン制御部１１２はユーザをコンピューティング・デバイス１０２にログインさせることができ、その結果、ユーザはコンピューティング・デバイス１０２の１つまたは複数のリソースにアクセスすることができる。所定の身元は、コンピューティング・デバイス１０２によって、たとえば、１つまたは複数のメモリ１１４に保存することができる。所定の身元は、ユーザの１つまたは複数の画像、１人または複数のユーザの定量化可能なフェースプリント情報、あるいは定量化可能なフェースプリント情報のサブセットを含むことができ、そのサブセットはユーザの画像を再構築するには不十分なものである。

【００３１】

所定の身元は、オプトイン・プロセスによるユーザの依頼により、コンピューティング・デバイス１０２にログオンするために顔認識技術を利用したいと希望するユーザのために保存することができる。たとえば、ユーザのためのデフォルト・ログイン手順は、ユーザ名とパスワードなど、第１および第２の英数字文字列を入力するようユーザに要求する可能性がある。しかし、ユーザがデフォルト・ログイン手順を使用して正常にログインすると、ユーザはそのユーザに関連する所定の身元をコンピューティング・デバイス１０２に保存させることを選択することができ、その結果、将来のログイン時にユーザは顔認識技術に基づくログイン手順を利用することができ、それはユーザ名とパスワードを入力するより時間がかからず、ユーザにとってあまり目障りではない可能性がある。

【００３２】

他の実現例では、ユーザは、コンピューティング・デバイス１０２のリソースにアクセスするためにログイン手順の一部として必要な英数字入力の量を削減するが排除しないために顔認識技術を使用することを選択することができる。たとえば、デフォルト・ログイン手順が第１の英数字情報（たとえば、ユーザ名）と第２の英数字情報（たとえば、パスワード）の両方を入力するようユーザに要求する場合、ユーザは、これらの英数字情報のうちの一方を入力する要件を排除するために顔認識技術を使用することを選択することができる。一実現例では、顔認識技術によって判別されたユーザの身元と保存された所定の

身元との一致が存在する場合、ユーザは、第１の英数字情報を入力するステップをスキップすることができ、第２の英数字情報のみを入力してコンピューティング・デバイス１０２にログインすることができる。

【００３３】

容量結合または抵抗結合のタッチ・センシティブ入力パネルを含むデバイスにログオンするために特に有用である可能性のある他の実現例では、顔認識技術を使用して、ログイン手順の一部として必要な英数字入力の量を排除することができる。たとえば、ユーザの画像を受信し、その画像が所定の身元と一致する身元に対応する場合、ユーザはコンピューティング・デバイスのタッチ・センシティブ・エリアに１つまたは複数のジェスチュアを入力するよう要求される可能性がある。ユーザによって入力されたジェスチュアが１つまたは複数の所定のジェスチュアと一致する場合、コンピューティング・デバイスにログオンするための条件として英数字情報を入力するようユーザに要求せずに、ユーザをコンピューティング・デバイスにログインさせることができる。しかし、受信画像が所定の身元と一致しない身元に対応する場合、ユーザは、コンピューティング・デバイスにログオンするための条件として特定の英数字情報を入力するよう要求される可能性がある。顔認識技術を使用して、英数字情報を入力する必要性を排除することにより、ユーザは、スマートフォンなどのモバイル・コンピューティング・デバイスを保護するプロセスが、モバイル・コンピューティング・デバイスをアンロックするために英数字情報を入力する必要がある場合より厄介ではないと気付く可能性がある。

【００３４】

他の実現例では、プロセッサ１１５、ユーザ認識部１０８、およびログイン制御部１１２によって実行される顔認識技術を使用して、異なる複数のユーザを１つの共用コンピューティング・デバイス１０２に効率よくログオンさせることができる。たとえば、複数のユーザ（たとえば、家族、同僚など）は１つのコンピューティング・デバイス１０２を共用することができ、それぞれのユーザは、異なるユーザデータ１２０をそのコンピューティング・デバイス１０２に保存しておくかまたはそのコンピューティング・デバイス１０２に関連して使用できるようにサーバ１０４に保存してそのサーバから取り出すことができる。ユーザデータ１２０は、たとえば、特定のユーザにとって個人的なドキュメント、プリファレンス、ブックマークおよびお気に入り、設定などを含むことができる。特定のユーザをコンピューティング・デバイス１０２にログインさせる行為は、その他のユーザに関連するユーザデータではなく、特定のユーザに関連するユーザデータ１２０をその特定のユーザに使用可能な状態にすることができる。

【００３５】

いくつかの実現例では、ユーザデータ１２０は、ユーザ設定データベース１５０を収容しているサーバ１０４から検索することができる。このような実現例では、ユーザ１９０は複数のデバイス（たとえば、コンピューティング・デバイス１０２など）を使用することができ、どのデバイスが使用されているかにかかわらず、自分のユーザデータ１２０が使用可能である可能性がある。コンピューティング・デバイス１０２がユーザ１９０を識別すると、コンピューティング・デバイス１０２は、サーバ１０４からユーザ１９０のユーザデータ１２０を要求し、その後、ダウンロードすることができる。

【００３６】

あるユーザから他のユーザへの効率的な遷移を容易にするために、顔認識技術を使用することができる。たとえば、第１のユーザの身元（顔認識技術によって判別されたもの）が第１のユーザに関連する所定の身元と一致することに基づいて、第１のユーザをコンピューティング・デバイスにログオンさせることができる。ログインすると、第１のユーザは、コンピューティング・デバイスに保存され、第１のユーザに関連する第１のリソース（たとえば、ユーザデータ１２０）にアクセスすることを許可されるが、第１のユーザが第２のユーザに関連する第２のリソースにアクセスすることを禁止される可能性がある。次に、第２のユーザの顔の第２の画像がカメラ１０６を介して受信されると、受信した第２の画像に基づいて、第２のユーザの身元を判別することができる。第２のユーザの身元

が第２のユーザに関連する所定の身元と一致する場合、第２のユーザをコンピューティング・デバイスにログインさせることができ、第２のユーザは、コンピューティング・デバイスに保存され、第２のユーザに関連する第２のリソースにアクセスすることを許可されるが、第２のユーザが第１のユーザに関連する第１のリソースにアクセスすることを禁止される可能性がある。このように、１つのコンピューティング・デバイスを共用する家族の複数のメンバーは、コンピューティング・デバイスに対して自分自身を示すだけで、自分の個別ユーザデータ１２０をコンピューティング・デバイスによって自動的にロードさせることができ、ログインしていないときに家族の他のメンバーが自分の個別ユーザデータにアクセスできないことも認識している。

【００３７】

一実現例では、第１のユーザをコンピューティング・デバイス１０２にログインさせ、所定の身元と一致する第２のユーザの画像が受信されると、コンピューティング・デバイスが第２のユーザに関連する第２のリソースを提供し、第１のユーザに関連する第１のリソースを提供しないように、ユーザ（複数も可）は、第１のユーザをコンピューティング・デバイスからログオフさせなければならないことと、第２のユーザをコンピューティング・デバイスにログオンさせなければならないことを確認するよう指示される可能性がある。この確認は、様々な形でコンピューティング・デバイスに提供することができる。たとえば、上述の通り、第２のユーザに関連するパスワードが要求される場合もあれば、単なるキーストローク（たとえば、「Ｅｎｔｅｒ」キーまたは「Ｙ」キーを叩くこと）が要求される場合もある。このように、偶発的な第１のユーザのログアウトおよび第２のユーザのログインを回避することができる。

【００３８】

他の実現例では、コンピューティング・デバイス１０２を使用する許可を受けていないユーザがそのデバイスを使用しようと試みると、無許可ユーザである可能性のある人の画像を収集してデバイスに保存するかまたはコンピューティング・デバイスの許可ユーザに送信することができる。たとえば、無許可ユーザがコンピューティング・デバイスにログオンして使用しようと試みたが、失敗した場合（たとえば、無許可ユーザが誤ったユーザ名およびパスワードの英数字情報を入力した場合）、カメラ１０６は無許可ユーザの画像を記録し、その画像をメモリ１１４に保存することができる。他の実現例では、記録画像を許可ユーザに送信することができる。たとえば、記録画像をコンピューティング・デバイス１０２からサーバ１０４に送信することができ、そのサーバは記録画像を許可ユーザがアクセスできるアカウント（たとえば、電子メール・アカウント）またはデバイス（たとえば、スマートフォンまたは携帯電話あるいはその他のモバイル・デバイス）に転送することができる。次に、許可ユーザは、無許可ユーザによるログイン試行に応じて適切な措置を講じることができる。

【００３９】

いくつかの実現例では、ユーザの存在は、コンピューティング・デバイス１０２を休眠状態から起こす可能性がある。このような休眠状態は、いかなるユーザ（たとえば、ユーザ１９０）もデバイス１０２にログインしていない状態またはモード、あるいはデバイス１０２のコンポーネントまたはその一部分が電源オフまたは電源切断していて、ほとんどの動作状態が揮発性メモリ（たとえば、スリープ・モードの場合）または不揮発性メモリ（たとえば、冬眠モードの場合）のいずれかであるデバイス１０２のメモリ１１４に保存されるスリープ・モードまたは冬眠モードなどの低電力モードを含むことができる。

【００４０】

デバイス１０２は、ユーザ１９０がコンピューティング・デバイス１０２に接近したときにユーザ１９０の存在を検出するように構成することができる。様々な実現例では、デバイス１０２は、ユーザ（たとえば、ユーザ１９０）の存在を検出するように構成された近接センサ１１７を含むことができる。低電力モードでは、この近接センサまたはその他の検出センサあるいは１０６は、デバイス１０２の大部分が低電力モードであっても、ユーザを検出するために電源がオンにされるまたは電源が入れられることができる。様々な

実現例では、近接センサ１１７は、ユーザ１９０の存在または移動を（たとえば、接触などを介して）感知するように構成されたタッチパッド、マウス、容量センサ、導電センサ、赤外線センサ、動作検知器などを含むことができる。そして、ユーザの存在がコンピューティング・デバイス１０２をその休眠状態から起こした後、ユーザの身元を判別することができる。

【００４１】

一実現例では、デバイス１０２は、ユーザ１９０の存在を検出したときに、ユーザ１９０の身元を判別するように構成されたユーザ認識部１０８を含むことができる。ユーザ認識部１０８は、カメラ１０６から受信した画像の特徴を所定のユーザに関連する特徴と比較するように構成されたハードウェアまたはソフトウェアを含むことができる。

【００４２】

様々な実現例では、ユーザ認識部１０８は、ユーザ１９０のデジタル画像を可能性のあるユーザのリストと比較することができる。ユーザ認識部１０８は、可能性のあるユーザのリストの中から、検出されたユーザ１９０と最も厳密に一致するユーザを選択することができる。いくつかの実現例では、ユーザ認識部１０８は、検出されたユーザ１９０について十分に厳密な一致がなされない場合には可能性のあるユーザから誰も選択しないように構成することができ、一致が十分であることは定義済みの基準によって判断される。

【００４３】

可能性のあるユーザの誰もが検出されたユーザ１９０と一致しないという状況では、コンピューティング・デバイス１０２は、いかなるユーザもコンピューティング・デバイス１０２にログインさせない可能性がある。検出されたユーザ１９０をコンピューティング・デバイス１０２にログインさせないことは、コンピューティング・デバイス１０２を低電力状態を解除しないことまたはコンピューティング・デバイス１０２を低電力状態に戻すことを含むことができる。他の実現例では、コンピューティング・デバイス１０２は、デフォルトのユーザ設定、プリファレンス、またはデータ１２０のセットの全部または一部をロードすることができる。一実現例では、コンピューティング・デバイス１０２はゲスト・ユーザ設定のセットをロードすることができる。このような実現例では、ゲスト・ユーザ設定は、コンピューティング・デバイス１０２に保存されたデータに対するアクセスをまったく可能にしないかまたは限定的なアクセスを可能にする可能性がある。このような実現例では、ゲスト・ユーザ設定は、インターネットに対するアクセスを可能にするかまたはコンピューティング・デバイス１０２およびコンピューティング・デバイス１０２の諸機能に対するその他の限定的かつ制限されたアクセスを可能にする可能性がある。

【００４４】

様々な実現例では、ユーザ認識部１０８は、カメラ１０６によって記録された画像に基づいて顔認識を実行することができる。このような実現例では、ユーザ認識部１０８は、カメラ１０６によって検出されたユーザ１９０の顔の特徴を１人または複数の可能性のあるユーザの顔の特徴と比較することができる。この比較はその他の身体特徴の比較を含むことができる。たとえば、コンピューティング・デバイス１０２は、カメラによって収集されたデジタル画像に基づいてユーザ１９０の身長を計算することができる。他の例では、コンピューティング・デバイス１０２は、ユーザ１９０の両目の間の距離またはその他の生体計測特徴を計算することができる（たとえば、固有顔分析など）。

【００４５】

一実現例では、デバイス１０２は、所与のユーザの設定、プリファレンスなど（ひとまとめにしてユーザデータ１２０と呼ぶ）にアクセスし、それをデバイス１０２のメモリ１１４にロードするかまたはその他の方法でデバイス１０２にアクセスするかまたはログインするための動作を実行するように構成されたログイン制御部１１２を含むことができる。様々な実現例では、ユーザデータ１２０は、たとえば、様々なネットワーク・ドライブ、プリンタ、あるいはデバイス、またはこれらの組み合わせを装着し、様々なネットワーク接続を確立し、特定のカラースキームまたはグラフィカル・ユーザインターフェース（ＧＵＩ）テーマを設定し、ブックマークまたはファイルおよびアイコン設定、ボリューム

およびマルチメディア設定、保存パスワードまたは認証情報などをロードするよう、装置に指示するデータを含むことができる。

【００４６】

他の実現例では、ユーザデータ１２０は、ユーザ１９０をコンピューティング・デバイス１０２にログインさせたときに開かれるかまたは実行される予定のアプリケーション、ドキュメント、ファイル、またはタブのリストを含むことができる。いくつかの実現例では、これらのアプリケーション、ドキュメント、ファイル、またはタブは、前にユーザ１９０をこのようなコンピューティング・デバイス１０２にログインさせたときに開いていたかまたは積極的に実行された可能性がある。このような実現例では、このユーザデータ１２０は、ユーザ１９０が複数の機械または装置間で自分の作業環境を同期させることを可能にするかまたは容易にする可能性がある。

【００４７】

様々な実現例では、ログイン制御部１１２は、ユーザデータ１２０をユーザ設定データベース（ＤＢ）１５０に保存するリモート・サーバ１０４からユーザデータ１２０を取得することができる。このような実現例では、リモート・サーバ１０４は、上述の通り、複数のデバイス（たとえば、コンピューティング・デバイス１０２など）間でユーザデータ１２０を同期させるように構成することができる。様々な実現例では、ログイン制御部１１２は、ユーザ１９０をコンピューティング・デバイス１０２にログインさせている間に行われるユーザデータ１２０への変更によってリモート・サーバ１０４またはユーザ設定データベース（ＤＢ）１５０を更新するように構成することができる。

【００４８】

上述の通り、いくつかの実現例では、ログイン・プロセスは、ユーザ１９０からの積極的な関与を必要とする、パスワードまたはその他のセキュリティ認証情報を要求する可能性がある。このような実現例では、デバイス１０２は、ユーザ１９０に対してその認証情報（たとえば、パスワードなど）を促すように構成されたログイン・ユーザインターフェース（ＵＩ）１１０を含むことができる。ログイン制御部１１２は、ユーザが適正な認証情報を入力した場合に、ユーザデータがすでにロードされているかまたはロードされる過程にあって、ユーザが自分のユーザデータに迅速にアクセスできるように、許可またはセキュリティ認証情報の適正な提示を見越してユーザのユーザデータ１２０を投機的にロードすることができる。

【００４９】

図２は、開示されている主題によるコンピューティング・デバイス２０２の実現例のブロック図である。コンピューティング・デバイス２０２は、デスクトップ・コンピュータ、ラップトップ、タブレット、ネットブック、スマートフォンなどを含むことができる。それぞれがそれぞれ異なるユーザに関連付けられている複数のユーザデータ（たとえば、ユーザデータ２２０ａ、２２０ｂ、および２２０ｃなど）をデバイス２０２内にローカルに保存できることを除き、コンピューティング・デバイス２０２は図１のコンピューティング・デバイス１０２と同様のものにすることができる。ユーザ認識部１０８は、ユーザデータ２２０ａ、２２０ｂ、および２２０ｃに関連するユーザの中からユーザ１９０を選択するかまたは認識しようと試みることができる。このような実現例では、複数のユーザデータは、検出されたユーザ１９０を識別するために使用できるデータ（たとえば、顔の特徴パターン、ユーザ１９０の写真など）を含むことができる。

【００５０】

様々な実現例では、ユーザデータのいずれも検出されたユーザ１９０に関連付けられていない場合、ログイン制御部１１２は、上述の通り、プリロードしないかまたはユーザ１９０をデバイス２０２にログインさせない可能性がある。一実現例では、ログインＵＩ１１０は、存在する場合もあれば、ユーザ１９０に対してデフォルト・ログイン画面またはＵＩを表示する場合もある。デフォルト・ログイン画面またはユーザインターフェースを介して（たとえば、ユーザ名およびパスワードを使用するかまたは認証情報をまったく使用せずに）コンピューティング・デバイス２０２に手動でログインすると、ログイン制御

部１１２はユーザ１９０のために新しいユーザデータ・セットを作成することができる。
【００５１】
一実現例では、新しいユーザデータ・セットの作成はユーザの承諾を前提とする場合がある。いくつかの実現例では、ユーザは、ユーザデータ・セットの作成および任意のデータ収集（たとえば、サーバ１０４上にユーザデータを保存することなど）を明示的に許可するよう指示される可能性がある。さらに、ユーザは、このようなデータ収集動作への参加／不参加を選択することができる。さらに、収集したデータは、たとえば、新しいユーザデータ・セットを作成するために使用できるユーザデータの包括セットを作成するためにデータ分析を実行する前に、匿名扱いにすることができる。たとえば、ユーザデータの包括セットは、ユーザの顔のパターンおよび特徴に関する符号化または暗号化された情報を含むことができるが、符号化または暗号化されたデータからユーザの画像を構築することは許可されない。
【００５２】
代わって、ログイン制御部１１２は、ユーザ１９０のデータが保存されているリモート・サーバからユーザ１９０に関連するユーザデータのセットを要求することができる。ユーザ１９０のデータは、ローカルに保存されているユーザデータのセット（たとえば、ユーザデータ２２０ａ、２２０ｂ、および２２０ｃなど）に追加することができ、ユーザ１９０がコンピューティング・デバイス２０２に自動的にログインしようと試みるその後の場合において使用することができる。
【００５３】
いくつかの実現例では、それぞれ、図１および図２のデバイス１０２および２０２の組み合わせが存在する可能性がある。このような実現例では、何らかのユーザデータをローカルに保存することができ、その他のデータをリモートに保存することができる。代わって、ユーザデータの第１の部分（たとえば、アイコン配置、カラースキームなど）をローカルに保存することができ、ユーザデータの第２の部分（たとえば、アクティブ・タブ、プリンタ設定、ドライブ・マッピングなど）をリモートに保存することができ、ユーザが使用できる様々なデバイス間で同期させることもできる。
【００５４】
図３は、開示されている主題によるシステム３００の実現例のブロック図である。一実現例では、システム３００は、装置、電子デバイス、またはコンピュータ３０２を含むことができる。コンピューティング・デバイス３０２は、デスクトップ・コンピュータ、ラップトップ、タブレット、ネットブック、スマートフォンなどを含むことができる。
【００５５】
この場合も、装置３０２は、図２のコンピューティング・デバイス２０２と同様のものにすることができる。しかし、図３では、一実現例において、ユーザ認識部１０８は、カメラ１０６またはユーザ認識部１０８の範囲内にある複数の有力なまたは可能性のあるユーザ（たとえば、ユーザ３９０ａおよび３９０ｂ）の中から単一ユーザ（たとえば、ユーザ１９０）を選択するように構成することができる。
【００５６】
例示されている実現例では、装置３０２は、一世帯内のユーザの家族によって使用される共用コンピュータを含むことができる。他の実現例では、装置３０２は、複数の従業員によって使用される職場環境内の共用コンピュータである場合もある。このような実現例では、装置３０２は、２人以上の可能性のあるユーザを検出し、装置３０２にログインするためにその可能性のあるユーザから１人を選択することができる。
【００５７】
このような一実現例では、ユーザ認識部１０８は、デバイス３０２に最も近いユーザ１９０を識別するように構成することができる。他の実現例では、ユーザ認識部１０８は、コンピューティング・デバイス２０２を、好ましい主要ユーザ（たとえば、ユーザ１９０）またはそのコンピューティング・デバイス２０２のための主要ユーザに関連付けるように構成することができる。この主要ユーザは、複数の可能性のあるユーザに含まれる場合

、ログインするために選択される可能性がある。様々な実現例では、ユーザ認識部１０８は、定義済みの基準のセットに基づいて複数の可能性のあるユーザから１人のユーザを選択するように構成することができる。

【００５８】

様々な実現例では、ユーザ１９０の識別はユーザの傾向に基づいて行うことができる。たとえば、第１のユーザ（たとえば、ユーザ１９０）は、特定の期間中に（たとえば、午後８時から午後１０時）最も頻繁に装置３０２にログインする可能性がある。第２のユーザ（たとえば、ユーザ３９０ａ）は、第２の期間中に（たとえば、午前９時から午後１時）最も頻繁に装置３０２にログインする可能性がある。そして、第３のユーザ（たとえば、ユーザ３９０ｂ）は、第３の期間中に（たとえば、午後２時３０分から午後５時３０分）最も頻繁に装置３０２にログインする可能性がある。ユーザ１９０、３９０ａ、および３９０ｂのこのような習慣に基づいて、装置３０２は、可能性がありかつ検出されたユーザのうち、どのユーザを主要ユーザとして選択すべきかを識別することができる。ユーザを選択するために、装置３０２によってその他のユーザの傾向（たとえば、位置、最新使用、使用頻度などに基づく）を使用することができる。また、このようなユーザの傾向に基づいた識別技法は単一ユーザが識別される場合にのみ使用できることは言うまでもない。このような実現例では、ユーザ習慣は、複数の見込みのある候補ユーザを提供し、装置３０２が検出されたユーザと突き合わせようと試みる可能性のあるユーザ候補の数を（少なくとも最初に）削減することができる。

【００５９】

図４は、開示されている主題によるシステム４００の実現例のブロック図である。一実現例では、システム４００は、装置、電子デバイス、またはコンピューティング・デバイス４０２と、サーバ４０４とを含むことができる。コンピューティング・デバイス４０２は、デスクトップ・コンピュータ、ラップトップ、タブレット、ネットブック、スマートフォンなどを含むことができる。

【００６０】

例示されている実現例は、装置４０２がユーザ１９０を識別することができる他の手段を示している。図１、図２、および図３に関して上述した通り、この装置は、コンピューティング・デバイス４０２内でローカルに使用可能であるかまたはリモート・リポジトリ（たとえば、サーバ１０４上など）内に保存されている、ユーザの顔の特徴などの生体計測情報に基づいてユーザを識別することができる。例示されている実現例では、識別情報はリモート記憶システム内で見つけることができる。様々な実現例では、識別情報は分散方式で保存される可能性もある（たとえば、ソーシャル・メディア・サイト、写真共有サイトなど）。

【００６１】

一実現例では、ユーザ認識部１０８は、検出されたユーザ１９０を認識するために１つまたは複数のサーバ４０４内に保存されたユーザ識別子４０６を使用するように構成することができる。ユーザ識別子４０６の例としては、サーバ４０４またはユーザ１９０に関連するサイトからの写真などを含むことができる。たとえば、ユーザ認識部１０８は、可能性のあるユーザに関連するかまたは所定の設定で定義された社内ディレクトリ、ソーシャル・メディア・サイト、または写真共有サイトをチェックするように構成することができる。ユーザ認識部１０８は、サーバ（複数も可）４０４上で見つかった写真を、ユーザ１９０がデバイス４０２にログインするのを待っている間に撮られたユーザ１９０の写真と比較することができる。様々な実現例では、ユーザ認識部１０８は、可能性のあるユーザの限定的なリストのみをチェックするように構成することができる（たとえば、前にデバイス４０２にログインしたユーザ、会社内のユーザなど）。

【００６２】

図５Ａは、開示されている主題によるシステム５００の実現例のブロック図である。一実現例では、システム５００は、ユーザ１９０によって使用される装置５０２と、サーバ１０４とを含むことができる。上述の通り、装置５０２は、プロセッサ１１５と、メモリ

１１４と、１つまたは複数のカメラ１０６と、ログイン・ユーザインターフェース１１０と、ユーザ認識部１０８とを含むことができる。加えて、様々な実現例では、装置５０２は、ユーザ１９０に対して情報をグラフィック表示するように構成されたディスプレイまたはモニター１１６を含むことができる。

【００６３】

様々な実現例では、カメラ１０６は、カメラ１０６がその中で動作するように構成されている検出エリア５５０を含むかまたは有することができる。たとえば、ディスプレイ１１６のベゼル部分に組み込まれているカメラ１０６の場合、カメラは、たとえば、カメラ１０６から約２メートル放射状に広がる円弧内のディスプレイ１１６の正面に視野またはより一般的には「検出エリア５５０」を有することができる。したがって、カメラ１０６は、カメラ１０６の検出エリア５５０の外側のもの（たとえば、ディスプレイ１１６の後ろにあるものなど）を検出するように構成されていない可能性がある。いくつかの実現例では、カメラ１０６のための範囲はユーザ１９０によって制御可能なものにすることができ、その結果、カメラは、カメラに比較的近いユーザのみを検出するかまたはカメラからより遠くに離れているユーザを検出するように構成することができる。

【００６４】

例示されている実現例では、ユーザ１９０は、上述の通り、すでに検出され、装置５０２にログインしている可能性がある。このため、ユーザ１９０のユーザデータ１２０は、上述の通り、進行中のロギングの一部として、メモリ１１４にロードされているかまたはその他の方法で装置５０２に使用可能な状態になっている可能性がある。いくつかの実現例では、ユーザデータ１２０は、ユーザ１９０による装置５０２の使用の一部として、変更または編集されている可能性がある。たとえば、ユーザ１９０は、様々なドキュメントまたはタブ、変更した構成設定（たとえば、電子メール・サーバ、ネットワーク設定など）、あるいはその他の形式のユーザデータ１２０を開くかまたは閉じている可能性がある。

【００６５】

例示されている実現例では、ユーザ１９０はカメラ１０６の検出エリア５５０を離れる可能性がある。カメラ１０６または装置５０２は、装置５０２に関するユーザ１９０のステータスのこの変化を検出することができる。この文脈で、「ユーザ・ステータスの変化」は、ユーザの存在の変化（たとえば、ユーザが装置から歩き去ったかなど）、装置に関するユーザの単独使用または共用使用の変化（たとえば、ユーザが装置に対して単独アクセス可能であるか、複数のユーザが装置を共用しているか、第２の個人またはユーザがログインしたユーザについて盗聴またはスパイ行為を行えるかなど）、あるいは装置５０２に対するユーザの注意（attentiveness）の変化（たとえば、ユーザが積極的に装置５０２を使用しているかまたは単にカメラの検出エリア内にいるだけかなど）などを含むことができる。

【００６６】

例示されている実現例では、ユーザ１９０はカメラ１０６の検出エリア５５０を離れる可能性がある。たとえば、ユーザ１９０は装置５０２から歩き去る可能性がある。このような実現例では、カメラ１０６またはユーザ認識部１０８は、上述の通り、装置５５０に関するユーザ１９０の関係のステータスのこの変化を検出することができる。ユーザ１９０のステータスのこの変化に応じて、ログイン／許可制御部（login／authorization manager）６１２は、ユーザ１９０の許可レベル（authorization level）を調整することができる。

【００６７】

たとえば、一実現例では、ユーザ１９０がカメラ１０６の検出エリア５５０を離れたことに応じて、ログイン／許可制御部６１２は、ユーザ１９０を装置５０２からログアウトさせることができる。この文脈で、ユーザ１９０を装置５０２からログアウトさせることは、装置５０２を使用するためのユーザ１９０の許可を調整するための方法と見なすことができる。このような実現例では、これは、ユーザ１９０のユーザデータ１２０を更新す

るかまたはサーバ１０４と同期させることを含むことができる。このような実現例では、ユーザ１９０が装置（たとえば、装置５０２または他の装置など）にもう一度ログインする場合、更新されたユーザデータ１２０を使用して、ユーザ１９０を装置にログインさせることができる。ユーザ１９０の公開されたアプリケーション、ドキュメントなどがユーザデータ１２０に含まれる実現例では、ユーザ１９０は、ユーザ１９０がログアウトしていない場合と同じように、装置５０２（またはその他の装置）を原則的に使用し続けることができる可能性がある。

【００６８】

他の実現例では、ユーザ１９０がカメラ１０６の検出エリア５５０を離れたことに応じて、ログイン／許可制御部５１２は、ユーザ１９０を装置５０２から部分的にログアウトさせることができる。この場合も、この文脈で、ユーザ１９０を装置５０２から部分的にログアウトさせることは、装置５０２を使用するためのユーザ１９０の許可を調整するための方法と見なすことができる。たとえば、ログインＵＩ１１０は、ディスプレイ１１６を介して表示された通常のグラフィック情報（たとえば、ウィンドウ、ドキュメントなど）を除去し、その代わりに、ディスプレイ１１６を介して通常のグラフィック情報を表示する前にユーザ自身を再認証するようユーザ１９０に要求するログインまたはロック画面を表示することができるであろう。このような実現例では、ユーザデータ１２０は、実現例次第で、サーバ１０４と同期している場合もあれば、同期していない場合もある。様々な実現例では、再認証は、図１、図２、図３、あるいは図４、またはこれらの組み合わせに関して上述した技法を介して自動的に行うことができる。

【００６９】

他の実現例では、ユーザ１９０がカメラ１０６の検出エリア５５０を離れたことに応じて、ログイン／許可制御部５１２は、装置５０２を電力低減状態（reduced power state）（たとえば、電力中断状態（suspend power state）、電力休止状態（hibernate power state）など）にするかまたは遷移させることができる。この文脈で、装置５０２を電力低減状態にすることは、装置５０２を使用するためのユーザ１９０の許可を調整することと見なすことができ、装置が電力低減状態にある場合、ユーザ１９０は装置５０２をどのように使用できるかが限定される可能性がある。様々な実現例では、ログイン／許可制御部５１２は、装置５０２の一部分を電力低減状態にするかまたは遷移させることができる。たとえば、ログイン／許可制御部５１２は、ユーザ１９０が検出ゾーン５５０内にいないかまたはそうではなくユーザ１９０が装置５０２に対してディスプレイ１１６を見ている可能性がないというステータスを有する（たとえば、ユーザ１９０の背中が装置５０２に向かっている可能性があるなど）場合に、ディスプレイ１１６をオフにするかまたはディスプレイ１１６の輝度を低減することができる。様々な実現例では、装置５０２は、様々な電力モード間での装置５０２の遷移を管理する電力制御部５３０を含むことができる。このような実現例では、ログイン／許可制御部５１２は、電力制御部５３０がこのような遷移を実行することを要求することができる。

【００７０】

逆に、ユーザ１９０が装置５０２と対話する可能性があるという状態にユーザ１９０のステータスが変化した場合、ログイン／許可制御部５１２は、装置５０２（またはその一部分）を電力低減モードから前の電力モードまたはアクティブ電力モード（たとえば、作業電力モードなど）に移動または遷移させることができる。様々な実現例では、ステータス変化検出および電力モード遷移は、図１、図２、図３、あるいは図４、またはこれらの組み合わせに関して上述した技法を介して自動的に行うことができる。

【００７１】

様々な実現例では、１つまたは複数のセキュリティ方式に対してユーザ１９０を認証することもできる。たとえば、ユーザ１９０は、ネットワーク、様々なファイル（たとえば、ネットワーク・ドライブ、暗号化ファイルなど）、ソフトウェアまたはＷｅｂサービス（たとえば、従業員データベース、金融Ｗｅｂサイトなど）にアクセスするために、認証または許可の詳細を提供している可能性がある。このような実現例では、これらのサービ

スまたはファイルのそれぞれが異なる許可方式を使用することができる。たとえば、第１のサービスは、ユーザ１９０が積極的に装置５０２からログアウトするまで、ユーザ１９０に許可を与えることができ、第２のサービスは、ユーザ１９０が装置５０２に向かっている限り、許可を与えることができるなどである。このような実現例では、ログイン／許可制御部５１２は、複数のサービスによって使用されるそれぞれのルール・システムまたは方式に基づいて、ユーザ１９０の許可を選択的に取り消すことができる。たとえば、上記の実現例では、カメラ１０６あるいはユーザ認識部１０８またはその両方によって検出された通り、ユーザ１９０が検出ゾーン５５０を離れることにより自分のステータスを変更する場合、ログイン／許可制御部５１２は、（検出ゾーン５５０から外へ移動することが積極的に装置５５０からログオフすることと見なされない場合）第１のサービスに対する許可を維持することができるが、第２のサービスに対する許可を取り消すことができる。

【００７２】

この文脈で、「セキュア・サービス（複数も可）」という用語は、このようなセキュア・サービスをユーザ１９０が使用する前にユーザ１９０の許可を必要とする１つまたは複数のサービス（たとえば、Ｗｅｂサイト、ファイル・アクセス、装置使用アクセスなど）であって、ユーザの許可レベルに基づいてユーザがセキュア・サービスを使用できる方法を制限または限定する可能性もあるものを指す。

【００７３】

様々な実現例では、セキュア・サービスに関するこのような認証または許可の詳細は、上述の通り、自動ログイン・プロセスの一部として自動的に提供されるかまたは提供されている可能性がある。他の実現例では、このような認証または許可の詳細は、ユーザ１９０によって手動でまたはその他の手段（たとえば、Ｗｅｂブラウザ内のクッキー、サードパーティ認証サービスによるユーザ名／パスワードのペアなど）を介して自動的に提供されている可能性がある。いくつかの実現例では、ユーザ１９０の許可は、ログイン／許可制御部５１２によって、全部または一部を管理することができる。

【００７４】

ログイン／許可制御部５１２が複数のセキュア・サービスに対するユーザ１９０の許可を選択的に取り消すかまたは調整することができるという例示されている実現例では、ログイン／許可制御部５１２は、これらのセキュア・サービスに関連するグラフィック情報の一部分がどのようにディスプレイ１１６によって表示されるかを変更することができる。たとえば、ユーザ１９０がセキュア・サービスに関連するＷｅｂサイトをＧＵＩウィンドウに含めるかまたは表示させ、ログイン／許可制御部５１２がそのセキュア・サービスに関するユーザ１９０の認証を取り消した場合、保護されているがもはや許可されていないＷｅｂサイトを含むかまたは表示しているＧＵＩウィンドウは、閉じられるか、薄暗くなるか、読めなくなるか、最小化されるか、またはその他の方法でディスプレイ１１６による表示から隠蔽または除去される可能性がある。同様に、保護されているがもはや許可されていないファイルまたはドキュメントは、閉じられるか、暗号化されるか、または隠蔽される可能性があり、そこに含まれる情報は無許可閲覧者（たとえば、後述の通り、図５Ｂのユーザ５９０ａ）にとってアクセス不能になる可能性がある。

【００７５】

様々な実現例では、ログイン／許可制御部５１２は、１つまたは複数のルールに基づいて装置５０２を使用するためのユーザ１９０の許可レベルを変更または調整することができる。たとえば、ログイン／許可制御部５１２は、ユーザ１９０が検出ゾーン５５０から不在であった時間量に基づいてユーザ１９０の許可レベルを変更または調整することができる。一実現例では、ユーザ１９０が比較的短期間の間（たとえば、３０秒、１分、または２分など）検出エリア５５０から不在であっただけである場合、ログイン／許可制御部５１２は、ディスプレイ１１６をロックするかまたはオフにするだけである可能性がある。それに対して、ユーザ１９０が比較的長期間の間（たとえば、５分、１０分、または２０分など）検出エリア５５０から不在であった場合、ログイン／許可制御部５１２は、ユ

ーザ１９０を装置５０２からログアウトさせ、装置５０２を電力低減モード（たとえば、電力中断モード、電力休止モードなど）にする可能性がある。

【００７６】

様々な実現例では、ログイン／許可制御部５１２は、様々な要因または尺度が１つまたは複数の閾値を超えるかどうかに基づいて、ユーザ１９０の許可レベルを調整する決定を行うことができる。いくつかの実現例では、これらの影響を及ぼす要因または尺度としては、１つまたは複数のシステム・リソースの可用性（たとえば、バッテリの電力レベル、ネットワークの帯域幅、ネットワーク・タイプ、プロセッサの能力、メモリ使用量、ストレージの可用性など）、１つまたは複数のシステム・リソースの消費速度、装置に関するユーザ１９０のステータスの変化が経過した時間量、ユーザ（たとえば、ユーザ１９０、図５Ｂのユーザ５９０ａなど）の物理的位置、装置５０２の物理的位置などを含むことができるが、これらに限定されない。

【００７７】

図５Ｂは、開示されている主題によるシステム５０１の実現例のブロック図である。一実現例では、システム５０１は、ユーザ１９０によって使用される装置５０２ｂを含むことができる。上述の通り、装置５０２ｂは、プロセッサ１１５と、メモリ１１４と、ディスプレイ１１６と、１つまたは複数のカメラ１０６と、ログイン／許可制御部５１２と、ログイン・ユーザインターフェース１１０と、ユーザ認識部１０８とを含むことができる。様々な実現例では、カメラ１０６は、上述の通り、カメラ１０６がその中で動作するように構成されている検出エリア５５０を含むかまたは有することができる。

【００７８】

例示されている実現例では、ユーザ１９０は、上述の通り、すでに検出され、装置５０２ｂにログインしている可能性がある。このため、ユーザ１９０のユーザデータ１２０は、上述の通り、進行中のロギングの一部として、メモリ１１４にロードされているかまたはその他の方法で装置５０２ｂに使用可能な状態になっている可能性がある。いくつかの実現例では、ユーザデータ１２０は、ユーザ１９０による装置５０２ｂの使用の一部として、変更または編集されている可能性がある。たとえば、ユーザ１９０は、様々なドキュメントまたはタブ、変更した構成設定（たとえば、電子メール・サーバ、ネットワーク設定など）、あるいはその他の形式のユーザデータ１２０を開くかまたは閉じている可能性がある。

【００７９】

例示されている実現例では、ユーザ５９０ａが検出エリア５５０に入る可能性がある。第２または追加のユーザ（たとえば、ユーザ５９０ａまたはユーザ５９０ｂが検出エリア５５０に入る場合はユーザ５９０ｂなど）の追加は、装置５０２ｂに関する第１のユーザ１９０のステータスの変化と見なすことができる。このような実現例では、ログイン／許可制御部５１２は、装置５０２ｂに関する第１のユーザ１９０の許可を変更または調整することができる。

【００８０】

たとえば、一実現例では、ログイン／許可制御部５１２は、ディスプレイ１１６によって表示されている情報であって、新しいユーザ５９０ａが見るための許可を受けていない情報をそのユーザ５９０ａが見られないように、ディスプレイ１１６を薄暗くするかまたはオフにすることができる。同様に、音声出力またはその他の出力を制限することもできる。このような出力の制限は実質的に、装置５０２ｂのディスプレイ１１６、音声出力、またはその他の出力を視聴するために第１のユーザ１９０が前に持っていた許可を取り消す可能性がある。

【００８１】

他の実現例では、ログイン／許可制御部５１２は、第２のユーザ５９０ａの身元を判別することができる。いくつかの実現例では、これは、新しいユーザ５９０ａに関連するユーザデータ５２０ａにアクセスすることを含むことができる。この識別に基づいて、ログイン／許可制御部５１２は、第２のユーザ５９０ａが保持している許可レベルを判別する

ことができる。ログイン／許可制御部５１２は、新しいユーザ５９０ａの許可レベルを第１のユーザ１９０の許可レベルと比較することができる。上述の通り、様々なセキュア・サービスについて様々な許可レベルが存在する可能性がある。このような実現例では、ログイン／許可制御部５１２は、第１のユーザ１９０の第１の許可レベルおよび第２のユーザ５９０ａの第２の許可レベルに基づいて、装置５０２ｂの使用を制限することができる。

【００８２】

たとえば、一実現例では、装置５０２ｂは、ディスプレイ１１６によって表示されている情報がユーザ１９０とユーザ５９０ａの両方によって表示される許可を受けていない場合、ディスプレイ１１６（またはその他の出力装置など）を薄暗くするかまたはオフにすることができる。他の実現例では、ディスプレイ１１６は、ユーザ１９０とユーザ５９０ａの両方によって表示される許可を受けていない情報を含むディスプレイ１１６の一部分（たとえば、ＧＵＩウィンドウなど）を薄暗くするかまたは隠蔽することができるが、両方のユーザ１９０および５９０ａに対して表示できる部分は変更されないまたは目に見える状態である可能性がある。このような実現例では、ログイン／許可制御部５１２は、第１のユーザ１９０の有効許可レベルを、ユーザ１９０の実際の許可レベルから、検出エリア５５０内のすべてのユーザ（たとえば、ユーザ１９０およびユーザ５９０ａなど）の許可レベルの共通部分（集合論の用語）に対応する許可レベルに調整することができる。

【００８３】

他の実現例では、ログイン／許可制御部５１２は、ユーザ１９０の有効許可レベルを、ユーザ１９０またはユーザ５９０ａのいずれか一方の高い方の許可レベルに調整することができる。他の実現例では、ログイン／許可制御部５１２は、有効許可レベルを、ユーザ１９０および５９０ａの許可レベルの和集合（この場合も集合論の用語）に調整することができる。様々な実現例では、ユーザ１９０の許可レベルを調整し、装置５０２ｂが調整された許可レベルと一致している方法で使用されるのを禁止するためのその他のルールまたは方式を使用することができる。

【００８４】

一実現例では、ユーザ５９０ａが検出エリア５５０を離れるかまたはそこから不在の状態になり、ユーザ１９０が検出エリア５５０内に単独で残される場合、装置に対するユーザ１９０のステータスが変化している可能性がある。このような実現例では、ログイン／許可制御部５１２は、ユーザ１９０の許可レベルをユーザ１９０の前の認証レベルまたは本来の認証レベルに戻すかまたは再調整することができる。他の実現例では、追加のユーザ（たとえば、ユーザ５９０ｂ）が検出エリア５５０に入った場合、この場合もユーザ１９０のステータスが変化している可能性があり、ログイン／許可制御部５１２は、この場合も、検出エリア５５０内のユーザ（たとえば、ユーザ１９０、５９０ａ、５９０ｂ、ユーザ１９０および５９０ｂなど）に基づいて、ユーザ１９０の許可レベルを調整することができる。

【００８５】

様々な実現例では、装置５０２ｂに関するユーザ１９０のステータスの変化の検出は、他のユーザ（たとえば、ユーザ５９０ａなど）の検出または他のユーザの存在の退去の検出と、二次的な考慮事項（たとえば、時間要素など）の両方によってトリガされる可能性がある。たとえば、ユーザ１９０のステータスの変化を発生させるために、ユーザ５９０ａは、検出エリア５５０内に入ることと、所定の分数または秒数の間（たとえば、１０秒など）検出エリア５５０内に存在を維持することの両方を行わなければならない可能性がある。このような実現例では、「誤検出」またはその他の統計誤差の発生を低減することができる。たとえば、ユーザ５９０ｂが歩いていて不注意で装置５０２ｂの検出エリア５５０内に入ってしまっただけでディスプレイ１１６が突然オフになることは、ユーザ１９０を混乱させることになる可能性がある。このような実現例では、ログイン／許可制御部５１２は、何らかの閾値またはヒステリシス効果を使用して、装置に関するユーザ１９０のステータスの望ましくない変化または頻繁な変化を低減することができる。

【００８６】
図５Ｃは、開示されている主題によるシステム５０１の実現例のブロック図である。一実現例では、システム５０１は、ユーザ１９０によって使用される装置５０２ｃを含むことができる。上述の通り、装置５０２ｃは、プロセッサ１１５と、メモリ１１４と、ディスプレイ１１６と、１つまたは複数のカメラ１０６と、ログイン／許可制御部５１２と、ログイン・ユーザインターフェース１１０と、ユーザ認識部１０８とを含むことができる。様々な実現例では、カメラ１０６は、上述の通り、カメラ１０６がその中で感知または動作するように構成されている検出エリア５５０を含むかまたは有することができる。
【００８７】
例示されている実現例では、ユーザ１９０は、上述の通り、すでに検出され、装置５０２ｃにログインしている可能性がある。このため、ユーザ１９０のユーザデータ１２０は、上述の通り、進行中のロギングの一部として、メモリ１１４にロードされているかまたはその他の方法で装置５０２ｃに使用可能な状態になっている可能性がある。例示されている実現例では、ユーザ１９０のユーザデータ１２０は、保存することができるかまたはアクティブ・ユーザデータ５２２であると見なすことができる。例示されている実現例では、アクティブ・ユーザデータ５２２は、装置５０２ｃに積極的にログインしたユーザに関するユーザデータを含むことができる。いくつかの実現例では、ユーザデータ１２０または５２２は、上述の通り、ユーザ１９０による装置５０２ｃの使用の一部として、変更または編集されている可能性がある。
【００８８】
例示されている実現例では、ユーザ５９０ａが検出エリア５５０に入る可能性がある。第２または追加のユーザ（たとえば、ユーザ５９０ａまたはユーザ５９０ｂが検出エリア５５０に入る場合はユーザ５９０ｂなど）の追加は、装置５０２ｃに関する第１のユーザ１９０のステータスの変化と見なすことができる。このような実現例では、ログイン／許可制御部５１２は、図５Ｂに関して上述した通り、装置５０２ｃに関する第１のユーザ１９０の許可を変更または調整することができる。
【００８９】
しかし、例示されている実現例では、ユーザ１９０はその後、検出ゾーン５５０を離れることを選択する可能性がある。このような実現例では、検出エリア５５０からのユーザ１９０の不在は、装置５０２ｃに関するユーザ１９０のステータスの変化を発生させる可能性がある。図５Ａに関して上述した通り、ログイン／許可制御部５１２は、ユーザ１９０を装置５０２ｃからログアウトさせることにより、第１のユーザ１９０の許可を変更または調整することができる。様々な実現例では、これは、アクティブ・ユーザデータ５２２のステータスからユーザ１９０のユーザデータ１２０を除去することを含むことができる。他の実現例では、ログイン／許可制御部５１２は、（たとえば、画面ロック、パスワード再許可などにより）ユーザ１９０を装置５０２ｃからロックアウトすることができる。
【００９０】
一実現例では、ユーザ５９０ａは検出エリア５５０内で一人になる可能性がある。このような実現例では、ログイン／許可制御部５１２は、図１、図２、図３、および図４に関して上述した通り、第２のユーザ５９０ａの身元を自動的に判別し、第２のユーザまたは新しいユーザ５９０ａを装置５０２ｃに自動的にログインさせることができる。このような実現例では、ユーザ５９０ａのユーザデータ５２０ａはアクティブ・ユーザデータ５２２と見なされるかまたはそれになる可能性がある。
【００９１】
様々な実現例では、ユーザ１９０は装置５０２ｃからログアウトするかまたはその制御を放棄するためのその他の手段を選択することができる。たとえば、一実現例では、ユーザ１９０は、検出エリア５５０内に留まるが、ユーザ５９０ａの後ろに移動する可能性がある。たとえば、ユーザ１９０は装置５０２ｃの正面の椅子から立ち上がる可能性があり、次にユーザ５９０ａがその椅子に座る可能性があり、ユーザ１９０がユーザ５９０ａの

後ろに立つ可能性がある。逆に、いくつかの実現例では、ユーザ１９０は、上述の通り、積極的に装置５０２ｃからログアウトするかまたは自分自身をロックアウトする可能性がある。このような実現例では、ログイン／許可制御部５１２は、第１のユーザ１９０が装置５０２ｃの制御を第２のユーザ５９０ｂに譲り渡した時期を判別するように構成することができる。

【００９２】

様々な実現例では、ログイン／許可制御部５１２は、アクティブ・ユーザデータ５２２を新しい第２のユーザ５９０ｂのユーザデータ５２０ｂで、全部または一部を置き換えるように構成することができる。たとえば、一実現例では、ログイン／許可制御部５１２は、第１のユーザ１９０の構成を維持し、ユーザデータ１２０またはその一部分をアクティブ・ユーザデータ５２２として設定しながら、装置５０２ｃを使用できる用途および方法を管理する許可レベルを、第１のユーザ１９０の許可レベルから第２のユーザ５９０ｂの許可レベルに変更するように構成することができる。このような実現例では、より高いかまたは大きい許可レベルを有する制御部またはユーザ（たとえば、ユーザ５９０ａなど）は、ユーザ１９０を装置５０２ｃから完全にログアウトさせずに、自分のより高い許可レベルで装置５０２ｃに一時的にアクセスするかまたはそれを使用することができる。

【００９３】

図６は、開示されている主題によるシステム６００の実現例のブロック図である。一実現例では、システム６００は、ユーザ１９０によって使用される装置６０２を含むことができる。上述の通り、装置６００は、プロセッサ１１５と、メモリ１１４と、ディスプレイ１１６と、１つまたは複数のカメラ１０６と、ログイン／許可制御部６１２と、電力制御部６３０と、ログイン・ユーザインターフェース１１０と、ユーザ認識部１０８とを含むことができる。様々な実現例では、カメラ１０６は、上述の通り、カメラ１０６がその中で感知または動作するように構成されている検出エリア（図６では図示せず）を含むかまたは有することができる。

【００９４】

例示されている実現例では、ユーザ１９０は、上述の通り、すでに検出され、装置６０２にログインしている可能性がある。このため、ユーザ１９０のユーザデータ１２０は、上述の通り、進行中のロギングの一部として、メモリ１１４にロードされているかまたはその他の方法で装置６０２に使用可能な状態になっている可能性がある。いくつかの実現例では、ユーザデータ１２０は、上述の通り、ユーザ１９０による装置６０２の使用の一部として、変更または編集されている可能性がある。

【００９５】

一実現例では、カメラ１０６またはユーザ認識部１０８は、装置に関するユーザ１９０の注意をモニターするように構成することができる。この文脈で、「装置に対する注意」とは、何らかの関心または集中力を持って装置の出力（たとえば、ディスプレイ１１６など）を聞くまたは見ることあるいは（たとえば、キーボード、マウス、タッチスクリーンなどにより）装置６０２に情報または命令を入力することを含むことができる。このような実現例では、装置６０２は、装置に関するユーザ１９０の注意をモニターするように構成されたアテンション・モニター（attention monitor）６０８を含むことができる。様々な実現例では、アテンション・モニター６０８は、装置６０２のカメラ１０６、ユーザ認識部１０８、ログイン／許可制御部６１２、またはその他のコンポーネントに含めることができる。

【００９６】

様々な実現例では、アテンション・モニター６０８は、ユーザ１９０の目の位置または動き、ユーザの頭の向き（たとえば、ユーザ１９０が装置６０２を見ているかまたは装置６０２から目をそらしている場合など）、上述の通り、ユーザ１９０の存在または不在、ユーザ１９０の入力速度（たとえば、所与の期間あたりのキーストロークまたはマウスの動きなど）などをモニターすることにより、ユーザ１９０の注意を測定することができる。

【００９７】
様々な実現例では、アテンション・モニター６０８は、１つまたは複数のルールまたは閾値に基づいて、ユーザ１９０の注意を判断することができる。たとえば、ユーザ１９０が比較的短期間の間（たとえば、５秒など）装置６０２から目をそらしている場合、アテンション・モニター６０８は、ユーザ１９０が依然として装置６０２対して注意していると判断することができる。逆に、ユーザ１９０が比較的長期間の間（たとえば、１分、５分など）目をそらしている場合、アテンション・モニター６０８は、ユーザ１９０がもはや装置６０２に対して注意していないと判断することができる。
【００９８】
一実現例では、装置６０２に対するユーザ１９０の注意の変化は、装置６０２に関するユーザ１９０のステータスの変化と見なすことができる。このような実現例では、ログイン／許可制御部６１２は、上述の通り、ユーザ１９０の許可レベルを調整することができる（たとえば、ユーザ１９０を装置６０２からログアウトさせること、装置６０２を低電力モードにすることなど）。様々な実現例では、ログイン／許可制御部６１２は、ユーザ１９０の許可レベルを調整することができ、これは、アプリケーションの実行を休止すること、１つまたは複数のセキュア・サービスからユーザ１９０を認証解除すること、あるいは装置６０２の１つまたは複数の部分を電力低減モードにすることなどを含むことができる。
【００９９】
たとえば、例示されている実現例では、ユーザ１９０が自分の頭の向きを装置６０２からそらした場合、ログイン／許可制御部６１２はディスプレイ１１６をオフにすることができる。ユーザ１９０の頭の向きを装置６０２に戻すことにより装置６０２に関するユーザ１９０のステータスがもう一度変化したことをアテンション・モニター６０８が検出すると、ログイン／許可制御部６１２は、ディスプレイ１１６をオンに戻すことによりユーザ１９０の許可レベルを調整することができる。
【０１００】
いくつかの実現例では、アテンション・モニター６０８は、装置６０２上で実行されているアプリケーション（複数も可）を考慮しながら、ユーザ１９０の注意を判断することができる。たとえば、ユーザ１９０がワードプロセシング・アプリケーションとは対照的に動画アプリケーションを実行している場合に、上述の閾値またはルールは注意のなさをより大きく考慮に入れることができる。このような実現例では、ユーザ１９０が比較的長期間の間（たとえば、５分など）目をそらしているが、動画が装置６０２上で再生されている場合、アテンション・モニター６０８は、ユーザ１９０が依然として装置６０２に注意していると判断することができる。しかし、ユーザ１９０が極めて長期間の間（たとえば、１５分など）目をそらしていて、動画が装置６０２上で再生されている場合、アテンション・モニター６０８は、ユーザ１９０がもはや装置６０２を注意していないと判断することができる。
【０１０１】
たとえば、他の実現例では、ログイン／許可制御部６１２は、ユーザ１９０が装置６０２から目をそらしている場合に、ビデオ・アプリケーションの実行を休止することができる。しかし、ログイン／許可制御部６１２は、ユーザ１９０が装置６０２から目を離している場合に、オーディオ・アプリケーションの実行を休止しないと決定する場合もある。その代わり、ログイン／許可制御部６１２は、ユーザ１９０が装置６０２から歩き去った場合に、オーディオ・アプリケーションの実行をミュートまたは休止すると決定する可能性がある。
【０１０２】
さらに他の実現例では、ログイン／許可制御部６１２は、装置６０２にとって使用可能なシステム・リソースのレベルに基づいて、ユーザ１９０の許可レベルをどのように調整するかを決定することができる。たとえば、ログイン／許可制御部６１２は、装置６０２が外部電源を使用している（たとえば、コンセントに差し込まれているなど）場合、ディ

スプレイ１１６をオフにしない可能性がある。しかし、装置６０２がバッテリを使用して電力を供給している場合、ログイン／許可制御部６１２は、より積極的に装置６０２の電力消費量を削減する可能性がある。

【０１０３】

ユーザの存在または注意を判別するために顔認識技術を使用することは、過去に使用されていた場合より、高電力状態と低電力状態との間でより動的な装置の切り替えを可能にすることができ、その結果、装置６０２についてエネルギー節約およびバッテリ寿命の延長が可能になる。たとえば、所定のタイムアウト期間の満了に基づいて装置６０２を高電力状態から低電力状態に切り替える決定を行うのではなく、ユーザ１９０がもはや装置の正面に存在しない場合またはユーザがもはや装置に注意していない場合に、装置６０２を低電力状態に切り替えることができる。その後、カメラ１０６またはユーザ認識部１０８またはアテンション・モニター６０８によって判断された通り、ユーザ１９０が装置に戻るかまたはもう一度、装置６０２に注意している場合、装置を低電力状態から高電力状態に切り替えることができる。

【０１０４】

所定のタイムアウトの満了ではなく、ユーザの不在または注意欠如の自動検出を高電力状態から低電力状態への変更の条件とすることにより、ユーザ１９０が実際に装置６０２を使用していない場合に装置６０２を適切な時期に低電力状態に切り替えることができる。所定のタイムアウト期間はときにはユーザが依然として装置を使用している時間に対応し、したがって、ユーザの経験を妨害する可能性があり、その他の時期にはユーザが装置の使用を止めた後の長い時間に対応し、したがって、エネルギーまたはバッテリ寿命を浪費する可能性がある。したがって、ユーザの不在または注意欠如の検出に基づいて装置６０２を高電力状態から低電力状態に自動的に遷移させると、その結果、装置６０２のエネルギー効率が向上する可能性がある。

【０１０５】

同様に、装置６０２を低電力状態から高電力状態に自動的に遷移させるためにカメラ１０６、ユーザ認識部１０８、およびアテンション・モニター６０８によって提供される顔認識技術を使用することは、装置を低電力状態から高電力状態に遷移させるために、ユーザが英数字情報を入力したり、装置６０２のいずれかのキーを押す必要がない可能性があるので、より良好でよりシームレスな経験をユーザに提供する。その経験はユーザにとってよりシームレスなものになるので、低電力状態と高電力状態との遷移はユーザにとってあまり邪魔なものではなくなり、したがって、ユーザは装置６０２によって提供されるエネルギー節約型の電力管理技法をより自発的に使用する可能性がある。

【０１０６】

図７は、開示されている主題による技法の実現例の流れ図である。様々な実現例では、技法８００は、図１、図２、図３、図４、図５、図６、または図１０のものなどのシステムによって使用または生成することができる。開示されている主題は技法８００によって示されているアクションの順序または数に限定されないことは言うまでもない。

【０１０７】

ブロック７０２は、一実現例において、上述の通り、コンピューティング・デバイスに動作可能に結合されたカメラを介して第１のユーザの画像を受信できることを示している。ブロック７０４は、一実現例において、受信画像に基づいて第１のユーザの身元を判別できることを示している。ブロック７０６は、一実現例において、判別された身元が所定の身元と一致する場合に、少なくとも第１のユーザの身元が所定の身元と一致することに基づいて、第１のユーザをコンピューティング・デバイスにログインさせることができることを示している。

【０１０８】

図８は、本明細書に記載されている技法を使用できる汎用コンピュータ・デバイス８００および汎用モバイル・コンピュータ・デバイス８５０の一例を示している。コンピューティング・デバイス８００は、ラップトップ、デスクトップ、ワークステーション、携帯

情報端末、サーバ、ブレード・サーバ、メインフレーム、およびその他の適切なコンピュータなど、様々な形のデジタル・コンピュータを表すためのものである。コンピューティング・デバイス８５０は、携帯情報端末、携帯電話、スマートフォン、およびその他の同様のコンピューティング・デバイスなど、様々な形のモバイル・デバイスを表すためのものである。本明細書に示されているコンポーネント、その接続および関係、ならびにその機能は、模範的なものに過ぎず、本明細書に記載されているかあるいは請求されているかまたはその両方がなされている本発明の実現例を限定するためのものではない。

【０１０９】

コンピューティング・デバイス８００は、プロセッサ８０２と、メモリ８０４と、記憶装置８０６と、メモリ８０４および高速拡張ポート８１０に接続する高速インターフェース８０８と、低速バス８１４および記憶装置８０６に接続する低速インターフェース８１２とを含む。コンポーネント８０２、８０４、８０６、８０８、８１０、および８１２のそれぞれは、様々なバスを使用して相互接続され、共通マザーボード上にまたはその他の方法で適宜装着することができる。プロセッサ８０２は、高速インターフェース８０８に結合されたディスプレイ８１６などの外部入出力装置上でＧＵＩ用のグラフィック情報を表示するためにメモリ８０４内にまたは記憶装置８０６上に保存された命令を含む、コンピューティング・デバイス８００内で実行するための命令を処理することができる。その他の実現例では、複数のメモリおよび複数のメモリ・タイプとともに、複数のプロセッサあるいは複数のバスまたはその両方を適宜使用することができる。また、複数のコンピューティング・デバイス８００を接続し、それぞれのデバイスが（たとえば、サーバ・バンク、ブレード・サーバ・グループ、またはマルチプロセッサ・システムとして）必要な動作の各部分を提供することができる。

【０１１０】

メモリ８０４はコンピューティング・デバイス８００内で情報を保存する。一実現例では、メモリ８０４は１つまたは複数の揮発性メモリ・ユニットである。他の実現例では、メモリ８０４は１つまたは複数の不揮発性メモリ・ユニットである。また、メモリ８０４は、磁気ディスクまたは光ディスクなど、他の形のコンピュータ可読媒体にすることもできる。

【０１１１】

記憶装置８０６は、コンピューティング・デバイス８００のための大容量記憶装置を提供することができる。一実現例では、記憶装置８０６は、フロッピー・ディスク装置、ハードディスク装置、光ディスク装置、またはテープ装置、フラッシュ・メモリまたはその他の同様のソリッドステート・メモリ・デバイス、あるいはストレージ・エリア・ネットワークまたはその他の構成のデバイスを含むデバイス・アレイなどのコンピュータ可読媒体にすることができるかまたはそれを含むことができる。コンピュータ・プログラム・プロダクトは情報担体において有形に実施することができる。コンピュータ・プログラム・プロダクトは、実行されたときに、上記のものなどの１つまたは複数の方法を実行する命令も含むことができる。情報担体は、メモリ８０４、記憶装置８０６、またはプロセッサ８０２上のメモリなどのコンピュータ可読媒体または機械可読媒体である。

【０１１２】

高速コントローラ８０８はコンピューティング・デバイス８００に関する帯域幅集約型動作を管理し、低速コントローラ８１２はより低い帯域幅集約型動作を管理する。このような機能の割り振りは模範的なものに過ぎない。一実現例では、高速コントローラ８０８は、メモリ８０４、ディスプレイ８１６（たとえば、グラフィックス・プロセッサまたはアクセラレータを介する）、および様々な拡張カード（図示せず）受け入れることができる高速拡張ポート８１０に結合される。この実現例では、低速コントローラ８１２は、記憶装置８０６および低速拡張ポート８１４に結合される。低速拡張ポートは、様々な通信ポート（たとえば、ＵＳＢ、Ｂｌｕｅｔｏｏｔｈ、イーサネット、ワイヤレス・イーサネット）を含むことができ、キーボード、ポインティング・デバイス、スキャナ、または、たとえば、ネットワーク・アダプタを介するスイッチまたはルータなどのネットワーキン

グ・デバイスなどの１つまたは複数の入出力装置に結合することができる。

【０１１３】

コンピューティング・デバイス８００は、同図に示されている通り、いくつかの異なる形で実現することができる。たとえば、これは、１台の標準的なサーバ８２０として実現するかまたはこのようなサーバのグループ内で複数回実現することができる。また、これは、ラック・サーバ・システム８２４の一部として実現することもできる。加えて、これは、ラップトップ・コンピュータ８２２などのパーソナル・コンピュータ内に実現することもできる。代わって、コンピューティング・デバイス８００からのコンポーネントは、デバイス８５０などのモバイル・デバイス（図示せず）内のその他のコンポーネントと組み合わせることができる。このようなデバイスのそれぞれはコンピューティング・デバイス８００、８５０のうちの１つまたは複数を含むことができ、システム全体は、相互に通信する複数のコンピューティング・デバイス８００、８５０で構成することができる。

【０１１４】

コンピューティング・デバイス８５０は、数あるコンポーネントの中でも特に、プロセッサ８５２と、メモリ８６４と、ディスプレイ８５４などの入出力装置と、通信インターフェース８６６と、トランシーバ８６８とを含む。デバイス８５０には、追加の記憶域を提供するために、マイクロドライブまたはその他のデバイスなどの記憶装置も設けることができる。コンポーネント８５０、８５２、８６４、８５４、８６６、および８６８のそれぞれは、様々なバスを使用して相互接続され、これらのコンポーネントのうちのいくつかは共通マザーボード上にまたはその他の方法で適宜装着することができる。

【０１１５】

プロセッサ８５２は、メモリ８６４内に保存された命令を含む、コンピューティング・デバイス８５０内の命令を実行することができる。このプロセッサは、個別かつ複数のアナログおよびデジタル・プロセッサを含む、複数チップのチップセットとして実現することができる。このプロセッサは、たとえば、ユーザインターフェースの制御、デバイス８５０によって実行されるアプリケーション、およびデバイス８５０による無線通信など、デバイス８５０のその他のコンポーネントの協調を可能にすることができる。

【０１１６】

プロセッサ８５２は、ディスプレイ８５４に結合された制御インターフェース８５８およびディスプレイ・インターフェース８５６を介してユーザと通信することができる。ディスプレイ８５４は、たとえば、ＴＦＴ　ＬＣＤ（薄膜トランジスタ液晶ディスプレイ）またはＯＬＥＤ（有機発光ダイオード）ディスプレイあるいはその他の適切なディスプレイ技術にすることができる。ディスプレイ・インターフェース８５６は、グラフィックおよびその他の情報をユーザに提示するためにディスプレイ８５４を駆動するための適切な回路を含むことができる。制御インターフェース８５８は、ユーザからコマンドを受け取り、プロセッサ８５２にサブミットするためにそれを変換することができる。加えて、デバイス８５０と他のデバイスとのニアエリア通信を可能にするために、プロセッサ８５２と連絡している外部インターフェース８６２を設けることができる。外部インターフェース８６２は、たとえば、いくつかの実現例では有線通信を可能にし、またはその他の実現例では無線通信を可能にすることができ、複数のインターフェースを使用することもできる。

【０１１７】

メモリ８６４はコンピューティング・デバイス８５０内で情報を保存する。メモリ８６４は、１つまたは複数のコンピュータ可読媒体、１つまたは複数の揮発性メモリ・ユニット、あるいは１つまたは複数の不揮発性メモリ・ユニットのうちの１つまたは複数として実現することができる。拡張メモリ８７４を設け、たとえば、ＳＩＭＭ（シングル・インライン・メモリ）カード・インターフェースを含むことができる拡張インターフェース８７２を介してデバイス８５０に接続することもできる。このような拡張メモリ８７４は、デバイス８５０に余分な記憶空間を提供することができ、あるいは、デバイス８５０用のアプリケーションまたはその他の情報を保存することもできる。具体的には、拡張メモリ

８７４は、上記のプロセスを実行するかまたは補うための命令を含むことができ、セキュア情報を含むこともできる。したがって、たとえば、拡張メモリ８７４は、デバイス８５０のためのセキュリティとして設けることができ、デバイス８５０の安全な使用を可能にする命令でプログラミングすることもできる。加えて、非ハッカブルな方法でＳＩＭＭカード上に識別情報を載せることなど、追加情報とともに、ＳＩＭＭカードを介してセキュア・アプリケーションを提供することもできる。

【０１１８】

メモリは、後述の通り、たとえば、フラッシュ・メモリあるいはＮＶＲＡＭメモリまたはその両方を含むことができる。一実現例では、コンピュータ・プログラム・プロダクトは情報担体において有形に実施される。コンピュータ・プログラム・プロダクトは、実行されたときに、上記のものなどの１つまたは複数の方法を実行する命令を含む。情報担体は、たとえば、トランシーバ８６８または外部インターフェース８６２により受け取ることができる、メモリ８６４、拡張メモリ８７４、またはプロセッサ８５２上のメモリなどのコンピュータ可読媒体または機械可読媒体である。

【０１１９】

デバイス８５０は、必要な場合にデジタル信号処理回路を含むことができる通信インターフェース８６６を介して無線で通信することができる。通信インターフェース８６６は、数ある中でも特に、ＧＳＭ音声呼び出し、ＳＭＳ、ＥＭＳ、またはＭＭＳメッセージング、ＣＤＭＡ、ＴＤＭＡ、ＰＤＣ、ＷＣＤＭＡ、ＣＤＭＡ２０００、またはＧＰＲＳなどの様々なモードまたはプロトコルに基づく通信を可能にすることができる。このような通信は、たとえば、無線周波トランシーバ８６８を介して行うことができる。加えて、短距離通信は、Ｂｌｕｅｔｏｏｔｈ、ＷｉＦｉ、またはその他のこのようなトランシーバ（図示せず）などを使用して、行うことができる。加えて、ＧＰＳ（全地球測位システム）レシーバ８７０は追加のナビゲーション関連および位置関連の無線データをデバイス８５０に提供することができ、このデータはデバイス８５０上で実行されるアプリケーションによって適宜使用することができる。

【０１２０】

デバイス８５０はオーディオ・コーデック８６０を使用して聞こえるように通信することもでき、このオーディオ・コーデックはユーザからの口語情報を受信し、それを使用可能なデジタル情報に変換することができる。オーディオ・コーデック８６０は、同様に、たとえば、デバイス８５０のハンドセット内のスピーカなどを介して、ユーザのために可聴音を発生することができる。このような音は、音声電話呼び出しからの音を含むことができ、記録された音（たとえば、音声メッセージ、音楽ファイルなど）を含むことができ、また、デバイス８５０上で動作しているアプリケーションによって生成された音を含むこともできる。

【０１２１】

コンピューティング・デバイス８５０は、同図に示されている通り、いくつかの異なる形で実現することができる。たとえば、これは、携帯電話８８０として実現することができる。また、これは、スマートフォン８８２、携帯情報端末、またはその他の同様のモバイル・デバイスの一部として実現することもできる。

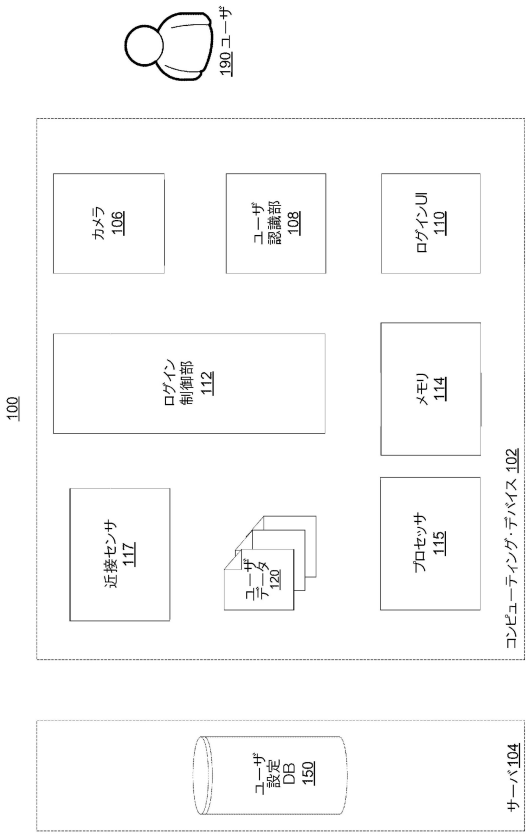
【０１２２】

本明細書に記載されているシステムおよび技法の様々な実現例は、デジタル電子回路、集積回路、特別設計ＡＳＩＣ（特定用途向け集積回路）、コンピュータ・ハードウェア、ファームウェア、あるいはソフトウェア、またはこれらの組み合わせで実現することができる。これらの様々な実現例は、記憶システム、少なくとも１つの入力装置、および少なくとも１つの出力装置からデータおよび命令を受信するためならびにこれらに対してデータおよび命令を送信するために結合され、専用または汎用である可能性のある、少なくとも１つのプログラマブル・プロセッサを含むプログラマブル・システム上で実行可能あるいは解釈可能またはその両方である１つまたは複数のコンピュータ・プログラムにおける実現例を含むことができる。

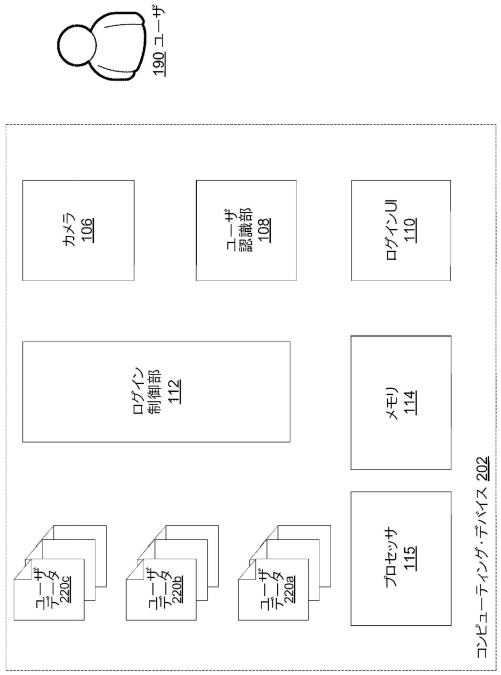
【０１２３】
これらのコンピュータ・プログラム（プログラム、ソフトウェア、ソフトウェア・アプリケーション、またはコードとしても知られている）は、プログラマブル・プロセッサ用の機械命令を含み、高レベル手続き型あるいはオブジェクト指向またはその両方のプログラミング言語で、あるいはアセンブリ／機械語で、もしくはその両方で実現することができる。本明細書で使用する「機械可読媒体」、「コンピュータ可読媒体」という用語は、機械可読信号として機械命令を受信する機械可読媒体を含み、プログラマブル・プロセッサに機械命令あるいはデータまたはその両方を提供するために使用される任意のコンピュータ・プログラム・プロダクト、装置、あるいはデバイス（たとえば、磁気ディスク、光ディスク、メモリ、プログラム可能論理デバイス（ＰＬＤ））、またはこれらの組み合わせを指す。「機械可読信号」という用語は、プログラマブル・プロセッサに機械語あるいはデータまたはその両方を提供するために使用される任意の信号を指す。
【０１２４】
ユーザとの対話を可能にするために、本明細書に記載されているシステムおよび技法は、ユーザに対して情報を表示するための表示装置（たとえば、ＣＲＴ（陰極線管）またはＬＣＤ（液晶ディスプレイ）モニター）ならびにそれによりユーザがコンピュータに対して入力を提供することができるキーボードおよびポインティング・デバイス（たとえば、マウスまたはトラックボール）を有するコンピュータ上に実現することができる。ユーザとの対話を可能にするためにその他の種類のデバイスを使用することもでき、たとえば、ユーザに提供されるフィードバックは任意の形の感覚フィードバック（たとえば、視覚フィードバック、聴覚フィードバック、または触覚フィードバック）にすることができ、ユーザからの入力は、音響、音声、または触覚入力を含む、任意の形で受け取ることができる。
【０１２５】
本明細書に記載されているシステムおよび技法は、バックエンド・コンポーネント（たとえば、データ・サーバとして）を含むか、ミドルウェア・コンポーネント（たとえば、アプリケーション・サーバ）を含むか、またはフロントエンド・コンポーネント（たとえば、それによりユーザが本明細書に記載されたシステムおよび技法の実現例と対話できるグラフィカル・ユーザインターフェースまたはＷｅｂブラウザを有するクライアント・コンピュータ）を含むか、またはこのようなバックエンド・コンポーネント、ミドルウェア・コンポーネント、あるいはフロントエンド・コンポーネントの任意の組み合わせを含む、コンピューティング・システムで実現することができる。システムのコンポーネントは、任意の形または媒体のデジタル・データ通信（たとえば、通信ネットワーク）によって相互接続することができる。通信ネットワークの例としては、ローカル・エリア・ネットワーク（「ＬＡＮ」）、広域ネットワーク（「ＷＡＮ」）、およびインターネットを含む。
【０１２６】
このコンピューティング・システムはクライアントとサーバを含むことができる。クライアントとサーバは一般に相互に遠く離れており、典型的に通信ネットワークにより相互に作用する。クライアントとサーバの関係は、それぞれのコンピュータ上で実行され、相互にクライアント・サーバの関係を有するコンピュータ・プログラムにより発生する。
【０１２７】
いくつかの実現例が記載されている。それにもかかわらず、本発明の精神および範囲を逸脱せずに様々な変更が可能であることは理解されるであろう。
【０１２８】
加えて、望ましい結果を達成するために、図に描写されている論理の流れは、示されている特定の順序または順番を必要としない。加えて、その他のステップを提供することができるかまたは記載されている流れから複数ステップを除去することができ、記載されているシステムにその他のコンポーネントを追加することができるかまたはそのシステムからその他のコンポーネントを除去することができる。したがって、その他の実現例は特許

請求の範囲に含まれるものである。

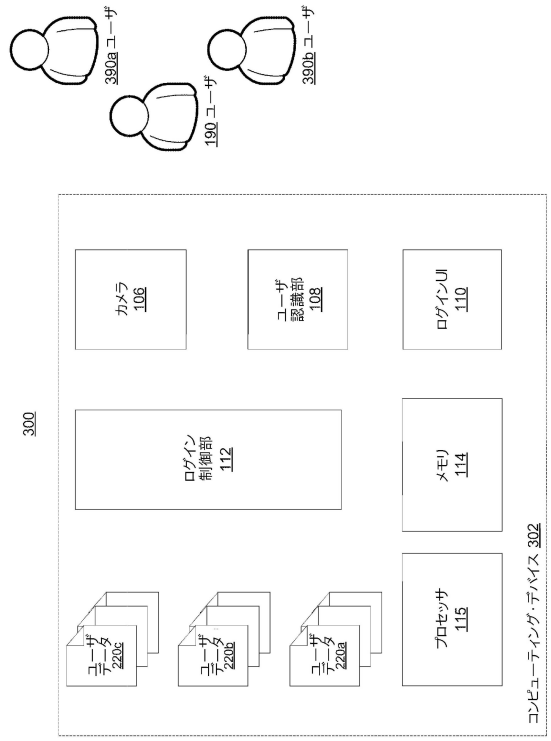
【図１】



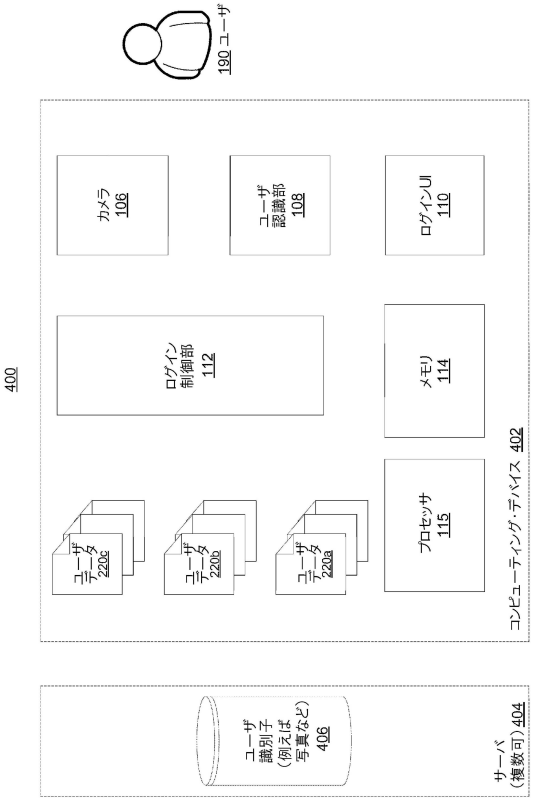
【図２】



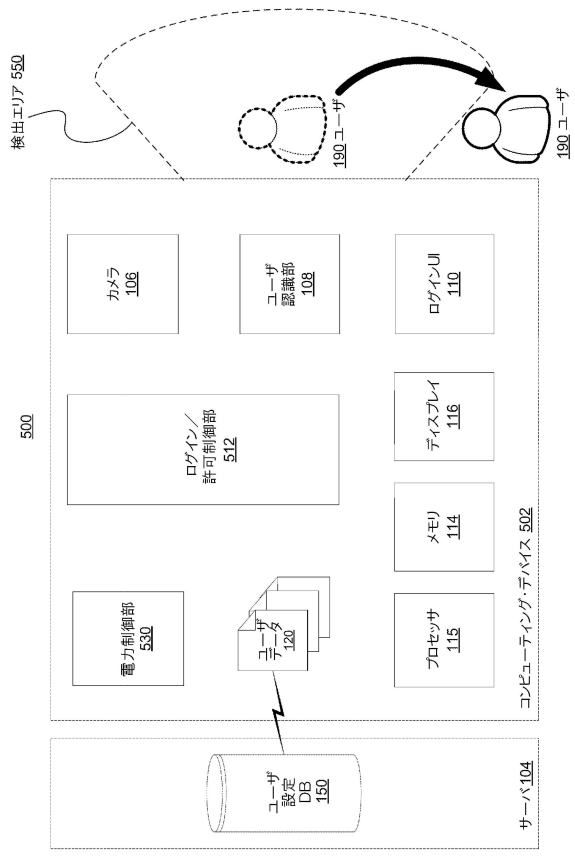
【図３】


390a ユーザ
190 ユーザ
390b ユーザ
300
カメラ 106
ユーザ認識部 108
ログインUI 110
ログイン制御部 112
メモリ 114
プロセッサ 115
ユーザデータ 220c
ユーザデータ 220b
ユーザデータ 220a
コンピューティング・デバイス 302

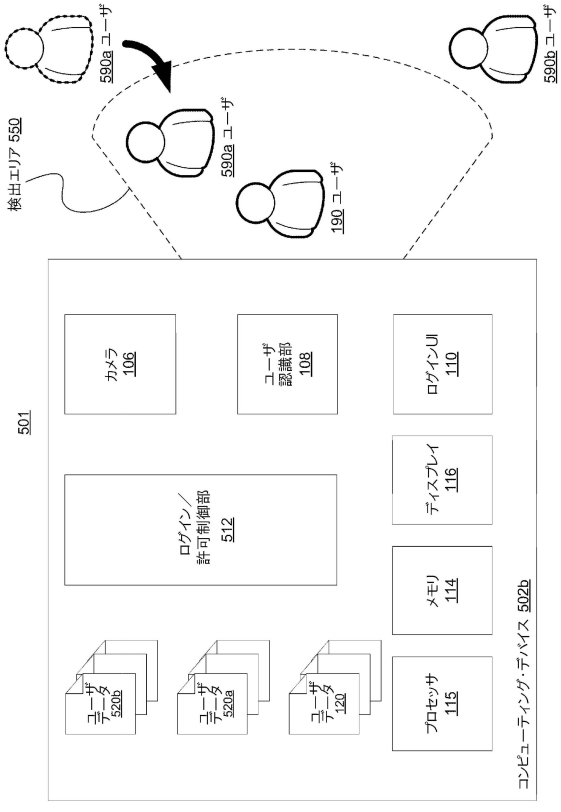
【図４】


190 ユーザ
400
カメラ 106
ユーザ認識部 108
ログインUI 110
ログイン制御部 112
メモリ 114
プロセッサ 115
ユーザデータ 220c
ユーザデータ 220b
ユーザデータ 220a
コンピューティング・デバイス 402
ユーザ識別子（例えば写真など） 406
サーバ（複数可） 404

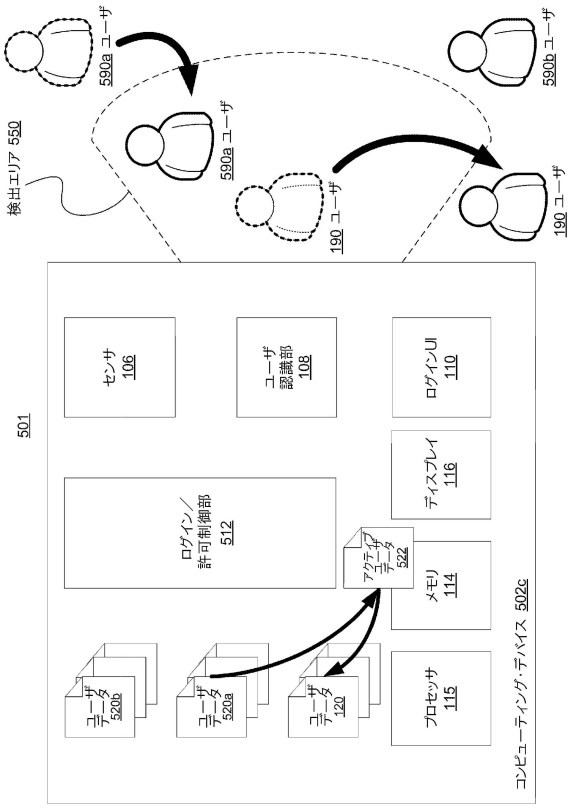
【図５Ａ】


検出エリア 550
190 ユーザ
190 ユーザ
500
カメラ 106
ユーザ認識部 108
ログインUI 110
ログイン／許可制御部 512
ディスプレイ 116
メモリ 114
プロセッサ 115
電力制御部 530
ユーザデータ 120
コンピューティング・デバイス 502
ユーザ設定DB 150
サーバ 104

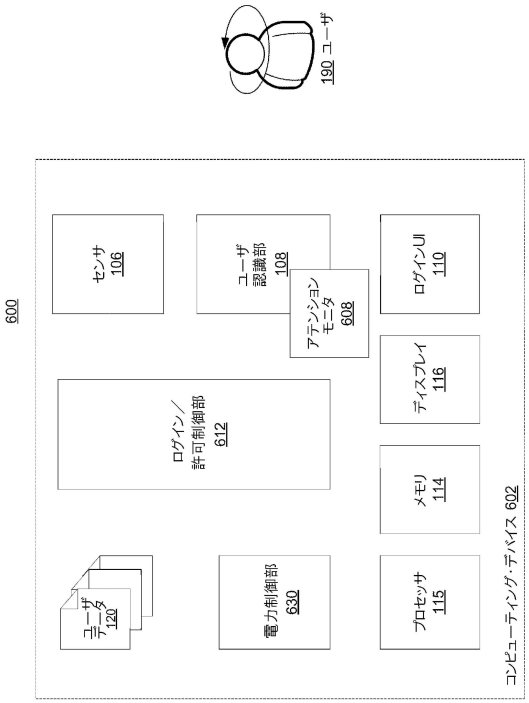
【図５Ｂ】


590a ユーザ
590b ユーザ
検出エリア 550
590a ユーザ
190 ユーザ
501
カメラ 106
ユーザ認識部 108
ログインUI 110
ログイン／許可制御部 512
ディスプレイ 116
メモリ 114
プロセッサ 115
ユーザデータ 520b
ユーザデータ 520a
ユーザデータ 120
コンピューティング・デバイス 502b

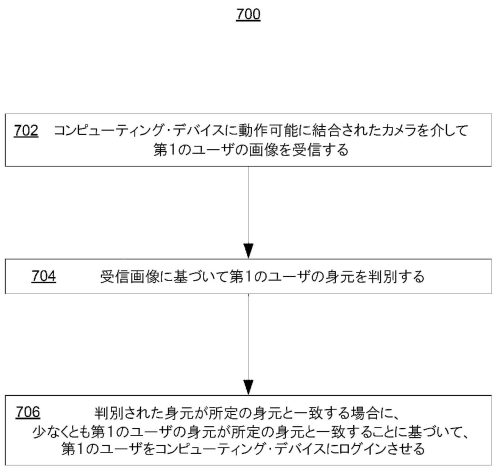
【図５Ｃ】


590a ユーザ
590b ユーザ
検出エリア 550
590a ユーザ
190 ユーザ
190 ユーザ
501
センサ 106
ユーザ認識部 108
ログインUI 110
ディスプレイ 116
ログイン／許可制御部 512
アクティブユーザデータ 522
メモリ 114
ユーザデータ 520b
ユーザデータ 520a
ユーザデータ 120
プロセッサ 115
コンピューティング・デバイス 502c

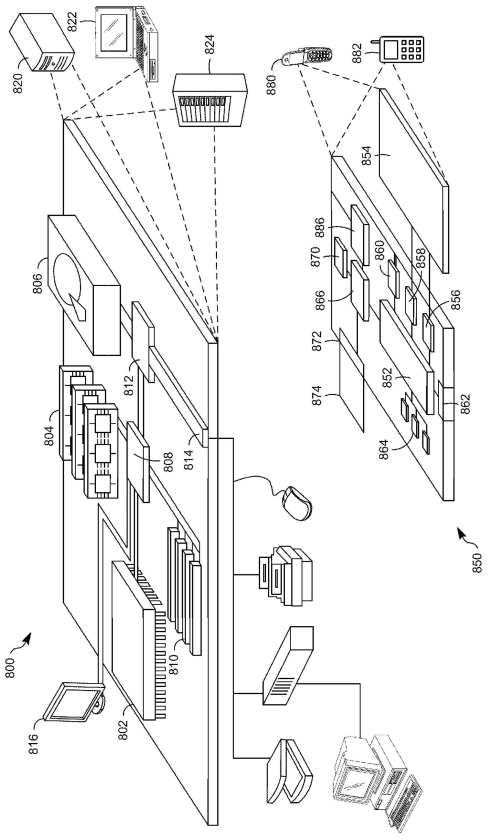
【図６】


190 ユーザ
600
センサ 106
ユーザ認識部 108
アテンションモニタ 608
ログインUI 110
ディスプレイ 116
ログイン／許可制御部 612
メモリ 114
ユーザデータ 120
電力制御部 630
プロセッサ 115
コンピューティング・デバイス 602

【図７】


700
702 コンピューティング・デバイスに動作可能に結合されたカメラを介して第1のユーザの画像を受信する
704 受信画像に基づいて第1のユーザの身元を判別する
706 判別された身元が所定の身元と一致する場合に、少なくとも第1のユーザの身元が所定の身元と一致することに基づいて、第1のユーザをコンピューティング・デバイスにログインさせる

【図８】


820
822
824
880
882
854
886
870
860
858
806
866
856
872
852
862
874
812
804
808
814
864
850
800
810
816
802

フロントページの続き

合議体
審判長　辻本　泰隆
審判官　佐久　聖子
審判官　須田　勝巳

(56)参考文献　特開平１１－２５０４０（ＪＰ，Ａ）
特開２００３－６７３３９（ＪＰ，Ａ）
特開２００７－１３３８４５（ＪＰ，Ａ）
特開２００７－５８３５７（ＪＰ，Ａ）
特開２００７－１１４９３１（ＪＰ，Ａ）
特開２００３－２３３８１６（ＪＰ，Ａ）
特開２００７－４８２１８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 21/32