(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2020-201595
(P2020-201595A)
(43)公開日　令和2年12月17日(2020.12.17)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/32	(2013.01)	G06F	21/32		5B043
G06F 21/31	(2013.01)	G06F	21/31		
G06F 21/62	(2013.01)	G06F	21/62	354	
G06T 7/00	(2017.01)	G06T	7/00	510F	

審査請求 未請求　請求項の数 10　ＯＬ　（全 21 頁）

(21)出願番号　特願2019-106387 (P2019-106387)
(22)出願日　令和1年6月6日 (2019.6.6)

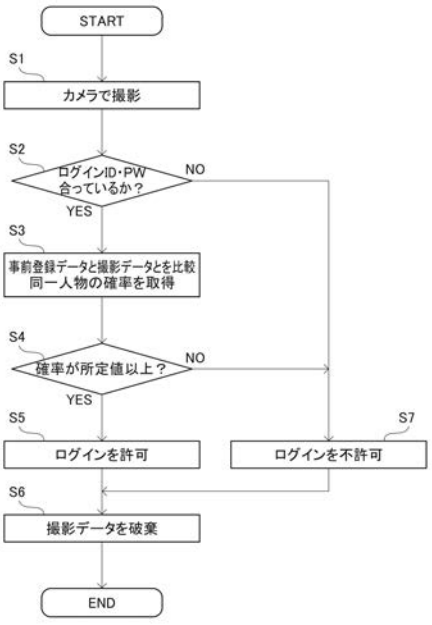
(71)出願人　516346218
株式会社サテライトオフィス
東京都江東区東陽４－１０－４　東陽町Ｓ
Ｈビル５Ｆ
(74)代理人　100168538
弁理士　加藤　来
(72)発明者　原口　豊
東京都江東区東陽４－１０－４　東陽町Ｓ
Ｈビル５Ｆ　株式会社サテライトオフィス
内

Ｆターム(参考)　5B043 AA09　BA04　CA09　DA05　FA02
GA18

最終頁に続く

(54)【発明の名称】ログイン認証システムのプログラム、ログイン認証システム

(57)【要約】　（修正有）
【課題】ＩＤ・パスワード入力のみの構成と比べてセキュリティレベルを高めることができるログイン認証システムのプログラムを提供する。
【解決手段】ログイン認証システムのプログラムは、ユーザー端末のカメラを用いて撮影する撮影ステップＳ１と、ユーザー端末において入力されたユーザーＩＤおよびログインパスワードが登録されたものか否かを判定するＩＤ・パスワード判定ステップＳ２と、撮影した画像データと事前に登録された顔写真データとを画像認証手段によって比較して同一人物の可能性を数値で得る確率値取得ステップＳ３と、同一人物の可能性の数値が所定値以上か否かを判定するユーザー判定ステップＳ４と、Ｓ２の所定要件、かつ、Ｓ４の所定要件の両方を満たすか否かを判定する要件判定ステップおよび、両方を満たしたとき、ログインを許可するログイン許可ステップＳ５とを具備する。
【選択図】図２



【特許請求の範囲】
【請求項１】
ユーザー端末がサーバにアクセスする際に入力データが所定要件を満たした場合にログインを許可するログイン認証システムのプログラムであって、
前記ユーザー端末のカメラを用いてユーザーの顔を撮影する撮影ステップと、
撮影した画像データと事前に登録されたユーザーの顔写真データとを画像認証手段によって比較して同一人物の可能性を数値で得る確率値取得ステップと、
同一人物の可能性の数値が所定値以上か否かを判定することにより撮影されたユーザーが登録ユーザーか否かを判定するユーザー判定ステップと、
前記同一人物の可能性の数値が所定値以上であるとき、ユーザー端末のログインを許可するログイン許可ステップとを具備していることを特徴とするログイン認証システムのプログラム。
【請求項２】
ユーザー端末がサーバにアクセスする際に入力データが所定要件を満たした場合にログインを許可するログイン認証システムのプログラムであって、
前記ユーザー端末のカメラを用いてユーザーの顔を撮影する撮影ステップと、
前記ユーザー端末において入力されたユーザー固有情報およびユーザーログインパスワード情報が事前に登録されたユーザー固有情報およびユーザーログインパスワード情報か否かを判定するＩＤ・パスワード判定ステップと、
撮影した画像データと事前に登録されたユーザーの顔写真データとを画像認証手段によって比較して同一人物の可能性を数値で得る確率値取得ステップと、
同一人物の可能性の数値が所定値以上か否かを判定することにより撮影されたユーザーが登録ユーザーか否かを判定するユーザー判定ステップと、
前記ＩＤ・パスワード判定ステップにおけるユーザー固有情報およびユーザーログインパスワードについての所定要件、かつ、ユーザー判定ステップにおける登録ユーザーの顔認証についての所定要件の両方を満たすか否かを判定する要件判定ステップと、
前記両方を満たしたとき、ユーザー端末のログインを許可するログイン許可ステップとを具備していることを特徴とするログイン認証システムのプログラム。
【請求項３】
前記ログイン許可ステップの後に、撮影ステップにおいて撮影した画像データを破棄する画像データ破棄ステップをさらに具備していることを特徴とする請求項１または請求項２に記載のログイン認証システムのプログラム。
【請求項４】
前記ユーザー判定ステップにおける所定値が、システム管理者によって設定自在な構成であることを特徴とする請求項１乃至請求項３のいずれか１つに記載のログイン認証システムのプログラム。
【請求項５】
ユーザー端末がサーバにアクセスする際に入力データが所定要件を満たした場合にログインを許可するログイン認証システムのプログラムであって、
前記ユーザー端末のカメラを用いてユーザーの２次元コードを読み取る読み取りステップと、
読み取った２次元コードの情報が事前に登録されたユーザー情報か否かを判定する２次元コード判定ステップと、
前記読み取った２次元コードの情報が事前に登録されたユーザー情報であると判定したとき、ユーザー端末のログインを許可するログイン許可ステップとを具備していることを特徴とするログイン認証システムのプログラム。
【請求項６】
ユーザー端末がサーバにアクセスする際に入力データが所定要件を満たした場合にログインを許可するログイン認証システムのプログラムであって、
前記ユーザー端末のカメラを用いてユーザーの２次元コードを読み取る読み取りステッ

プと、
前記ユーザー端末において入力されたユーザー固有情報およびユーザーログインパスワード情報が事前に登録されたユーザー固有情報およびユーザーログインパスワード情報か否かを判定するＩＤ・パスワード判定ステップと、
読み取った２次元コードの情報が事前に登録されたユーザー情報か否かを判定する２次元コード判定ステップと、
前記ＩＤ・パスワード判定ステップにおけるユーザー固有情報およびユーザーログインパスワードについての所定要件、かつ、２次元コード判定ステップにおけるユーザー情報についての所定要件の両方を満たすか否かを判定する要件判定ステップと、
前記両方を満たしたとき、ユーザー端末のログインを許可するログイン許可ステップとを具備していることを特徴とするログイン認証システムのプログラム。
【請求項７】
ユーザー端末がサーバにアクセスする際に入力データが所定要件を満たした場合にログインを許可するログイン認証システムであって、
前記ユーザー端末またはサーバの制御部が、前記ユーザー端末のカメラを用いてユーザーの顔を撮影し、撮影した画像データと事前に登録されたユーザーの顔写真データとを画像認証手段によって比較して同一人物の可能性を数値で得て、同一人物の可能性の数値が所定値以上か否かを判定することにより撮影されたユーザーが登録ユーザーか否かを判定し、同一人物の可能性の数値が所定値以上であるとき、ユーザー端末のログインを許可する構成であることを特徴とするログイン認証システム。
【請求項８】
ユーザー端末がサーバにアクセスする際に入力データが所定要件を満たした場合にログインを許可するログイン認証システムであって、
前記ユーザー端末またはサーバの制御部が、前記ユーザー端末のカメラを用いてユーザーの顔を撮影し、ユーザー端末において入力されたユーザー固有情報およびユーザーログインパスワード情報が事前に登録されたユーザー固有情報およびユーザーログインパスワード情報か否かを判定し、撮影した画像データと事前に登録されたユーザーの顔写真データとを画像認証手段によって比較して同一人物の可能性を数値で得て、同一人物の可能性の数値が所定値以上か否かを判定することにより撮影されたユーザーが登録ユーザーか否かを判定し、ユーザー固有情報およびユーザーログインパスワードについての所定要件、かつ、登録ユーザーの顔認証についての所定要件の両方を満たすか否かを判定し、両方を満たしたとき、ユーザー端末のログインを許可する構成であることを特徴とするログイン認証システム。
【請求項９】
ユーザー端末がサーバにアクセスする際に入力データが所定要件を満たした場合にログインを許可するログイン認証システムであって、
前記ユーザー端末またはサーバの制御部が、前記ユーザー端末のカメラを用いてユーザーの２次元コードを読み取り、読み取った２次元コードの情報が事前に登録されたユーザー情報か否かを判定し、ユーザー情報であると判定したとき、ユーザー端末のログインを許可する構成であることを特徴とするログイン認証システム。
【請求項１０】
ユーザー端末がサーバにアクセスする際に入力データが所定要件を満たした場合にログインを許可するログイン認証システムであって、
前記ユーザー端末またはサーバの制御部が、前記ユーザー端末のカメラを用いてユーザーの２次元コードを読み取り、ユーザー端末において入力されたユーザー固有情報およびユーザーログインパスワード情報が事前に登録されたユーザー固有情報およびユーザーログインパスワード情報か否かを判定し、読み取った２次元コードの情報が事前に登録されたユーザー情報か否かを判定し、ユーザー固有情報およびユーザーログインパスワードについての所定要件、かつ、ユーザー情報についての所定要件の両方を満たすか否かを判定し、両方を満たしたとき、ユーザー端末のログインを許可する構成であることを特徴とす

るログイン認証システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ユーザー端末がサーバにアクセスする際に入力データが所定要件を満たした場合にログインを許可するログイン認証システム、およびログイン認証システムのプログラムに関する。
【背景技術】
【０００２】
従来、引継情報を記憶する引継情報記憶部と、ユーザー端末、関連サーバに接続される制御部とを備え、制御部が、ユーザー端末からログイン要求を受け付けた場合、ユーザー端末から取得した認証情報を用いて第１の認証処理を実行してログインを許可し、ログインしたユーザー端末から関連サーバへの遷移要求を取得した場合、引継情報を生成し、引継情報記憶部に記録し、関連サーバに対して引継情報を提供し、関連サーバから、引継情報を取得した場合、パスワードを生成して引継情報記憶部に記録して、関連サーバに提供し、ユーザー端末から、再ログイン要求を受け付けた場合、引継情報及びパスワードを関連サーバから取得し、引継情報記憶部に記録された引継情報及びパスワードと、取得した引継情報及びパスワードとを用いて第２の認証処理を実行することを特徴とするログイン管理システムが知られている（例えば、特許文献１）。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特許６４９５９９６号公報（特に、請求項１、請求項１１参照）
【発明の概要】
【発明が解決しようとする課題】
【０００４】
しかしながら、上述した従来のログイン管理システムは、第１の認証処理を実行してログインを許可する構成であったため、セキュリティレベルが十分でないという問題があった。
例えば、ログインパスワードが１時間のみ有効な構成であったとしても、ユーザーＩＤおよびログインパスワードが盗まれて１時間以内に使用された場合に対応できないという問題があった。
【０００５】
そこで、本発明は、前述したような従来技術の問題を解決するものであって、すなわち、本発明の目的は、ＩＤ・パスワード入力のみの構成と比べてセキュリティレベルを高めることができるログイン認証システムのプログラム、および、ログイン認証システムを提供することである。
【課題を解決するための手段】
【０００６】
本請求項１に係る発明は、ユーザー端末がサーバにアクセスする際に入力データが所定要件を満たした場合にログインを許可するログイン認証システムのプログラムであって、前記ユーザー端末のカメラを用いてユーザーの顔を撮影する撮影ステップと、撮影した画像データと事前に登録されたユーザーの顔写真データとを画像認証手段によって比較して同一人物の可能性を数値で得る確率値取得ステップと、同一人物の可能性の数値が所定値以上か否かを判定することにより撮影されたユーザーが登録ユーザーか否かを判定するユーザー判定ステップと、前記同一人物の可能性の数値が所定値以上であるとき、ユーザー端末のログインを許可するログイン許可ステップとを具備していることにより、前述した課題を解決するものである。
【０００７】
本請求項２に係る発明は、ユーザー端末がサーバにアクセスする際に入力データが所定

要件を満たした場合にログインを許可するログイン認証システムのプログラムであって、前記ユーザー端末のカメラを用いてユーザーの顔を撮影する撮影ステップと、前記ユーザー端末において入力されたユーザー固有情報およびユーザーログインパスワード情報が事前に登録されたユーザー固有情報およびユーザーログインパスワード情報か否かを判定するＩＤ・パスワード判定ステップと、撮影した画像データと事前に登録されたユーザーの顔写真データとを画像認証手段によって比較して同一人物の可能性を数値で得る確率値取得ステップと、同一人物の可能性の数値が所定値以上か否かを判定することにより撮影されたユーザーが登録ユーザーか否かを判定するユーザー判定ステップと、前記ＩＤ・パスワード判定ステップにおけるユーザー固有情報およびユーザーログインパスワードについての所定要件、かつ、ユーザー判定ステップにおける登録ユーザーの顔認証についての所定要件の両方を満たすか否かを判定する要件判定ステップと、前記両方を満たしたとき、ユーザー端末のログインを許可するログイン許可ステップとを具備していることにより、前述した課題を解決するものである。

【０００８】

本請求項３に係る発明は、請求項１または請求項２に記載されたログイン認証システムのプログラムの構成に加えて、前記ログイン許可ステップの後に、撮影ステップにおいて撮影した画像データを破棄する画像データ破棄ステップをさらに具備していることにより、前述した課題をさらに解決するものである。

【０００９】

本請求項４に係る発明は、請求項１乃至請求項３のいずれか１つに記載されたログイン認証システムのプログラムの構成に加えて、前記ユーザー判定ステップにおける所定値が、システム管理者によって設定自在な構成であることにより、前述した課題をさらに解決するものである。

【００１０】

本請求項５に係る発明は、ユーザー端末がサーバにアクセスする際に入力データが所定要件を満たした場合にログインを許可するログイン認証システムのプログラムであって、前記ユーザー端末のカメラを用いてユーザーの２次元コードを読み取る読み取りステップと、読み取った２次元コードの情報が事前に登録されたユーザー情報か否かを判定する２次元コード判定ステップと、前記読み取った２次元コードの情報が事前に登録されたユーザー情報であると判定したとき、ユーザー端末のログインを許可するログイン許可ステップとを具備していることにより、前述した課題を解決するものである。

【００１１】

本請求項６に係る発明は、ユーザー端末がサーバにアクセスする際に入力データが所定要件を満たした場合にログインを許可するログイン認証システムのプログラムであって、前記ユーザー端末のカメラを用いてユーザーの２次元コードを読み取る読み取りステップと、前記ユーザー端末において入力されたユーザー固有情報およびユーザーログインパスワード情報が事前に登録されたユーザー固有情報およびユーザーログインパスワード情報か否かを判定するＩＤ・パスワード判定ステップと、読み取った２次元コードの情報が事前に登録されたユーザー情報か否かを判定する２次元コード判定ステップと、前記ＩＤ・パスワード判定ステップにおけるユーザー固有情報およびユーザーログインパスワードについての所定要件、かつ、２次元コード判定ステップにおけるユーザー情報についての所定要件の両方を満たすか否かを判定する要件判定ステップと、前記両方を満たしたとき、ユーザー端末のログインを許可するログイン許可ステップとを具備していることにより、前述した課題を解決するものである。

【００１２】

本請求項７に係る発明は、ユーザー端末がサーバにアクセスする際に入力データが所定要件を満たした場合にログインを許可するログイン認証システムであって、前記ユーザー端末またはサーバの制御部が、前記ユーザー端末のカメラを用いてユーザーの顔を撮影し、撮影した画像データと事前に登録されたユーザーの顔写真データとを画像認証手段によって比較して同一人物の可能性を数値で得て、同一人物の可能性の数値が所定値以上か否

かを判定することにより撮影されたユーザーが登録ユーザーか否かを判定し、同一人物の可能性の数値が所定値以上であるとき、ユーザー端末のログインを許可する構成であることにより、前述した課題を解決するものである。

【００１３】

本請求項８に係る発明は、ユーザー端末がサーバにアクセスする際に入力データが所定要件を満たした場合にログインを許可するログイン認証システムであって、前記ユーザー端末またはサーバの制御部が、前記ユーザー端末のカメラを用いてユーザーの顔を撮影し、ユーザー端末において入力されたユーザー固有情報およびユーザーログインパスワード情報が事前に登録されたユーザー固有情報およびユーザーログインパスワード情報か否かを判定し、撮影した画像データと事前に登録されたユーザーの顔写真データとを画像認証手段によって比較して同一人物の可能性を数値で得て、同一人物の可能性の数値が所定値以上か否かを判定することにより撮影されたユーザーが登録ユーザーか否かを判定し、ユーザー固有情報およびユーザーログインパスワードについての所定要件、かつ、登録ユーザーの顔認証についての所定要件の両方を満たすか否かを判定し、両方を満たしたとき、ユーザー端末のログインを許可する構成であることにより、前述した課題を解決するものである。

【００１４】

本請求項９に係る発明は、ユーザー端末がサーバにアクセスする際に入力データが所定要件を満たした場合にログインを許可するログイン認証システムであって、前記ユーザー端末またはサーバの制御部が、前記ユーザー端末のカメラを用いてユーザーの２次元コードを読み取り、読み取った２次元コードの情報が事前に登録されたユーザー情報か否かを判定し、ユーザー情報であると判定したとき、ユーザー端末のログインを許可する構成であることにより、前述した課題を解決するものである。

【００１５】

本請求項１０に係る発明は、ユーザー端末がサーバにアクセスする際に入力データが所定要件を満たした場合にログインを許可するログイン認証システムであって、前記ユーザー端末またはサーバの制御部が、前記ユーザー端末のカメラを用いてユーザーの２次元コードを読み取り、ユーザー端末において入力されたユーザー固有情報およびユーザーログインパスワード情報が事前に登録されたユーザー固有情報およびユーザーログインパスワード情報か否かを判定し、読み取った２次元コードの情報が事前に登録されたユーザー情報か否かを判定し、ユーザー固有情報およびユーザーログインパスワードについての所定要件、かつ、ユーザー情報についての所定要件の両方を満たすか否かを判定し、両方を満たしたとき、ユーザー端末のログインを許可する構成であることにより、前述した課題を解決するものである。

【発明の効果】

【００１６】

本請求項１に係る発明のログイン認証システムのプログラムによれば、顔の画像データの入力が要求されるため、ＩＤ・パスワード入力のみの構成と比べてセキュリティレベルを高めることができる。

【００１７】

本請求項２に係る発明のログイン認証システムのプログラムによれば、ＩＤ・パスワード入力に加えて顔の画像データの入力が要求されて所謂、２要素認証となるため、ＩＤ・パスワード入力のみの構成と比べてセキュリティレベルを高めることができる。

例えば、ログインパスワードが１時間のみ有効な構成であり、ユーザーＩＤおよびログインパスワードが盗まれて１時間以内に使用された場合、ログインしようとする者（盗んだ者）が登録ユーザー本人でないと画像認証によって判定されるため、盗んだ者による不正ログインをブロックすることができる。

【００１８】

本請求項３に係る発明のログイン認証システムのプログラムによれば、請求項１または請求項２に係る発明が奏する効果に加えて、ログイン後はログインに使用した画像データ

が破棄されるため、再利用されて不正ログインされてしまうことを回避することができる。

つまり、１回限りの所謂、ワンタイムで認証コードとして顔の画像データの入力によりセキュリティレベルがより高められ、より強固なセキュリティを実現することができる。

【００１９】

本請求項４に係る発明のログイン認証システムのプログラムによれば、請求項１乃至請求項３のいずれか１つに係る発明が奏する効果に加えて、所定値を比較的高めに設定することにより撮影されたユーザーの顔が登録されたユーザーの顔写真データの顔と同一人物である確率（可能性）が比較的高い場合のみ顔認証されるため、セキュリティレベルを比較的高くすることができる。

【００２０】

本請求項５に係る発明のログイン認証システムのプログラムによれば、ユーザーの２次元コードの入力が要求されるため、ＩＤ・パスワード入力のみの構成と比べてセキュリティレベルを高めることができる。

【００２１】

本請求項６に係る発明のログイン認証システムのプログラムによれば、ＩＤ・パスワード入力に加えてユーザーの２次元コードの入力が要求されて所謂、２要素認証となるため、ＩＤ・パスワード入力のみの構成と比べてセキュリティレベルを高めることができる。

【００２２】

本請求項７に係る発明のログイン認証システムによれば、請求項１に係る発明が奏する効果と同様、顔の画像データの入力が要求されるため、ＩＤ・パスワード入力のみの構成と比べてセキュリティレベルを高めることができる。

【００２３】

本請求項８に係る発明のログイン認証システムによれば、請求項２に係る発明が奏する効果と同様、ＩＤ・パスワード入力に加えて顔の画像データの入力が要求されて所謂、２要素認証となるため、ＩＤ・パスワード入力のみの構成と比べてセキュリティレベルを高めることができる。

【００２４】

本請求項９に係る発明のログイン認証システムによれば、請求項５に係る発明が奏する効果と同様、ユーザーの２次元コードの入力が要求されるため、ＩＤ・パスワード入力のみの構成と比べてセキュリティレベルを高めることができる。

【００２５】

本請求項１０に係る発明のログイン認証システムによれば、請求項６に係る発明が奏する効果と同様、ＩＤ・パスワード入力に加えてユーザーの２次元コードの入力が要求されて所謂、２要素認証となるため、ＩＤ・パスワード入力のみの構成と比べてセキュリティレベルを高めることができる。

【図面の簡単な説明】

【００２６】

【図１】本発明の第１実施例であるログイン認証システムの概略を示す図。

【図２】本発明の第１実施例であるログイン認証システムのプログラムの動作を示すチャート図。

【図３】（Ａ）は第１本発明の実施例であるログイン認証システムのログインの際に撮影した画像データであり、（Ｂ）は事前に登録されたユーザーの顔写真データであり、（Ｃ）は画像認証手段によって算出された同一人物である確率の例を示す図。

【図４】本発明の第２実施例であるログイン認証システムの概略を示す図。

【図５】本発明の第２実施例であるログイン認証システムのプログラムの動作を示すチャート図。

【図６】本発明の第３実施例であるログイン認証システムの概略を示す図。

【図７】本発明の第３実施例であるログイン認証システムのプログラムの動作を示すチャート図。

【図８】本発明の第４実施例であるログイン認証システムの概略を示す図。
【図９】本発明の第４実施例であるログイン認証システムのプログラムの動作を示すチャート図。
【発明を実施するための形態】
【００２７】
本発明のログイン認証システムのプログラムは、ユーザー端末のカメラを用いてユーザーの顔を撮影する撮影ステップと、撮影した画像データと事前に登録されたユーザーの顔写真データとを画像認証手段によって比較して同一人物の可能性を数値で得る確率値取得ステップと、同一人物の可能性の数値が所定値以上か否かを判定することにより撮影されたユーザーが登録ユーザーか否かを判定するユーザー判定ステップと、同一人物の可能性の数値が所定値以上であるとき、ユーザー端末のログインを許可するログイン許可ステップとを具備していることにより、ＩＤ・パスワード入力のみの構成と比べてセキュリティレベルを高めることができるものであれば、その具体的な実施態様は、如何なるものであっても構わない。
また、本発明のログイン認証システムのプログラムは、ユーザー端末のカメラを用いてユーザーの２次元コードを読み取る読み取りステップと、読み取った２次元コードの情報が事前に登録されたユーザー情報か否かを判定する２次元コード判定ステップと、読み取った２次元コードの情報が事前に登録されたユーザー情報であると判定したとき、ユーザー端末のログインを許可するログイン許可ステップとを具備していることにより、ＩＤ・パスワード入力のみの構成と比べてセキュリティレベルを高めることができるものであれば、その具体的な実施態様は、如何なるものであっても構わない。
ログイン認証システムは、ユーザー端末とサーバとを有し、ユーザー端末またはサーバの制御部が、ユーザー端末のカメラを用いてユーザーの顔を撮影し、撮影した画像データと事前に登録されたユーザーの顔写真データとを画像認証手段によって比較して同一人物の可能性を数値で得て、同一人物の可能性の数値が所定値以上か否かを判定することにより撮影されたユーザーが登録ユーザーか否かを判定し、同一人物の可能性の数値が所定値以上であるとき、ユーザー端末のログインを許可する構成であることにより、ＩＤ・パスワード入力のみの構成と比べてセキュリティレベルを高めることができるものであれば、その具体的な実施態様は、如何なるものであっても構わない。
また、ログイン認証システムは、ユーザー端末とサーバとを有し、ユーザー端末またはサーバの制御部が、ユーザー端末のカメラを用いてユーザーの２次元コードを読み取り、読み取った２次元コードの情報が事前に登録されたユーザー情報か否かを判定し、ユーザー情報であると判定したとき、ユーザー端末のログインを許可する構成であることにより、ＩＤ・パスワード入力のみの構成と比べてセキュリティレベルを高めることができるものであれば、その具体的な実施態様は、如何なるものであっても構わない。
本発明は、ユーザーの顔認証またはユーザーの２次元コード認証の所謂、１認証に限らず、顔認証またはユーザーの２次元コード認証とＩＤ・パスワード認証とを併用する所謂、２認証の構成でもよい。
【００２８】
例えば、ユーザー端末は、デスクトップ型パーソナルコンピュータ端末、ノート型パーソナルコンピュータ端末、スマートフォン端末、およびタブレット端末など、カメラと表示部と操作部とを有して情報を送受信するものであって、所謂インターネットである広域ネットワーク、ローカルネットワーク、電話回線などを含む通信ネットワークによりサーバと接続自在なものであれば如何なるものであっても構わない。
また、サーバは、１つのサーバやクラウド上の複数のサーバでもよい。
また、ログイン認証システムのプログラムの概念には、ログイン認証システムのアプリケーションソフトウェア自体だけでなく、ログイン認証システム（アプリケーションソフトウェア）の機能を拡張するログイン認証システム（アプリケーションソフトウェア）の追加用アドオンプログラム（以下、追加用アドオンプログラム）が含まれるものとする。
【実施例１】

【００２９】
以下に、本発明の第１実施例であるログイン認証システム１００のプログラムについて、図１乃至図３（Ｃ）に基づいて説明する。
ここで、図１は、本発明の第１実施例であるログイン認証システム１００の概略を示す図であり、図２は、本発明の第１実施例であるログイン認証システム１００のプログラムの動作を示すチャート図であり、図３（Ａ）は、本発明の第１実施例であるログイン認証システム１００のログインの際にカメラ１１４が撮影した画像データＰＴ１であり、図３（Ｂ）は、事前に登録されたユーザーの顔写真データＰＴ２であり、図３（Ｃ）は、画像認証手段によって算出された同一人物である確率の例を示す図である。
【００３０】
本発明の第１実施例であるログイン認証システム１００は、図１に示すように、ユーザー端末の一例であるコンピュータ端末１１０と、サーバ１２０とを備えている。
そして、ユーザーのコンピュータ端末１１０がサーバ１２０にアクセスする際に、入力データが所定要件を満たすか否かを判定し、満たした場合にログインを許可するように構成されている。
コンピュータ端末１１０は、表示部１１１と、操作部１１３と、カメラ１１４とを備えている。
このうち、表示部１１１は、ブラウザを表示し、ユーザーがログインする際にブラウザにログイン画面１１２を表示する。
ログイン画面１１２には、一例として、ユーザーＩＤ入力欄１１２ａ、パスワード入力欄１１２ｂ、カメラ撮影映像欄１１２ｃ、撮影ボタン１１２ｄ、ログインボタン１１２ｅが表示されるように構成されている。
【００３１】
ユーザーは、操作部１１３のキーボードを操作してユーザーＩＤ入力欄１１２ａにユーザーＩＤであるユーザー固有情報の一例として事前に登録された電子メールアドレスを入力する。
また、同様に、パスワード入力欄１１２ｂに事前に登録されたユーザーログインパスワード情報を入力する。
ここで、ログイン画面１１２が表示された際、カメラ１１４が起動してコンピュータ端末１１０の前に座っているユーザーをカメラ撮影映像欄１１２ｃに映し出すように構成されている。
ユーザーが、マウスのクリック操作などによって撮影ボタン１１２ｄを操作するとカメラ１１４が静止画像としてユーザーを撮影し、撮影された画像データＰＴ１がカメラ撮影映像欄１１２ｃに映し出される。
そして、ユーザーがカメラ撮影映像欄１１２ｃを確認し、その画像データＰＴ１でよいと判断したらマウスのクリック操作などによってログインボタン１１２ｅを操作する。
【００３２】
ここで、本実施例では、ユーザーのコンピュータ端末１１０またはサーバ１２０の制御部が、ユーザーのコンピュータ端末１１０のカメラ１１４を用いてユーザーの顔を撮影する。
さらに、ユーザーのコンピュータ端末１１０において入力されたユーザー固有情報およびユーザーログインパスワード情報が事前に登録されたユーザー固有情報およびユーザーログインパスワード情報か否かを判定する。
また、撮影した画像データＰＴ１と事前に登録されたユーザーの顔写真データＰＴ２とを例えば、クラウドサーバ上の画像認証手段によって比較して同一人物の可能性を数値で得て、同一人物の可能性の数値が所定値以上か否かを判定することにより撮影されたユーザーが登録ユーザーか否かを判定する。
【００３３】
そして、ユーザー固有情報およびユーザーログインパスワードについての所定要件、かつ、登録ユーザーの顔認証についての所定要件の両方を満たすか否かを判定し、両方を満

たしたとき、ユーザーのコンピュータ端末１１０のログインを許可するように構成されている。
これにより、ＩＤ・パスワード入力に加えて顔の画像データＰＴ１の入力が要求されて所謂、２要素認証となる。
その結果、ＩＤ・パスワード入力のみの構成と比べてセキュリティレベルを高めることができる。
【００３４】
続いて、ログイン認証システム１００のプログラムの動作について、より詳しく説明する。
図２に示すように、ステップＳ１では、撮影ステップとして、ユーザーのコンピュータ端末１１０のカメラ１１４を用いてユーザーの顔を撮影する。
例えば、図３（Ａ）に示すように、撮影した画像データＰＴ１にユーザーの顔が写っている。
なお、ユーザーが撮影ボタン１１２ｄを操作したことをトリガーとして撮影する旨を説明したが、ユーザーの操作なしで所定時間の一例として２秒毎に静止画像として撮影する構成としてもよいし、動画で撮影する構成でもよい。
【００３５】
ステップＳ２では、ＩＤ・パスワード判定ステップとして、ユーザーのコンピュータ端末１１０において入力されたユーザー固有情報およびユーザーログインパスワード情報が事前に登録されたユーザー固有情報およびユーザーログインパスワード情報か否かを、コンピュータ端末１１０またはサーバ１２０の制御部（ログイン認証システム１００のプログラム）が判定する。
登録されたものであると判定した場合はステップＳ３へ進み、他方、否と判定した場合はステップＳ７へ進む。
【００３６】
例えば、ログインしようとするユーザーが鈴木さんであり、ユーザーである鈴木さんが、事前に登録された鈴木さんのＩＤ（ユーザー固有情報）とパスワード（ユーザーログインパスワード情報）を入力したとする。
そして、ログインボタン１１２ｅが操作されたとき、入力されたＩＤ（ユーザー固有情報）およびパスワード（ユーザーログインパスワード情報）が、事前に登録されたユーザー固有情報およびユーザーログインパスワードとそれぞれ一致するか否かを、コンピュータ端末１１０またはサーバ１２０の制御部（ログイン認証システム１００のプログラム）が判定する。
【００３７】
ステップＳ３では、確率値取得ステップとして、撮影した画像データＰＴ１と事前に登録されたユーザーの顔写真データＰＴ２とを画像認証手段によって比較して同一人物の可能性を数値で得る。
画像認証手段は、例えば、クラウドサーバ（サーバ１２０）に設けられ、ユーザーのコンピュータ端末１１０からアップロードされた撮影された画像データＰＴ１（図３（Ａ）参照）と、事前に登録されたユーザーの顔写真データＰＴ２（図３（Ｂ）参照）とを比べ、同一人物の可能性を数値で算出するように構成されている。
例えば、図３（Ｂ）に示すように、ユーザー：鈴木さんの顔が写っている顔写真データＰＴ２が、ログイン認証システム１００に事前に登録されているものとする。
【００３８】
画像認証手段は、一例として、各データに写っている顔の眼の位置、鼻の位置、口の位置、眉毛の位置を特定する。
次に、眼（まぶたを含む）の形状、鼻の形状、口の形状、眉毛の形状、顔の輪郭などを特定する。
これらの要素がどれだけ共通しているか否かを判定し、アップロードされた撮影された画像データＰＴ１（図３（Ａ）参照）が、事前に登録されたユーザーの顔写真データＰＴ

２（図３（Ｂ）参照）の鈴木さんと同一人物の可能性を算出する。
例えば、図３（Ｃ）に示すように、「撮影された人が、登録されたユーザー：鈴木さんである確率９１％」と算出する。
そして、この確率の値「９１」を、コンピュータ端末１１０またはサーバ１２０の制御部（ログイン認証システム１００のプログラム）が取得する。
【００３９】
ステップＳ４では、ユーザー判定ステップとして、同一人物の可能性の数値が所定値以上か否かを判定することにより撮影されたユーザーが登録ユーザーか否かを、コンピュータ端末１１０またはサーバ１２０の制御部（ログイン認証システム１００のプログラム）が判定する。
所定値以上であると判定した場合はステップＳ５へ進み、他方、否であると判定した場合はステップＳ７へ進む。
例えば、取得した確率の値が「９１」であり、事前に登録された所定値が「９０」であるとする。
この場合、取得した確率の値「９１」と、事前に登録された所定値「９０」とを比べ、取得した確率の値「９１」が事前に登録された所定値「９０」以上であると判定し、撮影されたユーザーが登録ユーザー：鈴木さん本人であると判定する。
【００４０】
ステップＳ５では、要件判定ステップとして、ＩＤ・パスワード判定ステップＳ２におけるユーザー固有情報およびユーザーログインパスワードについての所定要件、かつ、ユーザー判定ステップＳ４における登録ユーザーの顔認証についての所定要件の両方を満たすか否かを、コンピュータ端末１１０またはサーバ１２０の制御部（ログイン認証システム１００のプログラム）が判定する。
そして、両方を満たしたとき、ログイン許可ステップとして、ユーザーのコンピュータ端末１１０のログインを許可する。
これにより、前述したように、ＩＤ・パスワード入力に加えて顔の画像データＰＴ１の入力が要求されて所謂、２要素認証となる。
その結果、ＩＤ・パスワード入力のみの構成と比べてセキュリティレベルを高めることができる。
【００４１】
ステップＳ６では、画像データ破棄ステップとして、撮影ステップＳ１において撮影した画像データＰＴ１を、コンピュータ端末１１０またはサーバ１２０の制御部（ログイン認証システム１００のプログラム）が破棄する。
これにより、ログイン後はログインに使用した画像データＰＴ１が破棄される。
その結果、再利用されて不正ログインされてしまうことを回避することができる。
つまり、１回限りの所謂、ワンタイムで認証コードとして顔の画像データＰＴ１の入力によりセキュリティレベルがより高められ、より強固なセキュリティを実現することができる。
ステップＳ７では、ユーザーのコンピュータ端末１１０のログインを、コンピュータ端末１１０またはサーバ１２０の制御部（ログイン認証システム１００のプログラム）が拒否する。
そして、ステップＳ６へ進み、画像データＰＴ１を破棄する。
【００４２】
なお、ユーザー判定ステップＳ４における所定値が、システム管理者によって設定自在に構成されている。
例えば、図示しない管理者用画面において、ユーザー判定ステップＳ４における所定値が変更自在に設けられている。
これにより、例えば、所定値を比較的高めに設定することによって撮影されたユーザーの顔が登録されたユーザーの顔写真データＰＴ２の顔と同一人物である確率（可能性）が比較的高い場合のみ顔認証される。

その結果、セキュリティレベルを適度に比較的高くすることができる。
例えば、一卵性双生児の双子の一方が他方になりすましてログインしようとしても、そもそも双子の他方のパスワードを知らないことに加え、同一人物である可能性の確率が所定値未満となり、ログインしようとしているユーザーは登録されたユーザーと同一人物ではないと判定される。
他方、所定値を比較的低めに設定することによって、事前に登録されたユーザーの顔写真データＰＴ２に写っている顔と比べて、化粧メイクが濃い場合、化粧メイクを変えた場合やコンタクトレンズを変えた場合であっても、同一人物である可能性の確率が所定値以上となり、ログインしようとしているユーザーは登録されたユーザーであると判定される。

【００４３】
なお、本実施例では、発明を理解しやすいように、先にＩＤ・パスワードによる認証であるＩＤ・パスワード判定ステップＳ２を行い、後に顔認証であるユーザー判定ステップＳ４を行う構成について説明したが、この順番に限らない。
ＩＤ・パスワード判定ステップＳ２とユーザー判定ステップＳ４との順番が逆の構成でもよいし、ＩＤ・パスワード判定ステップＳ２とユーザー判定ステップＳ４とを同時に行う構成でもよい。

【００４４】
このようにして得られた本発明の第１実施例であるログイン認証システム１００のプログラムは、ユーザー端末の一例であるコンピュータ端末１１０のカメラ１１４を用いてユーザーの顔を撮影する撮影ステップＳ１と、ユーザーのコンピュータ端末１１０において入力されたユーザー固有情報およびユーザーログインパスワード情報が事前に登録されたユーザー固有情報およびユーザーログインパスワード情報か否かを判定するＩＤ・パスワード判定ステップＳ２と、撮影した画像データＰＴ１と事前に登録されたユーザーの顔写真データＰＴ２とを画像認証手段によって比較して同一人物の可能性を数値で得る確率値取得ステップＳ３と、同一人物の可能性の数値が所定値以上か否かを判定することにより撮影されたユーザーが登録ユーザーか否かを判定するユーザー判定ステップＳ４と、ＩＤ・パスワード判定ステップＳ２におけるユーザー固有情報およびユーザーログインパスワードについての所定要件、かつ、ユーザー判定ステップＳ４における登録ユーザーの顔認証についての所定要件の両方を満たすか否かを判定する要件判定ステップＳ５と、両方を満たしたとき、ユーザーのコンピュータ端末１１０のログインを許可するログイン許可ステップＳ５とを具備していることにより、ＩＤ・パスワード入力のみの構成と比べてセキュリティレベルを高めることができる。

【００４５】
さらに、ログイン許可ステップＳ５の後に、撮影ステップＳ１において撮影した画像データＰＴ１を破棄する画像データ破棄ステップＳ６をさらに具備していることにより、１回限りの所謂、ワンタイムで認証コードとして顔の画像データＰＴ１の入力によりセキュリティレベルがより高められ、より強固なセキュリティを実現することができる。

【００４６】
また、ユーザー判定ステップＳ４における所定値が、システム管理者によって設定自在な構成であることにより、セキュリティレベルを適度に調整することができる。

【００４７】
また、本発明の第１実施例であるログイン認証システム１００は、ユーザーのコンピュータ端末１１０とサーバ１２０とを備え、ユーザーのコンピュータ端末１１０またはサーバ１２０の制御部が、ユーザーのコンピュータ端末１１０のカメラ１１４を用いてユーザーの顔を撮影し、ユーザーのコンピュータ端末１１０において入力されたユーザー固有情報およびユーザーログインパスワード情報が事前に登録されたユーザー固有情報およびユーザーログインパスワード情報か否かを判定し、撮影した画像データＰＴ１と事前に登録されたユーザーの顔写真データＰＴ２とを画像認証手段によって比較して同一人物の可能性を数値で得て、同一人物の可能性の数値が所定値以上か否かを判定することにより撮影

されたユーザーが登録ユーザーか否かを判定し、ユーザー固有情報およびユーザーログインパスワードについての所定要件、かつ、登録ユーザーの顔認証についての所定要件の両方を満たすか否かを判定し、両方を満たしたとき、ユーザーのコンピュータ端末１１０のログインを許可する構成であることにより、ＩＤ・パスワード入力のみの構成と比べてセキュリティレベルを高めることができるなど、その効果は甚大である。

【実施例２】

【００４８】

続いて、本発明の第２実施例であるログイン認証システム１００について、図４および図５に基づいて説明する。

ここで、図４は、本発明の第２実施例であるログイン認証システム１００の概略を示す図であり、図５は、本発明の第２実施例であるログイン認証システム１００のプログラムの動作を示すチャート図である。

第２実施例のログイン認証システム１００は、第１実施例のログイン認証システム１００におけるＩＤ・パスワード認証および顔認証の２要素認証を顔認証のみの１認証に変更したものであり、多くの要素について第１実施例のログイン認証システム１００と共通するので、共通する事項については詳しい説明を省略する。

【００４９】

図４に示すように、本発明の第２実施例であるログイン認証システム１００は、ユーザー端末の一例であるコンピュータ端末１１０と、サーバ１２０とを備えている。

そして、ユーザーのコンピュータ端末１１０またはサーバ１２０の制御部が、ユーザーのコンピュータ端末１１０のカメラ１１４を用いてユーザーの顔を撮影する。

さらに、撮影した画像データＰＴ１と事前に登録されたユーザーの顔写真データＰＴ２とを画像認証手段によって比較して同一人物の可能性を数値で得て、同一人物の可能性の数値が所定値以上か否かを判定することにより撮影されたユーザーが登録ユーザーか否かを判定する。

そして、同一人物の可能性の数値が所定値以上であるとき、ユーザーのコンピュータ端末１１０のログインを許可するように構成されている。

これにより、顔の画像データＰＴ１の入力が要求される。

その結果、ＩＤ・パスワード入力のみの構成と比べてセキュリティレベルを高めることができる。

【００５０】

続いて、ログイン認証システム１００のプログラムの動作について、より詳しく説明する。

図５に示すように、ステップＳ１１では、撮影ステップとして、前述したステップＳ１と同様、ユーザーのコンピュータ端末１１０のカメラ１１４を用いてユーザーの顔を撮影する。

ステップ１２では、確率値取得ステップとして、前述したステップＳ３と同様、撮影した画像データＰＴ１と事前に登録されたユーザーの顔写真データＰＴ２とを画像認証手段によって比較して同一人物の可能性を数値で得る。

【００５１】

ステップＳ１３では、ユーザー判定ステップとして、前述したＳ４と同様、同一人物の可能性の数値が所定値以上か否かを判定することにより撮影されたユーザーが登録ユーザーか否かを、コンピュータ端末１１０またはサーバ１２０の制御部（ログイン認証システム１００のプログラム）が判定する。

所定値以上であると判定した場合はステップＳ１４へ進み、他方、否であると判定した場合はステップＳ１６へ進む。

ステップＳ１４では、ログイン許可ステップとして、ユーザーのコンピュータ端末１１０のログインを許可する。

【００５２】

ステップＳ１５では、画像データ破棄ステップとして、前述したステップＳ６と同様、

撮影ステップＳ１１において撮影した画像データＰＴ１を、コンピュータ端末１１０またはサーバ１２０の制御部（ログイン認証システム１００のプログラム）が破棄する。
ステップＳ１６では、ユーザーのコンピュータ端末１１０のログインを、コンピュータ端末１１０またはサーバ１２０の制御部（ログイン認証システム１００のプログラム）が拒否する。
そして、ステップＳ１５へ進み、画像データＰＴ１を破棄する。
【００５３】
このようにして得られた本発明の第２実施例であるログイン認証システム１００のプログラムは、ユーザーのコンピュータ端末１１０のカメラ１１４を用いてユーザーの顔を撮影する撮影ステップＳ１１と、撮影した画像データＰＴ１と事前に登録されたユーザーの顔写真データＰＴ２とを画像認証手段によって比較して同一人物の可能性を数値で得る確率値取得ステップＳ１２と、同一人物の可能性の数値が所定値以上か否かを判定することにより撮影されたユーザーが登録ユーザーか否かを判定するユーザー判定ステップＳ１３と、同一人物の可能性の数値が所定値以上であるとき、ユーザーのコンピュータ端末１１０のログインを許可するログイン許可ステップＳ１４とを具備していることにより、ＩＤ・パスワード入力のみの構成と比べてセキュリティレベルを高めることができる。
【００５４】
また、本発明の第２実施例であるログイン認証システム１００は、ユーザーのコンピュータ端末１１０とサーバ１２０とを備え、ユーザーのコンピュータ端末１１０またはサーバ１２０の制御部が、ユーザーのコンピュータ端末１１０のカメラ１１４を用いてユーザーの顔を撮影し、撮影した画像データＰＴ１と事前に登録されたユーザーの顔写真データＰＴ２とを画像認証手段によって比較して同一人物の可能性を数値で得て、同一人物の可能性の数値が所定値以上か否かを判定することにより撮影されたユーザーが登録ユーザーか否かを判定し、同一人物の可能性の数値が所定値以上であるとき、ユーザーのコンピュータ端末１１０のログインを許可する構成であることにより、ＩＤ・パスワード入力のみの構成と比べてセキュリティレベルを高めることができるなど、その効果は甚大である。
【実施例３】
【００５５】
続いて、本発明の第３実施例であるログイン認証システム１００について、図６および図７に基づいて説明する。
ここで、図６は、本発明の第３実施例であるログイン認証システム１００の概略を示す図であり、図７は、本発明の第３実施例であるログイン認証システム１００のプログラムの動作を示すチャート図である。
第３実施例のログイン認証システム１００は、第２実施例のログイン認証システム１００における顔認証を２次元コード認証に変更したものであり、多くの要素について第１実施例のログイン認証システム１００および第２実施例のログイン認証システム１００と共通するので、共通する事項については詳しい説明を省略する。
【００５６】
図６に示すように、本発明の第３実施例であるログイン認証システム１００は、ユーザー端末の一例であるコンピュータ端末１１０と、サーバ１２０とを備えている。
そして、ユーザーのコンピュータ端末１１０またはサーバ１２０の制御部が、ユーザーのコンピュータ端末１１０のカメラ１１４を用いてユーザーの２次元コードＣＤを読み取る。
ここで、ユーザーのコンピュータ端末１１０またはサーバ１２０の制御部は、２次元コードＣＤを読み取るプログラムを有している。
ユーザーの２次元コードＣＤは、例えば、ユーザーのスマートフォン端末に表示させたものでもよいし、ユーザーが首から提げたネームホルダーに記載されたものでもよい。
さらに、読み取った２次元コードＣＤの情報が事前に登録されたユーザー情報か否かを判定する。
【００５７】

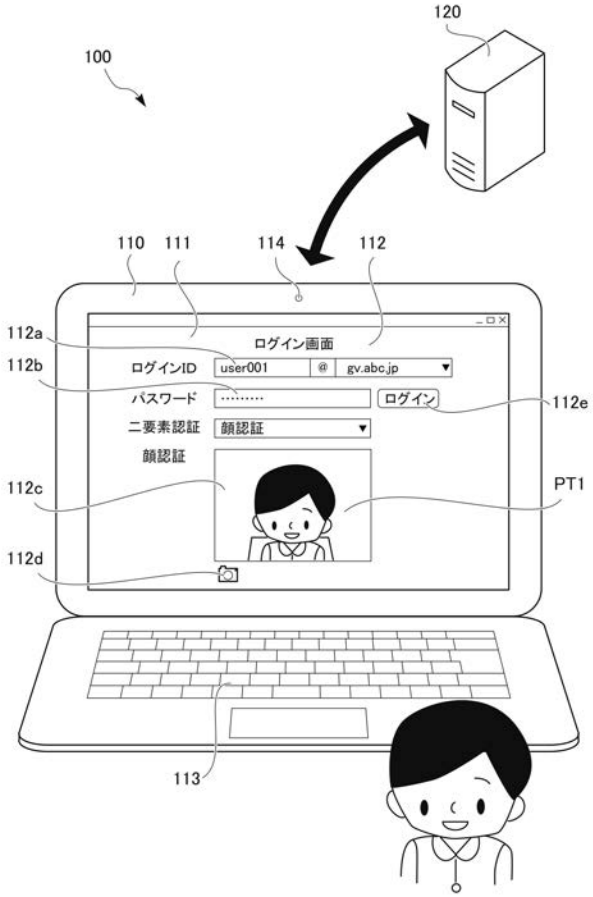
そして、ユーザー情報であると判定したとき、ユーザーのコンピュータ端末１１０のログインを許可するように構成されている。
これにより、ユーザーの２次元コードＣＤの入力が要求される。
その結果、ＩＤ・パスワード入力のみの構成と比べてセキュリティレベルを高めることができる。
【００５８】
続いて、ログイン認証システム１００のプログラムの動作について、より詳しく説明する。
図７に示すように、ステップＳ２１では、読み取りステップとして、ユーザーのコンピュータ端末１１０のカメラ１１４を用いてユーザーの２次元コードＣＤを読み取る。
ステップＳ２２では、２次元コード判定ステップとして、読み取った２次元コードＣＤの情報が事前に登録されたユーザー情報か否かを、コンピュータ端末１１０またはサーバ１２０の制御部（ログイン認証システム１００のプログラム）が判定する。
ユーザー情報であると判定した場合はステップＳ２３へ進み、他方、否であると判定した場合はステップＳ２４へ進む。
ステップＳ２３では、ログイン許可ステップとして、ユーザーのコンピュータ端末１１０のログインを許可する。
ステップＳ２４では、ユーザーのコンピュータ端末１１０のログインを、コンピュータ端末１１０またはサーバ１２０の制御部（ログイン認証システム１００のプログラム）が拒否する。
【００５９】
このようにして得られた本発明の第３実施例であるログイン認証システム１００のプログラムは、ユーザーのコンピュータ端末１１０のカメラ１１４を用いてユーザーの２次元コードＣＤを読み取る読み取りステップＳ２１と、読み取った２次元コードＣＤの情報が事前に登録されたユーザー情報か否かを判定する２次元コード判定ステップＳ２２と、読み取った２次元コードＣＤの情報が事前に登録されたユーザー情報であると判定したとき、ユーザーのコンピュータ端末１１０のログインを許可するログイン許可ステップＳ２３とを具備していることにより、ＩＤ・パスワード入力のみの構成と比べてセキュリティレベルを高めることができる。
【００６０】
また、本発明の第３実施例であるログイン認証システム１００は、ユーザーのコンピュータ端末１１０とサーバ１２０とを備え、ユーザーのコンピュータ端末１１０またはサーバ１２０の制御部が、ユーザーのコンピュータ端末１１０のカメラ１１４を用いてユーザーの２次元コードＣＤを読み取り、読み取った２次元コードＣＤの情報が事前に登録されたユーザー情報か否かを判定し、ユーザー情報であると判定したとき、ユーザーのコンピュータ端末１１０のログインを許可する構成であることにより、ＩＤ・パスワード入力のみの構成と比べてセキュリティレベルを高めることができるなど、その効果は甚大である。
【実施例４】
【００６１】
続いて、本発明の第４実施例であるログイン認証システム１００について、図８および図９に基づいて説明する。
ここで、図８は、本発明の第４実施例であるログイン認証システム１００の概略を示す図であり、図９は、本発明の第４実施例であるログイン認証システム１００のプログラムの動作を示すチャート図である。
第４実施例のログイン認証システム１００は、第１実施例のログイン認証システム１００における顔認証を２次元コード認証に変更したものであり、多くの要素について第１実施例のログイン認証システム１００乃至第３実施例のログイン認証システム１００と共通するので、共通する事項については詳しい説明を省略する。
【００６２】

図８に示すように、本発明の第３実施例であるログイン認証システム１００は、ユーザー端末の一例であるコンピュータ端末１１０と、サーバ１２０とを備えている。
そして、ユーザーのコンピュータ端末１１０またはサーバ１２０の制御部が、ユーザーのコンピュータ端末１１０のカメラ１１４を用いてユーザーの２次元コードＣＤを読み取る。
また、ユーザーのコンピュータ端末１１０において入力されたユーザー固有情報およびユーザーログインパスワード情報が事前に登録されたユーザー固有情報およびユーザーログインパスワード情報か否かを判定する。
【００６３】
さらに、読み取った２次元コードＣＤの情報が事前に登録されたユーザー情報か否かを判定する。
そして、ユーザー固有情報およびユーザーログインパスワードについての所定要件、かつ、ユーザー情報についての所定要件の両方を満たすか否かを判定し、両方を満たしたとき、ユーザーのコンピュータ端末１１０のログインを許可するように構成されている。
これにより、ＩＤ・パスワード入力に加えてユーザーの２次元コードＣＤの入力が要求されて所謂、２要素認証となる。
その結果、ＩＤ・パスワード入力のみの構成と比べてセキュリティレベルを高めることができる。
【００６４】
続いて、ログイン認証システム１００のプログラムの動作について、より詳しく説明する。
図９に示すように、ステップＳ３１では、読み取りステップとして、前述したステップＳ２１と同様、ユーザーのコンピュータ端末１１０のカメラ１１４を用いてユーザーの２次元コードＣＤを読み取る。
【００６５】
ステップＳ３２では、ＩＤ・パスワード判定ステップとして、前述したステップＳ２と同様、ユーザーのコンピュータ端末１１０において入力されたユーザー固有情報およびユーザーログインパスワード情報が事前に登録されたユーザー固有情報およびユーザーログインパスワード情報か否かを、コンピュータ端末１１０またはサーバ１２０の制御部（ログイン認証システム１００のプログラム）が判定する。
登録されたものであると判定した場合はステップＳ３３へ進み、他方、否と判定した場合はステップＳ３５へ進む。
【００６６】
ステップＳ３３では、２次元コード判定ステップとして、前述したステップＳ２２と同様、読み取った２次元コードＣＤの情報が事前に登録されたユーザー情報か否かを、コンピュータ端末１１０またはサーバ１２０の制御部（ログイン認証システム１００のプログラム）が判定する。
ユーザー情報であると判定した場合はステップＳ３４へ進み、他方、否であると判定した場合はステップＳ３５へ進む。
【００６７】
ステップＳ３４では、要件判定ステップとして、前述したステップＳ５と同様、ＩＤ・パスワード判定ステップＳ３２におけるユーザー固有情報およびユーザーログインパスワードについての所定要件、かつ、２次元コード判定ステップＳ３３におけるユーザー情報についての所定要件の両方を満たすか否かを、コンピュータ端末１１０またはサーバ１２０の制御部（ログイン認証システム１００のプログラム）が判定する。
そして、両方を満たしたとき、ログイン許可ステップとして、ユーザーのコンピュータ端末１１０のログインを許可する。
これにより、前述したように、ＩＤ・パスワード入力に加えてユーザーの２次元コードＣＤの入力が要求されて所謂、２要素認証となる。
その結果、ＩＤ・パスワード入力のみの構成と比べてセキュリティレベルを高めること

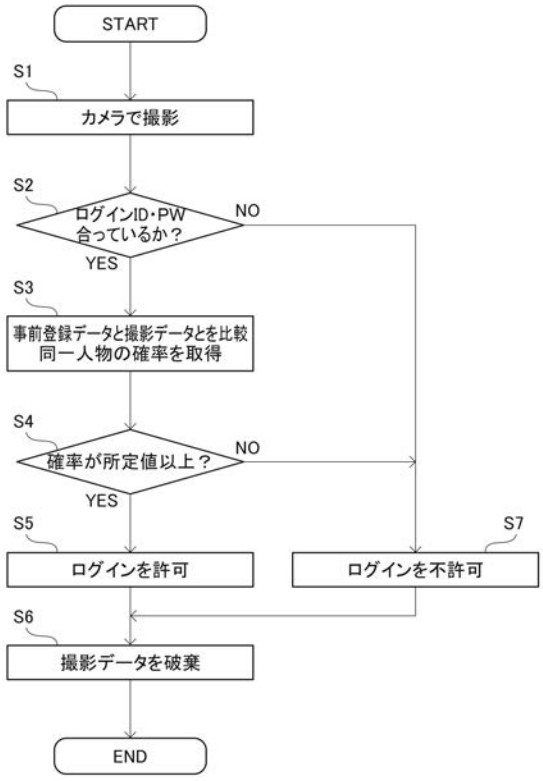
ができる。
ステップＳ３５では、ユーザーのコンピュータ端末１１０のログインを、コンピュータ端末１１０またはサーバ１２０の制御部（ログイン認証システム１００のプログラム）が拒否する。
【００６８】
なお、本実施例では、発明を理解しやすいように、先にＩＤ・パスワードによる認証であるＩＤ・パスワード判定ステップＳ３２を行い、後に２次元コード認証である２次元コード判定ステップＳ３３を行う構成について説明したが、この順番に限らない。
ＩＤ・パスワード判定ステップＳ３２と２次元コード判定ステップＳ３３との順番が逆の構成でもよいし、ＩＤ・パスワード判定ステップＳ３２と２次元コード判定ステップＳ３３とを同時に行う構成でもよい。
また、読み取りステップＳ３１の順番は、２次元コード判定ステップＳ３３より前であればよく、ＩＤ・パスワード判定ステップＳ３２より後でもよい。
【００６９】
このようにして得られた本発明の第４実施例であるログイン認証システム１００のプログラムは、ユーザーのコンピュータ端末１１０のカメラ１１４を用いてユーザーの２次元コードＣＤを読み取る読み取りステップＳ３１と、ユーザーのコンピュータ端末１１０において入力されたユーザー固有情報およびユーザーログインパスワード情報が事前に登録されたユーザー固有情報およびユーザーログインパスワード情報か否かを判定するＩＤ・パスワード判定ステップＳ３２と、読み取った２次元コードＣＤの情報が事前に登録されたユーザー情報か否かを判定する２次元コード判定ステップＳ３３と、ＩＤ・パスワード判定ステップＳ３２におけるユーザー固有情報およびユーザーログインパスワードについての所定要件、かつ、２次元コード判定ステップＳ３３におけるユーザー情報についての所定要件の両方を満たすか否かを判定する要件判定ステップＳ３４と、両方を満たしたとき、ユーザーのコンピュータ端末１１０のログインを許可するログイン許可ステップＳ３４とを具備していることにより、ＩＤ・パスワード入力のみの構成と比べてセキュリティレベルを高めることができる。
【００７０】
また、本発明の第４実施例であるログイン認証システム１００は、ユーザーのコンピュータ端末１１０とサーバ１２０とを備え、ユーザーのコンピュータ端末１１０またはサーバ１２０の制御部が、ユーザーのコンピュータ端末１１０のカメラ１１４を用いてユーザーの２次元コードＣＤを読み取り、ユーザーのコンピュータ端末１１０において入力されたユーザー固有情報およびユーザーログインパスワード情報が事前に登録されたユーザー固有情報およびユーザーログインパスワード情報か否かを判定し、読み取った２次元コードＣＤの情報が事前に登録されたユーザー情報か否かを判定し、ユーザー固有情報およびユーザーログインパスワードについての所定要件、かつ、ユーザー情報についての所定要件の両方を満たすか否かを判定し、両方を満たしたとき、ユーザーのコンピュータ端末１１０のログインを許可する構成であることにより、ＩＤ・パスワード入力のみの構成と比べてセキュリティレベルを高めることができるなど、その効果は甚大である。
【符号の説明】
【００７１】
１００　・・・　ログイン認証システム
１１０　・・・　コンピュータ端末（ユーザー端末）
１１１　・・・　表示部
１１２　・・・　ログイン画面
１１２ａ・・・　ユーザーＩＤ入力欄
１１２ｂ・・・　パスワード入力欄
１１２ｃ・・・　カメラ撮影映像欄
１１２ｄ・・・　撮影ボタン
１１２ｅ・・・　ログインボタン

１１３　・・・　操作部
１１４　・・・　カメラ
１２０　・・・　サーバ
ＰＴ１　・・・　（ログインする際に撮影した）画像データ
ＰＴ２　・・・　（事前に登録されたユーザーの）顔写真データ
ＣＤ　　・・・　２次元コード

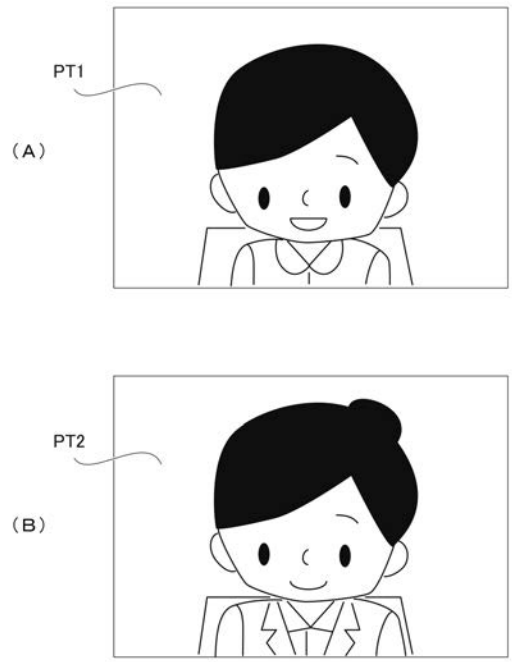
【図１】



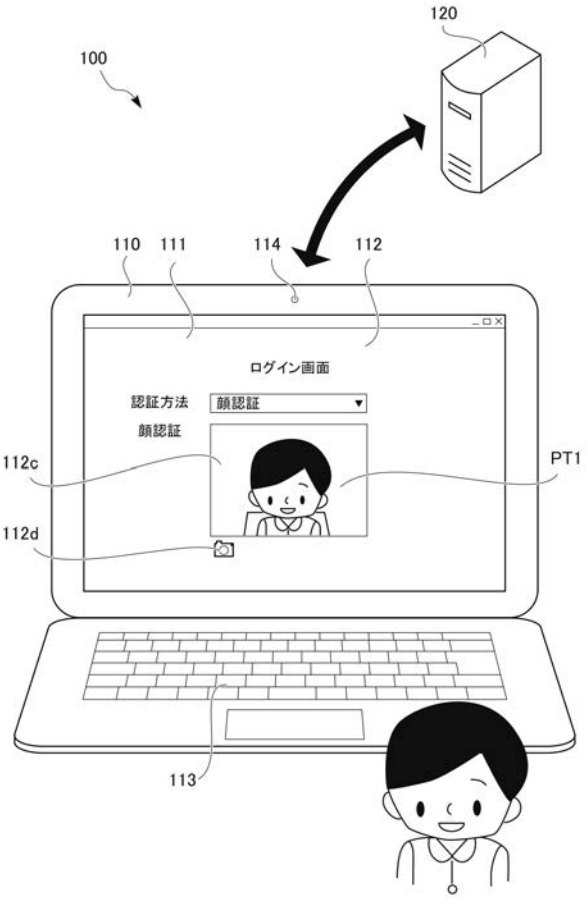
【図２】



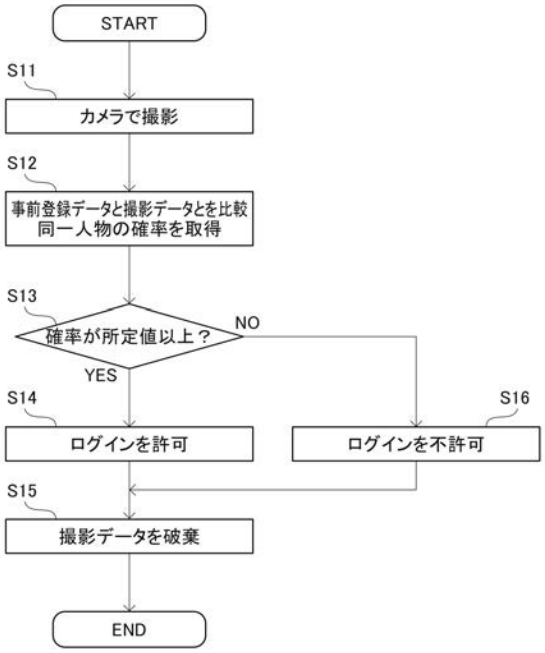
【図３】


PT1
（A）
PT2
（B）
（C）
撮影された人が、登録されたユーザー：鈴木えみさんである確率91%

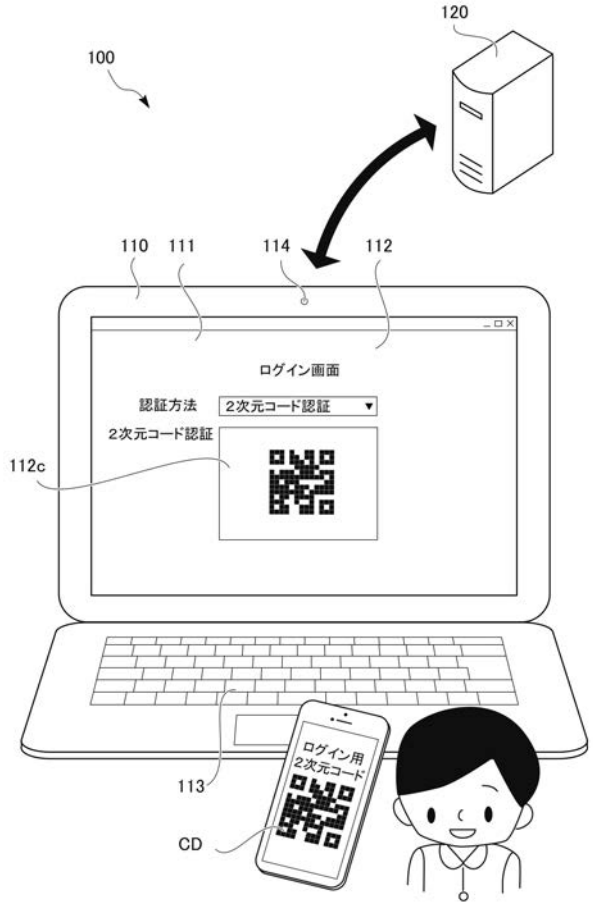
【図４】


120
100
110
111
114
112
ログイン画面
認証方法
顔認証
顔認証
112c
PT1
112d
113

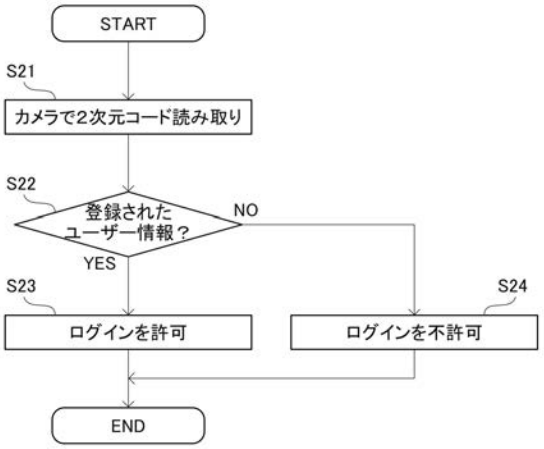
【図５】


START
S11
カメラで撮影
S12
事前登録データと撮影データとを比較
同一人物の確率を取得
S13
確率が所定値以上？
NO
YES
S14
ログインを許可
S16
ログインを不許可
S15
撮影データを破棄
END

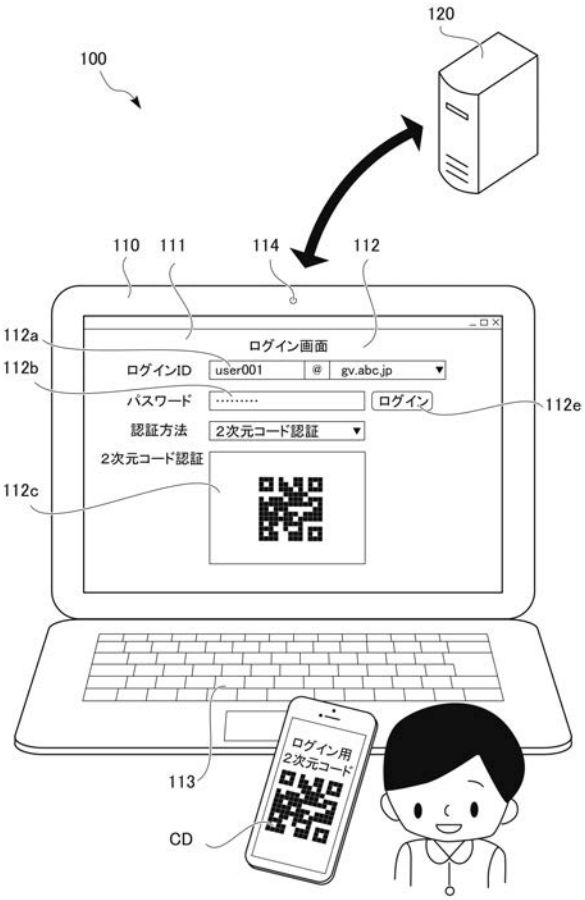
【図６】


120
100
110
111
114
112
ログイン画面
認証方法
2次元コード認証
2次元コード認証
112c
113
ログイン用
2次元コード
CD

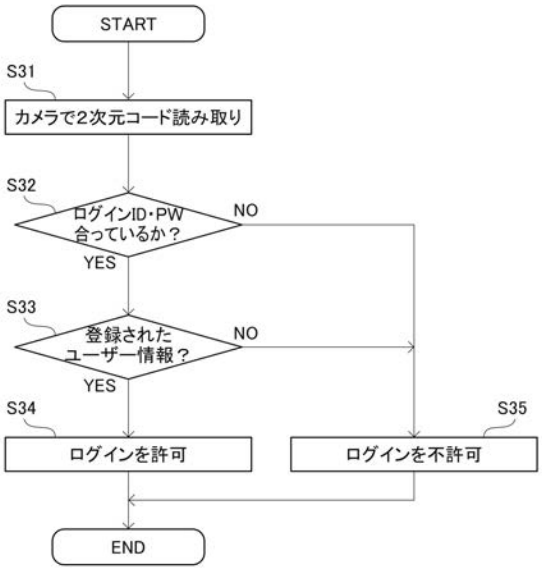
【図７】


START
S21
カメラで2次元コード読み取り
S22
登録された
ユーザー情報？
NO
YES
S23
ログインを許可
S24
ログインを不許可
END

【図８】


120
100
110
111
114
112
112a
ログイン画面
ログインID
user001
@
gv.abc.jp
112b
パスワード
ログイン
112e
認証方法
2次元コード認証
2次元コード認証
112c
ログイン用
2次元コード
113
CD

【図９】


START
S31
カメラで2次元コード読み取り
S32
ログインID・PW
合っているか？
NO
YES
S33
登録された
ユーザー情報？
NO
YES
S34
ログインを許可
S35
ログインを不許可
END

フロントページの続き

特許法第３０条第２項適用申請有り　平成３０年９月１４日にサテライトオフィス・シングルサインオン　ｆｏｒ　ＬＩＮＥ　ＷＯＲＫＳページに掲載　ｈｔｔｐｓ：／／ｗｗｗ．ｓａｔｅｒａｉｔｏ．ｊｐ／ＳＳＯ＿ＷｏｒｋｓＭｏｂｉｌｅ．ｈｔｍｌ　平成３０年９月１４日にサテライトオフィス・シングルサインオン　ｆｏｒ　ＬＩＮＥ　ＷＯＲＫＳページに動画アップロード　ｈｔｔｐｓ：／／ｗｗｗ．ｓａｔｅｒａｉｔｏ．ｊｐ／ＳＳＯ＿ＷｏｒｋｓＭｏｂｉｌｅ．ｈｔｍｌ＃ｔａｂＴｏｐ　平成３０年９月１４日にＹｏｕＴｕｂｅページに動画アップロード　ｈｔｔｐｓ：／／ｗｗｗ．ｙｏｕｔｕｂｅ．ｃｏｍ／ｗａｔｃｈ？ｔｉｍｅ＿ｃｏｎｔｉｎｕｅ＝７９＆ｖ＝５ｔｗＹＧｐ８ｖＥ３Ｅ　平成３０年９月１５日にＹｏｕＴｕｂｅページに動画アップロード　ｈｔｔｐｓ：／／ｗｗｗ．ｙｏｕｔｕｂｅ．ｃｏｍ／ｗａｔｃｈ？ｖ＝５ｔｗＹＧｐ８ｖＥ３Ｅ　平成３１年１月１５日にサテライトオフィス・シングルサインオン　ｆｏｒ　Ｇ　Ｓｕｉｔｅページに掲載　ｈｔｔｐｓ：／／ｗｗｗ．ｓａｔｅｒａｉｔｏ．ｊｐ／Ｇｏｏｇｌｅ＿Ａｐｐｓ＿ＳＳＯ．ｈｔｍｌ　平成３１年１月１５日にサテライトオフィス・シングルサインオン　ｆｏｒ　Ｇ　ＳｕｉｔｅページにＰＤＦ資料アップロード　ｈｔｔｐｓ：／／ｗｗｗ．ｓａｔｅｒａｉｔｏ．ｊｐ／Ｇｏｏｇｌｅ＿Ａｐｐｓ＿ＳＳＯ．ｈｔｍｌ＃ｔａｂＴｏｐ　平成３１年１月１５日にサテライトオフィス・シングルサインオン　ｆｏｒ　Ｗｏｒｋｐｌａｃｅ　ｂｙ　Ｆａｃｅｂｏｏｋページに掲載　ｈｔｔｐｓ：／／ｗｗｗ．ｓａｔｅｒａｉｔｏ．ｊｐ／ＳＳＯ＿Ｆａｃｅｂｏｏｋ．ｈｔｍｌ　平成３１年１月１５日にサテライトオフィス・シングルサインオン　ｆｏｒ　Ｃｈａｔｗｏｒｋページに掲載　ｈｔｔｐｓ：／／ｗｗｗ．ｓａｔｅｒａｉｔｏ．ｊｐ／ＳＳＯ＿Ｃｈａｔｗｏｒｋ．ｈｔｍｌ　平成３１年１月１５日にサテライトオフィス・シングルサインオン　ｆｏｒ　Ｄｒｏｐｂｏｘ　Ｂｕｓｉｎｅｓｓページに掲載　ｈｔｔｐｓ：／／ｗｗｗ．ｓａｔｅｒａｉｔｏ．ｊｐ／ＳＳＯ＿Ｄｒｏｐｂｏｘ．ｈｔｍｌ　平成３１年１月１５日にサテライトオフィス・シングルサインオン　ｆｏｒ　Ｓａｌｅｓｆｏｒｃｅページに掲載　ｈｔｔｐｓ：／／ｗｗｗ．ｓａｔｅｒａｉｔｏ．ｊｐ／ＳＳＯ＿Ｓａｌｅｓｆｏｒｃｅ．ｈｔｍｌ　平成３１年１月１８日にサテライトオフィス・シ