(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2009-187183
(P2009-187183A)
(43)公開日　平成21年8月20日(2009.8.20)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330B	5B285
H04L 9/32	(2006.01)	H04L	9/00	673A	5J104
		H04L	9/00	675D	

審査請求 有　請求項の数 36　ＯＬ　（全 26 頁）

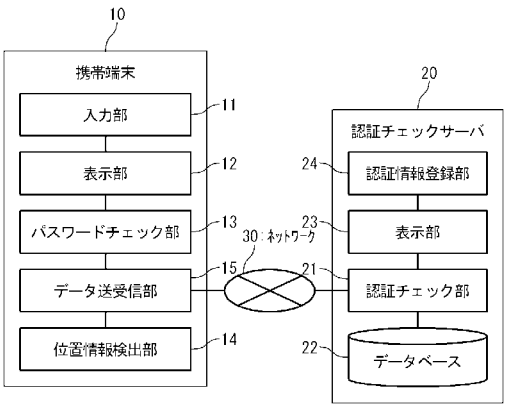
(21)出願番号　特願2008-25054(P2008-25054)
(22)出願日　平成20年2月5日(2008.2.5)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100102864
弁理士　工藤　実
(72)発明者　加藤　浩二
東京都港区芝五丁目７番１号　日本電気株式会社内

Ｆターム(参考)　5B285 AA01 BA02 CB02 CB42 CB49
CB62 CB72 CB85 DA03
5J104 AA07 KA02 KA04 KA20 MA01
NA05 NA38

(54)【発明の名称】認証チェックシステム、携帯端末、認証チェックサーバ、認証チェック方法、及びプログラム

(57)【要約】
【課題】第三者による携帯端末の不正利用を防止する。
【解決手段】携帯端末は、入力されたユーザＩＤ及びパスワードを確認し、確認結果がＯＫの場合、自身の位置情報を取得し、自身を示す端末ＩＤ、ユーザＩＤ、及び位置情報を送信し、ログイン許可通知を受信すればログイン処理を行う。認証チェックサーバは、端末ＩＤ、ユーザＩＤ、及び位置情報を受信し、端末ＩＤ、ユーザＩＤ、及び位置情報と、データベースに登録されている登録端末ＩＤ、登録ユーザＩＤ、及び登録位置情報とを比較し、前記端末ＩＤと前記登録端末ＩＤとが一致し、前記ユーザＩＤと前記登録ユーザＩＤとが一致し、前記位置情報と前記登録位置情報との比較結果が所定の条件に適合していれば、ログイン許可通知を送信する。
【選択図】図１



【特許請求の範囲】
【請求項１】
ログインを要求する際、入力されたユーザＩＤ及びパスワードを確認し、確認結果がＯＫの場合、自身の位置情報を取得し、自身を示す端末ＩＤ、前記ユーザＩＤ、及び前記位置情報を送信し、ログイン許可通知を受信する携帯端末と、
前記端末ＩＤ、前記ユーザＩＤ、及び前記位置情報を受信し、前記端末ＩＤ、前記ユーザＩＤ、及び前記位置情報と、データベースに登録されている登録端末ＩＤ、登録ユーザＩＤ、及び登録位置情報とを比較し、前記端末ＩＤと前記登録端末ＩＤとが一致し、前記ユーザＩＤと前記登録ユーザＩＤとが一致し、前記位置情報と前記登録位置情報との比較結果が所定の条件に適合していれば、前記ログイン許可通知を送信する認証チェックサーバと
を含む
認証チェックシステム。
【請求項２】
請求項１に記載の認証チェックシステムであって、
前記携帯端末は、起動する際、及びスリープ状態から復帰する際に、前記ユーザＩＤ及び前記パスワードの入力を要求し、前記ユーザＩＤ及び前記パスワードを確認し、確認結果がＯＫの場合、前記端末ＩＤ、前記ユーザＩＤ、及び前記位置情報を前記認証チェックサーバに送信する
認証チェックシステム。
【請求項３】
請求項１又は２に記載の認証チェックシステムであって、
前記携帯端末は、起動する際、及びスリープ状態から復帰する際に、前記端末ＩＤ及び前記位置情報を前記認証チェックサーバに送信し、前記端末ＩＤに対応する前記登録端末ＩＤが「接続禁止」として前記データベースに登録されている場合、前記認証チェックサーバから接続禁止通知を受信し、入力を拒否してロック状態とし、ログイン中であれば強制ログオフ処理を行う
認証チェックシステム。
【請求項４】
ログインを要求する際、自身の位置情報を取得し、前記位置情報を送信し、前記位置情報に対する応答としてログイン処理に必要な認証情報の入力要求を受信し、前記認証情報を送信し、前記認証情報に対する応答としてログイン許可通知を受信する携帯端末と、
前記位置情報を受信し、前記位置情報とデータベースに登録されている登録位置情報との間の距離を算出し、前記算出された距離に応じて前記認証情報を変更し、前記認証情報の入力要求を送信し、前記認証情報の入力要求に対する応答として前記認証情報を受信し、前記認証情報が前記データベースに登録されていれば、前記ログイン許可通知を送信する認証チェックサーバと
を含む
認証チェックシステム。
【請求項５】
請求項４に記載の認証チェックシステムであって、
前記認証チェックサーバは、前記算出された距離が所定の閾値以下であれば、前記認証情報として簡易パスワードを要求し、前記算出された距離が所定の閾値以下でなければ、前記認証情報として通常のパスワードを要求する
認証チェックシステム。
【請求項６】
請求項４に記載の認証チェックシステムであって、
前記認証チェックサーバは、前記算出された距離が近ければ、前記認証情報として認証パスワードの一部を要求し、前記算出された距離が遠ければ、前記認証情報として前記認証パスワードの全文を要求する

認証チェックシステム。
【請求項７】
ユーザＩＤ及びパスワードの入力を受け付ける入力部と、
前記ユーザＩＤ及び前記パスワードを確認するパスワードチェック部と、
前記ユーザＩＤ及び前記パスワードの確認結果がＯＫの場合、自身の位置情報を取得する位置情報取得部と、
ログイン許可判定のために、自身を示す端末ＩＤ、前記ユーザＩＤ、及び前記位置情報を送信し、判定結果に応じて、ログイン処理を行うためのログイン許可通知を受信するデータ送受信部と
を具備する
携帯端末。
【請求項８】
請求項７に記載の携帯端末であって、
前記パスワードチェック部は、前記ログイン許可通知に応じてログイン処理を行う際、前記位置情報に応じた認証情報の入力を要求する
携帯端末。
【請求項９】
請求項８に記載の携帯端末であって、
前記パスワードチェック部は、前記ログイン許可通知に応じてログイン処理を行う際、前記位置情報と所定の位置情報との間の距離が所定の閾値以下であれば、前記認証情報として簡易パスワードの入力を要求し、前記位置情報と前記所定の位置情報との間の距離が所定の閾値以下でなければ、前記認証情報として通常のパスワードの入力を要求する
携帯端末。
【請求項１０】
請求項８に記載の携帯端末であって、
前記パスワードチェック部は、前記ログイン許可通知に応じてログイン処理を行う際、前記位置情報と所定の位置情報との間の距離が近ければ、前記認証情報として認証パスワードの一部の入力を要求し、前記位置情報と前記所定の位置情報との間の距離が遠ければ、前記認証情報として前記認証パスワードの全文の入力を要求する
携帯端末。
【請求項１１】
請求項７乃至１０のいずれか一項に記載の携帯端末であって、
前記パスワードチェック部は、起動する際、及びスリープ状態から復帰する際に、前記ユーザＩＤ及び前記パスワードの入力を要求し、前記ユーザＩＤ及び前記パスワードを確認し、確認結果がＯＫの場合、前記端末ＩＤ、前記ユーザＩＤ、及び前記位置情報を送信する
携帯端末。
【請求項１２】
請求項７乃至１１のいずれか一項に記載の携帯端末であって、
前記パスワードチェック部は、起動する際、及びスリープ状態から復帰する際に、前記端末ＩＤ及び前記位置情報を送信し、前記端末ＩＤが「接続禁止」として設定されている場合、接続禁止通知を受信し、入力を拒否してロック状態とし、ログイン中であれば強制ログオフ処理を行う
携帯端末。
【請求項１３】
ログインを許可する携帯端末を示す登録端末ＩＤ、ログインを許可するユーザを示す登録ユーザＩＤ、及びログインを許可する場所を示す登録位置情報をデータベースに登録する認証情報登録部と、
ログインを要求する携帯端末を示す端末ＩＤ、前記携帯端末の利用者を示すユーザＩＤ、及び前記携帯端末の所在位置を示す位置情報を受信し、前記端末ＩＤ、前記ユーザＩＤ

、及び前記位置情報と、前記登録端末ＩＤ、前記登録ユーザＩＤ、及び前記登録位置情報とを比較し、前記端末ＩＤと前記登録端末ＩＤとが一致し、前記ユーザＩＤと前記登録ユーザＩＤとが一致し、前記位置情報と前記登録位置情報との比較結果が所定の条件に適合していれば、前記ログイン許可通知を送信する認証チェック部と
を具備する
認証チェックサーバ。
【請求項１４】
請求項１３に記載の認証チェックサーバであって、
前記認証チェック部は、前記位置情報と前記登録位置情報との間の距離を算出し、前記算出された距離に応じて、ログイン処理に必要な認証情報を変更する
認証チェックサーバ。
【請求項１５】
請求項１４に記載の認証チェックサーバであって、
前記認証チェック部は、前記算出された距離が所定の閾値以下であれば、前記認証情報として簡易パスワードを要求し、前記算出された距離が所定の閾値以下でなければ、前記認証情報として通常のパスワードを要求する
認証チェックサーバ。
【請求項１６】
請求項１４に記載の認証チェックサーバであって、
前記認証チェック部は、前記算出された距離が近ければ、前記認証情報として認証パスワードの一部を要求し、前記算出された距離が遠ければ、前記認証情報として前記認証パスワードの全文を要求する
認証チェックサーバ。
【請求項１７】
請求項１３乃至１６のいずれか一項に記載の認証チェックサーバであって、
前記認証情報登録部は、前記携帯端末を「接続禁止」とする旨の指示に応じて、前記端末ＩＤに対応する前記登録端末ＩＤに「接続禁止」を示す情報を関連付けて前記データベースに登録する
認証チェックサーバ。
【請求項１８】
請求項１７に記載の認証チェックサーバであって、
前記認証チェック部は、前記携帯端末が起動する際、及び前記携帯端末がスリープ状態から復帰する際に、前記携帯端末から前記端末ＩＤ及び前記位置情報を受信し、前記端末ＩＤに対応する前記登録端末ＩＤに「接続禁止」を示す情報が関連付けられている場合、前記携帯端末に対して接続禁止通知を送信し、前記携帯端末がログイン中であれば強制ログオフ処理を行う
認証チェックサーバ。
【請求項１９】
入力されたユーザＩＤ及びパスワードを確認し、確認結果がＯＫの場合、自身の位置情報を取得し、自身を示す端末ＩＤ、前記ユーザＩＤ、及び前記位置情報を送信し、ログイン許可通知を受信するステップと、
前記端末ＩＤ、前記ユーザＩＤ、及び前記位置情報を受信し、前記端末ＩＤ、前記ユーザＩＤ、及び前記位置情報と、データベースに登録されている登録端末ＩＤ、登録ユーザＩＤ、及び登録位置情報とを比較し、前記端末ＩＤと前記登録端末ＩＤとが一致し、前記ユーザＩＤと前記登録ユーザＩＤとが一致し、前記位置情報と前記登録位置情報との比較結果が所定の条件に適合していれば、前記ログイン許可通知を送信するステップと
を含む
認証チェック方法。
【請求項２０】
請求項１９に記載の認証チェック方法であって、

起動する際、及びスリープ状態から復帰する際に、前記ユーザＩＤ及び前記パスワードの入力を要求し、前記ユーザＩＤ及び前記パスワードを確認し、確認結果がＯＫの場合、前記端末ＩＤ、前記ユーザＩＤ、及び前記位置情報を送信するステップ
を更に含む
認証チェック方法。
【請求項２１】
請求項１９又は２０に記載の認証チェック方法であって、
起動する際、及びスリープ状態から復帰する際に、前記端末ＩＤ及び前記位置情報を送信し、前記端末ＩＤに対応する前記登録端末ＩＤが「接続禁止」として前記データベースに登録されている場合、前記認証チェックサーバから接続禁止通知を受信し、入力を拒否してロック状態とし、ログイン中であれば強制ログオフ処理を行うステップ
を更に含む
認証チェック方法。
【請求項２２】
ログインを要求する際、自身の位置情報を取得し、前記位置情報を送信し、前記位置情報に対する応答としてログイン処理に必要な認証情報の入力要求を受信し、前記認証情報を送信し、前記認証情報に対する応答としてログイン許可通知を受信するステップと、
前記位置情報を受信し、前記位置情報とデータベースに登録されている登録位置情報との間の距離を算出し、前記算出された距離に応じて前記認証情報を変更し、前記認証情報の入力要求を送信し、前記認証情報の入力要求に対する応答として前記認証情報を受信し、前記認証情報が前記データベースに登録されていれば、前記ログイン許可通知を送信するステップと
を含む
認証チェック方法。
【請求項２３】
請求項２２に記載の認証チェック方法であって、
前記算出された距離が所定の閾値以下であれば、前記認証情報として簡易パスワードを要求し、前記算出された距離が所定の閾値以下でなければ、前記認証情報として通常のパスワードを要求するステップ
を更に含む
認証チェック方法。
【請求項２４】
請求項２２に記載の認証チェック方法であって、
前記算出された距離が近ければ、前記認証情報として認証パスワードの一部を要求し、前記算出された距離が遠ければ、前記認証情報として前記認証パスワードの全文を要求するステップ
を更に含む
認証チェック方法。
【請求項２５】
ユーザＩＤ及びパスワードの入力を受け付けるステップと、
前記ユーザＩＤ及び前記パスワードを確認するステップと、
前記ユーザＩＤ及び前記パスワードの確認結果がＯＫの場合、自身の位置情報を取得するステップと、
ログイン許可判定のために、自身を示す端末ＩＤ、前記ユーザＩＤ、及び前記位置情報を送信し、判定結果に応じて、ログイン処理を行うためのログイン許可通知を受信するステップと
を、プロセッサに実行させるための
プログラム。
【請求項２６】
請求項２５に記載のプログラムであって、

前記ログイン許可通知に応じてログイン処理を行う際、前記位置情報に応じた認証情報の入力を要求するステップ
を、更にプロセッサに実行させるための
プログラム。
【請求項２７】
請求項２６に記載のプログラムであって、
前記位置情報と所定の位置情報との間の距離が所定の閾値以下であれば、前記認証情報として簡易パスワードの入力を要求するステップと、
前記位置情報と前記所定の位置情報との間の距離が所定の閾値以下でなければ、前記認証情報として通常のパスワードの入力を要求するステップと
を、更にプロセッサに実行させるための
プログラム。
【請求項２８】
請求項２６に記載のプログラムであって、
前記位置情報と所定の位置情報との間の距離が近ければ、前記認証情報として認証パスワードの一部の入力を要求するステップと、
前記位置情報と前記所定の位置情報との間の距離が遠ければ、前記認証情報として前記認証パスワードの全文の入力を要求するステップと
を、更にプロセッサに実行させるための
プログラム。
【請求項２９】
請求項２５乃至２８のいずれか一項に記載のプログラムであって、
起動する際、及びスリープ状態から復帰する際に、前記ユーザＩＤ及び前記パスワードの入力を要求し、前記ユーザＩＤ及び前記パスワードを確認し、確認結果がＯＫの場合、前記端末ＩＤ、前記ユーザＩＤ、及び前記位置情報を送信するステップ
を、更にプロセッサに実行させるための
プログラム。
【請求項３０】
請求項２５乃至２９のいずれか一項に記載のプログラムであって、
起動する際、及びスリープ状態から復帰する際に、前記端末ＩＤ及び前記位置情報を送信するステップと、
前記端末ＩＤが「接続禁止」として設定されている場合、接続禁止通知を受信し、入力を拒否してロック状態とし、ログイン中であれば強制ログオフ処理を行うステップと
を、更にプロセッサに実行させるための
プログラム。
【請求項３１】
ログインを許可する携帯端末を示す登録端末ＩＤ、ログインを許可するユーザを示す登録ユーザＩＤ、及びログインを許可する場所を示す登録位置情報を設定するステップと、
ログインを要求する携帯端末を示す端末ＩＤ、前記携帯端末の利用者を示すユーザＩＤ、及び前記携帯端末の所在位置を示す位置情報を受信し、前記端末ＩＤ、前記ユーザＩＤ、及び前記位置情報と、前記登録端末ＩＤ、前記登録ユーザＩＤ、及び前記登録位置情報とを比較し、前記端末ＩＤと前記登録端末ＩＤとが一致し、前記ユーザＩＤと前記登録ユーザＩＤとが一致し、前記位置情報と前記登録位置情報との比較結果が所定の条件に適合していれば、前記ログイン許可通知を送信するステップと
を、プロセッサに実行させるための
プログラム。
【請求項３２】
請求項３１に記載のプログラムであって、
前記位置情報と前記登録位置情報との間の距離を算出し、前記算出された距離に応じて、前記ログイン処理に必要な認証情報を変更するステップ

を、更にプロセッサに実行させるための
プログラム。
【請求項３３】
請求項３２に記載のプログラムであって、
前記算出された距離が所定の閾値以下であれば、前記認証情報として簡易パスワードを要求するステップと、
前記算出された距離が所定の閾値以下でなければ、前記認証情報として通常のパスワードを要求するステップと
を、更にプロセッサに実行させるための
プログラム。
【請求項３４】
請求項３２に記載のプログラムであって、
前記算出された距離が近ければ、前記認証情報として認証パスワードの一部を要求するステップと、
前記算出された距離が遠ければ、前記認証情報として前記認証パスワードの全文を要求するステップと
を、更にプロセッサに実行させるための
プログラム。
【請求項３５】
請求項３１乃至３４のいずれか一項に記載のプログラムであって、
前記携帯端末を「接続禁止」とする旨の指示に応じて、前記端末ＩＤに対応する前記登録端末ＩＤに「接続禁止」を示す情報を関連付けて設定するステップ
を、更にプロセッサに実行させるための
プログラム。
【請求項３６】
請求項３５に記載のプログラムであって、
前記携帯端末が起動する際、及び前記携帯端末がスリープ状態から復帰する際に、前記携帯端末から前記端末ＩＤ及び前記位置情報を受信するステップと、
前記端末ＩＤに対応する前記登録端末ＩＤに「接続禁止」を示す情報が関連付けられている場合、前記携帯端末に対して接続禁止通知を送信し、前記携帯端末がログイン中であれば強制ログオフ処理を行うステップと
を、更にプロセッサに実行させるための
プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、認証チェックシステムに関し、特に位置情報を検出できる携帯端末を利用した認証チェックシステムに関する。
【背景技術】
【０００２】
一般にログイン動作は、ユーザＩＤ（ｉｄｅｎｔｉｆｉｅｒ）及びパスワードの組み合わせをデータベースに登録しておき、指定されたユーザＩＤとパスワードの組み合わせが、データベースに登録されているかを確認し、登録されている場合には、ログインを許可し、登録されていない場合には、ログインを拒否している。
【０００３】
セキュリティの観点からパスワードは一定期間で変更することが推奨されているが、利用者（ユーザ）にすれば、一定期間でパスワードを変更することは面倒であり、設定したパスワードを忘れてしまう場合もある。
【０００４】
また、ログイン処理は、通常ユーザＩＤとパスワードを組み合わせて実行されるが、ユ

ーザＩＤ及びパスワードを不正に入手した第三者に対してログイン処理が許可されてしまうという問題がある。すなわち、ユーザＩＤ及びパスワードを不正に入手した第三者に対してログインが許可される場合がある。

【０００５】

更に、盗難／紛失した携帯端末に対して第三者の不正ログイン操作を抑止することができないという問題がある。

【０００６】

関連する技術として、特開２００５－０５０１５０号公報（特許文献１）に「測位情報による認証システム」が開示されている。

この認証システムは、情報端末が自身の現在位置を測定する測位手段と、利用者が認証要求するとき、ＩＤ或いはパスワード又は現在位置のうちのいずれか少なくとも一つを認証システムに送付する手段と、ＩＤ及びパスワード並びに認証要求する場所を限定する位置情報を登録する認証データベースと、ＩＤ或いはパスワード又は現在位置のうちの少なくともいずれか一つによって検索した位置情報と、現在位置と、がその許容範囲内で一致して、認証要求を認証する認証手段とを備える。

【０００７】

【特許文献１】特開２００５－０５０１５０号公報

【発明の開示】

【発明が解決しようとする課題】

【０００８】

本発明の目的は、ＧＰＳ（Ｇｌｏｂａｌ　Ｐｏｓｉｔｉｏｎｉｎｇ　Ｓｙｓｔｅｍ）センサや地表高センサ等の位置情報検出手段を具備した携帯端末やノートＰＣにおいて、位置情報検出手段から取得した位置情報を認証処理に使用し、位置情報検出手段から取得した位置情報が所定位置にある場合にログインを許可する認証チェックシステム、携帯端末、認証チェックサーバ、認証チェック方法、及びプログラムを提供することである。

【課題を解決するための手段】

【０００９】

本発明の認証チェックシステムは、ログインを要求する際、入力されたユーザＩＤ及びパスワードを確認し、確認結果がＯＫの場合、自身の位置情報を取得し、自身を示す端末ＩＤ、ユーザＩＤ、及び位置情報を送信し、ログイン許可通知を受信する携帯端末と、端末ＩＤ、ユーザＩＤ、及び位置情報を受信し、端末ＩＤ、ユーザＩＤ、及び位置情報と、データベースに登録されている登録端末ＩＤ、登録ユーザＩＤ、及び登録位置情報とを比較し、端末ＩＤと登録端末ＩＤとが一致し、ユーザＩＤと登録ユーザＩＤとが一致し、位置情報と登録位置情報との比較結果が所定の条件に適合していれば、ログイン許可通知を送信する認証チェックサーバとを含む。

【００１０】

本発明の他の認証チェックシステムは、ログインを要求する際、自身の位置情報を取得し、前記位置情報を送信し、前記位置情報に対する応答としてログイン処理に必要な認証情報の入力要求を受信し、前記認証情報を送信し、前記認証情報に対する応答としてログイン許可通知を受信する携帯端末と、前記位置情報を受信し、前記位置情報とデータベースに登録されている登録位置情報との間の距離を算出し、前記算出された距離に応じて前記認証情報を変更し、前記認証情報の入力要求を送信し、前記認証情報の入力要求に対する応答として前記認証情報を受信し、前記認証情報が前記データベースに登録されていれば、前記ログイン許可通知を送信する認証チェックサーバとを含む。

【００１１】

本発明の携帯端末は、ユーザＩＤ及びパスワードの入力を受け付ける入力部と、ユーザＩＤ及びパスワードを確認するパスワードチェック部と、ユーザＩＤ及びパスワードの確認結果がＯＫの場合、自身の位置情報を取得する位置情報取得部と、ログイン許可判定のために、自身を示す端末ＩＤ、ユーザＩＤ、及び位置情報を送信し、判定結果に応じて、ログイン処理を行うためのログイン許可通知を受信するデータ送受信部とを具備する。

【００１２】
本発明の認証チェックサーバは、ログインを許可する携帯端末を示す登録端末ＩＤ、ログインを許可するユーザを示す登録ユーザＩＤ、及びログインを許可する場所を示す登録位置情報をデータベースに登録する認証情報登録部と、ログインを要求する携帯端末を示す端末ＩＤ、携帯端末の利用者を示すユーザＩＤ、及び携帯端末の所在位置を示す位置情報を受信し、端末ＩＤ、ユーザＩＤ、及び位置情報と、登録端末ＩＤ、登録ユーザＩＤ、及び登録位置情報とを比較し、端末ＩＤと登録端末ＩＤとが一致し、ユーザＩＤと登録ユーザＩＤとが一致し、位置情報と登録位置情報との比較結果が所定の条件に適合していれば、ログイン許可通知を送信する認証チェック部とを具備する。
【００１３】
本発明の認証チェック方法は、ログインを要求する際、入力されたユーザＩＤ及びパスワードを確認し、確認結果がＯＫの場合、自身の位置情報を取得し、自身を示す端末ＩＤ、ユーザＩＤ、及び位置情報を送信し、ログイン許可通知を受信するステップと、端末ＩＤ、ユーザＩＤ、及び位置情報を受信し、端末ＩＤ、ユーザＩＤ、及び位置情報と、データベースに登録されている登録端末ＩＤ、登録ユーザＩＤ、及び登録位置情報とを比較し、端末ＩＤと登録端末ＩＤとが一致し、ユーザＩＤと登録ユーザＩＤとが一致し、位置情報と登録位置情報との比較結果が所定の条件に適合していれば、ログイン許可通知を送信するステップとを含む。
【００１４】
ログインを要求する際、自身の位置情報を取得し、前記位置情報を送信し、前記位置情報に対する応答としてログイン処理に必要な認証情報の入力要求を受信し、前記認証情報を送信し、前記認証情報に対する応答としてログイン許可通知を受信するステップと、前記位置情報を受信し、前記位置情報とデータベースに登録されている登録位置情報との間の距離を算出し、前記算出された距離に応じて前記認証情報を変更し、前記認証情報の入力要求を送信し、前記認証情報の入力要求に対する応答として前記認証情報を受信し、前記認証情報が前記データベースに登録されていれば、前記ログイン許可通知を送信するステップとを含む。
【００１５】
本発明のプログラムは、携帯端末側で実行されるプログラムであって、ユーザＩＤ及びパスワードの入力を受け付けるステップと、ユーザＩＤ及びパスワードを確認するステップと、ユーザＩＤ及びパスワードの確認結果がＯＫの場合、自身の位置情報を取得するステップと、ログイン許可判定のために、自身を示す端末ＩＤ、ユーザＩＤ、及び位置情報を送信し、判定結果に応じて、ログイン処理を行うためのログイン許可通知を受信するステップとを、プロセッサに実行させるためのプログラムである。
【００１６】
本発明の他のプログラムは、認証チェックサーバ側で実行されるプログラムであって、ログインを許可する携帯端末を示す登録端末ＩＤ、ログインを許可するユーザを示す登録ユーザＩＤ、及びログインを許可する場所を示す登録位置情報を設定するステップと、ログインを要求する携帯端末を示す端末ＩＤ、携帯端末の利用者を示すユーザＩＤ、及び携帯端末の所在位置を示す位置情報を受信し、端末ＩＤ、ユーザＩＤ、及び位置情報と、登録端末ＩＤ、登録ユーザＩＤ、及び登録位置情報とを比較し、端末ＩＤと登録端末ＩＤとが一致し、ユーザＩＤと登録ユーザＩＤとが一致し、位置情報と登録位置情報との比較結果が所定の条件に適合していれば、ログイン許可通知を送信するステップとを、プロセッサに実行させるためのプログラムである。
【発明の効果】
【００１７】
第三者による携帯端末の不正利用を防止することができる。
【発明を実施するための最良の形態】
【００１８】
以下に、本発明の第１実施形態について添付図面を参照して説明する。

図１を参照すると、本実施形態の認証チェックシステムは、携帯端末１０と、認証チェックサーバ２０と、ネットワーク３０を含む。携帯端末１０と認証チェックサーバ２０は、ネットワーク３０を介して接続されている。なお、携帯端末１０は、ネットワーク３０を経由して複数台の接続が可能である。すなわち、携帯端末１０は複数の場合がある。但し、実際には、ネットワーク３０を介さない場合も考えられる。この場合、携帯端末１０と認証チェックサーバ２０は、直接接続されているか、近距離無線通信等により直接通信を行うものとする。

【００１９】

携帯端末１０は、ネットワーク通信に対応し、認証処理の対象となる通信装置である。携帯端末１０の例としては、携帯電話機やノート型ＰＣ（パソコン）、ＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔｓ）、ネットワーク対応のゲーム機、その他のガジェット（ｇａｄｇｅｔ）等が考えられる。但し、実際には、これらの例に限定されない。例えば、携帯端末１０は、持ち運び可能な携帯端末に限らず、自動車、鉄道、船舶、及び航空機等の移動体に搭載された通信装置や、設置場所を移転することが可能なデスクトップ型ＰＣやインターネット家電等の固定端末／有線端末でも良い。

【００２０】

認証チェックサーバ２０は、ネットワーク通信に対応し、携帯端末１０に対する認証処理を行う通信装置である。認証チェックサーバ２０は、システム管理者により管理される。認証チェックサーバ２０の例として、ネットワーク対応のサーバ、携帯電話の基地局、無線ＬＡＮのアクセスポイント、携帯端末１０と同種の携帯端末等が考えられる。但し、実際には、これらの例に限定されない。

【００２１】

ネットワーク３０は、携帯端末１０と認証チェックサーバ２０を接続する通信回線である。ネットワーク３０は、有線／無線を問わない。また、ネットワーク３０は、複数のネットワークを接続するルータやスイッチ等の中継装置や、携帯端末１０又は認証チェックサーバ２０と連携するサーバ等の他の通信装置を含んでいても良い。ネットワーク３０の例として、インターネット、イントラネット、無線ＬＡＮ（Ｗｉｒｅｌｅｓｓ　ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ））スポット、家庭内ＬＡＮ、店舗内ＬＡＮ、専用線、電話通信網、ＩｒＤＡ（Ｉｎｆｒａｒｅｄ　Ｄａｔａ　Ａｓｓｏｃｉａｔｉｏｎ）、Ｂｌｕｅｔｏｏｔｈ（登録商標）、ＷｉＭＡＸ、３Ｇ（第３世代携帯電話）、シリアル通信等が考えられる。また、ネットワーク３０は、物理的な通信回線の上に論理的に構築されたＬ２ＴＰ（Ｌａｙｅｒ　２　Ｔｕｎｎｅｌｉｎｇ　Ｐｒｏｔｏｃｏｌ）やＶＬＡＮ（Ｖｉｒｔｕａｌ　ＬＡＮ）のような論理的な通信回線でも良い。但し、実際には、これらの例に限定されない。

【００２２】

携帯端末１０は、入力部１１と、表示部１２と、パスワードチェック部１３と、位置情報取得部１４と、データ送受信部１５を備える。

【００２３】

入力部１１は、携帯端末１０にデータを入力する。入力されるデータの例として、ユーザＩＤ及びパスワード、生体認証情報、ＩＣタグ等に記憶された情報、ＱＲコード（登録商標）等が考えられる。すなわち、入力部１１は、ユーザ認証に用いられるデータを携帯端末１０に提供する。ここでは、入力部１１は、携帯端末１０の所有者等の利用者（ユーザ）により入力されたユーザＩＤ及びパスワードを取得し、携帯端末１０に提供する。入力部１１の例として、キーボードやキーパッド、画面上のキーパッド、タッチパネル（ｔｏｕｃｈ　ｐａｎｅｌ）、タブレット（ｔａｂｌｅｔ）、又は、生体認証情報やＩＣチップ等の読取装置（ｒｅａｄｅｒ）等が考えられる。或いは、入力部１１は、外部の入力装置や通信装置からデータを取得するインターフェース（Ｉ／Ｆ：ｉｎｔｅｒｆａｃｅ）でも良い。但し、実際には、これらの例に限定されない。

【００２４】

表示部１２は、パスワード入力画面や、認証チェック結果を表示する。ここでは、表示

部１２は、利用者にユーザＩＤ及びパスワードの入力を促すための入力画面を表示する。表示部１２の例として、ＬＣＤ（Ｌｉｑｕｉｄ Ｃｒｙｓｔａｌ Ｄｉｓｐｌａｙ）やＰＤＰ（Ｐｌａｓｍａ Ｄｉｓｐｌａｙ Ｐａｎｅｌ）、又は、表示内容を壁やスクリーンに投影するプロジェクタ、表示内容を用紙等に印刷するプリンタ等が考えられる。或いは、表示部１２は、外部の表示装置に表示用のデータを提供して表示させるインターフェース（Ｉ／Ｆ：ｉｎｔｅｒｆａｃｅ）でも良い。但し、実際には、これらの例に限定されない。

【００２５】

パスワードチェック部１３は、入力部１１から受け取ったユーザＩＤ及びパスワードが携帯端末１０で有効であるかを確認する。但し、実際には、これらの例に限定されない。例えば、生体認証（バイオメトリクス認証）に対応している場合、パスワードチェック部１３は、ユーザＩＤ及びパスワードの代わりに、利用者（ユーザ）の指紋や虹彩等の生体認証情報をチェックする。また、パスワードチェック部１３は、認証チェックサーバ２０から受信した認証チェック結果を確認する。

【００２６】

位置情報取得部１４は、携帯端末１０の現在の位置情報を示すデータを取得するものである。このとき、位置情報検出部１４は、携帯端末１０の現在位置を示す位置情報を測定することで取得しても良いし、携帯端末１０の現在位置を示す位置情報を外部から受信して取得しても良い。例えば、位置情報取得部１４は、ＧＰＳ（Ｇｌｏｂａｌ Ｐｏｓｉｔｉｏｎｉｎｇ Ｓｙｓｔｅｍ）により携帯端末１０の緯度／経度情報を取得したり、地表高センサにより高さ情報を取得したりして、位置情報としてデータ化することが考えられる。また、位置情報取得部１４は、移動の始点となる特定の場所を定め、この特定の場所からの移動方向と移動距離を常に測定し、この移動方向と移動距離を位置情報としてデータ化することも考えられる。或いは、携帯端末１０を用いて通信する際に、携帯電話の基地局、無線ＬＡＮのアクセスポイント、ゲートウェイ（ｇａｔｅｗａｙ）やプロキシ（ｐｒｏｘｙ）のような、所定の場所にある中継局や中継装置を利用する場合、携帯端末１０が通信時に最初に利用する中継局や中継装置の位置情報を、携帯端末１０の位置情報としても良い。これらの中継局や中継装置の識別情報と位置情報とを関連付けて登録しておけば、中継局や中継装置の識別情報を取得することで、この識別情報に対応する位置情報を取得することができる。同様に、携帯端末１０を介して、自動改札機、ＥＴＣ（Ｅｌｅｃｔｒｏｎｉｃ Ｔｏｌｌ Ｃｏｌｌｅｃｔｉｏｎ Ｓｙｓｔｅｍ）、建物や部屋への入退場管理システム、店舗や施設の料金収受システム等を利用した際に、これらの機器から位置情報を取得し、取得された位置情報を、携帯端末１０の位置情報としても良い。なお、位置情報取得部１４は、携帯端末１０の位置情報を取得した際、現在の位置情報かどうか判断し易くするために、その位置情報を取得した時刻を、位置情報に関連付けておくようにしても良い。ここで、現在の位置情報とは、現在時刻に限らず、現在時刻の前後に取得された位置情報も含む。例えば、現在の位置情報は、現在時刻の前後１分以内に取得された位置情報でも良い。但し、実際には、これらの例に限定されない。

【００２７】

データ送受信部１５は、携帯端末１０に固有の端末ＩＤと、携帯端末１０の現在の位置情報を示すデータを認証チェックサーバ２０に送信し、認証チェックの実行結果データを受信する。なお、携帯端末１０に固有の端末ＩＤの例として、携帯端末１０の電話番号やメールアドレス、或いは携帯端末１０に搭載されたソフトウェアやハードウェアの識別番号等が考えられる。このとき、データ送受信部１５は、端末ＩＤ及び位置情報の組み合わせを暗号化して認証チェックサーバ２０に送信するようにしても良い。

【００２８】

なお、パスワードチェック部１３、位置情報取得部１４、及びデータ送受信部１５は、コンピュータに搭載されたＣＰＵ等のプロセッサ（ｐｒｏｃｅｓｓｏｒ：処理装置）及びメモリ（ｍｅｍｏｒｙ：記憶装置）の組み合わせでも良い。なお、メモリは、メディア（ｍｅｄｉａ：記憶媒体）でも良い。このとき、メモリは、パスワードチェック部１３、位

置情報取得部１４、及びデータ送受信部１５の機能を定義したプログラムを格納する。プロセッサは、このプログラムを実行することで、パスワードチェック部１３、位置情報取得部１４、及びデータ送受信部１５として機能する。また、パスワードチェック部１３、位置情報取得部１４、及びデータ送受信部１５は、携帯端末１０に接続される装置に搭載されていても良い。例えば、パスワードチェック部１３、位置情報取得部１４、及びデータ送受信部１５は、ＮＩＣ（Ｎｅｔｗｏｒｋ　Ｉｎｔｅｒｆａｃｅ　Ｃａｒｄ）等の拡張カードに搭載されていても良い。

【００２９】

認証チェックサーバ２０は、認証チェック部２１と、データベース２２と、表示部２３と、認証情報登録部２４を備える。

【００３０】

認証チェック部２１は、端末から送信された端末ＩＤと位置情報が、データベース２２に登録されているかを確認し、その結果、携帯端末１０に対してログインを許可するか、拒否するか、又は、強制ログオフをするかを判断する。なお、認証チェック部２１は、暗号化された端末ＩＤ及び位置情報の組み合わせを受信した場合、暗号化された端末ＩＤ及び位置情報の組み合わせを復号するようにしても良い。

【００３１】

データベース２２は、認証を許可する端末ＩＤと位置情報との組み合わせ情報が格納された認証情報登録データベースである。データベース２２の例として、ハードディスクのようなストレージ（外部記憶装置）等が考えられる。或いは、データベース２２は、大容量のメディア（ｍｅｄｉａ：記憶媒体）でも良い。また、データベース２２は、ネットワーク３０上に存在し、認証チェックサーバ２０と連携するデータベースサーバでも良い。但し、実際には、これらの例に限定されない。

【００３２】

表示部２３は、認証チェック部２１の処理結果を表示する。表示部２３の例として、ＬＣＤ（Ｌｉｑｕｉｄ　Ｃｒｙｓｔａｌ　Ｄｉｓｐｌａｙ）やＰＤＰ（Ｐｌａｓｍａ　Ｄｉｓｐｌａｙ　Ｐａｎｅｌ）、又は、表示内容を壁やスクリーンに投影するプロジェクタ、表示内容を用紙等に印刷するプリンタ等が考えられる。或いは、表示部２３は、外部の表示装置に表示用のデータを提供して表示させるインターフェース（Ｉ／Ｆ：ｉｎｔｅｒｆａｃｅ）でも良い。但し、実際には、これらの例に限定されない。

【００３３】

認証情報登録部２４は、各端末用の端末ＩＤと、ログインを許可する場所の位置情報との組み合わせ情報を、データベース２２に登録する。ここでは、認証情報登録部２４は、予め設定された端末ＩＤと位置情報との組み合わせ情報をデータベース２２に登録する。但し、実際には、認証情報登録部２４は、認証処理の際に、携帯端末１０から受け取った端末ＩＤと位置情報のうち少なくとも一方がデータベース２２に登録されていない場合、システム管理者からの指示又は所定の条件に応じて、この端末ＩＤと位置情報との組み合わせ情報をデータベース２２に登録するか判断し、その結果に応じて、この端末ＩＤと位置情報との組み合わせ情報をデータベース２２に登録するようにしても良い。また、認証情報登録部２４は、特定の端末ＩＤ、特定のユーザＩＤ、又は特定の位置情報でのログインを禁止する旨や、その他の必要な情報をデータベース２２に登録する。

【００３４】

なお、認証チェック部２１及び認証情報登録部２４は、コンピュータに搭載されたＣＰＵ等のプロセッサ（ｐｒｏｃｅｓｓｏｒ：処理装置）及びメモリ（ｍｅｍｏｒｙ：記憶装置）の組み合わせでも良い。なお、メモリは、メディア（ｍｅｄｉａ：記憶媒体）でも良い。このとき、メモリは、認証チェック部２１及び認証情報登録部２４の機能を定義したプログラムを格納する。プロセッサは、このプログラムを実行することで、認証チェック部２１及び認証情報登録部２４として機能する。

【００３５】

次に、図２のフローチャートを参照して、本実施形態の動作について詳細に説明する。

（１）ステップＡ１

認証情報登録部２４は、システム管理者からの指示に応じて、ログインを許可する携帯端末１０の端末ＩＤ、ユーザＩＤ、ログインを許可する場所の位置情報を、事前にデータベース２２に登録する。

（２）ステップＡ２

利用者は、携帯端末１０の電源をＯＮにする。すなわち、携帯端末１０は、利用者の直接的又は間接的な操作に応じて、起動、或いは、スタンバイ状態から回復する。すなわち、携帯端末１０が、使用可能又は動作可能な状態になる。但し、実際には、携帯端末１０の電源をＯＮにする方法は、利用者の操作に限定されない。例えば、携帯端末１０が、タイマー制御により所定の時間に、自動的に電源をＯＮにするようにしても良い。これにより、携帯端末１０が稼動し、以降の動作が可能になる。なお、利用者が携帯端末１０の電源をＯＮにする時期は、認証情報登録部２４が、ログインを許可する携帯端末１０の端末ＩＤ、ユーザＩＤ、ログインを許可する場所の位置情報を、データベース２２に登録する前でも良い。

（３）ステップＡ３

表示部１２は、携帯端末１０が動作を開始した後、自動的に、又は利用者の操作に応じて、パスワード入力画面を表示する。これにより、表示部１２は、利用者に対してログイン用のユーザＩＤ及びパスワードの入力を促す。

【００３６】

ここで、図３を参照して、パスワード入力画面の例について説明する。

パスワード入力画面は、「ユーザＩＤの入力欄」と、「パスワードの入力欄」と、「ログインボタン」を有する。「ユーザＩＤの入力欄」は、利用者が入力部１１からユーザＩＤを入力するための入力欄である。ここでは、「ユーザＩＤの入力欄」の直前に、「ユーザ名を入力してください。」のようにユーザＩＤの入力を促す文が表示されている。この文は、入力欄に表示されていても良い。「パスワードの入力欄」は、利用者が入力部１１からパスワードを入力するための入力欄である。ここでは、「パスワードの入力欄」の直前に、「パスワードを入力してください。」のようにパスワードの入力を促す文が表示されている。この文は、入力欄に表示されていても良い。「ログインボタン」は、押下されると、「ユーザＩＤの入力欄」に入力されたユーザＩＤと、「パスワードの入力欄」に入力されたパスワードを取得する。なお、「ログインボタン」は、利用者が入力部１１に対して指示又は操作することで押下される。例えば、キーボード操作による押下や、マウスのクリック等が考えられる。但し、実際には、これらの例に限定されない。なお、ユーザＩＤ及びパスワードの代わりに、生体認証情報やＩＣカードの情報を使用する場合は、「ユーザＩＤの入力欄」及び「パスワードの入力欄」の代わりに、生体認証情報やＩＣカードの情報の入力方法や入力を促す文を表示する。この表示に従って生体認証情報やＩＣカードの情報が入力された場合、生体認証情報やＩＣカードの情報が入力された旨を示す文や画像を表示するようにしても良い。

【００３７】

（４）ステップＡ４

利用者は、パスワード入力画面に対して、入力部１１からユーザＩＤとパスワードを入力する。このとき、入力部１１は、利用者により入力されたユーザＩＤとパスワードを取得し、パスワードチェック部１３に引き渡す。

（５）ステップＡ５

パスワードチェック部１３は、入力されたユーザＩＤ及びパスワードが、正しい情報であるかの判断をするパスワードチェック処理を行う。このパスワードチェックは、携帯端末１０に内蔵されたデータを参照して行う。パスワードチェック結果が「ＮＧ（失敗／拒否）」の場合には、表示部１２は、ユーザ固有情報の入力画面を再度表示して、ユーザＩＤ及びパスワードの入力を再度促す。

（６）ステップＡ６

パスワードチェック処理の結果が「ＯＫ（成功／許可）」の場合、位置情報取得部１４

は、携帯端末１０自身の物理的な位置情報を取得する。例えば、位置情報取得部１４は、ＧＰＳシステム等を利用して自身の緯度・経度・高度情報を特定し、携帯端末１０の位置情報として取得する。又は、位置情報取得部１４は、ＲＦＩＤ（Ｒａｄｉｏ　Ｆｒｅｑｕｅｎｃｙ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ）や非接触型ＩＣカードとカードリーダ、アンテナ等を利用して電磁界や電波等を用いた近距離無線通信が有効な範囲内で、移動センサ／高さセンサ等を利用して、より小規模な規定の範囲内における携帯端末１０の位置情報を検出する。但し、実際には、これらの例に限定されない。

（７）ステップＡ７

送受信装置１５は、携帯端末１０に固有の端末ＩＤと、利用者が入力したユーザＩＤと、携帯端末１０自身の位置情報を、ネットワーク３０を経由して認証チェック部２１に送信する。

（８）ステップＡ８

認証チェック部２１は、受信した端末ＩＤ、ユーザＩＤ、及び位置情報が、データベース２２に登録されているかを確認する。

【００３８】

ここで、図４を参照して、データベース２２に格納されている情報の例について説明する。

ここでは、データベース２２は、各々の情報をテーブル形式で格納しているものとする。このテーブルを認証情報テーブルと呼ぶ。認証情報テーブルは、「端末」、「ユーザ」、「位置情報（データ）」、「位置情報（場所）」、「利用可能」という項目を有する。「端末」は、端末ＩＤを示す。「ユーザ」は、ユーザＩＤを示す。「位置情報（データ）」は、緯度・経度・高度情報のような位置情報の座標を示す。「位置情報（場所）」は、具体的な地名や住所のような位置情報の識別情報を示す。「利用可能」は、関連付けられた端末ＩＤ、ユーザＩＤ、及び位置情報に該当する携帯端末１０の利用の可否に関する情報を示す。すなわち、「利用可能」は、携帯端末１０から受け取った端末ＩＤ、ユーザＩＤ、及び位置情報が、当該「利用可能」に関連付けられた端末ＩＤ、ユーザＩＤ、及び位置情報と一致する場合に、携帯端末１０の利用を許可するか否かを示す。なお、「利用可能」は、「端末」、「ユーザ」、及び「位置情報（データ）」の各々と個別に関連付けられていても良い。

【００３９】

（９）ステップＡ９

認証チェック部２１は、受信した端末ＩＤとユーザＩＤと位置情報がデータベース２２に登録済みかどうかのチェック結果の情報を表示部２３に表示する。

【００４０】

ここで、図５を参照して、表示部２３に表示されるチェック結果（確認結果）の情報の表示例について説明する。

ここでは、表示部２３は、チェック結果の情報をテーブル形式で表示する。このとき、チェック結果は、「接続状態」、「接続時刻」、「端末ＩＤ」、「ユーザＩＤ」、「位置情報」という項目を有する。「接続状態」は、認証チェック結果として、「ＯＫ（成功／許可）」、又は、「ＮＧ（失敗／拒否）」を示す。「ＯＫ（成功／許可）」であれば、認証チェックサーバ２０は、携帯端末１０から認証チェックサーバ２０又はネットワーク３０へのアクセス（接続）を許可する。「ＮＧ（失敗／拒否）」であれば、認証チェックサーバ２０は、携帯端末１０から認証チェックサーバ２０又はネットワーク３０へのアクセス（接続）を拒否、或いは制限する。なお、ここでは、携帯端末１０のアクセス（接続）に関する認証を例に説明しているが、実際には、携帯端末１０又は認証チェックサーバ２０の機能モジュールの利用許諾に関する認証や、認証チェックサーバ２０又はネットワーク３０上のサーバが提供するサービスの利用許諾に関する認証でも良い。この場合、「接続状態」は、「利用状態」としても良い。「接続時刻」は、認証チェックサーバ２０が携帯端末１０に対する認証チェックを行った時刻を示す。例えば、認証チェックサーバ２０が、携帯端末１０から認証チェックのための情報を受信した時刻を示す。すなわち、「接

続時刻」は、「認証時刻」でも良い。「端末ＩＤ」は、端末ＩＤを示す。「ユーザＩＤ」は、ユーザＩＤを示す。「位置情報」は、緯度・経度・高度情報のような位置情報の座標を示す。

【００４１】

（１０）ステップＡ１０

認証チェック部２１は、認証チェック結果として、「ＯＫ（成功／許可）」、又は、「ＮＧ（失敗／拒否）」を、携帯端末１０に送信する。なお、認証チェック部２１は、チェック結果以外の、データベース２２に登録されている他の情報等を送信しても良い。例えば、図４に示すような情報がデータベース２２に格納されている場合には、「位置情報（場所）」の情報も送信する。その後、認証チェック部２１は、再び、端末ＩＤ、ユーザＩＤ、及び位置情報を受信するまで待機する。

（１１）ステップＡ１１

携帯端末１０で、認証チェックサーバ２０から送信された認証チェック結果を受信し、認証チェック結果を確認する。このとき、データ送受信部１５は、認証チェックサーバ２０から認証チェック結果を受信する。パスワードチェック部１３は、データ送受信部１５が認証チェックサーバ２０から受信した認証チェック結果を確認する。

（１２）ステップＡ１２

パスワードチェック部１３は、認証チェック結果が「ＯＫ（成功／許可）」の場合、表示部１２に認証成功のメッセージを表示する。

【００４２】

ここで、図６を参照して、認証成功のメッセージの表示例について説明する。

ここでは、認証成功のメッセージとして、「認証ＯＫ」、「ユーザ名」、「端末ＩＤ」、「位置情報」、「場所（住所）」が表示される。「認証ＯＫ」は、認証が成功したことを示す。「ユーザ名」は、ユーザＩＤを示す。「端末ＩＤ」は、端末ＩＤを示す。「位置情報」は、緯度・経度・高度情報のような位置情報の座標を示す。「場所（住所）」は、具体的な地名や住所のような位置情報の識別情報を示す。

（１３）ステップＡ１３

認証チェック結果が「ＯＫ（成功／許可）」の場合、携帯端末１０に対してログインが許可され、ログイン後の処理が続行可能となり、ログイン中状態に遷移する。このとき、パスワードチェック部１３は、携帯端末１０の状態をログイン中状態に遷移する。また、認証チェックサーバ２０がプロバイダ等のウェブサービスを提供する事業者のサーバである場合、認証チェック部２１は、データ送受信部１５を介した携帯端末１０からのアクセス（接続）やサービス要求を受け付けるようにする。

（１４）ステップＡ１４

パスワードチェック部１３は、認証チェック結果が「ＮＧ（失敗／拒否）」の場合、表示部１２に認証失敗のメッセージを表示する。

（１５）ステップＡ１５

認証チェック結果が「ＮＧ（失敗／拒否）」の場合、携帯端末１０に対してログインが拒否され、ログイン処理が中断され、ログイン処理開始前状態に処理が戻る。ここでは、パスワードチェック部１３は、携帯端末１０のログイン処理を中断する。このとき、表示部１２は、再びパスワード入力画面を表示するようにしても良い。また、認証チェックサーバ２０がプロバイダ等のウェブサービスを提供する事業者のサーバである場合、認証チェック部２１は、携帯端末１０に対するサービスの提供を中断する。

【００４３】

これにより、従来のユーザＩＤ及びパスワードだけのログイン方式よりも認証処理が強化されたログイン処理を提供できる。

【００４４】

本実施形態では、まず、携帯端末１０側でパスワードチェック処理を行い、パスワードチェック処理の結果がＯＫの場合に、携帯端末１０の位置情報を取得して、認証チェックサーバ２０側で認証処理を行うため、２段階のチェックが可能になる。すなわち、利用者

は、（１）ユーザＩＤ及びパスワードのみ知っている利用者、（２）ユーザＩＤ及びパスワードに加えて使用が許可される場所（位置情報）を知っている利用者、の２種類に分けることも可能である。例えば、（１）のユーザＩＤ及びパスワードのみ知っている利用者は、携帯端末１０の制限された機能だけ使用する利用者とし、（２）のユーザＩＤ及びパスワードに加えて使用が許可される場所（位置情報）を知っている利用者は、携帯端末１０の全ての機能と、認証チェックサーバ２０及びネットワーク３０のサービスを利用する利用者とすることが考えられる。また、端末ＩＤとユーザＩＤを個別に認証するため、特定の携帯端末を使用すればログイン許可される利用者でも、他の携帯端末を使用すればログイン拒否されるようにすることが可能になる。このように、本実施形態では、端末ＩＤ、ユーザＩＤ、及び位置情報の全てが、一致した場合或いは所定の条件に適合した場合に、ログインを許可する。

【００４５】

また、該当携帯端末１０が盗難／紛失し、第三者が携帯端末１０を不特定の場所で利用した場合でも、端末から送信される位置情報が許可された場所と異なることが判断できるため、第三者の不正利用を防止することができる。

【００４６】

更に、端末から位置情報が送信されるため、端末の現在位置を把握することができ、盗難／紛失した場合でも、所在確認が容易に可能である。

【００４７】

なお、本実施形態において、ログイン中状態に、ログイン又は通信を許可する地域（エリア）の外に携帯端末１０が移動した場合、強制ログオフ処理を実行し、ログイン前の状態に戻るようにしても良い。このとき、認証チェック部２１は、周期的に携帯端末１０の位置情報を取得し、取得された位置情報がデータベース２２に登録されているかを確認し、取得された位置情報がデータベース２２に登録されていなければ、強制ログオフ処理を実行し、ログイン前の状態に戻るようにする。

【００４８】

以下に、本発明の第２実施形態について説明する。

第１実施形態では、電源ＯＮ時の動作について説明したが、本実施形態では、携帯端末１０の電源ＯＮ時の場合でなく、携帯端末１０にログイン後、しばらく操作がなかった場合にスリープ状態となり、そのスリープ状態から復帰する場合の動作について説明する。

【００４９】

図７のフローチャートを参照して、本実施形態の動作について詳細に説明する。

（１）ステップＢ１

ログイン中状態でスリープ状態である場合に、入力部１１に対して何らかの操作が行われたことを検出することにより、利用者が携帯端末１０側に対して何らかの操作を行ったことを検出する。なお、ログイン中状態でスリープ状態である場合に、送受信装置１５が外部から何らかの情報を受信したことを検出した場合にも、携帯端末１０に対して何らかの操作が行われたものとして検出するようにしても良い。

（２）ステップＢ２

位置情報取得部１４は、携帯端末１０の現在位置を示す位置情報を取得する。

（３）ステップＢ３

送受信装置１５は、取得した位置情報と、端末ＩＤ、ユーザＩＤを認証チェックサーバ２０に送信する。ここでは、送受信装置１５は、携帯端末１０に固有の端末ＩＤと、利用者が入力したユーザＩＤと、携帯端末１０自身の位置情報を、ネットワーク３０を経由して認証チェック部２１に送信する。

（４）ステップＢ４

認証チェック部２１は、受信した端末ＩＤ、ユーザＩＤ、及び位置情報が、データベース２２に登録されているかを確認する。

（５）ステップＢ５

認証チェック部２１は、受信した端末ＩＤとユーザＩＤと位置情報がデータベース２２

に登録済みかどうかのチェック結果の情報を表示部２３に表示する。
（６）ステップＢ６
認証チェック部２１は、認証チェック結果として、「ＯＫ（成功／許可）」、又は、「ＮＧ（失敗／拒否）」を、携帯端末１０に送信する。なお、チェック結果以外の、データベースに登録されている他の情報等を送信しても良い。例えば、図４に示すような情報がデータベースに格納されている場合には、「位置情報（場所）」の情報も送信する。その後、認証チェック部２１は、再び、端末ＩＤ、ユーザＩＤ、及び位置情報を受信するまで待機する。
（７）ステップＢ７
携帯端末１０で、認証チェックサーバ２０から送信された認証チェック結果を受信し、認証チェック結果を確認する。このとき、データ送受信部１５は、認証チェックサーバ２０から認証チェック結果を受信する。パスワードチェック部１３は、データ送受信部１５が認証チェックサーバ２０から受信した認証チェック結果を確認する。
（８）ステップＢ８
パスワードチェック部１３は、受信したチェック結果が「ＯＫ（成功／許可）」の場合、スリープに入る前に表示していた画面を表示部１２に表示し、処理を継続し、スリープ状態から復帰する。
（９）ステップＢ９
パスワードチェック部１３は、受信したチェック結果が「ＮＧ（失敗／拒否）」の場合、「端末は現在位置では利用できない」という旨のメッセージを表示部１２に表示する。但し、実際には、メッセージは文字に限らず、画像、音声、その他の「端末は現在位置では利用できない」という旨を示す通知でも良い。
（１０）ステップＢ１０
パスワードチェック部１３は、強制ログオフ処理を実行し、ログイン前の状態に戻る。このとき、表示部１２は、再びパスワード入力画面を表示するようにしても良い。また、認証チェックサーバ２０がプロバイダ等のウェブサービスを提供する事業者のサーバである場合、認証チェック部２１は、携帯端末１０に対するサービスの提供を中断する。
【００５０】
以上の動作により、既に電源ＯＮ状態で、携帯端末１０にログインしたままの状態で、携帯端末１０が放置された場合に、盗難／紛失が発生し、第三者が別場所で携帯端末１０を利用できることを防止できる。
【００５１】
以下に、本発明の第３実施形態について説明する。
本実施形態では、携帯端末１０の紛失／盗難が発生し、携帯端末１０を拾得した第三者のログイン要求を拒否する場合の動作について説明する。
【００５２】
図８のフローチャートを参照して、本実施形態の動作について説明する。
（１）ステップＣ１
利用者（ユーザ）は、携帯端末１０の紛失／盗難を認識した場合、データベース２２に格納されている携帯端末１０の情報レコードに対して、「接続禁止」の情報を設定する。このとき、入力部１１は、利用者（ユーザ）の入力操作に応じて、「接続禁止」の情報を設定するための指示データを取得し、この指示データを、データ送受信部１５を介して認証情報登録部２４に送信する。認証情報登録部２４は、この指示データに応じて、データベース２２に格納されている携帯端末１０の情報レコードに対して、「接続禁止」の情報を設定する。ここでは、認証情報登録部２４は、携帯端末１０の端末ＩＤに「接続禁止」を示す情報を関連付けてデータベース２２に登録する。
（２）ステップＣ２
携帯端末１０を拾得した第三者が、携帯端末１０の電源をＯＮにする、又は、スリープ状態から復帰させるとする。例えば、入力部１１は、第三者による操作に応じて、携帯端末１０の電源をＯＮにする、又は、スリープ状態から復帰させる。

（３）ステップＣ３
携帯端末１０は、自身の位置情報を位置情報取得装置から取得する。このとき、位置情報取得部１４は、携帯端末１０の現在の位置情報を、ＧＰＳシステム等の位置情報取得装置から取得する。
（４）ステップＣ４
データ送受信部１５は、端末ＩＤと取得した位置情報データを、認証チェック部２１に送信する。
（５）ステップＣ５
認証チェック部２１は、受信した端末ＩＤと位置情報がデータベースに登録されているか確認する。また、認証チェック部２１は、該当端末ＩＤが「接続禁止」として登録されているかを確認する。
（６）ステップＣ６
認証チェック部２１は、該当端末が「接続禁止」として登録されている場合、受信した端末ＩＤと位置情報を表示部２３に表示する。
（７）ステップＣ７
認証チェック部２１は、接続禁止を示す認証チェック結果を携帯端末１０に送信する。例えば、認証チェック部２１は、接続禁止を示す認証チェック結果として「ＦＯＲＢＩＤＤＥＮ」を携帯端末１０に送信する。
（８）ステップＣ８
携帯端末１０側で接続禁止の認証チェック結果を受信する。ここでは、データ送受信部１５は、認証チェック部２１から接続禁止を示す認証チェック結果を受信する。
（９）ステップＣ９
データ送受信部１５は、表示部１２に「端末利用不可」のメッセージを出力する。このとき、表示部１２は、「端末利用不可」のメッセージを表示する。但し、実際には、メッセージは文字に限らず、画像、音声、その他の「端末利用不可」を示す通知でも良い。
（１０）ステップＣ１０
パスワードチェック部１３は、ログイン中であれば、強制ログオフ処理を行い、ログオフ状態に遷移する。また、パスワードチェック部１３は、入力部１１からの入力を全て拒否するようにして、携帯端末１０をロック状態（何も操作ができない状態）にする。
（１１）ステップＣ１１
一定時間経過後、位置情報取得部１４は、携帯端末１０の現在の位置情報を取得する。データ送受信部１５は、認証チェック部２１に対して、位置情報取得部１４から取得した携帯端末１０の位置情報の送信を繰り返し行う。表示部２３は、データ送受信部１５から取得した携帯端末１０の位置情報を逐一表示する。

【００５３】
以上の動作により、携帯端末の盗難／紛失が発生した場合に、第三者に対する使用を抑止すると共に、現在の位置情報を検出することができるため、携帯端末を迅速に発見することができる。

【００５４】
例えば、会社から支給された携帯端末を利用する場所は、会社、自宅、会社－自宅間の通勤経路に限定される。従って、データベースに登録する位置情報は、会社であれば、自席や会議室等の限定された場所であり、自宅内でもリビング等に限定された場所となる。通勤経路に関しても、特定の路線の電車内に限定される。

【００５５】
携帯端末の紛失時には、携帯端末を拾得した第三者が近所の交番／駅の落し物窓口等に持参し、そこで携帯端末の操作が行われることになるため、データベースに登録された場所以外で利用されたことが通知される。

【００５６】
盗難時も同様であり、第三者が携帯端末の操作を行うのは、データベースに登録された以外の場所での利用となるため、その位置情報が通知される。よって、携帯端末の位置情

報が分かり、早期に発見することができる。

【００５７】

以下に、本発明の第４実施形態について説明する。

本実施形態では、データベース２２に、簡易パスワードと、通常のパスワードの２種類を用意する。

【００５８】

図９のフローチャートを参照して、本実施形態の動作について説明する。

（１）ステップＤ１

認証に先立ち、位置情報取得部１４は、携帯端末１０の現在の位置情報を、ＧＰＳシステム等の位置情報取得装置から取得する。

（２）ステップＤ２

データ送受信部１５は、携帯端末１０の位置情報を認証チェック部２１に送信する。

（３）ステップＤ３

認証チェック部２１は、データベース２２に登録されている位置情報と、携帯端末１０の位置情報を比較し、距離を算定する。

（４）ステップＤ４

認証チェック部２１は、算出された距離と閾値とを比較し、算出された距離が閾値以下であるか判定する。ここでは、この閾値は、認証チェック部２１又はデータベース２２等に、予め設定されているものとする。但し、実際には、この例に限定されない。例えば、ログインを許可する地域（エリア）を予め設定しておき、携帯端末１０の位置情報がこの地域（エリア）内であるか判定するようにすることも考えられる。この場合、「算出された距離」は、携帯端末１０の現在の位置情報であり、「閾値」は、この地域（エリア）の範囲を示す位置情報である。

（５）ステップＤ５

認証チェック部２１は、算出された距離が閾値以下であれば、使用することを想定された場所にいると判断し、簡易パスワードの入力を求める。このとき、認証チェック部２１は、簡易パスワードの入力のみを求め、通常のパスワードの入力が行われても認証しないようにしても良い。

（６）ステップＤ６

入力部１１は、認証チェック部２１からの簡易パスワードの入力要求に応じて、利用者（ユーザ）により入力された簡易パスワードを取得する。データ送受信部１５は、簡易パスワードを認証チェック部２１に送信する。このとき、データ送受信部１５は、端末ＩＤ、ユーザＩＤ、及び位置情報を、簡易パスワードと共に送信するようにしても良い。

（７）ステップＤ７

認証チェック部２１は、受信した簡易パスワードがデータベース２２に登録されているかを確認する。なお、認証チェック部２１は、簡易パスワードと共に、端末ＩＤ、ユーザＩＤ、及び位置情報を受信した場合、第１実施形態と同様に、受信した端末ＩＤ、ユーザＩＤ、及び位置情報が、データベース２２に登録されているかを確認するようにしても良い。

（８）ステップＤ８

認証チェック部２１は、受信した簡易パスワードがデータベース２２に登録されている場合、携帯端末１０に対して、ログインを許可する。このとき、パスワードチェック部１３は、携帯端末１０の状態をログイン中状態に遷移する。

（９）ステップＤ９

認証チェック部２１は、受信した簡易パスワードがデータベース２２に登録されていない場合、携帯端末１０に対して、ログインを許可しない。すなわち、認証チェック部２１は、携帯端末１０からのログインを拒否する。この場合、携帯端末１０は、認証が必要な機能やサービスを利用できない。このとき、パスワードチェック部１３は、携帯端末１０のログイン処理を中断する。また、表示部１２は、再びパスワード入力画面を表示するようにしても良い。

（１０）ステップＤ１０
また、認証チェック部２１は、算出された距離が閾値を超える場合は、使用することを想定した場所から離れた場所にいると判断し、通常のパスワード入力を求める。
（１１）ステップＤ１１
入力部１１は、認証チェック部２１からの通常のパスワードの入力要求に応じて、利用者（ユーザ）により入力された通常のパスワードを取得する。データ送受信部１５は、通常のパスワードを認証チェック部２１に送信する。このとき、データ送受信部１５は、端末ＩＤ、ユーザＩＤ、及び位置情報を、通常のパスワードと共に送信するようにしても良い。
（１２）ステップＤ１２
認証チェック部２１は、受信した通常のパスワードがデータベース２２に登録されているかを確認する。なお、認証チェック部２１は、通常のパスワードと共に、端末ＩＤ、ユーザＩＤ、及び位置情報を受信した場合、第１実施形態と同様に、受信した端末ＩＤ、ユーザＩＤ、及び位置情報が、データベース２２に登録されているかを確認するようにしても良い。
（１３）ステップＤ１３
認証チェック部２１は、受信した通常のパスワードがデータベース２２に登録されている場合、携帯端末１０に対して、ログインを許可する。このとき、パスワードチェック部１３は、携帯端末１０の状態をログイン中状態に遷移する。この場合、携帯端末１０は、利用可能な機能や、提供されるサービスに制限を受けない。或いは、認証チェック部２１は、通常のパスワードによるログインの場合、携帯端末１０に対して、限定的なログインを許可するようにしても良い。この場合、携帯端末１０は、利用可能な機能や、提供されるサービスが制限されることになる。
（１４）ステップＤ１４
認証チェック部２１は、受信した通常のパスワードがデータベース２２に登録されていない場合、携帯端末１０に対して、ログインを許可しない。すなわち、認証チェック部２１は、携帯端末１０からのログインを拒否する。この場合、携帯端末１０は、認証が必要な機能やサービスを利用できない。このとき、パスワードチェック部１３は、携帯端末１０のログイン処理を中断する。また、表示部１２は、再びパスワード入力画面を表示するようにしても良い。

【００５９】
このとき、例えば、簡易パスワードを「４桁程度の数字」にして、通常のパスワードを「８桁以上の英数字」にすることが考えられる。但し、実際には、この例に限定されない。

【００６０】
本実施形態の場合、先にユーザＩＤを入力させられないため、端末ＩＤと位置情報を関連させて、利用可能情報を登録しておくことになる。

【００６１】
なお、本実施形態において、上記の認証チェック部２１のように、パスワードチェック部１３が簡易パスワードと通常のパスワードの２種類のパスワードチェックを行うようにしても良い。この場合、簡易パスワードと通常のパスワードは、携帯端末１０側に登録されている。

【００６２】
図９のフローチャートに示す本実施形態の動作は、第１実施形態において、携帯端末１０が位置情報を送信する際（図２のステップＡ６以降）に行われるようにしても良い。

【００６３】
以下に、本発明の第５実施形態について説明する。
本実施形態では、予め登録されている位置情報と携帯端末１０の位置情報とを比較し、これらの位置情報の間の距離に応じて、要求するパスワードの文字数を変更する。例えば、認証チェック部２１は、距離が近い場合、認証を簡略化し、パスワードの一部を要求し

て、パスワードの一部が入力されれば通常のサービスを提供する。反対に、距離が遠い場合、認証を厳密化し、パスワードの全文を要求して、パスワードの全文が入力されれば通常のサービス、或いは、利用制限したサービスを提供する。

【００６４】

本実施形態では、第４実施形態と同様に、認証に先立ち、端末ＩＤと位置情報を送信する。また、一定の長さ以上のパスワードを予めサーバ側に格納しておく。パスワードは１種類で良い。

【００６５】

認証チェック部２１は、予め登録されている位置情報と、携帯端末１０から送信された位置情報とを比較し、これらの位置情報の間の距離を算定する。認証チェック部２１は、距離とパスワードを関連付け、携帯端末１０の位置情報が登録されている位置情報から近い場合、例えば登録されたパスワードの先頭の３文字分の入力を求めるようにする。認証チェック部２１は、携帯端末１０の位置情報が登録された位置情報から遠い場合、登録されたパスワードの全文を入力しなければならないようにする。

【００６６】

このとき、認証チェック部２１は、携帯端末１０の位置情報と登録されている位置情報との間の距離が所定の閾値以下であれば、携帯端末１０の位置情報が登録されている位置情報から近いと判断する。また、認証チェック部２１は、携帯端末１０の位置情報と登録されている位置情報との間の距離が所定の閾値より大きい場合、携帯端末１０の位置情報が登録されている位置情報から遠いと判断する。この閾値は、予め設定されていることが好適である。この閾値は、位置情報と共にデータベース２２に登録されていても良い。

【００６７】

図１０のフローチャートを参照して、本実施形態の動作について説明する。

（１）ステップＥ１

認証に先立ち、位置情報取得部１４は、携帯端末１０の現在の位置情報を、ＧＰＳシステム等の位置情報取得装置から取得する。

（２）ステップＥ２

データ送受信部１５は、携帯端末１０の位置情報を認証チェック部２１に送信する。

（３）ステップＥ３

認証チェック部２１は、データベース２２に登録されている位置情報と、携帯端末１０の位置情報を比較し、距離を算定する。データベース２２に登録されている位置情報は、任意に設定することが可能であるとする。例えば、データベース２２に登録されている位置情報は、会社の位置情報や、他の携帯端末の位置情報でも良い。

（４）ステップＥ４

認証チェック部２１は、算出された距離が近いか判定する。なお、算出された距離が近くない場合は、遠いと判断するようにすることが好適である。例えば、認証チェック部２１は、携帯端末１０の位置情報と登録されている位置情報との間の距離が所定の閾値以下であれば、携帯端末１０の位置情報が登録されている位置情報から近いと判断する。この閾値は、位置情報と共にデータベース２２に登録されていても良い。但し、実際には、この例に限定されない。

（５）ステップＥ５

認証チェック部２１は、算出された距離が近い場合、使用することを想定された場所にいると判断し、パスワードの一部の入力を求める。このとき、認証チェック部２１は、パスワードの一部ではなくパスワードの全文の入力が行われても認証するようにしても良い。但し、実際には、この例に限定されない。

（６）ステップＥ６

入力部１１は、認証チェック部２１からのパスワードの一部の入力要求に応じて、利用者（ユーザ）により入力されたパスワードの一部を取得する。データ送受信部１５は、パスワードの一部を認証チェック部２１に送信する。このとき、データ送受信部１５は、端末ＩＤ、ユーザＩＤ、及び位置情報を、パスワードの一部と共に送信するようにしても良

い。

（７）ステップＥ７

認証チェック部２１は、受信したパスワードの一部がデータベース２２に登録されているパスワードの一部と一致するかを確認する。このとき、対象となるパスワードの一部は、パスワードの全文の先頭の３文字分のように、パスワード中の所定の位置の文字列とする。すなわち、受信したパスワードの一部がデータベース２２に登録されているパスワードの全文のうちいずれか適当な部分と一致すれば良いというものではない。従って、認証チェック部２１は、受信したパスワードの一部がデータベース２２に登録されているパスワード中の予め決められた位置の文字列と一致するかを確認する。なお、認証チェック部２１は、パスワードの一部と共に、端末ＩＤ、ユーザＩＤ、及び位置情報を受信した場合、第１実施形態と同様に、受信した端末ＩＤ、ユーザＩＤ、及び位置情報が、データベース２２に登録されているかを確認するようにしても良い。

（８）ステップＥ８

認証チェック部２１は、受信したパスワードの一部がデータベース２２に登録されているパスワードの一部と一致する場合、携帯端末１０に対して、ログインを許可する。このとき、パスワードチェック部１３は、携帯端末１０の状態をログイン中状態に遷移する。

（９）ステップＥ９

認証チェック部２１は、受信したパスワードの一部がデータベース２２に登録されているパスワードの一部と一致しない場合、携帯端末１０に対して、ログインを許可しない。すなわち、認証チェック部２１は、携帯端末１０からのログインを拒否する。この場合、携帯端末１０は、認証が必要な機能やサービスを利用できない。このとき、パスワードチェック部１３は、携帯端末１０のログイン処理を中断する。また、表示部１２は、再びパスワード入力画面を表示するようにしても良い。

（１０）ステップＥ１０

また、認証チェック部２１は、算出された距離が遠い場合は、使用することを想定した場所から離れた場所にいると判断し、パスワードの全文入力を求める。例えば、認証チェック部２１は、携帯端末１０の位置情報と登録されている位置情報との間の距離が所定の閾値より大きい場合、携帯端末１０の位置情報が登録されている位置情報から遠いと判断する。この閾値は、位置情報と共にデータベース２２に登録されていても良い。但し、実際には、この例に限定されない。

（１１）ステップＥ１１

入力部１１は、認証チェック部２１からのパスワードの全文の入力要求に応じて、利用者（ユーザ）により入力されたパスワードの全文を取得する。データ送受信部１５は、パスワードの全文を認証チェック部２１に送信する。このとき、データ送受信部１５は、端末ＩＤ、ユーザＩＤ、及び位置情報を、パスワードの全文と共に送信するようにしても良い。

（１２）ステップＥ１２

認証チェック部２１は、受信したパスワードの全文がデータベース２２に登録されているパスワードの全文と一致するかを確認する。なお、認証チェック部２１は、パスワードの全文と共に、端末ＩＤ、ユーザＩＤ、及び位置情報を受信した場合、第１実施形態と同様に、受信した端末ＩＤ、ユーザＩＤ、及び位置情報が、データベース２２に登録されているかを確認するようにしても良い。

（１３）ステップＥ１３

認証チェック部２１は、受信したパスワードの全文がデータベース２２に登録されているパスワードの全文と一致する場合、携帯端末１０に対して、ログインを許可する。このとき、パスワードチェック部１３は、携帯端末１０の状態をログイン中状態に遷移する。この場合、携帯端末１０は、利用可能な機能や、提供されるサービスに制限を受けない。或いは、認証チェック部２１は、パスワードの全文によるログインの場合、携帯端末１０に対して、限定的なログインを許可するようにしても良い。この場合、携帯端末１０は、利用可能な機能や、提供されるサービスが制限されることになる。

（１４）ステップＥ１４

認証チェック部２１は、受信したパスワードの全文がデータベース２２に登録されていない場合、携帯端末１０に対して、ログインを許可しない。すなわち、認証チェック部２１は、携帯端末１０からのログインを拒否する。この場合、携帯端末１０は、認証が必要な機能やサービスを利用できない。このとき、パスワードチェック部１３は、携帯端末１０のログイン処理を中断する。また、表示部１２は、再びパスワード入力画面を表示するようにしても良い。

【００６８】

本実施形態により、携帯端末１０の現在位置が、携帯端末１０の使用が想定された場所近辺であれば、ユーザＩＤに続けて少ないパスワード文字数でログイン動作が行えるため、ログイン処理を迅速化できる。

【００６９】

逆に、携帯端末１０の現在位置が、携帯端末１０の使用が想定された場所から離れていた場合は、長いパスワード文字数を入力するため、セキュリティの安全性が向上する。

【００７０】

図１０のフローチャートに示す本実施形態の動作は、第１実施形態において、携帯端末１０が位置情報を送信する際（図２のステップＡ６以降）に行われるようにしても良い。

【００７１】

なお、上記の各実施形態は、組み合わせて実施することが可能である。

【００７２】

以上のように、本発明では、携帯端末がＧＰＳシステムや地表高センサ等の位置情報を取得する手段を具備する。例えば、ログイン時にユーザＩＤ及びパスワードに加えて、或いは代わりに、当該携帯端末が具備する位置情報取得装置から取得した位置情報が、サーバのデータベースに登録されているログイン許可位置情報と一致していたときにログインを許可し、利用者のみが知る利用可能位置情報を基に認証してログインさせることで、認証をより強化する。

【００７３】

また、本発明では、携帯端末からサーバに対して位置情報が送信され、その携帯端末に対してログインの許可／拒否を行う。例えば、紛失した／盗難された特定携帯端末に対して予めログイン禁止の情報を登録しておくことで、該携帯端末を利用して第三者によるログイン操作が行われた際に、ログインを拒否し、該携帯端末をロック状態にすることで、不正ログイン操作を抑止することができる。

【００７４】

更に、本発明では、認証時に位置情報を取得するため、サーバ側で携帯端末の現在位置が容易に検索可能となる。例えば、携帯端末の紛失／盗難時に、当該携帯端末を早期に発見できるという利点もある。

【図面の簡単な説明】

【００７５】

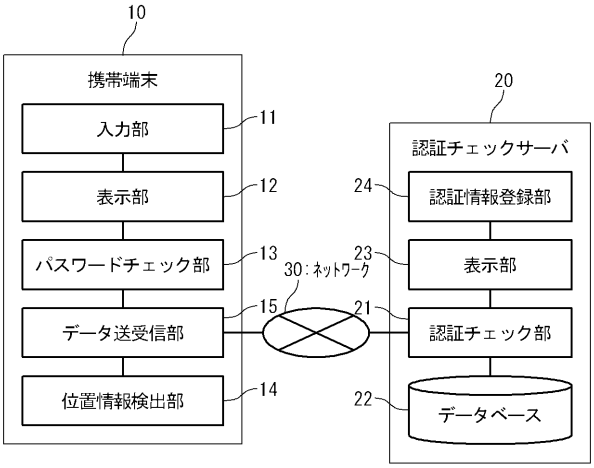
【図１】図１は、本発明の認証チェックシステムの構成例を示すブロック図である。
【図２】図２は、第１実施形態の動作を示すフローチャートである。
【図３】図３は、パスワード入力画面の例を示す図である。
【図４】図４は、データベースに格納されている情報の例を示す図である。
【図５】図５は、表示されるチェック結果（確認結果）の情報の表示例を示す図である。
【図６】図６は、認証成功のメッセージの表示例を示す図である。
【図７】図７は、第２実施形態の動作を示すフローチャートである。
【図８】図８は、第３実施形態の動作を示すフローチャートである。
【図９】図９は、第４実施形態の動作を示すフローチャートである。
【図１０】図１０は、第５実施形態の動作を示すフローチャートである。

【符号の説明】

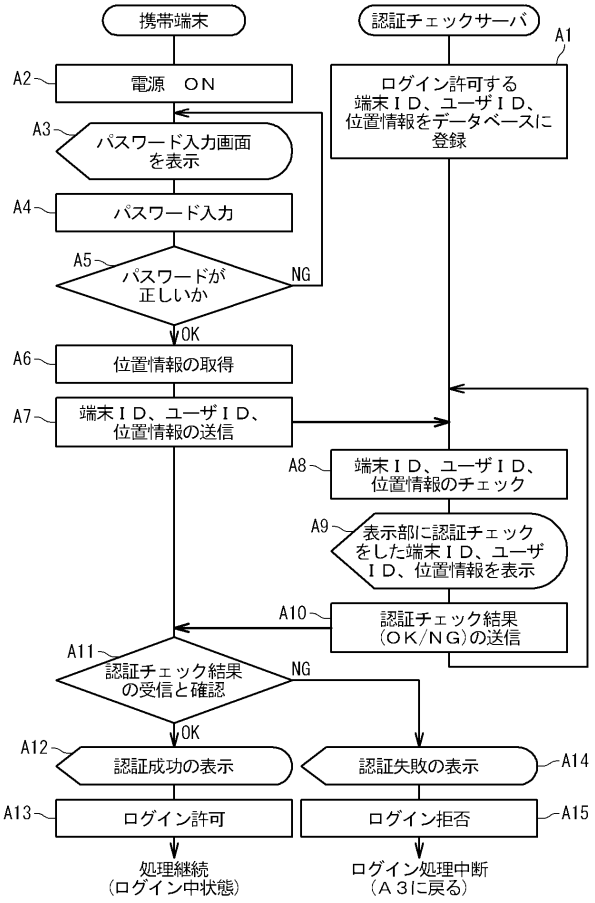
【００７６】

１０…　携帯端末
１１…　入力部
１２…　表示部
１３…　パスワードチェック部
１４…　位置情報取得部
１５…　データ送受信部
２０…　認証チェックサーバ
２１…　認証チェック部
２２…　データベース
２３…　表示部
２４…　認証情報登録部
３０…　ネットワーク

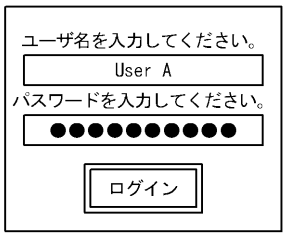
【図１】



【図２】



【図３】



【図４】

データベースの格納情報の例

端末	ユーザ	位置情報（データ）	位置情報（場所）	利用可能
AAAA	User A	X1-Y1-Z1	東京都港区芝1-2-3 ○○ビル ５Ｆ 柱番号 A-1	許可
BBBB	User B	X2-Y2-Z2	東京都港区芝1-2-3 ○○ビル ６Ｆ 柱番号 D-5	許可
CCCC	User C	X3-Y3-Z3	東京都港区芝1-2-3 ○○ビル ２Ｆ 柱番号 A-1	禁止
…	…	…	…	…

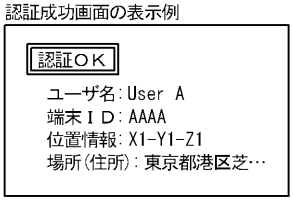
【図５】

認証チェックシステム側の確認結果の表示例

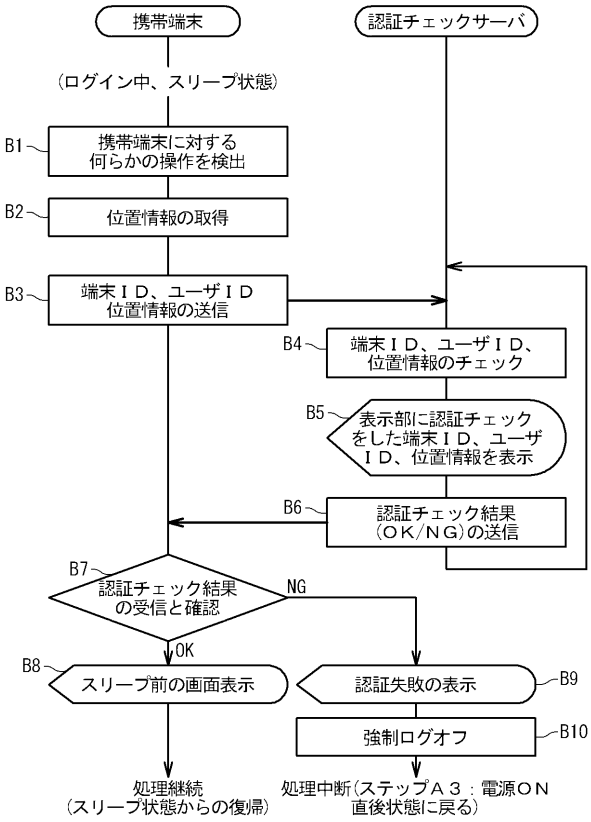
接続状態	接続時刻	端末ID	ユーザID	位置情報
…	…	…	…	…
OK	2007/01/02 12:00:00	AAAA	User A	X1-Y1-Z1
OK	2007/01/02 12:01:00	BBBB	User B	X2-Y2-Z2
NG	2007/01/02 12:02:00	CCCC	User C	X3-Y3-Z3
…	…	…	…	…

【図６】

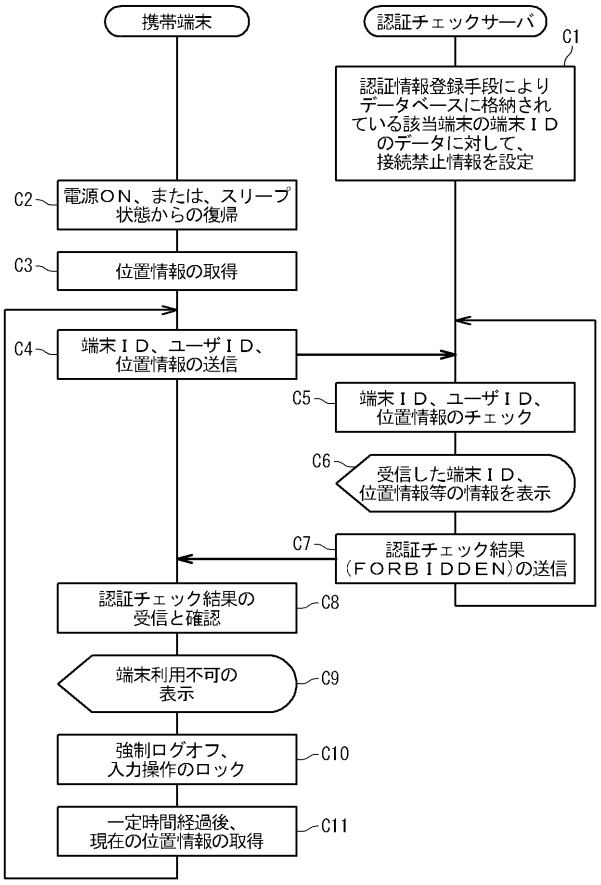
認証成功画面の表示例



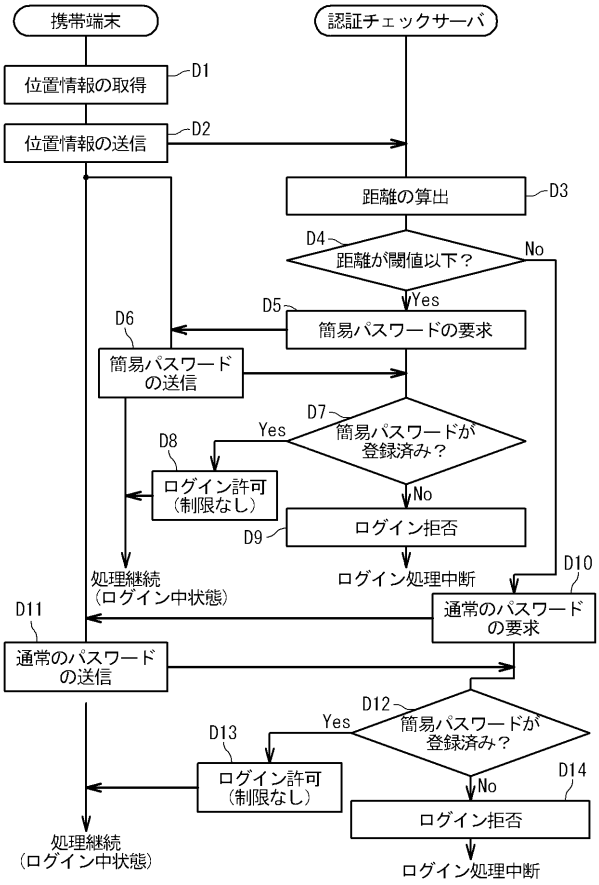
【図７】



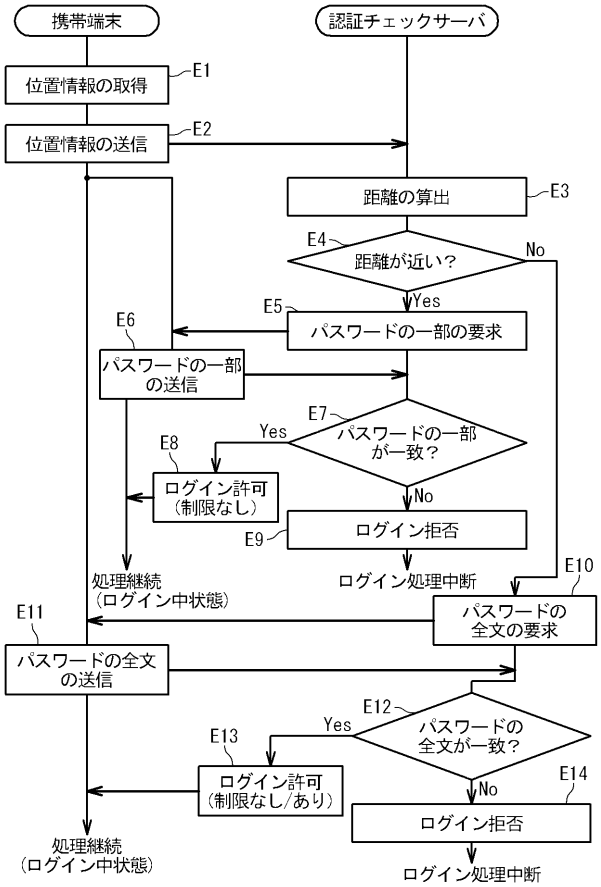
【図８】


携帯端末
認証チェックサーバ
C1
認証情報登録手段により
データベースに格納され
ている該当端末の端末ＩＤ
のデータに対して、
接続禁止情報を設定
C2
電源ＯＮ、または、スリープ
状態からの復帰
C3
位置情報の取得
C4
端末ＩＤ、ユーザＩＤ、
位置情報の送信
C5
端末ＩＤ、ユーザＩＤ、
位置情報のチェック
C6
受信した端末ＩＤ、
位置情報等の情報を表示
C7
認証チェック結果
（ＦＯＲＢＩＤＤＥＮ）の送信
認証チェック結果の
受信と確認
C8
端末利用不可の
表示
C9
強制ログオフ、
入力操作のロック
C10
一定時間経過後、
現在の位置情報の取得
C11

【図９】


携帯端末
認証チェックサーバ
位置情報の取得
D1
位置情報の送信
D2
距離の算出
D3
D4
距離が閾値以下？
No
Yes
D5
簡易パスワードの要求
D6
簡易パスワード
の送信
D7
簡易パスワードが
登録済み？
Yes
D8
ログイン許可
（制限なし）
No
D9
ログイン拒否
ログイン処理中断
処理継続
（ログイン中状態）
D10
通常のパスワード
の要求
D11
通常のパスワード
の送信
D12
簡易パスワードが
登録済み？
Yes
D13
ログイン許可
（制限なし）
No
D14
ログイン拒否
ログイン処理中断
処理継続
（ログイン中状態）

【図１０】


携帯端末
認証チェックサーバ
位置情報の取得
E1
位置情報の送信
E2
距離の算出
E3
E4
距離が近い？
No
Yes
E5
パスワードの一部の要求
E6
パスワードの一部
の送信
E7
パスワードの一部
が一致？
Yes
E8
ログイン許可
（制限なし）
No
E9
ログイン拒否
ログイン処理中断
処理継続
（ログイン中状態）
E10
パスワードの
全文の要求
E11
パスワードの全文
の送信
E12
パスワードの
全文が一致？
Yes
E13
ログイン許可
（制限なし/あり）
No
E14
ログイン拒否
ログイン処理中断
処理継続
（ログイン中状態）