(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5085605号
(P5085605)
(45)発行日　平成24年11月28日(2012.11.28)　(24)登録日　平成24年9月14日(2012.9.14)

(51)Int.Cl.　F I
G06F 21/20 (2006.01)　G06F 21/20 131A

請求項の数 9 (全 14 頁)

(21)出願番号　特願2009-113810(P2009-113810)
(22)出願日　平成21年5月8日(2009.5.8)
(65)公開番号　特開2010-262532(P2010-262532A)
(43)公開日　平成22年11月18日(2010.11.18)
審査請求日　平成22年3月9日(2010.3.9)

(73)特許権者　500257300
ヤフー株式会社
東京都港区赤坂９丁目７番１号
(74)代理人　100064621
弁理士　山川　政樹
(74)代理人　100098394
弁理士　山川　茂樹
(72)発明者　利波　泰史
東京都港区赤坂九丁目７番１号　ヤフー株式会社内
(72)発明者　布施　健太郎
東京都港区赤坂九丁目７番１号　ヤフー株式会社内

最終頁に続く

(54)【発明の名称】ログインを管理するサーバ、方法、およびプログラム

(57)【特許請求の範囲】
【請求項１】
所定のサービスへのユーザのログインを管理するサーバであって、
前記ユーザのユーザＩＤと関連付けて少なくとも１つのメールアドレスを記憶する記憶手段と、
前記ユーザＩＤを用いたログイン要求を受け付けたことに応じて、当該要求のあったことを通知するメッセージおよび当該メッセージを識別するＵＲＬを含んだ通知メールを生成する生成手段と、
前記生成手段により生成された通知メールを、前記記憶手段により記憶されているメールアドレスへ送信する送信手段と、
前記送信手段により送信された通知メールに含まれている前記ＵＲＬへのアクセスと共に、前記ユーザＩＤを用いたログインの抑止指示を受け付ける受付手段と、
前記受付手段によりアクセスを受け付けたことに応じて、前記ＵＲＬに対応するユーザＩＤと照合することにより認証を行う認証手段と、
前記ログインの抑止指示を受け付けた場合に、前記認証手段により認証されたユーザＩＤを用いた前記所定のサービスへのログインを抑止する抑止手段と、を備え、
前記生成手段は、前記抑止手段によるログインの抑止状態を解除するための、前記ユーザＩＤを用いた要求を受け付けたことに応じて、当該要求のあったことを通知するメッセージおよび当該メッセージを識別する前記ＵＲＬを含んだ通知メールを生成し、
前記受付手段は、前記通知メールに含まれている前記ＵＲＬへのアクセスと共に、前記

ユーザＩＤを用いたログインの抑止状態を解除する指示を受け付け、
前記抑止手段は、前記ログインの抑止状態を解除する指示を受け付けた場合に、前記認証手段により認証されたユーザＩＤを用いた前記所定のサービスへのログインの抑止状態を解除する
ことを特徴とするサーバ。
【請求項２】
前記抑止手段は、さらに、前記認証手段により認証されたユーザＩＤを用いたログイン中のセッションを無効化することを特徴とする請求項１に記載のサーバ。
【請求項３】
前記受付手段は、前記ログインの抑止状態を解除する指示を受け付けた場合に、前記ユーザＩＤに関連付けられているパスワードの変更入力をさらに受け付け、
前記抑止手段は、前記受付手段により受け付けたパスワードの変更入力に応じて、前記パスワードを変更することを特徴とする請求項１または２に記載のサーバ。
【請求項４】
前記ログイン要求を受け付けた場合に、前記送信手段により通知メールが送信される前に、当該通知メールの送信先である前記メールアドレスを示す情報を、当該ログイン要求元へ通知する第１の通知手段をさらに備える請求項１から請求項３のいずれかに記載のサーバ。
【請求項５】
前記ログインの抑止状態を解除する要求を受け付けた場合に、前記送信手段により通知メールが送信される前に、当該通知メールの送信先である前記メールアドレスを示す情報を、当該要求元へ通知する第２の通知手段をさらに備える請求項１から請求項４のいずれかに記載のサーバ。
【請求項６】
前記生成手段は、前記通知メールを生成する度に、前記ＵＲＬを都度変更して生成することを特徴とする請求項１から請求項５のいずれかに記載のサーバ。
【請求項７】
前記生成手段は、前記ユーザＩＤが用いられた端末の識別情報を含めて前記メッセージを生成することを特徴とする請求項１から請求項６のいずれかに記載のサーバ。
【請求項８】
所定のサービスへのユーザのログインをコンピュータが管理する方法であって、
前記ユーザのユーザＩＤと関連付けて少なくとも１つのメールアドレスを記憶する記憶ステップと、
前記ユーザＩＤを用いたログイン要求を受け付けたことに応じて、当該要求のあったことを通知するメッセージおよび当該メッセージを識別するＵＲＬを含んだ第１の通知メールを生成する第１の生成ステップと、
前記第１の生成ステップにより生成された前記第１の通知メールを、前記記憶ステップにより記憶されているメールアドレスへ送信する第１の送信ステップと、
前記第１の送信ステップにより送信された前記第１の通知メールに含まれている前記ＵＲＬへのアクセスと共に、前記ユーザＩＤを用いたログインの抑止指示を受け付ける第１の受付ステップと、
前記第１の受付ステップによりアクセスを受け付けたことに応じて、前記ＵＲＬに対応するユーザＩＤと照合することにより認証を行う第１の認証ステップと、
前記ログインの抑止指示を受け付けた場合に、前記第１の認証ステップにより認証されたユーザＩＤを用いた前記所定のサービスへのログインを抑止する抑止ステップと、
前記抑止ステップによるログインの抑止状態を解除するための、前記ユーザＩＤを用いた要求を受け付けたことに応じて、当該要求のあったことを通知するメッセージおよび当該メッセージを識別する前記ＵＲＬを含んだ第２の通知メールを生成する第２の生成ステップと、
前記第２の生成ステップにより生成された前記第２の通知メールを、前記記憶ステップ

により記憶されているメールアドレスへ送信する第２の送信ステップと、
前記第２の通知メールに含まれている前記ＵＲＬへのアクセスと共に、前記ユーザＩＤを用いたログインの抑止状態を解除する指示を受け付ける第２の受付ステップと、
前記第２の受付ステップによりアクセスを受け付けたことに応じて、前記ＵＲＬに対応するユーザＩＤと照合することにより認証を行う第２の認証ステップと、
前記ログインの抑止状態を解除する指示を受け付けた場合に、前記第２の認証ステップにより認証されたユーザＩＤを用いた前記所定のサービスへのログインの抑止状態を解除する解除ステップと
を有することを特徴とする方法。
【請求項９】
請求項８に記載の方法をコンピュータに実行させるプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、所定のサービスへのユーザのログインを管理するサーバ、方法、およびプログラムに関する。
【背景技術】
【０００２】
従来、インターネット上では、ユーザ認証により不特定多数のユーザが利用可能な様々なサービスが提供されている。このようなサービスへログインする際には、各ユーザに固有のＩＤとパスワードにより本人認証を行うことが多い。これにより、各ユーザ用にカスタマイズされたサービスが提供される。
【０００３】
ところが、ＩＤとパスワードによる認証のみでは、本来のユーザ以外の第三者に使用されるおそれもある。そこで、本来のユーザに成りすました不正なログインを防止する対策が検討されている。例えば、特許文献１では、ログインしたユーザの電子メールアドレスを宛先として、ログイン操作が行われたことを通知する電子メールを送信することが提案されている。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２００７－９４６１４号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
しかしながら、特許文献１の方法は、不正なログインを発見するためには有用であるものの、本来のユーザ（本人）がログインを抑止（ロック）するための仕組みが提供されていない。すなわち、不正なログインが発生した場合に、ログインをロックしたりロック解除したりする操作に対して、確実に本人認証を行うことは難しかった。
【０００６】
本発明は、ユーザ本人に不正なログインの発生を容易に気付かせると共に、以降のログインロックの操作に対して、確実に本人認証を行うことができるサーバ、方法、およびプログラムを提供することを目的とする。
【課題を解決するための手段】
【０００７】
本発明では、以下のような解決手段を提供する。
【０００８】
（１）　所定のサービスへのユーザのログインを管理するサーバであって、
前記ユーザのユーザＩＤと関連付けて少なくとも１つのメールアドレスを記憶する記憶手段と、

前記ユーザＩＤを用いたログイン要求を受け付けたことに応じて、当該要求のあったことを通知するメッセージおよび当該メッセージを識別するＵＲＬを含んだ通知メールを生成する生成手段と、
前記生成手段により生成された通知メールを、前記記憶手段により記憶されているメールアドレスへ送信する送信手段と、
前記送信手段により送信された通知メールに含まれている前記ＵＲＬへのアクセスと共に、前記ユーザＩＤを用いたログインの抑止指示を受け付ける受付手段と、
前記受付手段によりアクセスを受け付けたことに応じて、前記ＵＲＬに対応するユーザＩＤと照合することにより認証を行う認証手段と、
前記ログインの抑止指示を受け付けた場合に、前記認証手段により認証されたユーザＩＤを用いた前記所定のサービスへのログインを抑止する抑止手段と、を備えるサーバ。

【０００９】
このような構成によれば、当該サーバは、ログイン要求のあったユーザ本人のメールアドレスに対して、要求のあったことを通知するメッセージを含む通知メールを送信する。ユーザ本人は、この通知メールにより不正なログインの発生を容易に気付くことができる。

【００１０】
また、この通知メールには、通知メッセージを識別するＵＲＬを含むので、通知メールを受信したユーザ本人が、このＵＲＬへアクセスすることにより、ログインロックを実施することができる。このとき、当該サーバが生成したＵＲＬへのアクセスに応じてログインロックの指示を受け付けるため、通知メールを受信していない第三者によりアクセスされる可能性を低減でき、ユーザの本人認証を確実に行うことができる。

【００１１】
（２）　前記抑止手段は、さらに、前記認証手段により認証されたユーザＩＤを用いたログイン中のセッションを無効化することを特徴とする（１）に記載のサーバ。

【００１２】
このような構成によれば、当該サーバは、ログインの抑止指示に応じて、認証されたユーザＩＤを用いた以降のログイン、すなわちサービスの利用開始を抑止し、さらに、認証されたユーザＩＤを用いて現在ログイン中、すなわちサービスを利用中のセッションも無効化する。これにより、ログインロックの設定以降、第三者によるサービスの利用を拒絶することができる。

【００１３】
（３）　前記生成手段は、前記抑止手段によるログインの抑止状態を解除するための、前記ユーザＩＤを用いた要求を受け付けたことに応じて、当該要求のあったことを通知するメッセージおよび当該メッセージを識別する前記ＵＲＬを含んだ通知メールを生成し、
前記受付手段は、前記通知メールに含まれている前記ＵＲＬへのアクセスと共に、前記ユーザＩＤを用いたログインの抑止状態を解除する指示を受け付け、
前記前記抑止手段は、前記ログインの抑止状態を解除する指示を受け付けた場合に、前記認証手段により認証されたユーザＩＤを用いた前記所定のサービスへのログインの抑止状態を解除することを特徴とする（１）または（２）に記載のサーバ。

【００１４】
このような構成によれば、当該サーバは、ログインロックの解除要求を受け付けた場合に、要求されたユーザ本人のメールアドレスに対して、要求のあったことを通知するメッセージを含む通知メールを送信する。ユーザ本人は、この通知メールによりログインロックの解除要求がされたことを容易に気付くことができる。

【００１５】
また、この通知メールには、通知メッセージを識別するＵＲＬを含むので、通知メールを受信したユーザ本人は、実際に解除を行いたい場合には、このＵＲＬへアクセスすることにより、ログインロックの解除を実施することができる。このとき、当該サーバが生成したＵＲＬへのアクセスに応じてログインロックの解除指示を受け付けるため、通知メー

ルを受信していない第三者によりアクセスされる可能性を低減でき、ユーザの本人認証を確実に行うことができる。

【００１６】

（４） 前記受付手段は、前記ログインの抑止状態を解除する指示を受け付けた場合に、前記ユーザＩＤに関連付けられているパスワードの変更入力をさらに受け付け、

前記抑止手段は、前記受付手段により受け付けたパスワードの変更入力に応じて、前記パスワードを変更することを特徴とする（３）に記載のサーバ。

【００１７】

このような構成によれば、当該サーバは、ログインロックを解除する際に、ユーザ認証に用いるパスワードを変更する。したがって、例えば不正なログインの発生によりログインをロックした場合には、このロックを解除した後に再度不正なログインが発生する可能性を低減させることができる。

【００１８】

（５） 前記ログイン要求を受け付けた場合に、前記送信手段により通知メールが送信される前に、当該通知メールの送信先である前記メールアドレスを示す情報を、当該ログイン要求元へ通知する第１の通知手段をさらに備える（１）から（４）のいずれかに記載のサーバ。

【００１９】

このような構成によれば、当該サーバは、本人か第三者かが不明なユーザからのログイン要求があった場合に、本人へメール通知がなされること、さらには通知先のメールアドレスを、この要求元へ通知することができる。したがって、第三者による不正なログインがあった場合には、この通知により、第三者にログインを止めさせる牽制となり得る。

【００２０】

また、本人からの正当なログインである場合にも、この通知により、ユーザは、誤ったメールアドレスが登録されていないかどうかを確認することができる。したがって、本人以外の第三者へメール通知が送信されるのを抑制することができる。

【００２１】

（６） 前記ログインの抑止状態を解除する要求を受け付けた場合に、前記送信手段により通知メールが送信される前に、当該通知メールの送信先である前記メールアドレスを示す情報を、当該要求元へ通知する第２の通知手段をさらに備える（１）から（５）のいずれかに記載のサーバ。

【００２２】

このような構成によれば、当該サーバは、本人か第三者かが不明なユーザからのログインロックの解除要求があった場合に、本人へメール通知がなされること、さらには通知先のメールアドレスを、この要求元へ通知することができる。したがって、第三者による不正なログインロックの解除要求があった場合には、この通知により、第三者に対する牽制となり得る。

【００２３】

また、本人からの正当な解除要求である場合にも、この通知により、ユーザは、誤ったメールアドレスが登録されていないかどうかを確認することができる。したがって、本人以外の第三者へメール通知が送信されるのを抑制することができる。

【００２４】

（７） 前記生成手段は、前記通知メールを生成する度に、前記ＵＲＬを都度変更して生成することを特徴とする（１）から（６）のいずれかに記載のサーバ。

【００２５】

このような構成によれば、当該サーバは、ログインロック指示または解除指示の際にアクセスされるＵＲＬを都度変更して生成するので、送信される通知メール毎に含まれるＵＲＬは異なる。したがって、メール通知を受信した本人以外の第三者にＵＲＬが知られる可能性は大幅に低減するので、より確実に本人認証を行うことができる。

【００２６】

（８） 前記生成手段は、前記ユーザＩＤが用いられた端末の識別情報を含めて前記メッセージを生成することを特徴とする（１）から（７）のいずれかに記載のサーバ。

【００２７】

このような構成によれば、当該サーバは、ログイン要求またはログインロックの解除要求がなされた端末の識別情報を、ユーザ本人に通知することができる。したがって、第三者による要求があった場合には、この要求元を特定する手がかりを得ることができる。

【００２８】

（９） 所定のサービスへのユーザのログインをコンピュータが管理する方法であって、

前記ユーザのユーザＩＤと関連付けて少なくとも１つのメールアドレスを記憶する記憶ステップと、

前記ユーザＩＤを用いたログイン要求を受け付けたことに応じて、当該要求のあったことを通知するメッセージおよび当該メッセージを識別するＵＲＬを含んだ通知メールを生成する生成ステップと、

前記生成ステップにより生成された通知メールを、前記記憶ステップにより記憶されているメールアドレスへ送信する送信ステップと、

前記送信ステップにより送信された通知メールに含まれている前記ＵＲＬへのアクセスと共に、前記ユーザＩＤを用いたログインの抑止指示を受け付ける受付ステップと、

前記受付ステップによりアクセスを受け付けたことに応じて、前記ＵＲＬに対応するユーザＩＤと照合することにより認証を行う認証ステップと、

前記ログインの抑止指示を受け付けた場合に、前記認証ステップにより認証されたユーザＩＤを用いた前記所定のサービスへのログインを抑止する抑止ステップと、を含む方法。

【００２９】

このような構成によれば、当該方法を実行することにより、（１）と同様の効果が期待できる。

【００３０】

（１０） （９）に記載の方法をコンピュータに実行させるプログラム。

【００３１】

このような構成によれば、当該プログラムをコンピュータに実行させることにより、（１）と同様の効果が期待できる。

【発明の効果】

【００３２】

本発明によれば、ユーザ本人に不正なログインの発生を容易に気付かせると共に、以降のログインロックの操作に対して、確実に本人認証を行うことができる。

【図面の簡単な説明】

【００３３】

【図１】本発明の実施形態に係る管理サーバと関連要素とを含んだシステムの全体構成を示す図である。

【図２】本発明の実施形態に係る管理サーバのハードウェア構成を示す図である。

【図３】本発明の実施形態に係る管理サーバの機能構成を示す図である。

【図４】本発明の実施形態に係るログイン管理テーブルを示す図である。

【図５】本発明の実施形態に係る制御部における処理を示すフローチャートである。

【図６】本発明の実施形態に係る管理サーバがロック解除中にログイン要求を受け付けた場合に送信する通知メールの記載例である。

【図７】本発明の実施形態に係る管理サーバがログインロック中にロックの解除要求を受け付けた場合に送信する通知メールの記載例である。

【発明を実施するための形態】

【００３４】

以下、本発明の実施形態の一例について図を参照しながら説明する。

【００３５】
［システム全体構成］
図１は、本実施形態に係る管理サーバ１０と関連要素とを含んだシステムの全体構成を示す図である。このシステムは、管理サーバ１０と、不特定のユーザの端末２０と、所定のサービスの利用登録がされているユーザ本人の端末３０と、を備える。端末２０および端末３０は、インターネット等のネットワークを介して管理サーバ１０と接続されている。
【００３６】
管理サーバ１０は、端末２０からのログイン要求を受け付けると、予め登録されているユーザ本人のメールアドレスへ通知メールを送信し、通知メールを受信した端末３０のユーザ本人へログイン要求があったことを通知する。そして、通知メールに含まれるＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）によりアクセスされたことに応じて、本人のユーザＩＤを用いたログインをロックする。
【００３７】
また、管理サーバ１０は、端末２０からログインロックの解除要求を受け付けると、ログイン要求の場合と同様に通知メールを送信し、通知メールを受信した端末３０のユーザ本人へログインロックの解除要求があったことを通知する。そして、通知メールに含まれるＵＲＬによりアクセスされたことに応じて、本人のユーザＩＤを用いたログインロックを解除する。
【００３８】
なお、本システムでは、ユーザ認証を要するサービスの提供と、本発明に係るログインの管理を、単一の管理サーバ１０で実現する構成として説明するが、本発明の構成はこれには限られない。すなわち、各機能は、複数のサーバに分散されていてもよい。
【００３９】
［ハードウェア構成］
図２は、本実施形態に係る管理サーバ１０のハードウェア構成を示す図である。管理サーバ１０は、制御部３００を構成するＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）３１０（マルチプロセッサ構成ではＣＰＵ３２０等複数のＣＰＵが追加されてもよい）、バスライン２００、通信Ｉ／Ｆ（Ｉ／Ｆ：インタフェース）３３０、メインメモリ３４０、ＢＩＯＳ（Ｂａｓｉｃ　Ｉｎｐｕｔ　Ｏｕｔｐｕｔ　Ｓｙｓｔｅｍ）３５０、Ｉ／Ｏコントローラ３６０、ハードディスク３７０、光ディスクドライブ３８０、並びに半導体メモリ３９０を備える。尚、ハードディスク３７０、光ディスクドライブ３８０、並びに、半導体メモリ３９０はまとめて記憶装置４１０と呼ばれる。
【００４０】
制御部３００は、管理サーバ１０を統括的に制御する部分であり、ハードディスク３７０（後述）に記憶された各種プログラムを適宜読み出して実行することにより、上述したハードウェアと協働し、本発明に係る各種機能を実現している。
【００４１】
通信Ｉ／Ｆ３３０は、管理サーバ１０が、ネットワークを介して図１の端末２０、端末３０や他の情報端末等と情報を送受信する場合のネットワーク・アダプタである。通信Ｉ／Ｆ３３０は、モデム、ケーブル・モデムおよびイーサネット（登録商標）・アダプタを含んでよい。
【００４２】
ＢＩＯＳ３５０は、管理サーバ１０の起動時にＣＰＵ３１０が実行するブートプログラムや、管理サーバ１０のハードウェアに依存するプログラム等を記録する。
【００４３】
Ｉ／Ｏコントローラ３６０には、ハードディスク３７０、光ディスクドライブ３８０、および半導体メモリ３９０等の記憶装置４１０を接続することができる。
【００４４】
ハードディスク３７０は、本ハードウェアを管理サーバ１０として機能させるための各

種プログラムや、本発明の機能を実行するプログラム等を記憶する。なお、管理サーバ１０は、外部に別途設けたハードディスク（図示せず）を外部記憶装置として利用することもできる。

【００４５】

光ディスクドライブ３８０としては、例えば、ＤＶＤ－ＲＯＭドライブ、ＣＤ－ＲＯＭドライブ、ＤＶＤ－ＲＡＭドライブ、ＣＤ－ＲＡＭドライブを使用することができる。この場合は各ドライブに対応した光ディスク４００を使用する。光ディスク４００から光ディスクドライブ３８０によりプログラムまたはデータを読み取り、Ｉ／Ｏコントローラ３６０を介してメインメモリ３４０またはハードディスク３７０に提供することもできる。

【００４６】

なお、本発明でいうコンピュータとは、記憶装置、制御部等を備えた情報処理装置をいい、管理サーバ１０は、記憶装置４１０、制御部３００等を備えた情報処理装置により構成され、この情報処理装置は、本発明のコンピュータの概念に含まれる。

【００４７】

［機能構成］

図３は、本実施形態に係る管理サーバ１０の機能構成を示す図である。管理サーバ１０の制御部３００は、ログイン受付・制御部１１（第１の通知手段、第２の通知手段）と、通知メール生成部１２（生成手段）と、通知メール送信部１３（送信手段）と、ロック・解除制御受付部１４（受付手段）と、本人認証部１５（認証手段）と、ロック・解除制御部１６（抑止手段）と、を備える。また、管理サーバ１０の記憶装置４１０は、ログイン管理ＤＢ１７（記憶手段）を備える。

【００４８】

ログイン受付・制御部１１は、端末２０から、管理サーバ１０にて提供するサービスへのログイン要求を受け付ける。具体的には、ログイン受付・制御部１１は、端末２０から、ユーザＩＤおよびパスワードの入力を受け付け、ログイン管理ＤＢ１７に登録されているユーザ情報と照合することにより、認証を行う。

【００４９】

また、ログインロックが設定されている場合には、ログイン受付・制御部１１は、このログインロックの解除要求を受け付ける。なお、ログインロックの解除要求は、ログイン要求と共通の入力であってよい。この場合、ログイン受付・制御部１１は、現在のログインロックの状態に応じて、ロック中であれば解除要求であると判断する。

【００５０】

さらに、ログイン受付・制御部１１（第１の通知手段）は、ログイン要求を受け付けた場合に、後述の通知メールが送信される前に、この通知メールの送信先であるメールアドレスを示す情報を、ログイン要求元である端末２０へ通知する。また、ログイン受付・制御部１１（第２の通知手段）は、ログインロックの解除要求を受け付けた場合に、同様に通知メールが送信される前に、この通知メールの送信先であるメールアドレスを示す情報を、要求元である端末２０へ通知する。

【００５１】

通知メール生成部１２は、ログイン受付・制御部１１によりログイン要求を受け付けたことに応じて、この要求があったことを通知するメッセージを生成する。また、通知メール生成部１２は、この通知メッセージを識別するＵＲＬ（ワンタイムＵＲＬ）を、ユーザＩＤと関連付けて生成する。そして、通知メール生成部１２は、生成したメッセージとワンタイムＵＲＬとを含んだ通知メールを生成する。

【００５２】

ここで、ワンタイムＵＲＬは、通知メールを生成する度に新たに生成することとしてよい。これにより、通知メールに含まれるＵＲＬは、各々が異なることになるため、この通知メールを受信した端末３０からアクセスされたことが高い可能性で保証される。

【００５３】

図４は、本実施形態に係るログイン管理ＤＢ１７に格納されるログイン管理テーブルを

示す図である。このログイン管理テーブルには、ユーザＩＤに関連付けて、パスワード、ユーザのステータス、メールアドレス、ＵＲＬ、およびロックステータスが記憶されている。

【００５４】

ステータスは、ユーザの現在のステータス、すなわち、ログイン中であるかログアウト中であるかを示す。メールアドレスは、ユーザが受信可能な電子メールアドレスであり、ユーザ本人のみが頻繁に確認可能な、例えば、携帯電話のメールアドレス等であることが好ましい。ＵＲＬは、上述のワンタイムＵＲＬであり、ログインロック指示またはログインロックの解除指示を受け付けるための１度限りの識別コードである。また、ロックステータスは、該当のユーザＩＤによるログインロックの状態として、例えば、ロック受付中、ロック中、解除受付中、解除中、等の区分を示す。

【００５５】

図３に戻って、通知メール送信部１３は、通知メール生成部１２により生成された通知メールを、ログイン管理テーブルに記憶されているメールアドレスを宛先として送信する。送信された通知メールは、端末３０により受信されるので、ログイン受付・制御部１１によりログイン要求を受け付けたことをユーザ本人が認識できる。

【００５６】

ロック・解除制御受付部１４は、通知メールを受信した端末３０から、通知メールに含まれるワンタイムＵＲＬによるアクセスを受け付ける。このアクセスは、ログインロック指示またはログインロックの解除指示を意味している。例えば、ログイン受付・制御部１１でログイン要求を受け付けた場合には、ログイン管理テーブル（図４）のロックステータスはロック受付中となり、通知メールに含まれるワンタイムＵＲＬは、ログインロックを指示するページへのリンクとなる。また、ログイン受付・制御部１１でログインロックの解除要求を受け付けた場合には、ログイン管理テーブル（図４）のロックステータスは解除受付中となり、通知メールに含まれるワンタイムＵＲＬは、ログインロックの解除を指示するページへのリンクとなる。

【００５７】

また、ロック・解除制御受付部１４は、端末３０から、ユーザＩＤとパスワードの入力を受け付ける。ログインロックの解除指示の場合には、パスワード更新用に、さらに新たなパスワードの入力を受け付ける。

【００５８】

本人認証部１５は、ロック・解除制御受付部１４によりアクセスを受け付けたユーザのユーザＩＤの認証を行う。具体的には、本人認証部１５は、ロック・解除制御受付部１４により受け付けたユーザＩＤおよびパスワードを、ログイン管理ＤＢ１７に登録されているユーザ情報と照合することにより、認証を行う。

【００５９】

ロック・解除制御部１６は、本人認証部１５により本人からの指示であることが確認できた場合に、ログインロックまたはログインロックの解除を行う。すなわち、ログイン管理テーブル（図４）のロックステータスがロック中または解除中に変更される。これにより、以降のログイン要求に対する許可／不許可が決定される。なお、ログインロックを実行する場合には、ロック・解除制御部１６は、現在ログイン中のセッションも無効化（切断）し、第三者によるサービスの利用を拒絶する。

【００６０】

また、ロック・解除制御部１６は、ログインロックの解除を行った場合、ロック・解除制御受付部１４により受け付けた新たなパスワードにより、ログイン管理テーブル（図４）のパスワードフィールドを更新する。これにより、旧パスワードで再度ログインされるのを防止することができる。

【００６１】

［処理フロー］

図５は、本実施形態に係る管理サーバ１０の制御部３００における処理を示すフローチ

ャートである。
【００６２】
ステップＳ１では、制御部３００は、端末２０からのログイン要求を受け付け、パスワード認証を行う。なお、ロックステータスがロック中である場合には、このログイン要求は、すなわちログインロックの解除要求である。
【００６３】
また、制御部３００は、パスワード認証に成功すると、ログイン管理テーブル（図４）においてユーザＩＤと関連付けて登録されているメールアドレスへ通知メールが送信されることを端末２０へ通知する。このとき、メールアドレスを端末２０に表示させることが好ましい。
【００６４】
ステップＳ２では、制御部３００は、ステップＳ１で受け付けたログイン要求またはログインロックの解除要求に応じた通知メールを生成する。
【００６５】
ステップＳ３では、制御部３００は、ステップＳ２で生成した通知メールを、ユーザ本人固有のものとして予めログイン管理テーブル（図４）に登録されているメールアドレスを宛先として送信する。
【００６６】
ステップＳ４では、制御部３００は、ログインロックの指示またはログインロックの解除指示を受け付けたか否かを判定する。ワンタイムＵＲＬの所定の有効期間において、通知メールＩＤにて識別されるＵＲＬへのアクセスがあった場合にはＹＥＳと判定し、ステップＳ５に移る。一方、ワンタイムＵＲＬの所定の有効期間において、通知メールＩＤにて識別されるＵＲＬへのアクセスがなかった場合にはＮＯと判定し、ログインロックのステータス変更は行わずに処理を終了する。
【００６７】
ステップＳ５では、制御部３００は、ステップＳ４にてアクセスがあったユーザＩＤのパスワード認証を行う。
【００６８】
ステップＳ６では、制御部３００は、ステップＳ５で認証されたユーザＩＤに関するログインロックまたはログインロックの解除を実施する。また、ログインロックを解除する場合には、制御部３００は、ログイン管理テーブル（図４）に登録されているパスワードを新たなパスワードに更新する。
【００６９】
［通知メールの記載例］
図６および図７は、本実施形態に係る管理サーバ１０が送信する通知メールの記載例を示す図である。
【００７０】
図６は、ロック解除中にログイン要求を受け付けた場合に送信する通知メールの記載例である。
ここでは、通知メールを受信したユーザのユーザＩＤを用いたログイン要求があったことを示すメッセージ４１が記載されている。また、ログインロックを設定するためのワンタイムＵＲＬ４３が記載されている。
【００７１】
さらに、この例では、ログイン情報として、ユーザのＩＤが用いられた端末の識別情報４２が記載されている。具体的には、ユーザのＩＤ、ログイン時間、ＩＰアドレス等が用いられてよい。これにより、本人がログイン操作を行っていないにもかかわらず端末３０で通知メールを受信した場合には、ログイン要求を行った端末２０を特定できる可能性がある。更に、デバイスの種別（ＰＣ、携帯端末等の種別を含んでもよい）、ブラウザの種別（バージョン等も含んでよい）等をログイン情報としてさらに加えてもよい。
【００７２】

図７は、ログインロック中にロックの解除要求を受け付けた場合に送信する通知メールの記載例である。

ここでは、通知メールを受信したユーザのユーザＩＤを用いたロック解除の要求があったことを示すメッセージ５１が記載されている。また、ログインロックの解除設定をするためのワンタイムＵＲＬ５２が記載されている。

【００７３】

なお、図６および図７に示した通知メール中では、ユーザＩＤの一部を伏せておくことが好ましい。これにより、誤って本人以外のユーザがこの通知メールを受信した場合にも、不正にアクセスされる可能性を低減できる。

【００７４】

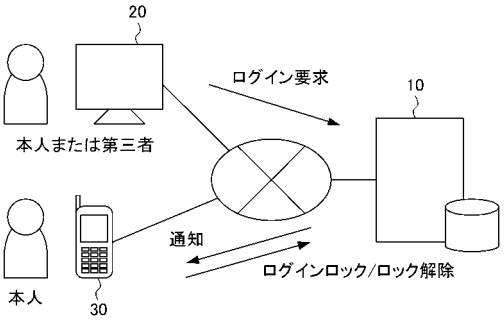
以上、本発明の実施形態について説明したが、本発明は上述した実施形態に限るものではない。また、本発明の実施形態に記載された効果は、本発明から生じる最も好適な効果を列挙したに過ぎず、本発明による効果は、本発明の実施形態に記載されたものに限定されるものではない。

【符号の説明】

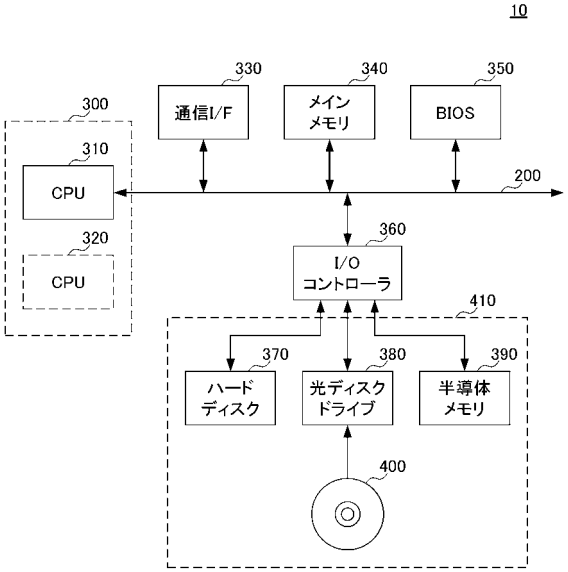
【００７５】

１０　管理サーバ
１１　ログイン受付・制御部
１２　通知メール生成部
１３　通知メール送信部
１４　ロック・解除制御受付部
１５　本人認証部
１６　ロック・解除制御部
１７　ログイン管理ＤＢ
２０、３０　端末
３００　制御部
４１０　記憶装置

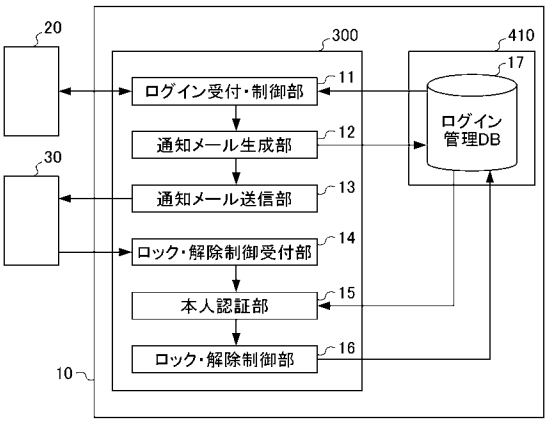
【図１】



【図２】



【図３】

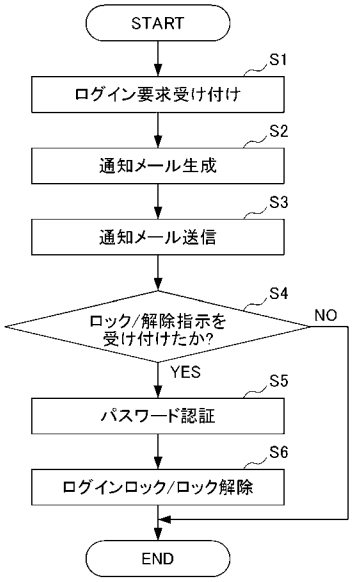


【図４】

ログイン管理テーブル

ユーザID	パスワード	ステータス	メールアドレス	URL	ロックステータス
ab0123	****	ログイン	abab@xxx	http://…/XYZ	ロック受付中
cd1234	****	ログアウト	cdcd@yyy	http://…/ABC	解除受付中
…	…	…	…	…	…

【図５】



【図６】

From: loginalart-master@zzz

Subject: ログインアラート 2008/12/16 18:16:14

Body:

ab0***さん

※このメールはログインアラートに設定されている通知先メールアドレス宛てにお送りしています。このメールに返信する必要はありません。

2008/12/16 18:16:14にログインされました。 41

▼ログイン情報 42
■ID:ab0***
■ログイン時間:2008/12/16 18:16:14
■IPアドレス:212.215.1.2
■デバイス:PC
■ブラウザ:FF3

▼心あたりのないログインの場合は下記のURLをクリックしてください
別のだれかによる不正利用の可能性があるので不正利用を防止するため、ただちにログインロック(ログイン停止)を設定することをおすすめします。

ログインロックを設定する場合は下記よりアクセスしてください。
Http://hogehoge/help/jp/edit/XYZ 43

※リンクの有効期限:2009年2月12日　10時28分です。

【図７】

From: loginalart-master@zzz

Subject: ログインロック解除方法のお知らせ

Body:

cd1***さん

※このメールはログインアラートに設定されている通知先メールアドレス宛てにお送りしています。このメールに返信する必要はありません。

ログインロック解除を続けるためには、以下の手順に従って実施してください。 51

1)ログインロック解除URLにアクセスしてください。

http://hogehoge/help/jp/edit/ABC 52

※リンクの有効期限:2009年2月12日　10時28分です。

2)ログインロック解除画面でIDとパスワードを入力してください。

フロントページの続き

(72)発明者　大塚　康弘
東京都港区赤坂九丁目７番１号　ヤフー株式会社内
(72)発明者　関口　叔子
東京都港区赤坂九丁目７番１号　ヤフー株式会社内
(72)発明者　キーティン　ジョン
東京都港区赤坂九丁目７番１号　ヤフー株式会社内
(72)発明者　伊東　諒
東京都港区赤坂九丁目７番１号　ヤフー株式会社内
(72)発明者　近藤　裕介
東京都港区赤坂九丁目７番１号　ヤフー株式会社内
(72)発明者　鳥谷部　有子
東京都港区赤坂九丁目７番１号　ヤフー株式会社内

審査官　宮司　卓佳

(56)参考文献　特開２００８－１８１３１０（ＪＰ，Ａ）
特開２００５－０２５４２７（ＪＰ，Ａ）
特開２００８－０８５６８１（ＪＰ，Ａ）
特開２００５－２０９０８３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２０