

請求の範囲

- [請求項1] 所定パターンに配列した複数のパターン要素を認証を受けるユーザに提示パターンとして提示したときの特定の位置のパターン要素に対して適用することによりワンタイムパスワードを生成するためのワンタイムパスワード導出ルールを前記ユーザのパスワードとし、前記ワンタイムパスワード内の所定の埋込位置にユーザIDを埋め込んだ認証用文字列に基づいて前記ユーザの認証を行う、認証サーバと認証要求クライアントとを含むユーザ認証システムであって、
- 前記認証サーバは、
- それぞれの前記ユーザID毎に、前記ユーザのユーザIDと、前記ユーザのワンタイムパスワード導出ルールと、前記ユーザIDを前記ワンタイムパスワード内に埋め込む埋込位置を識別するユーザID埋込位置とをお互いに関連付けてあらかじめ記憶するパスワード記憶部と、
- 前記提示パターンを決定する提示パターン決定情報を所定の発生規則により発生する提示パターン決定情報発生手段と、
- それぞれの前記ユーザID毎に、前記提示パターン決定情報に基づいて決定される前記提示パターンを構成する前記パターン要素に前記ユーザIDに関連付けられた前記ワンタイムパスワード導出ルールを適用した結果に対して、前記ユーザIDを前記ユーザID埋込位置に基づいて埋め込んだ検証コードを生成する検証コード生成手段と、
- 発生させられた前記提示パターン決定情報を、前記認証を受けるユーザの前記認証要求クライアントに送信する提示パターン決定情報送信手段と、
- を有し、
- 前記認証要求クライアントは、
- 前記認証サーバから送信された前記提示パターン決定情報を受信する提示パターン決定情報受信手段と、

前記提示パターン決定情報に基づいて前記提示パターンを構成するパターン要素を決定するパターン要素決定手段と、

決定されたそれぞれの前記パターン要素を前記所定パターンに配列して提示パターンを生成し、それを画面に表示させるパターン表示手段と、

前記提示パターンに含まれる前記パターン要素に前記ワンタイムパスワード導出ルールを適用した結果であるワンタイムパスワードに対して、前記ユーザIDを前記ユーザID埋込位置に埋め込んだ認証用文字列の入力を前記認証を受けるユーザから受け付ける認証用文字列入力手段と、

入力された前記認証用文字列を前記認証サーバに送信する認証用文字列送信手段と、

を有し、

前記認証サーバは、

前記認証用文字列を前記認証要求クライアントから受信する認証用文字列受信手段と、

受信した前記認証用文字列と前記ユーザID毎に生成された前記検証コードとを比較し、受信した前記認証用文字列に等しい前記検証コードが存在する場合に、その検証コードに対応する前記ユーザIDの認証を成功させるユーザ認証手段と、

をさらに有することを特徴とするユーザ認証システム。

[請求項2] 前記提示パターン決定情報は、前記提示パターンを構成する前記パターン要素である、請求項1に記載のユーザ認証システム。

[請求項3] 前記提示パターン決定情報は、所定のパターン要素列生成規則に適用することにより前記提示パターンを構成する前記パターン要素を発生するパターンシード値である、請求項1に記載のユーザ認証システム。

[請求項4] 前記検証コード生成手段は、いずれかの2つ以上の前記ユーザID

に対して等しい前記検証コードが存在する場合は、等しい前記検証コードが存在しなくなるまで、前記提示パターン決定情報発生手段によって新しい前記提示パターン決定情報を発生させ、それに基づいてそれぞれの前記ユーザIDに対して前記検証コードを生成することを反復する、請求項1から3のいずれか1項に記載のユーザ認証システム。

[請求項5] 前記認証用文字列送信手段は、入力された前記認証用文字列を記憶するとともに、ハッシュ関数でハッシュ化して前記認証サーバに送信するものであり、

前記ユーザ認証手段は、受信したハッシュ化された前記認証用文字列と、前記ユーザID毎に生成された前記検証コードを前記ハッシュ関数でハッシュ化したものとを比較し、受信したハッシュ化された前記認証用文字列に等しいハッシュ化された前記検証コードが存在する場合に、その検証コードに対応する前記ユーザID埋込位置を前記認証要求クライアントに送信して前記認証用文字列の中の前記ユーザIDの問い合わせを行い、前記問い合わせで得られた前記ユーザIDと前記検証コードに対応する前記ユーザIDが等しい場合に前記ユーザIDの認証を成功させるものであることを特徴とする、請求項4に記載のユーザ認証システム。

[請求項6] 所定パターンに配列した複数のパターン要素を認証を受けるユーザに提示パターンとして提示したときの特定の位置のパターン要素に対して適用することによりワンタイムパスワードを生成するためのワンタイムパスワード導出ルールを前記ユーザのパスワードとし、前記ワンタイムパスワード内の所定の埋込位置にユーザIDを埋め込んだ認証用文字列に基づいて前記ユーザの認証を行う、認証サーバと認証要求クライアントによって実行されるユーザ認証方法であって、

前記認証サーバが、

それぞれの前記ユーザID毎に、前記ユーザのユーザIDと、前記

ユーザのワンタイムパスワード導出ルールと、前記ユーザIDを前記ワンタイムパスワード内に埋め込む埋込位置を識別するユーザID埋込位置とをお互いに関連付けてあらかじめ記憶するステップと、

前記提示パターンを決定する提示パターン決定情報を所定の発生規則により発生するステップと、

それぞれの前記ユーザID毎に、前記提示パターン決定情報に基づいて決定される前記提示パターンを構成する前記パターン要素に前記ユーザIDに関連付けられた前記ワンタイムパスワード導出ルールを適用した結果に対して、前記ユーザIDを前記ユーザID埋込位置に基づいて埋め込んだ検証コードを生成するステップと、

発生させられた前記提示パターン決定情報を、前記認証を受けるユーザの前記認証要求クライアントに送信するステップと、

を有し、

前記認証要求クライアントが、

前記認証サーバから送信された前記提示パターン決定情報を受信するステップと、

受信した前記提示パターン決定情報に基づいて前記提示パターンを構成するパターン要素を決定するステップと、

決定されたそれぞれの前記パターン要素を前記所定パターンに配列して提示パターンを生成し、それを画面に表示させるステップと、

前記提示パターンに含まれる前記パターン要素に前記ワンタイムパスワード導出ルールを適用した結果であるワンタイムパスワードに対して、前記ユーザIDを前記ユーザID埋込位置に埋め込んだ認証用文字列の入力を前記認証を受けるユーザから受け付けるステップと、

入力された前記認証用文字列を前記認証サーバに送信するステップと、

を有し、

前記認証サーバが、

前記認証用文字列を前記認証要求クライアントから受信するステップと、

受信した前記認証用文字列と前記ユーザID毎に生成された前記検証コードとを比較し、受信した前記認証用文字列に等しい前記検証コードが存在する場合に、その検証コードに対応する前記ユーザIDの認証を成功させるステップと、

を有することを特徴とするユーザ認証方法。

[請求項7] 前記提示パターン決定情報は、前記提示パターンを構成する前記パターン要素である、請求項6に記載のユーザ認証方法。

[請求項8] 前記提示パターン決定情報は、所定のパターン要素列生成規則に適用することにより前記提示パターンを構成する前記パターン要素を発生するパターンシード値である、請求項6に記載のユーザ認証方法。

[請求項9] 前記検証コードを生成するステップは、いずれかの2つ以上の前記ユーザIDに対して等しい前記検証コードが存在する場合は、等しい前記検証コードが存在しなくなるまで、前記提示パターン決定情報を発生するステップによって新しい前記提示パターン決定情報を発生させ、それに基づいてそれぞれの前記ユーザIDに対して前記検証コードを生成することを反復する、請求項6から8のいずれか1項に記載のユーザ認証方法。

[請求項10] 入力された前記認証用文字列を前記認証サーバに送信する前記ステップは、入力された前記認証用文字列を記憶するとともに、ハッシュ関数でハッシュ化して前記認証サーバに送信することを含み、

受信した前記認証用文字列と前記ユーザID毎に生成された前記検証コードとを比較し、受信した前記認証用文字列に等しい前記検証コードが存在する場合に、その検証コードに対応する前記ユーザIDの認証を成功させる前記ステップは、受信したハッシュ化された前記認証用文字列と、前記ユーザID毎に生成された前記検証コードを前記ハッシュ関数でハッシュ化したものとを比較し、受信したハッシュ化

された前記認証用文字列に等しいハッシュ化された前記検証コードが存在する場合に、その検証コードに対応する前記ユーザID埋込位置及び前記ユーザIDの文字列の長さを前記認証要求クライアントに送信して前記認証用文字列の中の前記ユーザIDの問い合わせを行い、前記問い合わせで得られた前記ユーザIDと前記検証コードに対応する前記ユーザIDが等しい場合に前記ユーザIDの認証を成功させることを含む、ことを特徴とする、請求項9に記載のユーザ認証方法。

[請求項11]

所定パターンに配列した複数のパターン要素を認証を受けるユーザに提示パターンとして提示したときの特定の位置のパターン要素に対して適用することによりワンタイムパスワードを生成するためのワンタイムパスワード導出ルールを前記ユーザのパスワードとし、前記ワンタイムパスワード内の所定の埋込位置にユーザIDを埋め込んだ認証用文字列に基づいて前記ユーザの認証を行う、認証要求クライアントに接続された認証サーバであって、

それぞれの前記ユーザID毎に、前記ユーザのユーザIDと、前記ユーザのワンタイムパスワード導出ルールと、前記ユーザIDを前記ワンタイムパスワード内に埋め込む埋込位置を識別するユーザID埋込位置とをお互いに関連付けてあらかじめ記憶するパスワード記憶部と、

前記提示パターンを決定する提示パターン決定情報を所定の発生規則により発生する提示パターン決定情報発生手段と、

それぞれの前記ユーザID毎に、前記提示パターン決定情報に基づいて決定される前記提示パターンを構成する前記パターン要素に前記ユーザIDに関連付けられた前記ワンタイムパスワード導出ルールを適用した結果に対して、前記ユーザIDを前記ユーザID埋込位置に基づいて埋め込んだ検証コードを生成する検証コード生成手段と、

発生させられた前記提示パターン決定情報を、前記認証を受けるユーザの前記認証要求クライアントに送信する提示パターン決定情報送

信手段と、

前記認証要求クライアントから送信した、前記提示パターン決定情報に基づいて決定された前記提示パターンに含まれるパターン要素に前記ワンタイムパスワード導出ルールを適用した結果であるワンタイムパスワードに対して、前記ユーザIDを前記ユーザID埋込位置に埋め込んだ認証用文字列を受信する認証用文字列受信手段と、

受信した前記認証用文字列と前記ユーザID毎に生成された前記検証コードとを比較し、受信した前記認証用文字列に等しい前記検証コードが存在する場合に、その検証コードに対応する前記ユーザIDの認証を成功させるユーザ認証手段と、

を有することを特徴とする認証サーバ。

[請求項12]

所定パターンに配列した複数のパターン要素を認証を受けるユーザに提示パターンとして提示したときの特定の位置のパターン要素に対して適用することによりワンタイムパスワードを生成するためのワンタイムパスワード導出ルールを前記ユーザのパスワードとし、前記ワンタイムパスワード内の所定の埋込位置にユーザIDを埋め込んだ認証用文字列に基づいて前記ユーザの認証を行う、認証要求クライアントに接続された認証サーバによって実行されるユーザ認証方法であって、

それぞれの前記ユーザID毎に、前記ユーザのユーザIDと、前記ユーザのワンタイムパスワード導出ルールと、前記ユーザIDを前記ワンタイムパスワード内に埋め込む埋込位置を識別するユーザID埋込位置とをお互いに関連付けてあらかじめ記憶するステップと、

前記提示パターンを決定する提示パターン決定情報を所定の発生規則により発生するステップと、

それぞれの前記ユーザID毎に、前記提示パターン決定情報に基づいて決定される前記提示パターンを構成する前記パターン要素に前記ユーザIDに関連付けられた前記ワンタイムパスワード導出ルールを

適用した結果に対して、前記ユーザIDを前記ユーザID埋込位置に基づいて埋め込んだ検証コードを生成するステップと、

発生させられた前記提示パターン決定情報を、前記認証を受けるユーザの前記認証要求クライアントに送信するステップと、

前記認証要求クライアントから送信した、前記提示パターン決定情報に基づいて決定された前記提示パターンに含まれるパターン要素に前記ワンタイムパスワード導出ルールを適用した結果であるワンタイムパスワードに対して、前記ユーザIDを前記ユーザID埋込位置に埋め込んだ認証用文字列を受信するステップと、

受信した前記認証用文字列と前記ユーザID毎に生成された前記検証コードとを比較し、受信した前記認証用文字列に等しい前記検証コードが存在する場合に、その検証コードに対応する前記ユーザIDの認証を成功させるステップと、

を有することを特徴とするユーザ認証方法。