(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4258551号
(P4258551)

(45)発行日　平成21年4月30日(2009.4.30)　(24)登録日　平成21年2月20日(2009.2.20)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675A
G06F 21/20	(2006.01)	G06F	15/00	330E

請求項の数 9　(全 29 頁)

(21)出願番号　特願2007-14897(P2007-14897)
(22)出願日　平成19年1月25日(2007.1.25)
(65)公開番号　特開2008-182535(P2008-182535A)
(43)公開日　平成20年8月7日(2008.8.7)
審査請求日　平成20年2月13日(2008.2.13)

(73)特許権者　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　100086759
弁理士　渡辺　喜平
(72)発明者　坂本　祐
東京都港区芝五丁目７番１号　日本電気株式会社内

審査官　青木　重徳

最終頁に続く

(54)【発明の名称】認証システム、認証方法、及び認証プログラム

(57)【特許請求の範囲】
【請求項１】
通信回線を介して接続されたクライアント装置及びサーバ装置により、ハッシュアルゴリズムを用いて前記クライアント装置のユーザの認証を行う認証システムであって、
前記クライアント装置が、
ユーザの識別情報及びパスワードを含む認証情報を入力する認証情報入力手段と、
前記サーバ装置から送信されてきた第一のハッシュアルゴリズム識別子に対応する第一のハッシュアルゴリズムを用いて前記認証情報から第一のハッシュ値を生成し、前記第一のハッシュアルゴリズムを用いて前記第一のハッシュ値と前記サーバ装置から送信されてきた乱数から第二のハッシュ値を生成するクライアント側ハッシュ値生成手段と、
前記サーバ装置に認証処理を開始させるための認証要求情報を前記サーバ装置に送信し、前記サーバ装置から前記乱数と前記第一のハッシュアルゴリズム識別子を受信し、前記認証情報入力手段により入力された前記ユーザの識別情報と前記第二のハッシュ値を前記サーバ装置に送信し、前記サーバ装置から認証結果を受信する認証要求管理手段と、を備え、
前記サーバ装置が、
前記ユーザの識別情報ごとに、それぞれ対応する第二のハッシュアルゴリズム識別子と、このハッシュアルゴリズム識別子に対応する第二のハッシュアルゴリズムを用いて前記ユーザの識別情報及び前記パスワードを含む認証情報から予め生成された第三のハッシュ値とを含むユーザ情報を記憶するユーザ情報記憶手段と、

乱数を生成する乱数生成手段と、
ハッシュ値を生成するサーバ側ハッシュ値生成手段と、
前記クライアント装置から前記認証要求情報を受信すると、前記乱数生成手段に乱数を生成させ、前記乱数と前記第一のハッシュアルゴリズム識別子を前記クライアント装置に送信し、前記クライアント装置から前記ユーザの識別情報と前記第二のハッシュ値を受信すると、この受信した前記ユーザの識別情報に対応するユーザ情報を前記ユーザ情報記憶手段から取得し、前記取得したユーザ情報に含まれる前記第二のハッシュアルゴリズム識別子と前記第一のハッシュアルゴリズム識別子とが一致するか否かを判定し、一致する場合、前記サーバ側ハッシュ値生成手段に、前記第一のハッシュアルゴリズムを用いて前記取得したユーザ情報に含まれる第三のハッシュ値と前記乱数から第四のハッシュ値を生成させ、前記第二のハッシュ値と前記第四のハッシュ値とが一致するか否かを判定し、一致する場合、認証成功を示す認証結果を前記クライアント装置に送信し、一致しない場合、認証失敗を示す認証結果を前記クライアント装置に送信する認証情報管理手段と、を備えた
ことを特徴とする認証システム。
【請求項２】
前記サーバ装置における前記認証情報管理手段が、
前記第二のハッシュアルゴリズム識別子と前記第一のハッシュアルゴリズム識別子とが一致しないと判定した場合、前記第二のハッシュアルゴリズム識別子をハッシュアルゴリズム変更要求情報として前記クライアント装置に送信し、
前記クライアント装置における前記認証要求管理手段が、
前記第二のハッシュアルゴリズム識別子を受信すると、前記認証情報入力手段に、前記ユーザの識別情報、パスワード、及び新パスワードを再入力させ、前記クライアント側ハッシュ値生成手段に、前記第二のハッシュアルゴリズムを用いて再入力された前記ユーザの識別情報及び前記パスワードから新しい第三のハッシュ値を生成させるとともに、前記第一のハッシュアルゴリズムを用いて前記新しい第三のハッシュ値と前記乱数から新しい第四のハッシュ値を生成させ、さらに前記第一のハッシュアルゴリズムを用いて再入力された前記ユーザの識別情報及び前記新パスワードから第五のハッシュ値を生成させ、前記ユーザの識別情報、前記新しい第四のハッシュ値、及び前記第五のハッシュ値を前記サーバ装置に送信し、
前記サーバ装置における前記認証情報管理手段が、
前記ユーザの識別情報、前記新しい第四のハッシュ値、及び前記第五のハッシュ値を受信すると、前記サーバ側ハッシュ値生成手段に、前記第一のハッシュアルゴリズムを用いて前記取得したユーザ情報に含まれる第三のハッシュ値と前記乱数から第四のハッシュ値を生成させ、前記第四のハッシュ値と前記新しい第四のハッシュ値とが一致するか否かを判定し、一致する場合、前記ユーザ情報記憶手段における前記ユーザの識別情報に対応する前記第二のハッシュアルゴリズム識別子及び前記第三のハッシュ値を、それぞれ前記第一のハッシュアルゴリズム識別子及び前記第五のハッシュ値に更新して、認証成功を示す認証結果を前記クライアント装置に送信し、一致しない場合、認証失敗を示す認証結果を前記クライアント装置に送信する
ことを特徴とする請求項１記載の認証システム。
【請求項３】
前記クライアント装置が、当該クライアント装置において使用可能なハッシュアルゴリズムの識別子の一覧を記憶するハッシュアルゴリズム識別子記憶手段を備え、
前記サーバ装置が、ハッシュアルゴリズムの識別子ごとに、対応するハッシュアルゴリズムの強度を記憶するハッシュアルゴリズム強度記憶手段を備え、
前記クライアント装置における前記認証要求管理手段が、
前記認証要求情報を前記サーバ装置に送信するにあたり、前記ハッシュアルゴリズムの識別子の一覧を前記サーバ装置に送信し、
前記サーバ装置における前記認証情報管理手段が、

前記クライアント装置から前記認証要求情報と前記ハッシュアルゴリズムの識別子の一覧を受信すると、前記ハッシュアルゴリズム強度記憶手段に記憶されている各ハッシュアルゴリズムの強度にもとづいて、前記ハッシュアルゴリズムの識別子の一覧から最も強度の高いハッシュアルゴリズムの識別子を選択し、この選択した識別子を前記第一のハッシュアルゴリズム識別子として、前記乱数とともに前記クライアント装置に送信する

ことを特徴とする請求項１又は２記載の認証システム。

【請求項４】

通信回線を介して接続されたクライアント装置及びサーバ装置によりハッシュアルゴリズムを用いて、前記クライアント装置のユーザの認証を行う認証方法であって、

前記クライアント装置における認証要求管理手段が、前記サーバ装置に認証処理を開始させるための認証要求情報を前記サーバ装置に送信し、

前記サーバ装置における認証情報管理手段が、前記クライアント装置から前記認証要求情報を受信すると、前記サーバ装置における乱数生成手段に乱数を生成させ、前記乱数と所定の第一のハッシュアルゴリズム識別子を前記クライアント装置に送信し、

前記クライアント装置における前記認証要求管理手段が、前記サーバ装置から前記乱数と前記第一のハッシュアルゴリズム識別子を受信し、

前記クライアント装置における認証情報入力手段が、ユーザの識別情報及びパスワードを含む認証情報を入力し、

前記クライアント装置におけるクライアント側ハッシュ値生成手段が、前記第一のハッシュアルゴリズム識別子に対応する第一のハッシュアルゴリズムを用いて前記認証情報から第一のハッシュ値を生成し、前記第一のハッシュアルゴリズムを用いて前記第一のハッシュ値と前記乱数から第二のハッシュ値を生成し、

前記クライアント装置における前記認証要求管理手段が、前記ユーザの識別情報と前記第二のハッシュ値を前記サーバ装置に送信し、

前記サーバ装置におけるユーザ情報記憶手段が、前記ユーザの識別情報ごとに、それぞれ対応する第二のハッシュアルゴリズム識別子と、このハッシュアルゴリズム識別子に対応する第二のハッシュアルゴリズムを用いて前記ユーザの識別情報及び前記パスワードを含む認証情報から予め生成された第三のハッシュ値とを含むユーザ情報を予め記憶しており、

前記サーバ装置における前記認証情報管理手段が、前記クライアント装置から前記ユーザの識別情報と前記第二のハッシュ値を受信すると、この受信した前記ユーザの識別情報に対応するユーザ情報を前記ユーザ情報記憶手段から取得し、前記取得したユーザ情報に含まれる前記第二のハッシュアルゴリズム識別子と前記第一のハッシュアルゴリズム識別子とが一致するか否かを判定し、一致する場合、前記サーバ装置におけるサーバ側ハッシュ値生成手段に、前記第一のハッシュアルゴリズムを用いて前記取得したユーザ情報に含まれる第三のハッシュ値と前記乱数から第四のハッシュ値を生成させ、前記第二のハッシュ値と前記第四のハッシュ値とが一致するか否かを判定し、一致する場合、認証成功を示す認証結果を前記クライアント装置に送信し、一致しない場合、認証失敗を示す認証結果を前記クライアント装置に送信し、

前記クライアント装置における前記認証要求管理手段が、前記サーバ装置から認証結果を受信する

ことを特徴とする認証方法。

【請求項５】

前記サーバ装置における前記認証情報管理手段が、前記第二のハッシュアルゴリズム識別子と前記第一のハッシュアルゴリズム識別子とが一致しないと判定した場合、前記第二のハッシュアルゴリズム識別子をハッシュアルゴリズム変更要求情報として前記クライアント装置に送信し、

前記クライアント装置における前記認証要求管理手段が、前記第二のハッシュアルゴリズム識別子を受信すると、前記クライアント装置における前記認証情報入力手段に、前記ユーザの識別情報、パスワード、及び新パスワードを再入力させ、前記クライアント装置

における前記クライアント側ハッシュ値生成手段に、前記第二のハッシュアルゴリズムを用いて再入力された前記ユーザの識別情報及び前記パスワードから新しい第三のハッシュ値を生成させるとともに、前記第一のハッシュアルゴリズムを用いて前記新しい第三のハッシュ値と前記乱数から新しい第四のハッシュ値を生成させ、さらに前記第一のハッシュアルゴリズムを用いて再入力された前記ユーザの識別情報及び前記新パスワードから第五のハッシュ値を生成させて、前記ユーザの識別情報、前記新しい第四のハッシュ値、及び前記第五のハッシュ値を前記サーバ装置に送信し、

前記サーバ装置における前記認証情報管理手段が、前記ユーザの識別情報、前記新しい第四のハッシュ値、及び前記第五のハッシュ値を受信すると、前記サーバ装置における前記サーバ側ハッシュ値生成手段に、前記第一のハッシュアルゴリズムを用いて前記取得したユーザ情報に含まれる第三のハッシュ値と前記乱数から第四のハッシュ値を生成させ、前記第四のハッシュ値と前記新しい第四のハッシュ値とが一致するか否かを判定し、一致する場合、前記ユーザ情報記憶手段における前記ユーザの識別情報に対応する前記第二のハッシュアルゴリズム識別子及び前記第三のハッシュ値を、それぞれ前記第一のハッシュアルゴリズム識別子及び前記第五のハッシュ値に更新して、認証成功を示す認証結果を前記クライアント装置に送信し、一致しない場合、認証失敗を示す認証結果を前記クライアント装置に送信する

ことを特徴とする請求項４記載の認証方法。

【請求項６】

前記クライアント装置が、当該クライアント装置において使用可能なハッシュアルゴリズムの識別子の一覧を記憶するハッシュアルゴリズム識別子記憶手段を備えるとともに、前記サーバ装置が、ハッシュアルゴリズムの識別子ごとに、対応するハッシュアルゴリズムの強度を記憶するハッシュアルゴリズム強度記憶手段を備えており、

前記クライアント装置における前記認証要求管理手段が、前記認証要求情報を前記サーバ装置に送信するにあたり、前記ハッシュアルゴリズムの識別子の一覧を前記サーバ装置に送信し、

前記サーバ装置における前記認証情報管理手段が、前記クライアント装置から前記認証要求情報と前記ハッシュアルゴリズムの識別子の一覧を受信すると、前記ハッシュアルゴリズム強度記憶手段に記憶されている各ハッシュアルゴリズムの強度にもとづいて、前記ハッシュアルゴリズムの識別子の一覧から最も強度の高いハッシュアルゴリズムの識別子を選択し、この選択した識別子を前記第一のハッシュアルゴリズム識別子として、前記乱数とともに前記クライアント装置に送信する

ことを特徴とする請求項４又は５記載の認証方法。

【請求項７】

通信回線を介して接続されたクライアント装置及びサーバ装置によりハッシュアルゴリズムを用いて、前記クライアント装置のユーザの認証を行わせる認証プログラムであって、

前記クライアント装置を、

ユーザの識別情報及びパスワードを含む認証情報を入力する認証情報入力手段、

前記サーバ装置から送信されてきた第一のハッシュアルゴリズム識別子に対応する第一のハッシュアルゴリズムを用いて前記認証情報から第一のハッシュ値を生成し、前記第一のハッシュアルゴリズムを用いて前記第一のハッシュ値と前記サーバ装置から送信されてきた乱数から第二のハッシュ値を生成するクライアント側ハッシュ値生成手段、及び、

前記サーバ装置に認証処理を開始させるための認証要求情報を前記サーバ装置に送信し、前記サーバ装置から前記乱数と前記第一のハッシュアルゴリズム識別子を受信し、前記認証情報入力手段により入力された前記ユーザの識別情報と前記第二のハッシュ値を前記サーバ装置に送信し、前記サーバ装置から認証結果を受信する認証要求管理手段として機能させ、

前記サーバ装置を、

前記ユーザの識別情報ごとに、それぞれ対応する第二のハッシュアルゴリズム識別子と

、このハッシュアルゴリズム識別子に対応する第二のハッシュアルゴリズムを用いて前記ユーザの識別情報及び前記パスワードを含む認証情報から予め生成された第三のハッシュ値とを含むユーザ情報を記憶するユーザ情報記憶手段、

乱数を生成する乱数生成手段、

ハッシュ値を生成するサーバ側ハッシュ値生成手段、及び、

前記クライアント装置から前記認証要求情報を受信すると、前記乱数生成手段に乱数を生成させ、前記乱数と所定の第一のハッシュアルゴリズム識別子を前記クライアント装置に送信し、前記クライアント装置から前記ユーザの識別情報と前記第二のハッシュ値を受信すると、この受信した前記ユーザの識別情報に対応する前記ユーザ情報を前記ユーザ情報記憶手段から取得し、取得した前記ユーザ情報に含まれる前記第二のハッシュアルゴリズム識別子と前記第一のハッシュアルゴリズム識別子とが一致するか否かを判定し、一致する場合、前記サーバ側ハッシュ値生成手段に、前記第一のハッシュアルゴリズムを用いて前記取得したユーザ情報に含まれる第三のハッシュ値と前記乱数から第四のハッシュ値を生成させ、前記第二のハッシュ値と前記第四のハッシュ値とが一致するか否かを判定し、一致する場合、認証成功を示す認証結果を前記クライアント装置に送信し、一致しない場合、認証失敗を示す認証結果を前記クライアント装置に送信する認証情報管理手段

として機能させるための認証プログラム。

【請求項８】

前記サーバ装置における前記認証情報管理手段に、

前記第二のハッシュアルゴリズム識別子と前記第一のハッシュアルゴリズム識別子とが一致しないと判定された場合、前記第二のハッシュアルゴリズム識別子をハッシュアルゴリズム変更要求情報として前記クライアント装置に送信させ、

前記クライアント装置における前記認証要求管理手段に、前記第二のハッシュアルゴリズム識別子が受信されると、

前記クライアント装置における前記認証情報入力手段に、前記ユーザの識別情報、パスワード、及び新パスワードを再入力させ、

前記クライアント装置における前記クライアント側ハッシュ値生成手段に、前記第二のハッシュアルゴリズムを用いて再入力された前記ユーザの識別情報及び前記パスワードから新しい第三のハッシュ値を生成させるとともに、前記第一のハッシュアルゴリズムを用いて前記新しい第三のハッシュ値と前記乱数から新しい第四のハッシュ値を生成させ、さらに前記第一のハッシュアルゴリズムを用いて再入力された前記ユーザの識別情報及び前記新パスワードから第五のハッシュ値を生成させ、

前記クライアント装置における前記認証要求管理手段に、前記ユーザの識別情報、前記新しい第四のハッシュ値、及び前記第五のハッシュ値を前記サーバ装置へ送信させ、

前記サーバ装置における前記認証情報管理手段に、前記ユーザの識別情報、前記新しい第四のハッシュ値、及び前記第五のハッシュ値が受信されると、

前記サーバ装置における前記サーバ側ハッシュ値生成手段に、前記第一のハッシュアルゴリズムを用いて前記取得したユーザ情報に含まれる第三のハッシュ値と前記乱数から第四のハッシュ値を生成させ、

前記サーバ装置における前記認証情報管理手段に、前記第四のハッシュ値と前記新しい第四のハッシュ値とが一致するか否かを判定させ、一致する場合、前記ユーザ情報記憶手段における前記ユーザの識別情報に対応する前記第二のハッシュアルゴリズム識別子及び前記第三のハッシュ値を、それぞれ前記第一のハッシュアルゴリズム識別子及び前記第五のハッシュ値に更新させて、認証成功を示す認証結果を前記クライアント装置へ送信させ、一致しない場合、認証失敗を示す認証結果を前記クライアント装置へ送信させる

ことを実行させるための請求項７記載の認証プログラム。

【請求項９】

前記クライアント装置を、当該クライアント装置において使用可能なハッシュアルゴリズムの識別子の一覧を記憶するハッシュアルゴリズム識別子記憶手段として機能させるとともに、

前記サーバ装置を、ハッシュアルゴリズムの識別子ごとに、対応するハッシュアルゴリズムの強度を記憶するハッシュアルゴリズム強度記憶手段として機能させ、
前記クライアント装置における前記認証要求管理手段に、前記認証要求情報を前記サーバ装置へ送信させるにあたり、前記ハッシュアルゴリズムの識別子の一覧を前記サーバ装置へ送信させ、
前記サーバ装置における前記認証情報管理手段に、前記クライアント装置から前記認証要求情報と前記ハッシュアルゴリズムの識別子の一覧が受信されると、前記ハッシュアルゴリズム強度記憶手段に記憶されている各ハッシュアルゴリズムの強度にもとづいて、前記ハッシュアルゴリズムの識別子の一覧から最も強度の高いハッシュアルゴリズムの識別子を選択させ、この選択された識別子を前記第一のハッシュアルゴリズム識別子として、前記乱数とともに前記クライアント装置へ送信させる
ことを実行させるための請求項７又は８記載の認証プログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、認証システムで使用するハッシュアルゴリズムが変更された場合でも継続して利用することが可能な認証システム、認証方法、及び認証プログラムに関する。

【背景技術】

【０００２】

近年、インターネットなどの通信回線を介して、情報処理装置の間で営業秘密や個人情報などの送受信が広く一般に行われており、通信のセキュリティの確保は極めて重要となっている。

このような通信のセキュリティを確保すべく、従来から様々な技術が提案されているが、この中でもユーザ認証に関する技術として近年広く利用されているものに、ハッシュアルゴリズムを用いた認証システムがある。

【０００３】

ハッシュアルゴリズムとは、あるデータの全体を反映した別のデータをハッシュ値として生成するアルゴリズムである。元のデータがわずかでも異なれば、生成されるハッシ値は異なるものとなり、またハッシュ値を元のデータに変換することはできない。このため、万一ハッシュ値が第三者に知られても、元のデータが漏洩することはなく、ハッシュアルゴリズムは認証システムに好適に利用できるものとなっている。

【０００４】

このようなハッシュアルゴリズムを用いた認証システムに関する先行技術としては、以下のものを挙げることができる。

まず、特許文献１には、発生させた乱数をチャレンジデータとして、入力されたユーザＩＤとパスワード、及びチャレンジデータからハッシュ値を生成して認証に利用する認証装置が開示されている。

【０００５】

また、特許文献２には、生体情報データとキー値とからハッシュ値を計算してサーバに登録しておき、生体情報データとキー値を入力し、入力された生体情報データとキー値とからハッシュ値を計算し、登録してあるハッシュ値を計算したハッシュ値とを比較し、等しければ本人であると認証する個人認証システムが開示されている。

【０００６】

また、特許文献３には、利用者端末が指定されたハッシュアルゴリズムによりハッシュ値を計算し、検証装置が指定されたハッシュアルゴリズムにより再計算したハッシュ値と利用者端末から取得したハッシュ値とを比較して正当性を検証する時刻認証システムが開示されている。

【０００７】

しかしながら、これらの認証システムなどでは、使用するハッシュアルゴリズムが変更されると、認証サーバ装置側に記録している認証情報のハッシュ値は逆変換できないこと

から、そのまま認証システムを継続使用することができず、ユーザは再度認証情報を入力して、認証情報のハッシュ値を再作成する必要があるという問題があった。

また、このような場合、ユーザごとに使用するハッシュアルゴリズムを変えることができないため、全ユーザの認証情報をまとめて再作成する必要があり、再作成に相当の時間がかかり、その間認証システムが利用できないという問題があった。

さらに、認証サーバ装置側でハッシュアルゴリズムが変更されると、これに対応する認証クライアント装置側のハッシュアルゴリズムも同時に変更しなければならなかった。

【０００８】

ここで、認証処理におけるアルゴリズムの変更に関しては、例えば特許文献４に記載のコンピュータシステムにおける認証アルゴリズムを更新する方法などが提案されている。

この更新方法では、第１認証アルゴリズムと関連する第１のアカウントと第２認証アルゴリズムと関連する第２のアカウントを記憶手段に格納し、アカウントを切り換えるコマンドが実行されるとアカウントが切り換わり、これと同期して認証アルゴリズムも切り換わる構成となっている。

【０００９】

【特許文献１】特開２０００－０５７０９９号公報
【特許文献２】特開２００４－３１０２０２号公報
【特許文献３】特開２００５－０９４１４６号公報
【特許文献４】特表２００５－５２０４２３号公報

【発明の開示】

【発明が解決しようとする課題】

【００１０】

しかしながら、この更新方法を用いても、認証アルゴリズムとしてハッシュアルゴリズムを使用する認証システムに適用する場合には、ハッシュ値は元のデータに逆変換できないことから、ハッシュアルゴリズムを変更するにあたり、再度認証情報を入力し、切り替える新たなハッシュアルゴリズムを用いて認証のためのハッシュ値を再作成しておく必要があるという問題があった。

【００１１】

本発明は、上記の事情にかんがみなされたものであり、認証システムにおいて、認証クライアント装置と認証サーバ装置間でハッシュアルゴリズム識別子を送受信することにより、認証システムで使用するハッシュアルゴリズムが変更された場合でも継続してその認証システムを利用することが可能な認証システム、認証方法、及び認証プログラムの提供を目的とする。

【課題を解決するための手段】

【００１２】

上記目的を達成するため、本発明の認証システムは、通信回線を介して接続されたクライアント装置及びサーバ装置により、ハッシュアルゴリズムを用いてクライアント装置のユーザの認証を行う認証システムであって、クライアント装置が、ユーザの識別情報及びパスワードを含む認証情報を入力する認証情報入力手段と、サーバ装置から送信されてきた第一のハッシュアルゴリズム識別子に対応する第一のハッシュアルゴリズムを用いて認証情報から第一のハッシュ値を生成し、第一のハッシュアルゴリズムを用いて第一のハッシュ値とサーバ装置から送信されてきた乱数から第二のハッシュ値を生成するクライアント側ハッシュ値生成手段と、サーバ装置に認証処理を開始させるための認証要求情報をサーバ装置に送信し、サーバ装置から乱数と第一のハッシュアルゴリズム識別子を受信し、認証情報入力手段により入力されたユーザの識別情報と第二のハッシュ値をサーバ装置に送信し、サーバ装置から認証結果を受信する認証要求管理手段と、を備え、サーバ装置が、ユーザの識別情報ごとに、それぞれ対応する第二のハッシュアルゴリズム識別子と、このハッシュアルゴリズム識別子に対応する第二のハッシュアルゴリズムを用いてユーザの識別情報及びパスワードを含む認証情報から予め生成された第三のハッシュ値とを含むユーザ情報を記憶するユーザ情報記憶手段と、乱数を生成する乱数生成手段と、ハッシュ値

を生成するサーバ側ハッシュ値生成手段と、クライアント装置から認証要求情報を受信すると、乱数生成手段に乱数を生成させ、乱数と第一のハッシュアルゴリズム識別子をクライアント装置に送信し、クライアント装置からユーザの識別情報と第二のハッシュ値を受信すると、この受信したユーザの識別情報に対応するユーザ情報をユーザ情報記憶手段から取得し、取得したユーザ情報に含まれる第二のハッシュアルゴリズム識別子と第一のハッシュアルゴリズム識別子とが一致するか否かを判定し、一致する場合、サーバ側ハッシュ値生成手段に、第一のハッシュアルゴリズムを用いて取得したユーザ情報に含まれる第三のハッシュ値と乱数から第四のハッシュ値を生成させ、第二のハッシュ値と第四のハッシュ値とが一致するか否かを判定し、一致する場合、認証成功を示す認証結果をクライアント装置に送信し、一致しない場合、認証失敗を示す認証結果をクライアント装置に送信する認証情報管理手段とを備えた構成としてある。

【００１３】

認証システムをこのような構成にすれば、サーバ装置に、クライアント装置の利用者のユーザＩＤごとにハッシュ値とそのハッシュ値の計算に用いられたハッシュアルゴリズムの識別子をユーザ情報として予め記憶させ、クライアント装置からの認証要求に対して所定のハッシュアルゴリズム識別子を送信させ、クライアント装置からハッシュ値とユーザＩＤを受信したときに、当該ユーザＩＤに対応するハッシュアルゴリズムの識別子と、クライアント装置に送信したハッシュアルゴリズム識別子が一致するか否かを判定することができる。

そして、一致していると判定された場合に、サーバ装置で算出したハッシュ値とクライアント装置で算出したハッシュ値を比較することで、認証の成否を判定することができる。

【００１４】

このように、本発明の認証システムでは、クライアント装置とサーバ装置においてハッシュ値の算出にそれぞれ用いられたハッシュアルゴリズムが同一か否かをユーザごとに判定する構成となっており、同一である場合に、ハッシュ値を比較して認証処理を行うことが可能となっている。

このため、認証システムにおいて、認証処理に用いるハッシュアルゴリズムを変更する場合に、その変更を行うタイミングで、サーバ装置における全てのユーザ情報を一度に再作成する必要はなく、ユーザごとに認証処理を行うタイミングで更新することが可能となる。また、サーバ装置側のハッシュアルゴリズムを変更しても、クライアント装置側については、全てのクライアント装置における対応するハッシュアルゴリズムを一度に変更する必要はなく、個々のクライアント装置ごとに段階的に変更することも可能となる。

【００１５】

また、本発明の認証システムは、サーバ装置における認証情報管理手段が、第二のハッシュアルゴリズム識別子と第一のハッシュアルゴリズム識別子とが一致しないと判定した場合、第二のハッシュアルゴリズム識別子をハッシュアルゴリズム変更要求情報としてクライアント装置に送信し、クライアント装置における認証要求管理手段が、第二のハッシュアルゴリズム識別子を受信すると、認証情報入力手段に、ユーザの識別情報、パスワード、及び新パスワードを再入力させ、クライアント側ハッシュ値生成手段に、第二のハッシュアルゴリズムを用いて再入力されたユーザの識別情報及びパスワードから新しい第三のハッシュ値を生成させるとともに、第一のハッシュアルゴリズムを用いて新しい第三のハッシュ値と乱数から新しい第四のハッシュ値を生成させ、さらに第一のハッシュアルゴリズムを用いて再入力されたユーザの識別情報及び新パスワードから第五のハッシュ値を生成させ、ユーザの識別情報、新しい第四のハッシュ値、及び第五のハッシュ値をサーバ装置に送信し、サーバ装置における認証情報管理手段が、ユーザの識別情報、新しい第四のハッシュ値、及び第五のハッシュ値を受信すると、サーバ側ハッシュ値生成手段に、第一のハッシュアルゴリズムを用いて取得したユーザ情報に含まれる第三のハッシュ値と乱数から第四のハッシュ値を生成させ、第四のハッシュ値と新しい第四のハッシュ値とが一致するか否かを判定し、一致する場合、ユーザ情報記憶手段におけるユーザの識別情報に

対応する第二のハッシュアルゴリズム識別子及び第三のハッシュ値を、それぞれ第一のハッシュアルゴリズム識別子及び第五のハッシュ値に更新して、認証成功を示す認証結果をクライアント装置に送信し、一致しない場合、認証失敗を示す認証結果をクライアント装置に送信する構成としてある。

【００１６】

認証システムをこのような構成にすれば、クライアント装置とサーバ装置においてハッシュ値の算出にそれぞれ用いられたハッシュアルゴリズムが同一でない場合には、ユーザごとにハッシュ値の算出に使用するハッシュアルゴリズムを更新することができる。

すなわち、ハッシュアルゴリズムを変更するタイミングでサーバ装置におけるユーザ情報を新規に作成する必要はなく、各ユーザの認証を行うタイミングで、個別にユーザ情報を更新することができる。

このため、本発明の認証システムによれば、使用するハッシュアルゴリズムを変更する必要が生じても、ユーザ情報の作成などのために認証システムの利用を停止することを回避することが可能となっている。

【００１７】

また、本発明の認証システムは、クライアント装置が、当該クライアント装置において使用可能なハッシュアルゴリズムの識別子の一覧を記憶するハッシュアルゴリズム識別子記憶手段を備え、サーバ装置が、ハッシュアルゴリズムの識別子ごとに、対応するハッシュアルゴリズムの強度を記憶するハッシュアルゴリズム強度記憶手段を備え、クライアント装置における認証要求管理手段が、認証要求情報をサーバ装置に送信するにあたり、ハッシュアルゴリズムの識別子の一覧をサーバ装置に送信し、サーバ装置における認証情報管理手段が、クライアント装置から認証要求情報とハッシュアルゴリズムの識別子の一覧を受信すると、ハッシュアルゴリズム強度記憶手段に記憶されている各ハッシュアルゴリズムの強度にもとづいて、ハッシュアルゴリズムの識別子の一覧から最も強度の高いハッシュアルゴリズムの識別子を選択し、この選択した識別子を第一のハッシュアルゴリズム識別子として、乱数とともにクライアント装置に送信する構成としてある。

【００１８】

認証システムをこのような構成にすれば、認証システムにおいて使用するハッシュアルゴリズムを、ユーザごとに、クライアント装置及びサーバ装置において使用可能な最も強度の高いものに自動的に更新することができる。

このため、ハッシュアルゴリズムの脆弱性の発見等によりシステムで使用するハッシュアルゴリズムをさらに強度の高いものに変更する必要が出てきたときなどには、これを容易に認証システムに反映することが可能となっている。

【００１９】

また、本発明の認証方法は、通信回線を介して接続されたクライアント装置及びサーバ装置によりハッシュアルゴリズムを用いて、クライアント装置のユーザの認証を行う認証方法であって、クライアント装置における認証要求管理手段が、サーバ装置に認証処理を開始させるための認証要求情報をサーバ装置に送信し、サーバ装置における認証情報管理手段が、クライアント装置から認証要求情報を受信すると、サーバ装置における乱数生成手段に乱数を生成させ、乱数と所定の第一のハッシュアルゴリズム識別子をクライアント装置に送信し、クライアント装置における認証要求管理手段が、サーバ装置から乱数と第一のハッシュアルゴリズム識別子を受信し、クライアント装置における認証情報入力手段が、ユーザの識別情報及びパスワードを含む認証情報を入力し、クライアント装置におけるクライアント側ハッシュ値生成手段が、第一のハッシュアルゴリズム識別子に対応する第一のハッシュアルゴリズムを用いて認証情報から第一のハッシュ値を生成し、第一のハッシュアルゴリズムを用いて第一のハッシュ値と乱数から第二のハッシュ値を生成し、クライアント装置における認証要求管理手段が、ユーザの識別情報と第二のハッシュ値をサーバ装置に送信し、サーバ装置におけるユーザ情報記憶手段が、ユーザの識別情報ごとに、それぞれ対応する第二のハッシュアルゴリズム識別子と、このハッシュアルゴリズム識別子に対応する第二のハッシュアルゴリズムを用いてユーザの識別情報及びパスワードを

含む認証情報から予め生成された第三のハッシュ値とを含むユーザ情報を予め記憶しており、サーバ装置における認証情報管理手段が、クライアント装置からユーザの識別情報と第二のハッシュ値を受信すると、この受信したユーザの識別情報に対応するユーザ情報をユーザ情報記憶手段から取得し、取得したユーザ情報に含まれる第二のハッシュアルゴリズム識別子と第一のハッシュアルゴリズム識別子とが一致するか否かを判定し、一致する場合、サーバ装置におけるサーバ側ハッシュ値生成手段に、第一のハッシュアルゴリズムを用いて取得したユーザ情報に含まれる第三のハッシュ値と乱数から第四のハッシュ値を生成させ、第二のハッシュ値と第四のハッシュ値とが一致するか否かを判定し、一致する場合、認証成功を示す認証結果をクライアント装置に送信し、一致しない場合、認証失敗を示す認証結果をクライアント装置に送信し、クライアント装置における認証要求管理手段が、サーバ装置から認証結果を受信する方法としてある。

【００２０】

また、本発明の認証方法は、サーバ装置における認証情報管理手段が、第二のハッシュアルゴリズム識別子と第一のハッシュアルゴリズム識別子とが一致しないと判定した場合、第二のハッシュアルゴリズム識別子をハッシュアルゴリズム変更要求情報としてクライアント装置に送信し、クライアント装置における認証要求管理手段が、第二のハッシュアルゴリズム識別子を受信すると、クライアント装置における認証情報入力手段に、ユーザの識別情報、パスワード、及び新パスワードを再入力させ、クライアント装置におけるクライアント側ハッシュ値生成手段に、第二のハッシュアルゴリズムを用いて再入力されたユーザの識別情報及びパスワードから新しい第三のハッシュ値を生成させるとともに、第一のハッシュアルゴリズムを用いて新しい第三のハッシュ値と乱数から新しい第四のハッシュ値を生成させ、さらに第一のハッシュアルゴリズムを用いて再入力されたユーザの識別情報及び新パスワードから第五のハッシュ値を生成させて、ユーザの識別情報、新しい第四のハッシュ値、及び第五のハッシュ値をサーバ装置に送信し、サーバ装置における認証情報管理手段が、ユーザの識別情報、新しい第四のハッシュ値、及び第五のハッシュ値を受信すると、サーバ装置におけるサーバ側ハッシュ値生成手段に、第一のハッシュアルゴリズムを用いて取得したユーザ情報に含まれる第三のハッシュ値と乱数から第四のハッシュ値を生成させ、第四のハッシュ値と新しい第四のハッシュ値とが一致するか否かを判定し、一致する場合、ユーザ情報記憶手段におけるユーザの識別情報に対応する第二のハッシュアルゴリズム識別子及び第三のハッシュ値を、それぞれ第一のハッシュアルゴリズム識別子及び第五のハッシュ値に更新して、認証成功を示す認証結果をクライアント装置に送信し、一致しない場合、認証失敗を示す認証結果をクライアント装置に送信する方法としてある。

【００２１】

また、本発明の認証方法は、クライアント装置が、当該クライアント装置において使用可能なハッシュアルゴリズムの識別子の一覧を記憶するハッシュアルゴリズム識別子記憶手段を備えるとともに、サーバ装置が、ハッシュアルゴリズムの識別子ごとに、対応するハッシュアルゴリズムの強度を記憶するハッシュアルゴリズム強度記憶手段を備えており、クライアント装置における認証要求管理手段が、認証要求情報をサーバ装置に送信するにあたり、ハッシュアルゴリズムの識別子の一覧をサーバ装置に送信し、サーバ装置における認証情報管理手段が、クライアント装置から認証要求情報とハッシュアルゴリズムの識別子の一覧を受信すると、ハッシュアルゴリズム強度記憶手段に記憶されている各ハッシュアルゴリズムの強度にもとづいて、ハッシュアルゴリズムの識別子の一覧から最も強度の高いハッシュアルゴリズムの識別子を選択し、この選択した識別子を第一のハッシュアルゴリズム識別子として、乱数とともにクライアント装置に送信する方法としてある。

【００２２】

認証方法をこのような方法にすれば、認証システムにおいて使用するハッシュアルゴリズムをさらに強度の高いものに変更する場合などに、まずサーバ装置側のハッシュアルゴリズムを変更し、クライアント装置側については、個々のクライアント装置ごとに段階的に変更することが可能となる。

また、ハッシュアルゴリズムを変更するタイミングで、サーバ装置におけるユーザ情報を変更後のハッシュアルゴリズムを用いて事前に作成しておく必要はなく、ユーザの認証を行うタイミングで、個別に最強のハッシュアルゴリズムを用いて更新することができ、ユーザ情報の再作成などのために認証システムの利用を停止することを回避することが可能となっている。

【００２３】

また、本発明の認証プログラムは、通信回線を介して接続されたクライアント装置及びサーバ装置によりハッシュアルゴリズムを用いて、クライアント装置のユーザの認証を行わせる認証プログラムであって、クライアント装置を、ユーザの識別情報及びパスワードを含む認証情報を入力する認証情報入力手段、サーバ装置から送信されてきた第一のハッシュアルゴリズム識別子に対応する第一のハッシュアルゴリズムを用いて認証情報から第一のハッシュ値を生成し、第一のハッシュアルゴリズムを用いて第一のハッシュ値とサーバ装置から送信されてきた乱数から第二のハッシュ値を生成するクライアント側ハッシュ値生成手段、及び、サーバ装置に認証処理を開始させるための認証要求情報をサーバ装置に送信し、サーバ装置から乱数と第一のハッシュアルゴリズム識別子を受信し、認証情報入力手段により入力されたユーザの識別情報と第二のハッシュ値をサーバ装置に送信し、サーバ装置から認証結果を受信する認証要求管理手段として機能させ、サーバ装置を、ユーザの識別情報ごとに、それぞれ対応する第二のハッシュアルゴリズム識別子と、このハッシュアルゴリズム識別子に対応する第二のハッシュアルゴリズムを用いてユーザの識別情報及びパスワードを含む認証情報から予め生成された第三のハッシュ値とを含むユーザ情報を記憶するユーザ情報記憶手段、乱数を生成する乱数生成手段、ハッシュ値を生成するサーバ側ハッシュ値生成手段、及び、クライアント装置から認証要求情報を受信すると、乱数生成手段に乱数を生成させ、乱数と所定の第一のハッシュアルゴリズム識別子をクライアント装置に送信し、クライアント装置からユーザの識別情報と第二のハッシュ値を受信すると、この受信したユーザの識別情報に対応するユーザ情報をユーザ情報記憶手段から取得し、取得したユーザ情報に含まれる第二のハッシュアルゴリズム識別子と第一のハッシュアルゴリズム識別子とが一致するか否かを判定し、一致する場合、サーバ側ハッシュ値生成手段に、第一のハッシュアルゴリズムを用いて取得したユーザ情報に含まれる第三のハッシュ値と乱数から第四のハッシュ値を生成させ、第二のハッシュ値と第四のハッシュ値とが一致するか否かを判定し、一致する場合、認証成功を示す認証結果をクライアント装置に送信し、一致しない場合、認証失敗を示す認証結果をクライアント装置に送信する認証情報管理手段として機能させる構成としてある。

【００２４】

また、本発明の認証プログラムは、サーバ装置における認証情報管理手段に、第二のハッシュアルゴリズム識別子と第一のハッシュアルゴリズム識別子とが一致しないと判定された場合、第二のハッシュアルゴリズム識別子をハッシュアルゴリズム変更要求情報としてクライアント装置に送信させ、クライアント装置における認証要求管理手段に、第二のハッシュアルゴリズム識別子が受信されると、クライアント装置における認証情報入力手段に、ユーザの識別情報、パスワード、及び新パスワードを再入力させ、クライアント装置におけるクライアント側ハッシュ値生成手段に、第二のハッシュアルゴリズムを用いて再入力されたユーザの識別情報及びパスワードから新しい第三のハッシュ値を生成させるとともに、第一のハッシュアルゴリズムを用いて新しい第三のハッシュ値と乱数から新しい第四のハッシュ値を生成させ、さらに第一のハッシュアルゴリズムを用いて再入力されたユーザの識別情報及び新パスワードから第五のハッシュ値を生成させ、クライアント装置における認証要求管理手段に、ユーザの識別情報、新しい第四のハッシュ値、及び第五のハッシュ値をサーバ装置へ送信させ、サーバ装置における認証情報管理手段に、ユーザの識別情報、新しい第四のハッシュ値、及び第五のハッシュ値が受信されると、サーバ装置におけるサーバ側ハッシュ値生成手段に、第一のハッシュアルゴリズムを用いて取得したユーザ情報に含まれる第三のハッシュ値と乱数から第四のハッシュ値を生成させ、サーバ装置における認証情報管理手段に、第四のハッシュ値と新しい第四のハッシュ値とが一

致するか否かを判定させ、一致する場合、ユーザ情報記憶手段におけるユーザの識別情報に対応する第二のハッシュアルゴリズム識別子及び第三のハッシュ値を、それぞれ第一のハッシュアルゴリズム識別子及び第五のハッシュ値に更新させて、認証成功を示す認証結果をクライアント装置へ送信させ、一致しない場合、認証失敗を示す認証結果をクライアント装置へ送信させる構成としてある。

【００２５】

また、本発明の認証プログラムは、クライアント装置を、当該クライアント装置において使用可能なハッシュアルゴリズムの識別子の一覧を記憶するハッシュアルゴリズム識別子記憶手段として機能させるとともに、サーバ装置を、ハッシュアルゴリズムの識別子ごとに、対応するハッシュアルゴリズムの強度を記憶するハッシュアルゴリズム強度記憶手段として機能させ、クライアント装置における認証要求管理手段に、認証要求情報をサーバ装置へ送信させるにあたり、ハッシュアルゴリズムの識別子の一覧をサーバ装置へ送信させ、サーバ装置における認証情報管理手段に、クライアント装置から認証要求情報とハッシュアルゴリズムの識別子の一覧が受信されると、ハッシュアルゴリズム強度記憶手段に記憶されている各ハッシュアルゴリズムの強度にもとづいて、ハッシュアルゴリズムの識別子の一覧から最も強度の高いハッシュアルゴリズムの識別子を選択させ、この選択された識別子を第一のハッシュアルゴリズム識別子として、乱数とともにクライアント装置へ送信させる構成としてある。

【００２６】

認証プログラムをこのような構成にすれば、認証システムにおいて使用するハッシュアルゴリズムをさらに強度の高いものに変更する場合などに、各装置におけるハッシュアルゴリズムの変更を段階的に行うことが可能となる。

また、ハッシュアルゴリズムを変更するタイミングで、変更後のハッシュアルゴリズムを用いてユーザ情報をサーバ装置に事前に作成しておく必要はなく、ユーザの認証を行うタイミングで、ユーザ情報を個別に最強のハッシュアルゴリズムを用いて更新させることができるため、ユーザ情報の再作成などのために認証システムの利用を停止することを回避することが可能となっている。

【発明の効果】

【００２７】

本発明によれば、ハッシュアルゴリズムの脆弱性の発見等によりシステムで使用するハッシュアルゴリズムをさらに強度の高いものに変更する必要が出てきたときなどに、まず認証サーバ装置側のハッシュアルゴリズムを変更し、認証クライアント装置側については、全ての認証クライアント装置の対応するハッシュアルゴリズムを一気に変更しなくても、個々の認証クライアント装置ごとに段階的に変更することが可能となる。

また、ハッシュアルゴリズムを変更するタイミングで、ハッシュ値を含むユーザ情報を一度に新規に作成する必要がなく、各ユーザの認証を行うタイミングで個別にユーザ情報を更新することが可能となる。

【発明を実施するための最良の形態】

【００２８】

以下、本発明に係る認証システムの好ましい実施形態について、図面を参照しつつ説明する。

なお、以下の実施形態に示す本発明の認証システムは、プログラムに制御されたコンピュータにより動作するようになっている。コンピュータのＣＰＵは、プログラムにもとづいてコンピュータの各構成要素に指令を送り、認証クライアント装置及び認証サーバ装置の動作に必要となる所定の処理、例えば、所定のハッシュアルゴリズムを用いてユーザＩＤとパスワードなどからハッシュ値を生成する処理、認証クライアント装置及び認証サーバ装置でそれぞれ生成されたハッシュ値を比較する処理等を行わせる。このように、本発明の認証システムにおける各処理，動作は、プログラムとコンピュータとが協働した具体的手段により実現できるものである。

【００２９】

プログラムは予めＲＯＭ，ＲＡＭ等の記録媒体に格納され、コンピュータに実装された記録媒体から当該コンピュータにプログラムを読み込ませて実行されるが、例えば通信回線を介してコンピュータに読み込ませることもできる。

また、プログラムを格納する記録媒体は、例えば半導体メモリ，磁気ディスク，光ディスク、その他任意のコンピュータで読取り可能な任意の記録手段により構成できる。

【００３０】

まず、本発明の一実施形態の構成について、図１～図４を参照して説明する。図１は、本実施形態の認証システムの構成を示すブロック図である。図２は、同認証システムにおけるハッシュアルゴリズムリスト１４を示す図である。図３は、同認証システムにおけるハッシュアルゴリズム強度テーブル２３を示す図である。図４は、同認証システムにおけるユーザ情報管理テーブル２４を示す図である。

図１に示すように、本実施形態の認証システムは、ユーザＩＤとパスワードの組み合わせによって認証するシステムであり、認証クライアント装置１０と認証サーバ装置２０を有している。

【００３１】

認証クライアント装置１０は、ユーザからの認証要求、認証情報の入力の受付、認証サーバ装置２０への認証要求、ユーザへの認証結果の通知等を行う機能を備えており、図１に示すように、認証情報入力部１１、認証要求管理部１２、クライアント通信部１３、ハッシュアルゴリズムリスト１４、及びハッシュ値生成部１５を備えている。

【００３２】

認証情報入力部１１は、認証要求管理部１２からの要求にもとづいてユーザによる認証情報の入力を受け付ける機能、入力された認証情報を認証要求管理部１２に渡す機能を有する。

すなわち、認証情報入力部１１は、認証要求管理部１２から認証情報の入力要求情報を入力すると、ユーザに認証情報の入力を促すための認証情報入力画面などを認証クライアント装置１０における図示しない表示手段などに出力して、ユーザの操作により認証情報を入力する。そして、この入力された認証情報を認証要求管理部１２に出力する。なお、入力要求情報とは、トリガとなる情報であり、情報の内容としては任意のものを用いることができる。以下の各種要求情報についても同様であるが、その後の処理において用いられる情報、例えばハッシュアルゴリズム識別子等を要求情報として用いることも勿論可能である。

【００３３】

認証要求管理部１２は、ユーザからの認証要求にもとづきハッシュアルゴリズムリスト１４からハッシュアルゴリズム識別子の一覧を取得してクライアント通信部１３に渡す機能、クライアント通信部１３からチャレンジ（乱数と最高強度ハッシュアルゴリズム識別子）を取得すると、認証情報入力部１１に認証情報受付要求を行う機能、認証情報入力部１１から認証情報（ユーザＩＤとパスワード）を取得すると、最高強度ハッシュアルゴリズム識別子やユーザＩＤ、パスワード等をハッシュ値生成部１５に渡し、ハッシュ値生成部１５から生成されたハッシュ値を取得する機能、ハッシュ値をクライアント通信部１３に渡し、クライアント通信部１３からハッシュアルゴリズム変更要求や認証結果を取得し、認証結果をユーザに通知する機能を有する。

【００３４】

すなわち、認証要求管理部１２は、ユーザの操作により図示しない入力手段から認証要求情報を入力すると、ハッシュアルゴリズムリスト１４からハッシュアルゴリズム識別子の一覧を取得し、取得したハッシュアルゴリズム識別子の一覧をクライアント通信部１３に出力する。

また、認証要求管理部１２は、クライアント通信部１３からチャレンジ（乱数と最高強度ハッシュアルゴリズム識別子）を入力すると、認証情報入力部１１に認証情報受付要求情報を出力する。

【００３５】

さらに、認証要求管理部１２は、認証情報入力部１１から認証情報（ユーザＩＤとパスワード）を入力すると、最高強度ハッシュアルゴリズム識別子やユーザＩＤ、パスワード等をハッシュ値生成部１５に出力する。そして、ハッシュ値生成部１５から生成されたハッシュ値を入力する。

また、認証要求管理部１２は、ハッシュ値をクライアント通信部１３に出力して、クライアント通信部１３からハッシュアルゴリズム変更要求や認証結果を取入力し、入力した認証結果をユーザに参照可能とするため、認証クライアント装置１０における図示しない表示手段や印刷手段等に出力する。

これらの認証要求管理部１２により実行される各処理の詳細については、図６ａ及び図６ｂを用いて後述する。

【００３６】

クライアント通信部１３は、認証要求管理部１２から取得した情報をサーバ通信部２１に送信する機能、サーバ通信部２１から受信した情報を認証要求管理部１２に渡す機能を有する。

すなわち、クライアント通信部１３は、認証要求管理部１２から入力した各種情報を通信回線を介してサーバ通信部２１に送信する。また、サーバ通信部２１から通信回線を介して送信されてきた各種情報を受信すると、この受信した情報を認証要求管理部１２に出力する。

【００３７】

ハッシュアルゴリズムリスト１４は、認証クライアント装置１０のハッシュ値生成部１５で使用可能なハッシュアルゴリズムの識別子の一覧を記憶する記憶手段である。このハッシュアルゴリズムリスト１４に記憶されるハッシュアルゴリズム識別子の一覧のデータ構造は、例えば図２に示すようなものとすることができる。同図の例では、認証クライアント装置１０のハッシュ値生成部１５により使用可能なハッシュアルゴリズムとして、ＭＤ４、ＭＤ５、ＳＨＡ－１、ＳＨＡ－２５６等の識別子がそれぞれ記憶されている。

【００３８】

ハッシュ値生成部１５は、認証要求管理部１２から取得した情報を元にハッシュ値を生成する機能、生成したハッシュ値を認証要求管理部１２に渡す機能を有する。

すなわち、ハッシュ値生成部１５は、認証要求管理部１２から一定のハッシュアルゴリズム識別子と、ハッシュ値を生成するための元となる情報を入力すると、この入力した元となる情報を用いて、入力したハッシュアルゴリズム識別子に対応するハッシュアルゴリズム（例えば、ＭＤ４、ＳＨＡ－１等）により、ハッシュ値を生成する。そして、生成したハッシュ値を認証要求管理部１２に出力する。

【００３９】

認証サーバ装置２０は、認証クライアント装置１０からの認証要求に対して認証処理を実行し、その結果を認証クライアント装置１０に返却する機能を備えており、図１に示すように、サーバ通信部２１、認証情報管理部２２、ハッシュアルゴリズム強度テーブル２３、ユーザ情報管理テーブル２４、乱数生成部２５、及びハッシュ値生成部２６を有している。

【００４０】

サーバ通信部２１は、クライアント通信部１３から受信した情報を認証情報管理部２２に渡す機能、認証情報管理部２２から取得した情報をクライアント通信部１３に送信する機能を有する。

すなわち、サーバ通信部２１は、クライアント通信部１３から通信回線を介して送信されてきた各種情報を受信すると、この受信した情報を認証情報管理部２２に出力する。また、認証情報管理部２２から入力した各種情報を通信回線を介してクライアント通信部１３に送信する。

【００４１】

認証情報管理部２２は、サーバ通信部２１から認証要求とハッシュアルゴリズム識別子の一覧を取得すると、ハッシュアルゴリズム強度テーブル２３から各ハッシュアルゴリズ

ムの強度を取得し、ハッシュアルゴリズム識別子の一覧における最強のハッシュアルゴリズムを選択する機能、乱数生成部２５から乱数を取得する機能、チャレンジ（最高強度ハッシュアルゴリズム識別子と乱数）をサーバ通信部２１に渡し、サーバ通信部２１からユーザＩＤとハッシュ値を取得する機能、ユーザ情報管理テーブル２４から指定されたユーザＩＤに対応するユーザ情報を取得する機能、最高強度ハッシュアルゴリズム識別子や乱数、サーバ通信部２１から入力したハッシュ値等をハッシュ値生成部１５に渡し、ハッシュ値生成部１５から生成されたハッシュ値を取得する機能、ハッシュ値生成部１５により生成されたハッシュ値とサーバ通信部２１から入力したハッシュ値を比較して認証の成否を判定する機能、ユーザ情報管理テーブル２４に対してユーザＩＤに対応する最高強度ハッシュアルゴリズム識別子とハッシュ値を更新する機能を有している。

【００４２】

すなわち、認証情報管理部２２は、サーバ通信部２１から認証要求情報とハッシュアルゴリズム識別子の一覧を入力すると、ハッシュアルゴリズム強度テーブル２３から各ハッシュアルゴリズムの強度を取得する。このとき、ハッシュアルゴリズム強度テーブル２３に記憶されている全てのハッシュアルゴリズム識別子に対応する強度を取得する他、サーバ通信部２１から入力したハッシュアルゴリズム識別子の一覧におけるハッシュアルゴリズム識別子に対応する強度のみを取得することもできる。そして、認証情報管理部２２は、ハッシュアルゴリズム識別子の一覧のうち、最高の強度を備えたハッシュアルゴリズムの識別子（最高強度ハッシュアルゴリズム識別子）を選択する。

【００４３】

また、認証情報管理部２２は、最高強度ハッシュアルゴリズム識別子を選択すると、乱数生成部２５に乱数発生要求を行い、乱数生成部２５から乱数を入力する。

また、認証情報管理部２２は、乱数生成部２５から乱数を入力すると、この乱数と最高強度ハッシュアルゴリズム識別子をチャレンジとしてサーバ通信部２１に出力し、サーバ通信部２１からユーザＩＤとハッシュ値を入力する。

さらに、認証情報管理部２２は、サーバ通信部２１から入力したユーザＩＤにもとづいて、このユーザＩＤに対応するユーザ情報をユーザ情報管理テーブル２４から取得する。

【００４４】

また、認証情報管理部２２は、最高強度ハッシュアルゴリズム識別子や乱数、サーバ通信部２１から入力したハッシュ値等をハッシュ値生成部２６に出力し、ハッシュ値生成部２６から当該ハッシュ値生成部２６により生成されたハッシュ値を入力する。

また、認証情報管理部２２は、ハッシュ値生成部２６により生成されたハッシュ値とサーバ通信部２１から入力したハッシュ値を比較し、これらが一致すれば認証成功とし、一致しなければ認証失敗と判定し、この判定結果をサーバ通信部２１に出力する。

【００４５】

さらに、認証情報管理部２２は、一定の場合に、ユーザ情報管理テーブル２４に対してユーザＩＤに対応するハッシュアルゴリズム識別子とハッシュ値を更新する。

以上の認証情報管理部２２により実行される各処理の詳細については、図９ａ及び図９ｂを用いて後述する。

【００４６】

ハッシュアルゴリズム強度テーブル２３は、認証サーバ装置２０のハッシュ値生成部２６で使用可能なハッシュアルゴリズムの識別子の一覧と、それぞれのハッシュアルゴリズムの強度を記憶する記憶手段である。このハッシュアルゴリズム強度テーブル２３のデータ構造は、例えば図３に示すようなものとすることができる。同図では、ハッシュアルゴリズムＭＤ４，ＭＤ５，ＳＨＡ－１，ＳＨＡ－２５６を示す各識別子に対応付けて、それぞれの強度が１，１，２，３であることが示されている。

【００４７】

ユーザ情報管理テーブル２４は、ユーザ情報として、ユーザＩＤごとに、ユーザＩＤとパスワードから生成したハッシュ値と、その際に使用したハッシュアルゴリズムの識別子を記憶する記憶手段であり、本実施形態の認証システムにおける認証処理の実行に先立っ

て、これらの情報を予め記憶している。このユーザ情報管理テーブル２４は、例えば図４に示すようなものとすることができる。

【００４８】

乱数生成部２５は、認証情報管理部２２からの要求にもとづき乱数を生成し、生成した乱数を認証情報管理部２２に渡す機能を有する。

すなわち、乱数生成部２５は、認証情報管理部２２から乱数生成要求情報を入力すると、所定の計算方法により乱数を生成し、生成した乱数を認証情報管理部２２に出力する。このときに乱数生成部２５が用いる計算方法としては、乱数を生成できる限り任意のものとすることができる。

【００４９】

ハッシュ値生成部２６は、認証情報管理部２２から入力した情報にもとづきハッシュ値を生成する機能、生成したハッシュ値を認証情報管理部２２に渡す機能を有する。

すなわち、ハッシュ値生成部２６は、認証情報管理部２２から所定のハッシュアルゴリズム識別子と、ハッシュ値生成の元になる情報を入力すると、この入力した元になる情報を用いて、入力したハッシュアルゴリズム識別子に対応するハッシュアルゴリズムによりハッシュ値を生成し、生成したハッシュ値を認証情報管理部２２に出力する。

【００５０】

次に、本実施形態の認証システムにおける処理手順について、図５～図１３を参照して説明する。図５は、本実施形態の認証システムにおける変数の定義を示す図である。図６ａ、図６ｂは、それぞれ同認証システムにおける認証要求管理部１２による処理手順（ａ）、（ｂ）を示すフローチャートである。図７は、同認証システムにおけるクライアント通信部１３による処理手順を示すフローチャートである。図８は、同認証システムにおけるサーバ通信部２１による処理手順を示すフローチャートである。図９ａ、図９ｂは、それぞれ同認証システムにおける認証情報管理部２２による処理手順（ａ）、（ｂ）を示すフローチャートである。図１０は、同認証システムにおける乱数生成部２５による処理手順を示すフローチャートである。図１１は、同認証システムにおける認証情報入力部１１による処理手順を示すフローチャートである。図１２は、同認証システムにおける認証クライアント装置のハッシュ値生成部１５による処理手順を示すフローチャートである。図１３は、同認証システムにおける認証サーバ装置のハッシュ値生成部２６による処理手順を示すフローチャートである。

【００５１】

まず、図５を参照して、本実施形態の認証システムにおいて認証クライアント装置及び認証サーバ装置間で送受信される変数について説明する。

rand1は、乱数生成部２５により生成された乱数を示す変数である。以下、乱数と称する場合がある。

sHash_alg_idは、認証クライアント装置１０と認証サーバ装置２０で共に使用可能なハッシュアルゴリズムの中で、最も強度の高いハッシュアルゴリズムの識別子を示す変数である。以下、最高強度ハッシュアルゴリズム識別子と称する場合がある。

【００５２】

uidは、ユーザの操作により認証情報入力部１１に入力されたユーザＩＤを示す変数である。以下、ユーザＩＤと称する場合がある。

passwdは、ユーザの操作により認証情報入力部１１に入力されたパスワードを示す変数である。以下、パスワードと称する場合がある。

uid_passwd_sHashVは、uidとpasswdをハッシュ値を計算するための元になる情報として用い、sHash_alg_idが示すハッシュアルゴリズムに従って生成したハッシュ値を示す変数である。以下、第一のハッシュ値と称する場合がある。

【００５３】

uid_passwd_sHashV_rand1_sHashVは、uid_passwd_sHashVとrand1をハッシュ値を計算するための元になる情報として用い、sHash_alg_idが示すハッシュアルゴリズムに従って生成したハッシュ値を示す変数である。以下、第二のハッシュ値と称する場合がある。

uHash_alg_idは、ユーザ情報管理テーブル２４において、uidごとに記憶されているユーザ情報におけるハッシュアルゴリズム識別子を示す変数である。以下、ユーザＩＤ対応ハッシュアルゴリズム識別子と称する場合がある。

【００５４】

uid_passwd_uHashVは、uidとpasswdをハッシュ値を計算するための元になる情報として用い、uHash_alg_idが示すハッシュアルゴリズムに従って生成したハッシュ値を示す変数である。以下、第三のハッシュ値と称する場合がある。

uid_passwd_uHashV_rand1_sHashVは、uid_passwd_uHashVとrand1をハッシュ値を計算するための元になる情報として用い、sHash_alg_idが示すハッシュアルゴリズムに従って生成したハッシュ値を示す変数である。以下、第四のハッシュ値と称する場合がある。

【００５５】

Npasswdは、ユーザが入力した新しいパスワードを示す変数である。以下、新パスワードと称する場合がある。

uid_Npasswd_sHashVは、uidとNpasswdをハッシュ値を計算するための元になる情報として用い、sHash_alg_idが示すハッシュアルゴリズムに従って生成したハッシュ値を示す変数である。以下、第五のハッシュ値と称する場合がある。

【００５６】

＜処理手順Ａ：認証クライアント装置及び認証サーバ装置共通の最強ハッシュアルゴリズムとユーザ情報におけるハッシュ値の生成に使用されたハッシュアルゴリズムが同一である場合＞

次に、認証クライアント装置１０及び認証サーバ装置２０に共通の最強ハッシュアルゴリズムと、ユーザ情報管理テーブル２４に記憶されているハッシュ値の生成に使用されたハッシュアルゴリズムが同一である場合の認証システムにおける処理手順について、図６ａ～図１３のフローチャートを用いて説明する。

【００５７】

まず、ユーザが認証クライアント装置１０を使用して、認証サーバ装置２０に認証要求を行う場合、ユーザは図示しない入力手段を操作して、認証クライアント装置１０に認証要求情報を入力する。

認証要求管理部１２は、図６ａに示すように、認証クライアント装置１０に認証要求情報が入力されるかを監視し、認証要求情報が入力された場合（ステップ１０のＹｅｓ）、ハッシュアルゴリズムリスト１４からハッシュアルゴリズム識別子の一覧を取得する（ステップ１１）。

【００５８】

そして、認証要求管理部１２は、認証要求情報と、取得したハッシュアルゴリズム識別子の一覧をクライアント通信部１３に出力する（ステップ１２）。

なお、認証要求情報は、認証クライアント装置１０において認証を実行するためのトリガの役割を果たすものであり、その構成は特に限定されるものではなく任意の情報とすることが可能である。

【００５９】

次に、クライアント通信部１３は、図７に示すように、認証要求管理部１２から認証要求情報とハッシュアルゴリズム識別子の一覧を入力すると（ステップ３０のＹｅｓ）、これらの情報をサーバ通信部２１に送信する（ステップ３１）。

次に、サーバ通信部２１は、図８に示すように、クライアント通信部１３から認証要求情報とハッシュアルゴリズム識別子の一覧を受信すると（ステップ４０のＮｏ，ステップ４２のＹｅｓ）、これらの情報を認証情報管理部２２に出力する（ステップ４３）。

【００６０】

次に、認証情報管理部２２は、図９ａに示すように、サーバ通信部２１から認証要求情報とハッシュアルゴリズム識別子の一覧を入力すると（ステップ５０のＹｅｓ）、ハッシュアルゴリズム強度テーブル２３から各ハッシュアルゴリズムの強度を取得する（ステップ５１）。

そして、ハッシュアルゴリズム強度テーブル２３から取得した各ハッシュアルゴリズムごとの強度と、ハッシュアルゴリズム識別子の一覧にもとづいて、ハッシュアルゴリズム識別子の一覧に識別子が存在するハッシュアルゴリズムのうち、最も強度の高いハッシュアルゴリズムの識別子（sHash_alg_id：最高強度ハッシュアルゴリズム識別子）を選択する（ステップ５２）。

【００６１】

なお、ハッシュアルゴリズム識別子の一覧に存在する識別子が、ハッシュアルゴリズム強度テーブル２３に存在しておらず、認証クライアント装置１０と認証サーバ装置２０間で共通して使用できるハッシュアルゴリズムがない場合、認証情報管理部２２は、サーバ通信部２１及びクライアント通信部１３を介して、認証クライアント装置１０における認証要求管理部１２に接続拒否の応答情報を返すことなどの処理を行うことができる。

【００６２】

さらに、認証情報管理部２２は、乱数生成部２５に乱数生成要求情報を出力して、乱数生成部２５から乱数（rand1）を取得する（ステップ５３）。

このとき、乱数生成部２５は、図１０に示すように、認証情報管理部２２から乱数生成要求情報を入力すると（ステップ７０のＹｅｓ）、乱数（rand1）を生成し、生成した乱数を認証情報管理部２２に出力する（ステップ７１）。

なお、このとき用いる乱数の生成方法は、特に限定されるものではなく、任意の好適なものを用いることができる。

【００６３】

次に、認証情報管理部２２は、図９ａに示すように、取得した乱数（rand1）と最高強度ハッシュアルゴリズム識別子（sHash_alg_id）をチャレンジとして、サーバ通信部２１に出力する（ステップ５４）。

サーバ通信部２１は、図８に示すように、認証情報管理部２２から乱数（rand1）と最高強度ハッシュアルゴリズム識別子（sHash_alg_id）を入力すると（ステップ４０のＹｅｓ）、これらの情報をクライアント通信部１３に送信する（ステップ４１）。

【００６４】

クライアント通信部１３は、図７に示すように、サーバ通信部２１から乱数（rand1）と最高強度ハッシュアルゴリズム識別子（sHash_alg_id）を受信すると（ステップ３０のＮｏ，ステップ３２のＹｅｓ）、これらの情報を認証要求管理部１２に出力する（ステップ３３）。

【００６５】

認証要求管理部１２は、図６ａに示すように、クライアント通信部１３からチャレンジ（乱数と最高強度ハッシュアルゴリズム識別子）を入力すると（ステップ１３のＹｅｓ）、認証情報入力部１１に認証情報入力受付要求情報を出力する（ステップ１４）。

認証情報入力部１１は、図１１に示すように、認証要求管理部１２から認証情報入力受付要求情報を入力すると（ステップ８０のＹｅｓ）、認証情報の入力受付を行う（ステップ８１）。

【００６６】

その詳細な方法は特に限定されないが、例えば認証クライアント装置１０における図示しない表示手段に、ユーザの操作によって例えばユーザＩＤ（uid）及びパスワード（passwd）などの認証情報を入力するための入力領域を設けた画面を表示させ、当該画面を介して認証情報を入力させることができる。

そして、認証情報（uidとpasswd）の入力が完了すると（ステップ８２のＹｅｓ）、この認証情報を認証要求管理部１２に出力する（ステップ８３）。

【００６７】

次に、認証要求管理部１２は、図６ａに示すように、認証情報入力部１１から認証情報（uidとpasswd）を入力すると（ステップ１５のＹｅｓ）、この認証情報（uidとpasswd）と、最高強度ハッシュアルゴリズム識別子（sHash_alg_id）をハッシュ値生成部１５に出力し、ハッシュ値生成部１５から第一のハッシュ値（uid_passwd_sHashV）を入力する（

ステップ１６）。

【００６８】

このとき、ハッシュ値生成部１５は、図１２に示すように、認証要求管理部１２からハッシュ値生成要求情報として、最高強度ハッシュアルゴリズム識別子（sHash_alg_id）と、入力となる情報、すなわちハッシュ値生成のための計算要素となる入力情報として認証情報（uidとpasswd）を入力すると（ステップ９０のＹｅｓ）、この入力した識別子に対応するハッシュアルゴリズムにより、認証情報（uidとpasswd）を用いて第一のハッシュ値（uid_passwd_sHashV）を生成し、生成した第一のハッシュ値を認証要求管理部１２に出力する（ステップ９１）。

【００６９】

次に、認証要求管理部１２は、図６ａに示すように、最高強度ハッシュアルゴリズム識別子（sHash_alg_id）と、ハッシュ値生成の入力情報としての第一のハッシュ値（uid_passwd_sHashV）と乱数（rand1）をハッシュ値生成部１５に出力し、ハッシュ値生成部１５から第二のハッシュ値（uid_passwd_sHashV_rand1_sHashV）を入力する（ステップ１７）。

【００７０】

このとき、ハッシュ値生成部１５は、図１２に示すように、認証要求管理部１２からハッシュ値生成要求情報として、最高強度ハッシュアルゴリズム識別子（sHash_alg_id）と、ハッシュ値生成のための入力情報として乱数（rand1）と第一のハッシュ値（uid_passwd_sHashV）を入力すると（ステップ９０のＹｅｓ）、この入力した識別子に対応するハッシュアルゴリズムにより、乱数（rand1）と第一のハッシュ値（uid_passwd_sHashV）を用いて第二のハッシュ値（uid_passwd_sHashV_rand1_sHashV）を生成し、生成した第二のハッシュ値を認証要求管理部１２に出力する（ステップ９１）。

【００７１】

次に、認証要求管理部１２は、ユーザＩＤ（uid）と第二のハッシュ値（uid_passwd_sHashV_rand1_sHashV）をクライアント通信部１３に出力する（ステップ１８）。

クライアント通信部１３は、図７に示すように、認証要求管理部１２からユーザＩＤ（uid）と第二のハッシュ値（uid_passwd_sHashV_rand1_sHashV）を入力すると（ステップ３０のＹｅｓ）、これらの情報をサーバ通信部２１に送信する（ステップ３１）。

【００７２】

サーバ通信部２１は、図８に示すように、クライアント通信部１３からユーザＩＤ（uid）と第二のハッシュ値（uid_passwd_sHashV_rand1_sHashV）を受信すると（ステップ４０のＮｏ，ステップ４２のＹｅｓ）、これらの情報を認証情報管理部２２に出力する（ステップ４３）。

【００７３】

次に、認証情報管理部２２は、図９ａに示すように、サーバ通信部２１からユーザＩＤ（uid）と第二のハッシュ値（uid_passwd_sHashV_rand1_sHashV）を入力すると（ステップ５５のＹｅｓ）、ユーザ情報管理テーブル２４からユーザＩＤ（uid）に対応するユーザ情報を抽出して取得する（ステップ５６）。このユーザ情報には、図４を参照して説明したように、ユーザＩＤと予め生成された第三のハッシュ値とユーザＩＤ対応ハッシュアルゴリズム識別子（uHash_alg_id）が含まれている。

なお、ユーザ情報管理テーブル２４に、ユーザＩＤ（uid）に対応するユーザ情報が存在しない場合は、認証情報管理部２２はサーバ通信部２１及びクライアント通信部１３を介して認証要求管理部１２に認証失敗の認証結果を返すなどの処理を行うことができる。

【００７４】

次に、認証情報管理部２２は、最高強度ハッシュアルゴリズムの識別子（sHash_alg_id）とユーザＩＤ対応ハッシュアルゴリズム識別子（uHash_alg_id）を比較して、一致するか否かを判定する（ステップ５７）。

これらの識別子が一致する場合（ステップ５７のＹｅｓ）、認証情報管理部２２は、最高強度ハッシュアルゴリズムの識別子（sHash_alg_id）と、ハッシュ値生成のための入力情報としてユーザ情報における第三のハッシュ値（uid_passwd_uHashV）と乱数（rand1）

をハッシュ値生成部２６に出力し、ハッシュ値生成部２６から第四のハッシュ値（uid_passwd_uHashV_rand1_sHashV）を入力する（ステップ５８）。

【００７５】

このとき、ハッシュ値生成部２６は、図１３に示すように、認証情報管理部２２からハッシュ値生成要求情報として、最高強度ハッシュアルゴリズム識別子（sHash_alg_id）と、ハッシュ値生成のための入力情報として第三のハッシュ値（uid_passwd_uHashV）と乱数（rand1）を入力すると（ステップ１００のＹｅｓ）、この入力した識別子に対応するハッシュアルゴリズムにより、第三のハッシュ値（uid_passwd_uHashV）と乱数（rand1）を用いて第四のハッシュ値（uid_passwd_uHashV_rand1_sHashV）を生成し、生成した第四のハッシュ値を認証情報管理部２２に出力する（ステップ１０１）。

【００７６】

次に、認証情報管理部２２は、ハッシュ値生成部２６から入力した第四のハッシュ値（uid_passwd_uHashV_rand1_sHashV）と、第二のハッシュ値（uid_passwd_sHashV_rand1_sHashV）を比較して、一致するか否かを判定する（ステップ５９）。

そして、これらのハッシュ値が一致する場合、認証情報管理部２２は、認証結果として認証成功をサーバ通信部２１に出力する（ステップ６０）。

一方、これらのハッシュ値が一致しない場合、認証情報管理部２２は、認証結果として認証失敗をサーバ通信部２１に出力する（ステップ６１）。

【００７７】

そして、サーバ通信部２１は、この認証結果をクライアント通信部１３に送信し（図８のステップ４０のＹｅｓ，ステップ４１）、クライアント通信部１３は、サーバ通信部２１から受信した認証結果を認証要求管理部１２に出力する（図７のステップ３０のＮｏ，ステップ３２のＹｅｓ，ステップ３３）。

そして、認証要求管理部１２は、クライアント通信部１３から認証結果を入力すると（ステップ１９のＮｏ，ステップ２０のＹｅｓ）、例えば認証クライアント装置１０における図示しない表示手段に認証結果を出力することで、ユーザに認証結果を通知する（ステップ２１）。

【００７８】

＜処理手順Ｂ：認証クライアント装置及び認証サーバ装置共通の最強ハッシュアルゴリズムとユーザ情報におけるハッシュ値の生成に使用されたハッシュアルゴリズムが異なる場合＞

次に、認証クライアント装置１０及び認証サーバ装置２０に共通の最強ハッシュアルゴリズムと、ユーザ情報管理テーブル２４に記憶されているハッシュ値の生成に使用されたハッシュアルゴリズムが異なる場合の認証システムにおける処理手順について、図６ａ～図１３のフローチャートを用いて説明する。

【００７９】

まず、認証要求管理部１２が、認証クライアント装置１０に認証要求情報が入力された場合（図６ａのステップ１０のＹｅｓ）、ハッシュアルゴリズムリスト１４からハッシュアルゴリズム識別子の一覧を取得する動作（図６ａのステップ１１）から、認証情報管理部２２が、最高強度ハッシュアルゴリズムの識別子（sHash_alg_id）とユーザＩＤ対応ハッシュアルゴリズム識別子（uHash_alg_id）を比較して、一致するか否かを判定する動作（図９ａのステップ５７）までの処理手順は、上述した処理手順Ａにおけるものと同様である。

【００８０】

次に、処理手順Ｂでは、図９ａのステップ５７において、最高強度ハッシュアルゴリズムの識別子（sHash_alg_id）とユーザＩＤ対応ハッシュアルゴリズム識別子（uHash_alg_id）が一致しないと判定される（ステップ５７のＮｏ）。

このとき、認証情報管理部２２は、ハッシュアルゴリズム変更要求情報として、ユーザＩＤ対応ハッシュアルゴリズム識別子（uHash_alg_id）をサーバ通信部２１に出力する（ステップ６２）。

【００８１】
なお、ユーザＩＤ対応ハッシュアルゴリズム識別子（uHash_alg_id）のハッシュアルゴリズムの方が、最高強度ハッシュアルゴリズムの識別子（sHash_alg_id）のハッシュアルゴリズムより強度が高い場合、認証情報管理部２２により、サーバ通信部２１及びクライアント通信部１３を介して、認証要求管理部１２に接続拒否を返すなどの処理を行うようにすることもできる。
【００８２】
次に、サーバ通信部２１は、認証情報管理部２２から入力したハッシュアルゴリズム変更要求情報（ユーザＩＤ対応ハッシュアルゴリズム識別子（uHash_alg_id））をクライアント通信部１３に送信し（ステップ４０のＹｅｓ，ステップ４１）、クライアント通信部１３は、受信したハッシュアルゴリズム変更要求情報を認証要求管理部１２に出力する（ステップ３０のＮｏ，ステップ３２のＹｅｓ，ステップ３３）。
【００８３】
次に、認証要求管理部１２は、図６ａに示すように、クライアント通信部１３からハッシュアルゴリズム変更要求情報を入力すると（ステップ１９のＹｅｓ）、認証情報入力部１１に認証情報再入力受付要求情報を出力する（ステップ２２）。
【００８４】
なお、認証要求管理部１２がクライアント通信部１３からハッシュアルゴリズム変更要求情報を入力したときに、ステップ１４の処理により先に取得したユーザＩＤ（uid）とパスワード（passwd）が認証クライアント装置１０における所定の記憶手段に記憶されている場合は、認証情報入力部１１に認証情報再入力受付要求情報を送信する必要はない。
この場合、ステップ２３の処理結果をＹｅｓとして、ステップ２４以後における処理では、パスワード（passwd）と新パスワード（Npasswd）を同一のものとして取り扱う。
【００８５】
ただし、セキュリティ性の向上の観点から、パスワード（passwd）は、ステップ１６において、ハッシュ値生成部１５によるハッシュ値生成のための入力情報として使用した時点で破棄しておくことが好ましい。これは、ステップ２４，２６において、ハッシュ値生成部１５により、新パスワード（Npasswd）を用いてハッシュ値が生成される場合についても同様である。
【００８６】
次に、認証情報入力部１１は、図１１に示すように、認証要求管理部１２から認証情報再入力受付要求情報を入力すると（ステップ８０のＮｏ，ステップ８４のＹｅｓ）、ステップ８１の場合と同様に、認証情報の入力受付を行う（ステップ８５）。ただし、この場合は、ユーザＩＤ（uid）とパスワード（passwd）に加えて、新しいパスワード（Npasswd）を含めて認証情報とする。
そして、認証情報（uidとpasswdとNpasswd）の入力が完了すると（ステップ８６のＹｅｓ）、この認証情報を認証要求管理部１２に出力する（ステップ８７）。
【００８７】
次に、認証要求管理部１２は、図６ｂに示すように、認証情報入力部１１から認証情報（uidとpasswdとNpasswd）を入力すると（ステップ２３のＹｅｓ）、ユーザＩＤ対応ハッシュアルゴリズム識別子（uHash_alg_id）と、ハッシュ値生成のための入力情報としてユーザＩＤ（uid）とパスワード（passwd）をハッシュ値生成部１５に出力し、ハッシュ値生成部１５から第三のハッシュ値（uid_passwd_uHashV）を入力する（ステップ２４）。
【００８８】
このとき、ハッシュ値生成部１５は、図１２に示すように、認証要求管理部１２からハッシュ値生成要求情報として、ユーザＩＤ対応ハッシュアルゴリズム識別子（uHash_alg_id）と、ハッシュ値生成のための入力情報としてユーザＩＤ（uid）及びパスワード（passwd）とを入力すると（ステップ９０のＹｅｓ）、この入力した識別子に対応するハッシュアルゴリズムにより、ユーザＩＤ（uid）及びパスワード（passwd）を用いて第三のハッシュ値（uid_passwd_uHashV）を生成し、生成した第三のハッシュ値を認証要求管理部

１２に出力する（ステップ９１）。

【００８９】

次に、認証要求管理部１２は、図６ｂに示すように、最高強度ハッシュアルゴリズムの識別子（sHash_alg_id）と、ハッシュ値生成のための入力情報として乱数（rand1）とステップ２４で取得した第三のハッシュ値（uid_passwd_uHashV）をハッシュ値生成部１５に出力し、ハッシュ値生成部１５から第四のハッシュ値（uid_passwd_uHashV_rand1_sHashV）を入力する（ステップ２５）。

【００９０】

このとき、ハッシュ値生成部１５は、図１２に示すように、認証要求管理部１２からハッシュ値生成要求情報として、最高強度ハッシュアルゴリズムの識別子（sHash_alg_id）と、ハッシュ値生成のための入力情報として乱数（rand1）と図６ｂのステップ２４において認証要求管理部１２により取得された第三のハッシュ値（uid_passwd_uHashV）とを入力すると（ステップ９０のＹｅｓ）、この入力した識別子に対応するハッシュアルゴリズムにより、乱数（rand1）と第三のハッシュ値（uid_passwd_uHashV）を用いて第四のハッシュ値（uid_passwd_uHashV_rand1_sHashV）を生成し、生成した第四のハッシュ値を認証要求管理部１２に出力する（ステップ９１）。

【００９１】

次に、認証要求管理部１２は、図６ｂに示すように、最高強度ハッシュアルゴリズムの識別子（sHash_alg_id）と、ハッシュ値生成のための入力情報としてユーザＩＤ（uid）及び新パスワード（Npasswd）をハッシュ値生成部１５に出力し、ハッシュ値生成部１５から第五のハッシュ値（uid_Npasswd_sHashV）を入力する（ステップ２６）。

【００９２】

このとき、ハッシュ値生成部１５は、図１２に示すように、認証要求管理部１２からハッシュ値生成要求情報として、最高強度ハッシュアルゴリズムの識別子（sHash_alg_id）と、ハッシュ値生成のための入力情報としてユーザＩＤ（uid）及び新パスワード（Npasswd）とを入力すると（ステップ９０のＹｅｓ）、この入力した識別子に対応するハッシュアルゴリズムにより、ユーザＩＤ（uid）及び新パスワード（Npasswd）を用いて第五のハッシュ値（uid_Npasswd_sHashV）を生成し、生成した第五のハッシュ値を認証要求管理部１２に出力する（ステップ９１）。

【００９３】

そして、認証要求管理部１２は、以上のようにして取得したユーザＩＤ（uid）と第四のハッシュ値（uid_passwd_uHashV_rand1_sHashV）と第五のハッシュ値（uid_Npasswd_sHashV）をクライアント通信部１３に出力する（ステップ２７）。

クライアント通信部１３は、認証要求管理部１２から入力したユーザＩＤと第四のハッシュ値と第五のハッシュ値をサーバ通信部２１に送信し（ステップ３０のＹｅｓ，ステップ３１）、サーバ通信部２１はこれらの情報を受信して認証情報管理部２２に出力する（ステップ４０のＮｏ，ステップ４２のＹｅｓ，ステップ４３）。

【００９４】

次に、認証情報管理部２２は、図９ｂに示すように、サーバ通信部２１からユーザＩＤと第四のハッシュ値と第五のハッシュ値を入力すると（ステップ６３のＹｅｓ）、最高強度ハッシュアルゴリズムの識別子（sHash_alg_id）と、ハッシュ値生成のための入力情報として乱数（rand1）とステップ５６で取得したユーザ情報における第三のハッシュ値（uid_passwd_uHashV）をハッシュ値生成部２６に出力し、ハッシュ値生成部２６から第四のハッシュ値（uid_passwd_uHashV_rand1_sHashV）を入力する（ステップ６４）。

【００９５】

このとき、ハッシュ値生成部２６は、図１３に示すように、認証情報管理部２２からハッシュ値生成要求情報として、最高強度ハッシュアルゴリズムの識別子（sHash_alg_id）と、ハッシュ値生成のための入力情報として乱数（rand1）とユーザ情報における第三のハッシュ値（uid_passwd_uHashV）とを入力すると（ステップ１００のＹｅｓ）、この入力した識別子に対応するハッシュアルゴリズムにより、乱数（rand1）と第三のハッシュ

値（uid_passwd_uHashV）を用いて第四のハッシュ値（uid_passwd_uHashV_rand1_sHashV）を生成し、生成した第四のハッシュ値を認証情報管理部２２に出力する（ステップ１０１）。

【００９６】

次に、認証情報管理部２２は、サーバ通信部２１から入力した第四の第二のハッシュ値（uid_passwd_uHashV_rand1_sHashV）と、ハッシュ値生成部２６から入力した第四のハッシュ値（uid_passwd_uHashV_rand1_sHashV）を比較して、一致するか否かを判定する（ステップ６５）。

そして、これらのハッシュ値が一致しない場合（ステップ６５のＮｏ）、認証情報管理部２２は、認証結果として認証失敗をサーバ通信部２１に出力する（図９ａのステップ６１）。

【００９７】

一方、これらのハッシュ値が一致する場合は（ステップ６５のＹｅｓ）、認証情報管理部２２は、ユーザ情報管理テーブル２４に対して、ユーザＩＤ（uid）に対応するユーザ情報におけるユーザＩＤ対応ハッシュアルゴリズム識別子（uHash_alg_id）を、最高強度ハッシュアルゴリズムの識別子（sHash_alg_id）に更新する（ステップ６６）。

【００９８】

また、認証情報管理部２２は、同ユーザ情報における第三のハッシュ値（uid_passwd_uHashV）を、第五のハッシュ値（uid_Npasswd_sHashV）に更新する（ステップ６６）。

そして、認証情報管理部２２は、認証結果として認証成功をサーバ通信部２１に出力する（図９ａのステップ６０）。

【００９９】

サーバ通信部２１は、認証情報管理部２２から入力した認証結果をクライアント通信部１３に送信し（図８のステップ４０のＹｅｓ，ステップ４１）、クライアント通信部１３は、サーバ通信部２１から認証情報を受信すると（図７のステップ３０のＮｏ，ステップ３２のＹｅｓ）、これを認証要求管理部１２に出力する（ステップ３３）。

そして、認証要求管理部１２は、クライアント通信部１３から認証結果を入力すると（図６ａのステップ２０のＹｅｓ）、この認証結果を表示手段に出力することなどにより、ユーザに通知する（ステップ２１）。

【０１００】

以上説明したように、本実施形態の認証システムによれば、使用するハッシュアルゴリズムをより強度の高いものに変更する場合に、まず認証サーバ装置側のハッシュアルゴリズムを変更し、認証クライアント装置側については、全ての認証クライアント装置の対応するハッシュアルゴリズムを一気に変更しなくても、個々の認証クライアント装置ごとに段階的に変更することで、ハッシュアルゴリズムの変更を認証システムに反映させることが可能となる。

また、ハッシュアルゴリズムを変更した場合でも、ユーザ認証を行うタイミングで、認証処理を行うとともに既存のユーザ情報を個別に新たなハッシュアルゴリズムを用いて更新できるため、ハッシュアルゴリズムの変更時にユーザ情報を一括して新規に作成するために認証システムを停止することなく、その認証システムを継続して利用することが可能となる。

【０１０１】

本発明は、以上の実施形態に限定されるものではなく、本発明の範囲内において、種々の変更実施が可能であることは言うまでもない。

例えば、図１には、一の認証クライアント装置１０のみを示しているが、一の認証サーバ装置２０に二以上の認証クライアント装置１０を接続する構成とすることも可能である。また、ハッシュアルゴリズムとして、図２に示したもの以外の新たなアルゴリズムを追加するなど適宜変更することが可能である。

【産業上の利用可能性】

【０１０２】

本発明は、クライアント装置とサーバ装置間の通信のセキュリティを確保するために、認証処理において用いられるハッシュアルゴリズムを比較的頻繁に変更する可能性のある認証システムなどに、好適に利用することが可能である。

【図面の簡単な説明】

【０１０３】

【図１】本発明の一実施形態の認証システムの構成を示すブロック図である。

【図２】本発明の一実施形態の認証システムにおけるハッシュアルゴリズムリスト１４を示す図である。

【図３】本発明の一実施形態の認証システムにおけるハッシュアルゴリズム強度テーブル２３を示す図である。

【図４】本発明の一実施形態の認証システムにおけるユーザ情報管理テーブル２４を示す図である。

【図５】本発明の一実施形態の認証システムにおいて認証クライアント装置及び認証サーバ装置で送受信される変数の説明を示す図である。

【図６ａ】本発明の一実施形態の認証システムにおける認証要求管理部１２による処理手順（ａ）を示すフローチャートである。

【図６ｂ】本発明の一実施形態の認証システムにおける認証要求管理部１２による処理手順（ｂ）を示すフローチャートである。

【図７】本発明の一実施形態の認証システムにおけるクライアント通信部１３による処理手順を示すフローチャートである。

【図８】本発明の一実施形態の認証システムにおけるサーバ通信部２１による処理手順を示すフローチャートである。

【図９ａ】本発明の一実施形態の認証システムにおける認証情報管理部２２による処理手順（ａ）を示すフローチャートである。

【図９ｂ】本発明の一実施形態の認証システムにおける認証情報管理部２２による処理手順（ｂ）を示すフローチャートである。

【図１０】本発明の一実施形態の認証システムにおける乱数生成部２５による処理手順を示すフローチャートである。

【図１１】本発明の一実施形態の認証システムにおける認証情報入力部１１による処理手順を示すフローチャートである。

【図１２】本発明の一実施形態の認証システムにおける認証クライアント装置のハッシュ値生成部１５による処理手順を示すフローチャートである。

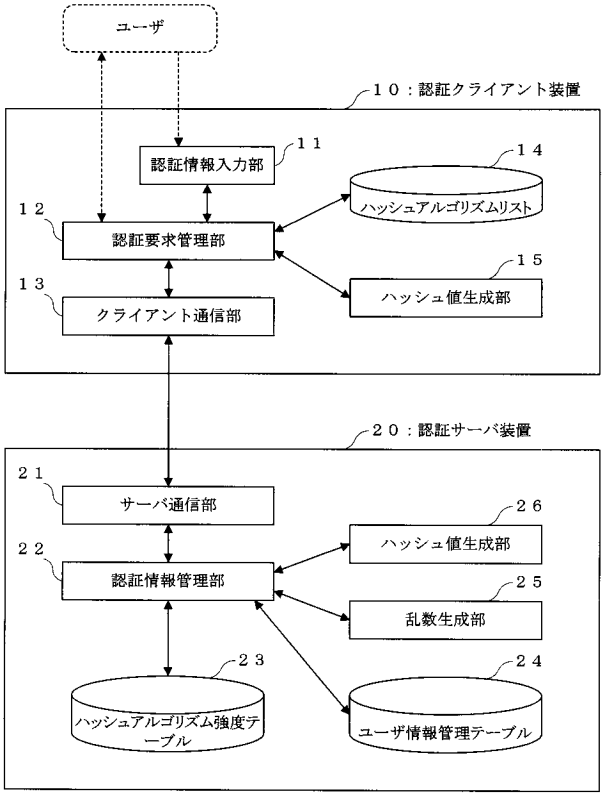
【図１３】本発明の一実施形態の認証システムにおける認証サーバ装置のハッシュ値生成部２６による処理手順を示すフローチャートである。

【符号の説明】

【０１０４】

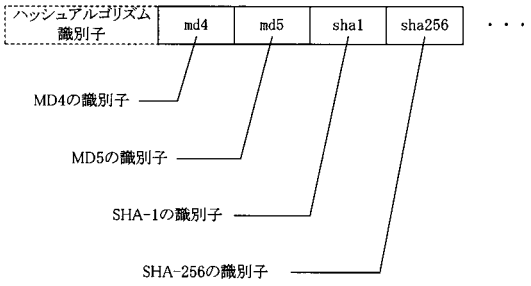
１０　認証クライアント装置
１１　認証情報入力部
１２　認証要求管理部
１３　クライアント通信部
１４　ハッシュアルゴリズムリスト
１５　ハッシュ値生成部
２０　認証サーバ装置
２１　サーバ通信部
２２　認証情報管理部
２３　ハッシュアルゴリズム強度テーブル
２４　ユーザ情報管理テーブル
２５　乱数生成部
２６　ハッシュ値生成部

【図１】



【図２】

ハッシュアルゴリズムリスト１４



【図３】

ハッシュアルゴリズム強度テーブル２３

ハッシュアルゴリズム識別子	強度
md4	1
md5	1
sha1	2
sha256	3

・
・
・

【図４】

ユーザ情報管理テーブル２４

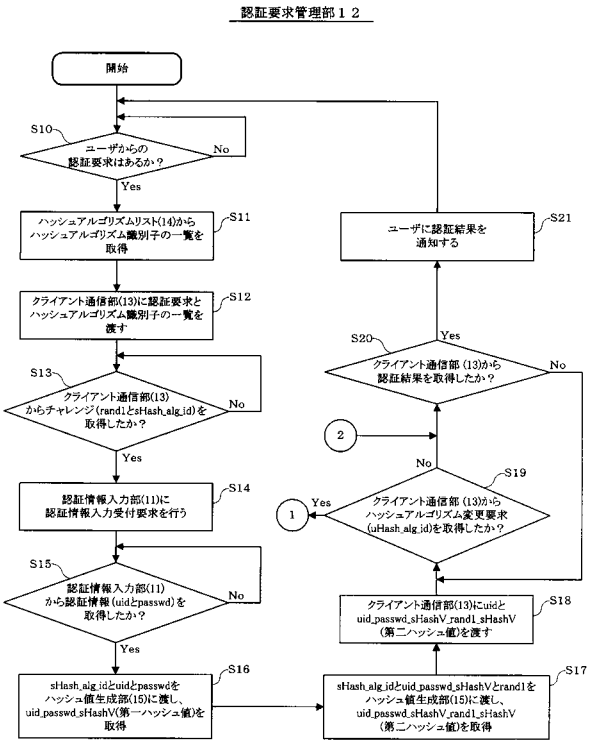
uid	uid_passwd_uHashV	uHash_alg_id
U000001	bc373d17c5dbb116db4d7924e9ec601f05461c33	sha1
U000002	2f7abb3ee7a652382bde496e2bcd5305	md5
U000003	b2c8fac8e42ea5864b267645c0f67d84cee645941a2bd33087707911d4da3c76	sha256

・
・
・

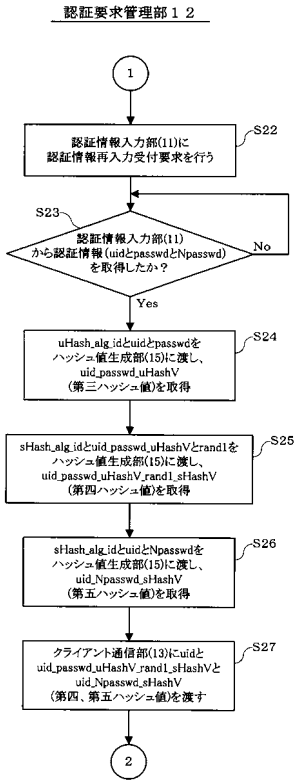
【図５】

変数	説明
rand1 (乱数)	乱数生成部(25)が生成した乱数
sHash_alg_id (最高強度ハッシュアルゴリズム識別子)	認証クライアント装置(10)と認証サーバ装置(20)で共に使用可能なハッシュアルゴリズムの中で最も強度の高いハッシュアルゴリズムのハッシュアルゴリズム識別子
uid (ユーザID)	ユーザが入力したユーザID
passwd (パスワード)	ユーザが入力したパスワード
uid_passwd_sHashV (第一のハッシュ値)	uidとpasswdからsHash_alg_idが示すハッシュアルゴリズムを使用して生成したハッシュ値
uid_passwd_sHashV_rand1_sHashV (第二のハッシュ値)	uid_passwd_sHashVとrand1からsHash_alg_idが示すハッシュアルゴリズムを使用して生成したハッシュ値
uHash_alg_id (ユーザID対応ハッシュアルゴリズム識別子)	ユーザ情報管理テーブル(23)に保持されているuidに対応するユーザ情報に保持されているハッシュアルゴリズム識別子
uid_passwd_uHashV (第三のハッシュ値)	uidとpasswdからuHash_alg_idが示すハッシュアルゴリズムを使用して生成したハッシュ値
uid_passwd_uHashV_rand1_sHashV (第四のハッシュ値)	uid_passwd_uHashVとrand1からsHash_alg_idが示すハッシュアルゴリズムを使用して生成したハッシュ値
Npasswd (新パスワード)	ユーザが入力した新しいパスワード
uid_Npasswd_sHashV (第五のハッシュ値)	uidとNpasswdからsHash_alg_idが示すハッシュアルゴリズムを使用して生成したハッシュ値

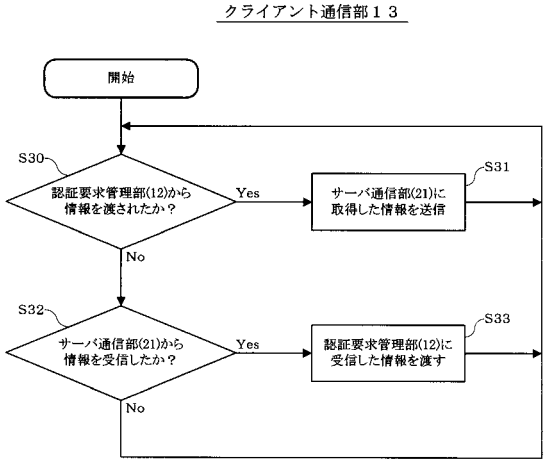
【図６ａ】


認証要求管理部１２
開始
S10
ユーザからの認証要求はあるか？
No
Yes
S11
ハッシュアルゴリズムリスト(14)からハッシュアルゴリズム識別子の一覧を取得
S12
クライアント通信部(13)に認証要求とハッシュアルゴリズム識別子の一覧を渡す
S13
クライアント通信部(13)からチャレンジ(rand1とsHash_alg_id)を取得したか？
No
Yes
S14
認証情報入力部(11)に認証情報入力受付要求を行う
S15
認証情報入力部(11)から認証情報(uidとpasswd)を取得したか？
No
Yes
S16
sHash_alg_idとuidとpasswdをハッシュ値生成部(15)に渡し、uid_passwd_sHashV(第一ハッシュ値)を取得
S17
sHash_alg_idとuid_passwd_sHashVとrand1をハッシュ値生成部(15)に渡し、uid_passwd_sHashV_rand1_sHashV(第二ハッシュ値)を取得
S18
クライアント通信部(13)にuidとuid_passwd_sHashV_rand1_sHashV(第二ハッシュ値)を渡す
S19
1
Yes
クライアント通信部(13)からハッシュアルゴリズム変更要求(uHash_alg_id)を取得したか？
No
2
S20
Yes
クライアント通信部(13)から認証結果を取得したか？
No
S21
ユーザに認証結果を通知する

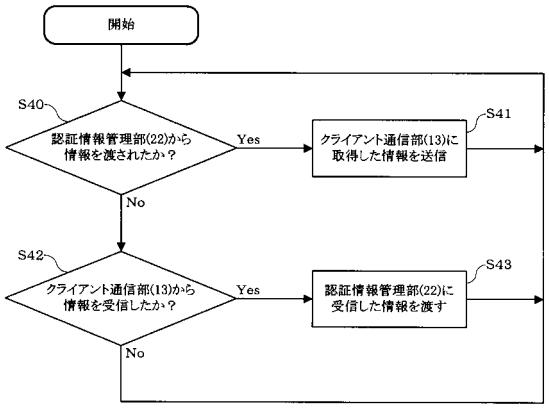
【図６ｂ】


認証要求管理部１２
1
S22
認証情報入力部(11)に認証情報再入力受付要求を行う
S23
認証情報入力部(11)から認証情報(uidとpasswdとNpasswd)を取得したか？
No
Yes
S24
uHash_alg_idとuidとpasswdをハッシュ値生成部(15)に渡し、uid_passwd_uHashV(第三ハッシュ値)を取得
S25
sHash_alg_idとuid_passwd_uHashVとrand1をハッシュ値生成部(15)に渡し、uid_passwd_uHashV_rand1_sHashV(第四ハッシュ値)を取得
S26
sHash_alg_idとuidとNpasswdをハッシュ値生成部(15)に渡し、uid_Npasswd_sHashV(第五ハッシュ値)を取得
S27
クライアント通信部(13)にuidとuid_passwd_uHashV_rand1_sHashVとuid_Npasswd_sHashV(第四、第五ハッシュ値)を渡す
2

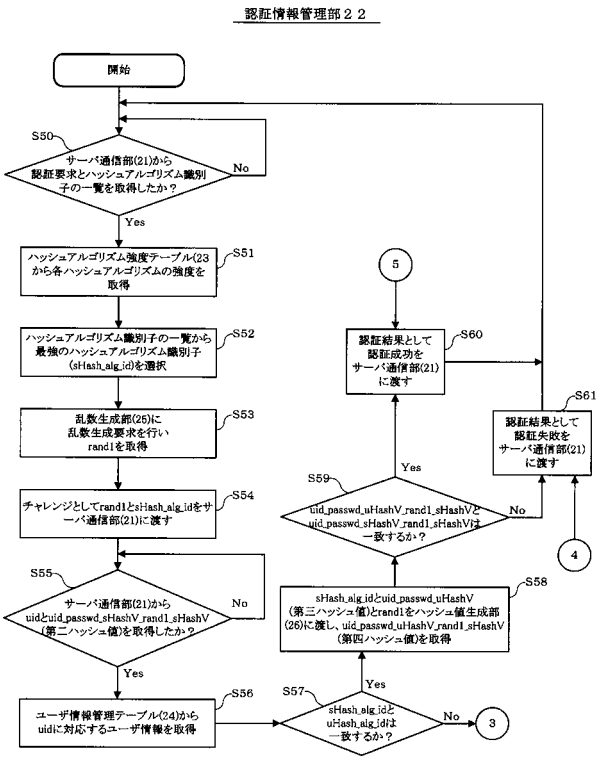
【図７】


クライアント通信部１３
開始
S30
認証要求管理部(12)から情報を渡されたか？
Yes
S31
サーバ通信部(21)に取得した情報を送信
No
S32
サーバ通信部(21)から情報を受信したか？
Yes
S33
認証要求管理部(12)に受信した情報を渡す
No

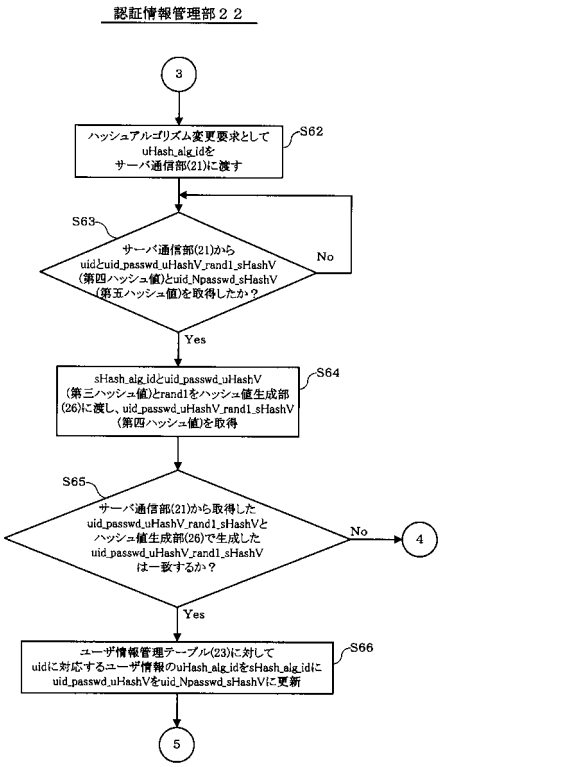
【図８】


サーバ通信部２１
開始
S40
認証情報管理部(22)から情報を渡されたか？
Yes
S41
クライアント通信部(13)に取得した情報を送信
No
S42
クライアント通信部(13)から情報を受信したか？
Yes
S43
認証情報管理部(22)に受信した情報を渡す
No

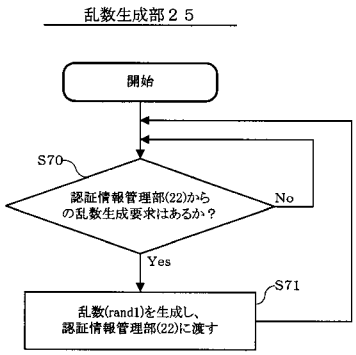
【図９ａ】



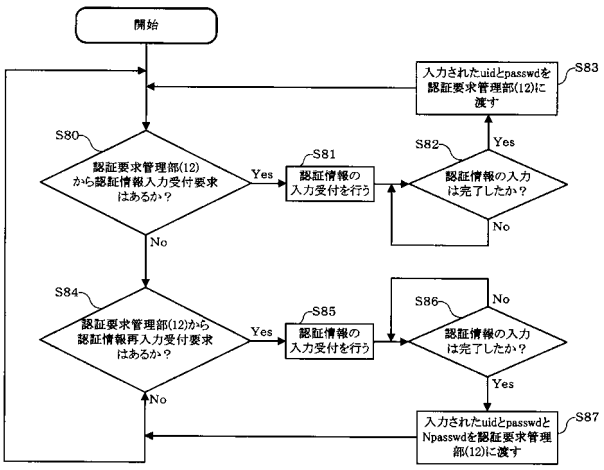
【図９ｂ】



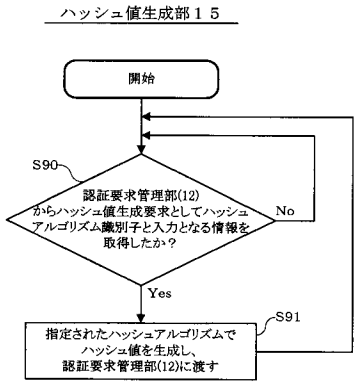
【図１０】



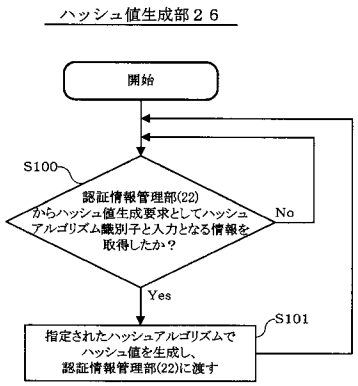
【図１１】



【図１２】


ハッシュ値生成部１５
開始
S90
認証要求管理部(12)
からハッシュ値生成要求としてハッシュ
アルゴリズム識別子と入力となる情報を
取得したか？
No
Yes
S91
指定されたハッシュアルゴリズムで
ハッシュ値を生成し、
認証要求管理部(12)に渡す

【図１３】


ハッシュ値生成部２６
開始
S100
認証情報管理部(22)
からハッシュ値生成要求としてハッシュ
アルゴリズム識別子と入力となる情報を
取得したか？
No
Yes
S101
指定されたハッシュアルゴリズムで
ハッシュ値を生成し、
認証情報管理部(22)に渡す

フロントページの続き

(56)参考文献 特表２００６－５１０２４１（ＪＰ，Ａ）
特開２００６－２３８２７３（ＪＰ，Ａ）
特開２００６－１２１６６２（ＪＰ，Ａ）
特開２００６－１０７２４７（ＪＰ，Ａ）
特開２００４－５３７１６（ＪＰ，Ａ）
特開２０００－５７０９９（ＪＰ，Ａ）
特開平１０－２２４３４３（ＪＰ，Ａ）
特開平７－３２５７８５（ＪＰ，Ａ）
特開平２－１８７７８５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３２
Ｇ０６Ｆ　２１／２０