【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成20年2月28日(2008.2.28)

【公表番号】特表2003-520467(P2003-520467A)
【公表日】平成15年7月2日(2003.7.2)
【出願番号】特願2001-547237(P2001-547237)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
Ｇ０６Ｆ　21/20　(2006.01)
Ｇ０９Ｃ　1/00　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ａ
Ｇ０６Ｆ　15/00　３３０Ｂ
Ｇ０９Ｃ　1/00　６４０Ｅ

【手続補正書】
【提出日】平成19年12月20日(2007.12.20)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】　ソフトウエアのプロバイダがソフトウエアのユーザを認証するための方法であって、
ユーザから受信された情報に応じてパズルを構成し、このパズルは情報を含んでおり、ここで構成するステップは、導出された値を生成するために情報から値を導出し、累乗値を生成するために導出された値を累乗し、そして累乗された値を導出された値の一部と結合するステップを含み、
パズルをユーザに送り、
パズルに対する解答をプロバイダに返し、
情報および乱数を蓄積し、
第一のハッシュ結果を生成するために、情報および乱数にハッシュ関数を実行し、そして
第一のハッシュ結果を暗号化するステップを含み、
ここで導出するステップは、暗号化されたハッシュ結果を第一および第二の成分に分割し、第二のハッシュ結果を生成するために第一の成分および乱数の連鎖にハッシュ関数を実行し、引き伸ばされた第二の成分を生成するために第二の成分に複数のゼロ値を付加し、排他的ＯＲ結果を生成するために、引き伸ばされた第二の成分と第二のハッシュ結果との間に排他的ＯＲ操作を実行し、そして導出された値を生成するために、第一の成分と排他的ＯＲ結果を結合するステップを含む
方法。
【請求項２】　ソフトウエアのプロバイダがソフトウエアのユーザを認証することを可能にする装置あって、
ユーザから受信された情報に応じてパズルを構成する手段と、このパズルは情報を含んでおり、ここでパズルを構成する手段はさらに、導出された値を生成するために情報から値を導出する手段、累乗値を生成するために導出された値を累乗する手段、そして累乗された値を導出された値の一部と結合する手段を含み、
パズルをユーザに送る手段、そして

パズルに対する解答をプロバイダに返す手段、
情報および乱数を蓄積する手段、
第一のハッシュ結果を生成するために、情報および乱数にハッシュ関数を実行する手段、そして
第一のハッシュ結果を暗号化する手段を含み、
ここで導出する手段は、暗号化されたハッシュ結果を第一および第二の成分に分割し、第二のハッシュ結果を生成するために第一の成分および乱数の連鎖にハッシュ関数を実行し、引き伸ばされた第二の成分を生成するために第二の成分に複数のゼロ値を付加し、排他的ＯＲ結果を生成するために、引き伸ばされた第二の成分と第二のハッシュ結果との間に排他的ＯＲ操作を実行し、そして導出された値を生成するために、第一の成分と排他的ＯＲ結果を結合する
装置。

【請求項３】　ソフトウエアのプロバイダがソフトウエアのユーザを認証することを可能にする装置あって、
処理装置と、そして
処理装置によってアクセスが可能であり、ユーザから受信された情報に応じてパズルを構成し、このパズルは情報を含み、そしてパズルをユーザに送る、処理装置によって実行可能な一連の命令を含む、処理装置が読み取り可能な蓄積媒体と
を含み、
ここでパズルは導出された値を生成するために情報から値を導出することにより構成され、累乗値を生成するために導出された値を累乗し、そして累乗された値を導出された値の一部と結合し、そして
ここで一連の命令は、情報および乱数を蓄積するために、第一のハッシュ結果を生成するため情報および乱数にハッシュ関数を実行するために、そして第一のハッシュ結果を暗号化するために処理装置によりさらに実行可能であり、ここで導出された値は暗号化されたハッシュ結果を第一および第二の成分に分割することにより導出され、第二のハッシュ結果を生成するために第一の成分および乱数の連鎖にハッシュ関数を実行し、引き伸ばされた第二の成分を生成するために第二の成分に複数のゼロ値を付加し、排他的ＯＲ結果を生成するために、引き伸ばされた第二の成分と第二のハッシュ結果との間に排他的ＯＲ操作を実行し、そして導出された値を生成するために、第一の成分と排他的ＯＲ結果を結合する
装置。