

【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 6 部門第 3 区分
 【発行日】平成 29 年 6 月 22 日 (2017.6.22)

【公表番号】特表 2016-522932 (P2016-522932A)
 【公表日】平成 28 年 8 月 4 日 (2016.8.4)
 【年通号数】公開・登録公報 2016-046
 【出願番号】特願 2016-511818 (P2016-511818)
 【国際特許分類】

G 0 6 F 21/45 (2013.01)

G 0 6 F 21/31 (2013.01)

【 F I 】

G 0 6 F 21/45

G 0 6 F 21/31

【手続補正書】

【提出日】平成 29 年 4 月 25 日 (2017.4.25)

【手続補正 1】

【補正対象書類名】特許請求の範囲

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項 1】

計算環境において、ソース・サービスとターゲット・サービスとの間で 1 組のパスワード資格証明を同期させる方法であって、前記 1 組のパスワード資格証明が、前記ソース・デバイスおよび前記ターゲット・サービスの各々へのアクセスを可能にし、前記方法が、プロセッサにより、同期タイムスタンプを提供するステップであって、前記同期タイムスタンプが、前記ソース・デバイスおよび前記ターゲット・サービス間の最後のパスワード資格証明同期に対応する、ステップと、

ハッシュされた 1 組の変更されたパスワード資格証明を受けるステップであって、前記ハッシュされた 1 組の変更されたパスワード資格証明が、前記最後のパスワード資格証明同期から前記 1 組のパスワード資格証明に対し行われた変更のみを含む、ステップと、

前記ハッシュされた 1 組の変更されたパスワード資格証明を、アイデンティティ認証における使用のために、前記ターゲット・サービスにエクスポートするステップと、
 を含む、方法。

【請求項 2】

請求項 1 記載の方法において、前記ハッシュされた 1 組の変更されたパスワード資格証明が、一次ハッシング・アルゴリズムによって計算され、前記方法が更に、前記ターゲット・サービスにエクスポートするために、前記ハッシュされた 1 組の変更されたパスワード資格証明に対応する二次ハッシュ・アルゴリズムを使用して、前記ハッシュされた 1 組の変更されたパスワード資格証明を秘密保護データに二次的にハッシングするステップ
 を含む、方法。

【請求項 3】

請求項 2 記載の方法において、前記ハッシュされた 1 組の変更されたパスワード資格証明を前記秘密保護データに二次的にハッシュするステップが、ランダム・ソルトおよび複数の繰り返しを使用するステップを含む、方法。

【請求項 4】

システムであって、

ターゲット・ディレクトリー・サービスと、

複数のドメインを含むドメイン・メッシュと、
前記ドメイン・メッシュに結合された同期ホストと、
を含み、

前記同期ホストが、前記ドメイン・メッシュにおいて受けたパスワード変更を、前記メッシュの外部にある前記ターゲット・ディレクトリー・サービスと同期させるように構成され、前記パスワード変更を同期させることが、

前記ドメイン・メッシュからの平文パスワードを表すハッシュ値を受け、
二次ハッシュ・アルゴリズムを使用して前記ハッシュ値に対し追加のハッシュを実行して保護パスワード・データーを生成し、

前記保護パスワード・データーを前記ターゲット・ディレクトリー・サービスにエクスポートする、
ことを含む、システム。

【請求項 5】

請求項 4 記載のシステムにおいて、前記同期ホストが、前記二次ハッシュ・アルゴリズムおよびランダム・ソルトを使用して、前記ハッシュ値を処理して前記保護パスワード・データーにする、システム。

【請求項 6】

請求項 4 記載のシステムにおいて、更に、パスワード変更データーのために、前記複数のドメインのうちの 1 つにおけるどのドメイン・コントローラーに連絡するか決定するために構成されたメッシュ・サービスを含む、システム。

【請求項 7】

請求項 4 記載のシステムにおいて、
前記複数のドメインに対する各ドメイン・コントローラー、
オンプレミス・サーバー・ドメイン・メッシュに結合された別のマシン、あるいは
前記ドメイン・メッシュから地理的に離れたクラウド・マシンまたは他のマシン、
の内の 1 つにおいて実行する前記同期ホストの少なくとも一部によって、前記二次ハッシュ・アルゴリズムを使用して前記ハッシュ値を処理して前記保護パスワード・データーにする、システム。

【請求項 8】

請求項 4 記載のシステムにおいて、前記ターゲット・ディレクトリー・サービスには、
複数のハッシング・アルゴリズムまたはアイデンティティに関連するハッシング・アルゴリズムの組み合わせの内任意のものを前記アイデンティティの認証の間に使用するために、
暗号化方式の指定が構成される、システム。

【請求項 9】

コンピューター実行可能命令を有する 1 つ以上のコンピューター読み取り可能記憶媒体であって、
前記コンピューター実行可能命令が 1 つ以上のプロセッサによって実行されると、前記 1 つ以上のプロセッサに動作を実行させ、前記動作が、

ターゲット・サービスにおいて、平文パスワードに対応する保護パスワード・データーを含む複数組のデーターを維持する動作であって、保護パスワード・データーがそれぞれのアイデンティティと関連し、前記保護パスワード・データーが、少なくとも 2 つのハッシング・アルゴリズムの組み合わせによって平文パスワードから計算され、前記ターゲット・サービスに同期される、動作と、

前記ターゲット・サービスにおいて、アイデンティティおよびパスワードに対応する資格証明を含むログイン試行を受ける動作と、

前記パスワードに対して少なくとも 1 つのハッシング・アルゴリズムを実行することに基づいて第 1 の値を計算する動作と、

前記アイデンティティを認証するために、前記第 1 の値を、前記アイデンティティに関連する保護パスワード・データーと比較する動作と、
を含む、1 つ以上のコンピューター読み取り可能記憶媒体。

【請求項 10】

請求項 9 記載の 1 つ以上のコンピューター読み取り可能記憶媒体において、更にコンピューター実行可能命令を有し、該コンピューター実行可能命令が前記 1 つ以上のプロセッサによって実行されると、前記 1 つ以上のプロセッサに、アイデンティティに関連するデーターを、少なくとも 1 つの異なるハッシング・アルゴリズムから計算されたデーターと交換することを含む動作を実行させる、1 つ以上のコンピューター読み取り可能記憶媒体。