

【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23年3月17日(2011.3.17)

【公表番号】特表2010-518493(P2010-518493A)

【公表日】平成22年5月27日(2010.5.27)

【年通号数】公開・登録公報2010-021

【出願番号】特願2009-548475(P2009-548475)

【国際特許分類】

G 06 F 21/20 (2006.01)

H 04 L 9/32 (2006.01)

【F I】

G 06 F 15/00 3 3 0 B

H 04 L 9/00 6 7 3 A

G 06 F 15/00 3 3 0 C

G 06 F 15/00 3 3 0 F

【手続補正書】

【提出日】平成23年1月31日(2011.1.31)

【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】

リクエスタによるコンピュータネットワークへのアクセスを動的に評価するためのコンピュータ実行方法であって、

装置においてリクエスタからの前記ネットワークへのアクセスに対する要求を受信するステップと、

前記リクエスタに関する認証情報を受信するステップと、

前記リクエスタに関する許可情報を受け入れるステップと、

前記リクエスタが真正であるかどうかを判断するために前記認証情報と許可情報を比較するステップと、

前記認証情報と前記許可情報との比較に基づいて認証スコアを生成するステップと、

前記認証スコアに基づいてネットワークアクセスを判断するステップと

を備える、コンピュータ実行方法。

【請求項2】

前記装置において前記ネットワークへのアクセスを前記リクエスタに許可するステップと、

前記装置において前記ネットワークへのアクセスを前記リクエスタに提供するステップと、

前記リクエスタに関する追加の認証情報を受信するステップと、

前記リクエスタに関する前記認証情報の変化を識別するステップであって、前記追加の認証情報の少なくとも一部が前記認証情報とは異なるステップと、

前記変化に基づいて前記装置において前記リクエスタに対して前記ネットワークへのアクセスを終了させるかどうかを判断するステップと

をさらに備える、請求項1に記載のコンピュータ実行方法。

【請求項3】

前記認証情報が(i)セキュリティ識別子及び個人識別番号を含む2要因認証情報又は

(i i) 前記リクエスタの生体認証データの1つを備える、請求項1に記載のコンピュータ実行方法。

【請求項4】

前記認証情報と前記許可情報とを比較するステップは、
前記認証情報が前記許可情報に実質的に類似するかどうかを判断するステップと、
前記認証情報の前記許可情報に対する類似性に基づいて前記認証スコアを生成するステップと
を備える、請求項1に記載のコンピュータ実行方法。

【請求項5】

前記認証情報と前記許可情報とを比較するステップは、
前記認証情報に基づいて前記リクエスタの識別性を判断するステップと、
前記ネットワークにおいて前記リクエスタによって要求されるサービスを判断するステップと、
前記リクエスタの前記識別性を前記サービスへのアクセスを許可されるユーザのリストと比較することにより、前記リクエスタが前記ネットワーク上で前記サービスにアクセスすることを許可されるかどうかを判断するステップと
を備える、請求項1に記載のコンピュータ実行方法。

【請求項6】

装置によるコンピュータネットワークへのアクセスを動的に評価するためのコンピュータ実行方法であって、
装置からの前記ネットワークへのアクセスに対する要求を受信するステップと、
前記要求を生成する前記装置に関する情報を受信するステップと、
前記装置情報と履歴装置情報とを比較するステップと、
前記装置情報と前記履歴装置情報との比較に基づいて前記装置が真正であるかどうかを判断するステップと、
前記装置情報と履歴装置情報との前記比較に基づいて認証スコアを生成するステップと
、
前記認証スコアに基づいて前記装置にネットワークアクセスを許可するかどうかを判断するステップと
を備える、コンピュータ実行方法。

【請求項7】

前記認証スコアに基づいて前記装置にネットワークアクセスを許可するかどうかを判断するステップは、
前記認証スコアを評価するステップと、
前記装置情報と前記履歴装置情報との前記比較の少なくとも一部を評価するステップと
、
前記認証スコア及び装置情報と前記履歴装置情報との前記比較の前記一部に基づいて前記装置にネットワークアクセスを許可するかどうかを判断するステップと
を備える、請求項6に記載のコンピュータ実行方法。

【請求項8】

前記装置が真正であるかどうかを判断するステップは、
前記装置情報が前記履歴装置情報に実質的に類似するかどうかを判断するステップと、
前記装置情報と前記履歴装置情報との間の類似性の量に基づいて前記認証スコアを生成するステップと
を備える、請求項6に記載のコンピュータ実行方法。

【請求項9】

前記ネットワークにおいて前記装置によって要求されるサービスを判断するステップと
、
前記装置の認証が前記要求されるサービスのために必要であるかどうかを判断するため
に、前記要求されるサービスに関連する規則の組を評価するステップと、

前記装置の認証が前記要求されるサービスのために必要でないと判断される場合、前記認証スコアを評価することなく前記ネットワーク上で前記サービスへのアクセスを許可するステップと

をさらに備える、請求項6に記載のコンピュータ実行方法。

【請求項 1 0】

装置によるコンピュータネットワークへのアクセスを動的に評価するためのシステムであって、

前記装置を使用するリクエスタに関する情報を受信し、且つ前記リクエスタの真正性を判断するための第1の論理要素と、

前記ネットワークにアクセスするための要求を生成する前記装置に関する情報を受信し、且つ前記装置が真正であるかどうかを判断するための第2の論理要素と、

前記装置の場所及び前記リクエスタの場所に関する情報を受信し、且つ前記装置及び前記リクエスタの前記場所が実質的に類似であるかどうかを判断するための第3の論理要素と

を備える、システム。

【請求項 1 1】

前記第1、第2及び第3の論理要素の前記判断を受信し、且つこれら判断に基づいて前記ネットワークへのアクセスを前記装置に許可するかどうかを判断するためのポリシーエンジンをさらに備える、請求項1 0に記載のシステム。

【請求項 1 2】

前記ポリシーエンジンがさらに、前記装置の前記場所及び前記リクエスタの前記場所に関する前記情報の少なくとも一部を受信し、且つ前記ネットワークへのアクセスを前記装置に許可するかどうかを判断することが前記装置の前記場所及び前記リクエスタの前記場所に関する前記情報の前記受信される一部の評価をさらに備える、請求項1 1に記載のシステム。

【請求項 1 3】

前記ポリシーエンジンは、前記装置が前記ネットワークにアクセスしている間、前記第1、第2及び第3の論理要素の少なくとも1つから更新される情報を受信し、前記更新される情報が、前記更新される情報と前記第1、第2及び第3の論理要素からの前記情報との相違と識別するために前記ポリシーエンジンによって分析される、請求項1 1に記載のシステム。

【請求項 1 4】

複数のアプリケーションをさらに備え、少なくとも一部の前記アプリケーションがアクセス規則を備え、前記ポリシーエンジンが、前記装置により要求されるアプリケーションに対する前記アクセス規則を評価し、且つ前記更新される情報と前記第1、第2及び第3の論理要素からの前記情報との前記相違が前記要求されるアプリケーションに対する前記アクセス規則の少なくとも1つに違反する場合に前記装置と前記ネットワークとの間の接続を終了させる、請求項1 3に記載のシステム。

【請求項 1 5】

前記第3の論理要素に通信可能に接続される存在フィードをさらに備え、前記存在フィードが前記リクエスタの前記場所に関する情報を備える、請求項1 0に記載のシステム。

【請求項 1 6】

前記第1の論理要素に通信可能に接続される許可保存場所をさらに備え、前記許可データベースが前記ネットワーク上の複数のサービスに関するユーザ許可情報を備える、請求項1 0に記載のシステム。

【請求項 1 7】

前記第2の論理要素に通信可能に接続される装置資源の保存場所をさらに備え、前記保存場所が前記ネットワークへのアクセスを有する複数の装置に関する情報を備える、請求項1 0に記載のシステム。