【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30年5月10日(2018.5.10)

【公表番号】特表2017-510013(P2017-510013A)
【公表日】平成29年4月6日(2017.4.6)
【年通号数】公開・登録公報2017-014
【出願番号】特願2017-501088(P2017-501088)
【国際特許分類】
Ｇ０６Ｆ　21/31　　(2013.01)
【ＦＩ】
Ｇ０６Ｆ　21/31

【手続補正書】
【提出日】平成30年3月19日(2018.3.19)
【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】
装置であって、
プロセッサー回路と、
前記プロセッサー回路による実行のためのサーバー・アプリケーションと、
を備え、前記サーバー・アプリケーションが、
第１アカウントを有するクライアントからの、１組のサーバー・デバイスにおけるサーバー・デバイスにアクセスするための第２アカウントを作成する要求を、クライアント・デバイスを介して受けるアカウント管理コンポーネントであって、
前記１組のサーバー・デバイスが、複数の違反境界にセグメント化され、前記複数の違反境界の各違反境界が、各違反境界内における１組のサーバー・デバイスへのアクセスを付与するように構成された１つのセキュリティ・グループに関連付けられる、管理コンポーネントと、
前記第１アカウントに関連付けられたセキュリティ情報に基づいて、前記第２アカウントを作成する前記要求を許可し、前記サーバー・デバイスを含む違反境界へのアクセスを付与するように構成されたセキュリティ・グループを識別し、前記第２アカウントによる、前記違反境界における前記サーバー・デバイスへのアクセスをイネーブルするために、前記第２アカウントを前記セキュリティ・グループと関連付ける、アカウント許可コンポーネントと、
前記クライアント・デバイスが前記サーバー・デバイスにアクセスすることをイネーブルするために、前記第２アカウントを作成するアカウント・プロビジョニング・コンポーネントと、
前記第２アカウントに関連付けられたアカウント情報を前記クライアント・デバイスに提供するアカウント通知コンポーネントと、
を含む、装置。
【請求項２】
請求項１記載の装置において、前記アカウント許可コンポーネントが、更に、
前記要求に関連付けられた範囲および役割を判定し、
前記第１アカウントに関連付けられた前記アカウント情報に基づいて、前記第１アカウントに関連付けられた範囲および役割を判定し、

前記第１アカウントの前記範囲および前記役割に少なくとも部分的に基づいて、前記要求を許可する、
ように構成される、装置。
【請求項３】
請求項２記載の装置において、前記アカウント・プロビジョニング・コンポーネントが、更に、
前記要求に関連付けられた役割および範囲に基づいて、１組の昇格アクセス許可を有する前記第２アカウントの存在を判定し、
前記第２アカウントが存在しないときに、前記サーバー・デバイスへのアクセスのために前記第２アカウントを作成し、
前記サーバー・デバイスへのアクセスのために前記第２アカウントをイネーブルする、
ように構成される、装置。
【請求項４】
請求項１記載の装置において、アクセス許可を高めるための前記要求が、存続期間と関連付けられ、前記存続期間が、前記サーバー・デバイスへのアクセスをイネーブルする規定時間期間を含み、前記第２アカウントが前記規定時間期間の終了時に自動的にディスエーブルされる、装置。
【請求項５】
請求項１記載の装置において、前記サーバー・デバイスが、前記第１アカウントに関連付けられた１組のアクセス許可よりも高い１組のアクセス許可を要求し、前記第２アカウントが、前記第１アカウントに関連付けられた前記１組のアクセス許可よりも高い１組の上位アクセス許可を有する、装置。
【請求項６】
コンピューター実装方法であって、
第１アカウントを有するクライアントからの、１組のサーバー・デバイスにおけるサーバー・デバイスにアクセスするための１組のアクセス許可を有する第２アカウントを作成する要求を、クライアント・デバイスを介して受けるステップであって、
前記１組のサーバー・デバイスが、複数の違反境界にセグメント化され、前記複数の違反境界の各違反境界が、違反境界内における１組のサーバー・デバイスへのアクセスを付与するように構成された１つのセキュリティ・グループに関連付けられる、ステップと、
回路によって、前記第１アカウントに関連付けられた認証トークンに少なくとも部分的に基づいて、前記第２アカウントを作成する前記要求を許可するステップと、
前記クライアント・デバイスが前記サーバー・デバイスにアクセスするのをイネーブルするために、前記第２アカウントをプロビジョニングするステップであって、
前記サーバー・デバイスを含む違反境界へのアクセスを付与するように構成されたセキュリティ・グループを識別し、前記第２アカウントによる、前記違反境界における前記サーバー・デバイスへのアクセスをイネーブルするために、前記第２アカウントを前記セキュリティ・グループと関連付ける、ステップと、
前記第２アカウントに関連付けられたアカウント情報を、前記クライアント・デバイスに提供するステップであって、前記アカウント情報が、前記クライアントの認証および許可情報に対応する、ステップと、
を含む、コンピューター実装方法。
【請求項７】
請求項６記載のコンピューター実装方法において、アクセス許可を高めるために、前記要求を許可する前記ステップが、更に、
前記要求に関連付けられた要求の範囲および役割を判定するステップと、
前記第１アカウントに関連付けられた前記アカウント情報に基づいて、前記第１アカウントに関連付けられたアカウントの範囲および役割を判定するステップと、
前記第１アカウントの前記範囲および前記役割に基づいて、前記要求を許可するステッ

プと、
を含む、コンピューター実装方法。
【請求項８】
請求項７記載のコンピューター実装方法において、前記第２アカウントをプロビジョニングする前記ステップが、更に、
前記要求に関連付けられた前記役割および範囲に基づいて、１組のアクセス許可を有する前記第２アカウントの存在を判定するステップと、
前記第２アカウントが存在しないときに、前記サーバー・デバイスへのアクセスのために前記第２アカウントを作成するステップと、
前記サーバー・デバイスへのアクセスのために前記第２アカウントをイネーブルするステップと、
を含む、コンピューター実装方法。
【請求項９】
請求項６記載のコンピューター実装方法において、アクセス許可を高めるための前記要求が存続期間と関連付けられ、前記存続期間が、前記サーバー・デバイスへのアクセスをイネーブルする規定時間期間を含み、前記第２アカウントが前記規定時間期間の終了時に自動的にディスエーブルされる、コンピューター実装方法。
【請求項１０】
請求項６記載のコンピューター実装方法において、前記サーバー・デバイスが、前記第１アカウントに関連付けられた１組のアクセス許可よりも高い１組のアクセス許可を要求し、前記第２アカウントが、前記第１アカウントに関連付けられた前記１組のアクセス許可よりも高い１組の上位アクセス許可を有する、コンピューター実装方法。
【請求項１１】
命令を含むコンピューター読み取り可能記憶媒体であって、前記命令が実行されると、システムに、
サーバー・デバイスにアクセスするための１組の昇格アクセス許可を有するジャスト・イン・タイム（ＪＩＴ）アカウントを求める要求をクライアント・デバイスから受けさせ、前記クライアント・デバイスが、関連するクライアント・アカウントを有し、
前記クライアント・アカウントに関連付けられたパスワード情報に少なくとも部分的に基づいて、前記ＪＩＴアカウントを求める前記要求を許可させ、
前記サーバー・デバイスを含む違反境界へのアクセスを付与するように構成されたセキュリティ・グループを識別することにより、また、前記ＪＩＴアカウントによる、前記違反境界における前記サーバー・デバイスへのアクセスをイネーブルするために、前記ＪＩＴアカウントを前記セキュリティ・グループと関連付けることにより、前記サーバー・デバイスへのアクセスをイネーブルするために前記ＪＩＴアカウントを作成させ、
前記ＪＩＴアカウントに関連付けられたアカウント情報を前記クライアント・デバイスに提供させる、コンピューター読み取り可能記憶媒体。
【請求項１２】
請求項１１記載のコンピューター読み取り可能記憶媒体において、アクセス許可を高めるために、前記要求を許可させる命令が、実行されると、前記システムに、更に
前記要求に関連付けられた範囲および役割を判定させ、
クライアント・アカウント情報に基づいて、前記クライアント・アカウントに関連付けられた範囲および役割を判定させ、
前記クライアント・アカウントの前記範囲および前記役割に基づいて、前記要求を許可させる、コンピューター読み取り可能記憶媒体。
【請求項１３】
請求項１２記載のコンピューター読み取り可能記憶媒体において、前記ＪＩＴアカウントを作成させる命令が、実行されると、前記システムに、更に、
前記１組の昇格アクセス許可を有する前記ＪＩＴアカウントの存在を判定させ、
前記ＪＩＴアカウントがＪＩＴアカウント・データストアに既に存在するときに、前記

ＪＩＴアカウント・データストアから前記ＪＩＴアカウントを取り出させ、
前記サーバー・デバイスへのアクセスのために前記ＪＩＴアカウントをイネーブルさせる、コンピューター読み取り可能記憶媒体。
【請求項１４】
請求項１３記載のコンピューター読み取り可能記憶媒体において、前記パスワード情報が、認証トークン管理アプリケーションによって生成されたランダム・パスワードを含み、前記ランダム・パスワードが少なくとも２つの異なるキャラクター・クラスを含む、コンピューター読み取り可能記憶媒体。
【請求項１５】
請求項１１記載のコンピューター読み取り可能記憶媒体において、実行されると、前記システムに、
前記ＪＩＴアカウントに関連付けられる存続期間を決定させ、
前記ＪＩＴアカウントが失効したことを前記ＪＩＴアカウントに関連付けられる前記存続期間が示すときに、前記ＪＩＴアカウントをディスエーブルさせる、
命令を含む、コンピューター読み取り可能記憶媒体。
【請求項１６】
請求項１１記載のコンピューター読み取り可能記憶媒体において、実行されると、前記システムに、
前記ＪＩＴアカウントがディスエーブルされ、前記クライアントによって規定時間期間にわたりアクセスされていないときに、前記ＪＩＴアカウントを削除させる命令を含む、コンピューター読み取り可能記憶媒体。