【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29年10月19日(2017.10.19)

【公表番号】特表2017-502620(P2017-502620A)
【公表日】平成29年1月19日(2017.1.19)
【年通号数】公開・登録公報2017-003
【出願番号】特願2016-552416(P2016-552416)
【国際特許分類】
Ｈ０４Ｌ　12/717　(2013.01)
【ＦＩ】
Ｈ０４Ｌ　12/717

【手続補正書】
【提出日】平成29年9月8日(2017.9.8)
【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】
管理ドメイン内の不良アクターを隔離する方法であって、
キャッシュされたアクターセットを格納するステップであって、前記キャッシュされたアクターセットの各々は、前記管理ドメイン内に存在するアクターのグループを指定する、ステップと、
特定のマネージドサーバに適用可能な複数のルールを格納するステップであって、前記ルールの各々は、サービスのプロバイダ、前記サービスのユーザ、および前記サービスの前記プロバイダと前記ユーザとの間の対話を制御している機能を指定する、ステップと、
前記複数のルールの所与のルールに関連して、各々が前記所与のルールにおいて指定された前記プロバイダ、および、前記所与のルールに指定された前記ユーザの少なくとも１つを含む前記キャッシュされたアクターセットのサブセットを含んでいる関連アクターセットを格納するステップと、
前記不良アクターを隔離するための指示を受信するステップと、
前記キャッシュされたアクターセットを更新して、前記不良アクターの状態における隔離された状態への変化を示すステップと、
前記所与のルールに対する前記関連アクターセットにおける変更されたアクターセットを識別するステップであって、前記変更されたアクターセットは、前記不良アクターの状態における前記隔離された状態への前記変化に基づいて更新されたものである、ステップと、
前記変更されたアクターセットを識別するステップに応答して、
前記変更されたアクターセットを記述している情報、および、前記特定のマネージドサーバによって格納されたローカルリストにおける前記変更されたアクターセットを追加、削除または変更するための指示を前記特定のマネージドサーバに送るステップと
を備えたことを特徴とする方法。
【請求項２】
前記不良アクターはターゲットマネージドサーバであり、および前記方法は、
前記ターゲットマネージドサーバの記述を変更して、前記ターゲットマネージドサーバの隔離固有の構成特性に対する値を設定することによって前記ターゲットマネージドサーバが隔離されることを示すステップをさらに備えたことを特徴とする請求項１に記載の方

法。
【請求項３】
前記不良アクターを隔離することを決定するステップをさらに備えたことを特徴とする請求項１に記載の方法。
【請求項４】
前記不良アクターはターゲットマネージドサーバであり、前記ターゲットマネージドサーバを隔離することを決定することは、ネットワーク攻撃が前記ターゲットマネージドサーバから生じたことを決定すること、または、前記ターゲットマネージドサーバが脆弱性を有することを決定することを含むことを特徴とする請求項３に記載の方法。
【請求項５】
前記変更されたアクターセットを記述している前記情報および前記指示を送るステップは、前記不良アクターから生じたインバウンドネットワークトラフィックを前記特定のマネージドサーバにブロックさせることを特徴とする請求項１に記載の方法。
【請求項６】
前記キャッシュされたアクターセットを更新するステップの前に、
前記不良アクターの記述に基づいて前記不良アクターに関する追加情報を決定するステップと、
前記不良アクターの前記記述を変更して前記追加情報を示すステップと
をさらに備えたことを特徴とする請求項１に記載の方法。
【請求項７】
前記不良アクターはターゲットマネージドサーバであり、前記方法は、
前記ターゲットマネージドサーバの記述に基づいて、前記ターゲットマネージドサーバが隔離された後に前記ターゲットマネージドサーバに適用可能な現在関連するルールを決定するステップと、
前記現在関連するルールが、前記ターゲットマネージドサーバが隔離される前に前記ターゲットマネージドサーバに適用可能であった以前関連したルールと異なるかどうかを判定するステップと、
前記現在関連するルールが前記以前関連したルールと異なるという判定に応答して、前記以前関連したルールに対して、追加、削除または変更されるべきルールを決定するステップと、
前記決定されたルールに基づいて機能レベルの指示を生成するステップと、
前記機能レベルの指示、ならびに、前記機能レベルの指示を追加、削除または変更するための指示を前記ターゲットマネージドサーバに送るステップと
をさらに備えたことを特徴とする請求項１に記載の方法。
【請求項８】
前記機能レベルの指示、および追加、削除または変更するための前記指示を送るステップは、アウトバウンドネットワークトラフィックを前記ターゲットマネージドサーバにブロックさせることを特徴とする請求項７に記載の方法。
【請求項９】
前記機能レベルの指示、および追加、削除または変更するための前記指示を送るステップは、管理インバウンドネットワークトラフィックのみを前記ターゲットマネージドサーバに許可させることを特徴とする請求項７に記載の方法。
【請求項１０】
前記不良アクターはターゲットマネージドサーバであり、前記方法は、
前記ターゲットマネージドサーバが隔離されたことに基づいて、変更された前記ターゲットマネージドサーバに関連する変更されたアクターセットを決定するステップと、
前記ターゲットマネージドサーバに関連する前記変更されたアクターセットを記述している情報、および、前記ターゲットマネージドサーバによって格納されたローカルリストにおける前記変更されたアクターセットを追加、削除または変更するための指示を前記ターゲットマネージドサーバに送るステップと

をさらに備えたことを特徴とする請求項１に記載の方法。
【請求項１１】
前記不良アクターはアンマネージドデバイスグループであり、前記方法は、アンマネージドデバイスを前記アンマネージドデバイスグループに追加することを決定するステップをさらに備えたことを特徴とする請求項１に記載の方法。
【請求項１２】
前記アンマネージドデバイスを前記アンマネージドデバイスグループに追加することを決定するステップは、前記アンマネージドデバイスがセキュリティ脅威をもたらすことを決定するステップを含むことを特徴とする請求項１１に記載の方法。
【請求項１３】
前記変更されたアクターセットを記述している前記情報および前記指示を送るステップは、前記アンマネージドデバイスから生じたインバウンドネットワークトラフィックを前記特定のマネージドサーバにブロックさせること、または前記アンマネージドデバイスに向けられたアウトバウンドネットワークトラフィックを前記特定のマネージドサーバにブロックさせることを特徴とする請求項１１に記載の方法。
【請求項１４】
前記ルールの各々は、次元を表しているラベル、および、前記ラベルに対応しているマネージドサーバに関連付けられた前記次元の値を使用して、前記サービスの前記プロバイダおよび前記サービスの前記ユーザの少なくとも１つを参照することを特徴とする請求項１に記載の方法。
【請求項１５】
前記キャッシュされたアクターセットの各々は１つまたは複数のアクターセットレコードを含み、各アクターセットレコードはマネージドサーバまたはアンマネージドデバイスグループを識別することを特徴とする請求項１に記載の方法。
【請求項１６】
前記アクターセットレコードの少なくとも１つは、ユニークな識別子、オペレーティングシステムの識別子、またはＩＰアドレスを含むことを特徴とする請求項１５に記載の方法。
【請求項１７】
管理ドメイン内の不良アクターを隔離するコンピュータプログラムモジュールを格納している非一時的コンピュータ可読記憶媒体であって、プロセッサによって実行可能な前記コンピュータプログラムモジュールは、
キャッシュされたアクターセットを格納するステップであって、前記キャッシュされたアクターセットの各々は、前記管理ドメイン内に存在するアクターのグループを指定する、ステップと、
特定のマネージドサーバに適用可能な複数のルールを格納するステップであって、前記ルールの各々は、サービスのプロバイダ、前記サービスのユーザ、および前記サービスの前記プロバイダと前記ユーザとの間の対話を制御している機能を指定する、ステップと、
前記複数のルールの所与のルールに関連して、各々が前記所与のルールにおいて指定された前記プロバイダ、および、前記所与のルールに指定された前記ユーザの少なくとも１つを含む前記キャッシュされたアクターセットのサブセットを含んでいる関連アクターセットを格納するステップと、
前記不良アクターを隔離するための指示を受信するステップと、
前記キャッシュされたアクターセットを更新して、前記不良アクターの状態における隔離された状態への変化を示すステップと、
前記所与のルールに対する前記関連アクターセットにおける変更されたアクターセットを識別するステップであって、前記変更されたアクターセットは、前記不良アクターの状態における前記隔離された状態への前記変化に基づいて更新されたものである、ステップと、
前記変更されたアクターセットを識別するステップに応答して、

前記変更されたアクターセットを記述している情報、および、前記特定のマネージドサーバによって格納されたローカルリストにおける前記変更されたアクターセットを追加、削除または変更するための指示を前記特定のマネージドサーバに送るステップと
を含んでいるステップを実行することを特徴とする非一時的コンピュータ可読記憶媒体。

【請求項１８】
前記ルールの各々は、次元を表しているラベル、および、前記ラベルに対応しているマネージドサーバに関連付けられた前記次元の値を使用して、前記サービスの前記プロバイダおよび前記サービスの前記ユーザの少なくとも１つを参照することを特徴とする請求項１７に記載の非一時的コンピュータ可読記憶媒体。

【請求項１９】
管理ドメイン内の不良アクターを隔離するシステムであって、前記システムは、
キャッシュされたアクターセットを格納するステップであって、前記キャッシュされたアクターセットの各々は、前記管理ドメイン内に存在するアクターのグループを指定する、ステップと、
特定のマネージドサーバに適用可能な複数のルールを格納するステップであって、前記ルールの各々は、サービスのプロバイダ、前記サービスのユーザ、および前記サービスの前記プロバイダと前記ユーザとの間の対話を制御している機能を指定する、ステップと、
前記複数のルールの所与のルールに関連して、各々が前記所与のルールにおいて指定された前記プロバイダ、および、前記所与のルールに指定された前記ユーザの少なくとも１つを含む前記キャッシュされたアクターセットのサブセットを含んでいる関連アクターセットを格納するステップと、
前記不良アクターを隔離するための指示を受信するステップと、
前記キャッシュされたアクターセットを更新して、前記不良アクターの状態における隔離された状態への変化を示すステップと、
前記所与のルールに対する前記関連アクターセットにおける変更されたアクターセットを識別するステップであって、前記変更されたアクターセットは、前記不良アクターの状態における前記隔離された状態への前記変化に基づいて更新されたものである、ステップと、
前記変更されたアクターセットを識別するステップに応答して、
前記変更されたアクターセットを記述している情報、および、前記特定のマネージドサーバによって格納されたローカルリストにおける前記変更されたアクターセットを追加、削除または変更するための指示を前記特定のマネージドサーバに送るステップと
を含んでいるステップを実行するための実行可能なコンピュータプログラムモジュールを格納している非一時的コンピュータ可読記憶媒体と、
前記コンピュータプログラムモジュールを実行するコンピュータプロセッサと
を備えたことを特徴とするシステム。

【請求項２０】
前記ルールの各々は、次元を表しているラベル、および、前記ラベルに対応しているマネージドサーバに関連付けられた前記次元の値を使用して、前記サービスの前記プロバイダおよび前記サービスの前記ユーザの少なくとも１つを参照することを特徴とする請求項１９に記載のシステム。