【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】令和2年3月26日(2020.3.26)

【公表番号】特表2019-510304(P2019-510304A)
【公表日】平成31年4月11日(2019.4.11)
【年通号数】公開・登録公報2019-014
【出願番号】特願2018-544782(P2018-544782)
【国際特許分類】
Ｇ０６Ｆ　21/57　　(2013.01)
【ＦＩ】
Ｇ０６Ｆ　21/57　　３７０

【手続補正書】
【提出日】令和2年2月10日(2020.2.10)
【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】
セキュリティ管理システムのコンピュータシステムにおいて、
組織のネットワーク上のユーザによるネットワーク・アクティビティについてのデータを取得するステップと、
前記ネットワーク・アクティビティについてのデータを使用して、前記ネットワーク上で前記ユーザがアクセスしたアプリケーションを特定するステップと、
前記ネットワーク・アクティビティについてのデータを使用して、前記ユーザがアクセスしたアプリケーションに対応する前記ネットワーク・アクティビティについてのアクセス情報を特定するステップと、
前記アクセス情報を使用して、前記アプリケーションについてのドメイン情報を検索するステップと、
前記アプリケーションについてのセキュリティ情報を求めるステップと、
前記セキュリティ情報を使用して、前記アクセスされたアプリケーションの安全度合いを演算するステップと、
前記安全度合いに基づいてセキュリティポリシーを適用することによって、前記アプリケーションに対する救済操作を実行するステップとを含む、コンピュータにより実現される方法。
【請求項２】
前記セキュリティ情報は、前記アプリケーションによる第１のセキュリティ脅威の第１インジケータである第１の値を含み、前記アプリケーションによる第２のセキュリティ脅威の第２インジケータである第２の値を含み、前記第１インジケータは、第１のデータソースから取得され、前記第２インジケータは、第２のデータソースから取得される、請求項１に記載のコンピュータにより実現される方法。
【請求項３】
前記安全度合いを演算するステップは、
前記第１の値に第１の重み値を乗算することに基づいて第１の重み付き値を演算するステップと、
前記第２の値に第２の重み値を乗算することに基づいて第２の重み付き値を演算するステップと、

前記第１の重み付き値と前記第２の重み付き値との総和に基づく重み付き総和を演算するステップと、
前記第１の重み値と前記第２の重み値との総和に基づく重み総和を演算するステップとを含み、
前記安全度合いは、前記重み付き総和を前記重み総和で除算することに基づいて演算される値である、請求項２に記載のコンピュータにより実現される方法。
【請求項４】
前記ネットワーク・アクティビティについてのデータを取得するステップは、前記ネットワーク上の１つ以上のネットワーク機器からネットワークデータを取得するステップを含み、前記ネットワークは、パブリックネットワークに対して安全であるセキュアな前記組織のコンピューティング環境において保護される、請求項１～３のいずれか１項に記載のコンピュータにより実現される方法。
【請求項５】
前記アプリケーションの組織情報を特定するステップと、
前記アプリケーションについての情報を表示するグラフィカルインタフェースを生成するステップとをさらに含み、前記アプリケーションについての情報は、前記組織情報と、前記アプリケーションについて演算された安全度合いとに基づいて表示され、前記グラフィカルインタフェースは、前記アプリケーションに対して行われた前記救済操作を示す、請求項１～４のいずれか１項に記載のコンピュータにより実現される方法。
【請求項６】
前記データは、前記ネットワーク上の通信用のデータであり、前記アプリケーションを特定するステップは、前記データを処理して、前記ユーザがアクセスしたアプリケーションの要求に対応する、前記データの部分を識別するステップを含み、前記データの部分は、前記アプリケーションの要求についてのアプリケーション情報を示し、前記アプリケーション情報は、前記アプリケーションが前記ユーザによってアクセスされたと特定するために使用される、請求項１～５のいずれか１項に記載のコンピュータにより実現される方法。
【請求項７】
前記アプリケーションに対応する前記ネットワーク・アクティビティについてのアクセス情報は、前記データの部分を使用して特定され、前記アクセス情報は、前記アプリケーションについての前記ネットワーク・アクティビティのタイムスタンプと、前記アプリケーションを提供するシステムのＩＰ（Internet Protocol）アドレスと、前記アプリケーションにアクセスするために使用されたデバイスのＭＡＣ（Media Access Control）アドレスと、前記ユーザについてのユーザ情報とを示す、請求項６に記載のコンピュータにより実現される方法。
【請求項８】
前記アクセス情報は、前記アプリケーションを提供するシステムのＩＰ（Internet Protocol）アドレスを示し、前記ドメイン情報を検索するステップは、前記第１アプリケーションのＩＰアドレスに基づいて、前記アプリケーションをホストするドメインに対応する前記ドメイン情報を求めるクエリを実行するステップを含む、請求項１～７のいずれか１項に記載のコンピュータにより実現される方法。
【請求項９】
前記アクセス情報は、前記アプリケーションのソース情報を示し、前記ソース情報は、ホストが提供する前記アプリケーションの場所を示し、前記ドメイン情報を検索するステップは、前記アプリケーションのソース情報に基づいて前記アプリケーションの認証を求める要求を前記ホストに送るステップを含む、請求項１～８のいずれか１項に記載のコンピュータにより実現される方法。
【請求項１０】
前記安全度合いに基づいてセキュリティポリシーを適用するステップは、前記安全度合いが前記アプリケーションのリスク閾値を満たすかどうかを決定するステップを含み、前

記救済操作は、前記アプリケーションが前記ネットワーク上で前記ユーザによってアクセスされないよう、前記ネットワークを設定することである、請求項１～９のいずれか１項に記載のコンピュータにより実現される方法。
【請求項１１】
セキュリティ管理システムのコンピュータシステムにおいて、
ユーザが第１のサービスプロバイダシステムからアクセスした第１アプリケーションについての第１データを、前記第１のサービスプロバイダシステムから取得するステップと、
前記ユーザが第２のサービスプロバイダシステムからアクセスした第２アプリケーションについての第２データを、前記第２のサービスプロバイダシステムから取得するステップと、
前記第１データおよび前記第２データを使用して、前記ユーザがアクセスした第３アプリケーションのアクセス情報を特定するステップと、
前記アクセス情報を使用して、前記第３アプリケーションを提供するプロバイダシステムについてのドメイン情報を検索するステップと、
前記第３アプリケーションについてのセキュリティ情報を求めるステップと、
前記セキュリティ情報を使用して、アクセスされた前記第３のアプリケーションの安全度合いを演算するステップと、
前記安全度合いに基づいてセキュリティポリシーを適用することによって、前記第３アプリケーションに対する救済操作を実行するステップとを含む、コンピュータにより実現される方法。
【請求項１２】
第１のサービスプロバイダシステムは、第２のサービスプロバイダシステムとは異なり、前記第１のサービスプロバイダシステムは、前記第１アプリケーションへのアクセスを、第１のクラウドサービスとして提供し、前記第２のサービスプロバイダシステムは、前記第２アプリケーションへのアクセスを、第２のクラウドサービスとして提供する、請求項１１に記載のコンピュータにより実現される方法。
【請求項１３】
前記第３アプリケーションの組織情報を特定するステップと、
前記第３アプリケーションについての情報を表示するグラフィカルインタフェースを生成するステップとをさらに含み、前記アプリケーションについての情報は、前記第３アプリケーションの前記組織情報と、演算された前記安全度合いとに基づいて表示され、前記グラフィカルインタフェースは、前記第３アプリケーションに対して実行された救済操作を示す、請求項１１または１２に記載のコンピュータにより実現される方法。
【請求項１４】
前記第１データは、前記第１アプリケーションが、前記第３アプリケーションを通して前記ユーザによってアクセスされたことを示し、前記第２データは、前記第２アプリケーションが、前記第３アプリケーションを通して前記ユーザによってアクセスされたことを示し、前記アクセス情報を特定ステップは、前記第１アプリケーションおよび前記第２アプリケーションへのアクセスを提供するために前記第３アプリケーションがアクセスされたと判定するステップを含む、請求項１１～１３のいずれか１項に記載のコンピュータにより実現される方法。
【請求項１５】
前記セキュリティ情報は、前記アプリケーションによる第１のセキュリティ脅威の第１インジケータである第１の値を含み、前記アプリケーションによる第２のセキュリティ脅威の第２インジケータである第２の値を含み、前記第１インジケータは、第１のソースから取得され、前記第１の値は、前記第２の値とは異なり、前記第２インジケータは、第２のソースから取得され、前記安全度合いを演算するステップは、
前記第１の値に第１の重み値を乗算することに基づいて第１の重み付き値を演算するステップと、

前記第２の値に第２の重み値を乗算することに基づいて第２の重み付き値を演算するステップとを含み、前記第１の重み値は、前記第２の重み値とは異なり、さらに、

前記第１の重み付き値と前記第２の重み付き値との総和に基づく重み付き総和を演算するステップと、

前記第１の重み値と前記第２の重み値との総和に基づく重み総和を演算するステップとを含み、

前記安全度合いは、前記重み付き総和を前記重み総和で除算することに基づいて演算される値である、請求項１１～１４のいずれか１項に記載のコンピュータにより実現される方法。

【請求項１６】

請求項１～１５のいずれか１項に記載の方法をコンピュータに実行させる、プログラム。

【請求項１７】

１つ以上のプロセッサと、

請求項１６に記載のプログラムを格納したメモリとを備える、システム。