【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11月26日(2020.11.26)

【公表番号】特表2019-533258(P2019-533258A)
【公表日】令和1年11月14日(2019.11.14)
【年通号数】公開・登録公報2019-046
【出願番号】特願2019-522880(P2019-522880)
【国際特許分類】
Ｇ０６Ｆ　21/56　　(2013.01)
【ＦＩ】
Ｇ０６Ｆ　21/56

【手続補正書】
【提出日】令和2年10月14日(2020.10.14)
【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】
ターゲットエンティティと、評判マネージャと、アンチマルウェアエンジンとを実行するように構成された少なくとも１つのハードウェアプロセッサを備えるクライアントシステムであって、
前記評判マネージャは、
評判サーバから、ターゲットエンティティの第１の評判インジケータであって、前記ターゲットエンティティが悪意のあるものである確率を示す前記第１の評判インジケータを受信したことに応答して、前記評判インジケータを前記アンチマルウェアエンジンに送信することと、
前記第１の評判インジケータを受信したことに応答して、前記ターゲットエンティティが第１の時間間隔中に所定のアクションのセットのうちのいずれかを実施したかどうかを判定することと、
前記ターゲットエンティティが前記第１の時間間隔中に所定のアクションの前記セットのうちのいずれをも実施しなかったときに、前記ターゲットエンティティの第２の評判インジケータを決定することであって、前記第２の評判インジケータは、前記ターゲットエンティティが悪意のあるものである可能性が、前記第１の評判インジケータによって示されたものよりも低いことを示す、決定することと、
前記第２の評判インジケータを決定したことに応答して、前記第２の評判インジケータを前記アンチマルウェアエンジンと前記評判サーバとに送信することと、
前記ターゲットエンティティが所定のアクションの前記セットのうちの第１のアクションを実施したときに、前記ターゲットエンティティの第３の評判インジケータを決定することであって、前記第３の評判インジケータは、前記ターゲットエンティティが悪意のあるものである可能性が、前記第１の評判インジケータによって示されたものよりも高いことを示す、決定することと、
前記第３の評判インジケータを決定したことに応答して、前記第３の評判インジケータを前記アンチマルウェアエンジンと前記評判サーバとに送信することと
を行うように構成され、
前記アンチマルウェアエンジンは、
前記第１の評判インジケータを受信したことに応答して、前記ターゲットエンティテ

ィが悪意のあるものであるかどうかを判定するために、第１のプロトコルを利用することと、
　前記第２の評判インジケータを受信したことに応答して、前記ターゲットエンティティが悪意のあるものであるかどうかを判定するために、第２のプロトコルを利用することであって、前記第２のプロトコルは前記第１のプロトコルよりも計算コストが高くない、利用することと、
　前記第３の評判インジケータを受信したことに応答して、前記ターゲットエンティティが悪意のあるものであるかどうかを判定するために、第３のプロトコルを利用することであって、前記第３のプロトコルは前記第１のプロトコルよりも計算コストが高い、利用することと
を行うように構成された、
クライアントシステム。
【請求項２】
請求項１に記載のクライアントシステムであって、前記評判マネージャは、
　前記第２の評判インジケータまたは前記第３の評判インジケータを決定したことに応答して、前記第１の時間間隔の後の第２の時間間隔を決定することと、
　前記第２の時間間隔を決定したことに応答して、前記ターゲットエンティティが前記第２の時間間隔中に所定のアクションの前記セットのうちのいずれかを実施したかどうかを判定することと、
　それに応答して、前記ターゲットエンティティが前記第２の時間間隔中に所定のアクションの前記セットのうちのいずれをも実施しなかったときに、前記ターゲットエンティティの第４の評判インジケータを決定することであって、前記第４の評判インジケータは、前記ターゲットエンティティが悪意のあるものである可能性が、前記第２の評判インジケータによって示されたものよりも低いことを示す、決定することと
を行うようにさらに構成された、クライアントシステム。
【請求項３】
請求項１に記載のクライアントシステムであって、前記第２の評判インジケータは、前記ターゲットエンティティの起動から経過した時間に従って決定される、クライアントシステム。
【請求項４】
請求項１に記載のクライアントシステムであって、前記第１の時間間隔は、前記ターゲットエンティティの起動から経過した時間に従って決定される、クライアントシステム。
【請求項５】
請求項１に記載のクライアントシステムであって、前記第１の時間間隔は、前記第１の評判インジケータに従って決定される、クライアントシステム。
【請求項６】
請求項１に記載のクライアントシステムであって、前記第１の時間間隔は、前記ターゲットエンティティが、前記第１の時間間隔より前に、所定のアクションの前記セットのうちの第２のアクションを実施したかどうかに従って決定される、クライアントシステム。
【請求項７】
請求項１に記載のクライアントシステムであって、前記第２の評判インジケータを決定することは、前記ターゲットエンティティが悪意のあるものである前記確率を、前記ターゲットエンティティの起動から経過した時間に従って決定された量だけ減少させることを含む、クライアントシステム。
【請求項８】
請求項１に記載のクライアントシステムであって、前記第３の評判インジケータを決定することは、前記ターゲットエンティティが悪意のあるものである前記確率を、前記第１のアクションのタイプに従って決定された量だけ増加させることを含む、クライアントシステム。
【請求項９】

請求項１に記載のクライアントシステムであって、前記第３の評判インジケータを決定することは、前記ターゲットエンティティが悪意のあるものである前記確率を、前記ターゲットエンティティが前記第１のアクションより前に第２のアクションを実施したかどうかに従って決定された量だけ増加させること含む、クライアントシステム。
【請求項１０】
請求項１に記載のクライアントシステムであって、前記評判マネージャは、
前記第３の評判インジケータを決定したことに応答して、前記ターゲットエンティティが所定のアクションの前記セットのうちの第２のアクションを実施したかどうかを判定することと、
それに応答して、前記ターゲットエンティティが前記第２のアクションを実施したときに、前記ターゲットエンティティの第４の評判インジケータを決定することであって、前記第４の評判インジケータは、前記ターゲットエンティティが悪意のあるものである可能性が、前記第３の評判インジケータによって示されたものよりも高いことを示す、決定することと
を行うようにさらに構成された、クライアントシステム。
【請求項１１】
請求項１に記載のクライアントシステムであって、前記評判マネージャは、
前記第３の評判インジケータを決定したことに応答して、前記クライアントシステム上で実行している別のエンティティの第４の評判インジケータを決定することであって、前記別のエンティティは前記ターゲットエンティティの構成要素を含む、決定すること
を行うようにさらに構成された、クライアントシステム。
【請求項１２】
請求項１に記載のクライアントシステムであって、前記第１のアクションは、前記ターゲットエンティティが、前記クライアントシステム上で実行している別のエンティティにコードのセクションを注入することを含み、前記評判マネージャは、前記第３の評判インジケータを決定したことに応答して、前記クライアントシステム上で実行している前記別のエンティティの第４の評判インジケータを決定することであって、前記第４の評判インジケータは、前記第４のエンティティが悪意のあるものである可能性が、前記ターゲットエンティティと同じくらいであることを示す、決定することを行うようにさらに構成された、クライアントシステム。
【請求項１３】
複数のクライアントシステムとの評判管理トランザクションを実施するように構成された少なくとも１つのハードウェアプロセッサを備えるサーバコンピュータシステムであって、評判管理トランザクションは、
前記複数のクライアントシステムのうちのクライアントシステムから受信された要求に応答して、エンティティ評判データベースからターゲットエンティティの第１の評判インジケータを取り出すことであって、前記第１の評判インジケータは前記ターゲットエンティティが悪意のあるものである確率を示す、取り出すことと、
前記第１の評判インジケータを取り出したことに応答して、前記第１の評判インジケータを前記クライアントシステムに送信することと、
前記第１の評判インジケータを送信したことに応答して、前記クライアントシステムから前記ターゲットエンティティの第２の評判インジケータを受信することと、
前記第２の評判インジケータを受信したことに応答して、前記第１の評判インジケータと前記第２の評判インジケータとを比較することと、
それに応答して、前記第２の評判インジケータが、前記ターゲットエンティティが悪意のあるものである確率が、前記第１の評判インジケータによって示されたものよりも低いことを示すときに、前記第２の評判インジケータを、前記複数のクライアントシステムから受信された評判インジケータの集合に追加することであって、前記集合のすべてのメンバーは、前記ターゲットエンティティのインスタンスについて決定される、追加することと、

前記第２の評判インジケータを前記集合に追加したことに応答して、評判更新条件が満たされるかどうかを判定することと、
それに応答して、前記更新条件が満たされたときに、前記評判データベース中の前記第１の評判インジケータを、前記集合に従って決定された更新された評判インジケータと置き換えることと
を含み、前記第２の評判インジケータを決定することは、
前記第１の評判インジケータを受信したことに応答して、前記ターゲットエンティティが第１の時間間隔中に所定のアクションのセットのうちのいずれかを実施したかどうかを判定することと、
前記ターゲットエンティティが前記第１の時間間隔中に所定のアクションの前記セットのうちのいずれをも実施しなかったときに、前記第２の評判インジケータを、前記ターゲットエンティティが悪意のあるものである可能性が、前記第１の評判インジケータによって示されたものよりも低いことを示すように、構築することと、
前記ターゲットエンティティが所定のアクションの前記セットのうちの第１のアクションを実施したときに、前記第２の評判インジケータを、前記ターゲットエンティティが悪意のあるものである可能性が、前記第１の評判インジケータによって示されたものよりも高いことを示すように、構築することと
を行うために、前記クライアントシステムを利用することを含む、
サーバコンピュータシステム。
【請求項１４】
請求項１３に記載のサーバコンピュータシステムであって、前記更新条件が満たされるかどうかを判定することは、第１のメンバーを前記集合に追加してから経過した時間を決定することを含む、サーバコンピュータシステム。
【請求項１５】
請求項１３に記載のサーバコンピュータシステムであって、前記更新条件が満たされるかどうかを判定することは、前記集合のメンバーのカウントを決定することを含む、サーバコンピュータシステム。
【請求項１６】
請求項１３に記載のサーバコンピュータシステムであって、前記更新評判インジケータを決定することは、前記集合のすべてのメンバーのうちで、前記ターゲットエンティティが悪意のあるものである確率が最も高いことを示すように、前記更新評判インジケータを構築することを含む、サーバコンピュータシステム。
【請求項１７】
請求項１３に記載のサーバコンピュータシステムであって、前記第２の評判インジケータを決定することは、前記ターゲットエンティティが悪意のあるものである可能性が、第３の評判インジケータによって示されたものよりも低いことを示すように、前記第２の評判インジケータを構築することをさらに含み、前記第３の評判インジケータを決定することは、
前記第２の評判インジケータを決定することに備えて、前記第１の時間間隔より前の第２の時間間隔を決定することと、
前記第２の時間間隔を決定したことに応答して、前記ターゲットエンティティが前記第２の時間間隔中に所定のアクションの前記セットのうちのいずれかを実施したかどうかを判定することと、
それに応答して、前記ターゲットエンティティが前記第２の時間間隔中に所定のアクションの前記セットのうちのいずれをも実施しなかったときに、前記第３の評判インジケータを、前記ターゲットエンティティが悪意のあるものである可能性が、前記第１の評判インジケータによって示されたものよりも低いことを示すように、構築することと
を行うために、前記クライアントシステムを利用することを含む、
サーバコンピュータシステム。
【請求項１８】

請求項１３に記載のサーバコンピュータシステムであって、前記第２の評判インジケータは、前記ターゲットエンティティの起動から経過した時間に従って決定される、サーバコンピュータシステム。
【請求項１９】
請求項１３に記載のサーバコンピュータシステムであって、前記第１の時間間隔は、前記ターゲットエンティティの起動から経過した時間に従って決定される、サーバコンピュータシステム。
【請求項２０】
請求項１３に記載のサーバコンピュータシステムであって、前記第１の時間間隔は、前記第１の評判インジケータに従って決定される、サーバコンピュータシステム。
【請求項２１】
請求項１３に記載のサーバコンピュータシステムであって、前記第１の時間間隔は、前記ターゲットエンティティが、前記第１の時間間隔より前に、所定のアクションの前記セットのうちの第２のアクションを実施したかどうかに従って決定される、サーバコンピュータシステム。
【請求項２２】
請求項１３に記載のサーバコンピュータシステムであって、前記第２の評判インジケータを決定することは、前記ターゲットエンティティが悪意のあるものである前記確率を、前記ターゲットエンティティの起動から経過した時間に従って決定された量だけ減少させることを含む、サーバコンピュータシステム。
【請求項２３】
命令のセットを記憶する非一時的コンピュータ可読媒体であって、命令の前記セットは、クライアントシステムのハードウェアプロセッサによって実行されたときに、前記クライアントシステムに、評判マネージャとアンチマルウェアエンジンとを形成させ、
前記クライアントシステムは、ターゲットエンティティを実行するように構成され、
前記評判マネージャは、
評判サーバから、ターゲットエンティティの第１の評判インジケータであって、前記ターゲットエンティティが悪意のあるものである確率を示す前記第１の評判インジケータを受信したことに応答して、前記評判インジケータを前記アンチマルウェアエンジンに送信することと、
前記第１の評判インジケータを受信したことに応答して、前記ターゲットエンティティが第１の時間間隔中に所定のアクションのセットのうちのいずれかを実施したかどうかを判定することと、
前記ターゲットエンティティが前記第１の時間間隔中に所定のアクションの前記セットのうちのいずれをも実施しなかったときに、前記ターゲットエンティティの第２の評判インジケータを決定することであって、前記第２の評判インジケータは、前記ターゲットエンティティが悪意のあるものである可能性が、前記第１の評判インジケータによって示されたものよりも低いことを示す、決定することと、
前記第２の評判インジケータを決定したことに応答して、前記第２の評判インジケータを前記アンチマルウェアエンジンと前記評判サーバとに送信することと、
前記ターゲットエンティティが所定のアクションの前記セットのうちの第１のアクションを実施したときに、前記ターゲットエンティティの第３の評判インジケータを決定することであって、前記第３の評判インジケータは、前記ターゲットエンティティが悪意のあるものである可能性が、前記第１の評判インジケータによって示されたものよりも高いことを示す、決定することと、
前記第３の評判インジケータを決定したことに応答して、前記第３の評判インジケータを前記アンチマルウェアエンジンと前記評判サーバとに送信することと
を行うように構成され、
前記アンチマルウェアエンジンは、
前記第１の評判インジケータを受信したことに応答して、前記ターゲットエンティテ

ィが悪意のあるものであるかどうかを判定するために、第１のプロトコルを利用することと、

前記第２の評判インジケータを受信したことに応答して、前記ターゲットエンティティが悪意のあるものであるかどうかを判定するために、第２のプロトコルを利用することであって、前記第２のプロトコルは前記第１のプロトコルよりも計算コストが高くない、利用することと、

前記第３の評判インジケータを受信したことに応答して、前記ターゲットエンティティが悪意のあるものであるかどうかを判定するために、第３のプロトコルを利用することであって、前記第３のプロトコルは前記第１のプロトコルよりも計算コストが高い、利用することと

を行うように構成された、

非一時的コンピュータ可読媒体。