【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22年12月16日(2010.12.16)

【公表番号】特表2008-522292(P2008-522292A)
【公表日】平成20年6月26日(2008.6.26)
【年通号数】公開・登録公報2008-025
【出願番号】特願2007-543583(P2007-543583)
【国際特許分類】
Ｇ０６Ｆ　21/20　　(2006.01)
Ｇ０６Ｆ　21/22　　(2006.01)
Ｇ０６Ｆ　21/24　　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　15/00　　３３０Ａ
Ｇ０６Ｆ　 9/06　　６６０Ｎ
Ｇ０６Ｆ　12/14　　５６０Ｃ

【手続補正書】
【提出日】平成22年10月7日(2010.10.7)
【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】
第一の複数のモジュールに対する第一の複数のシグネチャを格納するために設けられているデータベースと、
マシン内の第二の複数のモジュールに対応する第二の複数のシグネチャを受け取るためのレシーバと、
前記第二の複数のシグネチャのうちで受け取った少なくとも一つのシグネチャを前記データベース内の複数のシグネチャのうちの一つまたは複数のシグネチャと比較し、対応するシグネチャが前記データベース内で見つかる前記第二の複数のモジュールの第一のサブセットを識別し、対応するシグネチャが前記データベース内で見つからない前記第二の複数のモジュールの第二のサブセットを識別する動作をするバリデータと、
対応するシグネチャが前記データベース内で見つかる前記第二の複数のモジュールの前記第一のサブセットおよび対応するシグネチャが前記データベース内で見つからない前記第二の複数のモジュールの前記第二のサブセットに基づいて前記マシンに対するトラストスコアを生成するためのトラストスコアジェネレータと、
を有する装置。
【請求項２】
前記第一の複数のモジュールに対する前記第一の複数のシグネチャが、前記複数のモジュールに対する第一の複数のハッシュを含んでいる請求項１に記載の装置。
【請求項３】
前記装置は、さらに、対応するシグネチャが前記データベース内で見つからない前記第二の複数のモジュールの前記第二のサブセットに対応するシグネチャを第二のデータベースへ送るトランスミッタを有しており、前記レシーバは、前記第二のデータベースから第二のトラストスコアを受け取る動作をし、前記トラストスコアジェネレータは、対応するシグネチャがデータベース内で見つかる前記複数のモジュールの前記第一のサブセットおよび前記第二のトラストスコアに基づいて前記トラストスコアを生成する動作をするよう

になっている請求項１に記載の装置。
【請求項４】
前記データベースは、前記第一の複数のモジュールに対する第一の複数の識別子を格納するために設けられており、前記レシーバは、前記第二の複数のモジュールに対する第二の複数の識別子を受け取る動作をし、前記バリデータは、前記マシン内の前記複数のモジュールに対する前記第二の複数の識別子を用いて、前記第二の複数のシグネチャと前記データベース内の前記複数のシグネチャを比較する動作をするようになっている請求項１に記載の装置。
【請求項５】
さらに、リソースに対するアクセスを制御するためのポリシーを有しており、前記ポリシーが前記リソースに対する完全なアクセスをする資格を得るためのスレッショルドスコアを含んでいる請求項１に記載の装置。
【請求項６】
さらに、前記ポリシーが前記リソースに対する部分的なアクセスをする資格を得るための第二のスレッショルドスコアを含んでいる請求項５に記載の装置。
【請求項７】
前記レシーバは、モジュールのシグネチャを受け取り前記データベースへ加えるように動作をする請求項１に記載の装置。
【請求項８】
ネットワークと、
前記ネットワークに接続されたリソースと、
第一の複数のモジュールに対する第一の複数のシグネチャを含むインテグリティログを生成するためのインテグリティログジェネレータを有している前記ネットワークに接続されたコンピュータと、
前記ネットワークに接続されている装置と、を備え、該装置は、
第二の複数のモジュールに対する第二の複数のシグネチャを格納するために設けられているデータベースと、
前記コンピュータから前記インテグリティログを受け取るためのレシーバと、
前記インテグリティログと前記第一の複数のシグネチャの比較に基づいたトラストスコアを生成するためのトラストスコアジェネレータと、
前記リソースに対するアクセスを制御するためのポリシーと、を有しており、前記ポリシーは、前記リソースに対する完全なアクセスをする資格を得るためのスレッショルドスコアを含んでおり、前記リソースに対する前記コンピュータのアクセスが前記ポリシーにより制御されることを特徴とするシステム。
【請求項９】
前記システムは、さらに、第二の装置を含んでおり、前記第二の装置は、第三の複数のモジュールに対する第三の複数のシグネチャを格納するために設けられている第二のデータベースを有しており、前記装置は、対応するシグネチャが前記データベース内で見つからない前記第一の複数のモジュールのサブセットに対応するシグネチャを前記第二の装置に送るためのトランスミッタを有している請求項８に記載のシステム。
【請求項１０】
さらに、第二のネットワークを有しており、前記装置と前記第二の装置が前記第二のネットワークに接続されている請求項９に記載のシステム。
【請求項１１】
マシン内の複数のモジュールに対応する第一の複数のシグネチャを受け取るステップと、
前記複数のモジュールに対する前記第一の複数のシグネチャをデータベース内の第二の複数のシグネチャと比較するステップと、
対応するシグネチャが前記データベース内で見つかる前記複数のモジュールの第一のサブセットおよび対応するシグネチャが該データベース内で見つからない該複数のモジュー

ルの第二のサブセットを識別するステップと、
対応するシグネチャが前記データベース内で見つかる前記複数のモジュールの前記第一のサブセットおよび対応するシグネチャが該データベース内で見つからない該複数のモジュールの前記第二のサブセットに基づいて前記マシンに対するトラストスコアを生成するステップと、
を含む方法。
【請求項１２】
さらに、前記トラストスコアに基づいてネットワーク上のリソースに対するアクセスを制御するステップを含む請求項１１に記載の方法。
【請求項１３】
前記トラストスコアに基づいてネットワーク上のリソースに対するアクセスを制御するステップが、前記ネットワーク上の前記リソースに対するアクセスに対するポリシーにアクセスするステップと、前記ポリシーを用い、前記トラストスコアに基づいて前記リソースに対するアクセスを制御するステップと、を含んでいる請求項１２に記載の方法。
【請求項１４】
前記ポリシーを用い、前記トラストスコアに基づいて前記リソースに対するアクセスを制御するステップは、前記トラストスコアが前記ポリシーにしたがってスレッショルドスコアを超える場合、前記リソースに対する完全なアクセスを許可するステップを含む請求項１３に記載の方法。
【請求項１５】
前記ポリシーを用い、前記トラストスコアに基づいて前記リソースに対するアクセスを制御するステップは、前記トラストスコアが前記ポリシーにしたがって第二のスレッショルドスコア未満で第一のスレッショルドスコアより大きい場合、前記リソースに対する部分的なアクセスを許可するステップを含む請求項１３に記載の方法。
【請求項１６】
前記ポリシーを用い、前記トラストスコアに基づいて前記リソースに対するアクセスを制御するステップは、前記トラストスコアが前記ポリシーに係るスレッショルドスコア未満である場合、前記リソースに対するアクセスを拒否するステップを含む請求項１３に記載の方法。
【請求項１７】
前記トラストスコアを生成するステップは、前記トラストスコアを生成する際に、少なくとも第一のモジュールを少なくとも第二のモジュールよりも大きく重み付けるステップを含む請求項１１に記載の方法。
【請求項１８】
前記第一の複数のシグネチャを受け取るステップは、前記複数のモジュールに対応する前記第一の複数のシグネチャを含んでいるインテグリティログを受け取るステップを含む請求項１１に記載の方法。
【請求項１９】
前記方法は、さらに、
対応するシグネチャが前記データベース内で見つからない前記複数のモジュールの前記第二のサブセットに対応する前記シグネチャを第二のデータベースに送るステップと、
対応するシグネチャが前記第二のデータベース内で見つかる前記複数のモジュールの第三のサブセットおよび対応するシグネチャが前記第二のデータベース内で見つからない前記複数のモジュールの第四のサブセットを前記第二のデータベースから受け取るステップと、
を含み、
前記トラストスコアを生成するステップは、対応するシグネチャが前記データベース内で見つかる前記複数のモジュールの前記第一のサブセットおよび対応するシグネチャが前記第二のデータベース内で見つかる前記複数のモジュールの前記第三のサブセットに基づいて前記トラストスコアを生成するステップを含む請求項１１に記載の方法。

【請求項２０】
前記複数のモジュールに対応する第一の複数のシグネチャを受け取るステップは、前記第一の複数のシグネチャおよび前記複数のモジュールに対する複数の識別子を受け取るステップを含み、
前記複数のモジュールに対する前記第一の複数のシグネチャをデータベース内の第二の複数のシグネチャと比較するステップは、前記複数のモジュールに対する前記第一の複数のシグネチャを、前記複数のモジュールに対する前記複数の識別子を用いて、前記データベース内の第二の複数のシグネチャと比較するステップを含む請求項１１に記載の方法。
【請求項２１】
さらに、前記トラストスコアを前記マシンに送信するトランスミッタを有する請求項１に記載の装置。
【請求項２２】
さらに、前記トラストスコアを前記コンピュータに送信するトランスミッタを有する請求項８に記載のシステム。
【請求項２３】
さらに、前記トラストスコアを前記マシンに送信するステップを含む請求項１１に記載の方法。