【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3月1日(2018.3.1)

【公表番号】特表2017-512329(P2017-512329A)
【公表日】平成29年5月18日(2017.5.18)
【年通号数】公開・登録公報2017-018
【出願番号】特願2016-549102(P2016-549102)
【国際特許分類】
Ｇ０６Ｆ　21/56　(2013.01)
Ｇ０６Ｆ　17/30　(2006.01)
Ｈ０４Ｌ　12/66　(2006.01)
Ｈ０４Ｌ　12/723　(2013.01)
【ＦＩ】
Ｇ０６Ｆ　21/56　３６０
Ｇ０６Ｆ　17/30　２２０Ｂ
Ｈ０４Ｌ　12/66　Ｂ
Ｈ０４Ｌ　12/723

【手続補正書】
【提出日】平成30年1月17日(2018.1.17)
【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】
コンピュータによって実施される方法であって、
システムコンポーネントに関連付けられたイベントを検出するステップと、
構成可能なポリシーに基づいて前記イベントをフィルタリングするステップと、
前記検出するステップおよび前記フィルタリングするステップに少なくとも部分的に基づいて、前記システムコンポーネントを表しているデータオブジェクトにタグを割り当てるステップと、
を備えたことを特徴とする方法。
【請求項２】
前記検出するステップ、前記フィルタリングするステップ、および前記割り当てるステップは、カーネルレベルセキュリティエージェントによって行われることを特徴とする請求項１に記載の方法。
【請求項３】
前記タグは、文字列、整数、ハッシュ値、またはバイナリフラグの一つであることを特徴とする請求項１に記載の方法。
【請求項４】
前記構成可能なポリシーに少なくとも部分的に基づいて、前記イベントの前記検出を表しているデータオブジェクトに別のタグを割り当て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５】
前記タグは、別のタグを暗示するか、または別のタグと相互に排他的であることができることを特徴とする請求項１に記載の方法。
【請求項６】

前記割り当てるステップは、前記データオブジェクトよって表された前記システムコンポーネントの実際の動作、または特徴に少なくとも部分的に基づいていることを特徴とする請求項１に記載の方法。
【請求項７】
前記タグは、実行されたとき、前記データオブジェクトによって表された前記システムコンポーネントを分類し、前記システムコンポーネントの前記分類に関連付けられた新しいタグを割り当てるロジックに関連付けられたことを特徴とする請求項１に記載の方法。
【請求項８】
前記システムコンポーネントを表している前記データオブジェクトに関連付けられた前記タグに少なくとも部分的に基づいて、決定することまたは報告を生成することの少なくとも一つを行う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９】
ユーザが、前記タグを、前記データオブジェクトによって表された前記システムコンポーネントと関連付けることを可能にするステップと、
前記ユーザが、前記タグを、前記システムコンポーネントと関連付けることに少なくとも部分的に基づいて、前記データオブジェクトへの前記タグの前記割り当てを行うステップと、
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１０】
前記タグは、前記ユーザ、または別のエンティティの別のユーザによって前記システムコンポーネントと関連付けられたタグをサブスクライブする一つのエンティティの１または複数の他のユーザで共有可能であることを特徴とする請求項９に記載の方法。
【請求項１１】
コンピュータによって実施される方法であって、
複数のシステムコンポーネントに関連付けられたイベントを検出するステップと、
構成可能なポリシーと前記イベントの検出に少なくとも部分的に基づいて、前記複数のシステムコンポーネントの一つを表しているデータオブジェクトに割り当てられたタグを、前記複数の別のシステムコンポーネントを表している別のデータオブジェクトに伝播するステップと、
を備えたことを特徴とする方法。
【請求項１２】
前記タグは、文字列、整数、ハッシュ値、またはバイナリフラグの一つであることを特徴とする請求項１１に記載の方法。
【請求項１３】
前記伝播するステップは、前記構成可能なポリシーに少なくとも部分的に基づいて、前記データオブジェクトに割り当てられた複数のタグのすべてより少ないタグを伝播するステップを備えたことを特徴とする請求項１１に記載の方法。
【請求項１４】
前記伝播するステップは、前記構成可能なポリシーに少なくとも部分的に基づいて、前記タグを前記複数のシステムコンポーネントのサブセットを表しているデータオブジェクトに伝播するステップを備えたことを特徴とする請求項１１に記載の方法。
【請求項１５】
前記タグは、前記別のデータオブジェクトに関連付けられた別のタグと相互に排他的であり、前記方法は、タグ衝突を示すイベントを生成するステップをさらに備えたことを特徴とする請求項１１に記載の方法。
【請求項１６】
前記システムコンポーネントは、モジュール、プロセス、スレッド、ファイル、ドライバ、サービス、パイプ、ハンドル、名付けられたカーネルオブジェクト、メモリセグメント、ユーザ、暗号の署名者と署名権限、登録キー、インターネット・プロトコル（ＩＰ）アドレスとサブネット、ドメインネームサービス（ＤＮＳ）ドメイン、または完全修飾ド

メイン名（ＦＱＤＮｓ）の少なくとも一つを含むことを特徴とする請求項１１に記載の方法。
【請求項１７】
前記タグは、前記複数のシステムコンポーネントの少なくともサブセットのインスタンスを表すツリーオブジェクトに関連付けられたことを特徴とする請求項１１に記載の方法。
【請求項１８】
前記システムコンポーネントは、コンピューティングデバイスのシステムコンポーネントであり、前記伝播するステップは、１または複数の他のコンピューティングデバイスによって行われ、前記データオブジェクトと他のデータオブジェクトが、前記１または複数のコンピューティングデバイス上に記憶されていることを特徴とする請求項１１に記載の方法。
【請求項１９】
前記データオブジェクトによって表された前記システムコンポーネントが、第一のコンピューティングデバイスのシステムコンポーネントであって、前記別のデータオブジェクトによって表された前記別のシステムコンポーネントが、第二のコンピューティングデバイスのシステムコンポーネントであって、前記伝播するステップは、前記第一のコンピューティングデバイス、前記第二のコンピューティングデバイス、または第三の１または複数のコンピューティングデバイスのどれによっても行われることを特徴とする請求項１１に記載の方法。
【請求項２０】
プロセッサと、
前記プロセッサに接続されたメモリと、
を備えたシステムであって、
前記メモリは、複数のシステムコンポーネントを表しているデータオブジェクトと、
前記システムコンポーネントの少なくともサブセットのインスタンスの実行チェーンを表しているツリーオブジェクトと、
実行可能な指示であって、前記プロセッサによって実行されると、
前記ツリーオブジェクトのためのタグを、前記システムコンポーネントの前記サブセットを表している前記データオブジェクトに割り当てるステップと、
１または複数のタグを前記ツリーオブジェクトに割り当てるステップであって、それらのタグは、前記ツリーオブジェクトのための前記タグを有している前記データオブジェクトに適用するステップと、
前記システムコンポーネントの前記サブセットを表している前記データオブジェクトに割り当てられたタグ、およびツリーオブジェクトに割り当てられた前記タグに少なくとも部分的に基づいて、決定をするステップと、
を含む操作を行う、実行可能な指示と、
を格納することを特徴とするシステム。
【請求項２１】
前記操作は、システムコンポーネントの前記サブセットの別のシステムコンポーネントによって、前記システムコンポーネントの前記サブセットの一つのシステムコンポーネントの実行を検出するステップに応じて、前記ツリーオブジェクトを構成するステップをさらに含むことを特徴とする請求項２０に記載のシステム。
【請求項２２】
システムコンポーネントの前記サブセットは、プロセスおよび非プロセスシステムコンポーネントのどちらも含むことを特徴とする請求項２０に記載のシステム。
【請求項２３】
前記メモリは、複数のツリーオブジェクト、および前記複数のツリーオブジェクトによって表された実行チェーンの中に現れるシステムコンポーネントを表しているデータオブジェクトに割り当てられた前記複数のツリーオブジェクトのためのタグを記憶することを

特徴とする請求項２０に記載のシステム。
【請求項２４】
コンピューティングデバイスによって実行されたとき、
エンティティによって、別のエンティティのユーザによって指定されたタグをサブスクライブするステップであって、前記ユーザによって指定されたタグは、前記別のエンティティのコンピューティングデバイスのシステムコンポーネントを表しているデータオブジェクトに関連付けられているステップと、
前記別のエンティティのユーザによって指定されたタグを、前記エンティティのコンピューティングデバイスのシステムコンポーネントを表しているデータオブジェクトに割り当てるステップと、
前記別のエンティティのユーザによって指定されたタグに少なくとも部分的に基づいて決定をするステップと、
を備えた動作を前記コンピューティングデバイスに行わせる複数のプログラミング命令を記憶した１または複数の永続的なコンピュータで読み取り可能な媒体。
【請求項２５】
前記ユーザによって指定されたタグの一つは、未分類のシステムコンポーネントに適用された分類のタグであることを特徴とする請求項２４に記載の１または複数の永続的なコンピュータで読み取り可能な媒体。
【請求項２６】
ユーザによって指定されたタグは、サービスクラウドで共有され、およびタグ割り当てにおいてグローバルな変更を決定する際に前記サービスクラウドによって利用されることを特徴とする請求項２４に記載の１または複数の永続的なコンピュータで読み取り可能な媒体。