(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2017-512329
(P2017-512329A)
(43)公表日　平成29年5月18日(2017.5.18)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/56	(2013.01)	G06F	21/56	360	5K030
G06F 17/30	(2006.01)	G06F	17/30	220B	
H04L 12/66	(2006.01)	H04L	12/66	B	
H04L 12/723	(2013.01)	H04L	12/723		

審査請求 未請求　予備審査請求 未請求　（全 24 頁）

(21)出願番号　特願2016-549102 (P2016-549102)
(86)(22)出願日　平成27年1月29日 (2015.1.29)
(85)翻訳文提出日　平成28年7月28日 (2016.7.28)
(86)国際出願番号　PCT/US2015/013522
(87)国際公開番号　WO2015/116819
(87)国際公開日　平成27年8月6日 (2015.8.6)
(31)優先権主張番号　14/169,401
(32)優先日　平成26年1月31日 (2014.1.31)
(33)優先権主張国　米国 (US)

(71)出願人　514312332
クラウドストライク　インコーポレイテッド
アメリカ合衆国　９２６１８　カリフォルニア州　アーバイン　ラグーナ　キャニオン　ロード　１５４４０　スイート　２５０
(74)代理人　110001243
特許業務法人　谷・阿部特許事務所
(72)発明者　デイビット　エフ．ディール
アメリカ合衆国　５５４１７　ミネソタ州　ミネアポリス　エリオット　アベニュー　サウス　５３２４

最終頁に続く

(54)【発明の名称】セキュリティに関連のあるシステムオブジェクトのタグ付け

(57)【要約】
ここに記述される装置は、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間でタグを伝播するために構成される。そのような装置は、複数のシステムコンポーネントと関連付けられたイベントを検出することができる。イベントを検出すること、および構成可能なポリシーに少なくとも部分的に基づいて、装置は、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、別の複数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ことができる。そのようなタグの一つの例は、少なくともデータオブジェクトによって表されたシステムコンポーネントと、別のデータオブジェクトによって表された別のシステムコンポーネントのインスタンスの実行チェーンを表すツリーオブジェクトに関連付けられたものであることがある。そのようなタグの別の例は、装置に関連付けられたエンティティがサブスクライブする別のエンティティのユーザによって指定されたタグであることがある。

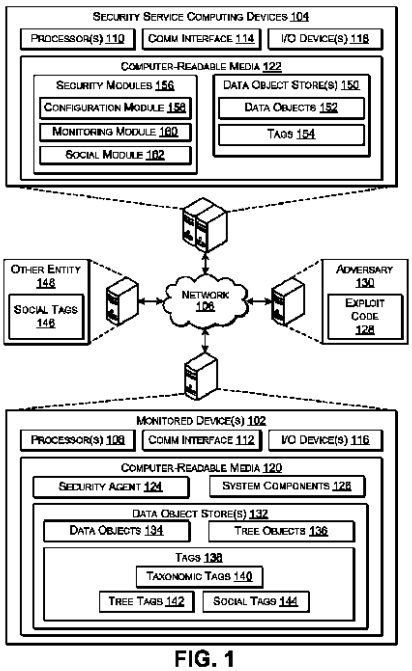


FIG. 1

【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すべてより小さ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、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、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る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。
【発明の詳細な説明】
【技術分野】
【０００１】

本願は、セキュリティに関連のあるシステムオブジェクトのタグ付けに関する。
【背景技術】
【０００２】
本願は、“Ｔａｇｇｉｎｇ　Ｓｅｃｕｒｉｔｙ－Ｒｅｌｅｖａｎｔ　Ｓｙｓｔｅｍ　Ｏｂｊｅｃｔｓ”と題され、２０１４年１月３１日に出願された米国特許出願第１４／１６９，４０１号に対して優先を主張する。米国特許出願第１４／１６９，４０１号は参照により本明細書に完全に組み込まれる。
【０００３】
インターネットの使用形態が日常生活の一部の中でますます大きくなるにつれて、システム資源、データ、および個人情報を盗み、または破壊する悪意のあるソフトウェア（しばしば“マルウェア”と言及される）や、他のセキュリティエクスプロイトの問題が増加している。政府、企業および個人は、これらのセキュリティエクスプロイトに関連した侵入、損害および窃盗を防ぐために重要な資源を費やすことがある。セキュリティエクスプロイトには多くの形態、例えば、コンピュータウイルス、ワーム、トロイの木馬、スパイウェア、キーストロークロガー、アドウェアおよびルートキット等で現れる。そのようなセキュリティエクスプロイトは様々な仕組み、例えば、フィッシングメール、悪意のあるクリック可能なリンク、感染したドキュメント、感染した実行ファイル、または感染したアーカイブ等で、またはそれを通じて届けられることができる。
【０００４】
これらの脅威に対処するためのツールは、システムコンポーネント、例えば、プロセスまたはファイル等のいくつかの面が、より多くの判定基準の一つに適合するかどうかテストする条件付きのロジックを適用することがある。判定基準を満たすことに基づいて、ツールはいくつかの行動または措置をとることがある。判定基準の修正は、特定されたシステムコンポーネントを改めることがあり、複雑になることがある。例えば、そのような修正は、ツールのソースコードの修正およびツールの再コンパイルを必要とすることがある。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】米国特許第１３／４９２，６７２号明細書
【特許文献２】米国特許第１３／７２８，７４６号明細書
【図面の簡単な説明】
【０００６】
詳細な説明は、付属の図に関して記述される。図では、参照番号の最も左の桁は、参照番号が最初に表示される図を識別する。異なる図の同じ参照番号の使用は、類似または同一の項目または特徴を示す。
【０００７】
【図１】監視対象装置とセキュリティサービスクラウドとの間の相互通信を可能にするためのフレームワークおよび装置の例を示す図である。
【図２】イベントに関連付けられたシステムコンポーネントの例として、構成可能なポリシーに基づくイベントのフィルタリング、およびイベントとフィルタリングに基づく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へのタグの割り当てを示す図である。
【図３】イベントに関連付けられたシステムコンポーネント、およびこれら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への伝播の例を示す図である。
【図４】システムコンポーネン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、ツリーオブジェクトへのタグの割り当て、および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へのツリーオブジェクトのためのタグの割り当ての例を示す図である。

【図５】一つのエンティティが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していること、およびそれらのユーザによって指定されたタグをエンティティの監視対象装置のデータオブジェクトの一つに割り当てることの例を示す図である。
【図６】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方法、およびこれら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、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ことの例を示しているフロー図である。
【発明を実施するための形態】
【０００８】
この開示は、セキュリティに関連のあるシステムイベント（以下、単に“イベント”）に関連付けられた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ための、およびそれらのイベントと構成可能なポリシーに基づいて、データオブジェクト間でタグを伝播するための技術および配置を含む。ここで使われるように、“タグ”という用語はデータオブジェクトのラベルまたは分類器の働きをするデータオブジェクトメタデータを指す。タグは、文字列、整数、ハッシュ値、バイナリフラグ、またはいくつかの他の効率的な表現であることができる。タグは報告、意思決定およびイベント生成のためのデータオブジェクトのフィルタリングを可能にし、どんな再コーディングまたは再コンパイルも必要としないデータオブジェクトの再分類を許可する。
【０００９】
様々な実施形態では、１または複数の監視対象装置はそれぞれ、それらの１または複数のコンピューティングデバイス上のそれぞれのイベントを監視するためのセキュリティエージェント、およびそれらのイベントに関連付けられたシステムコンポーネントを表すデータオブジェクトを維持するためのデータストアを備えることができる。それらの監視対象コンピューティングデバイスは、セキュリティサービスクラウドの装置と通信することができる。それらの監視対象コンピューティングデバイス上のイベントを監視し、セキュリティサービスクラウドのデータオブジェクトストアにあるそれらのイベントに関連付けられたシステムコンポーネントを表すデータオブジェクトを維持するように、セキュリティサービスクラウドを構成することもできる。セキュリティエージェントおよびセキュリティサービスクラウドは、同じイベント、異なるイベント、または重複しているイベントのセットを監視することができる。また、いくつかの実施形態では、セキュリティエージェントは、単にイベントを検出し、それらの検出したイベントをセキュリティサービスクラウドに通知することができる。セキュリティエージェントおよびセキュリティサービスクラウドのデータオブジェクトストアは、同じ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、異な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、または重複しているデータオブジェクトのセットを含むことができる。
【００１０】
セキュリティエージェントまたはセキュリティサービスクラウドは、構成可能なポリシーに基づいて、タグをデータオブジェクトに最初に割り当てることができる。そのようなタグは、システムコンポーネントのタイプ、機能、役割等を分類する“分類のタグ”と考慮されることがある。例えば、“ドキュメントプログラム”はそのような“分類のタグ”となることがある。セキュリティエージェントまたはセキュリティサービスクラウドは、システムコンポーネントが表す実際の動作または特徴に基づいて、タグをデータオブジェクトに割り当てることもできる。例えば、ドキュメントファイルを繰り返し開くプロセスの場合、セキュリティエージェントまたはセキュリティサービスクラウドは、タグ“ドキュメントプログラム”をプロセスに割り当てることができる。
【００１１】
セキュリティエージェントまたはセキュリティサービスクラウドは、イベントおよびそれらのイベントに関連付けられたシステムコンポーネントを検出するか、または通知されることができる。そのようなイベントは、プロセスが他のプロセスまたはスレッドを発生させること、プロセスを作成することまたはファイルを開くこと、等を含むことがある。

これらのイベントは、監視対象コンピューティングデバイス上で発生しているすべてのイベント、またはそれらのイベントのサブセットを含むことができる。サブセットの場合、セキュリティエージェントまたはセキュリティサービスクラウドは、セキュリティエージェントの設定または構成可能なポリシー（ここに使われるように、“構成可能なポリシー”は、セキュリティエージェントの設定、または、セキュリティエージェントまたはセキュリティサービスクラウドによって利用されるポリシーに言及することがある）に基づいて、イベントをフィルタに通すために構成されることができる。

【００１２】

検出されたイベントおよび構成可能なポリシーに基づいて、セキュリティエージェントまたはセキュリティサービスクラウドは、イベントに関連付けられたシステムコンポーネントを表している一つのデータオブジェクトに割り当てられたタグを、イベントに関連付けられた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ことができる。例えば、プロセスがファイルを作る場合、セキュリティエージェントまたはセキュリティサービスクラウドは、そのプロセスのためのデータオブジェクトの１または複数のタグを、そのファイルのためのデータオブジェクトに伝播することができる。セキュリティエージェントまたはセキュリティサービスクラウドは、構成可能なポリシーに少なくとも部分的に基づいて、プロセスのためのデータオブジェクトのタグのすべて、またはそれらのタグのサブセットだけを伝播することができる。また、伝播はどちらの方向でも起こることがあり、ファイルを表しているデータオブジェクトのタグは、プロセスを表しているデータオブジェクトに伝播されることもできる。別の例では、プロセスは多重スレッドを発生させることがあり、セキュリティエージェントまたはセキュリティサービスクラウドは、構成可能なポリシーに少なくとも部分的に基づいて、そのプロセスのためのデータオブジェクトの１または複数のタグを、すべてまたはそれらのスレッドのためのデータオブジェクトのサブセットだけに伝播することができる。

【００１３】

いくつかの実施形態では、セキュリティエージェントまたはセキュリティサービスクラウドは、検出されたイベントを表すデータオブジェクトを生成し、タグをそのデータオブジェクト、例えば、“疑わしいイベント”等に割り当てることができる。そのようなタグはその後のイベントの検出に応じて更新されることができる。例えば、最初のイベントが単に疑わしいだけの場合、２番目のイベントが起こるならばそれはセキュリティエクスプロイト行為であると後でみなされることがある。そのような場合、追加のコンテキスト（例えば、タグ“疑わしいイベント”を“エクスプロイト行為”に更新することができる）を反映するようにタグを更新することができる。

【００１４】

様々な実施形態では、セキュリティエージェントまたはセキュリティサービスクラウドは、イベントに関連付けられたシステムオブジェクトのインスタンスの実行チェーンを表すためにツリーオブジェクトを作ることもできる。例えば、イベントが別のプロセスを実行している一つのプロセスを含む場合、その実行チェーンをツリーオブジェクトの中に表すことができる。セキュリティエージェントまたはセキュリティサービスクラウドは、タグをツリーオブジェクトに割り当てることができ、ツリーオブジェクトタグをツリーオブジェクト内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ることができる。ツリーオブジェクトタグによって、ツリーオブジェクトに割り当てられたタグは、ツリーオブジェクトタグに割り当てられたデータオブジェクトのタグとして考慮されることがある。これはシステムコンポーネントの回顧の分類を可能にする。例えば、特定のプロセスについて、それが別のプロセスを最初に実行するとき、何も疑わしくないことがある。しかし、その他のプロセスがその後、さらにプロセスを実行し、さらなるプロセスがセキュリティエクスプロイト行為として認められる行動を行う場合、タグ“セキュリティエクスプロイト”は、実行チェーンを表しているツリーオブジェクトに割り当てられることができる。そして、そのツリーオブジェクトのためのツリーオブジェクトタグは、もとのプロセスに割り当てられるので、もとのプロセスが今度は、ツリーオブジェ

クトタグおよびツリーオブジェクトを通じて、タグ“セキュリティエクスプロイト”を有する。

【００１５】

さらなる実施形態では、セキュリティエージェントまたはセキュリティサービスクラウドは、ユーザが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ことを可能にすることができる。これらのユーザによって指定されたタグは、ユーザに関連付けられたエンティティのセキュリティエージェントによって利用されることができる。そのようなタグは、構成可能なポリシーでまだ分類されていなかったシステムコンポーネントを分類するために利用されることができる。例えば、特定のプロセスは、ドキュメントプログラムであることがあるが、構成可能なポリシーを利用しているセキュリティエージェントは、そのようなプロセスを認めないことができる。ユーザはタグ“ドキュメントプログラム”をそのプロセスを表しているデータオブジェクトに割り当てることができる。これらのユーザによって指定されたタグは、構成可能なポリシーおよび分類のタグを更新する際に、後に考慮されることができる。また、エンティティは、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ことがあり、その他のエンティティのユーザによって指定されたタグがエンティティのデータオブジェクトに割り当てられる原因となる。

【００１６】

いくつかの実施形態では、セキュリティエージェントまたはセキュリティサービスクラウドはその後、決定し、報告を生成し、またはイベントを生成するためでさえタグを利用することができる。例えば、伝播されたタグと衝突するタグが割り当てられていたデータオブジェクトにタグが伝播された場合、セキュリティエージェントまたはセキュリティサービスクラウドは、タグ衝突イベントを生成することができる。

【００１７】

追加的に、セキュリティエージェントまたはセキュリティサービスクラウドは、構成可能なポリシーの最新版に基づいて、データオブジェクトに割り当てられたタグを更新することができる。そのような更新は、セキュリティエージェントまたはセキュリティサービスクラウドの再コーディングまたは再コンパイルのような手間のかかる行為を行うことなしに、再分類を可能にすることができる。

【００１８】

フレームワークおよび装置の例

図１は、監視対象装置と遠隔のセキュリティサービスとの間の相互通信を可能にするためのフレームワークおよびシステムの例を示す。例示されたように、より多くの監視対象装置１０２の一つは、ネットワーク１０６を経由してセキュリティサービスクラウドのセキュリティサービスコンピューティングデバイス１０４と接続されることができる。様々な実施形態では、監視対象装置１０２はそれぞれ、サーバまたはサーバファーム、複数の、分散サーバファーム、メインフレーム、ワークステーション、パーソナルコンピュータ（PC）、ラップトップコンピュータ、タブレットコンピュータ、携帯情報端末（ＰＤＡ）、携帯電話、メディアセンタ、組み込みシステム、または他のどの種類の装置または装置群であることができる。複数のコンピューティングデバイス上で実施されたとき、監視対象装置１０２は、それのモジュールおよびデータを複数のコンピューティングデバイスの間に分散することができる。いくつかの実施例では、監視対象装置１０２は、１または複数のコンピューティングデバイス上で実施された１または複数の仮想マシンを表す。また、監視対象装置１０２はそれぞれ、エンティティと関連付けられたものであることがあり、そしてエンティティまたはエンティティ群は、セキュリティサービスプロバイダとの連携とセキュリティサービスを順に行うことができる。セキュリティサービスプロバイダは、セキュリティサービスクラウドを順に操作することができるが、セキュリティサービスコンピューティングデバイス１０４を含むことができる。

【００１９】

いくつかの実施形態では、セキュリティサービスコンピューティングデバイス１０４は

それぞれ、サーバまたはサーバファーム、複数の、分散サーバファーム、メインフレーム、ワークステーション、PC、ラップトップコンピュータ、タブレットコンピュータ、PDA、携帯電話、メディアセンタ、組み込みシステム、または他のどの種類の装置または装置群であるか、含むことができる。一つの実施例では、セキュリティサービスクラウドを実施しているセキュリティサービスコンピューティングデバイス１０４は、コミュニケーション、例えば、ノードのクラウドコンピューティングネットワーク等で動作している複数のコンピューティングデバイスを表す。複数のコンピューティングデバイス上で実施されたとき、セキュリティサービスコンピューティングデバイス１０４は、それのモジュールおよびデータを複数のコンピューティングデバイス間に分散することができる。いくつかの実施例では、１または複数のセキュリティサービスコンピューティングデバイス１０４は、１または複数のコンピューティングデバイス上で実施された１または複数の仮想マシンを表す。

【００２０】

ネットワーク１０６は、１または複数のあらゆるネットワーク、例えば、有線ネットワーク、無線ネットワーク、および有線と無線のネットワークの組み合わせ等を含むことができる。さらに、ネットワーク１０６は、パブリックまたはプライベートネットワーク（例えば、ケーブルネットワーク、インターネット、無線ネットワーク、等）の複数の異なるタイプの一つまたはあらゆる組み合わせを含むことができる。例えば、ネットワーク１０６は、エンティティの一つに関連付けられたパブリックネットワークおよびクライアントネットワークを含むことができる。そのようなクライアントネットワークはそれぞれ、プライベートネットワークであることがある。いくつかの例では、コンピューティングデバイスは、セキュアプロトコル、例えば、ハイパーテキスト・トランスファー・プロトコル・セキュア（ｈｔｔｐｓ）および／または他のどんなプロトコル、またはプロトコルのセット、例えば、トランスミッション・コントロール・プロトコル／インターネット・プロトコル（ＴＣＰ／ＩＰ）等を使用してネットワーク１０６を越えて通信する。

【００２１】

さらに示されたように、監視対象装置１０２はそれぞれ、プロセッサ１０８を備えることができ、そして、セキュリティサービスコンピューティングデバイス１０４はそれぞれ、プロセッサ１１０を備えることができる。プロセッサ１０８および１１０はそれぞれ、中央演算処理装置（ＣＰＵ）、グラフィックスプロセッシングユニット（ＧＰＵ）、またはＣＰＵとＧＰＵの両方、または他のプロセッシングユニット、または当技術分野で知られているコンポーネントであることができる。プロセッサ１０８および１１０は、異なるタイプのプロセッシングユニットまたはコンポーネントであることができるか、または同じ種類であることができる。

【００２２】

監視対象装置１０２はそれぞれ、通信インタフェース１１２を有することもでき、セキュリティサービスコンピューティングデバイス１０４はそれぞれ、通信インタフェース１１４を有することができる。通信インタフェース１１２および１１４は、それらのそれぞれの装置が他の装置（互いに含む）とネットワーク１０６を越えて通信することを可能にするあらゆる種類の有線または無線インタフェース（または両方）でもあることができる。通信インタフェース１１２および１１４は、同じまたは異なるタイプの通信インタフェースであることができる。

【００２３】

監視対象装置１０２はそれぞれ、入力／出力（Ｉ／Ｏ）装置１１６を備え、セキュリティサービスコンピューティングデバイス１０４はそれぞれ、Ｉ／Ｏ装置１１８を備える。Ｉ／Ｏ装置１１６および１１８は、入力装置、例えば、キーボード、マウス、タッチセンサー式のディスプレイ、音声入力装置、等、および出力装置、例えば、ディスプレイ、スピーカ、プリンタ、等を含むことができる。Ｉ／Ｏ装置１１６および１１８は、同じまたは異なるタイプのＩ／Ｏ装置であることができる。監視対象装置１０２のＩ／Ｏ装置１１６は、ユーザによって指定されたタグを入力すること、他のエンティティのタグをサブス

クライブすること、および報告を見ることに使用されることができる。セキュリティサービスコンピューティングデバイス１０４のＩ／Ｏ装置１１８は、構成可能なポリシーを指定し、分類のタグを指定し、そして報告を見ることに使用されることができる。

【００２４】

様々な実施形態では、監視対象装置はそれぞれ、１または複数のコンピュータで読み取り可能なメディア１２０を備え、そしてセキュリティサービスコンピューティングデバイス１０４はそれぞれ、１または複数のコンピュータで読み取り可能なメディア１２２を備える。コンピュータで読み取り可能なメディア１２０および１２２は、あらゆる有形の、永続的な記憶媒体でも含むことができる。例えば、コンピュータで読み取り可能なメディア１２０および１２２は、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリ、または他の記憶技術、ＣＤ－ＲＯＭ、ディジタル多目的ディスク（ＤＶＤ）、または他の光学記憶装置、磁気カセット、磁気テープ、磁気ディスク記憶装置、または他の磁気記憶装置、または望まれる情報を記憶するために使用されることができ、および監視対象装置１０２またはセキュリティサービスコンピューティングデバイス１０４のそれぞれによってアクセスされることができる他のあらゆるメディアでも含むことができるが、これに限定されるものではない。さらに、コンピュータで読み取り可能なメディア１２０と１２２は、取り外し可能な、および／または取り外し不可能であることができる。

【００２５】

図１に例示されたように、それぞれの監視対象装置１０２のコンピュータで読み取り可能なメディア１２０は、セキュリティエージェント１２４を記憶する。セキュリティエージェント１２４は、カーネルレベルエージェントであることができるか、または監視対象装置１０２上の一部、およびセキュリティサービスクラウド上の一部に存在することができる。セキュリティエージェント１２４は、システムコンポーネント１２６の実行行為に関連付けられたイベントの通知を受け取るイベント消費者、フィルタ、セキュリティエージェント１２４の他のモジュールにイベントを送るイベントバス、イベントのタイプを追跡し、および／またはイベントに関連付けられた状態を維持する相関器、および状態の情報を集め、イベントに際し行動するアクターを含むことができる。セキュリティエージェント１２４は、セキュリティサービスクラウド、例えば、１または複数のセキュリティサービス装置１０４等によってインストールされ、構成されることがあり、セキュリティエージェント１２４のモジュールの再設定を受け取り、生きている間は適用している。セキュリティエージェント１２４は、生きている間、セキュリティサービスクラウドから構成可能なポリシーを受け取り、適用することもできる。そのような構成可能なポリシーは、セキュリティエージェント１２４の設定と同じか、または異なるものであることがある。セキュリティエージェントの例は、“Ｋｅｒｎｅｌ－Ｌｅｖｅｌ Ｓｅｃｕｒｉｔｙ Ａｇｅｎｔ”と題され、２０１２年６月８日に出願された米国特許出願第１３／４９２，６７２号により詳細に記述されている。

【００２６】

システムコンポーネント１２６は、どのような種類のモジュール、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、または監視対象装置１０２の完全修飾ドメイン名（ＦＱＤＮ）でもあることができる。モジュールであるシステムコンポーネント１２６は、それのコンテンツのハッシュ値によって特定されることができる。これらのシステムコンポーネント１２６は、プラットフォームとアプリケーションコンポーネントの両方を含むことができる。言及されたように、セキュリティエージェント１２４は、実行行為の通知、例えば、システムコンポーネント１２６に関連付けられたイベント、フィルタおよびセキュリティエージェント１２４の設定に従って送られたイベント等を受け取り、イベントに際し行動する。そのような行動は、単にレコーディング、およびさらなるモニタリングであることがあるか、または改善か警報のレベルまで上がることがある。これらのイベントのモニタリングでは、セキュリテ

ィエージェント１２４は、エクスプロイトコード１２８の指示、または敵１３０の他の悪意のある行為を検出することを試みる。

【００２７】

セキュリティエージェント１２４は、データオブジェクトストア１３２をさらに含めるか、または関連付けられたものであることができる。図１は、セキュリティエージェント１２４から分離するようにデータオブジェクトストア１３２を示す一方、データオブジェクトストア１３２は、セキュリティエージェント１２４の一部であることができるか、またはセキュリティエージェント１２４から分離し、関連付けられたものであることができることを理解すべきである。データオブジェクトストア１３２は、監視対象装置１０２の現在と過去の状態を表すことができる。維持された過去の状態は、例えば、フォレンジックおよび現在の状態のポリシー理解を強化する状態等の少なくとも過去の状態のサブセットを含む。データオブジェクトストア１３２は、少なくとも３つの役割を有することができる。第一の役割では、データオブジェクトストア１３２は、もはや監視対象装置１０２上のどこにも記憶されていない、監視対象装置１０２の過去の状態へのアクセスを供給している歴史家としての役割を果たすことができる。第二の役割では、データオブジェクトストア１３２は、監視対象装置１０２のホストオペレーティングシステムの状態の記憶装置の悪意のある修正を検出することに使用されることができる、監視対象装置１０２の状態の独立モデルを維持しているバリデータのようにサービスを行うことができる。第三の役割では、データオブジェクトストア１３２は、遠隔のセキュリティサービスから受け取られる、生成またはフェッチすることが計算的に高価な、またはフェッチすることに高い待ち時間がある設定のキャッシュ、情報、および状態を供給する。そのようなデータオブジェクトストアの例は、“Ｒｅａｌ－Ｔｉｍｅ Ｒｅｐｒｅｓｅｎｔａｔｉｏｎ ｏｆ Ｓｅｃｕｒｉｔｙ－Ｒｅｌｅｖａｎｔ Ｓｙｓｔｅｍ Ｓｔａｔｅ”と題され、２０１２年１２月２７日に出願された米国特許出願第１３／７２８，７４６号により詳細に記述されている。

【００２８】

データオブジェクトストア１３２は、システムコンポーネント１２６およびイベントを表す複数のデータオブジェクト１３４を含むことができる。これらのデータオブジェクト１３４は、システムコンポーネント１２６を表しているノードデータオブジェクトとイベントを表しているエッジデータオブジェクトとともに、ノードとエッジから成る１または複数のグラフを形作ることができる。セキュリティエージェント１２４は、それのアクターまたは相関器のどれを通しても、データオブジェクト１３４を作成し、更新することができる。いくつかの実施形態では、データオブジェクトストア１３２は、フィルタから受け取ったイベントに基づいて、データオブジェクト１３４の作成および更新をすることができる機能的なコンポーネントに関連付けられたものであることもでき、セキュリティエージェント１２４のコンポーネントを送ることができる。

【００２９】

様々な実施形態では、データオブジェクトストア１３２は、１または複数のツリーオブジェクト１３６を維持することもできる。ツリーオブジェクト１３６は、システムコンポーネント１２６のインスタンスの実行チェーンを表すことができる。セキュリティエージェント１２４がイベントに応じてツリーオブジェクト１３６を作成するかどうかは、セキュリティサービスクラウドから受け取った構成可能なポリシーに基づいて決定されることができる。

【００３０】

図１にさらに示されたように、データオブジェクトストア１３２は、データオブジェクト１３４とツリーオブジェクト１３６のいくらかまたはすべてのタグ１３８を維持することができる。それぞれのタグ１３８は、データオブジェクト１３４またはツリーオブジェクト１３６のラベルか分類器の機能を果たす。タグ１３８が図１の中でデータオブジェクト１３４とツリーオブジェクト１３６から分離して示された一方で、それぞれのタグ１３８は、特定のデータオブジェクト１３４またはツリーオブジェクト１３６のメタデータと

して記憶されることができるが、そのような記憶装置は連続的であるか非連続的であることができることを理解すべきである。

【００３１】

タグ１３８は、構造を備えることができる。タグ１３８の存在は、別のタグ１３８（例えば、“Ｏｆｆｉｃｅ２０１０”は、“ドキュメントプログラム”を必要とする“Ｏｆｆｉｃｅ”を必要とする）またはタグ１３８のセット（例えば、“アップデーター”は、更新されることができる何かを示している他のいくらかのタグ１３８を必要とする）の少なくとも一つのメンバーを必要とすることができる。あるいは、そのような構造は、階層またはタグの重複を経由して避けられることができる。そのような選択肢は、タグ構造の計算による費用を避けるために考慮されることができる。タグ１３８は、お互いに相互に排他的であることもできる（例えば、“ドキュメントプログラム”と“システムプログラム”は相互に排他的であることができる）。

【００３２】

さらに、タグ１３８は、いくつかの種類、例えば、分類のタグ１４０、ツリータグ１４２、およびソーシャルタグ１４４等のどのようなものでもあることもできる。タグ１３８は、実施次第でどんな異なる種類のどのようなものでもあることができる。分類のタグ１４０は、主として宣言され、および標準化されることができ（例えば、セキュリティエージェント１２４によって、またはセキュリティサービスクラウドによって）、および意思決定と直接の行動を可能にすることができる定義された指示を渡すために使用されることができる。いくつかの実施形態では、分類のタグ１４０は、制御インタフェースを通してセキュリティサービスクラウドコードまたはセキュリティサービスプロバイダの権限を与えられた従業員のみによって、割り当てられることができる。分類のタグ１４０の例は、分類、例えば、検出に使うための“ＣＳ＿ＳｈｏｗＩｎＵＩ”タグ等であることができる。分類のタグ１４０は顧客に決して表示することなくフラグを立てられることができる。

【００３３】

ツリータグ１４２は、ツリーオブジェクト１３６とともに監視対象装置１０２上で動的に作成され、およびそれらのツリーオブジェクト１３６を特定するために役に立つ。それぞれのツリータグ１４２は、そのツリータグ１４２によって識別されたツリーオブジェクト１３６が含まれたシステムコンポーネント１２６を表すデータオブジェクト１３４に割り当てられることができる。ツリータグ１４２は、それらのそれぞれのツリーオブジェクト１３６に割り当てられた分類のタグ１４０、ソーシャルタグ１４４、または他のタグ１３８とデータオブジェクト１３４を関連付けるために役に立つ。

【００３４】

ソーシャルタグ１４４は、監視対象装置１０２のユーザによって作成され、割り当てられることができる。ソーシャルタグ１４４は、セキュリティサービスクラウドによって中心的に制御されるよりもむしろ監視対象装置１０２に関連付けられたエンティティによって制御されることができる。しかしながら、ソーシャルタグ１４４は、セキュリティサービスクラウドに供給され、データ分析論または分類のタグ１４０を割り当てるためにソーシャルタグ１４４を使用している手動の伝播ルールに基づくセキュリティサービスクラウド上で間接的な影響を及ぼすことがある。ソーシャルタグ１４４は、エンティティのユーザが作成したそれらのソーシャルタグ１４４の識別子を含むことができる。また、多くの分類のタグ１４０は、ソーシャルタグ１４４として現れることがある。例えば、エンティティに関連付けられたユーザは、“ドキュメントプログラム”タグ１４４を分類のタグ１４０で分類していないセキュリティサービスクラウドの実行ファイルに割り当てることができる。

【００３５】

また、いくつかの実施形態では、タグ１３８はすべての多様なモードの設定に代わる軽量なものとして、監視対象装置１０２の全体的な位置を調整するためにタグを付けられることができる“システム”データオブジェクト１３４のためのタグ１３８を含むことができる。これは、セキュリティエージェント１２４のイベントフィルタリングに位置チェッ

クを開始させることがある。

【００３６】

様々な実施形態では、セキュリティエージェント１２４は、セキュリティサービスクラウドから受け取った構成可能なポリシーに従って、タグ１３８をデータオブジェクト１３４に割り当てることができる。例えば、セキュリティエージェント１２４は、タイプ、実際の動作、またはシステムコンポーネント１２６の特徴、またはそれらのデータオブジェクト１３４が表すイベントに基づいて、データオブジェクト１３４の少なくともいくつかに分類のタグ１４０を割り当てることができる。セキュリティエージェント１２４は、構成可能なポリシーに少なくとも部分的に基づいて、タグ１３８をツリーオブジェクト１３６に割り当てることもできる。セキュリティエージェント１２４は、プログラムと手動のどちらも、タグ１３８の動的な制御を許可している標準的なイベントとともに、タグ１３８をデータオブジェクト１３４またはツリーオブジェクト１３６から動的に割り当てるか、取り外すことができる。また、または代わりに、タグ割り当ては、検出されたどのイベントによってでも引き起こされることができる。そのような状況では、タグ１３８は、イベントに関連付けられたシステムコンポーネント１２６を表しているデータオブジェクト１３４に、検出されたイベントを表すデータオブジェクト１３４に、または両方に割り当てられることができる。

【００３７】

さらに、図２に例示されたように、セキュリティエージェント１２４は、タグ１３８をイベント、および構成可能なポリシーに基づいて、データオブジェクト１３４に割り当てることができる。２０２で、セキュリティエージェント１２４は、システムコンポーネント１２６、例えば、ファイル２０４等に関連付けられたイベントの発生を検出することができる。セキュリティエージェントはその後、２０６で、構成可能なポリシーに基づいて、イベントをフィルタに通すことができる。イベントの検出とフィルタリングに基づいて、セキュリティエージェント１２４はそれから、２０８で、タグ１３８、例えば、タグＸ２１０等をシステムコンポーネント１２６（例えば、ファイル２０４を表しているファイルデータオブジェクト２１２）を表しているデータオブジェクト１３４に割り当てる。

【００３８】

いくつかの実施形態では、タグ１３８は、構成可能なポリシーとイベントの検出に少なくとも部分的に基づいて、セキュリティエージェント１２４によって、データオブジェクト１３４間を伝播されることができる。セキュリティエージェント１２４がイベントを検出するとき、セキュリティエージェント１２４は、構成可能なポリシーを調べ、どのタグ１３８がイベントに関連付けられたシステムコンポーネント１２６を表しているデータオブジェクト１３４の間に伝播されるべきかについて決定する。例えば、親プロセスが子プロセスを作成する場合、親プロセスを表しているデータオブジェクト１３４のタグ１３８のいくつか、またはすべては、セキュリティエージェント１２４によって、子プロセスを表しているデータオブジェクト１３４に伝播されることができる。伝播されたどちらのタグ１３８も、タグ１３８に関連付けられた伝播ルールに基づいて決定され、構成可能なポリシーに含まれることがある。構成可能なポリシーは、そのタグ１３８の伝播を起こすイベントを示すタグ１３８ごとに伝播マスクを含むことができる。そのような伝播マスクは、伝播イベントごとに、タグ１３８の巨大な数でも、小さい、固定された操作の数を可能にしているコンパイラで生成されたビットマスクであることができる。

【００３９】

例えば、構成可能なポリシーに従って、プロセスは、それがロードするファイルからの伝播によっていくつかのタグ１３８を得ることができ、および我々は、ファイルが主要なモジュールとしてロードされたかどうかに基づいて異なる伝播動作を定義するかもしれない。

【００４０】

図３は、そのようなタグの伝播例の一つを示す。図３に例示されたように、セキュリティエージェント１２４は、３０２において、プロセス３０４およびファイル３０６に関連

付けられたイベントを検出することができる。例えば、プロセス３０４は、ファイル３０６を作成し、読み込み、書き込み、または削除するかもしれない。それに応じて、および構成可能なポリシーに従って、セキュリティエージェント１２４は、３０８において、タグ３１０（“タグＸ３１０”として示された）を、プロセス３０４を表しているデータオブジェクト３１２からファイル３０６を表しているデータオブジェクト３１４に伝播することができる。プロセスデータオブジェクト３１２は、構成可能なポリシーに従って、ファイルデータオブジェクト３１４に伝播されていない追加のタグ、例えばタグＹ３１６等を有することもできる。

【００４１】

上述のように、セキュリティエージェント１２４は、構成可能なポリシーに従ってツリーオブジェクト１３６およびツリータグ１４２を作成することができる。図４は、そのようなツリーオブジェクト作成とツリータグ割り当ての例を示す。図４で示されたように、セキュリティエージェント１２４は、４０２でプロセス４０４とファイル４０６に関連付けられたイベント、例えばプロセス４０４によるファイル４０６の実行等を検出する。それに応じて、および構成可能なポリシーに従って、セキュリティエージェント１２４は、４０８において、ファイル４０６を実行しているプロセス４０４の実行チェーン４１２のためのツリーオブジェクト４１０を構成する。ツリーオブジェクト４１０作成の後で、セキュリティエージェント１２４は、追加のイベントおよびシステムコンポーネントの例を表すために実行チェーン４１２の表現を拡大することができる。例えば、ファイル４０６がその後に別のファイルを読み込む実行ファイルの場合は、セキュリティエージェント１２４は、実行チェーン４１２の拡張子を反映するためにツリーオブジェクト４１０の中の実行チェーン４１２の表現を更新することができる。セキュリティエージェント１２４は、タグ１３８、例えば、タグＡ４１４およびタグＢ４１６等をツリーオブジェクト４１０に割り当てることもできる。これらのタグ４１４および４１６は、分類のタグ１４０またはソーシャルタグ１４４であることができる。セキュリティエージェント１２４は、構成可能なポリシーに従ってタグ４１４および４１６を割り当てることができる。例えば、システムコンポーネント１２６または実行チェーン４１２に含まれたイベントが疑わしいと決定された場合、タグ“疑わしい”は、ツリーオブジェクト４１０に割り当てられることがある。ツリーオブジェクト４１０の作成のとき、セキュリティエージェント１２４は、ツリーオブジェクト４１０のためのツリータグ１４２も作成し、４１８において、ツリータグ１４２（“タグＴ４２０”として示された）を、プロセス４０４およびファイル４０６を表しているデータオブジェクト４２２および４２４にそれぞれ割り当てる。データオブジェクト４２２および４２４は、それぞれ単独のツリータグ１４２だけが割り当てられていることを示された一方で、どのデータオブジェクト１３４、例えば、データオブジェクト４２２および４２４等でも、システムコンポーネント１２６または複数のツリーオブジェクト１３６の中に現れるそのデータオブジェクト１３４によって表されたイベントである場合に、それに割り当てられた複数のツリータグ１４２を有することができることを理解すべきである。データオブジェクト４２２および４２４は、それらに割り当てられた他のタグ１３８を有することもできる。例えば、プロセスデータオブジェクト４２２は、それに割り当てられたタグＣ４２６を有することができる。セキュリティエージェント１２４がその後にタグ１３８に基づいて、データオブジェクト４２２および４２４をフィルタに通すとき、セキュリティエージェント１２４は、例えば、プロセスデータオブジェクト４２２がタグＣ４２６、タグＴ４２０、およびタグＴ４２０のおかげで、タグＡ４１４もタグＢ４１６も同様に有することを考慮する。プロセスデータオブジェクト４２２は、タグＡ４１４およびタグＢ４１６を他動的に有するために考慮される‐ツリータグＴ４２０とそれらの関係がプロセスデータオブジェクト４２２へのそれらのアプリケーションを確実にするのに十分であるように、これらのタグ４１４および４１６が明確に割り当てられる必要がない。

【００４２】

図１に戻り、セキュリティエージェント１２４またはセキュリティサービスプロバイダ

（例えば、ウェブページ）から受け取ったユーザインタフェースは、監視対象装置１０２のユーザが監視対象装置１０２に関連付けられたエンティティの代わりに、別のエンティティ１４８のソーシャルタグ１４６をサブスクライブすることを可能にすることもできる。監視対象装置１０２はその後、別のエンティティ１４８の監視対象装置から直接に、またはセキュリティサービスクラウドのセキュリティサービスコンピューティングデバイス１０４を通じてのどちらかから、ソーシャルタグ１４６を受け取ることができる。監視対象装置１０２は、ソーシャルタグ１４６が作成されるようにサブスクライブされたソーシャルタグ１４６を継続的に受け取り続けることもできる。ソーシャルタグ１４６を受け取ることに際し、セキュリティエージェント１２４は、ソーシャルタグ１４６をデータオブジェクト１３４に割り当てることができる。ソーシャルタグ１４６は、別のエンティティのデータオブジェクトに相当するデータオブジェクト１３４に割り当てられる。“相当する”データオブジェクトは、システムコンポーネント１２６またはイベントの同じ、または類似のタイプを表しているそれらであることがある。ソーシャルタグ１４６を受け取ること、および割り当てることに際し、それらのソーシャルタグ１４６は、ソーシャルタグ１４４の一部と考慮されることができる。

【００４３】

ソーシャルタグ１４４は、いくつかの機能を供給することに使用されることができる。例えば、ソーシャルタグ１４４は、複数のアナリストおよびエンティティの全域との間で、調整を許可する注釈のために任意に使用されることができる。パターンおよびファイル上のソーシャルタグ１４４は、ポリシーおよび異なるパターンのプライオリティーについてエンティティ優先の表現を可能にすること、および急なホワイトリストローカルプログラム、および全体のファイル、または特定のパターンに関してエンティティに許可することを可能にすることができる。

【００４４】

図５は、別のエンティティのソーシャルタグのサブスクリプションの例を示す。図５に例示されたように、５０４において、第一のエンティティ５０２は、第二のエンティティ５０８のソーシャルタグ５０６をサブスクライブすることができる。ソーシャルタグ５０６は、システムコンポーネント１２６または第二のエンティティの監視対象装置１０２のイベントを表すデータオブジェクト、例えば、データオブジェクト５１０等に割り当てられることができる。サブスクリプションに応答して、５１２において、第一のエンティティ５０２は、ソーシャルタグ５０６を受け取ることができる。第一のエンティティ５０２の監視対象装置１０２のセキュリティエージェント１２４は、その後、ソーシャルタグ５０６をデータオブジェクト５１４に割り当てることができる。データオブジェクト５１４は、その後、それら自身のどのようなタグ、例えば、タグＤ５１６等、およびサブスクライブされたソーシャルタグ５０６のどちらも有することができる。

【００４５】

様々な実施形態では、再び図１を参照して、セキュリティエージェント１２４は、報告、意思決定、またはイベント生成のためにタグ１３８を利用することができる。セキュリティエージェント１２４は、データオブジェクト１３４をフィルタに通すために構成可能なポリシーとタグ１３８を利用することができる。そのフィルタリングの結果は、その後、セキュリティエージェント１２４を通じて、またはセキュリティサービスクラウド（例えば、ウェブページ）によって供給されたユーザインタフェースを通じて、監視対象装置１０２のユーザに供給されることができる報告を生成することに利用されることができる。セキュリティエージェント１２４は、また、またはその代わりに、フィルタ処理したデータオブジェクト１３４に基づいて決定することができる。例えば、フィルタ処理したデータオブジェクト１３４が、タグ１３８“疑わしい”の付いたどんなデータオブジェクト１３４でも含む場合、セキュリティエージェント１２４は、追加のモニタリングを行うことか、または是正措置をとることを決定することができる。さらに、セキュリティエージェント１２４は、イベントを生成することができる。例えば、セキュリティエージェント１２４がタグ１３８をデータオブジェクト１３４に伝播し、そのデータオブジェクト１３

４が、伝播されたタグ１３８と衝突する別のタグ１３８を有している場合、セキュリティエージェント１２４は、タグ衝突を示すイベントを生成することができる。

【００４６】

タグ１３８は、セキュリティエージェント１２４によってランタイムポリシーを引き起こすために使用されることもできる。例えば、タグ１３８は、プロセスが外部のネットワークコネクションを作ることを許可されるべきではないことを示すことがある。そのようなタグ１３８は、セキュリティエージェント１２４によってタグ１３８の存在に関してフィルタを通すために使用される構成可能なポリシーからそれらの効果を取る。

【００４７】

様々な実施形態では、セキュリティサービスクラウドのセキュリティサービスコンピューティングデバイス１０４はそれぞれ、それのコンピュータで読み取り可能なメディア１２２、データオブジェクト１５２およびタグ１５４を含むことができるデータオブジェクトストア１５０を維持することができる。データオブジェクトストア１５０は、１または複数の監視対象装置１０２の現在と過去の状態を表すことができる。維持された過去の状態は、例えば、フォレンジックおよび現在の状態のポリシー理解を強化する状態等の少なくとも過去の状態のサブセットを含む。データオブジェクトストア１５０は、システムコンポーネント１２６および１または複数の監視対象コンピューティングデバイスのイベントを表す複数のデータオブジェクト１５２を含むことができる。これらのデータオブジェクト１５２は、システムコンポーネント１２６を表しているノードデータオブジェクトとイベントを表しているエッジデータオブジェクトとともに、ノードとエッジから構成される１または複数のグラフを形作ることもできる。データオブジェクトストア１５０は、監視対象装置１０２ごとに分離したグラフ、監視対象装置のうちの複数の監視対象装置のためのグラフ、または両方を維持することができる。監視対象装置１０２のうちの複数の監視対象装置を表しているグラフは、複数の監視対象装置１０２からシステムコンポーネント１２６に関連付けられたイベント、例えば、別の監視対象装置１０２上のファイルにアクセスしている、一つの監視対象装置１０２上のプロセス等の表現を含むことができる。示されていないが、データオブジェクトストア１５０は、監視対象装置１０２上に作成されたツリーオブジェクト１３６のコピーを含むことができる。

【００４８】

いくつかの実施形態では、タグ１５４は、１または複数の監視対象装置１０２のタグ１３８のスーパーセットを表すことができる。なぜなら、分類のタグ１４０は、セキュリティサービスコンピューティングデバイス１０４によって中心的に作成されることがあり、タグ１５４に含まれた分類のタグ１４０は、タグ１３８に含まれた分類のタグ１４０と同じであるか、少なくともすべてを含むことができるからである。タグ１５４に含まれた分類のタグ１４０は、監視対象装置のどんなデータオブジェクト１３４、またはツリーオブジェクト１３６にも未だ割り当てられていない追加の分類のタグ１４０を含むこともできる。タグ１５４のツリータグ１４２は、監視対象装置１０２のツリーオブジェクト１３６を識別することに加えて、ツリーオブジェクト１３６が属する監視対象装置１０２の識別子も含む。タグ１５４のソーシャルタグ１４４は、それらのソーシャルタグ１４４を作成したエンティティの識別を含む。上記のように、セキュリティサービスクラウドは、追加の分類のタグ１４０を定義する際に、これらのソーシャルタグ１４４を利用することができる。

【００４９】

セキュリティエージェント１２４およびセキュリティサービスクラウドによって実施されたタグ１３８および１５４のためのコミュニケーションモデルは、監視対象装置１０２とセキュリティサービスコンピューティングデバイス１０４との間を、どんな状況下でタグ１３８が流れるかについて定義することができる。この流れは、別の伝播操作として、または場合により２つの操作として実施されることができる。一つは受動的にタグ１３８を転送すること、およびもう一つは変更をタグの割り当てに能動的にプッシュすることである。

【００５０】
さらなる実施形態では、セキュリティサービスコンピューティングデバイスのセキュリティモジュール１５６は、インフォメーションセキュリティサービスを、それらの監視対象装置１０２を通して個々のユーザとクライアントエンティティに供給するために構成されることができる、例えば、セキュリティエージェント１２４およびデータオブジェクトストア１３２の維持と設定、脅威モデリング、および／または改善等。セキュリティモジュール１５６は、セキュリティエージェント１２４を構成するため、および構成可能なポリシーをセキュリティエージェント１２４に供給するための構成モジュール１５８、監視対象装置１０２上のイベントを検出するため、またはそれらのイベントの発生の指示を受け取るためのモニタリングモジュール１６０、およびセキュリティサービスのソーシャル面、例えば、ソーシャルタグ１４４の共有等を可能にするためのソーシャルモジュール１６２を含めることができる。
【００５１】
さらなる実施形態では、セキュリティモジュール１５６は、データオブジェクトストア１５０をビルド、および維持することができる。セキュリティモジュール１５６のモニタリングモジュール１６０は、イベントを検出するか、またはイベントの発生の指示を受け取り、データオブジェクトストア１５０をビルドするためにその情報を使用することができる。そのような情報は、イベントが実際に観察されたときに、実質的にリアルタイムで受け取られることができる。構成モジュール１５８は、監視対象装置１０２がモニタリングモジュール１６０に通知することになっているイベントと、監視対象装置１０２が共有することになっているタグ１３８を明記するように、監視対象装置１０２を構成することができる。さらに、構成モジュール１５８は、構成可能なポリシーを更新し、更新された構成可能なポリシーを監視対象装置１０２に広めることができる。そのような更新された構成可能なポリシーは、タグ１３８の割り当ての更新、いくつかのタグ１３８を取り外すこと、および他を追加することをもたらすことがある。更新された構成可能なポリシーは、異なる伝播動作をもたらすタグ１３８のための伝播マスクを更新することもできる。
【００５２】
いくつかの実施形態では、ソーシャルモジュール１６２は、ソーシャル面をセキュリティサービスに供給することもでき、ユーザおよび／またはクライアントエンティティのグループを成形し、ユーザおよび／またはグループを構成しているクライアントエンティティ間でセキュリティ情報を自動的に共有している。あるいは、または追加的に、ソーシャルモジュール１６２は、ユーザまたはエンティティに、他のユーザまたは他のエンティティのソーシャルタグ１４４をサブスクライブすることを可能にし、それらを回収することおよび供給すること、またはユーザ／エンティティにソーシャルタグ１４４をお互いに直接供給することを可能にすることのどちらか一方のサブスクライブされたタグ１４４のやりとりを可能にすることができる。
【００５３】
示されていないが、セキュリティモジュール１５６は、タグ１５４をフィルタに通すように行動するための１または複数のモジュールを含み、およびフィルタリングの際に行動することもできる。そのような行動は、セキュリティエージェント１２４に関して上記に述べるような方法で、意思決定、報告生成、またはイベント生成を含むことができる。行動はさらに、構成モジュール１５８に構成可能なポリシーを更新させることが含まれることがある。
【００５４】
プロセス例
図６は、プロセス例を示す。このプロセスは、ロジカルフローグラフとして示され、それぞれの動作は、ハードウェア、ソフトウェア、またはそれらの組み合わせで実施されることができる動作の順序を表す。ソフトウェアのコンテキストでは、１または複数のコンピュータで読み取り可能な記憶媒体に記憶されたコンピュータで実行可能な指示を表す動作は、１または複数のプロセッサによって実行されたとき、列挙された動作を行う。通常

、コンピュータで実行可能な指示は、ルーチン、プログラム、オブジェクト、コンポーネント、データ構造、および特定の機能を行うか、または特定の抽象的なデータタイプを実施するようなものを含む。動作が記述された命令は、制限として解釈されることは意図されておらず、および記述された動作はいくらでも、どんな命令の組み合わせでもあること、および／またはプロセスを並列に実施することができる。

【００５５】

図６は、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こと、およびこれら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、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ことのためのプロセスの例を示しているフロー図である。プロセスは６０２で、セキュリティエージェントまたはセキュリティサービスクラウドが、タグを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ことを含む。そのような割り当ては、構成可能なポリシーに基づくことができる。タグはそれぞれ、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ができ、および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ができる。また、タグは、構造を有することができる。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。さらに、タグは、実行されたとき、データオブジェクトによって表されたシステムコンポーネントを分類し、およびシステムコンポーネントの分類に関連付けられた新しいタグ（前のタグに加えて、または前のタグを置換することのどちらか）を割り当てるロジックに関連付けられることができる。６０４で、割り当てることは、ユーザがタグを、データオブジェクトによって表されたシステムコンポーネントに関連付けることをできるようにすること、およびユーザによって関連付けられたタグをデータオブジェクトに割り当てることを含むことができる。６０６で、割り当てることは、データオブジェクトによって表された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、タグを割り当てることを含むことができる。追加の、または代わりに、割り当てることは、そ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こと、および構成可能なポリシーを使用しているそのイベントのフィルタリングに少なくとも部分的に基づいて、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、タグを割り当てることを含むことができる。

【００５６】

６０８で、第一のエンティティのセキュリティエージェントは、第二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ことができる。セキュリティエージェントは、その後、第二のエンティティのユーザによって指定されたタグを第一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割り当てることができる。

【００５７】

６１０で、セキュリティエージェントまたはセキュリティサービスクラウドは、コンピューティングデバイスの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がコンピューティングデバイス上で発生していることを検出することができる。

【００５８】

６１２で、構成可能なポリシーに基づいて、セキュリティエージェントまたはセキュリティサービスクラウドは、別のタグをイベントの検出を表しているデータオブジェクトに割り当てることができる。６１４で、セキュリティエージェントまたはセキュリティサービスクラウドは、後のイベントを検出し、検出している後のイベントに少なくとも部分的に基づいて、別のタグを更新することができる。

【００５９】

６１６で、セキュリティエージェントまたはセキュリティサービスクラウドは、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を構成することができる。セキュリティエージェントまたはセキュリティサービスクラウドは、システムコンポーネントのサブセットの別のシステムコンポーネントによる、システムコンポーネントの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ことに応じて、ツリーオブジェクトを構成することができる。システムコンポーネントのサブセットは、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ができる。６１８で、セキュリティエージェントまたはセキュリティサービスクラウドは、ツリーオブジェクトのためのタグを、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割り当てることができる。

【００６０】

６２０で、イベントを検出すること、および構成可能なポリシーに少なくとも部分的に基づいて、セキュリティエージェントまたはセキュリティサービスクラウドは、複数のシステムコンポーネントの一つ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られたタグを、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。いくつかの実施形態では、伝播することは、構成可能なポリシーに少なくとも部分的に基づいて、データオブジェクトに割り当てられた複数のすべてより小さいタグを伝播することを備える。また、またはその代わりに、伝播することは、構成可能なポリシーの少なくとも部分的に基づいて、タグを、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ことを備えることができる。さらに、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ることができ、および伝播することは、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ることができる。そのような実施形態では、データオブジェクトおよび他のデータオブジェクトは、１または複数の他のコンピューティングデバイス上に記憶されることができる。加えて、いくつかの実施形態では、データオブジェクトによって表されたシステムコンポーネントは、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ることができ、別のデータオブジェクトによって表された別のシステムコンポーネントは、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ることができ、および伝播することは、第一のコンピューティングデバイス、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ができる。

【００６１】

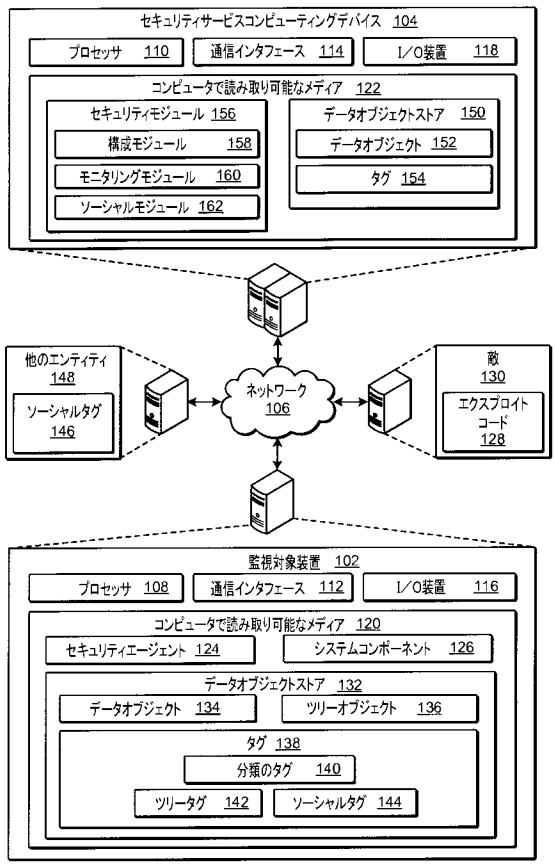
６２２で、セキュリティエージェントまたはセキュリティサービスクラウドは、タグ伝播に基づいてイベントを生成することができる。例えば、伝播されたタグは、別のデータオブジェクトに関連付けられた別のタグと相互に排他的であることができ、およびセキュリティエージェントまたはセキュリティサービスクラウドは、タグ衝突を示すイベントを生成することができる。また、またはその代わりに、６２４で、複数のシステムコンポーネントを表しているデータオブジェクトに関連付けられたタグに少なくとも部分的に基づいて、セキュリティエージェントまたはセキュリティサービスクラウドは、決定すること、または報告を生成することの少なくとも一つを行うことができる。

【００６２】

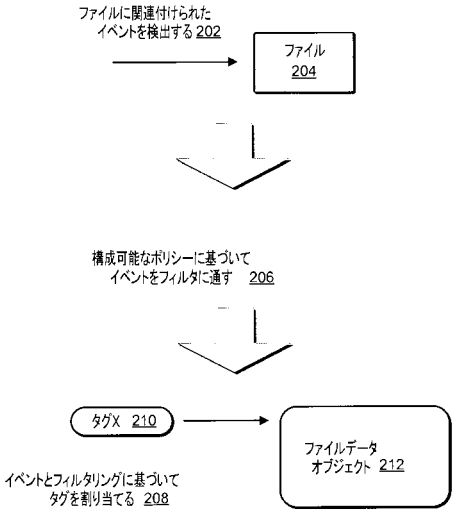
結論

発明の主題が構造の特徴および／または方法論的な行為に特有の言葉で記述されたが、添付の特許請求の範囲に定義された発明の主題は、必ずしも記述された特有の特徴または行為に限定されたものではないことを理解すべきである。むしろ、特有の特徴および行為は、特許請求の範囲を実施することの形態例として開示される。

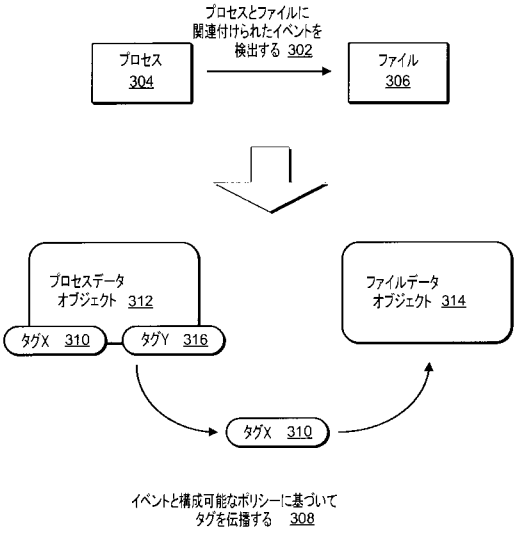
【図１】


セキュリティサービスコンピューティングデバイス 104
プロセッサ 110
通信インタフェース 114
I/O装置 118
コンピュータで読み取り可能なメディア 122
セキュリティモジュール 156
構成モジュール 158
モニタリングモジュール 160
ソーシャルモジュール 162
データオブジェクトストア 150
データオブジェクト 152
タグ 154
他のエンティティ 148
ソーシャルタグ 146
ネットワーク 106
敵 130
エクスプロイトコード 128
監視対象装置 102
プロセッサ 108
通信インタフェース 112
I/O装置 116
コンピュータで読み取り可能なメディア 120
セキュリティエージェント 124
システムコンポーネント 126
データオブジェクトストア 132
データオブジェクト 134
ツリーオブジェクト 136
タグ 138
分類のタグ 140
ツリータグ 142
ソーシャルタグ 144

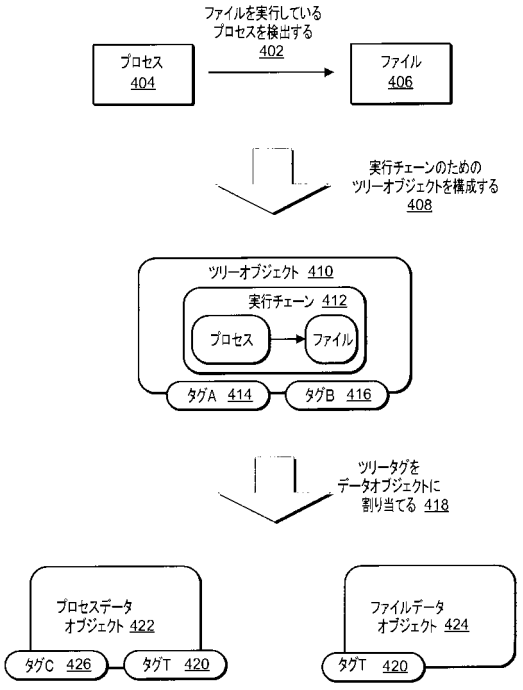
【図２】


ファイルに関連付けられたイベントを検出する 202
ファイル 204
構成可能なポリシーに基づいてイベントをフィルタに通す 206
タグX 210
ファイルデータオブジェクト 212
イベントとフィルタリングに基づいてタグを割り当てる 208

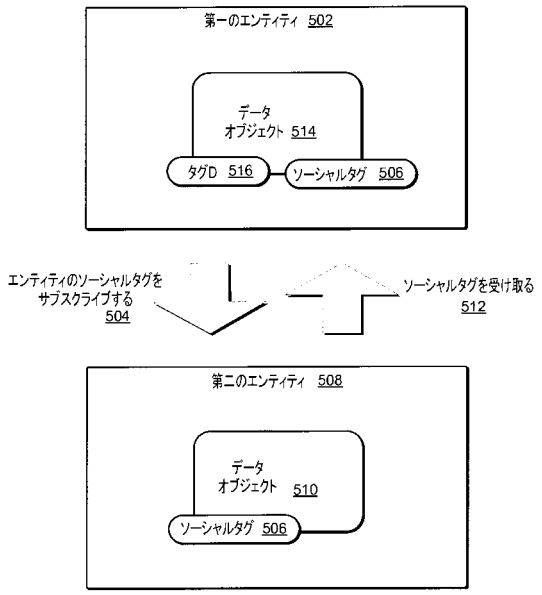
【図３】


プロセスとファイルに関連付けられたイベントを検出する 302
プロセス 304
ファイル 306
プロセスデータオブジェクト 312
タグX 310
タグY 316
ファイルデータオブジェクト 314
タグX 310
イベントと構成可能なポリシーに基づいてタグを伝播する 308

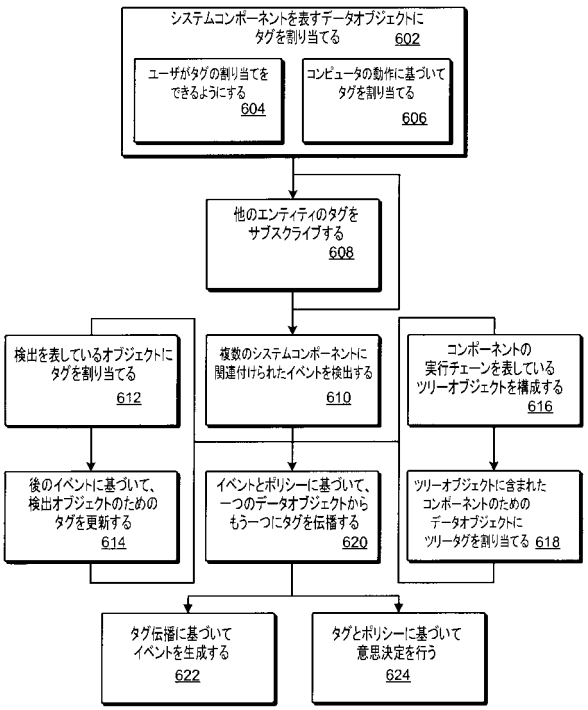
【図４】


ファイルを実行しているプロセスを検出する 402
プロセス 404
ファイル 406
実行チェーンのためのツリーオブジェクトを構成する 408
ツリーオブジェクト 410
実行チェーン 412
プロセス
ファイル
タグA 414
タグB 416
ツリータグをデータオブジェクトに割り当てる 418
プロセスデータオブジェクト 422
タグC 426
タグT 420
ファイルデータオブジェクト 424
タグT 420

【図５】


第一のエンティティ 502
データ
オブジェクト 514
タグD 516
ソーシャルタグ 506
エンティティのソーシャルタグを
サブスクライブする
504
ソーシャルタグを受け取る
512
第二のエンティティ 508
データ
オブジェクト 510
ソーシャルタグ 506

【図６】


システムコンポーネントを表すデータオブジェクトに
タグを割り当てる 602
ユーザがタグの割り当てを
できるようにする
604
コンピュータの動作に基づいて
タグを割り当てる
606
他のエンティティのタグを
サブスクライブする
608
検出を表しているオブジェクトに
タグを割り当てる
612
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
610
コンポーネントの
実行チェーンを表している
ツリーオブジェクトを構成する
616
後のイベントに基づいて、
検出オブジェクトのための
タグを更新する
614
イベントとポリシーに基づいて、
一つのデータオブジェクトから
もう一つにタグを伝播する
620
ツリーオブジェクトに含まれた
コンポーネントのための
データオブジェクトに
ツリータグを割り当てる 618
タグ伝播に基づいて
イベントを生成する
622
タグとポリシーに基づいて
意思決定を行う
624

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2015/013522

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/56(2013.01)i, G06F 17/30(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F 21/56; G06F 3/048; G06F 21/54; H04L 29/06; G06F 21/00; G06F 17/30

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: tag, detecting malware, event, propagate, share, classification

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2013-164821 A2 (SHINE SECURITY LTD.) 07 November 2013 See page 2, lines 2-18; page 4, line 6 - page 5, line 14; page 7, lines 14-17; page 10, line 24 - page 11, line 31; page 14, line 27 - page 15, line 19; page 18, line 17 - page 20, line 15; and figures 2-3, 6.	1-26
A	WO 2012-107557 A1 (TELEFONICA, S.A.) 16 August 2012 See page 7, lines 1-27; page 15, line 22 - page 16, line 34; and figure 3.	1-26
A	US 2008-0209505 A1 (VIKRANT GHAI et al.) 28 August 2008 See paragraphs [0060]-[0061]; and figures 1A, 5.	1-26
A	US 2008-0189796 A1 (CHRISTOPHER S. LINN et al.) 07 August 2008 See paragraphs [0005], [0028]-[0029]; and figures 2-3.	1-26
A	US 2008-0282198 A1 (DAVID A. BROOKS et al.) 13 November 2008 See paragraphs [0029]-[0030], [0041]-[0044]; and figures 1-2.	1-26

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory undertying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 April 2015 (27.04.2015)	**28 April 2015 (28.04.2015)**

Name and mailing address of the ISA/KR	Authorized officer
International Application Division Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea Facsimile No. ++82 42 472 7140	AHN, Jeong Hwan Telephone No. +82-42-481-8440

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2015/013522

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2013-164821 A2	07/11/2013	WO 2013-164821 A3	19/12/2013
WO 2012-107557 A1	16/08/2012	EP 2487860 A1	15/08/2012
		EP 2487860 B1	25/09/2013
		US 2014-0223555 A1	07/08/2014
US 2008-0209505 A1	28/08/2008	None	
US 2008-0189796 A1	07/08/2008	US 8181264 B2	15/05/2012
US 2008-0282198 A1	13/11/2008	US 2015-0052448 A1	19/02/2015
		US 8918717 B2	23/12/2014

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JP,KE,KG,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US

(72)発明者 マキシム ラモゼーブラサード
カナダ ケー１エヌ１ジェー６ オタワ オンタリオ ヨーク ストリート １２０１－１８０

Ｆターム(参考) 5K030 GA15 HA08 HD03 HD09 KA05 LD20