(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6643128号
(P6643128)
(45)発行日　令和2年2月12日(2020.2.12)　(24)登録日　令和2年1月8日(2020.1.8)

(51)Int.Cl.　　F I
G06F 21/53 (2013.01)　　G06F 21/53
G06F 9/455 (2006.01)　　G06F 9/455 150

請求項の数 18　(全 20 頁)

(21)出願番号　特願2016-23790(P2016-23790)
(22)出願日　平成28年2月10日(2016.2.10)
(65)公開番号　特開2016-149131(P2016-149131A)
(43)公開日　平成28年8月18日(2016.8.18)
審査請求日　平成31年2月4日(2019.2.4)
(31)優先権主張番号　14/622,224
(32)優先日　平成27年2月13日(2015.2.13)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　512132022
フィッシャー－ローズマウント　システムズ，インコーポレイテッド
アメリカ合衆国　テキサス　７８６８１－７４３０　ラウンド　ロック　ウェスト　ルイス　ヘナ　ブルバード　１１００　ビルディング　１　エマーソン　プロセス　マネージメント
(74)代理人　100079049
弁理士　中島　淳
(74)代理人　100084995
弁理士　加藤　和詳

最終頁に続く

(54)【発明の名称】仮想マシンイントロスペクションを通じたセキュリティ事象検出方法、装置、及び有形コンピュータ可読記憶媒体

(57)【特許請求の範囲】
【請求項１】
プロセス制御システムのコンピューティングデバイスにおけるセキュリティ事象検出方法であって、
前記コンピューティングデバイスで実行している第１の仮想マシンによる複数のリソースの使用量を、監視エージェントによって監視することであって、前記監視エージェントは、前記第１の仮想マシンとは分離して前記コンピューティングデバイスで実行している、監視することと、
前記複数のリソースの前記使用量をリソース使用パターンと比較することによって、潜在的セキュリティ事象を検出することと、
前記検出された潜在的セキュリティ事象に深刻度レベルを割り当てることと、
前記割り当てられた深刻度レベルに基づいて、セキュリティ措置を開始することと、を含む、セキュリティ事象検出方法。
【請求項２】
前記監視エージェントは、前記第１の仮想マシンを管理するハイパーバイザと通信して、前記第１の仮想マシンによる前記複数のリソースの前記使用量を監視する、請求項１に記載のセキュリティ事象検出方法。
【請求項３】
前記監視エージェントは、前記コンピューティングデバイスの第２の仮想マシン内で実行している、請求項１又は請求項２に記載のセキュリティ事象検出方法。

【請求項４】
前記監視エージェントは、前記第１の仮想マシンを管理するハイパーバイザの一部である、請求項１～請求項３の何れか１項に記載のセキュリティ事象検出方法。
【請求項５】
監視エージェントは、前記第１の仮想マシンのメモリ使用量、記憶ディスク使用量、ネットワーク使用量、及びハードウェア使用量のうちの少なくとも１つを監視する、請求項１～請求項４の何れか１項に記載のセキュリティ事象検出方法。
【請求項６】
前記検出された潜在的セキュリティ事象への最高深刻度レベルの割り当てに応答して、前記セキュリティ措置を開始することは、
第２の仮想マシンを、前記潜在的セキュリティ事象が検出される前に作成された前記第１の仮想マシンのスナップショットに基づいて、前記コンピューティングデバイスにインスタンス化させることと、
前記第１の仮想マシンの機能性を前記第２の仮想マシンに移動させることと、
前記第１の仮想マシンを終了させることと、を含む、請求項１～請求項５の何れか１項に記載のセキュリティ事象検出方法。
【請求項７】
前記第１の仮想マシンに整合性レベルを割り当てることと、
前記潜在的セキュリティ事象の検出に応答して、前記第１の仮想マシンの前記整合性レベルを引き下げることと、
前記第１の仮想マシンの前記整合性レベルが整合性レベル閾値を下回るときに、前記第１の仮想マシンの前記整合性レベルに基づいて前記セキュリティ措置を開始することと、をさらに含む、請求項１～請求項６の何れか１項に記載のセキュリティ事象検出方法。
【請求項８】
リソースモニタであって、プロセッサを介して、
コンピューティングデバイスで実行している第１の仮想マシンによる複数のリソースの使用量を監視することであって、前記リソースモニタは、前記第１の仮想マシンとは分離している、監視すること、及び
前記複数のリソースの前記使用量をリソース使用パターンと比較することによって、潜在的セキュリティ事象を検出することを行うための、リソースモニタと、　セキュリティ事象ハンドラであって、
前記検出された潜在的セキュリティ事象に深刻度レベルを割り当てること、及び
前記割り当てられた深刻度レベルに関して定義されるセキュリティ措置を開始することを行うための、セキュリティ事象ハンドラと、を備える、装置。
【請求項９】
前記リソースモニタは、前記第１の仮想マシンを管理するハイパーバイザと通信して、前記第１の仮想マシンの前記複数のリソースの前記使用量を監視するものである、請求項８に記載の装置。
【請求項１０】
前記リソースモニタは、前記第１の仮想マシンを管理するハイパーバイザの一部である、請求項８又は請求項９に記載の装置。
【請求項１１】
リソースモニタは、前記第１の仮想マシンのメモリ使用量、記憶ディスク使用量、ネットワーク使用量、及びハードウェア使用量のうちの少なくとも１つを監視するものである、請求項８～請求項１０の何れか１項に記載の装置。
【請求項１２】
前記検出された潜在的セキュリティ事象への最高深刻度レベルの割り当てに応答して、前記セキュリティ事象ハンドラは、
第２の仮想マシンを、前記潜在的セキュリティ事象が検出される前に作成された前記第１の仮想マシンのスナップショットに基づいて、前記コンピューティングデバイスにイン

スタンス化させることと、
前記第１の仮想マシンの機能性を前記第２の仮想マシンに移動させることと、
前記第１の仮想マシンを終了させることと、を行うものである、請求項８～請求項１１の何れか１項に記載の装置。
【請求項１３】
前記セキュリティ事象ハンドラは、
前記第１の仮想マシンに整合性レベルを割り当てることと、
潜在的セキュリティ事象の検出に応答して、前記第１の仮想マシンの前記整合性レベルを引き下げることと、
前記第１の仮想マシンの前記整合性レベルが整合性レベル閾値を下回るときに、前記第１の仮想マシンの前記整合性レベルに基づいてセキュリティ措置を開始することと、を行うものである、請求項８～請求項１２の何れか１項に記載の装置。
【請求項１４】
有形コンピュータ可読記憶媒体であって、実行されるときに、監視エージェントに、少なくとも
コンピューティングデバイスで実行している第１の仮想マシンによる複数のリソースの使用量を監視することであって、前記監視エージェントは、前記第１の仮想マシンとは分離して前記コンピューティングデバイスで実行している、監視することと、
前記複数のリソースの前記使用量をリソース使用パターンと比較することによって、潜在的セキュリティ事象を検出することと、
前記検出された潜在的セキュリティ事象に深刻度レベルを割り当てることと、
前記割り当てられた深刻度レベルに関して定義されるセキュリティ措置を開始することと、を行わせる命令を含む、有形コンピュータ可読記憶媒体。
【請求項１５】
前記命令は、実行されるときに、前記監視エージェントに、前記第１の仮想マシンを管理するハイパーバイザとさらに通信して、前記第１の仮想マシンの前記複数のリソースの前記使用量を監視させる、請求項１４に記載の有形コンピュータ可読記憶媒体。
【請求項１６】
前記監視エージェントは、前記第１の仮想マシンを管理するハイパーバイザの一部である、請求項１４又は請求項１５に記載の有形コンピュータ可読記憶媒体。

【請求項１７】
前記検出された潜在的セキュリティ事象への最高深刻度レベルの割り当てに応答して、前記命令は、実行されるときに、前記監視エージェントに、
第２の仮想マシンを、前記潜在的セキュリティ事象が検出される前に作成された前記第１の仮想マシンのスナップショットに基づいて、前記コンピューティングデバイスにインスタンス化させることと、
前記第１の仮想マシンの機能性を前記第２の仮想マシンに移動させることと、
前記第１の仮想マシンを終了させることと、を行わせる、請求項１４～請求項１６の何れか１項に記載の有形コンピュータ可読記憶媒体。
【請求項１８】
実行されるときに、前記監視エージェントに、
前記第１の仮想マシンに整合性レベルを割り当てることと、
潜在的セキュリティ事象の検出に応答して、前記第１の仮想マシンの前記整合性レベルを引き下げることと、
前記第１の仮想マシンの前記整合性レベルが整合性レベル閾値を下回るときに、前記第１の仮想マシンの前記整合性レベルに基づいて前記セキュリティ措置を開始することと、を行わせる命令を含む、請求項１４～請求項１７の何れか１項に記載の有形コンピュータ可読記憶媒体。
【発明の詳細な説明】

【技術分野】
【０００１】
本開示は、概してプロセス制御システムに関し、より具体的には、仮想マシンイントロスペクションを通じたセキュリティ事象検出のための方法及び装置に関する。
【背景技術】
【０００２】
化学、石油、または他のプロセスにおいて使用されるものなどのプロセス制御システムは、典型的には、アナログ、デジタル、または複合アナログ／デジタルバスを介して、少なくとも１つのホストまたはオペレータワークステーションと、１つ以上のフィールドデバイスとに通信可能に連結される、１つ以上のプロセス制御装置を含む。フィールドデバイスは、例えば、デバイス制御装置、弁、弁保定装置、スイッチ、及び伝送器（例えば、温度、圧力、及び流量センサ）であり得るが、弁の開閉及びプロセスパラメータの測定などのプロセス制御システム内部の機能を実施する。プロセス制御装置は、フィールドデバイスによって行われたプロセス測定値を示す信号及び／またはフィールドデバイスに付随する他の情報を受信し、この情報を使用して、制御ルーティンを実装し、次にバスまたは他の通信線でフィールドデバイスに送信されるプロセス制御システムの操作を制御するための制御信号を生成する。
【発明の概要】
【課題を解決するための手段】
【０００３】
プロセス制御システムのコンピューティングデバイスにおけるセキュリティ事象検出の開示される方法例は、コンピューティングデバイス上で実行している第１の仮想マシンによる複数のリソースの使用量を、監視エージェントによって監視することであって、該監視エージェントは、該第１の仮想マシンとは分離してコンピューティングデバイス上で実行している、監視することを含む。開示される方法例はまた、該複数のリソースの使用量をリソース使用パターンと比較することによって、潜在的セキュリティ事象を検出することも含む。開示される方法例はまた、該検出された潜在的セキュリティ事象に深刻度レベルを割り当てること、及び該割り当てられた深刻度に基づいてセキュリティ措置を開始することも含む。
【０００４】
開示される装置例は、リソースモニタであって、プロセッサを介して、コンピューティングデバイス上で実行している第１の仮想マシンによる複数のリソースの使用量を監視することであって、該リソースモニタは、該第１の仮想マシンとは分離している、監視すること、及び該複数のリソースの使用量をリソース使用パターンと比較することによって、潜在的セキュリティ事象を検出することを行うための、リソースモニタを含む。開示される装置例はまた、セキュリティ事象ハンドラであって、検出された潜在的セキュリティ事象に深刻度レベルを割り当てること、及び該割り当てられた深刻度レベルに関して定義されるセキュリティ措置を開始することを行うための、セキュリティ事象ハンドラも含む。
【０００５】
開示される有形コンピュータ可読記憶媒体例は、実行されるときに、監視エージェントに、コンピューティングデバイス上で実行している第１の仮想マシンによる複数のリソースの使用量を監視することであって、該監視エージェントは、該第１の仮想マシンとは分離して該コンピューティングデバイス上で実行している、監視することを行わせる命令を含む。開示される有形コンピュータ可読記憶媒体例はまた、実行されるときに、該マシンに、該複数のリソースの使用量をリソース使用パターンと比較することによって、潜在的セキュリティ事象を検出することを行わせる命令も含む。開示される有形コンピュータ可読記憶媒体例はまた、実行されるときに、該マシンに、該検出された潜在的セキュリティ事象に深刻度レベルを割り当てることと、割り当てられた深刻度レベルに関して定義されるセキュリティ措置を開始することと、を行わせる命令も含む。
【図面の簡単な説明】

【０００６】
【図１】プロセス制御システム例を例示する。
【図２】プロセス制御アプリケーションを実行する仮想マシン上のセキュリティ事象を検出するためのシステム例を例示する。
【図３】セキュリティ事象を検出するための図２の監視エージェント例の実装例を例示する。
【図４】セキュリティ事象を検出するために図２及び図３の監視エージェント例によって使用されるセキュリティ事象パターンを定義するために使用される、インターフェース例を例示する。
【図５】セキュリティ事象の検出に応答するために図２及び図３の監視エージェント例による措置を定義するために使用される、インターフェース例を例示する。
【図６】図２及び図３の監視エージェントを実装して、セキュリティ事象を検出するために実行され得る方法例を表すフロー図である。
【図７】図２及び図３の監視エージェントを実装して、セキュリティ事象を検出するために実行され得る方法例を表すフロー図である。
【図８】図６及び／または図７によって表される方法を実施して、図２及び図３の監視エージェント例を実装するための機械可読命令を実行するように構造化される、プロセッサシステム例のブロック図である。
【発明を実施するための形態】
【０００７】
本開示は、概してプロセス制御システムに関し、より具体的には、仮想マシンイントロスペクションを通じたセキュリティ事象検出のための方法及び装置に関する。プロセス制御システムは、該制御システム内に配置されるフィールドデバイスを管理するルーティン、制御ストラテジ、及び／またはアルゴリズムを実施するために制御装置と相互作用するプロセス制御アプリケーションを実行する、ワークステーション及び／またはサーバを含む。フィールドデバイスは、例えば、弁、弁保定装置、スイッチ、及び伝送器であってもよく、弁の開閉及びプロセス制御パラメータの測定などのプロセス制御機能を実施してもよい。フィールドデバイスの管理に加えて、制御装置は、フィールドデバイスから受信する情報に基づいて、プロセスデータ（例えば、プロセス制御情報）を生成してもよい。プロセスデータは、プロセス統計値、アラーム、監視情報、プロセス動向情報、診断情報、フィールドデバイス状態情報、及び／またはフィールドデバイスからのメッセージを含んでもよい。
【０００８】
プロセス制御システムは、多くの場合、プロセス制御システムに関わるワークステーション及び／またはサーバを悪意のある攻撃から保護するために、例えば、アンチウイルスソフトウェア、アプリケーションホワイトリスト登録、ソフトウェアファイアウォール、及び／またはオペレーティングシステムセキュリティメカニズムなどの、セキュリティユーティリティに依存する。しかしながら、かかるセキュリティユーティリティは、すり抜けられる可能性がある。現在のマルウェアは、アンチウイルスユーティリティを無効にするか、またはそれから逃れ、自身を能動的に動作するプロセス内に挿入することができる。例えば、マルウェアは、ルートキット（例えば、オペレーティングシステムのカーネルに影響を及ぼすマルウェア）及びブートキット（例えば、コンピュータのブートプロセスに影響を及ぼすマルウェア）をインストールすることができる。多くの場合、ルートキット及びブートキットは、その活動を能動的に隠し、セキュリティユーティリティの前にロードされる。これは、マルウェアが自身を確立し、検出されることなく危険に晒されたコンピュータ上に留まることを可能にする。いくつかの実施例では、マルウェアは、危険に晒されたシステムへのバックドアを確立し、攻撃者が通常のセキュリティユーティリティ及び認証証明書（例えば、ユーザ名及びパスワード、認証コードなど）をすり抜けることを可能にする。いくつかの実施例では、マルウェアは、攻撃者がそのマルウェアを使用してより大きな目的を達成する準備ができるまで、休止したまま検出されずにいることがで

きる。

【０００９】

下記に説明される通り、プロセス制御アプリケーションは、仮想化環境（例えば、仮想マシン、コンテナなど）内で実行される。仮想化環境では、管理装置（例えば、ハイパーバイザ、コンテナデーモンなど）は、仮想化環境を管理し（例えば、展開する、終了させる、監視するなど）、仮想化環境の複数のインスタンスが同一の物理的ハードウェア上で実行することを可能にする。それに加えて、管理装置は、仮想化環境を物理的ハードウェアから隔離する。管理装置は、仮想ハードウェア（例えば、仮想プロセッサ（単数または複数）、仮想メモリ、仮想記憶など）、及びそれらの仮想リソースへの加減されたアクセスを作成する。管理装置は、仮想化環境の活動内への可視性を可能にする。例えば、管理装置は、仮想化環境内のメモリ、記憶ディスク、ネットワーク、及び周辺ハードウェア（例えば、ユニバーサルシリアルバス（ＵＳＢ）ドライブ、ＣＤ／ＤＶＤドライブなど）などの使用へのアクセスを有する。仮想化環境は、仮想リソースを使用するゲストオペレーティングシステム（ＯＳ）を実行する。ゲストＯＳは、あたかもそれが自然にインストールされているかのように実行する（例えば、物理的ハードウェアへの直接的なアクセスを有する）。ゲストＯＳにインストールされたマルウェアは、同一の仮想化環境内で実行しているセキュリティユーティリティを無効にする場合がある。しかしながら、かかる構成では、マルウェアは、異なる仮想化環境で実行している管理装置またはプロセス制御アプリケーションには影響を及ぼすことができない。

【００１０】

その活動を遮蔽するようにプログラムされたマルウェアを検出するために、監視エージェントが管理装置によって展開される。下記に説明される通り、監視エージェントは、その監視エージェントが監視している仮想化環境とは分離している。例えば、監視エージェントは、監視されている仮想マシンまたはコンテナとは異なる仮想マシン、コンテナ、または物理的マシン内で実行している。監視エージェントは、１つ以上の仮想化環境の活動を監視する。かかる様式では、仮想化環境内のマルウェアは、監視エージェントに影響を及ぼすことができない。いくつかの実施例では、監視エージェントは、管理装置に組み込まれる。

【００１１】

下記に説明されるいくつかの実施例では、監視エージェントは、イントロスペクションを使用して仮想化環境を監視する。通常、仮想化環境はホスト上で実行している他のプロセスから隔離されているため、仮想化リソースの使用に関する情報は、他のプロセスに利用可能ではない。イントロスペクションは、仮想化環境の外部のアプリケーション（例えば、監視エージェント）が、管理装置による仮想化リソースの使用量を調査するためのアクセスを認められているプロセスである。イントロスペクションは、監視エージェントが、ゲストＯＳ及び／またはゲストＯＳによって実行されるプロセス制御アプリケーションの状態（例えば、メモリ値、プロセッサレジスタなど）を分析することを可能にする。イントロスペクションを通じて、監視エージェントは、仮想化環境のリソース使用量を監視する。例えば、監視エージェントは、メモリ使用量、記憶ディスク使用量、ネットワーク使用量、及び周辺ハードウェア使用量などを監視することができる。

【００１２】

監視エージェントは、リソース使用量をセキュリティ事象パターンと比較する。セキュリティ事象パターンは、マルウェアが仮想化環境にインストールされている可能性を示す、ゲストＯＳによるリソースの使用を定義する。例えば、セキュリティ事象パターンは、アドレス解決プロトコル（ＡＲＰ）テーブルが汚染されていることを示すネットワーク使用量を検出するように定義され得る。かかるシナリオでは、ＡＲＰテーブルは、ネットワーク上のコンピュータのアドレスの短期メモリである。ＡＲＰテーブルを汚染することによって、マルウェアは、例えば、ネットワーク上での介入者攻撃を促進するために、コンピュータのＡＲＰテーブル上に偽のアドレスを置くことができる。汚染されたＡＲＰテーブルを検出するためのセキュリティ事象パターン例としては、インターネットプロトコル

（ＩＰ）アドレスマッピングへの以前の値とは異なる媒体アクセス制御（ＭＡＣ）アドレスと共に伝送されたイーサネットフレームを検出することが挙げられ得る。

【００１３】

下記に説明される通り、セキュリティ事象パターンは、異なる深刻度のレベルに関連付けられる。深刻度のレベルは、マルウェアが仮想化環境にインストールされている可能性及び／または検出されたマルウェアの有害性を示す、記号表示及び／または数値であり得る。例えば、セキュリティ事象パターンは、高、中、及び／または低深刻度に関連付けられ得る。例えば、無許可のＵＳＢデバイスはマルウェアのソースであり得るため、ＵＳＢデバイスの挿入を検出するセキュリティ事象パターンは、低深刻度レベルに関連付けられ得る。別の例として、ネットワークを通じて仮想化環境に接続する多数の試みを検出するセキュリティ事象パターンは、中深刻度レベルに関連付けられ得る。別の例として、特定のメモリ値が仮想化環境の初期インスタンス化と異なることを検出するセキュリティ事象パターンは、高深刻度レベルに関連付けられ得る。

【００１４】

下記に説明される通り、監視エージェントは、検出されるセキュリティ事象パターンの深刻度に基づいて、１つ以上の措置を開始し得る。例えば、低深刻度のセキュリティ事象パターンに関して、監視エージェントは、警告をワークステーション上に表示させる、及び／または警告メッセージを管理者に送信させてもよい。別の例として、中深刻度のセキュリティ事象パターンに関して、監視エージェントは、仮想化環境を、読み取り専用モードにさせてもよい（例えば、プロセス制御アプリケーションは、フィールドデバイスの状態を読み取ることのみできるが、そのフィールドデバイスにコマンドを発行することはできない）。別の例として、深刻なセキュリティ事象パターンに関して、監視エージェントは、代替仮想環境を展開させ、影響を受けた仮想環境を終了させてもよい。

【００１５】

下記に説明される通り、いくつかの実施例では、監視エージェントは、仮想化環境に整合性レベル（例えば、信用レベル）を割り当てる。整合性レベルは、仮想化環境が危険に晒されている可能性を表す。監視エージェントがセキュリティ事象パターンを検出すると、監視エージェントは、そのセキュリティ事象パターンに関連付けられる深刻度に応じて整合性レベルを調節する。例えば、仮想化環境が初めに展開されるとき、監視エージェントは、仮想化環境に１００の整合性レベルを割り当てることができる。かかる例では、低レベルのセキュリティ事象パターンの検出に際して、監視エージェントは、整合性レベルを設定した量（例えば、１、５、１０など）だけ引き下げることができる。いくつかの実施例では、検出されるセキュリティ事象パターンの効果は、時間と共に減衰する。例えば、監視エージェントは、低深刻度のセキュリティ事象パターンの整合性レベルに対する効果を、低深刻度のセキュリティ事象パターンが検出された後、２４時間後に除去してもよい。いくつかの実施例では、管理者は、１つ以上の整合性レベル閾値を設定し、整合性レベル閾値を満たす整合性レベルに応答して実行するように、監視エージェントのためにセキュリティ措置を定義する。例えば、１００中７５の整合性レベル閾値において、監視エージェントは、管理者に警告を送信してもよい。別の例として、１００中５０の整合性レベル閾値において、監視エージェントは、仮想化環境内で実行しているアプリケーションが、フィールドデバイスの状態を読み取ることのみできるが、フィールドデバイスまたは外部コンピュータにコマンドを送信することはできないように、仮想化環境を設定してもよい。別の例として、１００中２５の整合性レベル閾値において、監視エージェントは、代替仮想環境を展開させ、影響を受けた仮想環境を終了させてもよい。

【００１６】

下記に説明される通り、管理者は、例えば、メモリ使用量、記憶ディスク使用量、ネットワーク使用量、及びハードウェア使用量に基づいて、セキュリティ事象パターン定義する。メモリ使用量の例としては、揮発性メモリ及び不揮発性メモリからの読み取り及び／または揮発性メモリ及び不揮発性メモリへの書き込み、メモリに記憶される値、ならびに／またはメモリへのアクセスに関連する機能の使用（例えば、メモリ割り当て、メモリゼ

ロ化など）が挙げられる。記憶ディスク使用量の例としては、記憶ディスクへの読み取り及び書き込み、記憶ディスクに記憶される値（例えば、マスターブートレコード、レジストリファイルなど）、ならびにメモリへのアクセスに関連する機能の使用（例えば、ディレクトリ管理、ボリューム管理など）が挙げられる。ネットワーク使用量の例としては、ネットワーク接続上で送信及び受信されるメッセージ、接続試行などが挙げられる。ハードウェア使用量の例としては、プロセッサ使用量、ハードウェア割り込み、周辺ハードウェアの検出、キーボード入力などが挙げられる。いくつかの実施例では、管理者は、セキュリティ事象パターンの検出に応答して実施するように、監視エージェントのために措置を定義する。それに加えて、いくつかの実施例では、管理者は、セキュリティ事象パターンの検出が仮想化環境の整合性レベルに対して有する効果を定義する。

【００１７】

図１は、本明細書に説明されるセキュリティ事象検出システムと共に使用可能なプロセス制御システム例１００を例示する。システム例１００は、フィールドバス１０２（ＨＡＲＴ（登録商標）及び／またはＦＯＵＮＤＡＴＩＯＮ（商標）フィールドバスなど）、高速分散バス、内蔵先行制御、ならびに先行ユニット及びバッチ管理を含む、１つ以上のスマートプラント性能を統合するプラントプロセス制御アーキテクチャを用いる。プロセス制御システム１００内のフィールドバスネットワークフィールドデバイス１０４は、デバイスの管理、構成、監視、及び診断などを含む多様なアプリケーションのための下部構造を提供する。

【００１８】

プロセス制御システム例１００は、フィールドデバイス例１０４、制御装置例１０６、Ｉ／Ｏデバイス例１０８、ワークステーション例１１０、及びサーバ例１１２を含む。フィールドデバイス例１０４は、プロセスを制御及び／または監視し、また例えば、弁、センサ、近接スイッチ、モータ始動装置、ドライブなどを含むことができる。例示される実施例では、フィールドデバイス１０４は、フィールドバス１０２を介してＩ／Ｏデバイス１０８に通信可能に連結される。Ｉ／Ｏデバイス例１０８は、フィールドデバイス例１０４との通信を促進する。Ｉ／Ｏデバイス例１０８は、多様なフィールドデバイス１０４と（例えば、デジタル及び／またはアナログ通信を介して）通信するための多様なモジュールを支持する。例えば、Ｉ／Ｏデバイス１０８は、３線式温度プローブと連動するためのアナログモジュール、及びデジタル弁制御装置と連動するためのデジタルモジュールを有してもよい。Ｉ／Ｏデバイス例１０８は、フィールドデバイス１０４からデータを受信し、そのデータを、制御装置例１０６によって処理され得る通信に変換する。それに加えて、Ｉ／Ｏデバイス例１０８は、制御装置例１０６からのデータ及び／または通信を、フィールドデバイス１０４によって処理され得るフォーマットに変換する。いくつかの実施例では、Ｉ／Ｏデバイス１０８及び制御装置（単数または複数）１０６は、１つのユニットに組み合わされる。

【００１９】

制御装置例１０６は、有線または無線ネットワーク（例えば、ＬＡＮ、ＷＡＮ、インターネットなど）を介してワークステーション１１０及び／またはサーバ１１２に連結される。制御装置例１０６は、ルーティンを制御して、例えば、監視アプリケーション、アラーム管理アプリケーション、プロセス動向及び／または履歴アプリケーション、診断アプリケーション、バッチプロセス及び／またはキャンペーン管理アプリケーション、統計アプリケーション、ストリーミング動画アプリケーション、先行制御アプリケーション、安全計装アプリケーション、事象アプリケーションなどを含むプロセス制御アプリケーションのために、フィールドデバイス１０４からの出力に基づいてプロセスデータを算出する。制御装置１０６は、周期的な間隔で、及び／またはプロセスデータの処理もしくは生成時に、プロセスデータをワークステーション１１０及び／またはサーバ１１２に転送する。制御装置１０６によって伝送されるプロセスデータとしては、プロセス制御値、データ値、アラーム情報、テキスト、ブロックモード要素状態情報、診断情報、エラーメッセージ、パラメータ、事象、及び／またはデバイス識別子が挙げられ得る。

【００２０】
図１に例示される実施例では、ワークステーション１１０及び／またはサーバ１１２は、プロセス制御アプリケーションを実行する。プロセス制御アプリケーションは、制御装置例１０６と通信して、フィールドデバイス１０４を監視、制御、及び／または診断する。例えば、プロセス制御アプリケーションは、制御自動化、プロセス制御システム１００の図形表示、変化管理、プロセス制御編集、データ収集、データ分析などを含んでもよい。いくつかの実施例では、ワークステーション１１０は、プロセスデータを図形形式にして、ワークステーション１１０のユーザが、フィールドデバイス１０４によって生成されるプロセスデータを（アプリケーションを介して）図形的に見ることを可能にするために、ユーザインターフェースを介してプロセス制御アプリケーションを表示する。いくつかの実施例では、プロセス制御アプリケーションがサーバ１１２上で実行しているとき、操作者は、プロセス制御アプリケーションにアクセスするためにワークステーション（例えば、ワークステーション１１０）からサーバ１１２へのリモート接続を確立することができる。

【００２１】
いくつかの実施例では、セキュリティ及び拡張性を改善するために、プロセス制御アプリケーションは、ワークステーション１１０及び／またはサーバ１１２上の仮想化環境（例えば、仮想マシン、コンテナなど）内のゲストオペレーティングシステム（ＯＳ）によって実行されてもよい。下記にさらに詳細に開示される通り、仮想化環境は、ゲストＯＳによって実行されるプロセス制御アプリケーションをワークステーション１１０及び／またはサーバ１１２の物理的ハードウェアから隔離する。仮想化環境でのプロセス制御アプリケーションの実行はまた、プロセス制御アプリケーションが互いに隔離されることを可能にする。例えば、あるプロセス制御アプリケーションが危険に晒されている（例えば、セキュリティ事象を有する）場合、異なる仮想化環境内の同一のワークステーション１１０及び／またはサーバ１１２上で実行している他のプロセス制御アプリケーションは、影響を受けないままである。

【００２２】
図２は、プロセス制御アプリケーション２０４を有する仮想マシン２０２上でセキュリティ事象を検出するためのシステム例２００を例示する。例示される実施例では、システム２００は、ホスト２０６（例えば、図１のワークステーション１１０、サーバ１１２、制御装置１０８、Ｉ／Ｏデバイス１０８など）上で実行する。ホスト２０６は、物理的ハードウェア２０８（例えば、プロセッサ（単数または複数）、メモリ、記憶装置、周辺デバイス、ネットワークアクセスなど）及びハイパーバイザ２１０を含む。ハイパーバイザ例２１０は、物理的ハードウェア２０８を管理し、複数の仮想マシン２０２がホスト２０６上で実行することを可能にする仮想化ハードウェア（例えば、仮想化プロセッサ（単数または複数）、仮想化メモリ、仮想化記憶など）を作成する。ハイパーバイザ例２１０は、仮想マシン例（単数または複数）２０２を隔離し、物理的ハードウェア例２０８へのアクセスを制御する。かかる様式では、仮想マシン２０２上で実行しているゲストＯＳ２１２（例えば、Ｗｉｎｄｏｗｓ（登録商標）、Ｌｉｎｕｘ、ＵＮＩＸなど）を危険に晒すセキュリティ事象が検出されると、他の仮想マシン及び／または物理的リソース２０８は、保護される。

【００２３】
例示される実施例では、監視エージェント２１４は、システム２００内で動作する。監視エージェント例２１４は、セキュリティ事象パターンを検出するように構造化される。セキュリティ事象パターンは、マルウェアがゲストＯＳ２１２上に存在している可能性を示す、メモリ使用量２１６、記憶ディスク使用量２１８、ネットワーク使用量２２０、及び／またはハードウェア使用量２２２のパターンである。監視エージェント例２１４は、仮想マシン例２０２から分離しており、その結果、ゲストＯＳ例２１２上に存在するマルウェアは、監視エージェント２１４に影響を及ぼすことができない。例えば、監視エージェント２１４は、プロセス制御アプリケーション２０４とは異なる仮想マシンまたは異な

るコンテナ内で実行していてもよい。いくつかの実施例では、監視エージェント２１４は、ハイパーバイザ２１０内に統合される。

【００２４】

監視エージェント例２１４は、仮想マシン２０２のメモリ使用量２１６、記憶ディスク使用量２１８、ネットワーク使用量２２０、及び／またはハードウェア使用量２２２への即時アクセスを促進するイントロスペクション機能を含む。イントロスペクション機能は、監視エージェント２１４がハイパーバイザ２１０から仮想マシン２０２に関する情報を要求することを可能にする。ハイパーバイザ２１０は仮想リソースを作成及び／または維持するため、イントロスペクション機能は、監視エージェント２１４が、監視エージェント２１４が仮想マシン２０２によって使用される物理的リソースの内容及び使用量を調査し得るように、仮想リソースを物理的リソース２０８に関連付けることを可能にする。例えば、ハイパーバイザ２１０は、仮想メモリを物理的メモリにマッピングする仮想メモリページテーブルを維持し得る。かかる実施例では、監視エージェント２１４が仮想マシン２０２によって使用される仮想メモリを監視するとき、イントロスペクション機能は、監視エージェント２１４が、物理的メモリ内のどの場所が仮想マシン２０２によって使用されているかを知るために仮想メモリページテーブルにアクセスすることを可能にする。

【００２５】

図２に例示される実施例では、監視エージェント２１４は、メモリ使用量２１６、記憶ディスク使用量２１８、ネットワーク使用量２２０、及び／またはハードウェア使用量２２２を即時に監視して（例えば、リソース使用量２１６～２２２は、その発生の数秒以内に監視される）、マルウェアが仮想マシン２０２にインストールされているという推測をもたらすセキュリティ事象パターンを検出する。例えば、リソースモニタ２１４は、記憶ディスク上のマスターブートレコードの変化を、その変化の発生の直後に検出することができる。いくつかの実施例では、監視エージェント２１４は、別個の事象を検出する。例えば、監視エージェント２１４は、特定のメモリ値がいつ変化するかを検出することができる。いくつかの実施例では、監視エージェント２１４は、連続的な事象を検出する。例えば、監視エージェント２１４は、イーサネットフレームを監視して、ＡＲＰテーブルの汚染を検出することができる（例えば、インターネットプロトコル（ＩＰ）アドレスマッピングへの以前の値とは異なる媒体アクセス制御（ＭＡＣ）アドレスを有するイーサネットフレームを検出する）。

【００２６】

いくつかの実施例では、監視エージェント２１４は、管理者と通信して、セキュリティ事象パターンが検出されると管理者に警告する、及び／または特定の仮想マシン２０２の整合性レベルを通信する。いくつかの実施例では、監視エージェント２１４は、ハイパーバイザ２１０と通信して、検出されたセキュリティ事象パターンへの応答を開始する。例えば、特定のセキュリティ事象パターンに応答して、監視エージェント２１４は、仮想マシン２０２上で実行しているプロセス制御アプリケーション２０４が、フィールドデバイス１０４から状態更新を受信することはできるが、プロセス制御アプリケーション２０４が、フィールドデバイス１０４にコマンドを発行するか、または他のワークステーション及び／またはサーバと通信することはできないように、影響を受けた仮想マシン２０２に入力されるネットワークトラフィックのみを可能にするようにハイパーバイザ２１０にコマンドすることができる。

【００２７】

いくつかの実施例では、監視エージェント２１４は、時折（例えば、周期的に、非周期的になど）、仮想マシン２０２のスナップショットを取得させる。スナップショットは、特定の時点の仮想マシン２０２の状態（例えば、ディスクデータ、メモリ値、構成など）のコピーである。スナップショットは、将来、仮想マシン２０２をキャプチャした状態に戻すために使用することができる。いくつかの実施例では、スナップショットは、（例えば、管理者によって）予定されてもよい。いくつかのかかる実施例では、監視エージェント２１４は、特定の深刻度（例えば、中深刻度、高深刻度など）のセキュリティ事象パタ

ーンが検出された、及び／または仮想マシン２０２の整合性レベルが特定の閾値を下回る場合に、スナップショットを中止または遅延してもよい。いくつかの実施例では、監視エージェント２１４は、整合性レベルが閾値を上回る場合にスナップショットを取得させてもよい。

【００２８】

いくつかの実施例では、深刻なセキュリティ事象パターンの検出に応答して、及び／または仮想マシン２０２の整合性レベルが閾値を下回る場合に、監視エージェント２１４は、新たな仮想マシン２０２をハイパーバイザ２１０によって展開させることができる。いくつかの実施例では、新たな仮想マシン２０２は、ゲストＯＳ２０４のクリーンインストールに基づく。いくつかの実施例では、新たな仮想マシン２０２は、セキュリティ事象が検出される前の仮想マシン２０２のスナップショットに基づく。いくつかのかかる実施例では、機能性（例えば、フィールドデバイス１０４、通信表示デバイスなどとの通信）が、新たな仮想マシン２０２に移動される。いくつかの実施例では、新たな仮想マシン２０２がフィールドデバイス１０４と通信した後、監視エージェント２１４は、危険に晒されている仮想マシン２０２を終了させる。

【００２９】

図３は、セキュリティ事象を検出するための図２の監視エージェント例２１４の実装例を例示する。例示される実施例では、監視エージェント２１４は、リソースモニタ３００、セキュリティ事象ハンドラ３０２、セキュリティ事象パターン管理装置３０４、及びセキュリティ事象パターンデータベース３０６を含む。リソースモニタ例３００は、仮想マシン２０２のメモリ使用量２１６、記憶ディスク使用量２１８、ネットワーク使用量２２０、及び／またはハードウェア使用量２２２を監視する。例示される実施例では、リソースモニタ３００は、リソース２１６～２２２が仮想マシン２０２によって使用されている際にリソース使用量を監視する。リソースモニタ例３００は、セキュリティ事象パターンデータベース３０６からセキュリティ事象パターンを検索して、リソース使用量２１６～２２２のどの態様を監視するかを決定する。例えば、セキュリティ事象パターンがＡＲＰテーブルを監視するように定義される場合、リソースモニタ３００は、ネットワーク使用量２２０を監視して、（例えば、ＡＲＰテーブルが汚染されたことを示す）インターネットプロトコル（ＩＰ）アドレスマッピングへの以前の値とは異なる媒体アクセス制御（ＭＡＣ）アドレスと共に伝送されたイーサネットフレームを検出する。リソース使用量２１６～２２２がセキュリティ事象パターンを満たす場合、リソースモニタ例３００は、セキュリティ事象ハンドラ例３０２に検出されたセキュリティ事象を知らせる。

【００３０】

例示される実施例では、セキュリティ事象ハンドラ３０２は、セキュリティ事象パターンを検出するリソースモニタ３００に応答してセキュリティ措置を実施するように構造化される。セキュリティ措置は、監視エージェント２１４が、セキュリティ事象パターンに定義される、及び／または検出されたセキュリティ事象パターンの深刻度レベルによって定義される通りに実施するための措置である。いくつかの実施例では、セキュリティ措置は、セキュリティ事象パターン及び／または深刻度レベルが定義されるときに、管理者３０８によって定義される。例示される実施例では、セキュリティ事象ハンドラ３０２は、管理者３０８と通信する。いくつかの実施例では、セキュリティ事象ハンドラ３０２は、管理者３０８に通知を送信する。いくつかの実施例では、通知は、検出されたセキュリティ事象パターン及びタイムスタンプに関する情報を含む。いくつかの実施例では、セキュリティ事象ハンドラ３０２は、管理者３０２に、セキュリティ事象パターンが検出されたことを通信システム（例えば、電子メール、テキストメッセージ、音声メッセージなど）を介して通知する。

【００３１】

図３に例示される実施例では、セキュリティ事象ハンドラ３０２は、ハイパーバイザ２１０と通信する。いくつかの実施例では、セキュリティ事象ハンドラ３０２は、仮想マシン２０２による物理的リソース２０８（図２）へのアクセスを制限するように、ハイパー

バイザ２１０に要求を発行する。例えば、セキュリティ事象ハンドラ３０２は、周辺デバイス（例えば、ＵＳＢドライブ、ディスクドライブなど）へのアクセスを防止するように、またはネットワークデバイス上の出力トラフィックを防止するように、要求を発行することができる。いくつかの実施例では、セキュリティ事象ハンドラ３０２は、仮想マシン２０２の新たなコピーが展開され、フィールドデバイス１０４、制御装置１０６、及び／またはＩ／Ｏデバイス１０８との通信が新たな仮想マシン２０２に移動され、古い仮想マシン２０２が終了されることを要求することができる。

【００３２】

いくつかの実施例では、セキュリティ事象ハンドラ３０２は、仮想マシン２０２の整合性レベルを管理する（例えば、監視する、調節するなど）ことができる。整合性レベルは、仮想マシン２０２がマルウェアによって危険に晒されている可能性を表す。いくつかの実施例では、セキュリティ事象ハンドラ３０２がリソースモニタ３００によって検出されるセキュリティ事象パターンを取り扱うときに、セキュリティ事象ハンドラ３０２は、仮想マシン２０２の整合性レベルを調節する。いくつかの実施例では、整合性レベルに対する効果は、セキュリティ事象パターンに関連付けられる深刻度に依存する。例えば、仮想マシン２０２の整合性レベルは、初めに１００に設定され得る。かかる実施例では、低深刻度に関連付けられるセキュリティ事象パターンがリソースモニタ３００によって検出されると、セキュリティ事象ハンドラ３０２は、仮想マシン２０２の整合性レベルを９５に引き下げることができる。管理者３０８は、整合性レベル閾値及び対応するセキュリティ措置を定義することができる。例えば、管理者３０８は、仮想マシン２０２の整合性レベルが７５を下回るときにセキュリティ事象ハンドラ３０２が警告する（例えば、警告メッセージを表示する、メッセージ（例えば、電子メール、ページ、ショートメッセージサービスメッセージ（ＳＭＳ）など）を送信する）ように、整合性レベル閾値を設定することができる。いくつかの実施例では、セキュリティ事象ハンドラ３０２は、検出されたセキュリティ事象の深刻度に基づいて、一定時間後に特定の検出されたセキュリティ事象の効果を逆転する（例えば、仮想マシン２０２の整合性レベルを引き上げるなど）。例えば、仮想マシン２０２の整合性レベルに対する低深刻度のセキュリティ事象の効果は、２４時間後に取り除かれてもよい。

【００３３】

図３の例示される実施例では、セキュリティ事象管理装置３０４は、セキュリティ事象パターンデータベース３０６内でセキュリティ事象パターンを管理する（例えば、作成する、消去する、修正するなど）。図４及び５に関連して下記により詳細に説明される通り、セキュリティ事象管理装置例３０４は、管理者３０８が、セキュリティ事象パターン及び／もしくはセキュリティ措置を定義する、既存のセキュリティ事象パターン及び／もしくはセキュリティ措置を修正する、ならびに／または既存のセキュリティ事象パターン及び／もしくはセキュリティ措置を消去することを可能にする、インターフェースを提供する。

【００３４】

図２の監視エージェント２１４を実装する様式例が図３に例示されているが、図３に例示される要素、プロセス、及び／またはデバイスのうちの１つ以上は、組み合わされる、分割される、再配置される、省略される、取り除かれる、及び／または任意の他の方法で実装されてもよい。さらに、リソースモニタ例３００、セキュリティ事象ハンドラ例３０２、セキュリティ事象パターン管理装置例３０４、及び／またはより一般的には図２の監視エージェント例２１４は、ハードウェア、ソフトウェア、ファームウェア、ならびに／またはハードウェア、ソフトウェア、及び／もしくはファームウェアの任意の組み合わせによって実装されてもよい。したがって、例えば、リソースモニタ例３００、セキュリティ事象ハンドラ例３０２、セキュリティ事象パターン管理装置例３０４、及び／またはより一般的には図２の監視エージェント例２１４のうちのいずれかは、１つ以上のアナログもしくはデジタル回路（単数もしくは複数）、論理回路、プログラム可能プロセッサ（単数もしくは複数）、特定用途向け集積回路（単数もしくは複数）（ＡＳＩＣ（単数もしく

は複数））、プログラム可能論理デバイス（単数もしくは複数）（ＰＬＤ（単数もしくは複数））、及び／またはフィールドプログラム可能論理デバイス（単数もしくは複数）（ＦＰＬＤ（単数もしくは複数））によって実装されてもよい。本特許を請求する装置またはシステムのいずれかが純粋にソフトウェア及び／またはファームウェア実装を網羅するように読み取ると、リソースモニタ例３００、セキュリティ事象ハンドラ例３０２、及び／またはセキュリティ事象パターン管理装置例３０４のうちの少なくとも１つは、ソフトウェア及び／またはファームウェアを記憶する有形コンピュータ可読記憶デバイスまたは記憶ディスク、例えば、メモリ、デジタル多用途ディスク（ＤＶＤ）、コンパクトディスク（ＣＤ）、ブルーレイディスクなどを含むように本明細書に明白に定義される。またさらに、図２の監視エージェント例２１４は、図３に例示されるものに加えてか、もしくはそれらの代わりに、１つ以上の要素、プロセス、及び／もしくはデバイスを含んでもよく、ならびに／または例示される要素、プロセス、及びデバイスのいずれかもしくは全てのうちの複数を含んでもよい。

【００３５】

図４は、セキュリティ事象を検出するために図２及び３の監視エージェント例２１４によって使用されるセキュリティ事象パターンを定義するために使用され得る、インターフェース例４００を例示する。いくつかの実施例では、インターフェース４００は、セキュリティ事象管理装置例３０４（図３）によって提供される。インターフェース例４００は、セキュリティ事象パターンデータベース例３０６（図３）に記憶されるセキュリティ事象パターンを管理する（例えば、作成する、消去する、修正するなど）ために使用される。例示される実施例では、インターフェース４００は、名称フィールド例４０２、深刻度フィールド例４０４、カテゴリフィールド例４０５、及び条件フィールド例４０６を含む。名称フィールド例４０２は、管理者例３０８（図３）がセキュリティ事象パターンに固有の識別子を割り当てるのを促進するために提供される。深刻度フィールド例４０４は、管理者例３０８が、マルウェアが仮想マシン２０２（図２）上にインストールされている可能性を示す深刻度レベル（例えば、高、中、低、危機的、緊急、重篤、最小など）を割り当てるのを促進するために提供される。

【００３６】

例示される実施例では、カテゴリフィールド４０５は、セキュリティ事象パターンが関連するリソースの種類を示すために提供される。例えば、カテゴリフィールド４０５は、特定のセキュリティ事象パターンがメモリ使用量２１６（図２）に関連していることを示すことができる。条件フィールド例４０６は、管理者例３０８が、どの条件がメモリ使用量２１６、記憶ディスク使用量２１８、ネットワーク使用量２２０、及び／またはハードウェア使用量２２２（図２）に関連するかを定義し、合致する場合、セキュリティ事象パターンを構成する、１つ以上の条件文を作成するのを促進するために提供される。いくつかの実施例では、条件文は、監視エージェントがメモリ使用量２１６、記憶ディスク使用量２１８、ネットワーク使用量２２０、及び／またはハードウェア使用量２２２の監視を通じてアクセスを有する特性に関連する、ブール文及び／または閾値である。

【００３７】

図５は、セキュリティ事象パターンの検出に応答するために図２及び３の監視エージェント例によって使用される措置を定義するために使用され得る、インターフェース例５００を例示する。いくつかの実施例では、インターフェース５００は、セキュリティ事象管理装置例３０４（図３）によって提供される。インターフェース例５００は、管理者（例えば、図３の管理者３０８）が、セキュリティ事象パターンを検出するリソースモニタ３００（図３）に応答してセキュリティ事象ハンドラ例３０２（図３）によって実施されるための措置を定義するのを促進する。例示される実施例では、セキュリティハンドラ３０２によって実施されるための措置は、深刻度に基づいて定義される。例えば、中深刻度のセキュリティ事象パターンの検出に応答して、セキュリティハンドラ３０２は、フィールドデバイス１０４にコマンドを発行するプロセス制御アプリケーション２０４（図２）の能力を制限することができる。いくつかの実施例では、セキュリティハンドラ３０２によ

って実施されるための措置は、特定のセキュリティ事象パターンに基づいてもよい。

【００３８】

図２及び３の監視エージェント例２１４を実装するための方法例を表すフローチャートが、図６及び／または７に示される。この実施例では、方法は、プロセッサ、例えば、図８に関連して下記に説明されるプロセッサプラットフォーム例８００に示されるプロセッサ８１２などによる実行のためのプログラムを含む機械可読命令を使用して、実装することができる。プログラムは、プロセッサ８１２に関連付けられるＣＤ－ＲＯＭ、フロッピーディスク、ハードドライブ、デジタル多用途ディスク（ＤＶＤ）、ブルーレイディスク、またはメモリなどの有形コンピュータ可読記憶媒体上に記憶されるソフトウェアに具現化されてもよいが、プログラム全体及び／またはその一部は、別法として、プロセッサ８１２以外のデバイスによって実行される、及び／またはファームウェアもしくは専用ハードウェアに具現化されてもよい。さらに、プログラム例は、図６及び／または７に例示されるフローチャートを参照して説明されるが、監視エージェント例２１４を実装する多数の他の方法が、別法として使用されてもよい。例えば、ブロックの実行の順序は、変更されてもよく、及び／または説明されるブロックのうちのいくつかは、変更されるか、取り除かれるか、もしくは組み合わされてもよい。

【００３９】

上述の通り、図６及び／または７の方法例は、例えば、ハードディスクドライブ、フラッシュメモリ、読み取り専用メモリ（ＲＯＭ）、コンパクトディスク（ＣＤ）、デジタル多用途ディスク（ＤＶＤ）、キャッシュ、ランダムアクセスメモリ（ＲＡＭ）、及び／または、情報が任意の期間（例えば、一時的にバッファリングするため、及び／または情報をキャッシュするために、長期間、永久的に、短期間）記憶される任意の他の記憶デバイスもしくは記憶ディスクなどの有形コンピュータ可読記憶媒体上に記憶される、コード化された命令（例えば、コンピュータ及び／または機械可読命令）を使用して、実装することができる。本明細書で使用される、有形コンピュータ可読記憶媒体という用語は、任意の種類のコンピュータ可読記憶デバイス及び／または記憶ディスクを含み、伝搬信号を除外し、伝送媒体を除外するように明白に定義される。本明細書で使用される、「有形コンピュータ可読記憶媒体」及び「有形機械可読記憶媒体」は、互換的に使用される。それに加えてまたは別法として、図６及び／または７の方法例は、例えば、ハードディスクドライブ、フラッシュメモリ、読み取り専用メモリ、コンパクトディスク、デジタル多用途ディスク、キャッシュ、ランダムアクセスメモリ、及び／または、情報が任意の期間（例えば、一時的にバッファリングするため、及び／または情報をキャッシュするために、長期間、永久的に、短期間）記憶される任意の他の記憶デバイスもしくは記憶ディスクなどの非一時的コンピュータ及び／または機械可読媒体上に記憶される、コード化された命令（例えば、コンピュータ及び／または機械可読命令）を使用して、実装することができる。本明細書で使用される、非一時的コンピュータ可読媒体という用語は、任意の種類のコンピュータ可読記憶デバイス及び／または記憶ディスクを含み、伝搬信号を除外し、伝送媒体を除外するように明白に定義される。本明細書で使用される、語句「少なくとも」が、請求項の前提部分において移行用語として使用される場合、それは、用語「含む（ｃｏｍｐｒｉｓｉｎｇ）」が非限定であるのと同一の様式で非限定である。

【００４０】

図６は、セキュリティ事象を検出し、応答するための、図２及び３の監視エージェントを実装するために使用され得る方法例を表すフロー図である。初めに、リソースモニタ３００（図３）は、プロセス制御アプリケーション２０４（図２）を実行している仮想マシン２０２（図２）によるリソースの使用量を監視する（ブロック６０２）。ブロック６０２におけるリソースの使用量の監視は、図７と共に下記にさらに説明される。リソースモニタ３００は、潜在的セキュリティ事象が検出されるまで、リソース使用量を継続して監視する（ブロック６０４）。リソースモニタ３００は、検出された潜在的セキュリティ事象に深刻度レベルを割り当てた（ブロック６０６）。いくつかの実施例では、深刻度レベルは、セキュリティ事象パターンデータベース３０６に記憶されるセキュリティ事象パタ

ーンに基づいて割り当てられる。セキュリティ事象ハンドラ３０２（図３）は、割り当てられた深刻度レベルに基づいてセキュリティ措置を開始する（ブロック６０８）。いくつかの実施例では、実施されるためのセキュリティ措置は、管理者３０８（図３）によって予め定義される。いくつかの実施例では、セキュリティ事象ハンドラ３０２は、検出される潜在的セキュリティ事象の深刻度に基づいて、仮想マシン２０２の整合性レベルを調節する。リソースモニタ３００は、仮想マシン２０２の監視が継続されるべきかどうかを決定する（ブロック６１０）。仮想マシン２０２の監視が継続される場合、リソースモニタ３００は、潜在的セキュリティ事象を検出するために仮想マシン２０２によって使用されるリソースの使用量を監視する（ブロック６０２）。そうではない場合、仮想マシン２０２の監視は継続されず、方法６００は終了する。

【００４１】

図７は、図６のブロック６０２におけるセキュリティ事象の検出を実装するために実施され得る方法例を表す、フロー図である。初めに、リソースモニタ３００（図３）は、仮想マシン２０２（図２）のメモリ使用量２１６（図２）を監視し、その使用量をセキュリティパターンと比較する（ブロック７００）。リソースモニタ３００は、メモリ使用量２１６が、セキュリティ事象パターンデータベース３０６（図３）内のセキュリティ事象パターンに合致するかどうか（例えば、条件を満たす、閾値を満たすなど）を決定する（ブロック７０２）。いくつかの実施例では、メモリ使用量２１６は、図４の種類フィールド４０５によって示される通り、メモリ使用量に関連するセキュリティ事象パターンデータベース３０６内のセキュリティ事象パターンと比較される。メモリ使用量２１６がセキュリティ事象パターンに合致するとリソースモニタ３００が決定する場合、リソースモニタ３００は、潜在的メモリ関連セキュリティ事象が発生したことを（例えば、セキュリティ事象ハンドラ３０２に）示す（ブロック７０３）。

【００４２】

リソースモニタ３００は、仮想マシン２０２の記憶ディスク使用量２１８（図２）を監視する（ブロック７０６）。リソースモニタ３００は、記憶ディスク使用量２１８が、セキュリティ事象パターンデータベース３０６内のセキュリティ事象パターンに合致するかどうか（例えば、条件を満たす、閾値を満たすなど）を決定する（ブロック７０８）。いくつかの実施例では、記憶使用量２１８は、種類フィールド４０５によって示される通り、記憶ディスク使用量に関連するセキュリティ事象パターンデータベース３０６内のセキュリティ事象パターンと比較される。記憶ディスク使用量２１８がセキュリティ事象パターンに合致するとリソースモニタ３００が決定する場合、リソースモニタ３００は、潜在的記憶ディスクセキュリティ事象が発生したことを（例えば、セキュリティ事象ハンドラ３０２に）示す（ブロック７０９）。

【００４３】

リソースモニタ３００は、仮想マシン２０２のネットワーク使用量２２０（図２）を監視する（ブロック７１０）。リソースモニタ３００は、ネットワーク使用量２２０が、セキュリティ事象パターンデータベース３０６内のセキュリティ事象パターンに合致するかどうか（例えば、条件を満たす、閾値を満たすなど）を決定する（ブロック７１２）。いくつかの実施例では、ネットワーク使用量２２０は、種類フィールド４０５によって示される通り、ネットワーク使用量に関連するセキュリティ事象パターンデータベース３０６内のセキュリティ事象パターンと比較される。ネットワーク使用量２２０がセキュリティ事象パターンに合致するとリソースモニタ３００が決定する場合、リソースモニタ３００は、潜在的ネットワーク関連セキュリティ事象が発生したことを（例えば、セキュリティ事象ハンドラ３０２に）示す（ブロック７１３）。

【００４４】

リソースモニタ３００は、仮想マシン２０２のハードウェア使用量２２２（図２）を監視する（ブロック７１４）。リソースモニタ３００は、ハードウェア使用量２２２が、セキュリティ事象パターンデータベース３０６内のセキュリティ事象パターンに合致するかどうか（例えば、条件を満たす、閾値を満たすなど）を決定する（ブロック７１６）。い

くつかの実施例では、ハードウェア使用量２２２は、種類フィールド４０５によって示される通り、ハードウェア使用量に関連するセキュリティ事象パターンデータベース３０６内のセキュリティ事象パターンと比較される。ハードウェア使用量２２２がセキュリティ事象パターンに合致するとリソースモニタ３００が決定する場合、リソースモニタ３００は、潜在的ハードウェア関連セキュリティ事象が発生したことを（例えば、セキュリティ事象ハンドラ３０２に）示す（ブロック７１７）。次に、方法７００は終了する。

【００４５】

図８は、図６及び／または７の方法ならびに図２及び３の監視エージェント２１４を実装するための命令を実行するように構造化される、プロセッサプラットフォーム例８００のブロック図である。プロセッサプラットフォーム８００は、例えば、サーバ、パーソナルコンピュータ、ワークステーション、または任意の他の種類のコンピューティングデバイスであり得る。

【００４６】

例示される実施例のプロセッサプラットフォーム８００は、プロセッサ８１２を含む。例示される実施例のプロセッサ８１２は、ハードウェアである。例示される実施例では、プロセッサ８１２は、リソースモニタ例３００、セキュリティ事象ハンドラ例３０２、及びセキュリティ事象パターン管理装置例３０６を含む。例えば、プロセッサ８１２は、任意の所望のファミリーまたは製造者からの１つ以上の集積回路、論理回路、マイクロプロセッサ、または制御装置によって実装することができる。

【００４７】

例示される実施例のプロセッサ８１２は、ローカルメモリ８１３（例えば、キャッシュ）を含む。例示される実施例のプロセッサ８１２は、バス８１８を介して揮発性メモリ８１４及び不揮発性メモリ８１６を含むメインメモリと通信する。揮発性メモリ８１４は、同期型動的ランダムアクセスメモリ（ＳＤＲＡＭ）、動的ランダムアクセスメモリ（ＤＲＡＭ）、ＲＡＭＢＵＳ動的ランダムアクセスメモリ（ＲＤＲＡＭ）、及び／または任意の他の種類のランダムアクセスメモリデバイスによって実装されてもよい。不揮発性メモリ８１６は、フラッシュメモリ及び／または任意の他の所望の種類のメモリデバイスによって実装されてもよい。メインメモリ８１４、８１６へのアクセスは、メモリ制御装置によって制御される。

【００４８】

例示される実施例のプロセッサプラットフォーム８００はまた、インターフェース回路８２０も含む。インターフェース回路８２０は、例えば、イーサネットインターフェース、ユニバーサルシリアルバス（ＵＳＢ）、及び／またはＰＣＩエクスプレスインターフェースなどの任意の種類のインターフェース標準によって実装されてもよい。

【００４９】

例示される実施例では、１つ以上の入力デバイス８２２が、インターフェース回路８２０に接続される。入力デバイス（単数または複数）８２２は、ユーザがデータ及びコマンドをプロセッサ８１２に入力することを許可する。入力デバイス（単数または複数）は、例えば、音センサ、マイクロフォン、カメラ（静止またはビデオ）、キーボード、ボタン、マウス、タッチスクリーン、トラックパッド、トラックボール、イソポイント（ｉｓｏｐｏｉｎｔ）、及び／または音声認識システムによって実装することができる。

【００５０】

１つ以上の出力デバイス８２４もまた、例示される実施例のインターフェース回路８２０に接続される。出力デバイス８２４は、例えば、ディスプレイデバイス（例えば、発光ダイオード（ＬＥＤ）、有機発光ダイオード（ＯＬＥＤ）、液晶ディスプレイ、ブラウン管ディスプレイ（ＣＲＴ）、タッチスクリーン、触覚出力デバイス、プリンタ、及び／またはスピーカ）によって実装することができる。したがって、例示される実施例のインターフェース回路８２０は、典型的にはグラフィックドライバカード、グラフィックドライバチップ、またはグラフィックドライバプロセッサを含む。

【００５１】

例示される実施例のインターフェース回路８２０はまた、ネットワーク８２６（例えば、イーサネット接続、デジタル加入者線（ＤＳＬ）、電話線、同軸ケーブル、携帯電話システムなど）を介して外部マシン（例えば、任意の種類のコンピューティングデバイス）とのデータ交換を促進する通信デバイス、例えば、伝送器、受信器、送受信器、モデム、及び／またはネットワークインターフェースカードなども含む。

【００５２】

例示される実施例のプロセッサプラットフォーム８００はまた、ソフトウェア及び／またはデータを記憶するための１つ以上の大容量記憶デバイス８２８も含む。かかる大容量記憶デバイス８２８の例としては、フロッピーディスクドライブ、ハードドライブディスク、コンパクトディスクドライブ、ブルーレイディスクドライブ、ＲＡＩＤシステム、及びデジタル多用途ディスク（ＤＶＤ）ドライブが挙げられる。

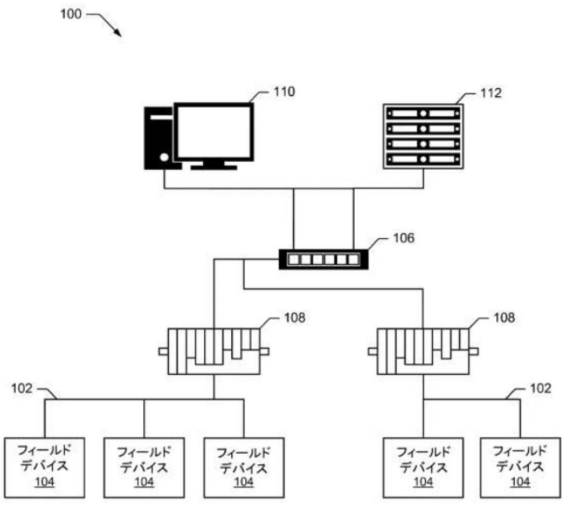
【００５３】

図６及び／または７の方法を実装するためのコード化された命令８３２は、大容量記憶デバイス８２８内、揮発性メモリ８１４内、不揮発性メモリ８１６内、及び／またはＣＤもしくはＤＶＤなどの取り外し可能な有形コンピュータ可読記憶媒体上に記憶されてもよい。

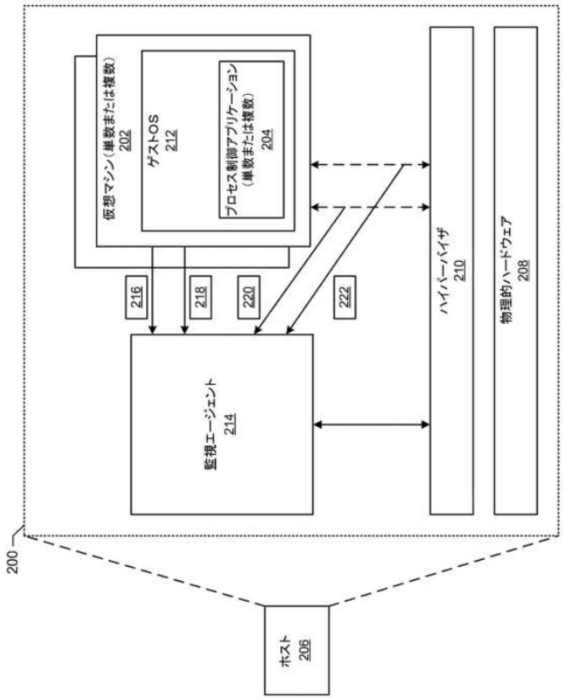
【００５４】

特定の方法、装置、及び製品の例が本明細書に開示されているが、本特許の対象の範囲は、それらに限定されるものではない。対照的に、本特許は、本特許の特許請求の範囲に適正に該当する全ての方法、装置、及び製品を網羅する。

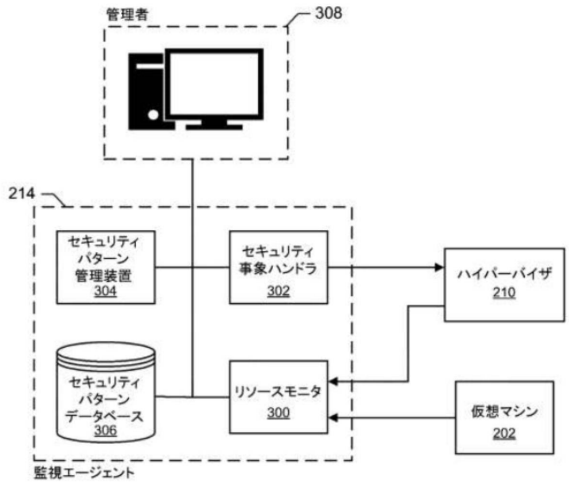
【図１】



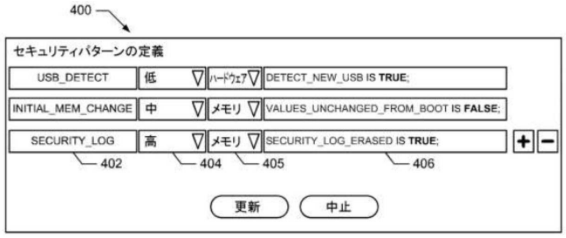
【図２】



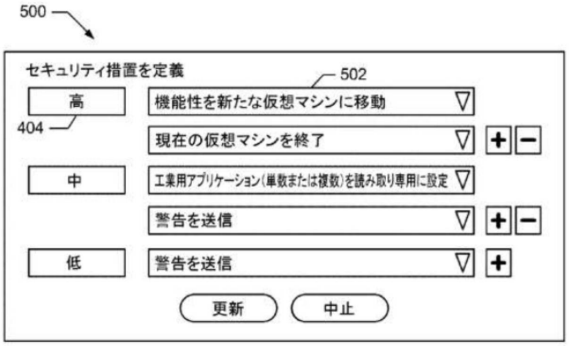
【図３】


管理者
308
214
セキュリティパターン管理装置 304
セキュリティ事象ハンドラ 302
ハイパーバイザ 210
セキュリティパターンデータベース 306
リソースモニタ 300
仮想マシン 202
監視エージェント

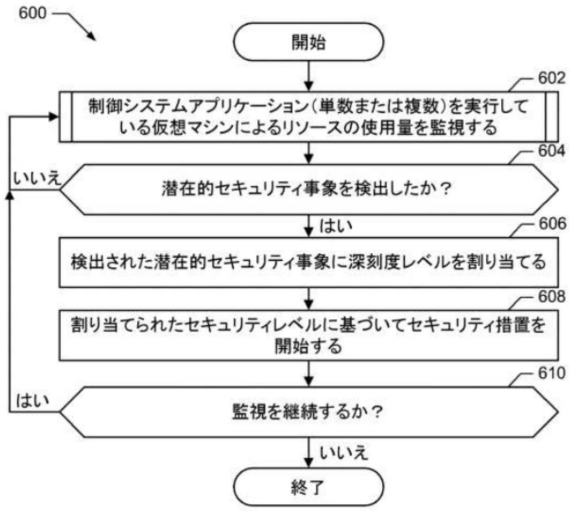
【図４】


400
セキュリティパターンの定義
USB_DETECT
低
ハードウェア
DETECT_NEW_USB IS TRUE;
INITIAL_MEM_CHANGE
中
メモリ
VALUES_UNCHANGED_FROM_BOOT IS FALSE;
SECURITY_LOG
高
メモリ
SECURITY_LOG_ERASED IS TRUE;
402
404
405
406
更新
中止

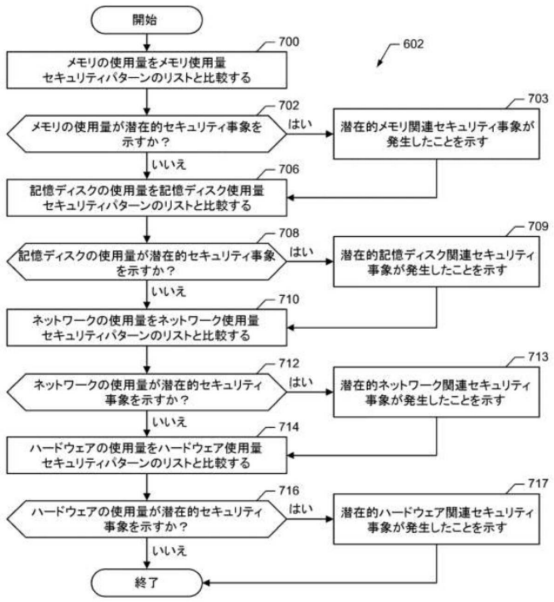
【図５】


500
セキュリティ措置を定義
502
高
404
機能性を新たな仮想マシンに移動
現在の仮想マシンを終了
中
エ業用アプリケーション(単数または複数)を読み取り専用に設定
警告を送信
低
警告を送信
更新
中止

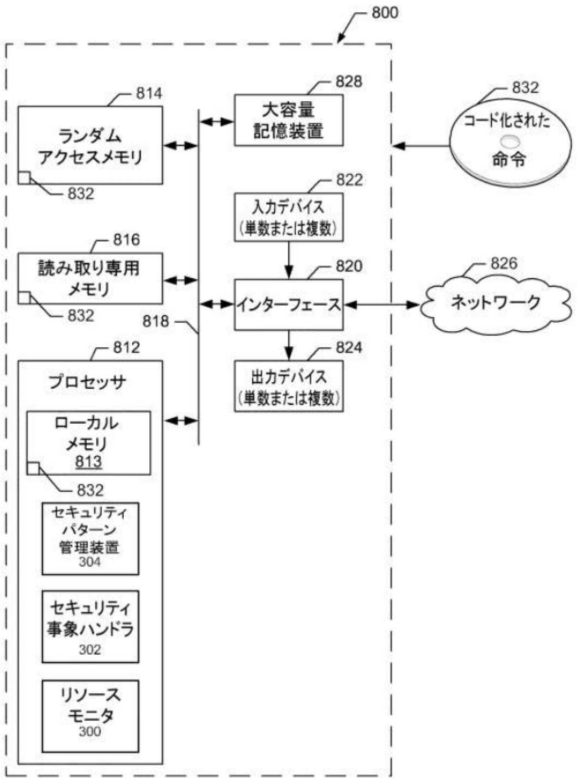
【図６】


600
開始
602
制御システムアプリケーション(単数または複数)を実行している仮想マシンによるリソースの使用量を監視する
604
潜在的セキュリティ事象を検出したか？
いいえ
はい
606
検出された潜在的セキュリティ事象に深刻度レベルを割り当てる
608
割り当てられたセキュリティレベルに基づいてセキュリティ措置を開始する
610
監視を継続するか？
はい
いいえ
終了

【図７】


開始
602
700
メモリの使用量をメモリ使用量セキュリティパターンのリストと比較する
702
メモリの使用量が潜在的セキュリティ事象を示すか？
はい
703
潜在的メモリ関連セキュリティ事象が発生したことを示す
いいえ
706
記憶ディスクの使用量を記憶ディスク使用量セキュリティパターンのリストと比較する
708
記憶ディスクの使用量が潜在的セキュリティ事象を示すか？
はい
709
潜在的記憶ディスク関連セキュリティ事象が発生したことを示す
いいえ
710
ネットワークの使用量をネットワーク使用量セキュリティパターンのリストと比較する
712
ネットワークの使用量が潜在的セキュリティ事象を示すか？
はい
713
潜在的ネットワーク関連セキュリティ事象が発生したことを示す
いいえ
714
ハードウェアの使用量をハードウェア使用量セキュリティパターンのリストと比較する
716
ハードウェアの使用量が潜在的セキュリティ事象を示すか？
はい
717
潜在的ハードウェア関連セキュリティ事象が発生したことを示す
いいえ
終了

【図８】


800
814
ランダム
アクセスメモリ
832
828
大容量
記憶装置
832
コード化された
命令
822
入力デバイス
(単数または複数)
816
読み取り専用
メモリ
832
820
インターフェース
826
ネットワーク
818
812
プロセッサ
824
出力デバイス
(単数または複数)
ローカル
メモリ
813
832
セキュリティ
パターン
管理装置
304
セキュリティ
事象ハンドラ
302
リソース
モニタ
300

フロントページの続き

(72)発明者　ロバート　エー.　ミキサー
アメリカ合衆国　７８６１３　テキサス州　シーダー　パーク　ラリー　ロード　１２７

審査官　岸野　徹

(56)参考文献　特開２０１３－０６１９９４（ＪＰ，Ａ）
特開２０１４－１３０６４８（ＪＰ，Ａ）
特開２０１０－０１５５１３（ＪＰ，Ａ）
特開２００８－１２３０６５（ＪＰ，Ａ）
特開２０１３－１６１２８３（ＪＰ，Ａ）
特表２００７－５３６６５７（ＪＰ，Ａ）
米国特許出願公開第２０１５／００１３００８（ＵＳ，Ａ１）
特表２０１５－５１９６５２（ＪＰ，Ａ）
米国特許出願公開第２０１５／０００７３５０（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／５３
Ｇ０６Ｆ　９／４５５