(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7374792号
(P7374792)

(45)発行日　令和5年11月7日(2023.11.7)

(24)登録日　令和5年10月27日(2023.10.27)

(51)国際特許分類

Ｇ０６Ｆ　21/57　(2013.01)	Ｇ０６Ｆ	21/57	３７０
Ｇ０６Ｆ　21/55　(2013.01)	Ｇ０６Ｆ	21/55	３２０

ＦＩ

請求項の数　21　外国語出願　（全21頁）

(21)出願番号　特願2020-15140(P2020-15140)
(22)出願日　令和2年1月31日(2020.1.31)
(65)公開番号　特開2020-166830(P2020-166830A)
(43)公開日　令和2年10月8日(2020.10.8)
審査請求日　令和4年7月20日(2022.7.20)
(31)優先権主張番号　2019109169
(32)優先日　平成31年3月29日(2019.3.29)
(33)優先権主張国・地域又は機関
ロシア(RU)
(31)優先権主張番号　16/504,911
(32)優先日　令和1年7月8日(2019.7.8)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　515348585
エーオー カスペルスキー ラボ
ＡＯ Ｋａｓｐｅｒｓｋｙ Ｌａｂ
ロシア国、１２５２１２ モスクワ、レニングラドスコ ショス ３９エー／３
(74)代理人　110002147
弁理士法人酒井国際特許事務所
(72)発明者　アンドレイ ピー．ドウフヴァロフ
ロシア国，１２５２１２ モスクワ，レニングラドスコ ショス ３９エー／３，エーオー カスペルスキー ラボ内
(72)発明者　パーベル ヴィー．ジヤキン
ロシア国，１２５２１２ モスクワ，レニングラドスコ ショス ３９エー／３，エーオー カスペルスキー ラボ内

最終頁に続く

(54)【発明の名称】　技術的システムの要素のＩＴセキュリティを段階的に増加させるシステムおよび方法

(57)【特許請求の範囲】

【請求項１】

技術システムの構成要素のＩＴセキュリティを段階的に強化する方法であって、

データ交換プロトコルを使用して、複数の構成要素間のトラフィックをインターセプトすることによって、前記技術システムおよび前記技術システムに含まれる前記複数の構成要素に関するデータを収集することと、

脆弱な構成要素に対する疑わしい動作の検出、および前記構成要素に関する統計データのうち、１つまたは複数によって、前記技術システムの前記脆弱な構成要素を識別することと、

前記脆弱な構成要素を解析して、前記脆弱な構成要素の脆弱性の重大度分類を生成することと、

前記脆弱な構成要素間で構成要素同士を比較して、前記脆弱な構成要素のうち最も脆弱な部分を識別することと、

保護された環境で前記脆弱な構成要素のうちの前記最も脆弱な部分を操作することと、を含む方法。

【請求項２】

前記技術システムに関する前記データは、前記技術システムの１つまたは複数のレベルの構造、および各レベルでの、また各レベル全体にわたる前記複数の構成要素間の複数のリンクを含む、請求項１に記載の方法。

【請求項３】

前記技術システムの前記複数の構成要素を監視して、センサの不具合、ウイルスおよび悪意あるファイルの開封によるコンピュータの感染のうち１つまたは複数を含むエラーおよび誤作動情報を収集することをさらに含む、請求項１に記載の方法。

【請求項４】

前記統計データは、所定の期間内での前記各脆弱な構成要素のエラーおよび不具合を示す、請求項１に記載の方法。

【請求項５】

構成要素のハードウェアコンポーネントおよび保護されたオペレーティングシステムとの互換性を解析することによって、前記保護されたオペレーティングシステムの制御下で、前記技術システムの前記構成要素が作動できるかどうかを識別し、前記保護された環境は、前記保護されたオペレーティングシステムであること、をさらに含む、請求項１に記載の方法。

【請求項６】

前記保護されたオペレーティングシステムをハイパーバイザモードで起動することと、

前記保護されたオペレーティングシステムに前記脆弱な構成要素の機能の一部を転送し、前記技術システムの前記複数の構成要素間でのデータ交換をセキュアに制御することをさらに含む、請求項５に記載の方法。

【請求項７】

前記技術システムは、前記転送の間、機能的に利用可能である、請求項６に記載の方法。

【請求項８】

前記保護された環境で前記脆弱な構成要素のうち前記最も脆弱な部分を操作することは、前記技術システム内にインストールされたエージェントを使用して、前記複数の構成要素のうちのプロテクションが強化されている構成要素と、他の構成要素との間のインタラクションを提供することを含む、請求項１に記載の方法。

【請求項９】

前記保護された環境で前記脆弱な構成要素のうち前記最も脆弱な部分を操作することは、保護されたオペレーティングシステムに、前記脆弱な構成要素の前記脆弱な部分の制御を転送することを含む、請求項１に記載の方法。

【請求項１０】

技術システムの構成要素のＩＴセキュリティを段階的に強化するセキュリティシステムであって、

データ交換プロトコルを使用して、複数の構成要素間のトラフィックをインターセプトすることによって、前記技術システムおよび前記技術システムに含まれる前記複数の構成要素に関するデータを収集し、

脆弱な構成要素に対する疑わしい動作の検出、および前記構成要素に関する統計データのうち、１つまたは複数によって、前記技術システムの前記脆弱な構成要素を識別し、

前記脆弱な構成要素を解析して、前記脆弱な構成要素の脆弱性の重大度分類を生成し、

前記脆弱な構成要素間で構成要素同士を比較して、前記脆弱な構成要素のうち最も脆弱な部分を識別し、

保護された環境で前記脆弱な構成要素のうち前記最も脆弱な部分を操作する、

ように構成されたハードウェアプロセッサを含む、セキュリティシステム。

【請求項１１】

前記技術システムに関する前記データは、前記技術システムの１つまたは複数のレベルの構造、および各レベルでの、また各レベル全体にわたる前記複数の構成要素間の複数のリンクを含む、請求項１０に記載のセキュリティシステム。

【請求項１２】

前記ハードウェアプロセッサは、

前記技術システムの前記複数の構成要素を監視して、センサの不具合、ウイルスおよび悪意あるファイルの開封によるコンピュータの感染のうち１つまたは複数を含むエラーおよび誤作動情報を収集するようにさらに構成される、請求項１０に記載のセキュリティシ

ステム。
【請求項１３】
前記統計データは、所定の期間内での前記各脆弱な構成要素のエラーおよび不具合を示す、請求項１０に記載のセキュリティシステム。
【請求項１４】
前記ハードウェアプロセッサは、
前記構成要素のハードウェアコンポーネントおよび保護されたオペレーティングシステムとの互換性を解析することによって、前記保護されたオペレーティングシステムの制御下で、前記技術システムの前記構成要素が作動できるかどうかを識別し、
前記保護された環境は、前記保護されたオペレーティングシステムであるようにさらに構成される、請求項１０に記載のセキュリティシステム。
【請求項１５】
前記ハードウェアプロセッサは、
前記保護されたオペレーティングシステムをハイパーバイザモードで起動し、
前記保護されたオペレーティングシステムに前記脆弱な構成要素の機能の一部を転送し、前記技術システムの前記複数の構成要素間でのデータ交換をセキュアに制御するようにさらに構成される、請求項１４に記載のセキュリティシステム。
【請求項１６】
前記技術システムは、前記転送の間、機能的に利用可能である、請求項１５に記載のセキュリティシステム。
【請求項１７】
前記保護された環境で前記脆弱な構成要素のうち前記最も脆弱な部分を操作することは、前記技術システム内にインストールされたエージェントを使用して、前記複数の構成要素のうちのプロテクションが強化されている構成要素と、他の構成要素との間のインタラクションを提供することを含む、請求項１０に記載のセキュリティシステム。
【請求項１８】
前記保護された環境で前記脆弱な構成要素のうち前記最も脆弱な部分を操作することは、保護されたオペレーティングシステムに、前記脆弱な構成要素の前記脆弱な部分の制御を転送することを含む、請求項１０に記載のセキュリティシステム。
【請求項１９】
技術システムの構成要素のＩＴセキュリティを段階的に強化するための命令を記憶している非一時的なコンピュータ可読記憶媒体であって、前記命令は
データ交換プロトコルを使用して、複数の構成要素間のトラフィックをインターセプトすることによって、前記技術システムおよび前記技術システムに含まれる前記複数の構成要素に関するデータを収集することと、
脆弱な構成要素に対する疑わしい動作の検出、および前記構成要素に関する統計データのうち、１つまたは複数によって、前記技術システムの前記脆弱な構成要素を識別することと、
前記脆弱な構成要素を解析して、前記脆弱な構成要素の脆弱性の重大度分類を生成することと、
前記脆弱な構成要素間で構成要素同士を比較して、前記脆弱な構成要素のうち最も脆弱な部分を識別することと、
保護された環境で前記脆弱な構成要素のうちの前記最も脆弱な部分を操作することとを含む、非一時的なコンピュータ可読記憶媒体。
【請求項２０】
前記命令は、
前記構成要素のハードウェアコンポーネントおよび保護されたオペレーティングシステムとの互換性を解析することによって、前記保護されたオペレーティングシステムの制御下で、前記技術システムの前記構成要素が作動できるかどうかを識別し、前記保護された環境は、前記保護されたオペレーティングシステムであること、をさらに含む、請求項１

９に記載の媒体。
【請求項２１】
前記命令は、
前記保護されたオペレーティングシステムをハイパーバイザモードで起動することと、
前記保護されたオペレーティングシステムに前記脆弱な構成要素の機能の一部を転送し、前記技術システムの前記複数の構成要素間でのデータ交換をセキュアに制御することをさらに含む、請求項２０に記載の媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、サイバーセキュリティ分野に関し、より詳細には、技術的システムの要素のＩＴセキュリティを段階的に増加させるシステムおよび方法に関する。
【背景技術】
【０００２】
産業セキュリティにおける現在の問題の１つは、技術プロセス（Technological Process：ＴＰ）が安全に作動するかどうかの問題である。ＴＰの作動に対する主要な脅威としては、操作制御における意図的でない誤りまたは悪意ある動作、機器およびサブユニットの摩耗および不具合、制御システムおよびＩＴシステムに対するコンピュータ攻撃などが挙げられる。
【０００３】
企業での自動制御システム（Automated Control System：ＡＣＳ）は、技術システムを制御し、さらに十分なセキュリティレベルを提供する必要性がある。技術システム構成要素は、その構成要素を制御するオペレーティングシステムおよびファームウェアと同様に、旧式になることが多い。また、技術プロセスの中断につながるため、頻繁なアップデートは不可能である。さらに、プログラムの新しいバージョンは、技術システム構成要素の機能的安定性に悪影響を与えるエラーを含む可能性がある。そのうえ、独立して設置するように設計された既存の旧式ＡＣＳは、多くの場合、コンピュータネットワークに接続されているが、外部からの悪意ある動作イベントでのＩＴセキュリティを保障する手段を備えていない。
【０００４】
さらに、技術システム制御に向けた既存のソリューションは、現在の本質的なセキュリティ要件に留意することなく開発されたものであり、それにより、そのプロテクションのレベルを上げるのに問題をもたらす。残念なことに、既存のソリューションは、通常、大量の旧式コードによりかえって複雑であり、それにより、それらの再加工を著しく複雑にし、商業的観点および技術的観点の両方からリソースを極めて浪費させ、かつリスキーなものである。
【０００５】
多くの場合、企業で働く人材が、ＩＴセキュリティの十分な技術を持ち合わせてなく、強固なパスワードを採用せず、個人情報記憶媒体およびモバイルデバイスをコンピュータおよびサーバに接続し、ソーシャルネットワークおよび私的メールを使用して、レターおよびメッセージから添付ファイルを開封するが、それにより、悪意あるソフトウェアでコンピュータを感染させ、コンピュータセキュリティ関連インシデントをもたらす可能性があるという点に留意すべきである。
【０００６】
技術システムのＩＴセキュリティを強化するソリューションが必要である。
【発明の概要】
【発明が解決しようとする課題】
【０００７】
本開示は、技術システム構成要素のＩＴセキュリティを段階的に強化するシステムおよび方法について記載する。

【０００８】
本開示の技術的効果は、記載される目的を実現することである。
【課題を解決するための手段】
【０００９】
一変形態様に従って、技術システム構成要素のＩＴセキュリティを段階的に強化する方法が提示され、該方法は、データ交換プロトコルを使用して、複数の構成要素間のトラフィックをインターセプトすることによって、技術システムおよび技術システムに含まれる複数の構成要素に関するデータを収集することと、脆弱な構成要素に対する疑わしい動作の検出、および構成要素に関する統計データのうち１つまたは複数によって技術システムの脆弱な構成要素を識別することと、脆弱な構成要素を解析して、脆弱な構成要素の脆弱性の重大度分類を生成することと、脆弱な構成要素間で構成要素同士を比較して、脆弱な構成要素のうち最も脆弱な部分を識別することと、保護された環境で脆弱な構成要素のうちの最も脆弱な部分を操作することとを含む。
【００１０】
方法の一態様では、技術システムに関するデータは、技術システムの１つまたは複数のレベルの構造、および各レベルでの、また各レベル全体にわたる複数の構成要素間の複数のリンクを含む。
【００１１】
一態様では、該方法は、技術システムの複数の構成要素を監視して、センサの不具合、ウイルスおよび悪意あるファイルの開封によるコンピュータの感染のうち１つまたは複数を含むエラーおよび誤作動情報を収集することをさらに含む。
【００１２】
方法の一態様では、統計データは、所定の期間内での各脆弱な構成要素のエラーおよび不具合を示す。
【００１３】
一態様では、該方法は、構成要素のハードウェアコンポーネントおよび保護されたオペレーティングシステムとの互換性を解析することによって、保護されたオペレーティングシステムの制御下で、技術システム構成要素が作動できるかどうかを識別し、該保護された環境は、保護されたオペレーティングシステムであることをさらに含む。
【００１４】
一態様では、該方法は、保護されたオペレーティングシステムをハイパーバイザモードで起動することと、保護されたオペレーティングシステムに脆弱な構成要素の機能の一部を転送し、技術システムの複数の構成要素間でのデータ交換をセキュアに制御することをさらに含む。
【００１５】
方法の一態様では、技術システムは、転送の間、機能的に利用可能である。
【００１６】
方法の一態様では、保護された環境で脆弱な構成要素のうちの最も脆弱な部分を操作することは、技術システム内にインストールされたエージェントを使用して、複数の構成要素のうちのプロテクションが強化されている構成要素と、他の構成要素との間のインタラクションを提供することを含む。
【００１７】
方法の一態様では、保護された環境で脆弱な構成要素のうちの最も脆弱な部分を操作することは、保護されたオペレーティングシステムに、脆弱な構成要素の脆弱な部分の制御を転送することを含む。
【００１８】
その他の例示的態様では、技術システム構成要素のＩＴセキュリティを段階的に強化するセキュリティシステムが提供される。セキュリティシステムは、データ交換プロトコルを使用して、複数の構成要素間のトラフィックをインターセプトすることによって、技術システムおよび技術システムに含まれる複数の構成要素に関するデータを収集し、脆弱な

構成要素に対する疑わしい動作の検出、および構成要素に関する統計データのうち１つまたは複数によって技術システムの脆弱な構成要素を識別し、脆弱な構成要素を解析して、脆弱な構成要素の脆弱性の重大度分類を生成し、脆弱な構成要素間で構成要素同士を比較して、脆弱な構成要素のうち最も脆弱な部分を識別し、保護された環境で脆弱な構成要素のうち最も脆弱な部分を操作するように構成されたハードウェアプロセッサを含んでもよい。

【００１９】

その他の例示的態様では、上述の方法を実行するための命令が、非一時的なコンピュータ可読媒体に含まれてもよい。

【００２０】

例示的態様の簡略化された上記概要は、本開示の基本的な理解をもたらすために提供される。本概要は、すべての企図された態様の広範な概要ではなく、またすべての態様の主要なまたは重要な要素を特定することも、本発明の任意のまたはすべての態様の範囲を描写することも意図されていない。その唯一の目的は、１つまたは複数の態様を、以下の本開示のより詳細な説明の序文として、簡略化した形で示すことである。上記の目的を達成するために、本発明の１つまたは複数の態様は、特許請求の範囲で説明され、かつ例示的に示される特徴を含む。

【図面の簡単な説明】

【００２１】

本明細書に組み込まれ、かつ本明細書の一部を構成する添付図面は、発明を実施するための形態と共に本開示の１つまたは複数の例示的態様を示すものであり、それらの原理および実装形態を説明するために提供される。

【００２２】

【図１ａ】図１ａは、技術システムの一例を概略的に示す図である。

【図１ｂ】図１ｂは、本開示の例示的態様に従って、技術システムの実装形態の特定例を概略的に示す図である。

【図２】図２は、本開示の例示的態様に従って、技術システムのＩＴセキュリティの提案される段階的強化システムの実現化例を示す図である。

【図３】図３は、本開示の例示的態様に従って、技術システムのＩＴセキュリティの提案される段階的強化方法の実現化例を示す図である。

【図４】図４は、本開示の例示的態様に従って、本開示が実現され得る汎用コンピュータシステムの一例を示す図である。

【発明を実施するための形態】

【００２３】

例示的態様が、技術システム構成要素のＩＴセキュリティを段階的に強化するシステム、方法、およびコンピュータプログラム製品のコンテキストで本明細書に記載される。以下の説明は例示のためのものであり、いかなる点においても限定することを意図するものではないことを当業者であれば理解されるであろう。本開示から利益を得る当業者であれば、その他の態様は容易に連想されるであろう。添付図面に示される例示的な態様の実装形態に、参照番号が項目ごとに付与される。同一または類似の項目であることを言及するために、同じ参照番号が図面および以下の説明を通して可能な範囲で使用される。

【００２４】

以下の定義および概念は、本開示の変形態様を説明する際に使用される。

【００２５】

一態様では、制御客体は、その状態を変更するために、（制御するおよび／または疑わしい）外部動作が施される技術的対象である。特定の態様では、制御客体は、デバイス（電動機のような）および／または技術プロセス（またはその一部）を含んでもよい。

【００２６】

一態様では、技術プロセス（ＴＰ）は、物的生産プロセスであり、物的実体（作業の主体）の状態の逐次的変更を含む。

【００２７】
一態様では、技術プロセス制御（プロセス制御）は、製品の製造中に、技術プロセスのプロセス変量を制御するために使用される各種の方法である。
【００２８】
一態様では、プロセス変量（Process Variable：ＰＶ）は、観察または監視されるＴＰの特定部分の現在の測定値である。プロセス変量は、例えば、センサからの測定値である。
【００２９】
一態様では、外部動作は、その動作が施される構成要素、例えば技術システム（Technological System：ＴＳ）の構成要素などの状態を、特定方向で変更する方法である。いくつかの実施形態では、動作は、非一時的信号の形態で、ＴＳの１つの構成要素から、ＴＳの別の構成要素に伝送される。
【００３０】
一態様では、制御客体の状態は、その実質的属性を統合したものであり、状態パラメータによって表され、制御サブシステムからの制御動作を含む外部動作の影響を受けて変更または維持される。
【００３１】
一態様では、状態パラメータは、客体の実質的属性の特徴を表す１つまたは複数の数値である。特定の一態様では、状態パラメータは、物理量の数値である。
【００３２】
一態様では、制御客体の形式状態とは、（ＴＰの場合は）プロセスチャートおよびその他の技術文書、または（デバイスの場合は）タイムテーブルに対応する制御客体の状態である。
【００３３】
一態様では、制御動作は、（動作の目的が客体の状態に作用することである）計画的な、（ＴＰによって提供される）制御客体に対する制御サブシステムの制御主体による正当な外部動作であり、結果として、制御客体の状態を変更するか、または制御客体の状態を維持するものである。
【００３４】
一態様では、疑わしい動作は、制御主体による動作を含む、制御客体の状態に対する計画的または意図的でない違法な（ＴＰによって提供されたものではない）外部動作である。
【００３５】
一態様では、制御主体は、制御動作を制御客体に適用するか、または客体に制御動作を直接適用する前に、別の制御主体に制御動作を変換するように伝送するデバイスである。
【００３６】
一態様では、マルチレベル制御サブシステムは、いくつかのレベルを伴う制御主体の集合である。
【００３７】
一態様では、サイバー物理システムは、物理プロセスへの計算リソースの統合化を意味するＩＴ概念である。このようなシステムでは、センサ、装置、およびＩＴシステムは、１つの企業または事業の枠を超えた価値創造チェーン全体に沿ってつながっている。これらのシステムは、変化に対する予測、自動調節および自動調整のために標準的インターネットプロトコルによって互いに相互作用している。サイバー物理システムの例は、技術システムおよび産業用モノのインターネットである。
【００３８】
一態様では、モノのインターネット（Internet of Things：ＩｏＴ）は、互いにまたは外部と相互作用する組込み技術が搭載された物理的実体（「モノ」）のコンピュータネットワークである。モノのインターネットは、ポータブルデバイス、交通機関のエレクトロニックシステム、スマートカー、スマートシティ、産業システムなどの技術を含む。
【００３９】

一態様では、産業用モノのインターネット（Industrial Internet of Things：ＩＩｏＴ）は、モノのインターネットのサブカテゴリであり、同様に、ポータブルデバイス、「スマートホーム」技術および自動制御を伴う自動車などの消費者指向用途を含む。両コンセプトの際立った特徴としては、インターネットを通してデータを送信し、かつソフトウェアによって制御される組込みセンサを備えるデバイス、工作機械およびインフラストラクチャなどである。

【００４０】

一態様では、技術システム（ＴＳ）は、マルチレベル制御サブシステムの各制御主体と制御客体（ＴＰまたはデバイス）との機能的相互関連グループであり、制御主体の状態の変更を通して、制御客体の状態の変更を実現するものである。技術システムの構造は、技術システムの基本的構成要素（マルチレベル制御サブシステムの相互関連制御主体および制御客体）、およびこれらの構成要素間のリンクによって形成される。技術システム内の制御客体が技術プロセスの場合、制御の最終目標は、制御客体の状態の変更によって、作業対象物（原材料、半製品など）の状態を変更することである。技術システム内の制御客体がデバイスの場合、制御の最終目標は、デバイス（交通機関、スペースクラフト）の状態を変更することである。ＴＳの各構成要素の機能的関係は、これらの構成要素の状態の関係を意味する。各構成要素間の直接的な物理リンクが存在すらしない（例えば、アクチュエータと技術オペレーションとの間の物理リンクが存在しない）場合があるが、それにもかかわらず、これらの状態パラメータが物理的に接続していない場合であっても、例えば、切削速度はスピンドルの回転速度に機能的に関連するものである。

【００４１】

一態様では、制御主体の状態は、その実質的属性を統合したものであり、状態パラメータによって表され、外部動作の影響を受けて、変更または維持され得る。

【００４２】

一態様では、制御主体の実質的属性は、（状態の実質的パラメータに応じて）制御客体の状態の実質的属性に直接影響を与える属性である。制御客体の実質的属性は、ＴＳに対して制御される機能的要因（精度、安全性、有効性）に直接影響を与える属性、例えば、一定の形式で指定される条件に対応する切削条件、その旅程に対応する電車の進行、許容範囲内での反応器温度の維持などである。制御客体の状態パラメータは、制御される要因に応じて選択され、かつ制御客体に対して制御動作を行う制御主体の関連状態パラメータに応じて選択される。

【００４３】

一態様では、ハイパーバイザ（仮想マシンの監視）は、他のプログラム（他のハイパーバイザを含む）のための機能的環境を含むプログラムであり、コンピュータハードウェアをシミュレーションして、そのハードウェアと、その環境で作動するゲストオペレーティングシステムとを制御するものである。

【００４４】

本開示の一態様では、仮想マシンにおける有害性に対するファイルを解析するシステムの構成要素とは、統合マイクロ回路（特定用途向け集積回路、Application-Specific Integrated Circuit：ＡＳＩＣ）、またはフィールドプログラマブルゲートアレイ（Field-Programmable Gate Array：ＦＰＧＡ）などのハードウェアを用いて、または、例えば、マイクロプロセッサシステムおよびプログラム命令のセットなどのソフトウェアおよびハードウェアの組み合わせの形態で、またニューロンシナプスチップをベースとして実現される、実際のデバイス、システム、構成要素、および構成要素のグループを指す。システムの示される構成要素の機能性は、ハードウェアによって独占的に、またソフトウェアによって実現されるシステムの構成要素の機能性の一部とハードウェアによるものの一部との組み合わせの形態によっても実現されてよい。特定の変形態様では、一部の構成要素またはすべての構成要素は、汎用コンピュータ（図４に示すような）のプロセッサに実装され得る。システムの構成要素全体は、単一のコンピューティングデバイスの内部で、またはいくつかの相互接続しているコンピューティングデバイスの間で分散して実現する

ことができる。

【００４５】

図１ａは、構成要素１１０ａおよび１１０ｂを含む、技術システム１００の一例を概略的に示し、ここで、ＴＳの構成要素とは、制御客体１１０ａ、マルチレベル制御サブシステム１２０を形成している制御主体１１０ｂ、水平リンク１３０ａおよび垂直リンク１３０ｂである。制御主体１１０ｂは、レベル１４０によってグルーピングされる。

【００４６】

図１ｂは、技術システム１００’の実装の特定例を概略的に示す。制御客体１１０ａ’は、ＴＰまたはデバイスである。制御動作は、制御客体１１０ａ’を対象とするものであり、該制御動作は、自動制御システム（ＡＣＳ）１２０’によって、作り上げられて、実現される。３つのレベル１４０’が、各制御主体１１０ｂ’を含むＡＣＳ内で区別されており、該各制御主体１１０ｂ’は、水平リンク（この図では、レベル内のリンクは示さず）によって水平に、かつ垂直リンク１３０ｂ’（各レベル間の）によって垂直に、互いに相互関連している。関係性は機能的であり、すなわち、一般的に、１つのレベルでの制御主体１１０ｂ’の状態の変化は、同じレベルおよび他のレベルで接続している制御主体１１０ｂ’の状態の変化を誘発する。制御主体の状態の変化に関する情報は、制御主体間で確立されている水平および垂直リンクに沿って、信号の形態で伝送される。すなわち、該当の制御主体の状態の変化に関する情報は、他の制御主体１１０ｂ’に対する外部動作である。ＡＣＳ１２０’内の各レベル１４０’は、制御主体１１０ｂ’の目的に従って区別される。レベル数は、ＡＣＳ１２０’の複雑さに依存して変動する場合がある。単純なシステムでは、１つまたは複数の下位レベルを含むことがある。ＴＳの構成要素（１１０ａ、１１０ｂ）と、ＴＳ１００のサブシステムとの物理的連結には、有線ネットワーク、無線ネットワーク、統合マイクロ回路が使用されてよい。ＴＳの構成要素（１１０ａ、１１０ｂ）と、ＴＳ１００のサブシステムとの論理的連結には、イーサネット、産業用イーサネット、または産業用ネットワークが使用されてよい。使用される産業用ネットワークおよびプロトコルは、Ｐｒｏｆｉｂｕｓ、ＦＩＰ、ＣｏｎｔｒｏｌＮｅｔ、ＩｎｔｅｒＢｕｓ－Ｓ、ＤｅｖｉｃｅＮｅｔ、Ｐ－ＮＥＴ、ＷｏｒｌｄＦＩＰ、ＬｏｎｇＷｏｒｋ、Ｍｏｄｂｕｓなどの種々のタイプまたは規格である。

【００４７】

上位レベル（監視制御データ収集（Supervisory Control And Data Acquisition：ＳＣＡＤＡ）のレベル）は、ディスパッチャ／オペレータ制御のレベルであり、少なくとも、コンピュータとヒューマンマシンインターフェース（Human-Machine Interface：ＨＭＩ）とを制御するコントローラ（図１ｂでは、単一の制御主体内部のＳＣＡＤＡを示す）である制御主体１１０ｂ’を含む。このレベルは、ＴＳの構成要素（１１０ａ’、１１０ｂ’）の状態を追跡し、ＴＳの構成要素（１１０ａ’、１１０ｂ’）の状態に関する情報を収集して、コンパイルし、必要があればそれを修正するように設計される。

【００４８】

中間レベル（ＣＯＮＴＲＯＬレベル）は、コントローラのレベルであり、少なくとも、プログラマブル論理コントローラ（Programmable Logic Controller：ＰＬＣ）、カウンタ、リレー、レギュレータである制御主体を含む。ＰＬＣタイプの制御主体１１０ｂ’は、「測定制御装置」タイプの制御主体から、および制御客体１１０ａ’の状態に従う「センサ」タイプの制御主体１１０ｂ’から情報を受信する。ＰＬＣタイプの制御主体は、「アクチュエータ」タイプの制御主体用のプログラム制御アルゴリズムに従って、制御動作を作り上げる（生成する）。アクチュエータは、下位レベルで、これを（制御客体に適用して）直接実現する。アクチュエータは、作動デバイス（装置）の一部である。

【００４９】

下位レベル（入力／出力レベル）は、センサおよび検出器、制御客体１１０ａ’の状態を制御する測定制御装置（Measurement and Control Instruments：ＭＣＩ）、ならびにアクチュエータなどの制御主体のレベルである。アクチュエータは、制御客体１１０ａ’の状態に直接作用し、それを形式状態、すなわち技術的使途、（ＴＰの場合は）技術チ

ャート、または他のいくつかの技術文書、（デバイスの場合は）タイムテーブルに応じる状態に適合させる。このレベルでは、「センサ」タイプの制御主体１１０ｂ’からの信号は、中間レベル１４０’の制御主体の入力と連係され、「ＰＬＣ」タイプの制御主体１１０ｂ’によって作り上げられる制御動作は、その動作を実行する「アクチュエータ」タイプの制御主体１１０ｂ’と連係される。アクチュエータは、作動デバイスの一部である。作動デバイスは、レギュレータまたは制御デバイスから届く信号に従って調整要素を動かす。作動デバイスは、自動制御チェーンの末端リンクであり、一般に、
・増幅装置（コンタクタ、周波数変換器、アンプなど）
・フィードバック要素（出力軸の位置センサ、終了位置の信号、手動駆動など）を備えた（電気、空気圧、油圧駆動式）アクチュエータ
・調整要素（ゲート、バルブ、スライド、ダンパーなど）
、のユニットで構成される。

【００５０】

適用条件に応じて、作動デバイスは、それぞれ異なるように設計されてよい。アクチュエータおよび調整要素は通常、作動デバイスの基本ユニットの１つである。

【００５１】

特定例では、作動デバイス全体がアクチュエータと呼ばれる。

【００５２】

異なるレベルの列挙した制御主体（１１０ａ’、１１０ｂ’）は、技術システム構成要素１１０である。

【００５３】

図２は、技術システムのＩＴセキュリティを段階的に強化するシステムを示す。手法は、ＩＴセキュリティを強化する必要が最もある技術システム構成要素１１０を選択して、かつ仮想化技術を用いて、単独および独立した環境に段階的に転送するという構想に基づくものである。例示的態様では、ＩＴセキュリティを段階的に強化することは、保護された仮想環境への技術システムの異なるレベルの逐次的転送を意味する。各段階（ステップ）で、図２に記載されるシステムは、技術システムの他の構成要素１１０と比較して、強化セキュリティが最も必要とされる技術システム構成要素１１０を選択する。各段階は、技術システム１１０全体の（管理者などによって定義されているような）適切なレベルの安全性に達するまで繰り返される。保護された仮想環境への構成要素の逐次的な転送は、一部の態様では、技術システム１１０のプロセスを停止することなく、スムーズに行われる可能性がある。加えて、仮想環境への構成要素の転送時に、不具合率（例えば、転送中にスクリプトをテストする際のエラー、構成要素と仮想環境または他の要因との不互換性）が存在する可能性もある。例えば、単一の構成要素を、保護された仮想環境に転送する場合は、不具合の確率は最小（例えば、所定の閾値未満）である一方で、複数の構成要素またはシステム全体を、一度に保護された仮想環境に転送すると、不具合の確率が比例して高くなる。

【００５４】

技術システムのＩＴセキュリティを強化するためのシステムは、収集モジュール２１０、解析モジュール２２０、およびプロテクションモジュール２３０を含む。

【００５５】

収集モジュール２１０は、
・技術システムに関するデータを収集
・技術システムの各構成要素１１０に関するデータを収集
・解析モジュール２２０に収集したそのデータを送信
するように設計される。

【００５６】

一変形態様では、収集モジュール２１０は、少なくともＴＳの構造を含むＴＳに関するデータを収集する。別の変形態様では、収集モジュール２１０は、少なくとも、レベルの構造、ならびにそのレベルのうちの各構成要素１１０の互いのリンク、およびＴＳの他の

レベルの構成要素１１０とのリンクを含む、ＴＳの各レベルに関するデータを収集する。さらに別の変形形態では、収集モジュール２１０は、技術システムの作動を支援する補助的ＩＴシステムに関するデータを収集する。補助的ＩＴシステムは、サーバ、ユーザワークステーション、技術システム構成要素１１０および外部サーバとの通信のためのチャネル、モバイルデバイス、産業用モノのインターネットのデバイス、およびデータ記憶媒体を含む。

【００５７】

一般的には、収集モジュール２１０によって収集されるデータは、技術システムの各構成要素１１０に関する情報を含む。

【００５８】

一変形態様では、収集モジュール２１０は、サーバに働きかけて、例えば、ＴＳの各構成要素１１０間のトラフィックをインターセプトすることによって、または産業用データ交換プロトコルを使用して、ＴＳの構成要素１１０と相互作用することによって、遠隔的にＴＳの構成要素１１０に関する情報を収集する。別の変形態様では、収集モジュール２１０は、例えば、プログラムエージェントの形態で、ＴＳの構成要素１１０に常駐していてもよく、ＴＳの構成要素１１０とＴＳの他の構成要素１１０とのリンクに関する必要なデータを収集する。

【００５９】

一変形態様では、収集モジュール２１０は、ＴＳの構成要素１１０の監視を実行して、それ自体が作動している間に発生するエラーおよび誤作動、例えば、センサの不具合、外部デバイスの接続（例えば、ＵＳＢポートの使用による）または悪意あるファイル（電子メールおよびソーシャルエンジニアリングを用いて受信されるような）の開封が原因のウイルスによるコンピュータの感染などの統計値を収集する。

【００６０】

該収集されたデータは、収集モジュール２１０によって、解析モジュール２２０に送信される。

【００６１】

解析モジュール２２０は、

・各ステップ中に、技術システムの各レベルの脆弱性を識別
・構成要素の脆弱性のそれぞれの重大度を識別し、少なくとも１つの最も脆弱な構成要素（例えば、最も重大な脆弱性を伴う構成要素）を識別
・インターセプト装置にソリューションを送信

するように設計される。

【００６２】

解析モジュール２２０は、受信したそのデータを用いて操作し、まず真っ先に、ＩＴプロテクションが必要であるＴＳの構成要素１１０を識別することで、既存の技術システムの解析を実施する。これに関して、ＴＳの異なるレベルで脆弱性は識別される。一変形態様では、従来技術の既知の脆弱性識別方法が、解析モジュール２２０によって使用される。一変形態様では、脆弱性は、ＴＳの構成要素１１０に対する、解析モジュール２２０により疑われた動作によって識別される。この場合、疑わしい動作に対するＴＳの構成要素１１０の反応を反映しているデータが、収集モジュール２１０によって収集されて、解析モジュール２２０に再度送信されてもよい。さらに別の変形態様では、解析モジュール２２０は、統計データに基づいて脆弱性を識別する。例えば、ＴＳの最も脆弱な構成要素１１０は、それ自体が作動している間、または特定の期間内に発生するエラーまたは不具合の最大数を有する構成要素とみなされる。

【００６３】

別の変形形態では、解析モジュール２２０は、統計データによって、例えば、それ自体が作動している間に発生する、構成要素の不具合の数によって、エラーの数または頻度によって、ＴＳの脆弱な構成要素１１０を識別する。

【００６４】

ＴＳのレベルでの脆弱性の識別の後に、解析モジュール２２０は、構成要素のＩＴプロテクションを強化するために働きかける必要があるＴＳの少なくとも１つの構成要素１１０を識別する。

【００６５】

一般的に、解析モジュール２２０は、保護されたオペレーティングシステム（Ｋａｓｐｅｒｓｋｙ　ＯＳ（登録商標）のような）の制御下で、技術システム構成要素１１０が作動できるかどうかを識別する。これは、例えば、ＴＳの構成要素１１０のハードウェアコンポーネントの解析およびセキュアオペレーティングシステムとの互換性の助けを借りて実現できる。

【００６６】

解析モジュール２２０は、プロテクションモジュール２３０に解析結果を送信する。

【００６７】

プロテクションモジュール２３０は、

・技術システムの識別された脆弱な構成要素にインストールされる

・技術システム構成要素１１０のＩＴセキュリティを保証する少なくとも１つの動作を実行する、ように設計される。

【００６８】

一態様では、技術システム構成要素の情報セキュリティを保証する動作は、ハイパーバイザモードで動作している保護されたオペレーティングシステムの制御下で、技術システム構成要素を作動させるときに実装される。別の変形態様では、技術システム構成要素の情報セキュリティを保証する動作は、技術システム構成要素上で保護されたオペレーティングシステムを起動することを含む。

【００６９】

一般的に、プロテクションモジュール２３０は、保護されたオペレーティングシステムであり、技術システム構成要素１１０にインストールされるように設計される。

【００７０】

一変形態様では、保護されたオペレーティングシステムは、ハイパーバイザモードで起動され、それにより、修正が困難で／高コストで／リスクの大きい既存のオペレーティングシステムおよびＴＳの構成要素１１０のアプリケーションを、保護された環境で実行することが可能になる。本開示の好適な変形態様で、ハイパーバイザの主要機能は、ＴＳの構成要素１１０のＩＴセキュリティを強化することであり、従来のハイパーバイザで行われていたような、異なるゲストオペレーティングシステムの間でハードウェアプラットホームのリソースを分割することは、しないことを理解することが重要である。したがって、ＩＴセキュリティの必要なレベルを備えていない既存の技術システムの場合、ＴＳの構成要素１１０の一部の機能は、プロテクションモジュール２３０に転送されるかまたはその中で複製される。ＩＴセキュリティを強化する必要があるＴＳの構成要素１１０を、保護されたオペレーティングシステムの制御またはハイパーバイザ制御下のゲストオペレーティングシステムに逐次的に転送することにより、各ＴＳの構成要素１１０間での情報交換の追加の制御が可能である。機能的な技術システムは、この逐次的な転送の各ステップの間、完全に利用可能である。

【００７１】

一変形態様では、プロテクションモジュール２３０は、技術システム構成要素１１０と相互作用し、この構成要素は、技術システム構成要素１１０にインストールされたエージェントを介してプロテクションモジュール２３０によってセキュリティが強化されたものである。

【００７２】

本発明のシステムの実現例を以下に記載する。

【００７３】

例１。ＯＳ　ＷｉｎｄｏｗｓまたはＬｉｎｕｘ（登録商標）の制御下で、技術システムの上位レベル制御主体、技術システム構成要素１１０がある。制御主体のＩＴセキュリテ

ィを強化する必要がある。例えば、それは、ＯＳ　Ｗｉｎｄｏｗｓ下のＳＣＡＤＡアプリケーションである。一般に、ＯＳ　ＷｉｎｄｏｗｓはＩＴ保護環境ではないことが知られている。さらに、重大な脆弱性を排除するアップデートを頻繁にインストールすると、技術的プロセスを中断することになり、業務プロセスへのリスクの度合いが上がることになる。また、人員がＩＴセキュリティに関する十分な技術を持ち合わせていない場合が多い（ＴＳの制御主体にフラッシュメモリやパーソナル電話を接続する場合もある）ことも、言及する必要がある。

【００７４】

さらに、悪意あるアプリケーションが、制御主体をセキュリティ侵害し、かつ悪意あるアクティビティ実施後に、悪意あるアプリケーションのアクティビティによって起こったイベントに関する記録をシステムログから消去することも知られている。

【００７５】

一変形態様では、ログ内のすべての記録は、ゲストオペレーティングシステムに実装され、かつ技術システム構成要素１１０にインストールされたエージェントによって、ハイパーバイザモードで実装されているプロテクションモジュール２３０に一度に送信される。この場合、ゲストオペレーティングシステムで実行する悪意あるアプリケーションは、そのアクティビティをプロテクションモジュール２３０から隠すことはできない。

【００７６】

類似の例示的態様としては、監査ログ（どのユーザが、いつゲストＯＳで動作したか）の処理がある。監査ログは、ゲストオペレーティングシステムに実装されたエージェントによって、プロテクションモジュール２３０に送信することができる。

【００７７】

別の例示的態様は、ゲストオペレーティングシステムに実装されたエージェントによって、ゲストオペレーティングシステムに実装されている個々のアプリケーション（ＳＣＡＤＡのような）のログを、プロテクションモジュール２３０に送信することである。

【００７８】

さらに別の変形態様は、プロテクションモジュール２３０を用いるハードウェアの制御である。したがって、ハイパーバイザレベルでのＵＳＢポートへのアクセスに関するポリシーの柔軟な調整が可能であり、例えば、ユーザがゲストＯＳで操作中の場合、アクセスを禁じ、管理者がゲストＯＳで操作中の場合、アクセスを許可する。

【００７９】

また、プロテクションモジュール２３０を用いて、リモート接続のセキュリティを強化することも可能である。技術システム構成要素１１０上のＯＳがセキュリティ侵害された（リモートアクセスが有効になっており、いくつかのアプリケーションまたはサービスがリモートアクセスのためにインストールされている）場合、侵入は、ハイパーバイザによって生じることはなく、この場合、このハイパーバイザは補助的ファイアウォールの役割を果たす。さらに別の態様では、プロテクションモジュール２３０による２ファクタ認証を用いてゲストＯＳへのリモートアクセスが実現可能である。

【００８０】

さらに別の例示的態様では、別個のアプリケーション（ＳＣＡＤＡのような）が、プロテクションモジュール２３０の能力を利用する。例えば、セキュリティポリシーの制御のためのメカニズムがハイパーバイザによって実現されるので、このアプリケーションに類似のメカニズムを組み込む必要がない。特定の許可を得るためにハイパーバイザにアクセスして、ソリューションを得る能力を追加するだけで十分である。

【００８１】

さらに別の変形形態では、制御主体が異常を伴って作動している（疑わしい動作が、制御主体に行使されている）場合、プロテクションモジュール２３０は、アプリケーション（ＳＣＡＤＡのような）と制御主体とのインタラクションを禁止してもよい。

【００８２】

アプリケーション（例えば、ＳＣＡＤＡ）が仮想環境で動作する場合、アプリケーショ

ンは、プロテクションモジュール２３０を検出しないが、これは、アプリケーションが、例えば、保護されたオペレーティングシステムを表して、ハイパーバイザレベルで動作することができるためである。したがって、アプリケーションは、プロテクションモジュール２３０の存在を認識しない。プロテクションモジュール２３０は、次に、ハイパーバイザレベルで、ゲストオペレーティングシステム内のアプリケーションから出力されるパケットをインターセプトし、アプリケーション（例えば、ＳＣＡＤＡ）によって、安全でない構成要素に送信されるデータパケットを判定する。この判定は、本開示を通して、例えば、データパケットの構成を調べることによって、またはゲストＯＳ内のエージェントによって実施されてよいが、これらに限定されない。

【００８３】

例２。技術システム内で、ＴＳの旧式の構成要素１１０（例えば、下位レベルの制御主体）が使用され、そのソフトウェアが、ＴＳの構成要素１１０の製造業者によってアップデートすることができない。さらに、このＴＳの構成要素１１０が、（例えば、上位または中間レベルの制御主体のアップデート後に）技術システムの新しいプロセスとの互換性がないとする。セキュアなＯＳが、プロテクションモジュール２３０の役割を果たし、それにより、技術システム構成要素１１０が、セキュアなＯＳの制御下で動作する。ここで、このセキュアなＯＳは、ＴＳの該構成要素１１０のために修正され、その適切な作動を保証するものである。その結果、制御主体の既知の脆弱性は排除され、制御主体に対する要件に応じてその機能性を拡張し、技術システムの新しいプロセスとの互換性を保証することができる。

【００８４】

技術システム構成要素１１０の保護されたシステムの制御への上述の逐次的な転送により、保護されたＯＳの制御下での技術システム構成要素１１０すべての段階的な移動、すなわち、保護されたＯＳの制御下での技術システム全体の移動が可能になる。

【００８５】

図３は、仮想マシンにおける有害性に対する提案されたファイル解析方法の実現化例を示す。

【００８６】

最初のステップ３１０で、収集モジュール２１０を使用して、技術システムおよび技術システムのすべての構成要素１１０のデータを収集する。一変形態様では、収集モジュール２１０は、サーバに働きかけ、例えば、ＴＳの各構成要素１１０間のトラフィックをインターセプトすることによって、またはデータ交換用産業プロトコルを使用して、ＴＳの構成要素１１０と相互作用することによって、ＴＳの構成要素１１０の情報を遠隔的に収集する。別の変形態様では、収集モジュール２１０は、例えば、プログラムエージェントの形態で、ＴＳの構成要素１１０に常駐していてもよく、ＴＳの構成要素１１０およびＴＳの他の構成要素１１０とのリンクに関する必要なデータを収集する。さらに別の変形態様では、収集モジュール２１０は、ＴＳの構成要素１１０の監視を実行して、それ自体が作動している間に発生するエラーおよび誤作動の統計値を収集する。

【００８７】

次に、ステップ３２０で、解析モジュール２２０を使用して技術システムの脆弱性、および技術システムの少なくとも１つの最も脆弱な構成要素１１０を識別する。一変形態様では、従来技術の既知の脆弱性識別方法が、解析モジュール２２０によって使用される。別の変形態様では、脆弱性は、ＴＳの構成要素１１０に対する、解析モジュール２２０により疑われた動作によって識別される。

【００８８】

次に、ステップ３３０で、プロテクションモジュール２３０が技術システムの識別された脆弱な構成要素１１０にインストールされる。一変形態様では、プロテクションモジュール２３０は、保護されたオペレーティングシステムである。

【００８９】

続いて、ステップ３３０で、プロテクションモジュール２３０を使用して、技術システ

ムの識別された脆弱な構成要素１１０のＩＴセキュリティを保証する少なくとも１つの動作を実施する。一変形態様では、技術システム構成要素１１０のＩＴセキュリティを保証する動作とは、ハイパーバイザモードで実装されている保護されたオペレーティングシステムの制御下での技術システム構成要素の動作である。別の変形態様では、技術システム構成要素１１０のＩＴセキュリティを保証する動作は、ハイパーバイザモードで、実装されている技術システム構成要素上で保護されたオペレーティングシステムを起動することである。さらに別の変形態様では、プロテクションモジュール２３０は、技術システム構成要素１１０と相互作用し、この構成要素は、技術システム構成要素１１０にインストールされたエージェントを介してプロテクションモジュール２３０によってセキュリティが強化されたものである。

【００９０】

図４は、例示的態様に従って、技術システム構成要素のＩＴセキュリティを段階的に強化するシステムおよび方法の態様が実装されることがあるコンピュータシステム２０を示すブロック図である。コンピュータシステム２０は、上述したようなシステム１００の任意の構成要素に相当し得るという点に留意すべきである。コンピュータシステム２０は、例えば、デスクトップコンピュータ、ノートブックコンピュータ、ラップトップコンピュータ、モバイルコンピューティングデバイス、スマートフォン、タブレットコンピュータ、サーバ、メインフレーム、埋め込み型デバイス、およびコンピューティングデバイスの他の形態など、複数のコンピューティングデバイスの形態、または、単一のコンピューティングデバイスの形態である場合がある。

【００９１】

示すように、コンピュータシステム２０は、中央演算処理装置（Central Processing Unit：ＣＰＵ）２１、システムメモリ２２、および、中央演算処理装置２１に関連付けられたメモリを含む種々のシステムコンポーネントを接続しているシステムバス２３を含む。システムバス２３は、バスメモリまたはバスメモリコントローラ、周辺バス、および任意の他のバスアーキテクチャと相互作用することが可能なローカルバスを含んでもよい。各バスの例としては、ＰＣＩ、ＩＳＡ、ＰＣＩ－Ｅｘｐｒｅｓｓ、ＨｙｐｅｒＴｒａｎｓｐｏｒｔ（商標）、ＩｎｆｉｎｉＢａｎｄ（商標）、シリアルＡＴＡ、I^2C、およびその他の好適なインターコネクトなどを挙げてよい。中央演算処理装置２１（プロセッサとも称される）は、単一のまたは複数のコアを有する単一のまたは複数のプロセッサのセットを含むことができる。プロセッサ２１は、本開示の技術を実装する１つまたは複数のコンピュータ実行可能コードを実行してもよい。システムメモリ２２は、本明細書で使用するデータおよび／またはプロセッサ２１によって実行可能なコンピュータプログラムを記憶する任意のメモリであってよい。システムメモリ２２は、ランダムアクセスメモリ（Random Access Memory：ＲＡＭ）２５などの揮発性メモリ、および読み取り専用メモリ（Read Only Memory：ＲＯＭ）２４、フラッシュメモリなどの不揮発性メモリ、またはこれらの任意の組み合わせを含んでもよい。基本入出力システム（Basic Input/Output System：ＢＩＯＳ）２６は、例えば、ＲＯＭ２４を使用してオペレーティングシステムをロードするときの手順などの、コンピュータシステム２０の各要素間の情報の伝送の基本手順を記憶していてもよい。

【００９２】

コンピュータシステム２０は、１つまたは複数の取り外し可能記憶デバイス２７、１つまたは複数の非取り外し可能記憶デバイス２８、またはこれらの組み合わせなどの１つまたは複数の記憶デバイスを含んでもよい。１つまたは複数の取り外し可能記憶デバイス２７、および非取り外し可能記憶デバイス２８は、記憶インターフェース３２を介してシステムバス２３に接続される。一態様では、記憶デバイスおよび対応するコンピュータ可読記憶媒体は、コンピュータシステム２０のコンピュータ命令、データ構造、プログラムモジュール、および他のデータを記憶するための電力独立型モジュールである。システムメモリ２２、取り外し可能記憶デバイス２７、非取り外し可能記憶デバイス２８は、種々のコンピュータ可読記憶媒体を使用してもよい。コンピュータ可読記憶媒体の例としては、

例えば、キャッシュ、ＳＲＡＭ、ＤＲＡＭ、ゼロ・コンデンサＲＡＭ、ツイントランジスタＲＡＭ、ｅＤＲＡＭ、ＥＤＯ ＲＡＭ、ＤＤＲ ＲＡＭ、ＥＥＰＲＯＭ、ＮＲＡＭ、ＲＲＡＭ（登録商標）、ＳＯＮＯＳ、ＰＲＡＭなどのマシンメモリ、ソリッドステートドライブ（Solid State Drive：ＳＳＤ）またはフラッシュドライブのようなフラッシュメモリまたはその他のメモリ技術、ハードディスクドライブまたはフロッピーディスクのような磁気カセット、磁気テープ、および磁気ディスク記憶装置、コンパクトディスク（Compact Disk Read Only Memory：ＣＤ－ＲＯＭ）またはデジタル多用途ディスク（Digital Versatile Disk：ＤＶＤ）のような光記憶装置、および所望のデータを記憶するために使用されてよく、コンピュータシステム２０によってアクセス可能な任意の他の媒体が挙げられる。

【００９３】

コンピュータシステム２０のシステムメモリ２２、取り外し可能記憶デバイス２７、および非取り外し可能記憶デバイス２８は、オペレーティングシステム３５、追加のプログラムアプリケーション３７、他のプログラムモジュール３８およびプログラムデータ３９を記憶するために使用されてよい。コンピュータシステム２０は、例えば、キーボード、マウス、スタイラス、ゲームコントローラ、音声入力デバイス、タッチ入力デバイスなどの、入力デバイス４０からのデータを通信するための周辺インターフェース４６、または、例えばシリアルポート、パラレルポート、ユニバーサルシリアルバス（Universal Serial Bus：ＵＳＢ）または他の周辺インターフェースなどの１つまたは複数の入出力ポートを介した、プリンタまたはスキャナなどの他の周辺デバイスを含んでもよい。例えば１つまたは複数のモニタ、プロジェクタまたは統合ディスプレイなどのディスプレイデバイス４７は、例えばビデオアダプタなどの出力インターフェース４８を通してシステムバス２３に接続されてもよい。ディスプレイデバイス４７に加えて、コンピュータシステム２０は、例えばスピーカおよび他の音響映像デバイスなどの他の周辺出力デバイス（図示せず）を搭載してもよい。

【００９４】

コンピュータシステム２０は、１つまたは複数のリモートコンピュータ４９へのネットワーク接続を使用して、ネットワーク環境で動作してよい。リモートコンピュータ（またはコンピュータ）４９は、コンピュータシステム２０の性質について記載されている上述の各要素のほとんどまたはすべてを含む、ローカルコンピュータワークステーションまたはサーバであってもよい。例えば、ルータ、ネットワーク局、ピアデバイスまたは他のネットワークノードなどのその他のデバイスが、コンピュータネットワーク内に存在する場合があるが、これらに限定されない。コンピュータシステム２０は、例えば、ローカルエリアコンピュータネットワーク（Local-Area Computer Network：ＬＡＮ）５０、広域コンピュータネットワーク（Wide-Area Computer Network：ＷＡＮ）、イントラネットおよびインターネットなどの１つまたは複数のネットワークを介して、リモートコンピュータ４９と通信するための１つまたは複数のネットワークインターフェース５１またはネットワークアダプタを含んでもよい。ネットワークインターフェース５１の例としては、イーサネットインターフェース、フレームリレーインターフェース、ＳＯＮＥＴインターフェースおよび無線インターフェースを挙げてもよい。

【００９５】

本開示の態様は、システム、方法、および／またはコンピュータプログラム製品であってもよい。コンピュータプログラム製品は、プロセッサに本開示の態様を実行させるコンピュータ可読プログラム命令を有する、コンピュータ可読記憶媒体（またはメディア）を含んでもよい。

【００９６】

コンピュータ可読記憶媒体は、命令またはデータ構造の形態でプログラムコードを保持し、記憶することができる有形デバイスであってもよく、コンピュータシステム２０などのコンピューティングデバイスのプロセッサによってアクセス可能なものである。コンピュータ可読記憶媒体は、電子記憶デバイス、磁気記憶デバイス、光記憶デバイス、電磁記

憶デバイス、半導体記憶デバイス、またはこれらの任意の好適な組み合わせであってもよい。例として、このようなコンピュータ可読記憶媒体は、ランダムアクセスメモリ（ＲＡＭ）、読み取り専用メモリ（ＲＯＭ）、ＥＥＰＲＯＭ、ポータブルコンパクトディスク読み取り専用メモリ（ＣＤ－ＲＯＭ）、デジタル多用途ディスク（ＤＶＤ）、フラッシュメモリ、ハードディスク、ポータブルコンピュータディスケット、メモリースティック、フロッピーディスク、あるいは、例えば命令がそこに溝状に記録されたパンチカードまたは隆起した構造などの機械的にコード化されたデバイスが挙げられる。本明細書で使用する場合、コンピュータ可読記憶媒体は、それ自体が、例えば、電波またはその他の自ら伝搬する電磁波、導波管または伝送媒体を通して伝搬する電磁波、あるいは有線によって伝送される電気信号などの一時的な信号であると解釈されるものではない。

【００９７】

本明細書に記載されるコンピュータ可読プログラム命令は、コンピュータ可読記憶媒体から、対応するコンピューティングデバイスに、もしくは、例えば、インターネット、ローカルエリアネットワーク、広域ネットワークおよび／または無線ネットワークなどのネットワークを介して、外部コンピュータまたは外部記憶デバイスにダウンロードされ得る。ネットワークは、銅製の伝送ケーブル、光伝送ファイバ、無線伝送、ルータ、ファイアウォール、スイッチ、ゲートウェイコンピュータおよび／またはエッジサーバを含んでもよい。各コンピューティングデバイスのネットワークインターフェースは、ネットワークからコンピュータ可読プログラム命令を受信して、対応するコンピューティングデバイス内部のコンピュータ可読記憶媒体に記憶するために、コンピュータ可読プログラム命令を転送する。

【００９８】

本開示の動作を実行するためのコンピュータ可読プログラム命令は、オブジェクト指向プログラミング言語、および従来の手続き型プログラミング言語を含む、１つまたは複数のプログラミング言語の任意の組み合わせで書き込まれる組み立て命令、命令セットアーキテクチャ（Instruction-Set-Architecture：ＩＳＡ）命令、機械命令、機械依存命令、マイクロコード、ファームウェア命令、ステート設定データ、あるいはソースコードまたはオブジェクトコードであってもよい。コンピュータ可読プログラム命令は、全面的にユーザのコンピュータで、部分的にユーザのコンピュータで、スタンドアロンソフトウェアパッケージとして、部分的にユーザコンピュータと部分的にリモートコンピュータとで、もしくは全面的にリモートコンピュータまたはサーバで実行されてよい。後半のシナリオでは、リモートコンピュータは、ＬＡＮまたはＷＡＮを含む任意のタイプのネットワークを通してユーザのコンピュータに接続されているか、または、接続は、外部コンピュータに向かって（例えば、インターネットを通して）構築されてもよい。いくつかの態様では、例えば、プログラマブル論理回路、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）またはプログラマブルロジックアレイ（Programmable Logic Array：ＰＬＡ）を含む電子回路は、本開示の態様を実施するために、コンピュータ可読プログラム命令の状態情報を利用して、コンピュータ可読プログラム命令を実行し、電子回路をパーソナライズしてもよい。

【００９９】

種々の態様では、本開示に記載されるシステムおよび方法を、モジュールの意味で扱うことができる。本発明で使用する場合、用語「モジュール」は、例えば、特定用途向け集積回路（ＡＳＩＣ）またはＦＰＧＡなどのハードウェアを使用して、または、例えば、マイクロプロセッサシステム、および（実行中に）マイクロプロセッサシステムを特殊目的デバイスに変換するモジュールの機能性を実装するための命令のセットなどのハードウェアとソフトウェアとの組み合わせとして実装される、実世界デバイス、コンポーネント、またはコンポーネントの機構を意味する。モジュールはまた、単独でハードウェアによって促進される特定の機能と、ハードウェアとソフトウェアとの組み合わせによって促進される他の機能との、２つの組み合わせとして実装されてもよい。特定の実装形態では、少なくとも一部、および場合によっては、すべてのモジュールは、コンピュータシステムの

プロセッサ（例えば、上記図４で詳細に記載されたもの）によって実施されてよい。したがって、各モジュールは、様々な好適な構成で実現される可能性があり、本明細書に例示されるいずれの特定の実装にも限定されるべきではない。

【０１００】

明瞭であるために、態様の決まりきった特徴のすべては本明細書に開示していない。本開示の任意の実際の実装形態の開発時に、開発者の特定の目的を達成するために非常に多くの実装形態固有の決定が行われる必要があり、これらの特定の目的は異なる実装形態および異なる開発者によって変更されることを理解されるであろう。このような開発作業は、複雑であり、かつ時間がかかる可能性があるが、それでも本開示から利益を得る当業者にとって日常的な技術的業務であるものと理解される。

【０１０１】

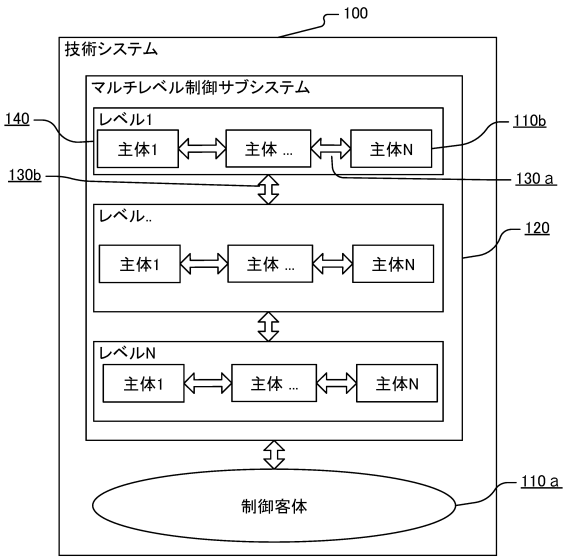
さらに、本明細書で用いる表現や用語は説明上のものであって、限定のためではなく、本明細書の用語や表現は、当業者の知見と組み合わされて、本明細書で提示する教示および指導に照らして当業者によって解釈されるものと理解すべきである。加えて、明示的記載がない限り、本明細書または特許請求の範囲におけるいかなる用語も、一般的でない、あるいは特別な意味を持つものとみなされることを意図していない。

【０１０２】

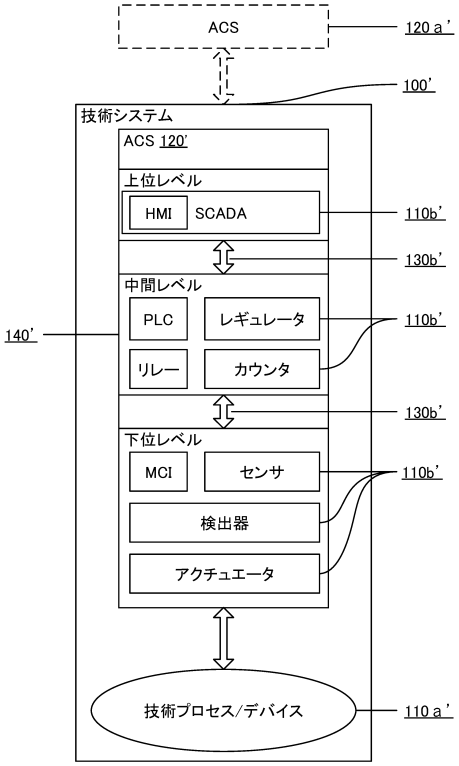
本明細書に開示された様々な態様は、本明細書で例示により言及された公知のモジュールと均等な現在および将来の公知の均等物を含む。さらに、態様および応用例を示し、かつ説明したが、本明細書に開示された発明の概念から逸脱することなく、上述したよりも多くの変更が可能であることは、本開示から利益を得る当業者には明らかであろう。

【図面】

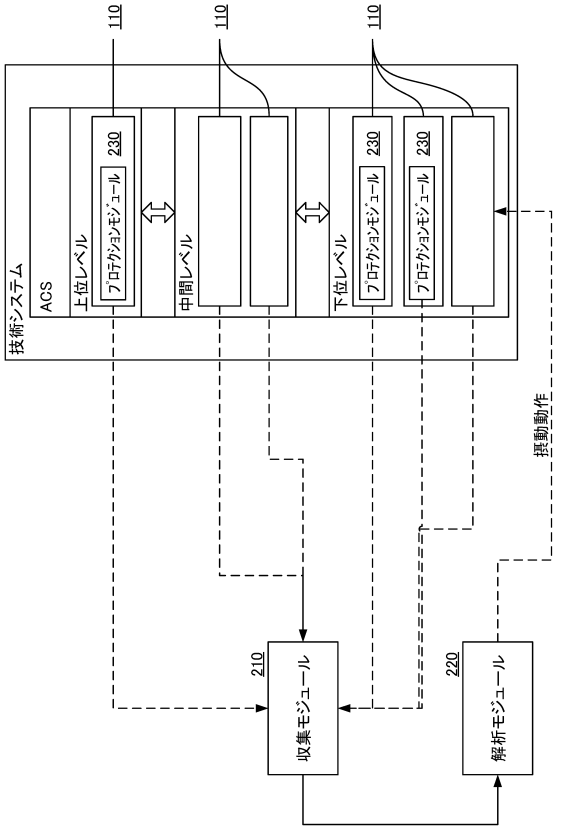
【図１ａ】



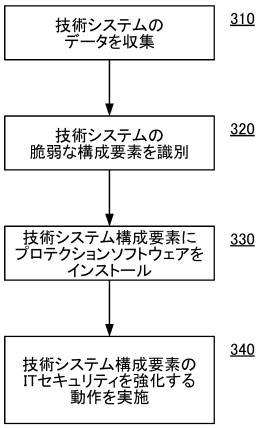
【図１ｂ】



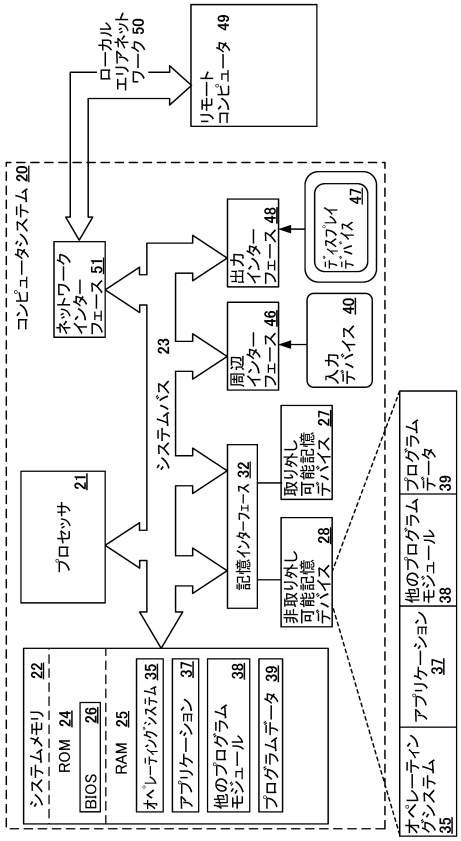
【図２】



【図３】



【図４】


コンピュータシステム 20
ローカルエリアネットワーク 50
リモートコンピュータ 49
ネットワークインターフェース 51
出力インターフェース 48
ディスプレイデバイス 47
周辺インターフェース 46
入力デバイス 40
システムバス 23
プロセッサ 21
記憶インターフェース 32
取り外し可能記憶デバイス 27
非取り外し可能記憶デバイス 28
システムメモリ 22
ROM 24
BIOS 26
RAM 25
オペレーティングシステム 35
アプリケーション 37
他のプログラムモジュール 38
プログラムデータ 39
オペレーティングシステム 35
アプリケーション 37
他のプログラムモジュール 38
プログラムデータ 39

フロントページの続き

(72)発明者　ドミトリー エー．クラーギン
ロシア国，１２５２１２ モスクワ，レニングラドスコ ショス ３９エー／３，エーオー カスペルスキー ラボ内

審査官　平井 誠

(56)参考文献　米国特許出願公開第２０１５／００８８７３３（ＵＳ，Ａ１）
国際公開第２０１５／１１４７９１（WO，Ａ１）
特表２０１７－５２５０５５（ＪＰ，Ａ）
特表２０１４－５０３０９９（ＪＰ，Ａ）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／５５－５７