

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7495190号
(P7495190)

(45)発行日 令和6年6月4日(2024.6.4)

(24)登録日 令和6年5月27日(2024.5.27)

(51)国際特許分類

G 0 6 F 21/57 (2013.01)

F I

G 0 6 F 21/57 3 5 0

請求項の数 17 (全35頁)

(21)出願番号	特願2022-500153(P2022-500153)	(73)特許権者	390009531
(86)(22)出願日	令和2年7月1日(2020.7.1)		インターナショナル・ビジネス・マシー
(65)公表番号	特表2022-539465(P2022-539465		ンズ・コーポレーション
	A)		INTERNATIONAL BUSI
(43)公表日	令和4年9月9日(2022.9.9)		NESS MACHINES CORPO
(86)国際出願番号	PCT/EP2020/068570		RATION
(87)国際公開番号	WO2021/004863		アメリカ合衆国10504 ニューヨー
(87)国際公開日	令和3年1月14日(2021.1.14)		ク州 アーモンク ニュー オーチャード
審査請求日	令和4年12月23日(2022.12.23)		ロード
(31)優先権主張番号	16/509,137		New Orchard Road, A
(32)優先日	令和1年7月11日(2019.7.11)		rmonk, New York 105
(33)優先権主張国・地域又は機関	米国(US)	(74)代理人	04, United States of
			America
			100112690
			弁理士 太佐 種一
			最終頁に続く

(54)【発明の名称】 コンテナのためのブラックボックス・セキュリティ

(57)【特許請求の範囲】

【請求項1】

コンテナのセキュリティを管理するためのシステムであって、
コンピュータ実行可能構成要素を記憶するメモリと、
前記メモリ内に記憶されたコンピュータ実行可能構成要素を実行するプロセッサと、
を備え、
前記コンピュータ実行可能構成要素は、
コンテナ・メモリへの1つまたは複数のタイプの管理アクセスが非活動化される定義さ
れたセキュアな状態に前記システムをセキュアにブートするために、信頼できるブート・
シーケンスの少なくとも一部を実行する、ブート構成要素と、
前記信頼できるブート・シーケンスの一部として開始され、また、前記コンテナ・メモ
リと共に使用するために1つまたは複数の復号鍵をセキュアに取得する、コア・サービス
構成要素と、
前記コンテナ・メモリに関連付けられたコンテナによって要求された1つまたは複数のフ
ァイルが暗号化されているかどうかを決定し、暗号化されている場合であって、前記コン
テナのエントリポイント・プロセスまたは前記エントリポイント・プロセスの下位によっ
てアクセスされる場合に、前記1つまたは複数の復号鍵を使用して前記1つまたは複数の
ファイルのランタイム復号を実行する、ランタイム復号構成要素と、
を備える、システム。

【請求項2】

非活動化される前記コンテナ・メモリへの前記1つまたは複数のタイプの管理アクセスは、

前記信頼できるブート・シーケンスに関連付けられた信頼できるカーネルに関して修正される、修正されたカーネルからのブーティングを介した、前記コンテナ・メモリへの管理アクセス、または、

前記信頼できるカーネルのカーネル・モジュールに加えて、追加のカーネル・モジュールをロードすることを介した、前記コンテナ・メモリへの管理アクセス、

のうちの、1つまたは複数を含む、
請求項1に記載のシステム。

【請求項3】

非活動化される前記コンテナ・メモリへの前記1つまたは複数のタイプの管理アクセスは、

1つまたは複数の仮想メモリ管理デバイスを介した、前記コンテナ・メモリへの管理アクセス、または、

1つまたは複数のランタイム・デバッグ機能を介した、前記コンテナ・メモリへの管理アクセス、

のうちの、1つまたは複数を含む、
請求項1に記載のシステム。

【請求項4】

非活動化される前記コンテナ・メモリへの前記1つまたは複数のタイプの管理アクセスは、

実行プロセスに関連付けられたメモリを閲覧するために前記実行プロセスを一時停止することを介した、前記コンテナ・メモリへの管理アクセス、または、

カーネル・メモリ・スワップ動作を介した、前記コンテナ・メモリへの管理アクセス、
のうちの、1つまたは複数を含む、
請求項1に記載のシステム。

【請求項5】

前記信頼できるブート・シーケンスは、前記コア・サービス構成要素を測定すること、および、結果として生じるコア・サービス構成要素測定結果を、信頼できる処理モジュール（TPM）プラットフォーム構成レジスタ（PCR）に記憶することを含む、請求項1ないし4のいずれかに記載のシステム。

【請求項6】

前記コア・サービス構成要素は、信頼できる第三者サービス・デバイスに対する信頼できる処理モジュール（TPM）リモート認証を使用して、前記1つまたは複数の復号鍵をセキュアに取得する、請求項1ないし5のいずれかに記載のシステム。

【請求項7】

前記ランタイム復号構成要素は、暗号化されていないファイルに対する1つまたは複数の要求をパス・スルーし、前記ランタイム復号構成要素は、プロセス識別子（PID）が前記コンテナの前記エントリポイント・プロセス、または前記エントリポイント・プロセスの下位プロセスに属することを保証するために、暗号化されたファイルを要求する1つまたは複数のプロセスの前記PIDをチェックする、請求項1ないし6のいずれかに記載のシステム。

【請求項8】

前記ランタイム復号構成要素は、前記コンテナをインスタンス化するために暗号化されたコンテナ・イメージを復号するために、前記1つまたは複数の復号鍵を使用する、請求項1ないし6のいずれかに記載のシステム。

【請求項9】

コンテナのセキュリティを管理するためのコンピュータ実装方法であって、

プロセッサに動作可能に結合されたブート構成要素によって、コンテナ・メモリへの1つまたは複数のタイプの管理アクセスが非活動化される定義されたセキュアな状態にコン

10

20

30

40

50

ピューティング・システムをセキュアにブートするために、信頼できるブート・シーケンスの少なくとも一部を実行すること、

前記ブート構成要素によって、前記プロセッサに動作可能に結合されたコア・サービス構成要素を前記信頼できるブート・シーケンスの一部として開始すること、

前記コア・サービス構成要素によって、前記コンテナ・メモリと共に使用するために1つまたは複数の復号鍵をセキュアに取得すること、および、

前記プロセッサに動作可能に結合されたランタイム復号構成要素によって、前記コンテナ・メモリに関連付けられたコンテナによって要求された1つまたは複数のファイルが暗号化されているかどうかを決定し、暗号化されている場合であって、前記コンテナによってアクセスされる場合に、前記1つまたは複数の復号鍵を使用して前記1つまたは複数のファイルのランタイム復号を実行すること、
を含む、コンピュータ実装方法。

10

【請求項10】

非活動化される前記コンテナ・メモリへの前記1つまたは複数のタイプの管理アクセスは、

前記信頼できるブート・シーケンスに関連付けられた信頼できるカーネルに関して修正される、修正されたカーネルからのブーティングを介した、前記コンテナ・メモリへの管理アクセス、または、

前記信頼できるカーネルのカーネル・モジュールに加えて、追加のカーネル・モジュールをロードすることを介した、前記コンテナ・メモリへの管理アクセス、

20

のうちの、1つまたは複数を含む、
請求項9に記載のコンピュータ実装方法。

【請求項11】

非活動化される前記コンテナ・メモリへの前記1つまたは複数のタイプの管理アクセスは、

1つまたは複数の仮想メモリ管理デバイスを介した、前記コンテナ・メモリへの管理アクセス、または、

1つまたは複数のランタイム・デバッグ機能を介した、前記コンテナ・メモリへの管理アクセス、

30

のうちの、1つまたは複数を含む、
請求項9に記載のコンピュータ実装方法。

【請求項12】

非活動化される前記コンテナ・メモリへの前記1つまたは複数のタイプの管理アクセスは、

実行プロセスに関連付けられたメモリを閲覧するために前記実行プロセスを一時停止することを介した、前記コンテナ・メモリへの管理アクセス、または、

カーネル・メモリ・スワップ動作を介した、前記コンテナ・メモリへの管理アクセス、
のうちの、1つまたは複数を含む、

請求項9に記載のコンピュータ実装方法。

【請求項13】

40

前記信頼できるブート・シーケンスは、前記コア・サービス構成要素を測定すること、および、結果として生じるコア・サービス構成要素測定結果を、信頼できる処理モジュール(TPM)プラットフォーム構成レジスタ(PCR)に記憶することを含み、また前記1つまたは複数の復号鍵を前記セキュアに取得することは、信頼できる第三者サービス・デバイスに対するTPMリモート認証を採用する、請求項9ないし12のいずれかに記載のコンピュータ実装方法。

【請求項14】

前記プロセッサに動作可能に結合された前記ランタイム復号構成要素によって、前記コンテナ・メモリに関連付けられたコンテナによってアクセスされる1つまたは複数のファイルのランタイム復号を実行するために、前記1つまたは複数の復号鍵を使用することは、

50

前記ランタイム復号構成要素によって、暗号化されていないファイルに対する1つまたは複数の要求をパス・スルーすること、および、

前記ランタイム復号構成要素によって、プロセス識別子（PID）が前記コンテナのエントリポイント・プロセス、または前記エントリポイント・プロセスの下位プロセスに属することを保証するために、暗号化されたファイルを要求する1つまたは複数のプロセスの前記PIDをチェックすること、

を含む、請求項9ないし13のいずれかに記載のコンピュータ実装方法。

【請求項15】

前記ランタイム復号構成要素によって、前記コンテナをインスタンス化するために暗号化されたコンテナ・イメージを復号するために、前記1つまたは複数の復号鍵を採用することをさらに含む、請求項9ないし14のいずれかに記載のコンピュータ実装方法。

【請求項16】

前記コンピュータ実装方法は、コンテナ・サーバにおける前記コンテナのインスタンス化およびランタイム中に、前記コンテナ・メモリへの前記1つまたは複数のタイプの管理アクセスから、前記コンテナに関連付けられたデータをセキュアにすることによって、前記コンテナ・サーバにおける前記コンテナのセキュリティを強化する、請求項9ないし15のいずれかに記載のコンピュータ実装方法。

【請求項17】

コンピュータ可読媒体上に記憶され、デジタル・コンピュータの内部メモリ内にロード可能な、コンピュータ・プログラムであって、前記プログラムがコンピュータ上で実行されるときに、請求項9ないし16のいずれかに記載の方法を実行するためのソフトウェア・コード部分を含む、コンピュータ・プログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本開示は、オペレーティング・システム・レベル仮想化技術に関し、オペレーティング・システム・カーネルは、コンテナとして知られる複数の分離されたユーザ・スペース・インスタンスをサポートする。

【背景技術】

【0002】

「コンテナ」技術の使用は、主にコンテナが、オペレーティング・システムの増大、および、対応的により高い仮想機械に関連付けられたリソース・オーバーヘッドなしに、物理的なインフラストラクチャ・コストの削減、ならびに、より良好な拡張容易性および柔軟性などの、仮想機械の利益の多くを有するため、クラウド・コンピューティング環境において勢いを増してきた。本明細書は、本明細書における技術の一態様を説明するために「コンテナ」という用語を用いるが、業界ではコンテナについての他の用語が知られていることを理解されよう。たとえばコンテナは時折、Open Container Initiative（OCI）コンテナ、Kubernetesコンテナ、Windows（R）Serverコンテナ、Hyper-Vコンテナ、Intel Clearコンテナ、またはKataコンテナと呼ばれている。コンテナ技術は一般に、ポータブル・コンテナが、1つまたは複数の仮想機械あるいは他のオペレーティング・システムを実行できるようにする。コンテナは分離されているため、互いに干渉することはできず、互いのリソースに許可なくアクセスすることはできない。本明細書で使用される「コンテナ」という用語は、いずれかの特定タイプのコンテナに限定されるものではない。

【0003】

本明細書は、本明細書における技術の別の態様を説明するために「コンテナ・エンジン」という用語を用いるが、業界ではコンテナ・エンジンについての他の用語が知られていることを理解されよう。コンテナ・エンジンは一般に、コンテナを分離するコンテナのためのランタイム環境を提供する。「ドッカー」は、幅広く使用されるコンテナ・エンジンの一例である。コンテナ・エンジンは一般に、とりわけ、アプリケーション・プログラミ

10

20

30

40

50

ング・インターフェース（API）およびコンテナによる使用のための他の機構を提供する、コンテナ・デーモンを含むことができる。コンテナ・エンジンは、さらに、コンテナの開始、停止、一時停止、一時停止解除、および削除の責務を負う、実行論理を含むことができる。本明細書で使用される「コンテナ・エンジン」という用語は、いずれかの特定タイプのコンテナ・エンジンに限定されるものではない。

【0004】

コンテナは一般に、ローカルまたはネットワーク化されたコンテナ・レジストリに記憶可能な、「コンテナ・イメージ」として伝送および記憶される。コンテナ・イメージは、任意の望ましい情報でタグ付け可能である。場合によっては、コンテナ・イメージはその256ビット・ハッシュによって識別可能である。

10

【0005】

場合によっては、コンテナは複数の協働コンテナの「スウォーム」において協働することができる。スウォームとは、複数の協働コンテナのグループである。スウォームは、ネットワークを介して共同するノードのグループの各々において、コンテナを含むことができる。サービスは、単一のコンテナではなくスウォーム上で実行可能である。各スウォームは、作業者にタスクをディスパッチするマネージャを有し、またマネージャは作業者としても働くことができる。マネージャは、タスクを割り当て、失敗した作業者のタスクを再割り当てする、リーダーを選択することができる。リーダー以外のマネージャは、以前に選択したリーダーが失敗した場合、新しいリーダーを選択するために待機することができる。スウォームを使用することで、コンテナを採用するサービスを必要に応じて拡大および縮小することができる。

20

【0006】

コンテナは様々なセキュリティ機構を採用する。一般に、コンテナ技術はコンテナ分離を提供するため、コンテナは互いに干渉することはできず、また互いのリソースに許可なくアクセスすることはできない。さらに、コンテナ・イメージがレジストリのストレージ内にある間、またはコンテナ・イメージが伝送されている間に、コンテナ・コードおよびデータを保護するために、コンテナ・イメージまたはその一部を暗号化することができる。しかしながら、コンテナ・イメージが暗号鍵を用いてホストするためにダウンロードされると、すべてのコンテナ・イメージ・コンテンツはプレーンテキストで復号可能であり、水平攻撃、および、不正管理者、すなわちコンテナを実行するオペレーティング・システムのルート・ユーザの、盗み見の影響を受けやすい。本開示の態様は、こうした管理アクセスを防ぐセキュリティ強化手段を提供し、それによってコンテナのセキュリティを向上させる。

30

【0007】

コンテナは、しばしばクラウド・コンピューティング環境においてサーバ上でホストされる。本開示は、クラウド・コンピューティング実施形態の詳細な説明を含み、本明細書に示される教示の実施例は、クラウド・コンピューティング環境に限定されるものではないことが理解されよう。むしろ、本開示の実施形態は、現在知られているかまたは後に開発されるいずれかの他のタイプのコンピューティング環境に関して実施可能である。

【0008】

したがって当分野では、前述の問題に対処することが求められている。

40

【発明の概要】

【0009】

本明細書で説明する1つまたは複数の実施形態において、コンテナのセキュリティ強化を容易にする、システム、コンピュータ実装方法、装置、またはコンピュータ・プログラム製品、あるいはその組み合わせが説明される。

【0010】

第1の態様から見ると、本発明は、コンテナのセキュリティを管理するためのシステムを提供し、システムは、コンピュータ実行可能構成要素を記憶するメモリと、メモリ内に記憶されたコンピュータ実行可能構成要素を実行するプロセッサとを備え、コンピュータ

50

実行可能構成要素は、コンテナ・メモリへの1つまたは複数のタイプの管理アクセスが非活動化される定義されたセキュアな状態にシステムをセキュアにブートするために、信頼できるブート・シーケンスの少なくとも一部を実行するブート構成要素と、信頼できるブート・シーケンスの一部として開始され、また、コンテナ・メモリと共に使用するために1つまたは複数の復号鍵をセキュアに取得する、コア・サービス構成要素と、コンテナ・メモリに関連付けられたコンテナのエントリポイント・プロセスまたはエントリポイント・プロセスの下位によってアクセスされる1つまたは複数のファイルのランタイム復号を実行するために、1つまたは複数の復号鍵を使用するランタイム復号構成要素と、を備える。

【0011】

さらなる態様から見ると、本発明は、コンテナのセキュリティを管理するためのコンピュータ実装方法を提供し、方法は、プロセッサに動作可能に結合されたブート構成要素によって、コンテナ・メモリへの1つまたは複数のタイプの管理アクセスが非活動化される定義されたセキュアな状態にコンピューティング・システムをセキュアにブートするために、信頼できるブート・シーケンスの少なくとも一部を実行すること、ブート構成要素によって、プロセッサに動作可能に結合されたコア・サービス構成要素を信頼できるブート・シーケンスの一部として開始すること、コア・サービス構成要素によって、コンテナ・メモリと共に使用するために1つまたは複数の復号鍵をセキュアに取得すること、および、プロセッサに動作可能に結合されたランタイム復号構成要素によって、コンテナ・メモリに関連付けられたコンテナによってアクセスされる1つまたは複数のファイルのランタイム復号を実行するために、1つまたは複数の復号鍵を使用すること、を含む。

【0012】

さらなる態様から見ると、本発明は、コンテナのセキュリティを管理するためのコンピュータ・プログラム製品を提供し、コンピュータ・プログラム製品は、処理回路によって読み取り可能であり、本発明のステップを実行するための方法を実行するための処理回路による実行のための命令を記憶する、コンピュータ可読記憶媒体を備える。

【0013】

さらなる態様から見ると、本発明は、コンピュータ可読媒体上に記憶され、デジタル・コンピュータの内部メモリ内にロード可能な、コンピュータ・プログラムを提供し、当該プログラムがコンピュータ上で実行されるときに、本発明のステップを実行するためのソフトウェア・コード部分を含む。

【0014】

さらなる態様から見ると、本発明は、コンテナのセキュリティを容易にするコンピュータ・プログラム製品を提供し、コンピュータ・プログラム製品は、共に具体化されるプログラム命令を有するコンピュータ可読記憶媒体を備え、プログラム命令は、処理構成要素によって、コンテナ・メモリへの1つまたは複数のタイプの管理アクセスが非活動化される定義されたセキュアな状態にコンピューティング・システムをセキュアにブートするために、信頼できるブート・シーケンスの少なくとも一部を実行すること、コア・サービス構成要素を信頼できるブート・シーケンスの一部として開始すること、コア・サービス構成要素によって、コンテナ・メモリと共に使用するために1つまたは複数の復号鍵をセキュアに取得すること、および、処理構成要素によって、コンテナ・メモリに関連付けられたコンテナによってアクセスされる1つまたは複数のファイルのランタイム復号を実行するために、1つまたは複数の復号鍵を使用することを、処理構成要素に実行させるために、処理構成要素によって実行可能である。

【0015】

一実施形態によれば、システムは、コンピュータ実行可能構成要素を記憶するメモリと、メモリ内に記憶されたコンピュータ実行可能構成要素を実行するプロセッサとを、備えることができる。コンピュータ実行可能構成要素は、コンテナ・メモリへの1つまたは複数のタイプの管理アクセスが非活動化される定義されたセキュアな状態にシステムをセキュアにブートするために、信頼できるブート・シーケンスの少なくとも一部を実行する、

ブート構成要素を備えることができる。信頼できるブート・シーケンスの一部として開始されるコア・サービス構成要素は、コンテナ・メモリと共に使用するために1つまたは複数の復号鍵をセキュアに取得することができる。ランタイム復号構成要素は、コンテナ・メモリに関連付けられたコンテナによってアクセスされる1つまたは複数のファイルのランタイム復号を実行するために、1つまたは複数の復号鍵を使用することができる。

【0016】

一実施形態によれば、コンピュータ実装方法は、プロセッサに動作可能に結合されたブート構成要素によって、コンテナ・メモリへの1つまたは複数のタイプの管理アクセスが非活動化される定義されたセキュアな状態にコンピューティング・システムをセキュアにブートするために、信頼できるブート・シーケンスの少なくとも一部を実行することを、含むことができる。ブート構成要素は、プロセッサに動作可能に結合されたコア・サービス構成要素を信頼できるブート・シーケンスの一部として開始することができる。コンピュータ実装方法は、コア・サービス構成要素によって、コンテナ・メモリと共に使用するために1つまたは複数の復号鍵をセキュアに取得すること、および、プロセッサに動作可能に結合されたランタイム復号構成要素によって、コンテナ・メモリに関連付けられたコンテナによってアクセスされる1つまたは複数のファイルのランタイム復号を実行するために、1つまたは複数の復号鍵を使用することも、含むことができる。

【0017】

別の実施形態によれば、コンテナのセキュリティを容易にするコンピュータ・プログラム製品は、共に具体化されるプログラム命令を有するコンピュータ可読記憶媒体を備えることができる。プログラム命令は、処理構成要素によって実行可能であり、コンテナ・メモリへの1つまたは複数のタイプの管理アクセスが非活動化される定義されたセキュアな状態にコンピューティング・システムをセキュアにブートするために、信頼できるブート・シーケンスの少なくとも一部を実行すること、および、コア・サービスを信頼できるブート・シーケンスの一部として開始することを、処理構成要素に実行させることができる。プログラム命令は、コア・サービスによって、コンテナ・メモリと共に使用するために1つまたは複数の復号鍵をセキュアに取得すること、および、処理構成要素によって、コンテナ・メモリに関連付けられたコンテナによってアクセスされる1つまたは複数のファイルのランタイム復号を実行するために、1つまたは複数の復号鍵を使用することを、実行可能とすることもできる。

【0018】

さらなる実施形態によれば、コンピュータ実装方法は、プロセッサに動作可能に結合されたシステムによって、プロセッサに動作可能に結合されたドッカー構成要素による1つまたは複数のコンテナをインスタンス化すること、および、1つまたは複数のコンテナのうちの少なくとも1つについて、システムによって、1つまたは複数のコンテナのうちの少なくとも1つによる1つまたは複数のファイル・アクセスを管理することを、含むことができ、ランタイム復号構成要素は、暗号化されていないファイルにアクセスするための1つまたは複数の要求をパス・スルーし、またランタイム復号構成要素は、プロセス識別子（PID）が、1つまたは複数のコンテナのうちの少なくとも1つのエントリポイント・プロセス、あるいはエントリポイント・プロセスの下位プロセスに属することを保証するために、暗号化されたファイルへのアクセスを要求する1つまたは複数のプロセスのPIDをチェックする。

【0019】

さらに別の実施形態によれば、コンピュータ実装方法は、プロセッサに動作可能に結合されたブート構成要素によって、コンピューティング・システムをセキュアにブートするために、信頼できるブート・シーケンスの少なくとも一部を実行することを含むことができ、信頼できるブート・シーケンスは、1つまたは複数の信頼できる処理モジュール（TPM）プラットフォーム構成レジスタ（PCR）をリセットすること、および、一連のブート構成要素を実行することを含み、一連のうちの各ブート構成要素は、一連のうちの次のブート構成要素を測定し、対応するPCR値を記憶する。一連のブート構成要素のうち

の少なくとも1つのブート構成要素は、コア・サービス構成要素を備えることができる。コンピュータ実装方法は、プロセッサに動作可能に結合されたコア・サービス構成要素によって、信頼できる第三者サービス・デバイスに対するTPMリモート認証を実行すること、および、コア・サービス構成要素によって、信頼できる第三者サービス・デバイスからコンテナについての1つまたは複数の復号鍵をセキュアに取得すること、および、コンテナに関連付けられたコンテナ・メモリ内にコンテナについての1つまたは複数の復号鍵を記憶することも、含むことができる。

【0020】

次に本発明を、下記の図面に示された好ましい実施形態を参照しながら、単なる例として説明する。

【図面の簡単な説明】

【0021】

【図1】本明細書で説明する1つまたは複数の実施形態に従った、クラウド・コンピューティング環境を示す図である。

【図2】本明細書で説明する1つまたは複数の実施形態に従った、抽象モデル層を示す図である。

【図3】本明細書で説明する1つまたは複数の実施形態に従った、例示の非限定的コンピューティング環境を示すブロック図である。

【図4A】本明細書で説明する1つまたは複数の実施形態に従った、コンテナを取り出し、記憶、および実行する、例示の非限定的システムを示すブロック図である。

【図4B】本明細書で説明する1つまたは複数の実施形態に従った、コンテナを取り出し、記憶、および実行する、例示の非限定的システムを示すブロック図である。

【図5】本明細書で説明する1つまたは複数の実施形態に従った、コンテナをセキュアにするために修正されたドッカー技術を採用する、例示の非限定的システムを示すブロック図である。

【図6】本明細書で説明する1つまたは複数の実施形態に従った、例示の非限定的ブート構成要素を示す概略ブロック図である。

【図7】本明細書で説明する1つまたは複数の実施形態に従った、例示の非限定的コア・サービス構成要素を示す概略ブロック図である。

【図8】本明細書で説明する1つまたは複数の実施形態に従った、例示の非限定的ランタイム復号構成要素の概略ブロック図である。

【図9】本明細書で説明する1つまたは複数の実施形態に従った、コンテナをホストするシステムのセキュリティ強化を容易にする、例示の非限定的コンピュータ実装方法を示すフロー図である。

【図10】本明細書で説明する1つまたは複数の実施形態に従った、コンテナをホストするシステムのセキュリティ強化を容易にする、例示の非限定的コンピュータ実装方法を示すフロー図である。

【図11】本明細書で説明する1つまたは複数の実施形態に従った、コンテナをホストするシステムのセキュリティ強化を容易にする、例示の非限定的コンピュータ実装方法を示すフロー図である。

【発明を実施するための形態】

【0022】

以下の詳細な説明は単なる例示であり、実施形態または適用例あるいはその両方または実施形態の使用を、限定することは意図されていない。

【0023】

次に、図面を参照しながら1つまたは複数の実施形態を説明するが、全体を通じて同様の参照番号は同様の要素を示すために使用される。以下の説明において、説明の目的で、1つまたは複数の実施形態をより完全に理解するために多数の特定の詳細が示される。しかしながら、様々な場合に、1つまたは複数の実施形態はこれらの特定の詳細を用いることなく実施可能であることは明らかである。

10

20

30

40

50

【0024】

クラウド・コンピューティングは、最小の管理作業またはサービス・プロバイダとの対話で迅速に供給および解放可能な、構成可能コンピューティング・リソース（たとえば、ネットワーク、ネットワーク帯域幅、サーバ、処理、メモリ、ストレージ、アプリケーション、仮想機械、およびサービス）の共有プールへの、好都合なオンデマンド・ネットワーク・アクセスを実行可能にするための、サービス・デリバリのモデルである。このクラウド・モデルは、少なくとも5つの特徴、少なくとも3つのサービス・モデル、および少なくとも4つの展開モデルを含むことができる。

【0025】

特徴は下記の通りである。

オンデマンド・セルフサービス：クラウド消費者は、ヒトがサービス・プロバイダと対話することを要求せずに必要に応じて自動的に、サーバ時間およびネットワーク・ストレージなどのコンピューティング機能を、一方的に提供することができる。

ブロード・ネットワーク・アクセス：機能はネットワークを介して利用可能であり、異種のシンまたはシック・クライアント・プラットフォーム（たとえば、携帯電話、ラップトップ、およびPDA）による使用を促進させる標準メカニズムを介してアクセス可能である。

リソース・プーリング：プロバイダのコンピューティング・リソースは、需要に従って動的に割り当ておよび再割り当てされた異なる物理リソースおよび仮想リソースを、マルチテナント・モデルを使用して複数の消費者にサービスするためにプールされる。消費者は一般に、提供されるリソースの正確なロケーションを介した制御または知識を有さないが、より高い抽象度でロケーション（たとえば、国、州、またはデータセンタなど）を指定することができるという点で、ロケーション独立感が存在する。

迅速順応性：機能は、急速にスケール・アウトするために迅速かつ順応的に、場合によっては自動的に提供可能であり、また、急速にスケール・インするために迅速に解放可能である。消費者にとって、提供に使用可能な機能はしばしば無制限に、いつでもいかなる量でも購入可能であるように見える。

測定されるサービス：クラウド・システムは、サービスのタイプ（たとえば、ストレージ、処理、帯域幅、およびアクティブ・ユーザ・アカウント）に適切な何らかの抽象度で、計測機能を活用することによって、リソースの使用を自動的に制御および最適化する。リソース使用率は、監視、制御、および報告可能であり、利用されるサービスのプロバイダおよび消費者の両方に透明性を提供する。

【0026】

サービス・モデルは下記の通りである。

Software as a Service (SaaS)：消費者に提供される機能は、クラウド・インフラストラクチャ上で実行するプロバイダのアプリケーションを使用することである。アプリケーションには、ウェブ・ブラウザ（たとえば、ウェブ・ベースの電子メール）などのシン・クライアント・インターフェースを介して様々なクライアント・デバイスからアクセス可能である。消費者は、制限されたユーザ特有のアプリケーション構成設定の起こり得る例外を伴う、ネットワーク、サーバ、オペレーティング・システム、ストレージ、あるいは個々のアプリケーション機能を含む、基礎となるクラウド・インフラストラクチャを管理または制御しない。

Platform as a Service (PaaS)：消費者に提供される機能は、プロバイダによってサポートされるプログラミング言語およびツールを使用して作成された、消費者作成または獲得アプリケーションを、クラウド・インフラストラクチャ上に展開することである。消費者は、ネットワーク、サーバ、オペレーティング・システム、またはストレージを含む、基礎となるクラウド・インフラストラクチャを管理または制御しないが、展開されたアプリケーション、および場合によっては環境構成をホストするアプリケーションを介した制御を有する。

Infrastructure as a Service (IaaS)：消費者に提供

10

20

30

40

50

される機能は、処理、ストレージ、ネットワーク、ならびに、オペレーティング・システムおよびアプリケーションを含むことが可能な任意のソフトウェアを消費者が展開および実行することが可能な他の基本コンピューティング・リソースを、提供することである。消費者は、基礎となるクラウド・インフラストラクチャを管理または制御しないが、オペレーティング・システム、ストレージ、展開されたアプリケーション、および場合によっては、選択ネットワーキング構成要素（たとえば、ホスト・ファイアウォール）の制限された制御を介した制御を有する。

【0027】

展開モデルは下記の通りである。

プライベート・クラウド：クラウド・インフラストラクチャは、一組織のためにのみ動作する。組織または第三者によって管理可能であり、構内または構外に存在可能である。

コミュニティ・クラウド：クラウド・インフラストラクチャは、いくつかの組織によって共有され、共有懸案事項（たとえば、任務、セキュリティ要件、ポリシー、およびコンプライアンス考慮事項）を有する特定のコミュニティをサポートする。組織または第三者によって管理可能であり、構内または構外に存在可能である。

パブリック・クラウド：クラウド・インフラストラクチャは、一般人または大規模業界団体が使用可能であり、クラウド・サービスを販売する組織によって所有される。

ハイブリッド・クラウド：クラウド・インフラストラクチャは、固有のエンティティを保持するが、データおよびアプリケーションのポータビリティ（たとえば、クラウド間の負荷バランシングのためのクラウド・バースティング）を実行可能にする、標準化技術またはプロプライエタリ技術によって共に束縛される、2つまたはそれ以上の（プライベート、コミュニティ、またはパブリック）クラウドの構成物である。

【0028】

クラウド・コンピューティング環境は、ステートレスネス、疎結合、モジュール方式、および意味相互運用性に焦点を置いた、サービス指向である。クラウド・コンピューティングの中心は、相互接続されたノードのネットワークを含むインフラストラクチャである。

【0029】

次に図1を参照すると、例示的なクラウド・コンピューティング環境50が示されている。図に示されるように、クラウド・コンピューティング環境50は、たとえば携帯情報端末（PDA）または携帯電話54A、デスクトップ・コンピュータ54B、ラップトップ・コンピュータ54C、または自動車コンピュータ・システム54N、あるいはその組み合わせなどの、クラウド消費者によって使用されるローカル・コンピューティング・デバイスが通信する際に使用可能な、1つまたは複数のクラウド・コンピューティング・ノード10を含む。クラウド・コンピューティング・ノード10は、互いに通信可能である。クラウド・コンピューティング・ノード10は、上記で説明したようなプライベート、コミュニティ、パブリック、またはハイブリッド・クラウド、あるいはそれらの組み合わせなどの、1つまたは複数のネットワーク内で、物理的または仮想的にグループ化可能である（図示せず）。これによってクラウド・コンピューティング環境50は、クラウド消費者がローカル・コンピューティング・デバイス上のリソースを維持することを必要としないサービスとして、インフラストラクチャ、プラットフォーム、またはソフトウェア、あるいはその組み合わせを提供することができる。図1に示されるタイプのコンピューティング・デバイス54A～Nは単なる例示であることが意図されること、ならびに、コンピューティング・ノード10およびクラウド・コンピューティング環境50は、任意のタイプのネットワーク、または（たとえば、ウェブ・ブラウザを使用する）ネットワークアドレス可能接続、あるいはその両方を介して、任意のタイプのコンピュータ化されたデバイスと通信可能であることを理解されよう。

【0030】

次に図2を参照すると、クラウド・コンピューティング環境50（図1）によって提供される機能抽象層のセットが示されている。図2に示される構成要素、層、および機能は、単なる例示であることが意図され、本発明の実施形態はこれらに限定されないことをあ

10

20

30

40

50

らかじめ理解されたい。図示されるように、下記の層および対応する機能が提供される。

【0031】

ハードウェアおよびソフトウェア層60は、ハードウェアおよびソフトウェアの構成要素を含む。ハードウェア構成要素の例は、メインフレーム61、RISC（縮小命令セット・コンピュータ）アーキテクチャ・ベース・サーバ62、サーバ63、ブレードサーバ64、ストレージ・デバイス65、ならびに、ネットワークおよびネットワークング構成要素66を含む。いくつかの実施形態では、ソフトウェア構成要素はネットワーク・アプリケーション・サーバ・ソフトウェア67およびデータベース・ソフトウェア68を含む。

【0032】

仮想化層70は、以下の仮想エンティティ、仮想サーバ71、仮想ストレージ72、仮想プライベート・ネットワークを含む仮想ネットワーク73、仮想アプリケーションおよびオペレーティング・システム74、ならびに仮想クライアント75の例が提供可能な、抽象層を提供する。

【0033】

一例において、管理層80は、下記で説明する機能81～84を提供することができる。機能81～84は、たとえば、コンピューティング・リソース、および、クラウド・コンピューティング環境内でタスクを実行するために利用される他のリソースの、動的調達を提供する、リソース提供を含むことができる。計測および価格決定は、リソースがクラウド・コンピューティング環境内で利用される際のコスト追跡、およびこれらのリソースを消費するための課金または請求を提供することができる。一例において、これらのリソースはアプリケーション・ソフトウェア・ライセンスを含むことができる。セキュリティは、クラウド消費者およびタスクについての識別検証、ならびにデータおよび他のリソースについての保護を提供する。ユーザ・ポータルは、消費者およびシステム管理者に対して、クラウド・コンピューティング環境へのアクセスを提供することができる。サービス・レベル管理は、必要なサービス・レベルを満たすように、クラウド・コンピューティング・リソース割り振りおよび管理を提供することができる。サービス内容合意書（SLA）の計画および履行は、将来の要件がSLAに従って予測される、クラウド・コンピューティング・リソースについて、事前の取り決めおよび調達を提供することができる。さらに、機能85は、作業負荷層90内で実行するコンテナを管理するコンテナ・エンジンを提供することができる。

【0034】

作業負荷層90は、クラウド・コンピューティング環境が利用できる機能の例を提供する。この層から提供できる作業負荷および機能の例は、マッピングおよびナビゲーション91、ソフトウェア開発およびライフサイクル管理92、仮想クラスルーム教育配信93、データ分析処理94、トランザクション処理95、およびコンテナ96を含む。作業負荷層90は、任意選択として、機能85によって提供されるコンテナ・エンジンによって管理可能な多くのコンテナ96をホストすることができる。コンテナ96の各コンテナは、コンテナ・コードおよびデータを含むことができる。

【0035】

図3は、本明細書で説明する1つまたは複数の実施形態に従った、例示の非限定的コンピューティング環境のブロック図を示す。コンピューティング環境の様々な態様はハードウェア構成要素である一方で、他の態様はソフトウェア構成要素である。図3を参照すると、本開示の様々な態様を実装するのに適切な動作環境300は、コンピュータ310を含むことができる。コンピュータ310は、たとえば図1に示されたクラウド・コンピューティング・ノード10のうちの1つなどのクラウド・コンピューティング・ノードを備えることができる。したがって、コンピュータ310は、図1に示されたクラウド・コンピューティング環境50に参加することができる。他の実施形態では、コンピュータ310は、理解されるように、図1および図2に示されるクラウド・コンピューティング環境に参加することなく本開示の態様を実装することができる。

【0036】

コンピュータ 310 は、処理ユニット 311、システム・メモリ 312、およびシステム・バス 315 を含むことができる。システム・バス 315 は、システム・メモリ 312 を含むが限定されないシステム構成要素を、処理ユニット 311 に結合する。処理ユニット 311 は、任意の様々な使用可能プロセッサとすることができる。デュアル・マイクロプロセッサおよび他のマルチプロセッサ・アーキテクチャも、処理ユニット 311 として採用可能である。システム・バス 315 は、メモリ・バスもしくはメモリ・コントローラ、周辺バスもしくは外部バス、または、任意の様々な使用可能バス・アーキテクチャを使用するローカル・バス、あるいはその組み合わせを含む、いくつかのタイプのバス構造のいずれかとすることが可能であり、使用可能バス・アーキテクチャは、インダストリアル・スタンダード・アーキテクチャ (ISA)、マイクロチャネル・アーキテクチャ (MSA)、拡張 ISA (EISA)、インテリジェント・ドライブ・エレクトロニクス (IDE)、VESA ローカル・バス (VLB)、ペリフェラル・コンポーネント・インターコネクト (PCI)、カード・バス、ユニバーサル・シリアル・バス (USB)、アドバンスト・グラフィクス・ポート (AGP)、ファイアワイア (IEEE 1394)、およびスモール・コンピュータ・システムズ・インターフェース (SCSI) を含むが、限定されない。

【0037】

システム・メモリ 312 は、揮発性メモリ 313 および不揮発性メモリ 314 も含むことができる。基本入力／出力システム (BIOS) は、起動時などの、コンピュータ 310 内の要素間で情報を転送するための基本ルーチンを含み、不揮発性メモリ 314 内に格納される。実例として、また限定ではなく、不揮発性メモリ 314 は、読み取り専用メモリ (ROM)、プログラマブル ROM (PROM)、電気プログラマブル ROM (EPROM)、電気消去可能プログラマブル ROM (EEPROM)、フラッシュ・メモリ、または不揮発性ランダム・アクセス・メモリ (RAM) (たとえば、強誘電 RAM (FeRAM)) を含むことができる。揮発性メモリ 313 は、外部キャッシュ・メモリとして作用するランダム・アクセス・メモリ (RAM) を含むこともできる。実例として、また限定ではなく、RAM は、静的 RAM (SRAM)、動的 RAM (DRAM)、シンクロナス DRAM (SDRAM)、ダブル・データ・レート SDRAM (DDR SDRAM)、拡張 SDRAM (ESDRAM)、Synchlink DRAM (SLDRAM)、ダイレクト Rambus RAM (DRRAM)、ダイレクト Rambus 動的 RAM (DRDRAM)、および Rambus 動的 RAM などの、多くの形で使用可能である。

【0038】

コンピュータ 310 は、取り外し可能／取り外し不可、揮発性／不揮発性のコンピュータ記憶媒体を含むこともできる。図 3 は、たとえばディスク・ストレージ 316 を示す。ディスク・ストレージ 316 は、磁気ディスク・ドライブ、フロッピー (R) ・ディスク・ドライブ、テープ・ドライブ、Jaz ドライブ、Zip ドライブ、LS-100 ドライブ、フラッシュ・メモリ・カード、またはメモリ・スティックのようなデバイスを含むこともできるが、限定されない。ディスク・ストレージ 316 は、コンパクト・ディスク ROM デバイス (CD-ROM)、CD 記録可能ドライブ (CD-R ドライブ)、CD 書き換え可能ドライブ (CD-RW ドライブ)、またはデジタル・バーサタイル・ディスク ROM ドライブ (DVD-ROM) などの、光ディスク・ドライブを含むが限定されない、他の記憶媒体とは別々に、または組み合わせて、記憶媒体を含むこともできる。システム・バス 315 へのディスク・ストレージ 316 の接続を容易にするために、典型的には、インターフェース 315 などの、取り外し可能または取り外し不可のインターフェースが使用される。

【0039】

いくつかの実施形態では、暗号化されたコンテナ・イメージ 317 を、コンテナ・レジストリ 344 からコンピュータ 310 によって取り出し、ディスク・ストレージ 316 に記憶することができる。暗号化されたコンテナ・イメージ 317 は、暗号化形式でコンピュータ 310 に転送され、ディスク・ストレージ 316 に記憶されるため、コンピュータ

10

20

30

40

50

310の不正管理者が、暗号化されたコンテナ・イメージ317のコンテンツにアクセスするリスクは少ない。暗号化されたコンテナ・イメージ317は、ディスク・ストレージ316内に記憶される代わりに、または記憶されることに加えて、システム・メモリ312内に記憶可能であることにも留意されたい。

【0040】

図3は、一方で、ユーザ、アプリケーション、およびコンテナの間で仲介として作用し、また他方で、コンピュータ310のリソースとして作用する、ソフトウェアも示している。こうしたソフトウェアは、たとえばオペレーティング・システム330を含むことができる。ディスク・ストレージ316上に記憶可能なオペレーティング・システム330は、コンピュータ310のリソースを制御および割り振るよう作用する。いくつかの実施形態では、オペレーティング・システム330は仮想機械（VM）とすることができ、またコンピュータ310は複数のVMをホストすることができる。本開示は、様々なオペレーティング・システムまたはオペレーティング・システムの組み合わせで実装可能であることを理解されよう。

10

【0041】

ブート構成要素370などの1つまたは複数のブート構成要素は、オペレーティング・システム330のブーティングに関与することができる。ブート構成要素370は、オペレーティング・システム330をセキュアにブートするために、信頼できる処理モジュール（TPM）324と対話することができる。一般に、TPM 324は、信頼できるブート構成要素のハッシュをプラットフォーム構成レジスタ（PCR）325内にセキュアに記憶する。各ブート構成要素は、信頼できるブート・シーケンスにおける次のブート構成要素のハッシュを実行し、TPM 324を使用して、PCR 325内の対応するハッシュに照らして測定されたハッシュをチェックする。信頼できるブート・シーケンスにおける次のブート構成要素は、そのハッシュが正しい場合にのみロードされ、それによってブート構成要素が信頼できることが保証され、結果としてコンピュータ310は検証可能にセキュアな状態をブートさせることになる。

20

【0042】

ブート構成要素370は、コンピュータ310のセキュアな状態を要求することができる。たとえばブート構成要素370は、特定のオペレーティング・システム330の機能を制限またはブロックすることができる。本明細書でさらに説明するように、ブート構成要素370は、たとえばコンテナ・メモリへの、たとえばコンテナ374などのコンテナのために確保されているシステム・メモリ312の一部への、1つまたは複数のタイプの管理アクセスを非活動化することができる。

30

【0043】

さらに、ブート構成要素370は、信頼できるコア・サービス構成要素371が信頼できるブート・シーケンスの一部としてロードされることを、保証することができる。コア・サービス構成要素371は、暗号化されたコンテナ・イメージ317またはその一部を復号するために、復号鍵をセキュアに取得する責務を負うことができる。いくつかの実施形態では、コア・サービス構成要素371は、復号鍵をセキュアに取得するために、上記で紹介したTPM 324を使用することができる。コア・サービス構成要素371は、復号鍵を取得するために、信頼できる第三者サービス・デバイス345に対するTPM 324リモート認証を採用することができる。

40

【0044】

システム・アプリケーション331は、たとえば、システム・メモリ312内またはディスク・ストレージ316上のいずれかに記憶されたプログラム・モジュール332およびプログラム・データ333を介して、オペレーティング・システム330によるリソースの管理を利用することができる。同様に、コンテナ・エンジン372は、オペレーティング・システム330上で動作することができる。コンテナ・エンジン372は、たとえば、374、375、および376などのコンテナを、ロード、開始、または停止すること、あるいはその組み合わせが可能である。コンテナ・エンジン372は、コンテナ37

50

4、375、および376を分離することができるため、コンテナ374、375、および376は、互いに干渉すること、または互いのデータにアクセスすることはできない。本明細書でさらに詳細に説明するように、コンテナ・エンジン372は任意選択として、コンテナ374によって暗号化されたファイル・アクセスを管理することが可能なランタイム復号構成要素(RDC)373と共に、さらなるコンテナ・セキュリティを提供することができる。ランタイム復号構成要素373は、信頼できるコア・サービス構成要素371によってセキュアに取得された復号鍵を使用することができる。

【0045】

本開示の実施形態は、(1)特定タイプの管理メモリ・アクセスが非活動化された、コンピュータ310の定義された状態を強化するブート構成要素370、(2)コンテナ374のファイル・アクセスのために復号鍵をセキュアに取得するコア・サービス構成要素371、および(3)コンテナ374の代わりに復号鍵を使用するランタイム復号構成要素373の組み合わせを、少なくとも部分的に介して、コンテナ374のコードおよびデータに対する望ましくない管理者の盗み見を防止することができる。いくつかの実施形態では、ブート構成要素370、コア・サービス構成要素371、またはランタイム復号構成要素373、あるいはその組み合わせは、コンピュータ310に追加可能であり、個々のメモリまたはプロセッサ構成要素あるいはその組み合わせを有する、ハードウェア構成要素とすることができる。他の実施形態では、ブート構成要素370、コア・サービス構成要素371、またはランタイム復号構成要素373、あるいはその組み合わせは、信頼できるブート・シーケンスの実行を容易にするために、1つまたは複数の異なる動作を実行するための命令と共に設計された、コンピュータ・コードとすることができる。これらの手段の結果として、コンピュータ310の管理者は、システム・メモリ312内の暗号化されていないコンテナ374のコードおよびデータにアクセスすることはできず、コンピュータ310の管理者は、コンテナ374のコードおよびデータを復号するための復号鍵を取得することはできない。

【0046】

場合によっては、ユーザは、入力デバイス342を介してコマンドまたは情報をコンピュータ310に入力することができる。他の実施形態では、任意のエンティティがコマンドまたは情報をコンピュータ310に入力することができる。エンティティは、ロボット、人工知能デバイス、コンピュータなどを含むことができるが、限定されない。

【0047】

入力デバイス342は、マウスなどのポインティング・デバイス、トラックボール、スタイラス、タッチ・パッド、キーボード、マイクロフォン、ジョイスティック、ゲーム・パッド、衛星放送用アンテナ、スキャナ、TVチューナ・カード、デジタル・カメラ、デジタル・ビデオ・カメラ、ウェブ・カメラなどを含むが、限定されない。これらおよび他の入力デバイスは、インターフェース・ポート322を介するシステム・バス315を介して、処理ユニット311に接続する。インターフェース・ポート322は、たとえば、シリアル・ポート、パラレル・ポート、ゲーム・ポート、およびユニバーサル・シリアル・バス(USB)を含む。出力デバイス341は、入力デバイス342と同じタイプのポートのうちのいくつかを使用する。したがって、たとえばUSBポートは、コンピュータ310に入力を提供するために、およびコンピュータ310から情報を出力デバイス341に出力するために、使用することができる。出力アダプタ321は、特殊なアダプタを必要とする他の出力デバイス341の中でもとりわけ、モニタ、スピーカ、およびプリンタのようないくつかの出力デバイス341が存在することを示すために提供される。出力アダプタ321は、単なる例示であって限定ではなく、出力デバイス341とシステム・バス315との間に接続手段を提供する、ビデオおよびサウンド・カードを含む。他のデバイスまたはデバイスのシステムあるいはその両方が、入力および出力の両方の機能を提供することに留意されたい。

【0048】

コンピュータ310は、コンテナ・レジストリ344および信頼できる第三者サービス

10

20

30

40

50

・デバイス 345 などの、1つまたは複数のリモート・コンピュータへの論理接続を使用して、ネットワーク化環境で動作することができる。コンテナ・レジストリ 344 は、暗号化されたコンテナ・イメージ 317 が取得されるサーバを含むことができる。信頼できる第三者サービス・デバイス 345 は、たとえば、TPM 324 に関連してコア・サービス構成要素 371 によって、暗号化されたコンテナ・イメージ 317 のための復号鍵が取得されるサーバを含むことができる。コンピュータ 310 と通信可能な他のリモート・コンピュータは、コンピュータ、サーバ、ルータ、ネットワーク PC、ワークステーション、マイクロプロセッサ・ベース・アプリケーション、ピア・デバイス、または他の共通ネットワーク・ノードなどを含み、典型的には、コンピュータ 310 に関して説明する要素のうちの多くまたはすべてを含むこともできる。

10

【0049】

344 および 345 などのリモート・コンピュータは、ネットワーク・インターフェース 343 を介してコンピュータ 310 に論理的に接続可能であり、その後、通信接続 323 を介して物理的に接続可能である。ネットワーク・インターフェース 343 は、ローカル・エリア・ネットワーク (LAN)、ワイド・エリア・ネットワーク (WAN)、セルラ・ネットワークなどの、有線または無線、あるいはその両方の通信ネットワークを包含する。LAN 技術は、ファイバ分散データ・インターフェース (FDDI)、銅線分散データ・インターフェース (CDDI)、イーサネット (R)、トークン・リングなどを含む。WAN 技術は、2 地点間リンク、統合サービス・デジタル・ネットワーク (ISDN) およびその変形などの回路交換ネットワーク、パケット交換ネットワーク、およびデジタル加入者回線 (DSL) を含むが、限定されない。通信接続 323 は、ネットワーク・インターフェース 343 をシステム・バス 315 に接続するために採用されるハードウェア／ソフトウェアを指す。通信接続 323 は、明白に示すためにコンピュータ 310 内部に示されているが、コンピュータ 310 の外部であってもよい。ネットワーク・インターフェース 343 への接続のためのハードウェア／ソフトウェアは、単なる例示の目的で、通常の電話品質モデム、ケーブル・モデム、および DSL モデムを含むモデム、ISDN アダプタ、およびイーサネット (R) ・カードなどの、内部および外部技術も含むことができる。

20

【0050】

図 4A および図 4B は、本明細書で説明する 1つまたは複数の実施形態に従った、コンテナを取り出し、記憶、および実行する例示の非限定的システムのブロック図を示す。本明細書で説明する他の実施形態において採用される同様の要素を反復的に記述することは、簡潔にするために省略する。

30

【0051】

図 4A は、図 4B に示されるセキュリティ強化されたホスト機械 450 と対照的な、セキュリティの脆弱なホスト機械 410 を示す。図 4A および図 4B のどちらにおいても、ホスト機械 410、450 はそれぞれ、レジストリ 400 から暗号化されたコンテナ・イメージ 401 を取り出すことができる。レジストリ 400 は、複数の暗号化されたコンテナ・イメージ 401、402、403、および 404 を含む。

【0052】

ホスト機械 410 およびレジストリ 400 は、たとえば、図 1 に示されるクラウド・コンピューティング・ノード 10 の中の、クラウド・コンピューティング・ノードを提供することができる。ホスト機械 410 は、たとえば、図 3 に示されたブート構成要素 370、コア・サービス構成要素 371、およびランタイム復号構成要素 373 などの、セキュリティ機構を伴わない、ホスト・コンテナに装備されるサーバとすることができる。したがって、ホスト機械 410 は、暗号化されたコンテナ・イメージ 401 をレジストリ 400 からセキュアに取り出すことができる。鍵獲得構成要素 412 は、暗号化されたコンテナ・イメージ 401 を復号するための復号鍵を、さらに獲得することができる。

40

【0053】

暗号化されたコンテナ・イメージ 401 が復号され、復号されたコンテナ・イメージ 4

50

01Aとしてシステム・メモリ414にロードされると、復号されたコンテナ・イメージ401A内のコードおよびデータは、もはや効果的に保護されなくなる可能性がある。開発者が暗号化されたコンテナ・イメージ401内に入れるコード、データ、および構成は、よく見える状態またはわずかな作業で見えるため、ホスト機械410の管理者にさらされる。実際、場合によっては、復号されたコンテナ・イメージ401Aは、ホスト機械410においてプレーンテキストとして記憶することができる。

【0054】

さらに、ホスト機械410において、様々な管理アクセス機能416のいずれかを使用して、システム・メモリ414内の復号されたコンテナ・イメージ401Aにアクセスすることができる。たとえば、システム・メモリ414内のコンテナ・メモリへの管理アクセスは、たとえばホスト機械410が信頼できるブート・シーケンスを使用してブートされない状況において、修正されたカーネルからのブーティングを介して達成することができる。システム・メモリ414内のコンテナ・メモリへの管理アクセスは、信頼できるカーネルのカーネル・モジュールに加えて、追加のカーネル・モジュールのロードを介して達成することもできる。

【0055】

場合によっては、システム・メモリ414内のコンテナ・メモリへの管理アクセスは、たとえば/dev/mem、/dev/kmem、および/proc/kcoreの仮想メモリ管理デバイスを使用して、1つまたは複数の仮想メモリ管理デバイスを介して達成することもできる。システム・メモリ414内のコンテナ・メモリへの管理アクセスは、1つまたは複数のランタイム・デバッグ機能を介して達成することもできる。ランタイム・デバッグ機能は、一般に、プロセスを別のプロセスに付属させることを可能にし、またたとえば、ルートに実行プロセスを一時停止させ、それらのメモリでピークさせることを可能にすることができる機能である。ランタイム・デバッグ機能の例は、ptraceおよび拡張Berkeley Packet Filter (eBPF)を含む。

【0056】

場合によっては、システム・メモリ414内のコンテナ・メモリへの管理アクセスは、実行プロセスに関連付けられたメモリを閲覧するために実行プロセスを一時停止することを介して達成することもできる。システム・メモリ414内のコンテナ・メモリへの管理アクセスは、カーネル・メモリ・スワップ動作を介して達成することもでき、この動作では、カーネルは、システム・メモリ内に空間を供給するために、システム・メモリ414の一部をディスクに書き込む。カーネル・メモリ・スワップは、超過データをシステム・メモリ414内にロードすることによって、意図的にトリガすることができる。

【0057】

要約すると、ホスト機械410は暗号化されたコンテナ・イメージ401をレジストリ400からセキュアに取り出すことができる一方で、暗号化されたコンテナ・イメージ401は、ホスト機械410で復号された後、不正管理者に対して脆弱であり得る。401などの、場合によって暗号化されたコンテナ・イメージは、プロプライエタリ・コードおよびアルゴリズム、患者／健康データ、機械学習 (ML) モデルなどの、多種多様な機密情報のいずれかを含むことができる。下記で考察するように、ホスト機械450は、こうした機密情報を保護するために、ホスト機械450において暗号化されたコンテナ・イメージ401のセキュリティを向上させる、セキュリティ強化機構のセットを実装する。

【0058】

いくつかの実施形態では、ホスト機械450は向上したセキュリティを提供することができる。同様のホスト機械410、ホスト機械450は、たとえば、図1に示されるクラウド・コンピューティング・ノード10の中のクラウド・コンピューティング・ノードを提供することができ、ホスト機械450は、ホスト・コンテナに装備されたサーバを備えることができる。しかしながら、ホスト機械410とは対照的に、ホスト機械450は、たとえば、図3に示されるブート構成要素370、コア・サービス構成要素371、およびランタイム復号構成要素373などの、セキュリティ機構を実装することができる。し

10

20

30

40

50

たがって、ホスト機械 450 は、暗号化されたコンテナ・イメージ 401 をレジストリ 400 からセキュアに取り出し、暗号化されたコンテナ・イメージ 401 を復号するために復号鍵を獲得し、暗号化されたコンテナ・イメージ 401 を復号および実行することができる。

【0059】

ブート構成要素 370 は、システム・メモリ 454 内で、コンテナ・メモリへの 1 つまたは複数のタイプの管理アクセスが非活動化される、定義されたセキュアな状態にホスト機械 450 をセキュアにブートするために、ホスト機械 450 で信頼できるブート・シーケンスの一部を実施するために、1 つまたは複数の動作を実行することができる。図 4B では、管理アクセス機能 416 が非活動化され、復号されたコンテナ・イメージ 401A から生じ、管理アクセス機能 416 に向かう矢印はブロックされる。実装において、カーネル・コード、カーネル構成、およびコア・サービスの改ざんを防止するために、信頼できるブートを使用することによって、ホスト機械 450 の管理者またはルート・ユーザを含むすべてのユーザから、システム・メモリ 454 を保護することができる。さらに、特権の特定セットを有する特定のユーザ（たとえば、特定のオペレーティング・システム内で、様々なコマンドおよびファイルへのデフォルト・アクセスを有することが可能な、ルート・ユーザ）が、システム・メモリ 454 内でピークできるようにする、特定のカーネル・オプションおよび仮想デバイスを、非活動化することができる。代替として、システム・メモリ 454 をセキュアにするために、セキュア・ハードウェア技術を使用することができる。

【0060】

コア・サービス構成要素 371 は、信頼できるブート・シーケンスの一部として開始可能であり、図 4B に示されたセキュア鍵獲得 452 を実装することができる。セキュア鍵獲得 452 は、ホスト機械 450 の特定のユーザが復号鍵にアクセスできるようにすることなく、暗号化されたコンテナ・イメージ 401 と共に使用するために 1 つまたは複数の復号鍵をセキュアに取得することができる。たとえば、取り出された復号鍵を、管理アクセス機能 416 から保護されているシステム・メモリ 454 内に記憶することができる。

【0061】

例示の一実施形態において、コア・サービス構成要素 371 は、TPM 324 および PCR 325 を使用して信頼できるブート・シーケンスの一部として開始することができる。復号鍵が必要な場合、コア・サービス構成要素 371 は、信頼できる第三者サービス・デバイス 345 から復号鍵を獲得するために、TPM 324 を使用して TPM リモート認証を実行することができる。TPM リモート認証が成功した場合、信頼できる第三者サービス・デバイス 345 によって 1 つまたは複数の復号鍵をセキュア鍵獲得 452 に提供することができる。取得した復号鍵は、システム・メモリ 454 内に保持することが可能であり、ブート構成要素 370 によって実装された信頼できるブート・シーケンスは、ルート・ユーザがシステム・メモリ 454 から復号鍵を獲得できないことを保証する。

【0062】

コンテナがホスト機械 450 で開始されるとき、たとえばランタイム復号構成要素 373 は、セキュア鍵獲得 452 によって獲得された復号鍵を使用して、コンテナ・イメージを復号すること、たとえば、暗号化されたコンテナ・イメージ 401 を復号することができる、それによって、復号されたコンテナ・イメージ 401A をシステム・メモリ 454 内にロードすることができる。ランタイム復号構成要素 373 は、さらに、復号されたコンテナ・イメージ 401A によってアクセスされたファイルのランタイム復号を実行することができる。

【0063】

いくつかの実施形態では、ランタイム復号構成要素 373 は、ファイル・システム仲介として少なくとも部分的に実装可能である。コンテナがホスト機械 450 で開始されるとき、ファイル・システム仲介をコンテナのルート・ファイル・システム上に置き、すべてのファイル・アクセスがファイル・システム仲介を介して進むようにすることができる。

暗号化されていないファイルの場合、ファイル・アクセスは単にファイル・システム仲介を通過することができる。暗号化されたファイルがアクセスされるとき、要求側プロセスのプロセス識別子（PID）をチェックすることができる。PIDがコンテナのエントリポイント・プロセスまたはエントリポイント・プロセスの下位プロセスに属する場合、ファイルを復号することができる。要求側プロセスのPIDがエントリポイント・プロセスまたはエントリポイント・プロセスの下位に属さない場合、復号を防止することができる。

【0064】

要約すると、図4Bに関して、ホスト機械450は、単独または組み合わせて採用可能なくつかのセキュリティ強化手段を介して、コンテナの復号されたコードおよびデータをセキュアにすることができる。ホスト機械450は、ホスト機械450カーネルが信用できることを保証するために、また、それ以外の方法でシステム・メモリ454にアクセスできるようにする、様々な管理アクセス機能416のうちのいずれかを非活動化するために、セキュア状態にブートされる。ホスト機械450は、復号鍵をセキュアに取り出し、ホスト機械450のユーザによって復号鍵にアクセスできないシステム・メモリ454内などのロケーションに記憶するために、コア・サービス構成要素371などのセキュア鍵獲得452を含むことができる。次いで、ホスト機械450は、コンテナ・ランタイム時にコンテナ・データをセキュアに復号することができる。

【0065】

図5は、本明細書で説明する1つまたは複数の実施形態に従った、コンテナをセキュアにするための修正されたドッカー技術を採用する、例示の非限定的システムのブロック図を示す。本明細書で説明する他の実施形態において採用される同様の要素を反復的に記述することは、簡潔にするために省略する。

【0066】

図5に示される実施形態は、コンテナ・ランタイム動作のための修正されたドッカー・ベース・システムおよび方法500を含む。ドッカー構成要素501は、コンテナ・エンジンを提供するドッカー・デーモンである。ドッカー署名済みコンテナ・イメージ522に含まれるコンテナを実行するために、ドッカー構成要素501は、コンテナ・デーモンを提供するコンテナd（containerd）構成要素502を呼び出すことができる。本明細書で使用する際、「コンテナd構成要素」はコンテナ・デーモン構成要素を意味する。ドッカー構成要素501は、ドッカー高度多層統一ファイル・システム（AUFS）構成要素521も開始する。いくつかの実施形態では、ドッカー署名済みコンテナ・イメージ522は、ドッカー署名済みコンテナ・イメージ522が本明細書で開示するセキュリティ強化手段の対象となることを示すために、たとえば拡張ファイル属性または特殊ファイル名を使用して、注釈付けすることができる。

【0067】

コンテナd構成要素502は、個々のコンテナ530にランタイム環境を提供する、コンテナ・シム構成要素503を開始する。rootfsがコンテナ・ストレージ・ドライバによって取り付けられた後、コンテナd構成要素502は、ブラックボックス・デーモン構成要素512へのリモート・プロシージャ・コール（RPC）を行うことができる。

【0068】

この例では、ブラックボックス・デーモン構成要素512は、図3に関連して説明した371などのコア・サービス構成要素を実装する。ブラックボックス・デーモン構成要素512は、初期に、たとえば、PCR 325においてPCR#10によってセキュアにされる、信頼できるブート・シーケンスの一部として開始することができる。起動時、ブラックボックス・デーモン構成要素512は、TPMリモート認証を実行することが可能であり、その後、ブラックボックス・デーモン構成要素512は、たとえば、封止された復号鍵のリストを、信頼できる第三者サービス・デバイス345から取り出すことができる。ブラックボックス・デーモン構成要素512は、メモリ内の取り出された復号鍵を封止解除することができる。ブラックボックス・デーモン構成要素512は、完了時にTPM_PCR_Extend PCR#10を呼び出すことができる。

10

20

30

40

50

【0069】

コンテナ・ランタイムにおいて、コンテナd構成要素502からのRPC呼び出しに
答して、またドッカー署名済みコンテナ・イメージが署名された場合、ブラックボックス
・デーモン構成要素512は、たとえばエントリポイント・プロセスを始動すること、お
よび、クリア・テキストまたはそうでなければ復号されたファイルのみを、ルート・ユー
ザ（または、オペレーティング・システム内の様々なコマンドまたはファイルへのデフォ
ルト・アクセスを備える他のユーザ）などのユーザから保護されているメモリ内に記憶し
ながら、必要に応じてコンテナ530の代わりにファイルの復号を始めることができる。

【0070】

さらに、ブラックボックス・デーモン構成要素512は、コンテナ530のための復号
鍵を用いるFUSEプロセスを開始するために、ブラックボックス・ユーザ・スペース内
ファイル・システム（FUSE）構成要素514を開始することができる。ブラックボッ
クスFUSE構成要素514は、図5の実施形態においてランタイム復号構成要素373
を提供する。ブラックボックスFUSE構成要素514は、中間ファイル・システム層と
してのドッカーAUFS構成要素521である、コンテナ530のrootfsの上に位
置する。ブラックボックスFUSE構成要素514は、要求側プロセスが、コンテナ53
0のエントリポイント・プロセス（場合によっては、initプロセスでもよい）または
コンテナ530のエントリポイント（またはinit）プロセスの下位プロセスである場
合、暗号化されたファイルを復号する。ブラックボックスFUSE構成要素514は、要
求側プロセスについての任意の暗号化されていないファイルを取り出すこともできる。

【0071】

図6は、本明細書で説明する1つまたは複数の実施形態に従った、例示の非限定的ブー
ト構成要素の概略ブロック図を示す。本明細書で説明する他の実施形態において採用され
る同様の要素を反復的に記述することは、簡潔にするために省略する。

【0072】

ブート構成要素600の態様は、機械内で具体化される、たとえば、1つまたは複数の
機械に関連付けられた1つまたは複数のコンピュータ可読媒体内で具体化される、機械実
行可能構成要素を構成することができる。こうした構成要素は、1つまたは複数の機械、
たとえばコンピュータ、コンピューティング・デバイス、仮想機械などによって実行され
る場合、記載した動作を機械に実行させることができる。一態様において、メモリ608
は、コンピュータ実行可能構成要素および命令を記憶することができる。さらにプロセッ
サ604は、ブート構成要素600に関連付けられた命令（たとえば、コンピュータ実行
可能構成要素および命令）の動作を容易にすることができる。

【0073】

図6に示されるように、いくつかの実施形態では、ブート構成要素600はプロセッサ
604、TPM 606、およびメモリ608を含むことができる。他の実施形態では、
ブート構成要素600は、別々のプロセッサ604を有する代わりに、コア・サービス構
成要素700の1つまたは複数のプロセッサ704（図7）、ランタイム復号構成要素8
00のプロセッサ804（図8）、または処理ユニット311（図3）、あるいはその組
み合わせを備えるプロセッサにアクセスするか、またはプロセッサを共有する、あるいは
その両方が可能である。したがって、図示された実施形態ではブート構成要素600はハ
ードウェアであるが、いくつかの実施形態では、ブート構成要素600はコンピュータ・
コードとして実装可能であるか、またはブート構成要素600の1つまたは複数の動作は
コンピュータ・コードを介して実装可能である。

【0074】

TPM 606は、たとえばPCR 325のうちの1つのPCR内に、定義されたセキ
ュアな状態610を含むことができる。メモリ608は、たとえば次の構成要素612、
および任意選択として、定義されたセキュアな状態610を含むことができる。非限定的
な例では、図3の要素は図6において実装される。ブート構成要素600は、コンピュ
ータ310に組み込まれたブート構成要素370の一例を提供する。同様に、プロセッサ6

10

20

30

40

50

04はプロセッサ311を提供することができ、メモリ608は、システム・メモリ312またはコンピュータ310に含まれる他のメモリを提供することができ、またTPM 606は、図3のTPM 324を提供することができる。

【0075】

特定の実装において、ブート構成要素600の下に矢印で示されるように、ブート構成要素600は、システムについての信頼できるブート・シーケンスとして示される動作のシーケンスの一部を実施するために採用可能である。ブート構成要素600は、信頼できるブート・シーケンスの少なくとも一部を実行することができ、またその後、ブート構成要素600は、次の構成要素612を信頼できるブート・シーケンスの一部として動作または実行させることができる。信頼できるブート・シーケンスの結果は、こうした動作のシーケンスが、定義されたセキュアな状態610に従って定義されたセキュアな状態にシステムをセキュアにブートできることであり、コンテナ・メモリへの1つまたは複数のタイプの管理アクセスが非活動化される。

10

【0076】

非限定的な例では、ブート構成要素600は、定義されたセキュアな状態610を次の構成要素612が満たすことを保証するために、次の構成要素612をチェックすることができる。定義されたセキュアな状態610は、コンテナ・メモリへの1つまたは複数のタイプの管理アクセスが非活動化される状態を含むことができる。すなわち、定義されたセキュアな状態610に従ってコンピュータ310が完全にブートされた後、一般に特定のシステム・セクション（たとえば、システム・メモリ）への管理アクセスを提供する特定の機能を非活動化することができる。

20

【0077】

たとえば一実施形態において、次の構成要素612はオペレーティング・システム・カーネルを備えることができる。定義されたセキュアな状態610は、特定タイプの管理メモリ・アクセスに関連付けられた管理アクセス機能が非活動化される、カーネルのハッシュを備えることができる。ブート構成要素600は、次の構成要素612またはその一部のハッシュを実行することができ、ブート構成要素600は、測定されたハッシュが定義されたセキュアな状態610に記憶されたハッシュと一致することをチェックすることができる。ブート構成要素600は、ハッシュが一致する場合、次の構成要素612をロードすること、またはハッシュが一致しない場合、信頼できるブート・シーケンスを停止することができる。

30

【0078】

TPM 606は、たとえばPCR 325のうちの1つのPCR内に、次の構成要素612のハッシュをセキュアに記憶することができる。ブート構成要素600は、次の構成要素612のハッシュを測定し、ハッシュ値をTPM 606に渡すことができる。ハッシュ値が一致するとき、TPM 606は、次の構成要素612が安全にロード可能であることをブート構成要素600に通知することができ、また、ブート構成要素600は次の構成要素612をロードすることができる。ハッシュが一致しないとき、TPM 606はブート構成要素600に通知することができ、ブート構成要素600は信頼できるブート・シーケンスを停止することができる。

40

【0079】

場合によっては、図7に関して説明したようなコア・サービス構成要素は、定義されたセキュアな状態610の少なくとも1つの態様を備えることができる。こうした場合、ブート構成要素600は、非活動化された管理アクセス機能、および、ブートされたシステムにおけるコア・サービス構成要素の存在の、両方を補償することができる。ブート構成要素600は、コア・サービス構成要素のハッシュ、オペレーティング・システム・カーネル、または任意の他の次の構成要素612、あるいはそれらの組み合わせを、実行することができる。

【0080】

定義されたセキュアな状態610を指定するための他の手法は、他の実施形態において

50

実装可能である。たとえば、定義されたセキュアな状態 610 は、次の構成要素 612 において非活動化されるべき、管理アクセス機能のリストを含むことができる。ブート構成要素 600 は、メモリ 608 から定義されたセキュアな状態 610 を読み取ることができる。ブート構成要素 600 は、リスト表示された管理アクセス機能が非活動化されることを保証するために、次の構成要素 612 を検査することができる。リスト表示された管理アクセス機能が非活動化された場合、ブート構成要素 600 は、次の構成要素 612 をロードすることができる。リスト表示された管理アクセス機能が非活動化されなかった場合、ブート構成要素 600 は、信頼できるブート・シーケンスを停止することができる。

【0081】

図 7 は、本明細書で説明する 1 つまたは複数の実施形態に従った、例示の非限定的コア・サービス構成要素の概略ブロック図を示す。本明細書で説明する他の実施形態において採用される同様の要素を反復的に記述することは、簡潔にするために省略する。

【0082】

コア・サービス構成要素 700 の態様は、機械内で具体化される、たとえば、1 つまたは複数の機械に関連付けられた 1 つまたは複数のコンピュータ可読媒体内で具体化される、機械実行可能構成要素を構成することができる。こうした構成要素は、1 つまたは複数の機械、たとえばコンピュータ、コンピューティング・デバイス、仮想機械などによって実行される場合、記載した動作を機械に実行させることができる。一態様において、メモリ 708 は、コンピュータ実行可能構成要素および命令を記憶することができる。さらにプロセッサ 704 は、コア・サービス構成要素 700 に関連付けられた命令（たとえば、コンピュータ実行可能構成要素および命令）の動作を容易にすることができる。

【0083】

図 7 に示されるように、いくつかの実施形態では、コア・サービス構成要素 700 はプロセッサ 704、TPM 706、メモリ 708、および通信構成要素 712 を含むことができる。他の実施形態では、コア・サービス構成要素 700 は、別々のプロセッサ 704 を有する代わりに、ブート構成要素 600 の 1 つまたは複数のプロセッサ 604（図 6）、ランタイム復号構成要素 800 のプロセッサ 804（図 8）、または処理ユニット 311（図 3）、あるいはその組み合わせを備えるプロセッサにアクセスするか、またはプロセッサを共有する、あるいはその両方が可能である。したがって、図示された実施形態ではコア・サービス構成要素 700 はハードウェアであるが、いくつかの実施形態では、コア・サービス構成要素 700 はコンピュータ・コードとして実装可能であるか、またはコア・サービス構成要素 700 の 1 つまたは複数の動作はコンピュータ・コードを介して実装可能である。

【0084】

TPM 706 は、封止機密 710 を含むことができる。メモリ 708 は、たとえば復号鍵 720 を含むことができる。コア・サービス構成要素 700 は、任意選択として、ブート構成要素 600 を参照しながら上記で説明した信頼できるブート・シーケンスの一部として開始することができる。コア・サービス構成要素 700 は、コンテナ・メモリと共に使用するために、1 つまたは複数の復号鍵 720 をセキュアに取得することができる。非限定的な例では、図 3 の要素は図 7 において実装される。コア・サービス構成要素 700 は、図 3 のコア・サービス構成要素 371 の一実施形態の一例である。

【0085】

いくつかの例において、コア・サービス構成要素 700 は、コンピュータ 310 の起動時に、コンピュータ 310 においてホストされる複数のコンテナと共に使用するために、復号鍵 720 のパッケージを含むことができる。コア・サービス構成要素 700 は、たとえば、コンピュータ 310 に記憶された複数のコンテナ・イメージを識別することができ、コア・サービス構成要素 700 は、信頼できる第三者サービス・デバイス 345 に対する TPM 706 リモート認証を実行するために、通信構成要素 712 および TPM 706 を採用することができる。TPM 706 は、たとえば、信頼できる第三者サービス・デバイス 345 に対して封止機密 710 を提供することができる。信頼できる第三者サー

ビス・デバイス 345 は、封止機密 710 を使用してコンピュータ 310 を認証することができる。信頼できる第三者サービス・デバイス 345 は、次に、たとえば、要求された復号鍵の束をコア・サービス構成要素 700 に戻すことができる。コア・サービス構成要素 700 は、戻された復号鍵を復号鍵 720 としてメモリ 708 内に記憶することができる。その後、復号鍵は、適宜、対応するコンテナについての復号コンテナ・データに関連して使用することができる。

【0086】

いくつかの例において、コア・サービス構成要素 700 は、コンテナ・ランタイム時に個別のコンテナについて復号鍵 720 を取得することができる。コア・サービス構成要素 700 は、本明細書で説明するように、コンテナがコンピュータ 310 でロードされると、信頼できる第三者サービス・デバイス 345 に対する TPM 706 リモート認証を実行するために、通信構成要素 712 および TPM 706 を採用することができる。信頼できる第三者サービス・デバイス 345 はその後、たとえば要求された復号鍵をコア・サービス構成要素 700 に戻すことができる。コア・サービス構成要素 700 は、戻された復号鍵を、復号鍵 720 のうちの 1 つの復号鍵としてメモリ 708 内に記憶することができる。復号鍵はその後、復号コンテナ・データに関連して使用することができる。復号鍵 720 はメモリ 708 内にロードされ、メモリ 708 はブート構成要素 600 によって管理者の閲覧から保護されるため、復号鍵 720 は依然としてセキュアなままであり、許可なしにコンテナ・データを復号するためにアクセスすることは不可能である。

【0087】

図 8 は、本明細書で説明する 1 つまたは複数の実施形態に従った、例示の非限定的ランタイム復号構成要素の概略ブロック図を示す。本明細書で説明する他の実施形態において採用される同様の要素を反復的に記述することは、簡潔にするために省略する。

【0088】

ランタイム復号構成要素 800 の態様は、機械内で具体化される、たとえば、1 つまたは複数の機械に関連付けられた 1 つまたは複数のコンピュータ可読媒体内で具体化される、機械実行可能構成要素を構成することができる。こうした構成要素は、1 つまたは複数の機械、たとえばコンピュータ、コンピューティング・デバイス、仮想機械などによって実行される場合、記載した動作を機械に実行させることができる。一態様において、メモリ 808 は、コンピュータ実行可能構成要素および命令を記憶することができる。さらにプロセッサ 804 は、ランタイム復号構成要素 800 に関連付けられた命令（たとえば、コンピュータ実行可能構成要素および命令）の動作を容易にすることができる。

【0089】

図 8 に示されるように、ランタイム復号構成要素 800 は、プロセッサ 804、PID チェック構成要素 802、およびメモリ 808 を含むことができる。図 8 に示されるように、いくつかの実施形態では、ランタイム復号構成要素 800 は、プロセッサ 804、PID チェック構成要素 802、およびメモリ 808 を含むことができる。したがって、図示された実施形態では、ランタイム復号構成要素 800 はハードウェアであるが、いくつかの実施形態では、ランタイム復号構成要素 800 はコンピュータ・コードとして実装可能であるか、またはランタイム復号構成要素 800 の 1 つまたは複数の動作はコンピュータ・コードを介して実装可能である。他の実施形態では、ランタイム復号構成要素 800 は、別々のプロセッサ 804 を有する代わりに、ブート構成要素 600 の 1 つまたは複数のプロセッサ 604（図 6）、コア・サービス構成要素のプロセッサ 704（図 7）、または処理ユニット 311（図 3）、あるいはその組み合わせを備えるプロセッサにアクセスするか、またはプロセッサを共有する、あるいはその両方が可能である。

【0090】

メモリ 808 は、たとえば復号鍵 820 を含むことができる。ランタイム復号構成要素 800 は、システム・メモリ 312 内のコンテナ・メモリに関連付けられたコンテナ 374 によってアクセスされる 1 つまたは複数のファイルのランタイム復号を実行するために、復号鍵 820、たとえばコア・サービス構成要素 700 によって取り出された復号鍵を

使用することができる。非限定的な例では、図3の要素は図8において実装される。ランタイム復号構成要素800は、コンピュータ310に組み込まれたランタイム復号構成要素373の一例を提供することができる。同様に、プロセッサ804はプロセッサ311を提供することができ、メモリ808は、システム・メモリ312またはコンピュータ310に含まれる他のメモリを提供することができる。

【0091】

いくつかの例において、ランタイム復号構成要素800は、コンテナ374からファイル要求を受け取ることができる。ファイル要求は、たとえば暗号化されたファイル要求831および暗号化されていないファイル要求835を含むことができる。暗号化されたファイル要求831は暗号化されたファイルの要求であり、暗号化されていないファイル要求835は暗号化されていないファイルの要求である。ランタイム復号構成要素800は、要求831、835を異なって扱うことができるが、ランタイム復号構成要素800は、最終的に、要求されたファイルを、たとえば暗号化されたファイル要求831に対応するリターン832として、および、暗号化されていないファイル要求835に対応するリターン836として、戻すことが可能である。

【0092】

暗号化されたファイル要求831の場合、ランタイム復号構成要素800は、要求側プロセスのプロセス識別子(PID)をチェックするために、PIDチェック構成要素802を採用することができる。PIDチェック構成要素802は、要求側プロセスのPIDがコンテナ374のエントリポイント・プロセス、またはエントリポイント・プロセスの下位プロセスに属することを保証することができる。PIDがエントリポイント・プロセスまたは下位に属する場合、ランタイム復号構成要素800は、要求されたファイルをファイル・システム850から取り出し、復号鍵820を使用して要求されたファイルを復号し、要求されたファイルをリターン832するように進行することができる。PIDが許可されない場合、ランタイム復号構成要素800は、エラーを投げることができる。

【0093】

暗号化されていないファイル要求835の場合、一実装において、ランタイム復号構成要素800は、要求835をファイル・システム850へパス・スルーする。ファイル・システム850は、要求された暗号化されていないファイルをランタイム復号構成要素800に戻すことができ、ランタイム復号構成要素800は、要求されたファイルをリターン836で要求側コンテナに戻すことができる。

【0094】

図6、図7、および図8は別々の構成要素、すなわちブート構成要素600、コア・サービス構成要素700、およびランタイム復号構成要素800をそれぞれ示すが、2つまたはそれ以上の構成要素が共通の構成要素内で実装可能であることを理解されよう。さらに、ブート構成要素600、コア・サービス構成要素700、およびランタイム復号構成要素800の設計は、コンテナ・セキュリティの強化を容易にするために、他の構成要素選択肢、構成要素配置などを含むことができることを理解されよう。さらに、前述のシステムまたはデバイスあるいはその両方は、いくつかの構成要素間の対話に関して説明してきた。こうしたシステムおよび構成要素は、それらの構成要素またはそこで指定された下位構成要素、指定された構成要素または下位構成要素のうちのいくつか、または追加の構成要素、あるいはそれらの組み合わせを含むことができることを理解されたい。下位構成要素は、親構成要素内に含まれるのではなく、他の構成要素に通信可能に結合された構成要素として実装することも可能である。さらに、1つまたは複数の構成要素または下位構成要素あるいはその両方は、集合的な機能性を提供する単一の構成要素に組み合わせることもできる。構成要素は、簡潔にするために本明細書では特に記述されていないが、当業者に知られている、1つまたは複数の他の構成要素と対話することも可能である。

【0095】

図9は、本明細書で説明する1つまたは複数の実施形態に従った、コンテナをホストするシステムのセキュリティ強化を容易にする、例示の非限定的コンピュータ実装方法90

0のフロー図を示す。図9の方法は、図3に示されたコンピュータ310を参照しながら説明する。図9のコンピュータ実装方法は、コンピュータ310などのコンテナ・サーバにおけるコンテナ374のインスタンス化およびランタイム中に、コンテナ・メモリへの1つまたは複数のタイプの管理アクセスから、コンテナ374に関連付けられたデータをセキュアにすることによって、コンピュータ310などのコンテナ・サーバにおいて、374などのコンテナのセキュリティを強化する。

【0096】

902において、プロセッサ311に動作可能に結合されたブート構成要素370は、コンテナ・メモリ（システム・メモリ312のコンテナ・メモリ部分）への1つまたは複数のタイプの管理アクセスが非活動化される、定義されたセキュアな状態にコンピュータ310をセキュアにブートするために、信頼できるブート・シーケンスの少なくとも一部を実行する。非活動化されたコンテナ・メモリへの例示のタイプの管理アクセスは、信頼できるブート・シーケンスに関連付けられた信頼できるカーネルに関して修正される、修正されたカーネルからのブーティングを介したコンテナ・メモリへの管理アクセスと、信頼できるカーネルのカーネル・モジュールに加えて、追加のカーネル・モジュールのロードを介したコンテナ・メモリへの管理アクセスと、1つまたは複数の仮想メモリ管理デバイスを介したコンテナ・メモリへの管理アクセスと、1つまたは複数のランタイム・デバッグ機能を介したコンテナ・メモリへの管理アクセスと、実行プロセスに関連付けられたメモリを閲覧するために実行プロセスを一時停止することを介したコンテナ・メモリへの管理アクセスと、カーネル・メモリ・スワップ動作を介したコンテナ・メモリへの管理アクセスと、を含むが、限定されない。一実装において、信頼できるブート・シーケンスは、コア・サービス構成要素371に記憶されるかまたはコア・サービス構成要素371によってアクセス可能な、コンピュータ・コード上でハッシュを実行すること、および、PCR 325のうちの1つのPCR内に、結果として生じるコア・サービス構成要素371のハッシュ値を記憶することを、含むことができる。

【0097】

904において、ブート構成要素370は、プロセッサ311に動作可能に結合されたコア・サービス構成要素371を、信頼できるブート・シーケンスの一部として開始する。906において、一実装において、コア・サービス構成要素371は、システム・メモリ312のコンテナ・メモリ部分と共に使用するために1つまたは複数の復号鍵をセキュアに取得する。一実装において、1つまたは複数の復号鍵をセキュアに取得することは、信頼できる第三者サービス・デバイス345に対するTPM 324リモート認証を採用することができる。

【0098】

908において、たとえばランタイム復号構成要素373によって、コンテナ374によって要求されたファイルは暗号化されているかどうかが決定される。暗号化されている場合、910において、ランタイム復号構成要素373は、プロセス識別子（PID）がコンテナ374のエントリポイント・プロセスまたはエントリポイント・プロセスの下位プロセスに属することを保証するために、暗号化されたファイルを要求する1つまたは複数のプロセスのPIDをチェックすることができる。912において、ランタイム復号構成要素373は、コンテナ374によってアクセスされる1つまたは複数のファイルのランタイム復号を実行するために、コア・サービス構成要素371によって取得された1つまたは複数の復号鍵を使用することができ、コンテナ374は、システム・メモリ312のコンテナ・メモリ部分に関連付けられる。いくつかの例において、ランタイム復号構成要素373は、初期に、コンテナ374をインスタンス化するために暗号化されたコンテナ・イメージを復号するために、1つまたは複数の復号鍵を採用することができる。

【0099】

904における、ランタイム復号構成要素373による、コンテナ374によって要求されたファイルが暗号化されていないという決定に応答して、ランタイム復号構成要素373は、914において、暗号化されていないファイルに対する1つまたは複数の要求を

パス・スルーすることができる。

【0100】

図10は、本明細書で説明する1つまたは複数の実施形態に従った、コンテナをホストするシステムのセキュリティ強化を容易にする、別の例示の非限定的コンピュータ実装方法1000のフロー図を示す。図10の方法は、図5に示されるドッカー・ベースの実施形態を参照しながら説明する。1002において、プロセッサ（図5には図示せず）に動作可能に結合されたドッカー構成要素501は、コンテナ530などの1つまたは複数のコンテナをインスタンス化することができる。一実装において、ドッカー構成要素501による1つまたは複数のコンテナ530のインスタンス化は、プロセッサに動作可能に結合された少なくとも1つの第1のコンテナ・デーモン構成要素502をインスタンス化すること、第1のコンテナ・デーモン構成要素502によって、ブラックボックスFUSE構成要素514などのランタイム復号構成要素をインスタンス化すること、および、ブラックボックスFUSE構成要素514によって、1つまたは複数のコンテナ530のうちの少なくとも1つをインスタンス化することを、含むことができる。場合によっては、ブラックボックス・デーモン構成要素512は、コンテナ530をインスタンス化することができる。

10

【0101】

1004において、1つまたは複数のコンテナ530のうちの少なくとも1つについて、ブラックボックスFUSE構成要素514などのランタイム復号構成要素は、1つまたは複数のコンテナ530のうちの少なくとも1つによる1つまたは複数のファイル・アクセスを管理することができる。1008において、ブラックボックスFUSE構成要素514は、要求されたファイルは暗号化されているかどうかを決定することができる。要求されたファイルが暗号化されている場合、ブラックボックスFUSE構成要素514は、1010において、プロセス識別子（PID）がコンテナ530のエントリポイント・プロセスまたはエントリポイント・プロセスの下位プロセスに属することを保証するために、暗号化されたファイルへのアクセスを要求する1つまたは複数のプロセスのPIDをチェックすることが可能な、ファイル・システム仲介を備える。PIDが許可されている場合、1012において、ブラックボックスFUSE構成要素514は、要求されたファイルを取り出し、復号し、戻すことができる。たとえば、図5を参照しながら説明したように、ブラックボックス・デーモン構成要素512は、コンテナ530のための復号鍵を用いるFUSEプロセスを開始するために、ブラックボックス・ユーザ・スペース内ファイル・システム（FUSE）構成要素514を開始することができる。ブラックボックスFUSE構成要素514は、図5の実施形態において、ランタイム復号構成要素373を提供する。ブラックボックスFUSE構成要素514は、中間ファイル・システム層としてのドッカーAUF S構成要素521である、コンテナ530のroot fsの上に位置する。ブラックボックスFUSE構成要素514は、要求側プロセスが、コンテナ530のエントリポイント・プロセス（場合によっては、initプロセスでもよい）またはコンテナ530のエントリポイント（またはinit）プロセスの下位プロセスである場合、暗号化されたファイルを復号する。

20

30

【0102】

ブラックボックスFUSE構成要素514は、要求側プロセスについての任意の暗号化されていないファイルを取り出すこともできる。要求されたファイルが暗号化されていない場合、1014において、ブラックボックスFUSE構成要素514は、暗号化されていないファイルにアクセスするための1つまたは複数の要求をドッカーAUF S構成要素521へパス・スルーすることができる。

40

【0103】

図11は、本明細書で説明する1つまたは複数の実施形態に従った、コンテナをホストするシステムのセキュリティ強化を容易にする、別の例示の非限定的コンピュータ実装方法1100のフロー図を示す。図11の方法は図3を参照しながら説明する。

【0104】

50

1102において、プロセッサ311に動作可能に結合されたブート構成要素370は、コンピュータ310をセキュアにブートするために、信頼できるブート・シーケンスの少なくとも一部を実行することができる。信頼できるブート・シーケンスは、たとえば、1104において、1つまたは複数のPCR 325をリセットすること、および1106において、一連のブート構成要素を実行することを含むことができ、一連のうちの各ブート構成要素は、一連のうちの次のブート構成要素において記憶されているか、またはこれによってアクセス可能な、コンピュータ・コードのハッシュを実行し、また、対応するPCRハッシュ値を記憶するか、または記憶されたPCRハッシュ値と次のブート構成要素のハッシュ値とを比較するためにTPM 324を使用するか、あるいはその両方を行う。信頼できるブート・シーケンスは、システム・メモリ312のコンテナ・メモリ部分への1つまたは複数のタイプの管理アクセスが非活動化される定義されたセキュアな状態に、コンピュータ310をセキュアにブートする。本明細書で説明するように、一連のブート構成要素のうちの少なくとも1つのブート構成要素は、コア・サービス構成要素371を備えることができるか、またはコア・サービス構成要素371は、信頼できるブート・シーケンスの終わりにロードされる信頼できるカーネルに含めることができる。

【0105】

1108において、プロセッサ311に動作可能に結合されたコア・サービス構成要素371は、信頼できる第三者サービス・デバイス345に対するTPM 324リモート認証を実行することができる。1110において、コア・サービス構成要素371は、信頼できる第三者サービス・デバイス345からコンテナ374についての1つまたは複数の復号鍵をセキュアに取得することができ、また、コア・サービス構成要素371は、コンテナ374に関連付けられたコンテナ・メモリ内にコンテナ374についての1つまたは複数の復号鍵を記憶することができる。

【0106】

1112において、プロセス識別子(PID)がコンテナ374のエントリポイント・プロセスまたはエントリポイント・プロセスの下位プロセスに属することを保証するために、暗号化されたファイルへのアクセスを要求する1つまたは複数のプロセスの複数のPIDをチェックすることに少なくとも部分的により、プロセッサ311に動作可能に結合されたランタイム復号構成要素373は、コンテナ374による1つまたは複数のファイル・アクセスを管理することができ、1110において取得された1つまたは複数の復号鍵は、暗号化されたファイルを復号するために使用される。

【0107】

説明を簡略化するために、コンピュータ実装方法を一連の動作として示し、説明する。主題となるイノベーションは、例示された動作または動作の順序あるいはその両方によって限定されるものではなく、たとえば、動作は、様々な順序で、または同時に、あるいはその両方で、また本明細書で提示および説明されていない他の動作と共に、実行可能であることを諒解および理解されよう。さらに、開示された主題に従ってコンピュータ実装方法を実装するために、例示された動作のすべてを必要とするわけではない。加えて、当業者であれば、コンピュータ実装方法を、代替として状態図またはイベントを介して一連の相互関係状態として表すことができることを諒解および理解されよう。加えて、下記および本明細書全体を通じて開示されるコンピュータ実装方法は、こうしたコンピュータ実装方法をコンピュータに移送および転送することを容易にするために、製品上に記憶することが可能であることを、さらに理解されたい。本明細書で使用する製品という用語は、任意のコンピュータ可読デバイスまたは記憶媒体からアクセス可能なコンピュータ・プログラムを包含するものと意図される。

【0108】

さらに、データ・パケットの構成または構成要素間の通信あるいはその両方は、電気および機械構成要素ならびに回路要素の組み合わせから確立されるため、ヒトは、主題のデータ・パケット構成、主題の処理構成要素間の通信、または割り当て構成要素、あるいはその組み合わせを、複製または実行できない。たとえばヒトは、ブート・プロセスにおい

10

20

30

40

50

て次の構成要素のハッシュを測定すること、または暗号化されたファイルを復号することなどはできない。さらにヒトは、様々なコンテナ・セキュリティ・プロセス中に生成される情報に対応するビット・シーケンスを含むことができるデータをパケット化すること、または、本明細書で説明するセキュリティ・プロセス中に生成される情報に対応するビット・シーケンスを含むことができるデータを伝送することなどはできない。

【0109】

本発明は、任意の可能な技術的詳細集積レベルでの、システム、方法、装置、またはコンピュータ・プログラム製品、あるいはその組み合わせとすることができる。コンピュータ・プログラム製品は、プロセッサに本発明の態様を実施させるための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を含むことができる。コンピュータ可読記憶媒体は、命令実行デバイスによる使用のための命令を保持および記憶することが可能な、有形デバイスとすることができる。コンピュータ可読記憶媒体は、たとえば、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、またはそれらの任意の適切な組み合わせとすることができるが、限定されない。コンピュータ可読記憶媒体のより特定の例の網羅的でないリストは、ポータブル・コンピュータ・ディスク、ハード・ディスク、ランダム・アクセス・メモリ（RAM）、読み取り専用メモリ（ROM）、消去可能プログラマブル読み取り専用メモリ（EPROM またはフラッシュ・メモリ）、静的ランダム・アクセス・メモリ（SRAM）、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・バーサタイル・ディスク（DVD）、メモリ・スティック、フロッピー（R）・ディスク、パンチ・カードまたは溝内に命令が記録された隆起構造などの機械的符号化デバイス、およびそれらの任意の適切な組み合わせも含むことができる。本明細書で使用するコンピュータ可読記憶媒体は、それ自体が、電波または他の自由に伝搬する電磁波、導波路または他の伝送媒体（たとえば、光ファイバ・ケーブルを通過する光パルス）を介して伝搬する電磁波、あるいは電線を介して伝送される電気信号などの、一時的信号として解釈されるべきではない。

【0110】

本明細書で説明す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それぞれのコンピューティング／処理デバイスへ、あるいは、外部コンピュータまたは外部記憶デバイスへ、ネットワークを介して、たとえばインターネット、ローカル・エリア・ネットワーク、ワイド・エリア・ネットワーク、またはワイヤレス・ネットワーク、あるいはその組み合わせを介して、ダウンロードすることができる。ネットワークは、銅製伝送ケーブル、光伝送ファイバ、ワイヤレス伝送、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、またはエッジ・サーバ、あるいはその組み合わせを含むことができる。各コンピューティング／処理デバイス内のネットワーク・アダプタ・カードまたはネットワーク・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、コンピュータ可読プログラム命令を、それぞれのコンピューティング／処理デバイス内のコンピュータ可読記憶媒体に記憶するために転送する。本発明の動作を実施するためのコンピュータ可読プログラム命令は、アセンブラ命令、命令セット・アーキテクチャ（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、状態設定データ、集積回路要素用構成データ、あるいは、Smalltalk、C++などのオブジェクト指向プログラミング言語、および、「C」プログラミング言語または同様のプログラミング言語など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作成された、ソース・コードまたはオブジェクト・コードのいずれか、とすることができる。コンピュータ可読プログラム命令は、完全にユーザのコンピュータ上で、部分的にユーザのコンピュータ上で、スタンドアロン・ソフトウェア・パッケージとして、部分的にユーザのコンピュータ上および部分的にリモート・コンピュータ上で、あるいは、完全にリモート・コンピュータまたはサーバ上で、実行可能である。後者のシナリオでは、リモート・コンピュータは、ローカル・エリア・ネットワーク（LAN）またはワイド・エリア・ネットワーク（WAN）を含む任

意のタイプのネットワークを介して、ユーザのコンピュータに接続可能であるか、または、外部コンピュータへの（たとえば、インターネット・サービス・プロバイダを使用するインターネットを介した）接続が可能である。いくつかの実施形態では、たとえば、プログラマブル論理回路要素、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論理アレイ（PLA）を含む、電子回路要素は、本発明の態様を実行するために、電子回路要素を個人化するためのコンピュータ可読プログラム命令の状態情報を利用することによって、コンピュータ可読プログラム命令を実行することができる。

【0111】

本発明の態様は、本発明の実施形態に従った方法、装置（システム）、およびコンピュータ・プログラム製品の、フローチャートまたはブロック図あるいはその両方を参照しながら説明している。フローチャートまたはブロック図あるいはその両方の各ブロック、および、フローチャートまたはブロック図あるいはその両方におけるブロックの組み合わせは、コンピュータ可読プログラム命令によって実装可能であることを理解されよう。これらのコンピュータ可読プログラム命令は、コンピュータまたは他のプログラマブル・データ処理装置のプロセッサを介して実行する命令が、フローチャートまたはブロック図あるいはその両方の1つまたは複数のブロックに指定される機能／動作を実装するための手段を作り出すべく、汎用コンピュータ、特定用途向けコンピュータ、または、機械を作成するための他のプログラマブル・データ処理装置の、プロセッサに提供可能である。特定の様式で機能するように、コンピュータ、プログラマブル・データ処理装置、または他のデバイス、あるいはその組み合わせに命じることが可能な、これらのコンピュータ可読プログラム命令も、内部に命令が記憶されたコンピュータ可読記憶媒体が、フローチャートまたはブロック図あるいはその両方の1つまたは複数のブロックに指定される機能／動作の態様を実装する命令を含む製品を備えるように、コンピュータ可読記憶媒体内に記憶することが可能である。コンピュータ可読プログラム命令は、コンピュータ、他のプログラマブル装置、または他のデバイス上で実行する命令が、フローチャートまたはブロック図あるいはその両方の1つまたは複数のブロックに指定される機能／動作を実装するべく、コンピュータ上、他のプログラマブル・データ処理装置上、あるいは、一連の演算動作をコンピュータ、他のプログラマブル装置、またはコンピュータ実装プロセスを作り出すための他のデバイス上で実行させるための他のデバイス上に、ロードすることも可能である。

【0112】

図面内のフローチャートおよびブロック図は、本発明の様々な実施形態に従った、システム、方法、およびコンピュータ・プログラム製品の、可能な実装のアーキテクチャ、機能性、および動作を例示する。この点で、フローチャートまたはブロック図内の各ブロックは、指定された論理機能を実装するための1つまたは複数の実行可能命令を含む、命令のモジュール、セグメント、または部分を表すことができる。いくつかの代替の実装において、ブロック内に示される機能は、図面内に示される順序以外で実行可能である。たとえば連続して示される2つのブロックは、実際には、実質的に同時に実行可能であるか、または、時にはブロックは、関連する機能性に応じて逆の順序で実行可能である。ブロック図またはフローチャートあるいはその両方の各ブロック、ならびにブロック図またはフローチャートあるいはその両方のブロックの組み合わせは、指定される機能または動作を実行するか、あるいは特定用途向けハードウェアおよびコンピュータ命令の組み合わせを実施する、特定用途向けハードウェア・ベース・システムによって実装可能であることに留意されよう。

【0113】

上記で、1つまたは複数のコンピュータ上で実行するコンピュータ・プログラム製品のコンピュータ実行可能命令との全般的な関連において、主題を説明してきたが、当業者であれば、本開示は、他のプログラム・モジュールとの組み合わせも実装可能であるか、または他のプログラム・モジュールとの組み合わせでも実装可能であることを認識されよう。一般に、プログラム・モジュールは、特定のタスクを実行する、または、特定の抽象データ型を実装する、あるいはその両方の、ルーチン、プログラム、構成要素、データ構造

などを含む。さらに当業者であれば、発明的コンピュータ実装方法は、単一プロセッサまたはマルチプロセッサのコンピュータ・システム、ミニコンピューティング・デバイス、メインフレーム・コンピュータ、ならびに、コンピュータ、ハンドヘルド・コンピューティング・デバイス（たとえば、PDA、電話）、マイクロプロセッサ・ベースまたはプログラム可能な、消費者エレクトロニクスまたは産業用エレクトロニクスなどを含む、他のコンピュータ・システム構成と共に実践可能であることを理解されよう。例示の態様は、タスクが、通信ネットワークを介してリンクされたりリモート処理デバイスによって実行される、分散コンピューティング環境で実践することもできる。しかしながら、本開示の全部ではないがいくつかの態様は、スタンドアロン・コンピュータ上で実践可能である。分散コンピューティング環境では、プログラム・モジュールはローカルおよびリモートの両方のメモリ・ストレージ・デバイス内に配置可能である。

10

【0114】

本出願で使用される場合、「構成要素」、「システム」、「プラットフォーム」、「インターフェース」などの用語は、コンピュータ関連エンティティ、あるいは、1つまたは複数の特定の機能性を備える動作機械に関連するエンティティを指す、またはこれらを含む、あるいはその両方が可能である。本明細書で開示されるエンティティは、ハードウェア、ハードウェアとソフトウェアの組み合わせ、ソフトウェア、または実行中ソフトウェアの、いずれかとすることができる。たとえば構成要素は、プロセッサ上で実行するプロセス、プロセッサ、オブジェクト、実行ファイル、実行のスレッド、プログラム、またはコンピュータ、あるいはその組み合わせとすることができるが、それらであることに限定されない。例を挙げると、サーバ上で実行するアプリケーションおよびサーバは、どちらも構成要素とすることができる。1つまたは複数の構成要素は、プロセスまたは実行のスレッドあるいはその両方に常駐可能であり、構成要素は、1つのコンピュータ上に局在すること、または、2つまたはそれ以上のコンピュータ間で分散されること、あるいはその両方が可能である。別の例では、それぞれの構成要素は、記憶された様々なデータ構造を有する様々なコンピュータ可読媒体から実行することができる。構成要素は、1つまたは複数のデータ・パケット（たとえば、ローカル・システム内、分散システム内、または信号を介した他のシステムとのインターネットなどのネットワークにわたって、あるいはその組み合わせで、別の構成要素と対話する、1つの構成要素からのデータ）を有する信号に従うなど、ローカルまたはリモートあるいはその両方のプロセスを介して通信することができる。別の例として、構成要素は、プロセッサによって実行されるソフトウェアまたはファームウェア・アプリケーションによって動作される、電気または電子回路要素によって動作される機械部分によって提供される、特定の機能性を備える装置とすることができる。こうした場合には、プロセッサは装置の内部または外部であってよく、ソフトウェアまたはファームウェア・アプリケーションのうちの少なくとも一部を実行することができる。さらに別の例として、構成要素は、機械部分なしに電子構成要素を介して特定の機能性を提供する装置とすることができ、電子構成要素は、電子構成要素の機能性を少なくとも部分的にもたらす、ソフトウェアまたはファームウェアを実行するためのプロセッサまたは他の手段を含むことができる。一態様において、構成要素は、たとえばクラウド・コンピューティング・システム内で、仮想機械を介して電子構成要素をエミュレートすることができる。

20

30

40

【0115】

加えて、「または」という用語は、排他的「または」ではなく包括的「または」を意味することが意図される。すなわち、特に指定されていない限り、またはコンテキストから明らかでない限り、「XはAまたはBを採用する」とは、自然包括的並べ替えのいずれかを意味することが意図される。すなわち、XはAを採用する、XはBを採用する、またはXはAおよびBの両方を採用する場合、「XはAまたはBを採用する」は、前述のインスタンスのいずれかの下で満たされる。さらに、本明細書および添付の図面で使用される場合、冠詞「a」および「an」は、一般に、単数形を対象とすべきであることが特に指定されていない限り、またはコンテキストから明らかでない限り、「1つまたは複数」を意

50

味するものと解釈されるべきである。本明細書で使用される場合、「例」または「例示的」あるいはその両方の用語は、例、インスタンス、または例示として働くことを意味するように利用される。疑念を避けるために、本明細書で開示される主題は、こうした例によって限定されない。加えて、本明細書で「例」または「例示的」あるいはその両方と記載される任意の態様または設計は、他の態様または設計よりも好ましいまたは有利であるものとは必ずしも解釈されず、また、当業者に知られた同等の例示的構造および技術を除外することを意味するものでもない。

【0116】

本明細書で採用される場合、「プロセッサ」という用語は、実質的に、単一コア・プロセッサ、ソフトウェア・マルチスレッド実行機能を伴う単一プロセッサ、マルチコア・プロセッサ、ソフトウェア・マルチスレッド実行機能を伴うマルチコア・プロセッサ、ハードウェア・マルチスレッド技術を伴うマルチコア・プロセッサ、並列プラットフォーム、および分散共有メモリを伴う並列プラットフォームを備えるが、限定されない、任意のコンピューティング処理ユニットまたはデバイスを指すことができる。加えて、プロセッサは、集積回路、特定用途向け集積回路（ASIC）、デジタル信号プロセッサ（DSP）、フィールド・プログラマブル・ゲート・アレイ（FPGA）、プログラマブル論理コントローラ（PLC）、結合プログラマブル論理デバイス（CPLD）、離散ゲートまたはトランジスタ論理、離散ハードウェア構成要素、または、本明細書に記載される機能を実行するように設計されたそれらの任意の組み合わせを指すことができる。さらに、プロセッサは、ユーザ機器のスペース使用率を最適化するかまたは性能を強化するための、分子および量子ドット・ベース・トランジスタ、スイッチ、およびゲートなどであるが、限定されない、ナノスケール・アーキテクチャを活用することができる。プロセッサは、コンピューティング処理ユニットの組み合わせとしても実装可能である。本開示において、「ストア」、「ストレージ」、「データ・ストア」、「データ・ストレージ」、「データベース」などの用語、および、構成要素の動作および機能性に関連する実質的に任意の他の情報記憶構成要素は、「メモリ構成要素」、「メモリ」内で具体化されたエンティティ、またはメモリを備える構成要素を指すために利用される。本明細書で説明するメモリまたはメモリ構成要素あるいはその両方は、揮発性メモリまたは不揮発性メモリのいずれかとすることができるか、または、揮発性および不揮発性の両方のメモリを含むことができることを理解されよう。例を挙げると、限定的ではないが、不揮発性メモリは、読み取り専用メモリ（ROM）、プログラマブルROM（PROM）、電気的プログラマブルROM（EPROM）、電気的消去可能ROM（EEPROM）、フラッシュ・メモリ、または不揮発性ランダム・アクセス・メモリ（RAM）（たとえば、強誘電体RAM（FeRAM））を含むことができる。揮発性メモリは、たとえば、外部キャッシュ・メモリとして作用することが可能な、RAMを含むことができる。例を挙げると、限定的ではないが、RAMは、シンクロナスRAM（SRAM）、動的RAM（DRAM）、シンクロナスDRAM（SDRAM）、ダブル・データ・レートSDRAM（DDR SDRAM）、拡張SDRAM（ESDRAM）、SynchLink DRAM（SLDRAM）、ダイレクトRambus RAM（DRRAM）、ダイレクトRambus動的RAM（DRDRAM）、およびRambus動的RAM（RDRAM）などの、多くの形で利用可能である。加えて、本明細書のシステムの開示されたメモリ構成要素またはコンピュータ実装方法は、これらおよび任意の他の適切なタイプのメモリを含むことが意図されるが、含むことに限定はされない。

【0117】

上記で説明してきた内容は、システムおよびコンピュータ実装方法の単なる例を含むものである。もちろん、本開示を説明するために、構成要素またはコンピュータ実装方法の、あらゆる考え得る組み合わせを記述することは不可能であるが、当業者であれば、本開示の多くの他の組み合わせおよび並べ替えが可能であることが理解できる。さらに、「含む」、「有する」、「所有する」、などの用語が、詳細な説明、特許請求の範囲、付属書、および図面で使用される範囲で、こうした用語は、「備える」という用語と同様に、「

10

20

30

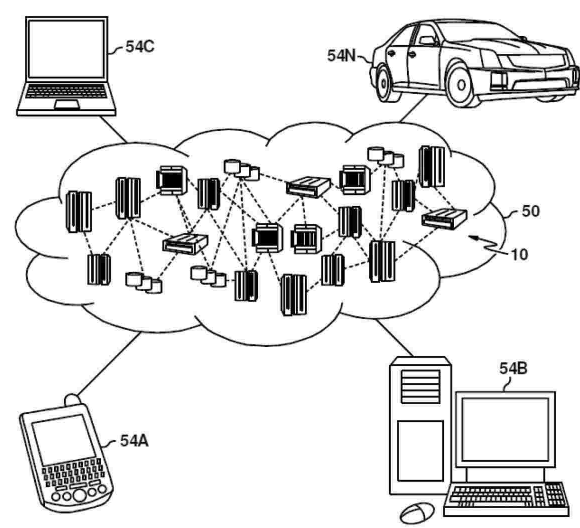
40

50

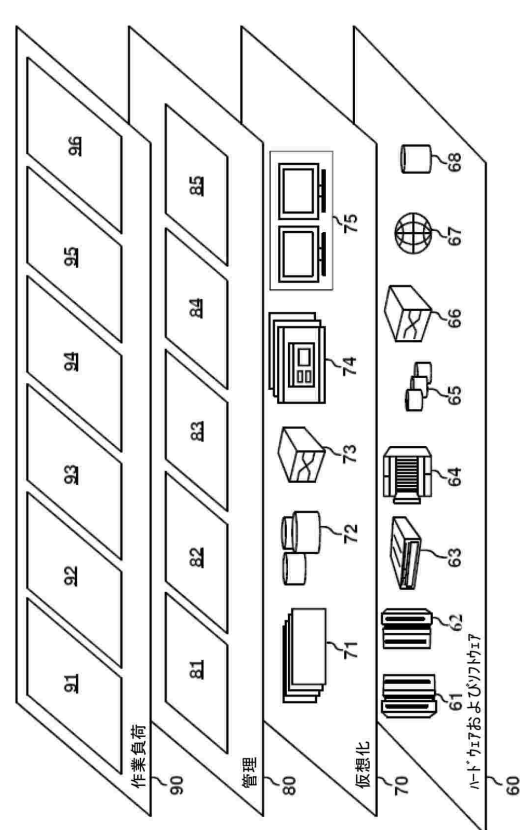
備える」が特許請求の範囲で遷移語として採用されるときに解釈されるように、包含的であることが意図される。様々な実施形態の記述は、例示の目的で提示されてきたが、網羅的であること、または開示された実施形態に限定されることは意図されない。当業者であれば、記述された実施形態の範囲を逸脱することなく、多くの修正および変形が明らかとなろう。本明細書で使用する用語は、市場に見られる技術を超える実施形態の原理、実際の適用例、または技術的改良を最もよく説明するため、または、本明細書で開示される実施形態を当業者が理解できるようにするために、選択された。

【図面】

【図 1】



【図 2】



10

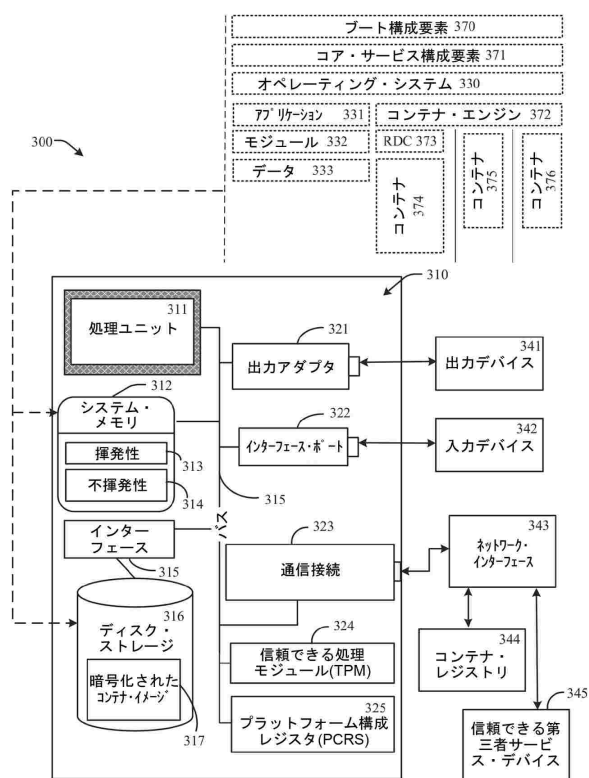
20

30

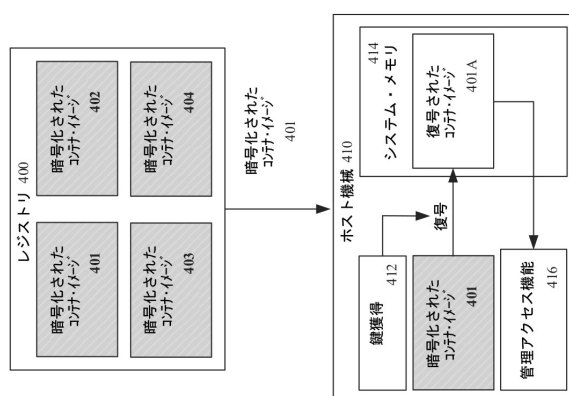
40

50

【圖 3】



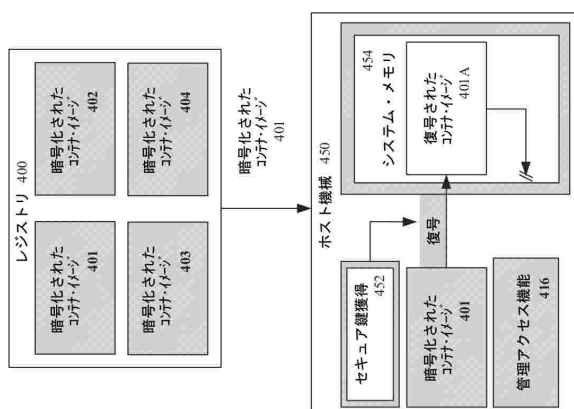
【図 4 A】



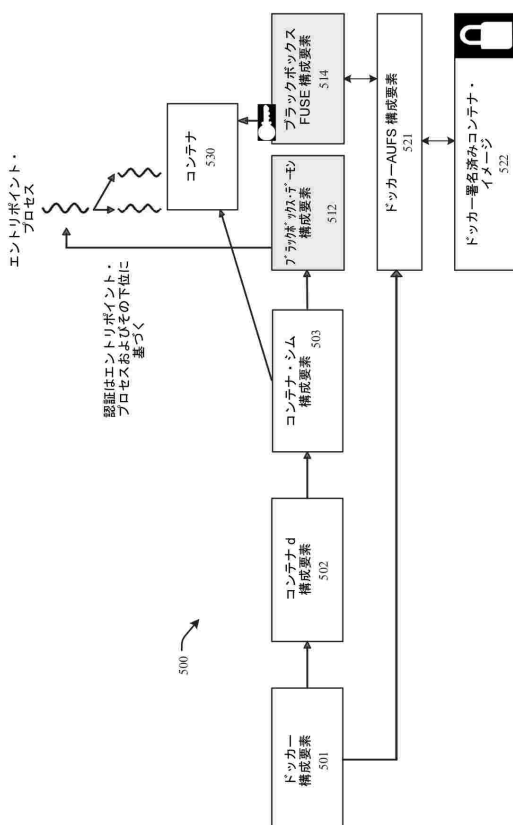
10

20

【図 4 B】



【図 5】

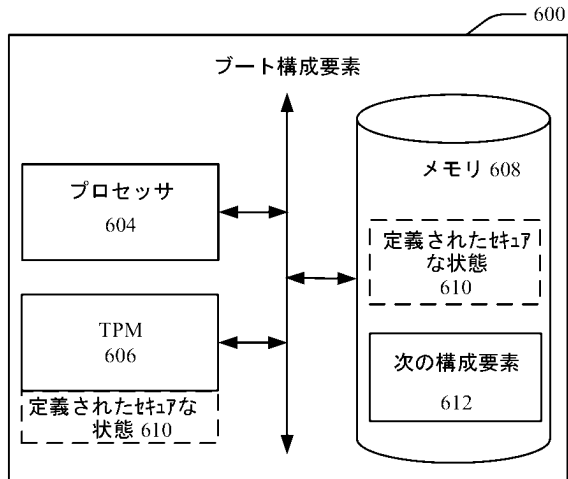


30

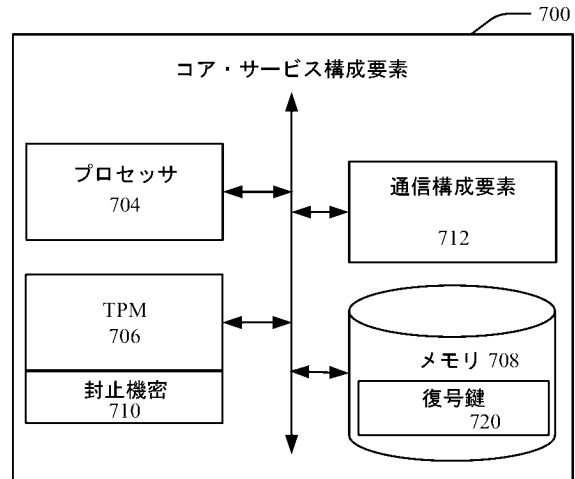
40

50

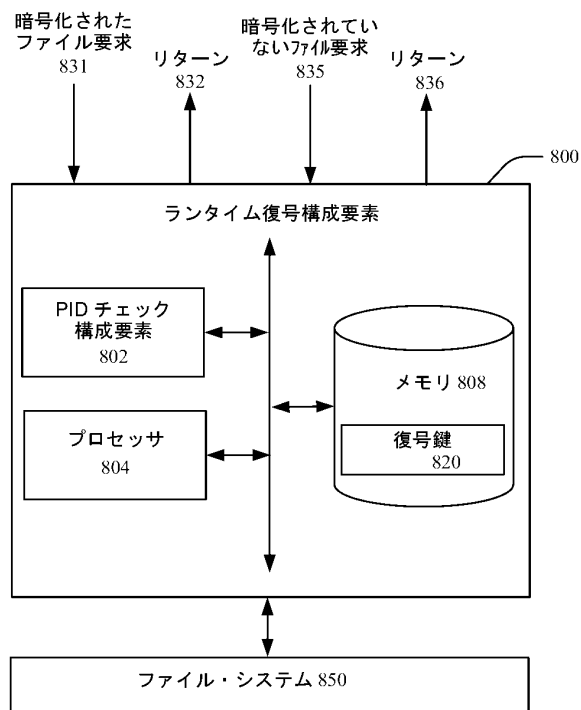
【図 6】



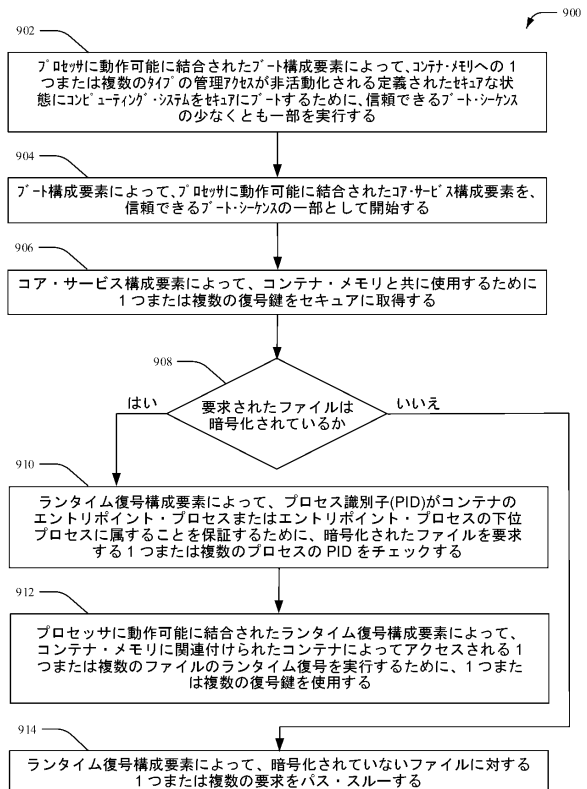
【図 7】



【図 8】



【図 9】



10

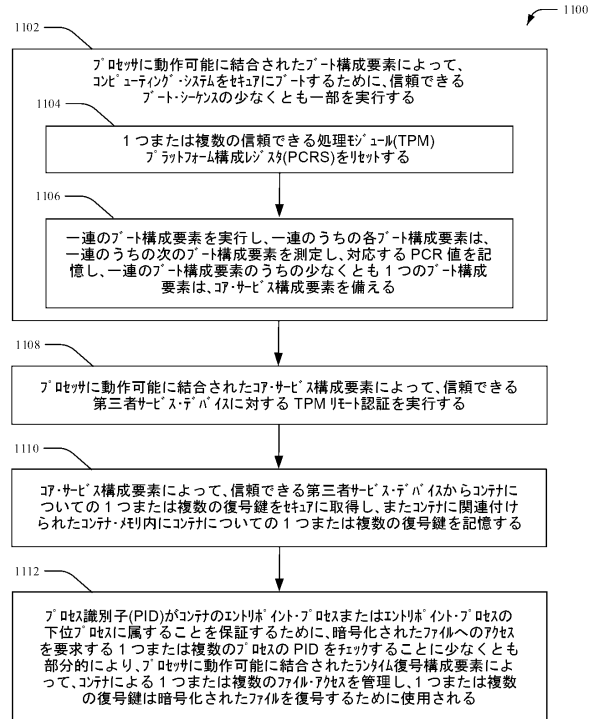
20

30

40

50

【図 11】



20

40

50

フロントページの続き

- (72)発明者

ハン、ハイ

アメリカ合衆国10598 ニューヨーク州ヨークタウン・ハイツ キッチャワン・ロード1101
- (72)発明者

ラム、ジア、ジュン、ブランドン

アメリカ合衆国10598 ニューヨーク州ヨークタウン・ハイツ キッチャワン・ロード1101
- (72)発明者

スネジャ、サヒル

アメリカ合衆国10598 ニューヨーク州ヨークタウン・ハイツ キッチャワン・ロード1101
- (72)発明者

コラー ジェミオ、リカルド、アンドレイ

アメリカ合衆国10598 ニューヨーク州ヨークタウン・ハイツ キッチャワン・ロード1101
- (72)発明者

ステインダー、マルゴザータ

アメリカ合衆国10598 ニューヨーク州ヨークタウン・ハイツ キッチャワン・ロード1101
- 審査官

上島 拓也
- (56)参考文献

特表2016-519827 (JP, A)

特開2008-226159 (JP, A)

特開2004-046307 (JP, A)
- (58)調査した分野

(Int.Cl., DB名)

G06F 21/57