

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7572169号
(P7572169)

(45)発行日 令和6年10月23日(2024.10.23)

(24)登録日 令和6年10月15日(2024.10.15)

(51)国際特許分類		F I	
H O 4 L	12/66 (2006.01)	H O 4 L	12/66
H O 4 L	12/22 (2006.01)	H O 4 L	12/22
H O 4 L	12/28 (2006.01)	H O 4 L	12/28 2 0 0 Z
H O 4 L	41/0895(2022.01)	H O 4 L	12/28 1 0 0 A
H O 4 L	41/40 (2022.01)	H O 4 L	41/0895
請求項の数 16 外国語出願 (全37頁) 最終頁に続く			
(21)出願番号	特願2020-102818(P2020-102818)	(73)特許権者	500520743
(22)出願日	令和2年6月15日(2020.6.15)		ザ・ボーイング・カンパニー
(65)公開番号	特開2021-10161(P2021-10161A)		The Boeing Company
(43)公開日	令和3年1月28日(2021.1.28)		アメリカ合衆国、2 2 2 0 2 ヴァージニア州、アーリントン、ロング・ブリッジ・ドライブ、9 2 9
審査請求日	令和5年6月9日(2023.6.9)	(74)代理人	110002077
(31)優先権主張番号	16/442,389		園田・小林弁理士法人
(32)優先日	令和1年6月14日(2019.6.14)	(72)発明者	グェン, ダニエル
(33)優先権主張国・地域又は機関	米国(US)		アメリカ合衆国 イリノイ 6 0 6 0 6 - 2 0 1 6, シカゴ, ノース リバーサイド プラザ 1 0 0
		(72)発明者	バングアルディア, マイケル
			アメリカ合衆国 イリノイ 6 0 6 0 6 - 2 0 1 6, シカゴ, ノース リバーサイド プラザ 1 0 0
			最終頁に続く

(54)【発明の名称】 航空機ネットワークサイバーセキュリティ装置及び方法

(57)【特許請求の範囲】

【請求項1】

航空ネットワーク（410）のマッピングを分かり難くする方法（600）であって、ネットワークモジュール（510）を、外部アクセスノード（430）と前記航空ネットワークのアビオニクスバス（412）との間に動作可能に接続すること（610）であって、前記外部アクセスノードと前記アビオニクスバスとの間の全ての通信が、前記ネットワークモジュールを通過する、ネットワークモジュール（510）を、外部アクセスノード（430）と前記航空ネットワークのアビオニクスバス（412）との間に動作可能に接続すること（610）、

前記アビオニクスバスの少なくとも第1の部分の構成要素の第1の組向けのネットワークアドレスを特定する第1のネットワークマップ（542）を生成すること（614）、前記第1のネットワークマップを前記ネットワークモジュールに読み込むこと（618）、

前記ネットワークモジュールの前記第1のネットワークマップを、前記外部アクセスノードにとってアクセス可能にすること（626）、

前記航空ネットワークの少なくとも第2の部分の構成要素の第2の組向けのネットワークアドレスを特定する少なくとも第2のネットワークマップ（546）を生成すること（614）であって、前記第2のネットワークマップが、前記第1のネットワークマップとは異なる、第2のネットワークマップ（546）を生成すること（614）、

前記第2のネットワークマップを前記ネットワークモジュールに読み込むこと（618）

）、及び

前記外部アクセスノードにとってアクセス可能な前記ネットワークマップを、前記第1のネットワークマップから前記第2のネットワークマップに変更すること（630）を含む、方法。

【請求項2】

少なくとも第1の仮想環境（540）と第2の仮想環境（544）を生成すること（612）、

前記第1のネットワークマップ（542）を前記第1の仮想環境（540）内に記憶すること（616）、及び

前記第2のネットワークマップ（546）を前記第2の仮想環境（544）内に記憶すること（616）を更に含む、

前記第1のネットワークマップを前記ネットワークモジュール（510）に読み込むこと（618）が、前記第1のネットワークマップを記憶した前記第1の仮想環境を前記ネットワークモジュールに読み込むこと（624）を含み、前記第2のネットワークマップを前記ネットワークモジュールに読み込むこと（618）が、前記第2のネットワークマップを記憶した前記第2の仮想環境を前記ネットワークモジュールに読み込むこと（624）を含む、請求項1に記載の方法（600）。

【請求項3】

前記アビオニクスバス（412）と前記外部アクセスノード（430）との間の通信を、前記第1の仮想環境（540）を通る通信に限定すること（628）を更に含む、請求項2に記載の方法（600）。

【請求項4】

前記外部アクセスノード（430）にとってアクセス可能な前記ネットワークマップを、前記第1のネットワークマップ（542）から前記第2のネットワークマップ（546）に変更すること（630）が、前記外部アクセスノードの前記第1の仮想環境（540）との通信を排除すること（632）、及び前記外部アクセスノードの前記第2の仮想環境（544）との通信を確立すること（636）を含む、請求項3に記載の方法（600）。

【請求項5】

前記外部アクセスノード（430）にとってアクセス可能な前記ネットワークマップを変更すること（630）が、少なくとも第1の所定の基準（524、526、528）を満たしたことに応答して、前記外部アクセスノードにとってアクセス可能な前記ネットワークマップを変更することを含む、請求項1から4のいずれか一項に記載の方法（600）。

【請求項6】

前記外部アクセスノード（430）にとってアクセス可能な前記ネットワークマップを変更するための前記少なくとも第1の所定の基準（524、526、528）が、前記外部アクセスノードにとってアクセス可能な前記ネットワークマップを変更するための固定された基準、又は前記外部アクセスノードにとってアクセス可能な前記ネットワークマップを変更するためのランダムな基準のうちの少なくとも一方を含む、請求項5に記載の方法（600）。

【請求項7】

請求項1から6のいずれか一項に記載の方法を実行する、航空ネットワーク（410）のマッピングを分かり難くするためのネットワークモジュール（510）であって、

前記ネットワークモジュールが、前記航空ネットワークと動作可能に接続され、

前記航空ネットワークのアビオニクスバス（412）と前記外部アクセスノード（430）との間に動作可能に配置され、前記外部アクセスノードと前記アビオニクスバスとの間の全ての通信が、前記ネットワークモジュールを通過し、

前記航空ネットワークの少なくとも第1の部分の構成要素の第1の組向けのネットワークアドレスを特定する第1のネットワークマップ（542）を生成し、

10

20

30

40

50

前記ネットワークモジュールの前記第1のネットワークマップを、前記外部アクセスノードにとってアクセス可能にし、

前記航空ネットワークの少なくとも第2の部分の構成要素の第2の組向けのネットワークアドレスを特定する第2のネットワークマップ(546)を生成することであって、前記第2のネットワークマップが、前記第1のネットワークマップとは異なる、第2のネットワークマップ(546)を生成し、

前記外部アクセスノードにとってアクセス可能な前記ネットワークマップを、前記第1のネットワークマップから前記第2のネットワークマップに変更するように構成されている、ネットワークモジュール。

【請求項8】

前記ネットワークモジュールが、
少なくとも第1の仮想環境(540)と第2の仮想環境(544)を生成し、
前記第1のネットワークマップ(542)を前記第1の仮想環境(540)内に記憶し、
前記第1の仮想環境を前記外部アクセスノード(430)にとってアクセス可能にし、
前記第2のネットワークマップ(546)を前記第2の仮想環境(544)内に記憶し、
前記外部アクセスノードにとってアクセス可能な前記仮想環境を、前記第1の仮想環境から前記第2の仮想環境に変更するように構成されている、請求項7に記載のネットワークモジュール(510)。

【請求項9】

第1の区画(556)と第2の区画(558)を備え、
前記第1の区画が、前記航空ネットワーク(410)と動作可能に接続され、且つ、前記少なくとも第1の仮想環境(540)と第2の仮想環境(544)を生成し、前記第1のネットワークマップ(542)を記憶した前記第1の仮想環境(540)を前記第2の区画に読み込み、前記アビオニクスバス(412)と前記外部アクセスノード(430)との間の通信を行わないように構成され、
前記第2の区画が、前記アビオニクスバスと前記外部アクセスノードとの間に動作可能に配置されるように構成されている、請求項8に記載のネットワークモジュール(510)。

【請求項10】

第1の区画(556)と第2の区画(558)を備え、前記第1の区画が、前記航空ネットワーク(410)と動作可能に接続され、且つ、前記第1のネットワークマップ(542)を記憶した前記第1の仮想環境(540)を前記第1の区画から前記第2の区画に読み込むように構成され、前記第2の区画が、前記アビオニクスバス(412)と前記外部アクセスノード(430)との間に動作可能に配置されるように構成され、前記ネットワークモジュールが、前記第1の区画と前記第2の区画との間のデータの流れを、前記第1の区画から前記第2の区画への単一方向のデータの流れに限定するように構成されている、請求項8に記載のネットワークモジュール(510)。

【請求項11】

前記第1の区画(556)と前記第2の区画(558)との間のデータの流れを、前記第1の区画から前記第2の区画への単一方向のデータの流れに限定するデータダイオード(518)を更に備える、請求項10に記載のネットワークモジュール(510)。

【請求項12】

請求項1から6のいずれか一項に記載の方法を実行することによって、航空機(120)の航空ネットワーク(410)のネットワークマッピングを分かり難くするためのシステムであって、

前記航空ネットワークの少なくとも第1の部分のネットワーク構成要素向けのネットワークアドレスを特定する第1のネットワークマップ(542)を含む第1のコンテナ(540)、

前記航空ネットワークの少なくとも第2の部分のネットワーク構成要素向けのネットワークアドレスを特定する第2のネットワークマップ(546)を含む第2のコンテナ(5

10

20

30

40

50

４４）であって、前記第２のネットワークマップが、前記第１のネットワークマップとは異なる、第２のコンテナ（５４４）、及び

前記航空ネットワークのアビオニクスバス（４１２）と外部アクセスノード（４３０）との間に前記第１のコンテナを配置するように構成された切り替えデバイス（５２０）であって、少なくとも第１の基準に応じて、前記外部アクセスノードにとってアクセス可能な前記ネットワークマップを、前記第１のネットワークマップから前記第２のネットワークマップに変更するために、前記第１のコンテナを前記アビオニクスバスと前記外部アクセスノードとの間に配置された前記第２のコンテナで置き替える、切り替えデバイス（５２０）を備える、システム。

【請求項１３】

前記切り替えデバイスが、動作の第１のモード（５２４）と前記第１のモードとは異なる動作の第２のモード（５２６）を有し、前記第１のモードと前記第２のモードが、セキュリティの異なるレベルを提供するように構成されている、請求項１２に記載のシステム。

【請求項１４】

前記システムが、ホストマシン（５１０）で動作し且つ前記第１のコンテナ（５４０）と前記第２のコンテナ（５４４）を実行するコンテナ管理者（５３６）を含む、請求項１２又は１３に記載のシステム。

【請求項１５】

前記ホストマシン（５１０）が、前記切り替えデバイス（５２０）を含む安全区画（５５６）、及び前記コンテナ管理者（５３６）を含む外部区画（５５８）を有する、請求項１４に記載のシステム。

【請求項１６】

各コンテナ（５４０、５４４）が、ネットワークゲートウェイとして構成されている、請求項１２から１５のいずれか一項に記載のシステム。

【発明の詳細な説明】

【技術分野】

【０００１】

本開示は、ネットワークセキュリティのためのシステム及び方法に関する。より具体的には、本開示の実施例は、サイバー攻撃の予備調査段階を妨害（中断）することに関する。

【背景技術】

【０００２】

航空機や他の輸送体の乗客のためのネットワーク接続性（例えば、インターネットアクセス）に対する需要が高まっている。乗客の接続性が向上すると、ネットワークセキュリティシステムが、悪意のあるネットワーク活動を阻止できることが益々重要になる。例えば、乗客向けに提供される外部アクセスポイントを介した予備調査を阻止するための改善されたシステム及び方法が必要とされている。

【発明の概要】

【０００３】

本開示は、コンピュータネットワークのマッピングを分かり難くすることに関連したシステム、装置、及び方法を提供する。ある実施例では、航空ネットワーク（avionic network）のマッピングを分かり難くする方法が、ネットワークモジュールを、外部アクセスノードと航空ネットワークのアビオニクスバスとの間に動作可能に接続することを含んでよく、外部アクセスノードとアビオニクスバスとの間の全ての通信は、ネットワークモジュールを通過する。該方法は、アビオニクスバスの少なくとも第１の部分の構成要素の第１の組向けのネットワークアドレスを特定する第１のネットワークマップを生成すること、第１のネットワークマップをネットワークモジュールに読み込むこと、及び第１のネットワークマップを外部アクセスノードにとってアクセス可能にすることを更に含んでよい。該方法は、航空ネットワークの少なくとも第２の部分の構成要素の第２の組の向けのネットワークアドレスを特定する少なくとも第２のネットワークマップを生成することであ

10

20

30

40

50

って、第2のネットワークマップが、第1のネットワークマップとは異なる、第2のネットワークマップを生成すること、及び第2のネットワークマップをネットワークモジュールに読み込むことを更に含んでよい。該方法は、外部アクセスノードにとってアクセス可能なネットワークマップを、第1のネットワークマップから第2のネットワークマップに変更することを更に含んでよい。

【0004】

ある実施例では、ネットワークモジュールが、航空ネットワークと動作可能に接続されてよく、航空ネットワークのアビオニクスバスと外部アクセスノードとの間に動作可能に配置されるように構成されてよく、外部アクセスノードとアビオニクスバスとの間の全ての通信は、ネットワークモジュールを通過する。該モジュールは、航空ネットワークの少なくとも第1の部分の構成要素の第1の組向けのネットワークアドレスを特定する第1のネットワークマップを生成し、第1のネットワークマップを外部アクセスノードにとってアクセス可能にするように構成されてよい。該モジュールは、航空ネットワークの少なくとも第2の部分の構成要素の第2の組向けのネットワークアドレスを特定する第2のネットワークマップを生成するように構成されてよく、第2のネットワークマップは、第1のネットワークマップとは異なる。該モジュールは、外部アクセスノードにとってアクセス可能なネットワークマップを、第1のネットワークマップから第2のネットワークマップに変更するように構成されてよい。

【0005】

ある実施例では、航空機の航空ネットワークのネットワークマッピングを分かり難くするためのシステムが、航空ネットワークの少なくとも第1の部分のネットワーク構成要素向けのネットワークアドレスを特定する第1のネットワークマップを含む第1のコンテナ、及び航空ネットワークの少なくとも第2の部分のネットワーク構成要素向けのネットワークアドレスを特定する第2のネットワークマップを含む第2のコンテナを含んでよく、第2のネットワークマップは、第1のネットワークマップとは異なる。該システムは、航空ネットワークのアビオニクスバスと外部アクセスノードとの間に第1のコンテナを配置し、少なくとも第1の基準に応じて、外部アクセスノードにとってアクセス可能なネットワークマップを第1のネットワークマップから第2のネットワークマップに変更するために、第1のコンテナをアビオニクスバスと外部アクセスノードとの間に配置された第2のコンテナで置き替えるように構成された、切り替えデバイスを更に含んでよい。

【0006】

特徴、機能、及び利点は、本開示の様々な実施例で個別に実現され得るか、又は、後述の説明及び図面を参照して更なる詳細が理解可能である、更に別の実施例において組み合わせられ得る。

【図面の簡単な説明】

【0007】

【図1】例示的な航空機の製造及び保守方法のステップを描くフローチャートである。

【図2】例示的な航空機の概略図である。

【図3】例示的なデータ処理システムの概略図である。

【図4】例示的な分散型データ処理システムの概略図である。

【図5】本開示の態様による、分かり難くするモジュールを含む例示的な航空機ネットワークシステムの概略図である。

【図6】図5の分かり難くするモジュールの概略図である。

【図7】図5の分かり難くするモジュールの動作を示す概略図である。

【図8】本教示による、コンピュータネットワークのマッピングを分かり難くする例示的な方法のステップを描くフローチャートである。

【発明を実施するための形態】

【0008】

コンピュータネットワークのマッピングを分かり難くする方法ならびに関連する装置の実施例が、以下で説明され、関連付けられた図面で示される。特段の定めがない限り、本

10

20

30

40

50

教示によるネットワークモジュール及び／又はその様々な構成要素は、本明細書で説明され、例示され、且つ／又は組み込まれた、構造、構成要素、機能、及び／又は変形例のうちの少なくとも1つを包含し得るが、それらを含有することが必要というわけではない。更に、特に除外されない限り、本教示に関連して本明細書で説明され、例示され、且つ／又は組み込まれているプロセスステップ、構造、構成要素、機能、及び／又は変形例は、他の類似のデバイス及び方法に含まれ得るが、開示される実施例の間で相互交換可能であることを含む。様々な実施例における下記の説明は、本質的に単なる例示であり、本開示、その用途、又は利用を限定することを意図するものではない。加えて、以下で説明される実施例によって提供される利点は、本質的に例示的であり、全ての実施例が、同じ利点又は同程度の利点を提供するわけではない。

10

【0009】

この詳細な説明は、直後に続く以下のセクションを含む。すなわち、(1) 概観、(2) 実施例、構成要素、及び代替例、(3) 例示的な組み合わせ及び更なる実施例、(4) 利点、特徴、及び便益、並びに(5) 結論である。実施例、構成要素、及び代替例のセクションは、AからEまでのサブセクションに更に分割される。それらのそれぞれは、それに従って符号が付けられている。

【0010】

概要

一般的に、コンピュータネットワークのマッピングを分かり難くする方法は、外部アクセスポイントとコンピュータネットワークの残りの部分との間にネットワークモジュールを動作可能に配置することを含む。ネットワークは、航空機、船舶若しくは他の船、列車、地下鉄、バス、自動車、及び／又はトラックに含まれ得るものなどの、適切なデータ処理システムを使用して乗客によってアクセス可能なネットワークを有する乗客輸送体に関連付けられてよい。例えば、輸送体は、乗客が、彼らのパーソナルデバイス（乗客デバイスとも呼ばれる）を使用してネットワークにアクセスすることを可能にするように構成された、ネットワークシステムを有する航空機であってよい乗客は、輸送体ネットワークに接続された乗客デバイスを使用して、例えば、機内娯楽システム、インターネットなどの外部ネットワーク、及び／又は輸送体ネットワークを介してアクセス可能な任意の他の適切なシステムと通信することができる。

20

【0011】

輸送体ネットワークアクセスは、乗客の利便性及び／又は楽しさを高めることができる。しかし、乗客が、輸送体ネットワークに接続されたデバイスを使用して、乗客には立ち入り禁止の輸送体ネットワークシステムの一部にアクセスすることを試みることがある。例えば、乗客は、乗客の使用向けに提供されたネットワークアクセスデバイスを介して、輸送体ネットワークの乗客ベースの部分に彼らのデバイスを接続することができ、次いで、乗客がアクセスすることを許可されていない制限されたネットワークシステムと通信することを試み得る。

30

【0012】

乗客又は他の当事者による輸送体ネットワークの制限されたシステムへの許可されていない侵入は、典型的には、ネットワークマッピングの特定、ポートスキャニング、及び／又は他のネットワーク情報の収集などの活動を含む、予備調査段階で開始され得る。ほとんどのネットワークセキュリティは、静的であり、防御の正確な評価が可能である。ネットワークモジュールは、乗客にとってアクセス可能なネットワークマッピングをマスキング及び変更することによって、この予備調査段階を中断するように構成され、それによって、侵入又は攻撃を未然に防ぐ。

40

【0013】

ネットワークモジュールは、外部アクセスポイントと輸送体ネットワークの残りの部分との間のゲートウェイ又はプロキシなどのインターフェースとして作用し、外部アクセスポイントに接続された全てのデバイスに人工ネットワークマッピングを提示するように構成されている。ネットワークモジュールは、予め選択された1以上の基準に従って、提示

50

される人工ネットワークマッピングを変更するように更に構成されている。例えば、ネットワークモジュールは、選択されたネットワーク条件若しくはモニタされたネットワーク活動、及び／又は任意の所望の基準に応じて、提示される人工ネットワークマッピングを、規則的な時間間隔において、ランダムな時間間隔において、輸送体の選択された地理的位置において変更することができる。

【0014】

該基準は、輸送体ネットワークの管理者などのネットワークモジュールのユーザによって選択されてよい。該基準は、ネットワークモジュールが設置されたとき、通常のネットワーク整備中など、及び／又はネットワークのセキュリティへの変更の部分として、他のネットワーク動作の部分として選択されてよい。該基準は、追加的に又は代替的に、航空機の予備飛行チェックリスト、列車が新しい経路に割り当てられたとき、又は通常の輸送体整備中などに、他の輸送体動作の部分として選択されてよい。該基準は、追加的に又は代替的に、新しいネットワーク侵入技法の登場、輸送体の乗客によるネットワーク侵入の試みの増加、及び／又は高度に繊細なシステムの輸送体ネットワークへの追加などの、セキュリティ情報又は懸念に応じて選択されてよい。

【0015】

コンピュータネットワークの制限されたシステムへの許可されていないアクセスを阻止するための技術的な解決策が、本明細書で開示される。具体的には、本開示のシステム／方法が、コンピュータ技術に関連し、コンピュータネットワークの領域で生じる技術的な問題、すなわち、許可されていないユーザが正確なネットワークマッピングを蓄積することを防ぐ技術的な問題に対処する。本明細書で開示されるシステム及び方法は、実際の静的なネットワークマッピングをマスキングし、ネットワークアクセスデバイスのユーザに人工動的ネットワークマッピングを提示することによって、この技術的な問題を解決する。したがって、本開示のシステム及び方法は、コンピュータでそれを実行する要件と共に、幾つかの既知の慣行の性能を列挙するだけではない。むしろ、それらは、ネットワークの領域内で特に生じる問題を克服するために、コンピュータ技術に根ざした解決策を必ず提供する。

【0016】

ネットワークマッピングを分かり難くする方法及び／又は分かり難くするモジュールの態様は、コンピュータ方法、コンピュータシステム、又はコンピュータプログラム製品として具現化され得る。したがって、分かり難くする方法又はモジュールの態様は、専らハードウェアの実施例、専らソフトウェアの実施例（ファームウェア、常駐ソフトウェア、マイクロコードなどを含む）、又はソフトウェア及びハードウェアの態様を組み合わせる実施例の形態を採り得るが、本明細書ではそれらは全て一般的に、「回路」、「モジュール」、又は「システム」と称され得る。更に、分かり難くする方法又はモジュールの態様は、コンピュータ可読プログラムコード／指示命令を具現化する1以上のコンピュータ可読媒体において具現化される、コンピュータプログラム製品の形態を採り得る。

【0017】

コンピュータ可読媒体の任意の組み合わせが利用され得る。コンピュータ可読媒体は、コンピュータ可読信号媒体及び／又はコンピュータ可読記憶媒体であり得る。コンピュータ可読記憶媒体は、電子的、磁氣的、光学の、電磁的、赤外線の、及び／又は半導体の、システム、装置、又はデバイス、或いは、それらの任意の好適な組み合わせを含み得る。コンピュータ可読記憶媒体のより具体的な実施例は、1以上の電線を有する電気接続、持ち運び可能な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）、読み出し専用メモリ（ROM）、消去可能プログラマブル読み出し専用メモリ（EPROM又はフラッシュメモリ）、光ファイバ、持ち運び可能なコンパクトディスク読み出し専用メモリ（CD-ROM）、光記憶デバイス、磁気記憶デバイス、及び／又は、それらの任意の好適な組み合わせなどを含み得る。この開示の文脈において、コンピュータ可読記憶媒体は、指示命令を実行するシステム、装置、又はデバイスによって使用するための又はそれらと接続しているプログラムを、包含又は記憶することが可能な、任意の適切な非一過性の

10

20

30

40

50

有形媒体を含み得る。

【0018】

コンピュータ可読信号媒体は、例えば、ベースバンドにおいて又は搬送波の部分として、コンピュータ可読プログラムコードが具現化された伝播データ信号を含んでもよい。このような伝播信号は、電磁的形態、光学的形態、及び／又はそれらの任意の好適な組み合わせを含むがそれらに限定されない、多種多様な形態のうちの任意の形態をとり得る。コンピュータ可読信号媒体は、指示命令を実行するシステム、装置、又はデバイスによって使用するための、又はそれらと接続しているプログラムを、通信、伝播、又は伝達することが可能な、コンピュータ可読記憶媒体ではない任意のコンピュータ可読媒体を含み得る。

【0019】

コンピュータ可読媒体で具現化されたプログラムコードは、無線、有線、光ファイバケーブル、RFなど、及び／又はそれらの任意の好適な組み合わせを含むが、それらに限定されない任意の適切な媒体を使用して伝達され得る。

【0020】

ネットワークマッピングを分かり難くする方法又はモジュールの態様の動作を実行するためのコンピュータプログラムコードは、Java、Smalltalk、C++などのオブジェクト指向プログラミング言語、及びCなどの従来の手続き型のプログラミング言語を含む、プログラミング言語の1以上の組み合わせで記述できる。モバイルアプリは、前述の言語や、Objective-C、Swift、C#、HTML5などの任意の適切な言語を使用して開発できる。プログラムコードは、専ら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上で、独立型の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で且つ部分的に遠隔コンピュータで、或いは専ら遠隔コンピュータ又はサーバで実行され得る。後者のシナリオでは、遠隔コンピュータが、ローカルエリアネットワーク（LAN）又はワイドエリアネットワーク（WAN）を含む任意の種類のネットワークを通じて、ユーザのコンピュータに接続されてよく、且つ／又は、（例えば、インターネットサービスプロバイダを使用して、インターネットを通じて）外部コンピュータへの接続が行われ得る。

【0021】

ネットワークマッピングを分かり難くする方法及びモジュールの態様は、方法、装置、システム、及び／又はコンピュータプログラム製品のフローチャートの例示及び／又はブロック図を参照して、以下で説明される。フローチャート及び／又はブロック図における各ブロック及び／又はブロックの組み合わせは、コンピュータプログラム指示命令によって実施され得る。これらのコンピュータプログラムの指示命令は、機械を作成するため、汎用コンピュータ、専用コンピュータ、又は他のプログラマブルデータ処理装置のプロセッサに供給されてもよく、その結果、コンピュータ又はその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される指示命令により、フローチャート及び／又はブロック図の（1以上の）ブロックにおいて特定される機能／作用を実施するための手段が作成される。ある実施例では、機械可読指示命令が、フィールドプログラマブルゲートアレイ（FPGA）などの、プログラマブル論理デバイスにプログラムされてよい。

【0022】

これらのコンピュータプログラム指示命令は、コンピュータ可読媒体であって、コンピュータ可読媒体に記憶された指示命令が、製造品を作製するような特定の状態で機能するよう、コンピュータ、他のプログラマブルデータ処理装置、及び／又は他のデバイスに指示し得る、コンピュータ可読媒体に記憶されることも可能であり、そのコンピュータプログラム指示命令は、フローチャート及び／又はブロック図の（1以上の）ブロック内で特定されている機能／作用を実施する指示命令を含む。

【0023】

コンピュータプログラム指示命令は、コンピュータ又は他のプログラマブル装置で実行される指示命令が、フローチャート及び／又はブロック図の（1以上の）ブロック内に特定された機能／作用を実施するためのプロセスを提供するように、デバイスで一連の動作ステップを実行してコンピュータ実装プロセスを行わせるために、コンピュータ、他のプ

10

20

30

40

50

ログラムブルデータ処理装置、及び／又は他のデバイスに読み込まれることも可能である。
【0024】

図面内の如何なるフローチャート及び／又はブロック図も、ネットワークマッピングを分かり難くする方法又はモジュールの態様による、システム、方法、及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、及び／又は動作を示すことを意図している。これに関して、各ブロックは、特定の（1以上の）論理機能を実施するための1以上の実行可能指示命令を含む、モジュール、セグメント、又はコードの部分を表わし得る。幾つかの実装では、ブロックに記載された機能が、図中に記載された順序から逸脱して現われることがある。例えば、関連する機能性に応じて、連続して示された2つのブロックが実際にはほぼ同時に実行されること、又は、それらのブロックが時には逆順で実行されることがある。各ブロック及び／又はブロックの組み合わせは、特定の機能又は作用を実施する、特殊用途ハードウェアに基づくシステム（又は、特殊用途のハードウェアとコンピュータ命令との組み合わせ）によって実装され得る。

10

【0025】

実施例、構成要素、及び代替手段

以下のセクションは、コンピュータネットワークのマッピングを分かり難くする例示的な方法ならびに関連するシステム及び／又は装置の選択された態様を説明する。これらのセクションの実施例は、例示を目的としており、本開示の範囲全体を限定するものと解釈すべきではない。各セクションは、1以上の個々の発明、並びに／又は、文脈から得られる若しくは関連する情報、機能、及び／若しくは構造を含み得る。

20

【0026】

例示的な航空機及び関連する方法

本明細書で開示される実施例は、例示的な航空機の製造及び保守方法100（図1参照）と、例示的な航空機120（図2参照）の文脈で説明され得る。方法100は、複数のプロセス、ステージ、又は段階を含む。製造前において、方法100は、航空機120の仕様及び設計段階104と、材料の調達段階106とを含み得る。製造中には、航空機120の構成要素及びサブアセンブリの製造段階108と、システムインテグレーション段階110とが行われ得る。その後、航空機120は、認可及び納品段階112を経て運航段階114に供され得る。（例えば、オペレータにより）運航される間に、航空機120は、定期的な整備及び保守116（航空機120の1以上のシステムの改造、再構成、改修なども含み得る）が予定され得る。本明細書で説明される実施例は、概して、航空機120の運航段階114中の運用上の使用に関するものであるが、それらは、方法100の他のステージで実施されてよい。

30

【0027】

方法100のプロセスのそれぞれは、システムインテグレータ、第三者、及び／又はオペレータ（例えば、顧客）によって実施又は実行され得る。この明細書の目的では、システムインテグレータが、任意の数の航空機製造業者及び主要システム下請業者を含み得るがそれらに限定されず、第三者は、任意の数のベンダー、下請業者、及び供給業者を含み得るがそれらに限定されず、且つ、オペレータは、航空会社、リース会社、軍事団体、サービス機関などであり得る。

40

【0028】

例示的な方法100は、航空機120を生産するために使用されてよい。航空機120は、上述されたように、輸送体ネットワークを有する輸送体の一実施例である。図2で示されているように、航空機120は、複数のシステム124及び内装126を備えた機体122を含んでよい。複数のシステム124の実施例には、推進システム128、電気システム130、液圧システム132、環境システム134、貨物システム136、着陸システム138、及び輸送体ネットワークシステム150のうちの1以上が含まれる。輸送体ネットワークシステム150は、例えば、乗客がアクセスすることが許可され得る乗客ベースのシステム160、及び乗客が通常はアクセスすることが許可されない航空機運航システム170を含んでよい。

50

【0029】

複数のシステム124のそれぞれは、含まれる機能に応じて、コントローラ、プロセッサ、アクチュエータ、エフェクタ (effector)、モータ、発電機などの、様々なサブシステムを備えてよい。任意の数の他のシステムが含まれてよい。航空宇宙の例を示しているが、本明細書で開示されている原理は、自動車産業、鉄道移動産業、及び海洋移動産業などの、他の産業にも適用され得る。したがって、航空機120に加えて、本明細書で開示される原理は、他の輸送体、例えば、地上輸送体、海洋輸送体などに適用され得る。本明細書で示され又は説明される装置及び方法は、製造及び保守方法100のステージのうちの任意の1以上の間に採用されてよい。

【0030】

例示的なデータ処理システム

図3で示されているように、この実施例は、本開示の態様による、データ処理システム200 (コンピュータ、計算システム、及び／又はコンピュータシステムとも称される) を説明する。この実施例では、データ処理システム200が、ネットワークマッピングを分かり難くする方法の態様を実装するのに適した例示的なデータ処理システムである。より具体的には、ある実施例では、データ処理システムの実施例であるデバイス (例えば、スマートフォン、タブレット、パーソナルコンピュータ) が、ネットワークのシステムを備えてよく、分かり難くするモジュールを備えてよく、及び／又は分かり難くするモジュールを通じてネットワークに接続されてよい。

【0031】

この例示的な実施例では、データ処理システム200が、システムバス202 (通信フレームワークとも称される) を含む。システムバス202は、プロセッサユニット204 (1以上のプロセッサとも称される)、メモリ206、固定記憶装置208、通信ユニット210、入力／出力 (I/O) ユニット212、コーデック (codec) 230、及び／又はディスプレイ214の間の通信を提供し得る。メモリ206、固定記憶装置208、通信ユニット210、入力／出力 (I/O) ユニット212、ディスプレイ214、及びコーデック230は、システムバス202を介してプロセッサユニット204によってアクセス可能であり得るリソースの実施例である。

【0032】

プロセッサユニット204は、メモリ206に読み込まれ得る指示命令を実行する役割を果たす。プロセッサユニット204は、特定の実装に応じて、幾つかのプロセッサ、マルチプロセッサコア、及び／又は特定の種類の1以上のプロセッサ (例えば、中央処理装置 (CPU)、グラフィックス処理ユニット (GPU) など) を備え得る。更に、プロセッサユニット204は、単一チップ上でメインプロセッサが二次プロセッサと共存する幾つかの異種プロセッサシステムを使用して実装され得る。別の例示的な実施例として、プロセッサユニット204は、同じ種類のプロセッサを複数個含む、対称型マルチプロセッサシステムであってよい。

【0033】

メモリ206及び固定記憶装置208は、記憶デバイス216の実施例である。記憶デバイスは、データ、機能的形態のプログラムコード、及び／又は他の適切な情報などの、情報 (例えば、デジタル情報) を (一時的にか又は恒久的にかの何れかで) 記憶することができる任意の適切なハードウェアを含んでよい。

【0034】

記憶デバイス216は、コンピュータ可読記憶デバイス又はコンピュータ可読媒体とも称され得る。メモリ206は、揮発性の記憶メモリ240及び不揮発性のメモリ242を含んでよい。ある実施例では、起動時などに、データ処理システム200内の要素間で情報を伝達するための、基本的なルーチンを含む基本入力／出力システム (BIOS) が、不揮発性のメモリ242内に記憶されてよい。固定記憶装置208は、特定の実装に応じて様々な形態を採ってよい。

【0035】

固定記憶装置 208 は、1 以上の構成要素又はデバイスを含んでよい。例えば、固定記憶装置 208 は、磁気ディスクドライブ（ハードディスクドライブ又は HDD と称される）、固体ディスク（SSD）、フロッピーディスク、テープドライブ、ジャズドライブ、ジップドライブ、フラッシュメモリカード、メモリスティックなど、又はそれらの任意の組み合わせなどの、1 以上のデバイスを含んでよい。これらのデバイスのうちの 1 以上は、取り外し可能及び／又は携帯可能であってよく、例えば、取り外し可能なハードドライブであってよい。固定記憶装置 208 は、個別の、又は、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-ドライブ）、CD 再書き込み可能ドライブ（CD-RW ドライブ）、及び／若しくはデジタル多用途ディスク ROM ドライブ（DVD-ROM）などの光ディスクドライブを含む、他の記憶媒体と組み合わせられた、1 以上の記憶媒体を含んでよい。固定記憶装置 208 のシステムバス 202 への接続を容易にするために、インターフェース 228 などの、取り外し可能又は取り外し不可能なインターフェースが通常使用される。

【0036】

入力／出力（I/O）ユニット 212 により、データ処理システム 200 に接続可能であり得る他のデバイス（すなわち、入力デバイス及び出力デバイス）によるデータの入力及び出力が可能になる。例えば、入力デバイス 232 は、キーボード、マウス、トラックボール、スタイラス、タッチパッド若しくはタッチスクリーン、マイクロフォン、ジョイスティック、ゲームパッド、サテライトディッシュ、スキャナ、TV チューナーカード、デジタルカメラ、デジタルビデオカメラ、ウェブカメラなどの、1 以上のポインティング及び／又は情報入力デバイスを含んでよい。これらの及び他の入力デバイスは、（1 以上の）インターフェースポート 236 を介して、システムバス 202 を通じて、プロセッサユニット 204 に接続されてよい。（1 以上の）インターフェースポート 236 は、例えば、シリアルポート、パラレルポート、ゲームポート、及び／又はユニバーサルシリアルバス（USB）を含んでよい。

【0037】

出力デバイス 234 は、同じ種類のポートのうちの幾つか、及びある場合では（1 以上の）入力デバイス 232 と同じ実際のポートを使用してよい。例えば、USB ポートは、データ処理システム 200 に入力を提供するため、及びデータ処理システム 200 から出力デバイス 234 に出力情報を提供するために使用されてよい。出力アダプター 238 が、特別なアダプターを必要とする幾つかの出力デバイス 234（例えば、とりわけ、モニタ、スピーカ、及びプリンター）が存在することを示すために設けられている。出力アダプター 238 は、例えば、出力デバイス 234 とシステムバス 202 との間の接続の手段を提供するビデオ及び音響カードを含んでよい。（1 以上の）遠隔コンピュータ 260 などの、他のデバイス及び／又はデバイスのシステムが、入力と出力の両方の機能を提供することができる。（例えば、CRT、LED、又は LCD モニタなどの）ディスプレイ 214 が、ユーザに情報を表示するように構成された、任意の適切なヒューマンマシンインターフェース又は他の機構を含んでよい。

【0038】

通信ユニット 210 は、他のデータ処理システム又はデバイスとの通信を提供するために採用された、任意の適切なハードウェア及び／又はソフトウェアを指す。通信ユニット 210 は、データ処理システム 200 の内側に示されているが、ある実施例では、少なくとも部分的にデータ処理システム 200 の外部にあってよい。通信ユニット 210 は、内部及び外部技術、例えば、モデム（通常の電話グレードのモデム、ケーブルモデム、及び DSL モデムを含む）、ISDN アダプター、並びに／又は有線及び無線イーサネットカード、ハブ、ルーターなどを含み得る。データ処理システム 200 は、1 以上の遠隔コンピュータ 260 への論理接続を使用して、ネットワーク化された環境で動作することができる。（1 以上の）遠隔コンピュータ 260 は、パーソナルコンピュータ（PC）、サーバ、ルーター、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の電化製品、ピアデバイス、スマートフォン、タブレット、別のネットワークノードなどを含んでよい。

(1以上の)遠隔コンピュータ260は、典型的には、データ処理システム200に関して説明される要素の多くを含む。(1以上の)遠隔コンピュータ260は、通信ユニット210を介してデータ処理システム200に接続されたネットワークインターフェース262を通じてデータ処理システム200と論理的に接続されてよい。ネットワークインターフェース262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)、及びセルラーネットワークなどの、有線及び／又は無線通信ネットワークを含む。LAN技術は、光ファイバ分散データインターフェース(FDDI)、銅分散データインターフェース(CDDI)、イーサネット、トークンリングなどを含んでよい。WAN技術は、ポイントトゥポイントリンク、回路切り替えネットワーク(例えば、デジタル総合サービス網(ISDN)及びその変形例)、パケット切り替えネットワーク、及びデジタル加入者回線(DSL)を含む。

10

【0039】

コーデック230は、ハードウェア、ソフトウェア、若しくはハードウェアとソフトウェアの組み合わせを備えた、エンコーダ、デコーダ、又はそれらの両方を含んでよい。コーデック230は、送信及び記憶のためにデータストリーム若しくは信号を符号化、圧縮、及び／又は暗号化し、(例えば、ビデオの再生若しくは編集のために)データストリーム若しくは信号を復号、解凍、及び／又は解読することによって、データストリーム若しくは信号を復号するように構成された、任意の適切なデバイス及び／又はソフトウェアを含んでよい。コーデック230は、分離した構成要素として描かれているが、コーデック230は、メモリ(例えば、不揮発性のメモリ242)内に含まれ又は実装されてよい。

20

【0040】

不揮発性のメモリ242は、リードオンリーメモリ(ROM)、プログラマブルROM(PROM)、電氣的プログラマブルROM(EPROM)、電氣的消去可能プログラマブルROM(EEPROM)、フラッシュメモリなど、又はそれらの任意の組み合わせを含んでよい。不揮発性のメモリ240は、外部キャッシュメモリとして作用し得る、ランダムアクセスメモリ(RAM)を含んでよい。RAMは、静的なRAM(SRAM)、動的なRAM(DRAM)、同期するDRAM(SDRAM)、ダブルデータレートSDRAM、改良されたSDRAM(ESDRAM)など、又はそれらの任意の組み合わせを含んでよい。

【0041】

オペレーティングシステム、アプリケーション、及び／又はプログラム用の指示命令は、システムバス202を通じてプロセッサユニット204と通信可能である、記憶デバイス216内に位置付けられ得る。これらの例示的な実施例では、指示命令が、固定記憶装置208内で機能的な形態を採る。これらの指示命令は、プロセッサユニット204による実行のためにメモリ206の中に読み込まれてよい。本開示の1以上の実施例のプロセスは、メモリ206などのメモリ内に位置付けられ得るコンピュータ実装された指示命令を使用して、プロセッサユニット204によって実行され得る。

30

【0042】

これらの指示命令は、プロセッサユニット204内のプロセッサによって実行される、プログラム指示命令、プログラムコード、コンピュータ可用プログラムコード、又はコンピュータ可読プログラムコードと称される。種々の実施例におけるプログラムコードは、メモリ206又は固定記憶装置208といった、種々の物理的記憶媒体又はコンピュータ可読記憶媒体に具現化され得る。プログラムコード218は、選択的に着脱可能なコンピュータ可読媒体220に機能的な形態で位置付けられてよく、プロセッサユニット204による実行のために、データ処理システム200に読み込まれるか又は伝達され得る。これらの実施例では、プログラムコード218及びコンピュータ可読媒体220が、コンピュータプログラム製品222を形成する。一実施例では、コンピュータ可読媒体220が、コンピュータ可読記憶媒体224又はコンピュータ可読信号媒体226を含み得る。

40

【0043】

コンピュータ可読記憶媒体224は、例えば、固定記憶装置208の部分であるハードドライブなどのように、記憶デバイスに伝達するための固定記憶装置208の部分である

50

ドライブ又は他のデバイスに挿入され又は配置される光ディスク又は磁気ディスクを含み得る。コンピュータ可読記憶媒体 224 はまた、データ処理システム 200 に接続された固定記憶装置（ハードドライブ、サムドライブ、又はフラッシュメモリなど）の形態も採り得る。ある事例では、コンピュータ可読記憶媒体 224 が、データ処理システム 200 から取り外し可能でなくてよい。

【0044】

これらの実施例では、コンピュータ可読記憶媒体 224 が、プログラムコード 218 を伝搬又は送信する媒体ではなく、プログラムコード 218 を記憶するために使用される非一過性の物理的な又は有形の記憶デバイスである。コンピュータ可読記憶媒体 224 は、コンピュータ可読有形記憶デバイス又はコンピュータ可読物理記憶デバイスとも称される。言い換えると、コンピュータ可読記憶媒体 224 は、人が触れることのできる媒体である。

【0045】

代替的に、プログラムコード 218 は、コンピュータ可読信号媒体 226 を使用して、データ処理システム 200 に（例えば、ネットワークを介して遠隔に）伝達され得る。コンピュータ可読信号媒体 226 は、例えば、プログラムコード 218 を包含する伝播されるデータ信号であってよい。例えば、コンピュータ可読信号媒体 226 は、電磁信号、光信号、及び／又は他の任意の適切な種類の信号であってよい。これらの信号は、無線通信リンク、光ファイバケーブル、同軸ケーブル、有線などの通信リンク、及び／又は他の任意の適切な種類の通信リンクを介して伝達されてよい。言い換えると、例示的な実施例では、通信リンク及び／又は接続が、物理的なもの又は無線によるものであってよい。

【0046】

ある例示的な実施例では、プログラムコード 218 が、データ処理システム 200 内で使用するため、コンピュータ可読信号媒体 226 を通じて、別のデバイス又はデータ処理システムからネットワークを介して固定記憶装置 208 へダウンロードされ得る。例えば、サーバデータ処理システム内のコンピュータ可読記憶媒体内に記憶されたプログラムコードは、ネットワークを介してサーバからデータ処理システム 200 にダウンロードされてよい。プログラムコード 218 を提供するコンピュータは、サーバコンピュータ、クライアントコンピュータ、又はプログラムコード 218 を記憶及び送信することができる何らかの他のデバイスであってよい。

【0047】

ある実施例では、プログラムコード 218 が、オペレーティングシステム（OS）250 を含んでよい。固定記憶装置 208 に記憶され得るオペレーティングシステム 250 は、データ処理システム 200 のリソースを制御し割り当てる。1 以上のアプリケーション 252 が、プログラムモジュール 254 を介してオペレーティングシステムのリソース管理を利用し、記憶デバイス 216 に記憶されたプログラムデータ 256 を利用する。OS 250 は、アプリケーション 252 によって共有され使用されるために、コンピュータ 200 のハードウェアリソースを管理し公開するように構成された、任意の適切なソフトウェアシステムを含んでよい。ある実施例では、OS 250 が、種々の種類のハードウェアの接続を容易にし、及び／又は、アプリケーション 252 にハードウェアと OS サービスへのアクセスを提供する、アプリケーションプログラミングインターフェース（API）を提供する。ある実施例では、特定のアプリケーション 252 が、（例えば、いわゆる「ミドルウェア」の場合のように）他のアプリケーション 252 によって使用されるための更なるサービスを提供してよい。本開示の態様は、様々なシステム又はオペレーティングシステムの組み合わせに関連して実装されてよい。

【0048】

データ処理システム 200 に関して図示されている種々の構成要素は、種々の実施例が実装され得るやり方に対して構造的限定を設けることを意図していない。本開示の 1 以上の実施例は、より少ない構成要素を含み、又はコンピュータ 200 について図示されているものに追加して及び／又は代えて構成要素を含む、データ処理システム内に実装されて

10

20

30

40

50

よい。図3で示されている他の構成要素は、描かれている実施例から変更されてよい。種々の実施例は、プログラムコードを実行することができる任意のハードウェアデバイス又はシステムを用いて実施されてよい。一実施例として、データ処理システム200は、無機構成要素と統合された有機構成要素を含むことができ、及び／又は全体的に人間を除く有機構成要素から成ってもよい。例えば、記憶デバイスは有機半導体で構成されてよい。

【0049】

ある実施例では、プロセッサユニット204が、特定の用途向けに又は特定の結果若しくは進歩を生み出すように特に製造され又は構成された、ハードウェア回路を有するハードウェアユニットの形態を採ってよい。この種類のハードウェアは、プログラムコード218を記憶デバイスからメモリの中に読み込んで動作を実行するように構成する必要なしに、動作を実行することができる。例えば、プロセッサユニット204は、回路システム、特定用途向け集積回路(ASIC)、プログラマブル論理デバイス、又は幾つかの動作を実行するように構成された(例えば、予め構成された又は再構成された)何らかの他の適切な種類のハードウェアであってよい。例えば、プログラマブル論理デバイスを用いて、デバイスは、幾つかの動作を実行するように構成され、後に再構成されてよい。プログラマブル論理デバイスの実施例は、プログラマブル論理アレイ、フィールドプログラマブル論理アレイ、フィールドプログラマブルゲートアレイ(FPGA)、及び他の適切なハードウェアデバイスを含む。この種類の実装では、実行可能な指示命令(例えば、プログラムコード218)が、例えば、ハードウェア記述言語(HDL)を使用してFPGAを具体化し、次いで、FPGAを(再)構成するために結果として得られたバイナリファイルを使用することによって、ハードウェアとして実装されてよい。

【0050】

別の一実施例では、データ処理システム200が、重要な作業を分離してカスタムハードウェアで実行することを可能にし得る、FPGAベースの(又はある場合ではASICベースの)状態機械(例えば、有限状態機械(FSM))の専用の組として実装されてよい。CPUなどのプロセッサが、提供された指示命令を実行する共用の汎用状態機械として説明され得る一方で、FPGAベースの(1以上の)状態機械は、専用に構築され、リソースを共有することなしにハードウェアコード化された論理を実行することができる。そのようなシステムは、しばしば、安全関連の作業や不可欠な作業のために利用される。

【0051】

更に別の例示的な一実施例では、プロセッサユニット204が、コンピュータ及びハードウェアユニット内に含まれるプロセッサの組み合わせを使用して実装され得る。プロセッサユニット204は、プログラムコード218を実行するように構成された幾つかのハードウェアユニット及び幾つかのプロセッサを有してよい。図示した実施例の場合、幾つかのハードウェアユニットにおいて幾つかのプロセスを実施することができ、幾つかのプロセッサにおいてその他のプロセスを実施することができる。

【0052】

別の一実施例では、システムバス202が、システムバス又は入力／出力バスなどの、1以上のバスを備えてよい。無論、バスシステムは、バスシステムに取り付けられた種々の構成要素又はデバイスの間でのデータの伝達を行う任意の適切な種類のアーキテクチャを使用して実装され得る。システムバス202は、メモリバス若しくはメモリコントローラを含む(1以上の)バスストラクチャ、周辺機器用バス若しくは外部バス、及び／又は任意の様々な利用可能なバスアーキテクチャ(例えば、業界標準アーキテクチャ(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ックスポート(AGP)、パーソナルコンピュータメモリカード国際協会バス(PCMCIA)、ファイヤーウォール(IEEE1394)、及びスモールコンピュータシステムズインタフェース(SCSI))のうちの幾つかの種類を含んでよい。

【0053】

加えて、通信ユニット 210 は、データの送信、データの受信、又はデータの送受信の両方を行う幾つかのデバイスを含んでよい。通信ユニット 210 は、例えば、モデム又はネットワークアダプタ、2つのネットワークアダプタ、又はこれらの何らかの組み合わせであってよい。更に、メモリは、例えば、メモリ 206、又は、システムバス 202 内に存在し得るインターフェース及びメモリコントローラハブ内に見出されるようなキャッシュであってよい。

【0054】

本明細書で説明するフローチャート及びブロック図は、様々な例示的な実施例による、システム、方法、及びコンピュータプログラム製品の可能な実施態様のアーキテクチャ、機能性、及び動作を示す。これに関して、フローチャート又はブロック図の各ブロックは、1以上の特定の論理的機能を実行するための1以上の実行可能な指示命令を含む、コードのモジュール、セグメント、又は部分を表わし得る。幾つかの代替的な実行態様では、ブロック内に記載された機能を、図面に記載された順序を逸脱して行うことができることに、留意すべきである。例えば、関連する機能性に応じて、連続して示す2つのブロックの機能が実質的に同時に実行され得るか、又は、それらのブロックの機能は、時に逆の順序で実行され得る。

【0055】

例示的な分散型データ処理システム

図4で示されているように、この実施例は、汎用ネットワークデータ処理システム 300（相互交換可能に、コンピュータネットワーク、ネットワークシステム、分散型データ処理システム、又は分散型ネットワークと称される）を説明する。そのマッピングは、本明細書で開示されるように、分かり難くするモジュール及び／又は分かり難くする方法の例示的な実施例によって保護され得る。例えば、上述されたネットワークモジュールは、ネットワークと動作可能に接続されてよく、無線ルーター又はイーサネットデバイスなどの、アクセスノード向けのプロキシとして作用する。

【0056】

図4は、1つの実施態様として提供されるもので、種々の実施例が実装される環境に関して、如何なる限定をも示唆することを意図していないことを理解されたい。図示されている環境に多数の修正を行うことが可能である。

【0057】

ネットワークシステム 300 は、デバイス（例えば、コンピュータ）のネットワークであり、それらのそれぞれは、データ処理システム 200、及び他の構成要素の一実施例であってよい。ネットワークデータ処理システム 300 は、ネットワーク 302 を含んでよく、これは、ネットワークデータ処理システム 300 内で接続される様々なデバイスとコンピュータとの間に通信リンクを提供するように構成された媒体である。ネットワーク 302 は、有線又は無線通信リンク、光ファイバケーブル、並びに／又は、ネットワークデバイス間でのデータ送信及び／若しくはデータ通信に適した任意の他の媒体、或いはこれらの任意の組み合わせなどの接続を含み得る。

【0058】

描かれている実施例では、1以上のコンピュータ可読メモリ又は記憶デバイス 308 と同様に、第1のネットワークデバイス 304 及び第2のネットワークデバイス 306 が、ネットワーク 302 に接続されている。ネットワークデバイス 304 及び 306 は、それぞれ、上述のように、データ処理システム 200 の実施例である。描かれている実施例では、デバイス 304 とデバイス 306 が、サーバコンピュータとして図示されている。サーバコンピュータは、とりわけ、サーバコンピュータ 304 と 306 に対してローカルな情報を記憶するように採用され得る1以上のサーバデータストア 322 と通信する。しかし、ネットワークデバイスは、限定するものではないが、1以上のパーソナルコンピュータ、パーソナルデジタルアシスタント（PDA）、タブレット、及びスマートフォンなどのモバイルコンピューティングデバイス、ハンドヘルドゲーム機、ウェアラブルデバイス、タブレットコンピュータ、ルーター、スイッチ、ヴォイスゲート、サーバ、電子記憶デバ

イス、撮像デバイス、メディアプレーヤー、及び／又は機械的な機能や他の機能を実行し得る他のネットワーク対応ツールなどを含んでよい。これらのネットワークデバイスは、有線、無線、光、及び他の適切な通信リンクを介して相互接続され得る。

【0059】

加えて、クライアント電子デバイス310とクライアント電子デバイス312及び／又はクライアントスマートデバイス314が、ネットワーク302に接続され得る。これらのデバイスのそれぞれは、図3に関して上述されたデータ処理システム200の一実施例である。クライアント電子デバイス310、312、及び314は、例えば、1以上のパーソナルコンピュータ、ネットワークコンピュータ、及び／又は、パーソナルデジタルアシスタント（PDA）、スマートフォン、ハンドヘルドゲーム機、ウェアラブルデバイス、及び／又はタブレットコンピュータなどのモバイルコンピューティングデバイスを含み得る。ある実施例では、そのようなクライアントコンピュータが、ネットワーク302に接続された航空機などの1以上の輸送体上の通信対応データ処理システムを含んでよい。図示した実施例では、サーバ304が、ブートファイル、オペレーティングシステム画像、及びアプリケーションを、クライアント電子デバイス310、312、及び314のうちの1以上に提供する。クライアント電子デバイス310、312、及び314は、サーバコンピュータ304などのサーバに対するそれらの関係上、「クライアント」と称され得る。クライアントデバイスは、1以上のクライアントデータストア320と通信し得る。1以上のクライアントデータストア320は、クライアントに対してローカルな情報（たとえば、（1以上の）クッキー及び／又は関連付けられた文脈情報）を記憶するために採用されてよい。ネットワークデータ処理システム300は、ここに示していない他のデバイスと同様に、より多い又はより少ないサーバとクライアントを含んでよく、或いはサーバとクライアントを全く含まないこともあり得る。

【0060】

ある実施例では、第1のクライアント電気デバイス310が、符号化されたファイルをサーバ304に伝達してよい。サーバ304は、ファイルを記憶してよく、ファイルを復号してよく、及び／又はファイルを第2のクライアント電気デバイス312に送信してよい。ある実施例では、第1のクライアント電気デバイス310が、解凍されたファイルをサーバ304に伝達してよく、サーバ304は、そのファイルを圧縮してよい。ある実施例では、サーバ304が、テキスト、音響、及び／又はビデオ情報を符号化してよく、その情報をネットワーク302を介して1以上のクライアントに送信してよい。

【0061】

クライアントスマートデバイス314は、スマートフォンやタブレットなどの、無線通信及びソフトウェアの実行が可能な任意の適切な携帯型電子デバイスを含み得る。一般的に言うと、「スマートフォン」という用語は、典型的には、タッチスクリーンインターフェース、インターネットアクセス、及びダウンロードされたアプリケーションを実行することができるオペレーティングシステムを有する、コンピュータの機能を実行するように構成された任意の適切な携帯型電子デバイスを示してよい。通話（例えば、携帯電話ネットワークでの）に加えて、スマートフォンは、電子メール、テキスト、及びマルチメディアメッセージの送受信、インターネットへのアクセス、及び／又はウェブブラウザとしての機能が可能である。スマートデバイス（例えば、スマートフォン）は、メディアプレーヤー、パーソナルデジタルアシスタント、デジタルカメラ、ビデオカメラ、及び／又はGPSシステムなどの他の既知の電子デバイスの機能も含み得る。スマートデバイス（例えば、スマートフォン）は、近接無線通信（NFC）、BLUETOOTH（登録商標）、WiFi、又はモバイルブロードバンドネットワークなどを通じて、無線で他のスマートデバイス、コンピュータ、又は電子デバイスに接続することが可能であり得る。無線接続は、情報交換可能なモバイルネットワークを形成するために、スマートデバイス、スマートフォン、コンピュータ、及び／又は他のデバイスの間で確立され得る。

【0062】

システム300内に位置付けられたデータ及びプログラムコードは、上述されたように

、ネットワーク接続された記憶デバイス 308 及び／又はネットワークコンピュータのうちの 1 つの固定記憶装置 208 などの、コンピュータ可読記憶媒体内又は上に記憶されてよい。例えば、プログラムコードは、サーバコンピュータ 304 のコンピュータ可読記憶媒体に記憶されてよく、クライアント 310 で使用するため、ネットワーク 302 を介してクライアント 310 にダウンロードされてよい。ある実施例では、クライアントデータストア 320 及びサーバデータストア 322 が、1 以上の記憶デバイス 308 及び／又は 208 に付属する。

【0063】

ネットワークデータ処理システム 300 は、種々の種類のネットワークのうちの 1 以上として実装されてよい。例えば、システム 300 は、イントラネット、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)、又はパーソナルエリアネットワーク (PAN) を含み得る。幾つかの実施例では、ネットワークデータ処理システム 300 が、インターネットを含み、ネットワーク 302 は、相互通信のための一式のプロトコルである TCP/IP (transmission control protocol/Internet protocol) を使用するネットワーク及びゲートウェイの世界的な集合体を表わしている。インターネットの心臓部には、主要なノード又はホストコンピュータ間の高速データ通信ラインのバックボーンがある。データとメッセージをルーティングするため、数千もの商用、政府機関、教育機関、及びその他のコンピュータシステムが利用可能である。幾つかの実施例では、ネットワーク 302 が、「クラウド」と称されることがある。このような実施例では、各サーバ 304 が、クラウドコンピューティングノードと称されてよく、クライアント電子デバイスは、クラウドコンシューマーなどと称されてよい。図 4 は、実施例として意図されたもので、例示的な実施例の構造的な限界を意図しているわけではない。

【0064】

例示的な航空機ネットワークシステム

図 5～図 7 で示されているように、このセクションは、例示的なネットワークシステム 400 を説明する。ネットワークシステム 400 は、上述されたように、ネットワークマッピングを分かり難くするためのネットワークモジュールを含む、ネットワークデータ処理システム 300 などのネットワークシステムの一実施例である。ネットワークシステム 400 は、航空機 120 及び／又は任意の他の適切な輸送体上に含まれてよい。

【0065】

ネットワークシステム 400 は、図 5 で示されているように、航空機ネットワーク 410 を含む。航空機ネットワーク 410 は、ネットワークシステム 400 内の様々なデバイス間に通信リンクを提供するように構成された媒体を備える。航空機ネットワーク 410 に接続されたデバイスは、上述された、データ処理システム 200 の実施例である 1 以上のデータ処理システムを含んでよい。航空機ネットワーク 410 は、有線又は無線通信リンク、光ファイバケーブル、並びに／又は、航空機ネットワークのデバイス間でのデータ送及び／若しくはデータ通信に適した他の媒体などの接続を含み得る。

【0066】

航空機ネットワーク 410 は、ネットワーク通信フレームワーク及び／又はアビオニクスバスとも称され得る、ネットワークバス 412 を含む。ネットワークバス 412 は、ネットワークプロセッサ 420、ネットワーク入力／出力インターフェース 424、及び少なくとも第 1 の記憶デバイスを含むネットワーク記憶エリア 422 に接続されている。ネットワークバス 412 は、ネットワークプロセッサ 420、入力／出力インターフェース 424、記憶エリア 422、及び／又は任意の他の適切なネットワークデバイスの間の通信 (例えば、データ送信) を容易にするように構成されている。

【0067】

ネットワークプロセッサ 420 は、指示命令を実行するように構成された 1 以上のプロセッサを含み、典型的には、上述された、プロセッサユニット 204 の一実施例であってよい。ネットワーク記憶エリア 422 は、データ、機能的な形態のプログラムコード、及び／又は他の適切な情報などの、情報 (例えば、デジタル情報) を (一時的にか又は恒久

10

20

30

40

50

的にかの何れかで) 記憶することができる任意の適切なハードウェア又はハードウェアの組み合わせを含んでよい。記憶エリアは、コンピュータ可読媒体、揮発性のメモリ、不揮発性のメモリ、固定記憶装置、及び／又は非固定記憶装置を含む、1以上のコンピュータ可読記憶デバイスの組み合わせを含んでよい。

【0068】

ネットワーク入力／出力インターフェース424は、航空機ネットワーク410に接続されたネットワークバス412と他のデバイスとの間のデータの入力及び出力(例えば、受信及び送信)を容易にするように構成されている。ネットワーク入力／出力インターフェース424は、例えば、1以上のスイッチ、ルーター、ハブ、ゲートウェイ、リピーター、ブリッジルーター、プロトコルコンバータ、モジュレータ、モデム、並びに／又は任意の他の適切なハードウェア及び／若しくはソフトウェアを含んでよい。ネットワーク入力／出力インターフェースは、(例えば、有線及び／若しくは無線通信リンクによって)複数のネットワークノード428に接続されている。それらのそれぞれは、データを受信し、生成し、記憶し、並びに／又は送信するように構成されている。ネットワークノードはまた、ネットワークアクセスデバイスとしても説明されてよく、有線及び／又は無線アクセスデバイスを含んでよい。ネットワークノード428は、乗客ベースのシステム414及び航空機運航システム416内に含まれる。

【0069】

航空機運航システム416は、航空機のシステム及び／又は従業員によって使用されるために取っておかれるネットワークデバイス及び／又は通信リングを含んでよい。例えば、航空機運航システム416は、HVACデバイスを動作させ、安全装備(例えば、酸素マスク、消火システムなど)を起動し、乗客に人間が知覚できる情報(例えば、火災警報、乗客に安全ベルトを装着するよう指示する信号など)を提供し、及び／又は通常は許可された輸送体のスタッフに制限されている任意の他の機能を実行するように構成され得る。更に又は代替的に、航空機運航システム416は、一次制御、二次制御、自動操縦システム、エンベロップ保護システム、推力非対称補償システムなどの、航空機の制御に関連付けられたシステムを含んでよく、又はそれらへのアクセスを提供してよい。例示的な航空機運航システム416は、航空機(例えば、航空機120)に接続されているとして本明細書で説明されるが、任意の適切な種類の輸送体上のネットワーク400が、航空機運航システム416に類似した輸送体運航システム又は特定の輸送体に適用可能な他のシステムを含んでよい。

【0070】

本開示の実施例では、航空機運航システム416が、ネットワークノード428のネットワークアクセスデバイス432を含む。航空機運航システム416のネットワークアクセスデバイス432は、ネットワーク入力／出力インターフェース424と直接的に通信する。航空機運航システムの他のネットワークノード428は、同様に、入力／出力インターフェースと通信してよい。航空機運航システム416のネットワークノードは、許可されたスタッフのみにとってアクセス可能であってよく、安全とみなされてよい。したがって、航空機運航システムのネットワークノードは、以下で説明されるように、分かり難くすることなしにネットワーク入力／出力インターフェース424を通じてネットワークバス412と通信してよい。

【0071】

乗客ベースのシステム414は、乗客が使用することを意図された、デバイス、媒体、及び通信リンクを含む。乗客ベースのシステム414は、例えば、乗客デバイス440を外部ネットワーク444と接続するように構成された、ネットワークノード及び／又はデバイスも含んでよい。更に又は代替的に、乗客ベースのシステム414の構成要素は、乗客が、デバイス440を使用して、機内娯楽オプションにアクセスする(例えば、航空機ネットワーク410内に記憶された映画や音楽をストリーミング又はダウンロードする)、飲食物を注文する、航空機客室乗務員からの支援をリクエストする、航空機のステータス(場所、速度、及び／又は予測される到着時間)の更新を取得することなどを可能にす

10

20

30

40

50

るように構成されてよい。

【0072】

本実施例では、乗客ベースのシステム414が、ネットワークノード428の無線ネットワークアクセスデバイス430を含む。無線ネットワークアクセスデバイス430は、航空機ネットワーク410へのアクセスを乗客デバイス440に提供してよい。乗客デバイス440は、スマートフォン、コンピュータ、ラップトップコンピュータ、タブレット、及び／又は無線通信を可能にする任意の他の適切な電子デバイスであってよい。乗客デバイス440は、乗客の個人的な所有物であってよく、又は乗客によって操作される任意の適切な電子デバイスであってよい。

【0073】

乗客デバイス440は、他のデータ処理システム又はデバイスとの通信を容易にするように構成された、無線通信デバイス442を含む。例えば、無線通信デバイス442は、上述されたデータ処理システム200の通信ユニット210の一実施例であってよい。無線通信デバイス442は、無線ネットワークアクセスデバイス430を通じて航空機ネットワーク410に接続してよく、それによって、乗客デバイス440が、航空機ネットワークと通信することを可能にする。無線通信デバイス442が、航空機ネットワーク410に接続されたときに、乗客440は、ネットワーク上にあり、ネットワークに接続され、及び／又はネットワーク化されているとして言及され得る。

【0074】

無線ネットワークアクセスデバイス430は、分かり難くするモジュール510を通じて、ネットワーク入力／出力インターフェース424と通信する。より具体的には、無線ネットワークアクセスデバイス430とネットワーク入力／出力インターフェース424との間の全ての通信は、分かり難くするモジュールの仮想コンテナ516を通じて行われる。仮想コンテナ516は、ネットワーク入力／出力インターフェースとして作用するように構成され、ルーター、ゲートウェイ、及び／又はプロキシサーバの一部又は全部の機能を実行すると説明され得る。

【0075】

分かり難くするモジュール510は、上述のデータ処理システム200などの分離したハードウェアモジュールの形態を採ってよく、若しくはネットワーク入力／出力インターフェース424のハードウェアで実行されるソフトウェアモジュールの形態を採ってよく、又は任意の効果的なやり方でソフトウェアとハードウェアの態様を組み合わせる。本実施例では、分かり難くするモジュール510が、専用記憶エリア512及び専用プロセッサ514を含む。プロセッサ514は、ネットワーク入力／出力インターフェース424と直接的に通信し、仮想コンテナ516から分離されている。仮想コンテナ516は、記憶エリア512を使用して、プロセッサ514によって実行される、仮想ソフトウェア環境として説明され得る。本明細書における仮想コンテナ516及び／又は他の仮想コンテナへの言及は、仮想ソフトウェア環境内で実行されるソフトウェア及び／又はプロセスを包含するものと理解され得る。

【0076】

ある実施例では、航空機ネットワーク410が、複数のネットワークアクセスデバイスのユーザからネットワークを保護するために、複数の分かり難くするモジュールを含んでよい。例えば、分かり難くするモジュールは、乗客ベースのシステム414のネットワークノード428の各ネットワークアクセスデバイスと、ネットワーク入力／出力インターフェース424と、の間に動作可能に配置されてよい。ある実施例では、分かり難くするモジュール510が、乗客ベースのシステム414のネットワークノード428の複数のネットワークアクセスデバイスと、ネットワーク入力／出力インターフェース424と、の間に動作可能に配置されてよい。航空機ネットワーク410のアーキテクチャに応じて、任意の数の分かり難くするモジュールが使用されてよい。ある実施例では、分かり難くする機能を調整するために、複数の分かり難くするモジュールが接続されてよい。

【0077】

乗客デバイス 440 が、航空機ネットワーク 410 に接続されると、ネットワークを介してデータ通信を送信及び受信することができるが、全てのそのような通信が、分かり難くするモジュール 510 を通じて経路指定されるわけではない。典型的な一実施例では、悪意のない乗客が、ネットワーク記憶エリア 422 へのアクセスを得るために、航空機ネットワーク 410 に接続されてよい。例えば、乗客は、映画を観るためにスマートフォンを接続してよい。

【0078】

そのような一実施例では、乗客デバイス 440 が、無線ネットワークアクセスデバイス 430 に通信を送り、ネットワーク記憶エリア 422 向けのネットワークアドレスをリクエストする。無線ネットワークアクセスデバイスは、そのリクエストを分かり難くするモジュール 510 に転送する。今度は、分かり難くするモジュール 510 が、そのリクエストをネットワーク入力／出力インターフェース 424 に転送する。入力／出力インターフェースは、ネットワーク記憶エリア 422 に割り当てられた静的なネットワークアドレスを提供し、モジュール 510 への返信を通信する。

【0079】

モジュール 510 は、無線ネットワークアクセスデバイス 430 を通じて、代替的なネットワークアドレスを乗客デバイス 440 に通信することによって、提供される静的なネットワークアドレスをマスキングする。引き続いて、乗客デバイス 440 によってネットワーク記憶エリア 422 送られたパケットは、代替的なネットワークアドレスにアドレス指定される。パケットが、無線ネットワークアクセスデバイス 430 によってモジュール 510 に渡されたときに、モジュールは、各パケットアドレスを、ネットワーク記憶エリア 422 に割り当てられた静的なネットワークアドレスに編集する。次いで、パケットは、ネットワーク入力／出力インターフェース 424 に渡され、記憶エリア 422 に渡される。

【0080】

分かり難くするモジュール 510 は、航空機ネットワーク 410 のネットワークアドレス空間又はマップと、生成された人工ネットワークマップと、の間の基本的な又は一対一のネットワークアドレス変換 (NAT) を実行するとして説明されてよい。すなわち、分かり難くするモジュールは、インターセプトされたパケットを編集して、航空機ネットワーク 410 の静的なアドレスを、生成された人工ネットワークマップからの代替的なアドレスで置き換え、その逆も行う。ある実施例では、分かり難くするモジュール 510 が、更に又は代替的に、ポートナンバーなどの他のパケット情報を編集する。

【0081】

航空機ネットワーク 410 の静的なネットワークマッピングをマスキングすることに加えて、分かり難くするモジュール 510 は、NAT 向けに使用される生成された人工ネットワークマップを変更するように構成されている。図 6 で示されているように、分かり難くするモジュール 510 は、それぞれが関連付けられたネットワークマップを有する、複数の仮想コンテナを含む。生成された人工マップを変更するために、分かり難くするモジュールは、どの仮想コンテナが起動しているかを変更する。

【0082】

再び図 5 を参照して、上述の実施例を継続すると、分かり難くするモジュール 510 によって乗客デバイス 440 に提供された、ネットワーク記憶エリア 422 向けの代替的なネットワークアドレスは、第 1 のネットワークマップから取得される。ネットワークマップ 546 へ変更した後で、乗客デバイス 440 から送られたパケットは、ネットワーク記憶エリア 422 への配信のために、もはや効果的にアドレス指定されない。乗客は、乗客デバイス 440 が、再び、ネットワーク記憶エリア 422 向けのネットワークアドレスをリクエストし、第 2 のネットワークマップからネットワーク記憶エリア向けの新しい代替的なネットワークアドレスを受け取る間、接続性の短い損失を経験し得る。

【0083】

分かり難くするモジュール 510 は、それによって、乗客デバイス 440 から、航空機

10

20

30

40

50

ネットワーク 410 のネットワークマッピングを分かり難くすることができる。モジュール 510 によって使用されるネットワークマップの変更によって、乗客デバイス 440 と承認されたネットワークデバイスとの間の通信の妨害（中断）を最小化することができる。すなわち、航空機ネットワーク 410 の乗客デバイス 440 の許可された動作は、通常、ネットワークアドレスにおける変更後の通信の自動的な再確立のためのプロトコルを含む、システム対システムの通信を含み得る。そのような通信は、最小化された妨害（中断）を経験し得る。しかし、許可されていない動作向けのネットワークマッピングの予備調査は、図 7 との関連で以下で更に説明される、ネットワークマップの変更によって妨害（中断）され得る。

【0084】

図 6 は、分かり難くするモジュール 510 の例示的な一実施例の概略的な描画である。モジュールの記憶エリアは、2つの区画、すなわち、安全アビオニクス区画 556 と外部区画 558 に分割される。アビオニクス区画 556 と外部区画 558 との間のデータの流れは、アビオニクス区画から外部区画への単一方向の流れに限定される。本実施例では、データの流れが、ソフトウェアデータダイオード 518 によって制限される。ある実施例では、区画 556 と 558 が、分離された記憶デバイス及び／又はデータ処理システムを備えてよく、データの流れは、ハードウェアデータダイオードによって制限され得る。

【0085】

外部区画 558 は、複数の分離された仮想環境を管理し、仮想環境の間でメモリ又はオペレーティングシステム（OS）サービスなどの、ハードウェア及び／又はソフトウェアリソースを割り当てるように構成された、仮想システムを含む。本実施例では、仮想化システムが、複数のコンテナを管理するリアルタイムハイパーバイザ 536 である。ある実施例では、仮想化システムが、コンテナ管理者を含んでよく、仮想環境は、仮想マシンを含んでよく、及び／又は任意の効果的な仮想化が使用されてよい。

【0086】

ハイパーバイザ 536 は、起動コンテナ 516、及びコンテナライブラリ 538 を維持する。図 6 で描かれているように、起動コンテナは、現在のところコンテナ 540 である。起動コンテナ 516 は、無線ネットワークアクセスデバイス 430 及びネットワーク入力／出力インターフェース 424 と通信し、上述されたように、プロキシサーバやゲートウェイとして作用する。

【0087】

コンテナライブラリ 538 は、少なくとも 1つの起動していないコンテナを含む。起動していないコンテナは、航空機ネットワーク 410 と通信せず、又は接続されていない。描かれている実施例では、ライブラリが、コンテナ 544、コンテナ 548、及びコンテナ 552 を含む、N 個の起動していないコンテナを有する。N は、任意の整数であってよいが、ライブラリ 538 内に含まれる起動していないコンテナの数は、ライブラリを管理することに関連付けられた処理及びメモリ要求を低減させるように制限され得る。

【0088】

ハイパーバイザ 536 は、コンテナを交替させてよく、コンテナライブラリ 538 から、起動コンテナになる次のコンテナを選択する。例えば、ハイパーバイザは、次の起動コンテナとしてコンテナ 544 を選択することができる。コンテナ 540 は、航空機ネットワーク 410 から切断されてよく、一時的に、無線ネットワークアクセスデバイス 430 とネットワーク入力／出力インターフェース 424 との間の通信を断ち切る。コンテナ 540 は、シャットダウンされてよく、又は起動していないコンテナとしてコンテナライブラリ 538 に返還されてよい。次いで、コンテナ 544 が、航空機ネットワーク 410 に接続されてよく、無線ネットワークアクセスデバイス 430 とネットワーク入力／出力インターフェース 424 との間の通信を再び促進する。次いで、コンテナ 544 は、起動コンテナ 516 になる。ハイパーバイザ 536 は、安全アビオニクス区画 556 から交替指示命令を受け取ったときに、コンテナを交替させる。

【0089】

10

20

30

40

50

各コンテナは、異なるネットワークマップを含む。本実施例では、コンテナ 540 が、ネットワークマップ 542 を含み、コンテナ 544 が、ネットワークマップ 546 を含み、コンテナ 548 が、ネットワークマップ 550 を含み、コンテナ 552 が、ネットワークマップ 554 を含む。分かり難くするモジュール 510 は、航空機ネットワーク 410 のネットワークマップと起動コンテナのネットワークマップとの間で、基本的な NAT を実行する。例えば、コンテナ 540 が起動している間に、分かり難くするモジュールは、ネットワークマップ 542 に従って NAT を実行する。

【0090】

分かり難くするモジュール 510 は、コンテナがハイパーバイザ 536 によって交替させられている際に、新しいコンテナ及びネットワークマップを生成するように構成されている。安全なアビオニクス区画 556 は、ネットワークマップ生成器 530 及びコンテナ生成器 534 を含む。ネットワークマップ生成器 530 は、ランダムなネットワークマップの生成を容易にするために、ランダム化エンジン 532 を含む。生成されたネットワークマップは、インターネットプロトコル (IP) アドレス、ポート、ネットワークアセット識別子、及び／又はネットワーク通信で使用される任意の他の情報を含んでよい。

【0091】

ある実施例では、ネットワークマップを生成することが、ランダムに選択されたネットワークアドレスを、航空機ネットワーク 410 のネットワークデバイス又は接続されたデータ処理システムに現在割り当てられている全てのネットワークアドレスに関連付けることを含んでよい。ランダムに選択されたネットワークアドレスを、現在使用されているネットワークアドレスのみに関連付けることは、各ネットワークマップを生成し記憶することに関連付けられた処理及びメモリ要件を低減させ得るが、安全アビオニクス区画 556 とネットワーク入力／出力インターフェース 424 との間の通信を必要とし得る。

【0092】

ある実施例では、ネットワークマップを生成することが、ランダムに選択されたネットワークアドレスを、航空機ネットワークによって使用される通信プロトコル向けに有効な全てのネットワークアドレスに関連付けることを含んでよい。そのような完全なマップは、生成及び記憶のために更なる処理及びメモリを必要とし得るが、安全アビオニクス区画 556 が、ネットワーク入力／出力インターフェース 424 と接続することなしに動作することを可能にし得る。

【0093】

ネットワークマップは、航空機ネットワーク 410 によって使用される通信プロトコルの制約の範囲内でランダム化されてよく、及び／又は、航空機ネットワーク 410 の管理者によって選択可能な制約の範囲内でランダム化されてよい。例えば、航空機ネットワーク 410 のネットワークアドレスは、プライベート IP アドレスとして使用されるために取っておかれた IP アドレスのうちの何れかからランダムに選択されたネットワークアドレスに関連付けられてよい。別の一実施例では、ネットワークの管理者が、ランダムに選択されたアドレスを、192.168.0.0 と 192.168.255.255 の間のプライベート IP アドレスのブロックに限定することができる。

【0094】

各生成されたネットワークマップは、対応する生成されたコンテナ内に記憶される。各コンテナ及び記憶されたネットワークマップは、次いで、外部区画 558 に渡され、コンテナライブラリ 538 に追加される。

【0095】

安全アビオニクス区画 556 は、切り替えデバイス 520 を更に含む。それは、外部区画 558 内でのコンテナの交替を開始するように構成されている。切り替えデバイス 520 は、1 以上の予め選択された基準に従って、ハイパーバイザ 536 に交替リクエストを送信することができる。その基準は、航空機ネットワーク 410 及び／又は分かり難くするモジュール 510 の管理者によって選択されてよい。典型的には、その基準が、任意の所望の更なる基準に加えて、ネットワーク 410 が動作するところの航空機が飛行中であ

10

20

30

40

50

ることを含んでよい。

【0096】

例えば、切り替えデバイス520は、航空機の位置に関して、航空機運航システム416内に含まれる航法システムから地理的位置データを受け取ることができる。航空機が特定の飛行経路又は民間ルートに割り当てられているときに、管理者は、1以上の地理的位置を選択することができる。引き続いて、航空機が選択された位置に到達したときに、切り替えデバイス520は、ハイパーバイザ536に交替リクエストを送信することができる。

【0097】

別の一実施例では、切り替えデバイス520が、乗客データを含む航空機運航システム416内のデータベースと通信することができる。切り替えデバイス520は、飛行中の乗客が以前に同じ飛行機で移動したか又は同じ飛行機に搭乗したことがあり、フラグ付きの移動ステータスを有し、及び／又は管理者によって選択された任意の基準を有するときに、データベースから警告を受け取ることができる。次いで、切り替えデバイス520は、飛行についての警告が受け取られていないときに、飛行中に一度だけ交替リクエストを送信することができるが、少なくとも1つの警告が受け取られたときには、30分毎に交替リクエストを送信することができる。

【0098】

別の一実施例では、切り替えデバイス520が、ネットワーク動作に関して、ネットワーク入力／出力インターフェース424と通信することができる。特定のネットワーク動作が生じたか又は選択された閾値を上回ったときに、切り替えデバイス520は、交替リクエストを送信することができる。例えば、交替は、制限されたシステムの中への侵入が検出された場合、又は乗客デバイスによるネットワークへの行為が通常のレベルを超えた場合に開始されてよい。

【0099】

切り替えデバイス520は、ハイパーバイザ536によるコンテナの交替の動的なトリガを可能にするようにも構成されてよい。例えば、切り替えデバイスは、ネットワーク410を介して航空機のパイロットによって使用されるコンピュータから交替リクエストを受け取り、及び／又は、客室乗務員などの許可されたスタッフにとって物理的にアクセス可能な分かり難くするモジュール510のローカルインターフェースから交替リクエストを受け取るように構成されてよい。

【0100】

本実施例では、切り替えデバイス520が、安全モードセレクトア522を含む。安全モードセレクトアは、交替のための基準の選択を単純化するように構成されたユーザインターフェースを含む。ユーザは、低い524、中間526、及び高い528の間で、安全設定を選択することができる。各モードは、切り替えデバイス520向けの基準の対応する組を選択する。例えば、各安全設定は、時間間隔ベースの基準を指定することができる。低い安全設定524は、交替の間に2時間の間隔を選択することができる。中間の安全設定526は、交替の間に1時間の間隔を選択することができる。高い安全設定528は、ランダムな間隔の交替を選択することができる。各間隔は、30分以下である。

【0101】

安全性の懸念が限られているときにより低い安全設定を選択することによって、処理負荷が結果として低減されるので好適であり得る。増加した熱生成及び電力需要などの更なる処理要件の効果が、航空機上では特に望ましくないだろう。

【0102】

安全モードセレクトア522によって、ネットワークセキュリティに関する知識又は技能が限られているユーザによる、分かり難くするモジュール510の使用が容易になり得る。例えば、安全モードセレクトア522は、航空乗務員が、各飛行の前に分かり難くするモジュール510の基準選択を更新することを可能にし得る。航空機ネットワーク410の管理者、航空機を運航する航空会社の技術支援スタッフ、分かり難くするモジュール51

10

20

30

40

50

0の製造業者、又は他の資格のある個人若しくは組織は、安全モードセクタ522を使用して選択可能なモードの定義を更新することができる。例えば、新しいネットワーク予備調査技法が頻繁に使用されるようになったとき、各モードでのコンテナ交替の間の時間を低減させる分り難くするモジュール向けのソフトウェア更新が公にされてよい。

【0103】

安全モードセクタは、スリープモード又はスタンバイモードを含んでもよい。そのようなモードでは、分り難くするモジュール510が、編集することなしに、ネットワーク入力／出力インターフェース424と無線ネットワークアクセスデバイス430との間でパケットを中継することができる。そのようなモードは、技術スタッフによる航空機ネットワーク410の整備を容易にすることができる。例えば、不具合のある無線ネットワークアクセスデバイスのトラブルシューティング又は乗客ベースのシステム414内の新しいモードの設置は、静的なネットワークで極めて単純になるだろう。ある実施例では、そのようなスタンバイモードが、飛行機が飛行中でないときは何時でも利用可能であり得る。しかし、高度に安全なエリア内の航空機にとって、分り難くするモジュール510の継続的な動作は適切であり得る。

【0104】

安全アビオニクス区画556は、乗客デバイス440にとってアクセス不可能に構成されている。安全アビオニクス区画は、航空機ネットワーク410のネットワーク入力／出力インターフェース424のみと通信し、他のネットワークノード又は乗客デバイスと通信しない。ある実施例では、安全アビオニクス区画556が、航空機ネットワーク410と接続されなくてよく、分り難くするモジュール510向けの管理機能は、局所的に実行され得る必要があり得る。

【0105】

分り難くするモジュール510は、安全アビオニクス区画556が乗客デバイス440にとってアクセス不可能なことを確実にするように構成されてもよい。そのような構成は、ハードウェア及び／又はソフトウェアの特徴を含んでよい。例えば、安全アビオニクス区画556は、外部区画558から分離された、専用プロセッサ及び記憶デバイスで実行されてよい。

【0106】

図7は、攻撃者による予備調査の下での、モジュール510によって航空機ネットワーク410のマッピングを分り難くすることを示す概略図である。本実施例では、攻撃者が、乗客デバイス440を使用する航空機の乗客である。攻撃者は、無線ネットワークアクセスデバイス430などのネットワークアクセスデバイスへのアクセスを有する、航空機上又は航空機外の任意の当事者を含んでよい。典型的には、予備調査が、応答を受け取るまで一連の有効なネットワークアドレスに照会を送ることによって、ネットワークアセットを位置特定することを含む。一般的な照会は、ピング(ping)又は他のエコーリクエストパケットを含んでよい。本実施例では、乗客デバイス440が、ピング560をローカルネットワークアドレス192.168.2.5に送る。

【0107】

ピング560は、乗客デバイス440から無線ネットワークアクセスデバイス430に送られ、分り難くするモジュール510に転送される。ピング560の次の経路は、分り難くするモジュール510のどのコンテナが現在起動しているかに応じる。コンテナ540が起動している場合、ピング560は、一点鎖線562によって示されている経路を辿るだろう。コンテナ540は、ピング560を受け取り、ネットワークマップ542に従ってピングパケットアドレスを編集する。図7で示されているように、ネットワークマップ542は、アドレス192.168.2.5を、航空機ネットワーク410の実際のアドレス192.168.1.1に関連付ける。編集されたピングは、ネットワーク入力／出力インターフェース424に転送される。それは、編集されたピングを192.168.1.1に配信する。そのアドレスは、ネットワークバス412に接続されたアビオニクスシステム423に割り当てられるので、乗客デバイス440は、アドレス192.168.2.5で、アクセスが制限されたシ

10

20

30

40

50

ステムの存在を示す返答を受け取るだろう。

【0108】

コンテナ544が起動している場合、ピング560は、破線564によって示されている経路を辿るだろう。コンテナ544は、ピング560を受け取り、ネットワークマップ546に従ってピングパケットアドレスを編集する。図7で示されているように、ネットワークマップ546は、アドレス192.168.2.5を、航空機ネットワーク410の実際のアドレス192.168.1.2に関連付ける。編集されたピングは、ネットワーク入力／出力インターフェース424に転送される。それは、編集されたピングを192.168.1.2に配信する。そのアドレスは、ネットワーク記憶エリア422に割り当てられるので、乗客デバイス440は、アドレス192.168.2.5で、アクセス可能なシステムの存在を示す返答を受け取るだろう。

10

【0109】

コンテナ548が起動している場合、ピング560は、実線566によって示されている経路を辿るだろう。コンテナ548は、ピング560を受け取り、ネットワークマップ550に従ってピングパケットアドレスを編集する。図7で示されているように、ネットワークマップ550は、アドレス192.168.2.5を、航空機ネットワーク410で現在使用されている任意のアドレスに関連付ける。ピングは、配信されないこととなる。乗客デバイス440は、アドレス192.168.2.5で、ネットワークアセットが存在しないことを示す時間切れメッセージを受け取るだろう。

20

【0110】

ピング560が、コンテナ540が起動している間に送られる一実施例を考える。攻撃者は、アドレス192.168.2.5で、アクセスが制限されたシステムの存在を記録し、更なるネットワークアセットを位置特定するために、他の有効なアドレスのピンギング (pinging) を継続する。予備調査が進んでいる一方で、分かり難くするモジュール510は、上述のようにコンテナを交替させ、それによって、コンテナ548が起動する。攻撃者が、再び192.168.2.5と通信することを試みたときに、ネットワークは、そのアドレスにデバイスが存在しないことを示すこととなる。

【0111】

航空機ネットワーク410の制限されたシステムの中への更なる侵入を進めるために、攻撃者は、したがって、予備調査段階を繰り返さなければならない。理想的には、攻撃者が、飛行継続期間中に予備調査段階にあるままであり、航空機ネットワーク410の任意のシステムに攻撃又は侵入を実行することができなくなるだろう。

30

【0112】

更に、利用される予備調査技法に応じて、分かり難くするモジュール510は、ネットワークで検出されないままであってよい。分かり難くするモジュール510及びコンテナは、発見の可能性を低減させるように構成されてよい。例えば、分かり難くするモジュールは、分かり難くするモジュールに割り当てられた静的なネットワークアドレスをマスクング又は匿名化するために、無線ネットワークアクセスデバイス430とネットワーク入力／出力インターフェース424との間でインターセプトされたパケットを編集するように構成されてよい。

40

【0113】

例示的な方法

このセクションは、図8を参照しながら、航空ネットワークのマッピングを分かり難くするための例示的な方法のステップを説明する。上述された航空機ネットワーク及び／又はネットワークモジュールの態様は、以下で説明される方法ステップにおいて利用されてよい。適切な場合には、各ステップを実行することにおいて使用され得る構成要素及びシステムに対する参照が行われ得る。これらの参照は例示のためのもので、本方法の任意の特定のステップを実行するのに可能なやり方を限定することを意図していない。

【0114】

図8は、例示的な方法で実行されるステップを示すフローチャートであり、本方法の完

50

全なプロセス又は全てのステップを列挙しているわけではない。方法 600 の様々なステップが以下で説明され、図 8 で示されているが、ステップは必ずしも全て実行される必要があるわけではなく、場合によっては、同時に、或いは図示された順序とは異なる順序で実行されることもある。

【0115】

ステップ 610 では、該方法が、アクセスノードとネットワークバスとの間にモジュールを配置することを含む。ある実施例では、該モジュールが、アクセスノードと、別の種類のネットワーク通信システム及び／又は任意のネットワークトポロジを有するネットワークの全ての他のノードと、の間に配置されてよい。該モジュールは、上述のデータ処理システム 200 などの固有のハードウェアモジュールであってよく、若しくはゲートウェイなどのネットワークインターフェースのハードウェアで実行されるソフトウェアモジュールであってよく、又は任意の効果的なやり方でソフトウェアとハードウェアの態様を組み合わせることができる。該モジュールは、プロセッサ及びコンピュータ可読記憶デバイスを含んでよく、及び／又はそれらで実行されてよい。

10

【0116】

該モジュールは、アクセスノード及びネットワークバスと動作可能に接続されてよい。該モジュールは、アクセスノード及び／又はネットワークバスと直接通信してよく、及び／又は、ゲートウェイ、ルーター、若しくはプロキシなどのネットワークインターフェースを通じて通信してよい。該モジュールは、非限定的に、無線通信リンク、光ファイバケーブル、又は同軸ケーブルを含む、任意の適切な通信リンクによって、アクセスノード、ネットワークバス、及び／又はネットワークインターフェースと接続されてよい。

20

【0117】

本方法のステップ 612 は、N 個のコンテナを生成することを含む。ここで、N は、任意の正の整数である。各コンテナは、独立した仮想化されたシステムがモジュールで実行されることを可能にするように構成された、オペレーティングシステムレベルの仮想化を含んでよい。コンテナを生成することは、コンテナ内にソフトウェア又はプロセスを記憶し、構成し、及び／又は初期化することを含んでよい。ある実施例では、該ステップが、完全な仮想化及び／又はハードウェア援用仮想化 (hardware-assisted virtualization) などの方法によって、仮想マシンなどの他の仮想環境を生成することを含んでよい。

【0118】

本方法のステップ 614 は、N 個のネットワークマップを生成することを含む。ここで、N は、任意の正の整数である。各マップは、関連付けられたネットワークアドレスの複数のペアを含んでよい。各マップは、ランダムに生成されてよく、ランダムネットワークアドレスをネットワークアドレスの組のそれぞれと関連付ける。ここで、ネットワークアドレスの組は、ネットワークバスを含むネットワークに割り当てられた各静的なアドレスを含んでよく、及び／又は、ネットワークでの動作において 1 以上の通信プロトコル内で有効な全てのネットワークアドレスを含んでよい。各マップは、更に又は代替的に、ポートナンバーや物理的アドレスなどの、他のネットワーク通信データを含んでよい。

30

【0119】

ステップ 616 では、該方法が、各ネットワークマップをコンテナ内に記憶することを含む。ネットワークマップをコンテナ内に記憶することは、ネットワークマップに関連付けられたデータを、記憶デバイス又はコンテナに割り当てられたエリア内に記憶することを含んでよい。それによって、データは、コンテナ内で実行されているソフトウェア及び／又はプロセスにとってアクセス可能である。

40

【0120】

ステップ 612 から 616 は、同時に実行されてよく、及び／又は順に繰り返し実行されてよい。例えば、コンテナ及びネットワークマップは、同時に生成されてよい。別の一実施例では、第 1 のコンテナが生成されてよく、第 1 のネットワークマップが生成されてよく、第 1 のネットワークマップは、第 1 のコンテナ内に記憶されてよい。次いで、第 2 のネットワークマップが生成されてよく、第 2 のネットワークマップは、第 2 のコンテナ

50

内に記憶されてよい。ステップ 6 1 2 から 6 1 6 は、更なるコンテナ及びネットワークマップが必要とされたときに、方法 6 0 0 の全体を通して繰り返されてよい。

【0 1 2 1】

ステップ 6 1 8 は、第 1 のコンテナをモジュールに読み込むことを含む。ステップ 6 1 8 のサブステップ 6 2 0 は、モジュールを安全区画と外部区画へ分割することを含む。その分割は、ハードウェア及び／又はソフトウェア内であってよい。例えば、区画は、単一の記憶デバイスのディスク区画化によって形成されてよく、プロセッサを共有してよい。別の一実施例では、各区画が、分離された記憶デバイスとプロセッサを備えてよい。

【0 1 2 2】

ステップ 6 1 8 のサブステップ 6 2 2 は、区画の間でのデータの流れを単一方向の流れに限定することを含む。データは、安全区画から外部区画への流れに限定されてよい。限定は、ソフトウェア又はハードウェアダイオードを含む、データダイオードで実行されてよい。サブステップ 6 2 0 及び 6 2 2 は、モジュール向けの設定プロセスの部分として、ステップ 6 1 0 の前に実行されてよい。次いで、ステップ 6 1 2 から 6 1 6 は、安全区画で実行されてよい。

10

【0 1 2 3】

サブステップ 6 2 4 は、第 1 のコンテナを安全区画から外部区画に読み込むことを含む。コンテナを読み込むことは、第 1 のコンテナに関連付けられたデータを、データダイオードを通して安全区画から外部区画に送信及び／又は通信することを含んでよい。コンテナを読み込むことは、コンテナを開始すること、並びに／又は、ハイパーバイザ、コンテナ管理者、及び／若しくは仮想化システムによるコンテナ制御の仮定を含んでもよい。ある実施例では、コンテナを読み込むことが、起動していないコンテナのライブラリ内にコンテナを記憶することを含んでよい。

20

【0 1 2 4】

ステップ 6 2 6 では、方法 6 0 0 が、第 1 のコンテナ内に記憶されたネットワークマップを、アクセスノードにとってアクセス可能にすることを含む。ネットワークマップをアクセス可能にすることは、起動していないコンテナのライブラリから第 1 のコンテナを選択すること、及び第 1 のコンテナを起動コンテナとして指定することを含んでよい。ネットワークマップをアクセス可能にすることは、第 1 のコンテナとアクセスノードとの間の通信を確立することを更に含んでよい。例えば、コンテナ内で実行されているサーバソフトウェアは、アクセスノードと通信するように置かれてよい。第 1 のコンテナは、ネットワークマップに従ってアクセスノードと通信してよい。

30

【0 1 2 5】

ステップ 6 2 8 は、アクセスノードとネットワークバスとの間の通信を、第 1 のコンテナを通る通信に限定することを含む。通信を限定することは、アクセスノードが単にモジュールに接続されるように、ネットワークのアーキテクチャを構成することを含んでよい。通信を限定することは、アクセスノードが単にモジュールの外部区画の選択された仮想コンテナと通信するように、モジュールを構成することを更に含んでよい。

【0 1 2 6】

第 1 のコンテナは、ゲートウェイ、ルーター、又はプロキシサーバなどの、ネットワークインターフェースとして作用するように構成されてよい。そのような構成は、サーバのオペレーティングシステムや仮想ルーターなどの、コンテナの範囲内のソフトウェア及び／又はプロセスの初期化を含んでよい。第 1 のコンテナは、アクセスノードとネットワークバスとの間の通信を容易にしてよく、第 1 のコンテナ内に記憶されたネットワークマップに従って、アクセスノードと通信してよい。

40

【0 1 2 7】

該方法のステップ 6 3 0 は、アクセスノードにとってアクセス可能なネットワークマップを変更することを含む。ステップ 6 3 0 のサブステップ 6 3 2 は、第 1 のコンテナを通る通信を排除することを含む。通信を排除することは、第 1 のコンテナ及び／又はコンテナ内で実行されているソフトウェア若しくはプロセスを断ち切ることを含んでよい。通信

50

を排除することは、コンテナ内で実行されているソフトウェア又はプロセスをシャットダウン又は終了することを更に含んでよい。

【0128】

ステップ630のサブステップ634は、第1のコンテナを第2のコンテナで置き替えることを含む。第2のコンテナは、ステップ612から616で生成されたN個のコンテナのうちの1つであってよく、ステップ618に従ってモジュールに読み込まれてよい。第2のコンテナは、起動していないコンテナのライブラリから選択されてよく、起動コンテナとして指定されてよい。第1のコンテナは、シャットダウンされてよい。

【0129】

ステップ630のサブステップ636は、第2のコンテナを通る通信を確立することを含む。ステップ626及び628と同様に、該サブステップは、第2のコンテナ内に記憶されたネットワークマップを、アクセスノードにとってアクセス可能にすることを含んでよく、アクセスノードとネットワークバスとの間の通信を、第2のコンテナを通る通信に限定することを含んでよい。第1のコンテナ内のものと類似した又は匹敵するソフトウェア及び／又はプロセスが、第2のコンテナ内で実行されて、第2のコンテナ内に記憶されたネットワークマップに従って、アクセスノードとネットワークバスとの間の通信を容易にすることができる。

【0130】

例示的な組み合わせ及び更なる実施例

このセクションは、コンピュータネットワークのマッピングを分かり難くする方法及び装置の更なる態様及び特徴を説明するが、かかるシステム及び方法は、非限定的に、一連の段落として提示され、一連の段落の一部又は全部は、明確性及び有効性のために英数字で指定され得る。これらの段落の各々は、任意の好適な方法で、1以上の他の段落と且つ／又は本出願の他の部分の開示と組み合わせることができる。以下の段落の幾つかは、明示的に他の段落に言及し、更に他の段落を限定することにより、非限定的に、好適な組み合わせの幾つかの例を提供するものである。

【0131】

A0.

航空ネットワークのマッピングを分かり難くする方法であって、

ネットワークモジュールを、外部アクセスノードと航空ネットワークのアビオニクスバスとの間に動作可能に接続することであって、外部アクセスノードとアビオニクスバスとの間の全ての通信が、ネットワークモジュールを通過する、ネットワークモジュールを、外部アクセスノードと航空ネットワークのアビオニクスバスとの間に動作可能に接続すること、

アビオニクスバスの少なくとも第1の部分の構成要素の第1の組向けのネットワークアドレスを特定する第1のネットワークマップを生成すること、

第1のネットワークマップをネットワークモジュールに読み込むこと、

ネットワークモジュールの第1のネットワークマップを、外部アクセスノードにとってアクセス可能にすること、

航空ネットワークの少なくとも第2の部分の構成要素の第2の組向けのネットワークアドレスを特定する少なくとも第2のネットワークマップを生成することであって、第2のネットワークマップが、第1のネットワークマップとは異なる、第2のネットワークマップを生成すること、

第2のネットワークマップをネットワークモジュールに読み込むこと、及び

外部アクセスノードにとってアクセス可能なネットワークマップを、第1のネットワークマップから第2のネットワークマップに変更することを含む、方法。

A1.

少なくとも第1の仮想環境と第2の仮想環境を生成すること、

第1のネットワークマップを第1の仮想環境内に記憶すること、及び

第2のネットワークマップを第2の仮想環境内に記憶することを更に含み、

10

20

30

40

50

第1のネットワークマップをネットワークモジュールに読み込むことが、第1のネットワークマップを記憶した第1の仮想環境をネットワークモジュールに読み込むことを含み、第2のネットワークマップをネットワークモジュールに読み込むことが、第2のネットワークマップを記憶した第2の仮想環境をネットワークモジュールに読み込むことを含む、段落A0に記載の方法。

A2.

アビオニクスバスと外部アクセスノードとの間の通信を、第1の仮想環境を通る通信に限定することを更に含む、段落A1に記載の方法。

A3.

外部アクセスノードにとってアクセス可能なネットワークマップを、第1のネットワークマップから第2のネットワークマップに変更することが、外部アクセスノードの第1の仮想環境との通信を排除すること、及び外部アクセスノードの第2の仮想環境との通信を確立することを含む、段落A2に記載の方法。

10

A4.

外部アクセスノードにとってアクセス可能なネットワークマップを、第1のネットワークマップから第2のネットワークマップに変更することが、ネットワークモジュールで、第1のネットワークマップを記憶した第1の仮想環境を、第2のネットワークマップを記憶した第2の仮想環境で置き換えることを含む、段落A2又はA3に記載の方法。

A5.

第1の仮想環境と第2の仮想環境のそれぞれが、コンテナである、段落A1からA4のいずれか1つに記載の方法。

20

A6.

第1の仮想環境と第2の仮想環境のそれぞれが、仮想マシンである、段落A1からA5のいずれか1つに記載の方法。

A7.

第1のネットワークマップを記憶した第1の仮想環境をネットワークモジュールに読み込むことが、第1の仮想環境を、ネットワークモジュールのアビオニクス区画からネットワークモジュールの外部区画に読み込むことを含み、該方法が、モジュールのアビオニクス区画と外部区画との間のデータの流れを、アビオニクス区画から外部区画への単一方向のデータの流れに限定することを更に含む、段落A1からA6のいずれか1つに記載の方法。

30

A8.

モジュールのアビオニクス区画と外部区画との間のデータの流れを、単一方向のデータの流れに限定することが、データダイオードを通してアビオニクス区画から外部区画にデータを送信することを含む、段落A7に記載の方法。

A9.

第1の仮想環境と第2の仮想環境を含む複数のN個の仮想環境を生成することを更に含み、Nは2より大きい整数である、段落A1からA8のいずれか1つに記載の方法。

A10.

外部アクセスノードにとってアクセス可能な、複数の仮想環境のうちの仮想環境を交替させることを更に含む、段落A9に記載の方法。

40

A11.

外部アクセスノードにとってアクセス可能なネットワークマップを変更することが、少なくとも第1の所定の基準を満たしたことに応答して、外部アクセスノードにとってアクセス可能なネットワークマップを変更することを含む、段落A0からA10のいずれか1つに記載の方法。

A12.

外部アクセスノードにとってアクセス可能なネットワークマップを変更するための少なくとも第1の所定の基準が、外部アクセスノードにとってアクセス可能なネットワークマップを変更するための固定された基準を含む、段落A11に記載の方法。

50

A 1 3 .

固定された基準が、設定された期間である、段落 A 1 2 に記載の方法。

A 1 4 .

固定された基準が、第 1 のネットワークマップと第 2 のネットワークマップを含むネットワークマップの組の所定のシーケンスである、段落 A 1 2 又は A 1 3 に記載の方法。

A 1 5 .

固定された基準が、航空機の所定の地理的位置である、段落 A 1 2 から A 1 4 のいずれか 1 つに記載の方法。

A 1 6 .

外部アクセスノードにとってアクセス可能なネットワークマップを変更するための少なくとも第 1 の所定の基準が、外部アクセスノードにとってアクセス可能なネットワークマップを変更するためのランダムな基準を含む、段落 A 1 1 から A 1 5 のいずれか 1 つに記載の方法。

A 1 7 .

ランダムな基準が、変動する期間を含む、段落 A 1 6 に記載の方法。

A 1 8 .

外部アクセスノードにとってアクセス可能なネットワークマップを変更するための少なくとも第 1 の所定の基準が、航空ネットワークのセキュリティの相対的なレベルに少なくとも部分的に基づく、段落 A 1 1 から A 1 7 のいずれか 1 つに記載の方法。

【 0 1 3 2 】

B 0 .

航空ネットワークのマッピングを分かり難くするためのネットワークモジュールであって、

ネットワークモジュールが、航空ネットワークと動作可能に接続され、

航空ネットワークのアビオニクスバスと外部アクセスノードとの間に動作可能に配置され、外部アクセスノードとアビオニクスバスとの間の全ての通信が、ネットワークモジュールを通過し、

航空ネットワークの少なくとも第 1 の部分の構成要素の第 1 の組向けのネットワークアドレスを特定する第 1 のネットワークマップを生成し、

ネットワークモジュールの第 1 のネットワークマップを、外部アクセスノードにとってアクセス可能にし、

航空ネットワークの少なくとも第 2 の部分の構成要素の第 2 の組向けのネットワークアドレスを特定する第 2 のネットワークマップを生成することであって、第 2 のネットワークマップが、第 1 のネットワークマップとは異なる、第 2 のネットワークマップを生成し、

外部アクセスノードにとってアクセス可能なネットワークマップを、第 1 のネットワークマップから第 2 のネットワークマップに変更するように構成されている、ネットワークモジュール。

B 1 .

ネットワークモジュールが、

少なくとも第 1 の仮想環境と第 2 の仮想環境を生成し、

第 1 のネットワークマップを第 1 の仮想環境内に記憶し、

第 1 の仮想環境を外部アクセスノードにとってアクセス可能にし、

第 2 のネットワークマップを第 2 の仮想環境内に記憶し、

外部アクセスノードにとってアクセス可能な仮想環境を、第 1 の仮想環境から第 2 の仮想環境に変更するように構成されている、段落 B 0 に記載のネットワークモジュール。

B 2 .

第 1 の区画と第 2 の区画を備え、

第 1 の区画が、航空ネットワークと動作可能に接続され、且つ、少なくとも第 1 の仮想環境と第 2 の仮想環境を生成し、第 1 のネットワークマップを記憶した第 1 の仮想環境を

10

20

30

40

50

第2の区画に読み込み、アビオニクスバスと外部アクセスノードとの間の通信を行わないように構成され、

第2の区画が、アビオニクスバスと外部ノードとの間に動作可能に配置されるように構成されている、段落B1に記載のネットワークモジュール。

B3.

第2の区画が、外部アクセスノードの第1の仮想環境との通信を排除し、外部アクセスノードの第2の仮想環境との通信を確立するように構成されている、段落B2に記載のネットワークモジュール。

B4.

第1の区画が、第2の区画で、第1のネットワークマップを記憶した第1の仮想環境を、第2のネットワークマップを記憶した第2の仮想環境で置き替えるように構成されている、段落B2又はB3に記載のネットワークモジュール。

B5.

第1の仮想環境と第2の仮想環境のそれぞれが、コンテナである、段落B1からB4のいずれか1つに記載のネットワークモジュール。

B6.

ネットワークモジュールが、外部アクセスノードにとってアクセス可能なコンテナを交替させるように構成されている、段落B5に記載のネットワークモジュール。

B7.

第1の仮想環境と第2の仮想環境のそれぞれが、仮想マシンである、段落B1からB6のいずれか1つに記載のネットワークモジュール。

B8.

ネットワークモジュールが、少なくとも第1の所定の基準を満たしたことに応答して、外部アクセスノードにとってアクセス可能なネットワークマップを変更するように構成されている、段落B0からB7のいずれか1つに記載のネットワークモジュール。

B9.

外部アクセスノードにとってアクセス可能なネットワークマップを変更するための少なくとも第1の所定の基準が、外部アクセスノードにとってアクセス可能なネットワークマップを変更するための固定された基準を含む、段落B8に記載のネットワークモジュール。

B10.

固定された基準が、設定された期間である、段落B9に記載のネットワークモジュール。

B11.

固定された基準が、第1のネットワークマップと第2のネットワークマップを含むネットワークマップの組の所定のシーケンスである、段落B9又はB10に記載のネットワークモジュール。

B12.

固定された基準が、航空ネットワークを有する航空機の所定の地理的位置である、段落9からB11のいずれか1つに記載のネットワークモジュール。

B13.

外部アクセスノードにとってアクセス可能なネットワークマップを変更するための少なくとも第1の所定の基準が、外部アクセスノードにとってアクセス可能なネットワークマップを変更するためのランダムな基準を含む、段落B8からB12のいずれか1つに記載のネットワークモジュール。

B14.

ランダムな基準が、変動する期間を含む、段落B13に記載のネットワークモジュール。

B15.

外部アクセスノードにとってアクセス可能なネットワークマップを変更するための少なくとも第1の所定の基準が、航空ネットワークのセキュリティの相対的なレベルに少なくとも部分的に基づく、段落B8からB14のいずれか1つに記載のネットワークモジュール。

10

20

30

40

50

B 1 6 .

第 1 の区画と第 2 の区画を備え、第 1 の区画が、航空ネットワークと動作可能に接続され、且つ、第 1 のネットワークマップを記憶した第 1 の仮想環境を第 1 の区画から第 2 の区画に読み込むように構成され、第 2 の区画が、アビオニクスバスと外部ノードとの間に動作可能に配置されるように構成され、ネットワークモジュールが、第 1 の区画と第 2 の区画との間のデータの流れを、第 1 の区画から第 2 の区画への単一方向のデータの流れに限定するように構成されている、段落 B 1 から B 1 5 のいずれか一項に記載のネットワークモジュール。

B 1 7 .

第 1 の区画と第 2 の区画との間のデータの流れを、第 1 の区画から第 2 の区画への単一方向のデータの流れに限定するデータダイオードを更に備える、段落 B 1 6 に記載のネットワークモジュール。

【 0 1 3 3 】

C 0 .

航空機の航空ネットワークのネットワークマッピングを分かり難くするためのシステムであって、

航空ネットワークの少なくとも第 1 の部分のネットワーク構成要素向けのネットワークアドレスを特定する第 1 のネットワークマップを含む第 1 のコンテナ、

航空ネットワークの少なくとも第 2 の部分のネットワーク構成要素向けのネットワークアドレスを特定する第 2 のネットワークマップを含む第 2 のコンテナであって、第 2 のネットワークマップが、第 1 のネットワークマップとは異なる、第 2 のコンテナ、及び

航空ネットワークのアビオニクスバスと外部アクセスノードとの間に第 1 のコンテナを配置するように構成された切り替えデバイスであって、少なくとも第 1 の基準に応じて、外部アクセスノードにとってアクセス可能なネットワークマップを、第 1 のネットワークマップから第 2 のネットワークマップに変更するために、第 1 のコンテナをアビオニクスバスと外部アクセスノードとの間に配置された第 2 のコンテナで置き替える、切り替えデバイスを備える、システム。

C 1 .

外部アクセスノードにとってアクセス可能なネットワークマップを第 1 のネットワークマップから第 2 のネットワークマップに変更するための少なくとも第 1 の基準が、固定された基準を含む、段落 C 0 に記載のシステム。

C 2 .

外部アクセスノードにとってアクセス可能なネットワークマップを第 1 のネットワークマップから第 2 のネットワークマップに変更するための少なくとも第 1 の基準が、ランダムな基準を含む、段落 C 0 又は C 1 に記載のシステム。

C 3 .

切り替えデバイスを含む安全区画、

外部アクセスノードにとってアクセス可能な外部区画、及び

安全区画から外部区画への単一方向のデータの流れを提供するデータダイオードを更に備える、段落 C 0 から C 2 のいずれか 1 つに記載のシステム。

C 4 .

切り替えデバイスが、動作の第 1 のモードと第 1 のモードとは異なる動作の第 2 のモードを有し、第 1 のモードと第 2 のモードが、セキュリティの異なるレベルを提供するように構成されている、段落 C 0 から C 3 のいずれか 1 つに記載のシステム。

C 5 .

システムが、ホストマシンで動作し且つ第 1 のコンテナと第 2 のコンテナを実行するコンテナ管理者を含む、段落 C 0 から C 4 のいずれか 1 つに記載のシステム。

C 6 .

ホストマシンが、切り替えデバイスを含む安全区画、及びコンテナ管理者を含む外部区画を有する、段落 C 5 に記載のシステム。

10

20

30

40

50

C 7 .

安全区画と外部区画との間で、安全区画から外部区画への単一方向のデータの流れのみが許容される、段落 C 6 に記載のシステム。

C 8 .

単一方向のデータの流れを提供するデータダイオードを更に備える、段落 C 7 に記載のシステム。

C 9 .

システムが、ネットワークゲートウェイとして構成されている、段落 C 0 から C 8 のいずれか 1 つに記載のシステム。

C 10 .

システムが、プロキシサーバである、段落 C 0 から C 9 のいずれか 1 つに記載のシステム。

C 11 .

各コンテナが、ネットワークゲートウェイとして構成されている、段落 C 0 から C 10 のいずれか 1 つに記載のシステム。

C 12 .

第 1 のネットワークマップと第 2 のネットワークマップを生成するように構成されたランダム化エンジンを更に備える、段落 C 0 から C 11 のいずれか 1 つに記載のシステム。

【 0 1 3 4 】

D 0 .

航空ネットワークのネットワークマッピングを分かり難くするための中間ネットワークゲートウェイであって、

外部ネットワークアクセスポイントとアビオニクスバスとの間の航空ネットワーク内に動作可能に配置されるように構成された外部区画であって、

それぞれが関連付けられた異なるネットワークマップを含む複数のコンテナ、及び複数のコンテナで実行されるコンテナ管理者を含む、外部区画、並びに

外部区画とデータ通信する安全区画であって、複数のコンテナから起動コンテナを選択するように構成された切り替えデバイスを含み、起動コンテナが、外部ネットワークアクセスポイントとアビオニクスバスとの間のプロキシサーバとして作用し、外部ネットワークアクセスポイントに関連付けられたネットワークマップを提供する、安全区画を備える、中間ネットワークゲートウェイ。

D 1 .

切り替えデバイスが、交替する基準で、複数のコンテナの中から起動コンテナを選択する、段落 D 0 に記載の中間ネットワークゲートウェイ。

D 2 .

安全区画が、ランダムな基準で種々のネットワークマップを生成する切り替えデバイスと動作可能に接続されたランダム化エンジンを更に含む、段落 D 0 又は D 1 に記載の中間ネットワークゲートウェイ。

D 3 .

安全区画が、ランダム化エンジンと動作可能に接続され且つ複数のコンテナを生成するように構成されたコンテナ生成器を更に含む、段落 D 2 に記載の中間ネットワークゲートウェイ。

【 0 1 3 5 】

利点、特徴、及び便益

本明細書で説明されている方法及び装置の種々の実施例は、サイバーアタックからコンピュータネットワークを保護するための既知の解決策より優れた幾つかの利点を提供する。例えば、本明細書で説明されている例示的な実施例は、許可されていない侵入が生じる前に、予備調査段階での攻撃を未然に防ぐ。

【 0 1 3 6 】

更に、他の便益の中で、本明細書で説明される例示的な実施例は、攻撃者に分かり難く

10

20

30

40

50

するモジュールの存在を警告することなしに、攻撃を未然に防ぐことを可能にする。

【0137】

更に、他の便益の中で、本明細書で説明されている例示的な実施例は、複数の予め設定される動的な変数に基づいて、セキュリティレベルを選択することを可能にする。

【0138】

更に、他の便益の中で、本明細書で説明されている例示的な実施例は、分かり難くするモジュールを直接的な攻撃から保護する。

【0139】

既知のシステム又はデバイスは、特にそのような制限された処理要求を伴って、これらの機能を実行することができない。したがって、本明細書で説明されている例示的な実施例は、航空機などの輸送体上のネットワークにとって特に有用である。しかし、本明細書で説明されている全ての実施例が、同じ利点又は同一程度の利点を提供する訳ではない。

【0140】

結論

上述の開示は、個別の有用性を備えた複数の個々の実施例を包括し得る。これらの発明の各々は、その好ましい形態（複数可）で開示されているが、数多くの変形例が可能であることから、本書で開示され例示されているそれらの特定の実施例を限定的な意味で捉えるべきではない。本開示内で使用されている限り、項の見出しは構成上の目的のものに過ぎない。本開示の主題は、本書に記載の様々な要素、特徴、機能、及び／又は特性の、新規的かつ非自明の組み合わせ及び部分的組み合わせの全てを含む。下記の特許請求の範囲は、新規的かつ進歩的であると見なされる、ある組み合わせ及び部分的組み合わせを特に指し示すものである。特徴、機能、要素、及び／又は特性のその他の組み合わせ及び部分的組み合わせは、この出願又は関連出願からの優先権を主張する出願において特許請求され得る。更に、そのような特許請求の範囲は、出願当初の特許請求の範囲より広いか、狭いか、等しいか、又はそれと異なるかにかかわらず、本開示の主題の範囲内に含まれるとみなされる。

10

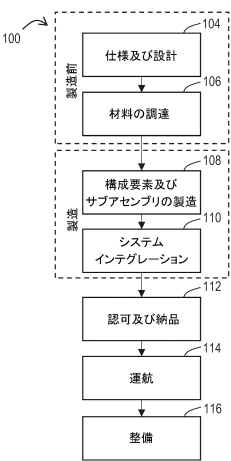
20

30

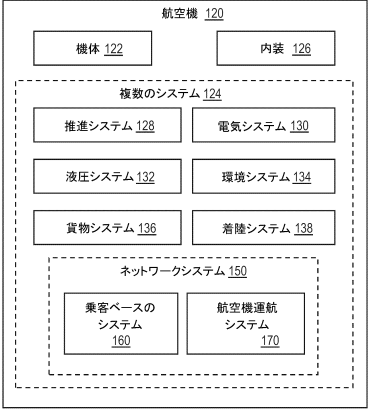
40

50

【図面】
【図 1】

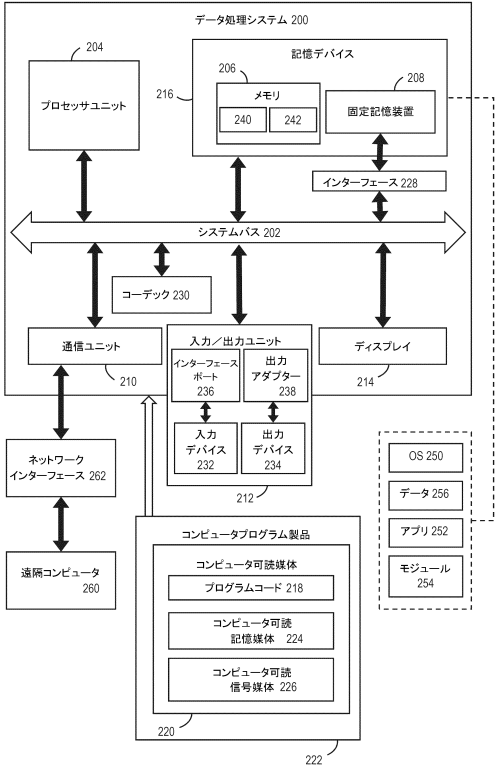


【図 2】

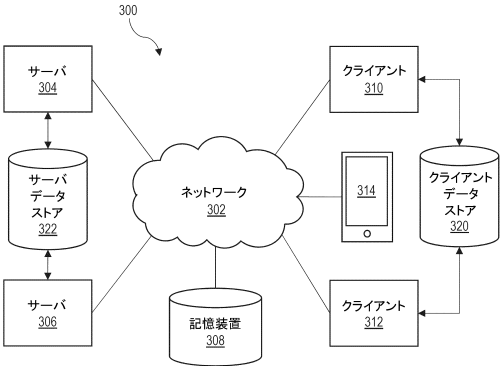


10

【図 3】



【図 4】



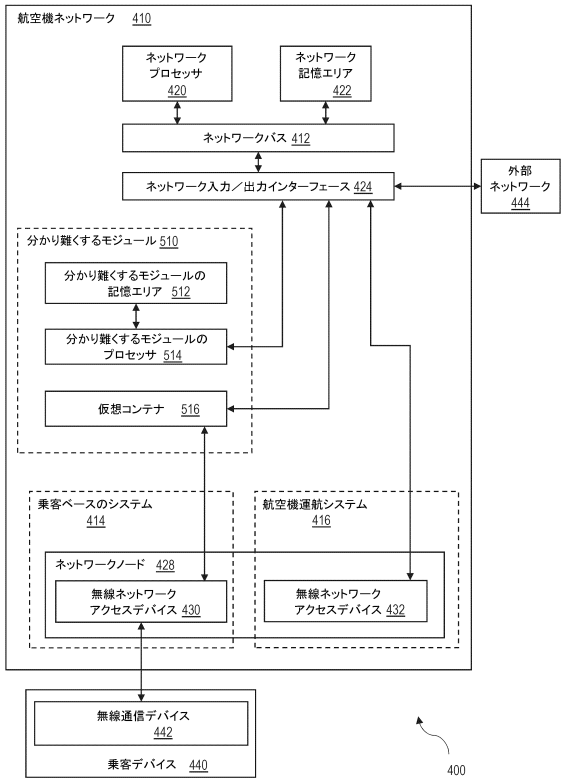
20

30

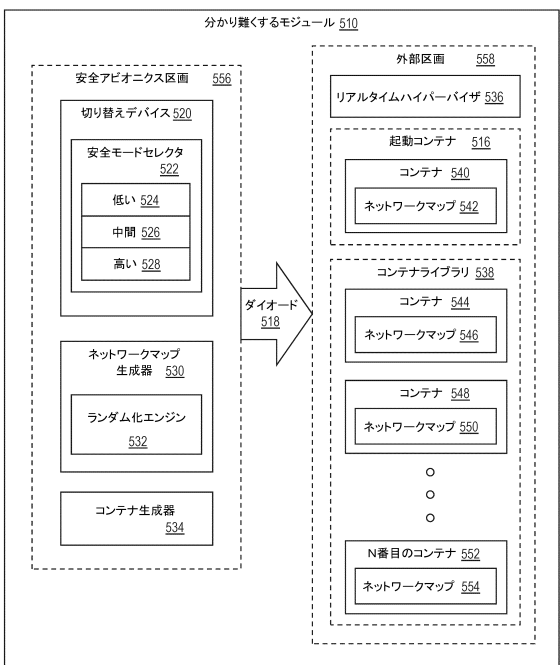
40

50

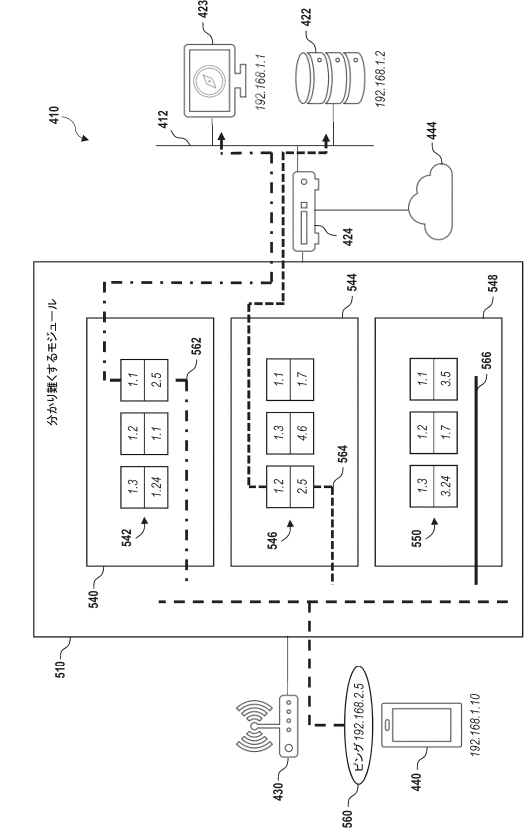
【図 5】



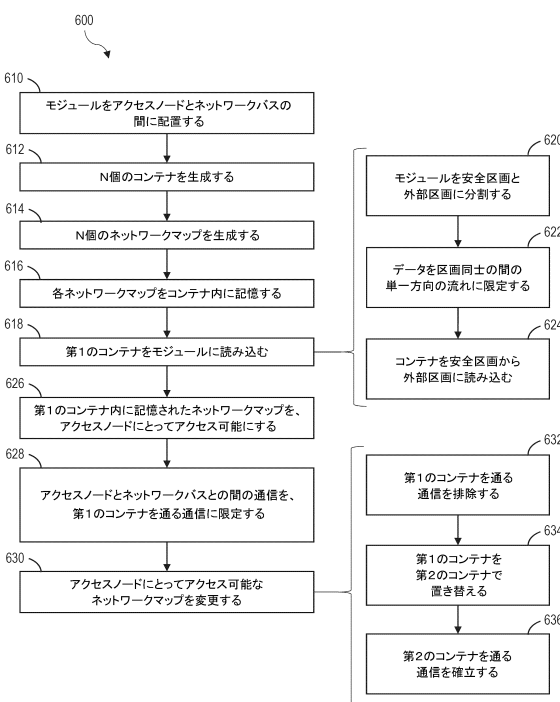
【図 6】



【図 7】



【図 8】



10

20

30

40

50

フロントページの続き

(51)国際特許分類
H 0 4 L 61/106(2022.01) F I
H 0 4 L 41/40
H 0 4 L 61/106

イド プラザ 1 0 0
(72)発明者 ウィリアムズ, アドニス
アメリカ合衆国 イリノイ 6 0 6 0 6 - 2 0 1 6, シカゴ, ノース リバーサイド プラザ 1 0 0
審査官 前田 健人
(56)参考文献 中国特許出願公開第1 0 9 0 7 6 3 3 8 (C N, A)
米国特許第0 9 0 4 3 9 3 8 (U S, B 1)
中国特許出願公開第1 0 1 5 2 3 8 5 4 (C N, A)
米国特許出願公開第2 0 1 0 / 0 0 1 4 5 3 7 (U S, A 1)
特開2 0 1 0 - 0 6 8 3 0 6 (J P, A)
(58)調査した分野 (Int.Cl., D B名)
H 0 4 L 1 2 / 2 2 - 1 2 / 6 6
H 0 4 L 4 1 / 0 0 - 4 1 / 5 0 7 4
H 0 4 L 6 1 / 0 0 - 6 1 / 5 9