

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7468652号
(P7468652)

(45)発行日 令和6年4月16日(2024.4.16)

(24)登録日 令和6年4月8日(2024.4.8)

(51)国際特許分類		F I	
G 0 6 F	21/55 (2013.01)	G 0 6 F	21/55
G 0 6 F	11/07 (2006.01)	G 0 6 F	11/07 1 9 3
		G 0 6 F	11/07 1 4 0 A
請求項の数 12 (全24頁)			
(21)出願番号	特願2022-532217(P2022-532217)	(73)特許権者	000004237 日本電気株式会社 東京都港区芝五丁目7番1号
(86)(22)出願日	令和2年6月26日(2020.6.26)	(74)代理人	100141519 弁理士 梶田 邦之
(86)国際出願番号	PCT/JP2020/025306	(72)発明者	羽角 太地 東京都港区芝五丁目7番1号 日本電気株式会社内
(87)国際公開番号	WO2021/260932	(72)発明者	島 成佳 東京都港区芝五丁目7番1号 日本電気株式会社内
(87)国際公開日	令和3年12月30日(2021.12.30)	審査官	児玉 崇晶
審査請求日	令和4年12月21日(2022.12.21)		
		最終頁に続く	

(54)【発明の名称】 分散システム、通信端末、機能復旧方法、及びプログラム

(57)【特許請求の範囲】

【請求項1】

1以上の通信端末と1以上のストレージデバイスとエッジサーバとがネットワークを介して通信する分散システムであって、

前記通信端末は、異常動作状態にある機能モジュールを検知し、前記エッジサーバへ前記異常動作状態を通知し、

前記エッジサーバは、前記機能モジュール及び関連機能モジュールのそれぞれに対応するイメージファイルを生成し、前記生成されたイメージファイルを分割した複数の分割イメージファイルを生成して、前記複数の分割イメージファイルを前記ストレージデバイスへ送信し、

前記ストレージデバイスは、前記分割イメージファイルを格納し、前記通信端末からの要求に応じて、前記機能モジュール及び前記関連機能モジュールに対応する分割イメージファイルを前記通信端末へ送信し、

前記通信端末は、前記ストレージデバイスから取得した前記複数の分割イメージファイルを結合して前記イメージファイルを生成し、前記生成されたイメージファイルに基づいて前記機能モジュール及び前記関連機能モジュールを起動する、ことを特徴とする分散システム。

【請求項2】

前記通信端末は、前記異常動作状態にある機能モジュールを検知すると、前記機能モジュール及び前記関連機能モジュールの動作を停止させ、前記機能モジュール及び前記関連

機能モジュールを廃棄することを特徴とする請求項 1 に記載の分散システム。

【請求項 3】

前記通信端末は、前記異常動作状態にある機能モジュールを検知すると、前記異常動作状態の内容を示すインシデントレポートを前記エッジサーバへ送信することを特徴とする請求項 1 または 2 に記載の分散システム。

【請求項 4】

前記エッジサーバは、前記インシデントレポートの内容にマッチする更新ポリシーに応じて、前記イメージファイルを生成することを特徴とする請求項 3 に記載の分散システム。

【請求項 5】

前記通信端末は、前記 1 以上のストレージデバイスのうち、前記通信端末の近隣に存在するストレージデバイスから、前記分割イメージファイルを取得することを特徴とする請求項 1 乃至 4 のいずれか 1 項に記載の分散システム。

10

【請求項 6】

前記近隣のストレージデバイスは、前記通信端末と通信リンクを直接確立することができるストレージデバイスであることを特徴とする請求項 5 に記載の分散システム。

【請求項 7】

前記近隣のストレージデバイスは、前記通信端末に対するホップ数に応じて決定されることを特徴とする請求項 5 に記載の分散システム。

【請求項 8】

前記エッジサーバは、前記複数の分割イメージファイルを、予め設定されたグループ内に含まれる複数のストレージデバイスに送信することを特徴とする請求項 1 乃至 7 のいずれか 1 項に記載の分散システム。

20

【請求項 9】

前記通信端末は、前記複数の分割イメージファイルのそれぞれを並列でダウンロードすることを特徴とする請求項 1 乃至 8 のいずれか 1 項に記載の分散システム。

【請求項 10】

分散システムを構成する通信端末であって、
複数の機能モジュールの動作状態を診断し、異常動作状態にある機能モジュールを検知するモジュール診断手段と、
前記異常動作状態にある機能モジュールの動作を停止させ、前記機能モジュールを廃棄するモジュール廃棄手段と、
前記機能モジュールに対応し、前記異常動作状態を解消するように生成されたイメージファイルを分割した複数の分割イメージファイルを取得し、前記複数の分割イメージファイルを結合する分割イメージファイル結合手段と、
前記複数の分割イメージファイルを結合して生成されたイメージファイルに基づいて、前記機能モジュールを起動するモジュール起動手段と
を備えることを特徴とする通信端末。

30

【請求項 11】

1 以上の通信端末と 1 以上のストレージデバイスとエッジサーバとがネットワークを介して通信する分散システムの機能復旧方法であって、

40

前記通信端末が、異常動作状態にある機能モジュールを検知し、前記エッジサーバへ前記異常動作状態を通知する通知ステップと、

前記エッジサーバが、前記機能モジュール及び関連機能モジュールのそれぞれに対応するイメージファイルを生成し、前記生成されたイメージファイルを分割した複数の分割イメージファイルを生成して、前記複数の分割イメージファイルを前記ストレージデバイスへ送信する第 1 の送信ステップと、

前記ストレージデバイスが、前記分割イメージファイルを格納し、前記通信端末からの要求に応じて、前記機能モジュール及び前記関連機能モジュールに対応する分割イメージファイルを前記通信端末へ送信する第 2 の送信ステップと、

前記通信端末が、前記ストレージデバイスから取得した前記複数の分割イメージファイ

50

ルを結合して前記イメージファイルを生成し、前記生成されたイメージファイルに基づいて前記機能モジュール及び前記関連機能モジュールを起動する起動ステップとを含むことを特徴とする機能復旧方法。

【請求項 12】

コンピュータを請求項 10 に記載の通信端末として機能させるためのプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、異常動作状態となった通信端末の機能を復旧させることができる分散システム、通信端末、機能復旧方法、及びプログラムに関する。

10

【背景技術】

【0002】

近年、I o T (Internet of Things) やサイバーフィジカルシステムなど、分散システムの社会的な実装が進んでいる。分散システムでは、多数の通信端末が、同じ分散システム内の他の端末と有線または無線ネットワークを介して接続するように構成される。一般に、分散システムを構成する通信端末は、コスト等の観点から必要最低限の計算資源やストレージしか持たない。また、当該通信端末は、インターネットやクラウドサーバとの接続も低速度の通信経路しか持たないか、あるいは、分散システム内の特定の端末（例えば、エッジサーバなど）との通信しか行わない。

【0003】

20

このような通信端末が、分散システム外部からの攻撃により設計上または運用上意図しない動作状態となった場合（例えば、ボットへの感染や攻撃者のコントロール下に置かれたような場合）、オペレーターは当該通信端末を分散システムから除外し、代替として、正常な機能を提供する代替の通信端末を配置する必要がある。また、通信端末が公共空間に配置され、当該通信端末の機能停止が社会的またはコスト的に大きな影響を与える場合には、正常な機能の提供を早急に再開しなくてはならない。

【0004】

特許文献 1 には、I o T におけるデバイスがハッキングなどの攻撃を受け、不正なアプリケーションや不正なファイルが当該デバイスの領域に導入された場合、当該領域を再起動し、不正なアプリケーションや不正なファイルを削除することで、当該領域の修復を行うことが記載されている。

30

【0005】

—また、Microsoft 社の Branch Cache（登録商標）は、ファイルの分散キャッシュに関し、かかる技術によると、一度、デバイスがサーバからコンテンツを入手すれば、当該デバイスが入手したコンテンツを近隣のデバイスも当該デバイスから入手できるようにして、ネットワーク帯域を低減させることができる。

【先行技術文献】

【特許文献】

【0006】

【文献】特開 2019-057167 号公報

40

【発明の概要】

【発明が解決しようとする課題】

【0007】

しかしながら、端末数の増加、物理的な距離、及び通信帯域などの要因により、オペレーターによる対応では、分散システムの迅速な機能復旧は困難である。上記特許文献 1 も、このような問題については言及していない。

【0008】

本発明の目的は、分散システムを構成する通信端末が、設計上または運用上の意図とは異なる動作状態となった場合に、迅速な機能復旧を可能にする分散システム、通信端末、機能復旧方法、及びプログラムを提供することにある。

50

【課題を解決するための手段】

【0009】

本発明の一態様による分散システムは、1以上の通信端末と1以上のストレージデバイスとエッジサーバとがネットワークを介して通信する分散システムであって、前記通信端末は、異常動作状態にある機能モジュールを検知し、前記エッジサーバへ前記異常動作状態を通知し、前記エッジサーバは、前記機能モジュール及び関連機能モジュールのそれぞれに対応するイメージファイルを生成し、前記生成されたイメージファイルを分割した複数の分割イメージファイルを生成して、前記複数の分割イメージファイルを前記ストレージデバイスへ送信し、前記ストレージデバイスは、前記分割イメージファイルを格納し、前記通信端末からの要求に応じて、前記機能モジュール及び前記関連機能モジュールに対応する分割イメージファイルを前記通信端末へ送信し、前記通信端末は、前記ストレージデバイスから取得した前記複数の分割イメージファイルを結合して前記イメージファイルを生成し、前記生成されたイメージファイルに基づいて前記機能モジュール及び前記関連機能モジュールを起動する、ことを特徴とする。

10

【0010】

本発明の一態様による通信端末は、分散システムを構成する通信端末であって、複数の機能モジュールの動作状態を診断し、異常動作状態にある機能モジュールを検知するモジュール診断手段と、前記異常動作状態にある機能モジュールの動作を停止させ、前記機能モジュールを廃棄するモジュール廃棄手段と、前記機能モジュールに対応し、前記異常動作状態を解消するように生成されたイメージファイルを分割した複数の分割イメージファイルを取得し、前記複数の分割イメージファイルを結合する分割イメージファイル結合手段と、前記複数の分割イメージファイルを結合して生成されたイメージファイルに基づいて、前記機能モジュールを起動するモジュール起動手段とを備えることを特徴とする。

20

【0011】

本発明の一態様による機能復旧方法は、1以上の通信端末と1以上のストレージデバイスとエッジサーバとがネットワークを介して通信する分散システムの機能復旧方法であって、前記通信端末が、異常動作状態にある機能モジュールを検知し、前記エッジサーバへ前記異常動作状態を通知する通知ステップと、前記エッジサーバが、前記機能モジュール及び関連機能モジュールのそれぞれに対応するイメージファイルを生成し、前記生成されたイメージファイルを分割した複数の分割イメージファイルを生成して、前記複数の分割イメージファイルを前記ストレージデバイスへ送信する第1の送信ステップと、前記ストレージデバイスが、前記分割イメージファイルを格納し、前記通信端末からの要求に応じて、前記機能モジュール及び前記関連機能モジュールに対応する分割イメージファイルを前記通信端末へ送信する第2の送信ステップと、前記通信端末が、前記ストレージデバイスから取得した前記複数の分割イメージファイルを結合して前記イメージファイルを生成し、前記生成されたイメージファイルに基づいて前記機能モジュール及び前記関連機能モジュールを起動する起動ステップとを含むことを特徴とする。

30

【0012】

本発明の一態様によるプログラムは、コンピュータを上記通信端末として機能させる。

【発明の効果】

40

【0013】

本発明によれば、分散システムを構成する通信端末が、設計上または運用上の意図とは異なる動作状態となった場合に、迅速な機能復旧を可能にする分散システム、通信端末、機能復旧方法、及びプログラムを提供することが可能になる。なお、本発明により、当該効果の代わりに、又は当該効果とともに、他の効果が奏されてもよい。

【図面の簡単な説明】

【0014】

【図1】第1の実施形態に係る分散システムの概要図である。

【図2】第1の実施形態に係る通信端末のモジュール構成図である。

【図3】第1の実施形態に係る通信端末の機能構成図である。

50

【図４】第１の実施形態に係るストレージデバイスの機能構成図である。

【図５】第１の実施形態に係るエッジサーバの機能構成図である。

【図６】第１の実施形態に係る通信端末の動作例を示すフローチャートである。

【図７】第１の実施形態に係るシステム情報の例を示す図である。

【図８】第１の実施形態に係るシステム情報の例を示す図である。

【図９】第１の実施形態に係るシステム情報の例を示す図である。

【図１０】第１の実施形態に係る分割イメージファイル情報の例を示す図である。

【図１１】第１の実施形態に係るストレージデバイスの動作例を示すフローチャートである。

【図１２】第１の実施形態に係るエッジサーバの動作例を示すフローチャートである。

10

【図１３】第１の実施形態に係るインシデントレポートの例を示す図である。

【図１４】第１の実施形態に係る更新ポリシーの例を示す図である。

【図１５】第１の実施形態に係るコンピュータのハードウェア構成例を示す概略ブロック図である。

【図１６】第２の実施形態に係る分散システムの概要図である。

【発明を実施するための形態】

【００１５】

以下、添付の図面を参照して本発明の実施形態を詳細に説明する。なお、本明細書及び図面において、同様に説明されることが可能な要素については、同一の符号を付することにより重複説明が省略され得る。

20

【００１６】

説明は、以下の順序で行われる。

１．第１の実施形態

１．１．システムの構成

１．２．通信端末の構成

１．３．ストレージデバイスの構成

１．４．エッジサーバの構成

１．５．通信端末の動作例

１．６．ストレージデバイスの動作例

１．７．エッジサーバの動作例

１．８．ハードウェア構成

１．９．技術的特徴

２．第２の実施形態

２．１．システムの構成

２．２．動作例

30

【００１７】

<<１．第１の実施形態>>

<１．１．システムの構成>

図１は、第１の実施形態に係る分散システムの概要図である。

【００１８】

40

分散システム１００は、１以上の通信端末１０１と、１以上のストレージデバイス１０２と、１以上のエッジサーバ１０３とを含む。図中の実線は接続経路を示し、通信端末１０１、ストレージデバイス１０２、及びエッジサーバ１０３は、図中の実線で示されるように、有線または無線ネットワークを介して通信可能に接続されている。また、通信端末１０１、ストレージデバイス１０２、及びエッジサーバ１０３の間には、１以上の障害物１０４が存在し得る。エッジサーバ１０３は、クラウドコンピューティングを実現するクラウドサーバ１０５にも接続され得る。分散システムは、サイバーフィジカルシステム（Cyber Physical System）であってもよい。また、通信端末１０１は、センサーなどを備えたＩｏＴを構成する端末とすることができる。エッジサーバ１０３は、データを生成する通信端末１０１の近傍において、生成されたデータの処理を可能にするエッジコンピ

50

ューティングを実現することができる。通信端末１０１、ストレージデバイス１０２、及びエッジサーバ１０３の数は、図示された数に限定されない。各構成要素の詳細は、後述する。

【００１９】

< １．２．通信端末の構成 >

図２は、第１の実施形態に係る通信端末１０１のモジュール構成図である。モジュールとは、通信端末１０１の各機能を論理的に分離可能なソフトウェア、ハードウェア、またはそれらの組み合わせによって実装した部品を指す。モジュールは、機能モジュールとも称する。

【００２０】

図示されるように、通信端末１０１は、１以上のモジュール１～ｎを含む。通信端末１０１は、ホストＯＳ２０２のモジュール診断機能２０１によって、当該１以上のモジュール１～ｎの動作状態を診断することができる。具体的には、モジュール診断機能２０１は、後述するシステム情報に基づいて、１以上のモジュール１～ｎが設計上または運用上の意図とは異なる動作状態（以下、異常動作状態ともいう）にあるかどうかを判定することができる。

【００２１】

図３は、第１の実施形態に係る通信端末１０１の機能構成図である。図示されるように、通信端末１０１は、システム情報取得部３０１、システム情報記憶部３０２、モジュール診断部３０３、モジュール廃棄部３０４、インシデントレポート送信部３０５、分割イメージファイル取得部３０６、分割イメージファイル記憶部３０７、分割イメージファイル結合部３０８、及びモジュール起動部３０９を有する。

【００２２】

システム情報取得部３０１は、分散システム１００に関するシステム情報を、エッジサーバ１０３から取得する。

【００２３】

システム情報記憶部３０２は、システム情報取得部３０１によって取得された分散システム１００に関するシステム情報を保持する。

【００２４】

モジュール診断部３０３は、システム情報記憶部３０２に保持されたシステム情報に基づいて、通信端末１０１上で動作する各モジュールの動作状態を診断し、異常動作状態にあるモジュールを検知する。

【００２５】

モジュール廃棄部３０４は、モジュール診断部３０３によって検知された異常動作状態にあるモジュールを廃棄する。廃棄とは、通信端末１０１からの削除を意味する。モジュール廃棄部３０４は、対象のモジュールを、当該モジュールが使用したデータとともにモジュールごと通信端末１０１から削除する。また、廃棄の対象には、異常動作状態にあるモジュールだけでなく、当該モジュールに関連する関連モジュール（関連機能モジュールとも称する）も含まれる。

【００２６】

インシデントレポート送信部３０５は、異常動作状態にあるモジュールの名前、バージョン、違反ポリシータイプ、及びログなど、異常状態の内容を示すインシデント情報をインシデントレポートとして、エッジサーバ１０３へ送信する。インシデントレポートは、モジュールの異常動作状態を通知するために用いられる。なお、インシデントとは、セキュリティ上、脅威となる可能性がある事象を指す。

【００２７】

分割イメージファイル取得部３０６は、ストレージデバイス１０２から、対象のモジュールに対応する更新されたイメージファイルを分割した分割イメージファイルを取得する。分割イメージファイル取得部３０６は、通信端末１０１の近隣に存在する１以上のストレージデバイス１０２から、分割イメージファイルを取得してもよい。近隣に存在する１

10

20

30

40

50

以上のストレージデバイス１０２は、通信端末１０１と通信リンクを直接確立することができる１以上のストレージデバイス１０２とすることができる。或いは、近隣に存在する１以上のストレージデバイス１０２は、通信端末１０１に対するホップ数に応じて決定してもよい。例えば、通信端末１０１に対するホップ数が所定のホップ数以下であるかどうかを判定して、対象のストレージデバイス１０２を決定してよい。ホップ数とは、送信先と送信元との間で通過しなければならない中間デバイスの数を指す。また、分割イメージファイル取得部３０６は、複数の分割イメージファイルのそれぞれを並列でダウンロードしてもよい。

【００２８】

分割イメージファイル記憶部３０７は、分割イメージファイル取得部３０６によって取得された分割イメージファイルを保持する。

【００２９】

分割イメージファイル結合部３０８は、分割イメージファイル記憶部３０７から分割イメージファイルを取得し、全ての分割イメージファイルが揃ったイメージファイルについて分割イメージファイルを結合し、イメージファイルを生成する。

【００３０】

モジュール起動部３０９は、分割イメージファイル結合部３０８によって生成されたイメージファイルをもとに、モジュールを起動する。

【００３１】

なお、通信端末１０１は、これらの構成要素以外の他の構成要素をさらに含み得る。即ち、通信端末１０１は、これらの構成要素の動作以外の動作も行い得る。例えば、通信端末１０１は、不図示のセンサーを備え、センサーによって取得したデータをエッジサーバ１０３またはクラウドサーバ１０５に送信するように構成することができる。また、２つのエッジサーバ１０３が図示されているが、同じエッジサーバとすることができる。

【００３２】

<１．３．ストレージデバイスの構成>

図４は、第１の実施形態に係るストレージデバイス１０２の機能構成図である。図示されるように、ストレージデバイス１０２は、システム情報取得部４０１、システム情報記憶部４０２、分割イメージファイル受信部４０３、分割イメージファイル記憶部４０４、ファイル要求取得部４０５、分割イメージファイル検索部４０６、及び分割イメージファイル送信部４０７を有する。ストレージデバイス１０２は、分散システム１００において分割イメージファイルを保持するために設けられたデバイスである。通信端末１０１は、一般に、多数の分割イメージファイルを保持しておくだけのリソースを有さないため、本実施形態における分散システム１００は、ストレージデバイス１０２によって多数の分割イメージファイルを保持しておくことが可能なように構成される。また、複数の通信端末１０１の分割イメージファイルを保持してもよい。

【００３３】

システム情報取得部４０１は、分散システム１００に関するシステム情報を、エッジサーバ１０３から取得する。

【００３４】

システム情報記憶部４０２は、システム情報取得部４０１によって取得された分散システム１００に関するシステム情報を保持する。

【００３５】

分割イメージファイル受信部４０３は、エッジサーバ１０３から、更新されたイメージファイルを分割した分割イメージファイルを受信する。

【００３６】

分割イメージファイル記憶部４０４は、分割イメージファイル受信部４０３によって受信された分割イメージファイルを保持する。分割イメージファイル記憶部４０４は、新たに受信した分割イメージファイルによって、対応する既存の分割イメージファイルを更新してもよい。

10

20

30

40

50

【0037】

ファイル要求取得部405は、通信端末101から、分割イメージファイルの取得要求を受信する。

【0038】

分割イメージファイル検索部406は、分割イメージファイル記憶部404によって保持された1以上の分割イメージファイルから、通信端末101からのファイル要求に応じた分割イメージファイルを検索して抽出する。

【0039】

分割イメージファイル送信部407は、分割イメージファイル検索部406によって抽出された分割イメージファイルを受信し、受信された分割イメージファイルを通信端末101へ送信する。

10

【0040】

なお、2つの通信端末101及び2つのエッジサーバ103が図示されているが、それぞれ同じ通信端末および同じエッジサーバとすることができる。

【0041】

<1.4. エッジサーバの構成>

図5は、第1の実施形態に係るエッジサーバ103の機能構成図である。図示されるように、エッジサーバ103は、システム情報記憶部501、システム情報送信部502、インシデントレポート受信部503、インシデントレポート記憶部504、イメージファイル更新部505、更新ポリシー記憶部506、イメージファイル分割部507、分割イメージファイル記憶部508、及び分割イメージファイル送信部509を有する。

20

【0042】

システム情報記憶部501は、分散システム100に関するシステム情報を保持する。

【0043】

システム情報送信部502は、システム情報記憶部501に保持されているシステム情報を、通信端末101及びストレージデバイス102へ送信する。

【0044】

インシデントレポート受信部503は、通信端末101からインシデントレポートを受信する。

【0045】

インシデントレポート記憶部504は、インシデントレポート受信部503によって受信されたインシデントレポートを保持する。

30

【0046】

イメージファイル更新部505は、更新ポリシー記憶部506に保持された更新ポリシーに従い、対象のモジュールごとにイメージファイル更新する。或いは、イメージファイル更新部505は、オペレーターの指示に従って、イメージファイルを更新する。

【0047】

更新ポリシー記憶部506は、モジュールごとに、異常動作状態にあると判定された場合の対処方法を示す更新ポリシー情報を保持する。対処方法には、例えば、各モジュールの違反ポリシータイプに対応するイメージファイルの更新方法が含まれる。更新ポリシーの詳細については後述する。

40

【0048】

イメージファイル分割部507は、事前に定められた所定の方法に従って、更新されたイメージファイルを分割する。イメージファイルの分割方法については後述する。

【0049】

分割イメージファイル記憶部508は、イメージファイル分割部507から得られた分割イメージファイルを保持する。

【0050】

分割イメージファイル送信部509は、ストレージデバイス102へ分割イメージファイルを送信する。送信先のストレージデバイス102は、予め設定されたグループ内に含

50

まれる複数のストレージデバイスとしてもよく、この場合、グループ内の複数のストレージデバイスに送信する分割イメージファイルでイメージファイルが再現できるように、各分割イメージファイルを送信する。

【0051】

なお、2つの通信端末101及び2つのストレージデバイス102が図示されているが、それぞれ同じ通信端末および同じストレージデバイスとすることができる。

【0052】

<1.5. 通信端末の動作例>

図6は、第1の実施形態に係る通信端末の動作例を示すフローチャートである。なお、以下の説明では、既に説明した事項については、詳細な説明は省略する。

【0053】

まず、S601において、システム情報取得部301は、エッジサーバ103からシステム情報を受信する。システム情報取得部301は、受信したシステム情報を、システム情報記憶部302に格納する

【0054】

S602において、モジュール診断部303は、システム情報記憶部302に格納されたシステム情報に基づいて、分散システム100内の各モジュールが異常動作状態にあるかどうか判定する。異常動作状態が検知された場合は、S603に進む。一方、異常動作状態が検知されない場合は、S601に戻り、処理を繰り返す。

【0055】

S603において、モジュール廃棄部304は、異常動作状態が検知されたモジュール、及び当該モジュールの関連モジュールを廃棄する。

【0056】

S604において、インシデントレポート送信部305は、異常動作状態が検知されたモジュールに関するインシデントレポートをエッジサーバ103へ送信する。

【0057】

S605において、通信端末101は、エッジサーバ103から、インシデントレポートに対する応答を受信したかどうか判定する。通信端末101は、エッジサーバ103から応答を受信するまで待機する。通信端末101が応答を受信すると、処理はS606に進む。

【0058】

S606において、通信端末101は、ストレージデバイス102から、廃棄されたモジュールに対応する分割イメージファイルをダウンロードして、分割イメージファイル記憶部307に格納する。

【0059】

S607において、分割イメージファイル結合部308は、分割イメージファイル記憶部307から取得した分割イメージファイルを結合して、モジュールごとに単一のイメージファイルを生成する。

【0060】

S608において、モジュール起動部309は、生成されたイメージファイルに基づいて、モジュールを再起動する。

【0061】

以上説明したように、通信端末101は、異常動作状態となった場合でも迅速な機能復旧を実現することができる。

【0062】

図7は、第1の実施形態に係るシステム情報の例を示す図である。図示されたシステム情報は、通信端末101がシステム情報記憶部302に保持するシステム情報の例である。

【0063】

図7(a)は、端末ID(識別子)と端末タイプ702との関係を示す。例えば、端末IDが「e001」である端末は、エッジサーバ103である。また、端末IDが「s001」

10

20

30

40

50

及び「s002」である端末は、ストレージデバイス102である。また、端末IDが、「d001」及び「d002」である端末は、通信端末101である。

【0064】

図7(b)は、自身の端末IDを示す。図示された例では、自身の端末IDが「d001」であることが示されている。

【0065】

図7(c)は、送信先端末IDと次に転送すべき端末IDとの関係を示す。例えば、送信先端末IDが「s001」の場合、次に転送すべき端末IDは「d001」である。また、送信先端末IDが「s002」の場合、次に転送すべき端末IDは「d002」である。また、送信先端末IDが「e001」の場合、次に転送すべき端末IDは「d002」である。

10

【0066】

図8も、第1の実施形態に係るシステム情報の例を示す図である。ここで図示されたシステム情報も、通信端末101がシステム情報記憶部302に保持するシステム情報の例である。

【0067】

図8(a)は、自身が保有すべきモジュールのリストを示す。例えば、図示されたモジュールのリストを有する通信端末101は、モジュールバージョンが「3.8.5」の「login」モジュールを有し、当該モジュールのイメージファイルは、128個に分割される。また、この通信端末101は、モジュールバージョンが「2.4.3」の「camera」モジュールを有し、当該モジュールのイメージファイルは、36個に分割される。また、この通信端末101は、モジュールバージョンが「0.1.1」の「detect-person」モジュールを有し、当該モジュールのイメージファイルは521個に分割される。

20

【0068】

図8(b)は、連携モジュールのリストを示す。例えば、モジュールバージョンが「2.4.3」の「camera」モジュールは、モジュールバージョンが「0.1.1」の「detect-person」モジュールと連携する。また、同「camera」モジュールは、モジュールバージョンが「3.8.5」の「login」モジュールとも連携する。連携モジュールは、関連モジュールとも称する。

【0069】

図9も、第1の実施形態に係るシステム情報の例を示す。ここで図示されたシステム情報も、通信端末101がシステム情報記憶部302に保持するシステム情報の例である。

30

【0070】

より具体的には、図9は、各モジュールの異常動作を判定するためのルールを示す。ここでは、ポリシータイプとその値によって、当該ルールが表される。

【0071】

例えば、モジュールバージョンが「3.8.5」の「login」モジュールには、ポリシータイプ「valid_account」が適用され、その値は「userA」である。これは、当該モジュールを利用する有効なアカウントが、「userA」であることを示す。同モジュールには、ポリシータイプ「login_from」が適用され、その値は「192.168.24.0/24」である。これは、当該モジュールにログインする装置のIPアドレスが、192.168.24.0~24の範囲内にあれば、正常であることを示す。

40

【0072】

また、モジュールバージョンが「2.4.3」の「camera」モジュールには、ポリシータイプ「ave_trans_rate」が適用され、その値は「3Mbps」である。これは、当該モジュールから送信されるデータの平均通信レートが、3Mbps(bit per second)以下である場合は、正常であることを示す。

【0073】

また、モジュールバージョンが「0.1.1」の「detect-person」モジュールには、ポリシータイプ「file_hash」が適用され、その値は「/etc/conf, 79a9e9766e8007d6c341c7e238045ae5」である。これは、指定されたディレクトリに存在するファイルのハッ

50

シュ値が、指定された値であれば、正常であることを示す。

【0074】

ここで、通信端末101のモジュール診断部303の動作例について、より詳細に説明する。

【0075】

モジュール診断部303は、システム情報記憶部302に記憶されたその通信端末101が持つべきモジュールのリスト（図8（a）参照）に基づいて、モジュールの過不足や、モジュールのポリシーに違反した動作状態を検出する。

【0076】

モジュールのポリシーは、図9に示されるように、モジュールごとにポリシータイプと値で定義される。例えば、ポリシータイプが「valid_account」である場合、値は、そのモジュールにログイン可能なアカウント名「userA」を示す。また、ポリシータイプが「login_from」である場合、値は、そのモジュールにログイン可能なネットワークセグメント「192.168.24.0/24」を示す。また、ポリシータイプが「ave_trans_rate」である場合、値は、そのモジュールが発生させるネットワーク通信の平均ビットレート「3Mbps」を示す。また、ポリシータイプが「file_hash」である場合、値は、そのモジュール内の特定のファイルのハッシュ値「/etc/conf, 79a9e9766e8007d6c341c7e238045ae5」を示す。

【0077】

上述したように、モジュール診断部303は、モジュールごとに事前に定義されたポリシーに違反した動作状態を検知すると、当該モジュールがサイバー攻撃を始めとした、設計上または運用上意図しない動作状態にあると判断する。このように、モジュール診断部303は、モジュールの異常動作を検知する。

【0078】

次に、通信端末101のモジュール廃棄部304の動作例について、より詳細に説明する。

【0079】

モジュール廃棄部304は、モジュール診断部303によって異常動作状態にあると判断されたモジュールの動作を停止させ、モジュールごとデータを廃棄する。例えば、モジュール廃棄部304は、モジュールに対応するコンテナを停止して、そのまま破棄する。

【0080】

モジュール廃棄部304は、当該モジュールの廃棄を実施する際に、システム情報記憶部302に保持されている連携モジュール情報（図8（b））も参照し、連携モジュールも再帰的に廃棄対象とする。連携モジュールも廃棄することで、異常をきたしたモジュールへファイル共有を行っていたり、設定ファイルや情報のやり取りを行っていたりする他のモジュールについても、一括で廃棄を行うことが可能となる。

【0081】

図10は、第1の実施形態に係る分割イメージファイル情報の例を示す。分割イメージファイル情報は、通信端末101の分割イメージファイル記憶部307に保持され、分割イメージファイル記憶部307に格納された分割イメージファイルの情報を示す。

【0082】

図示された分割イメージファイル情報は、モジュールバージョンが「3.8.5」の「login」モジュールについて、フラグメントナンバーが1、2、3、・・・の分割イメージファイルが格納されていることを示す。また、モジュールバージョンが「2.4.3」の「camera」モジュールについて、フラグメントナンバーが1、2、・・・の分割イメージファイルが格納されていることを示す。フラグメントナンバーは、イメージファイルの分割数を示す。

【0083】

<1.6.ストレージデバイスの動作例>

図11は、第1の実施形態に係るストレージデバイスの動作例を示すフローチャートで

10

20

30

40

50

ある。なお、以下の説明では、既に説明した事項については、詳細な説明は省略する。

【0084】

まず、S1101において、システム情報取得部401は、エッジサーバ103からシステム情報を受信する。システム情報取得部401は、受信されたシステム情報を、システム情報記憶部402に格納する。

【0085】

S1102において、分割イメージファイル受信部403は、エッジサーバ103から分割イメージファイルを受信したかどうか判定する。分割イメージファイル受信部403は、分割イメージファイルを受信するまで待機し、分割イメージファイルを受信すると、S1103に進む。

【0086】

S1103において、分割イメージファイル受信部403は、受信された分割イメージファイルを分割イメージファイル記憶部404に記憶する。

【0087】

次いで、S1104において、ファイル要求取得部405は、通信端末101からイメージファイル要求を受信したかどうか判定する。ファイル要求取得部405は、イメージファイル要求を受信するまで待機し、イメージファイル要求を受信すると、S1105に進む。

【0088】

S1105において、分割イメージファイル検索部406は、イメージファイル要求に対応する分割イメージファイルを、分割イメージファイル記憶部404から検索する。

【0089】

S1106において、分割イメージファイル送信部407は、検索された分割イメージファイルを通信端末101へ送信する。

【0090】

以上説明したように、ストレージデバイス102は、エッジサーバ103から分割イメージファイルを受信して、受信された分割イメージファイルを保持する。また、ストレージデバイス102は、通信端末101からの要求に応じて、分割イメージファイルを送信する。

【0091】

<1.7. エッジサーバの動作例>

図12は、第1の実施形態に係るエッジサーバの動作例を示すフローチャートである。なお、以下の説明では、既に説明した事項については、詳細な説明は省略する。

【0092】

まず、S1201において、システム情報送信部502は、システム情報記憶部501に保持されたシステム情報を、通信端末101及びストレージデバイス102に送信する。

【0093】

次いで、S1202において、インシデントレポート受信部503は、通信端末101からインシデントレポートを受信したかどうか判定する。インシデントレポート受信部503はインシデントレポートを受信するまで待機し、インシデントレポートを受信すると、S1203に進む。

【0094】

S1203において、イメージファイル更新部505は、受信されたインシデントレポートの内容にマッチする更新ポリシーが、更新ポリシー記憶部506に存在するかどうか判定する。更新ポリシーが存在する場合は、S1204に進み、イメージファイル更新部505は、更新ポリシーに従ってイメージファイルを更新する。一方、更新ポリシーが存在しない場合は、S1205に進み、オペレーターが手動でイメージファイルを更新する。

【0095】

次いで、S1206において、イメージファイル分割部507は、更新されたイメージファイルを分割して、分割イメージファイルを生成する。分割イメージファイルは、分割

10

20

30

40

50

イメージファイル記憶部 508 に記憶される。

【0096】

S1207において、分割イメージファイル送信部 509 は、分割イメージファイルをストレージデバイス 102 へ送信する。

【0097】

S1208において、システム情報送信部 502 は、通信端末 101 へシステム情報を送信する。

【0098】

以上説明したように、エッジサーバ 103 は、通信端末 101 からインシデントレポートを受信すると、更新ポリシーに従って対象モジュールのイメージファイルを更新する。また、エッジサーバ 103 は、更新されたイメージファイルを分割して分割イメージファイルを生成し、生成された分割イメージファイルをストレージデバイス 102 へ送信する。

【0099】

次に、イメージファイル更新部 505 の動作例について、図 13 及び図 14 を参照してより詳細に説明する。

【0100】

図 13 は、第 1 の実施形態に係るインシデントレポートの例を示す図である。図示されたインシデントレポートは、エッジサーバ 103 がインシデントレポート記憶部 504 に保持するインシデントレポートの例である。図示されるように、インシデントレポートは、受信日時、送信元端末 ID、モジュール ID、モジュールバージョン、違反ポリシータイプ、及びログを含む。

【0101】

図 14 は、第 1 の実施形態に係る更新ポリシーの例を示す図である。図示された更新ポリシーは、エッジサーバ 103 が更新ポリシー記憶部 506 に保持する更新ポリシーの例である。図示されるように、更新ポリシーは、モジュール ID、該当バージョン、違反ポリシータイプ、及び対処方法を含む。

【0102】

イメージファイル更新部 505 は、図 13 のインシデントレポートに含まれる違反ポリシータイプをもとに、図 14 の更新ポリシーに含まれる対処方法に従って、対象モジュールのイメージファイルを更新する。すなわち、イメージファイル更新部 505 は、対象モジュールの異常動作状態を解消するための新しいバージョンのイメージファイルを生成する。

【0103】

具体的には、イメージファイル更新部 505 は、新たに受信されたインシデントレポートが特定の更新ポリシーにマッチした場合、当該更新ポリシーの対処方法に従って、新しいバージョンのイメージファイルを生成する。

【0104】

例えば、モジュールバージョンが「3.8.5」の「login」モジュールに対して、「valid_account」の違反ポリシーが報告された場合には、「userC」による無効なアカウントのログイン試行が観測されただけなので、イメージファイルの更新は行わない。すなわち、違反ポリシーが報告されたとしても、必ずしもイメージファイルが更新されるわけではない。この場合、現在のバージョンのイメージファイルが後続の処理に用いられ、最終的に通信端末 101 は、異常動作の影響を受けていない新たにダウンロードされた現在のバージョンのイメージファイルに基づいて、対象モジュールを起動することになる。一方、同バージョンの「login」モジュールに対して、「login_from」の違反ポリシーが報告された場合には、許可されていない IP アドレス（「192.168.33.24」）からログインが成功しているため、当該アカウントを無効化したイメージファイルを生成する。

【0105】

一方、受信されたインシデントレポートがどの更新ポリシーにも該当しない場合には、オペレーターが手動でイメージファイルを更新し、新しいバージョンのイメージファイル

10

20

30

40

50

を生成する。

【0106】

次に、エッジサーバ103のイメージファイル分割部507の動作例について、より詳細に説明する。

【0107】

イメージファイル分割部507は、予め設定されたチャンクサイズごとにイメージファイルを分割して、分割イメージファイルを生成する。例えば、チャンクサイズが4,000,000に設定されていたとすると、500MBのイメージファイルを分割する場合、 $500 \times 1,000^2 / 4,000,000 = 125$ であるため、125個の分割イメージファイルが作成される。

【0108】

なお、上述したイメージファイルの分割方法は一例であり、イメージファイルに含まれるファイルやディレクトリ等の粒度で分割イメージファイルを生成してもよい。次期標準コンテナフォーマットであるOCI(Open Container Initiative) Image Format v2では、レイヤー単位ではなくファイルよりも細かい粒度でイメージファイルを分割することにより、イメージサイズを縮小する方式が議論されている。イメージファイルに対する小さい更新等であれば、数KBの更新データをネットワークに流せばよい。

【0109】

<1.8. ハードウェア構成>

図15は、第1の実施形態に係るコンピュータのハードウェア構成例を示す概略ブロック図である。図示されたコンピュータは、本実施形態の分散システムを構成する通信端末101、ストレージデバイス102、及びエッジサーバ103の各装置として動作し得る。

【0110】

コンピュータ1500は、CPU1501と、主記憶装置1502と、補助記憶装置1503と、インタフェース1504と、通信インタフェース1505とを備える。

【0111】

コンピュータ1500の動作は、プログラムの形式で補助記憶装置1503に記憶されている。CPU1501は、そのプログラムを補助記憶装置1503から読み出して主記憶装置1502に展開し、そのプログラムに従って、本実施形態で説明した各装置の動作を実行する。

【0112】

補助記憶装置1503は、一時的でない有形の媒体の例である。一時的でない有形の媒体の他の例として、インタフェース1504を介して接続される磁気ディスク、光磁気ディスク、CD-ROM(Compact Disk Read Only Memory)、DVD-ROM(Digital Versatile Disk Read Only Memory)、半導体メモリ等が挙げられる。また、プログラムが通信回線によってコンピュータ1500に配信される場合、配信を受けたコンピュータ1500がそのプログラムを主記憶装置1502に展開し、そのプログラムに従って動作してもよい。

【0113】

また、各装置の各構成要素の一部または全部は、汎用または専用の回路(circuitry)、プロセッサ等や、これらの組み合わせによって実現されてもよい。これらは、単一のチップによって構成されてもよいし、バスを介して接続される複数のチップによって構成されてもよい。各構成要素の一部または全部は、上述した回路等とプログラムとの組み合わせによって実現されてもよい。

【0114】

また、コンピュータ1500は、不図示の入出力装置を備え、オペレーター等による入出力動作が可能のように構成される。入力装置の例としては、マウスやキーボードなどがある。また、出力装置の例としては、液晶ディスプレイなどの表示装置がある。また、表示装置には、タッチパネルを備え、入力装置として動作する表示装置も含まれる。

【0115】

< 1. 9. 技術的特徴 >

本実施形態は、サイバーセキュリティにおける機能復旧フェーズに注目したセキュアなシステムアーキテクチャを提供する。本実施形態では、通信端末 101 の各機能をモジュール化し（コンテナアーキテクチャ等を利用）、モジュール化された機能群の、分割されたイメージファイルを、分散システム内に配置されている複数のストレージデバイス 102 が保持することで、冗長性を向上させることができる。

【0116】

また、本実施形態によれば、通信端末 101 は、特定の機能に関するイメージファイルをダウンロードして起動をできるため、ある機能に設計上または運用上意図しない動作が生じた場合においても、正常な機能の迅速な提供が可能となる。

【0117】

また、通信端末 101 は、分散システム 100 内から分割イメージファイルを収集するため、インターネットとの接続が低速度である場合にも近隣の通信端末 101 を経由してストレージデバイスよりダウンロードができることから、低通信コストかつ短い時間での機能復旧を可能とする。

また、同様の機能を有する他の通信端末 101 も、ストレージデバイス 102 より、修正された分割イメージファイルをダウンロードし、モジュールを最新に保つことができる（いわゆる、DevSecOps サイクルの高速化を実現することができる）。

【0118】

なお、上述した技術的特徴は本発明の実施形態の具体的な一例であり、当然ながら、本発明の実施形態は上述した技術的特徴に限定されない。

【0119】

<< 2. 第 2 の実施形態 >>

続いて、図 16 を参照して、本発明の第 2 の実施形態を説明する。上述した第 1 の実施形態は、具体的な実施形態であるが、第 2 の実施形態は、より一般化された実施形態である。

【0120】

< 2. 1. システムの構成 >

図 16 は、第 2 の実施形態における分散システムの概要図である。本実施形態における分散システム 1600 は、通信端末 1610 と、エッジサーバ 1620 と、ストレージデバイス 1630 とを含む。なお、通信端末 1610、エッジサーバ 1620、およびストレージデバイス 1630 の数は、図示された数に限定されない。また、通信端末 1610、エッジサーバ 1620、およびストレージデバイス 1630 は、互いに有線または無線ネットワークを介して通信可能に接続されている。

【0121】

通信端末 1610 は、モジュール診断部 1611、インシデントレポート送信部 1612、分割イメージファイル結合部 1613、及びモジュール起動部 1614 を有する。モジュール診断部 1611 は、異常動作状態にある機能モジュールを検知する。インシデントレポート送信部 1612 は、エッジサーバ 1620 へ異常動作状態を通知する。分割イメージファイル結合部 1613 は、ストレージデバイス 1630 から取得した分割イメージファイルを結合してイメージファイルを生成する。モジュール起動部 1614 は、生成されたイメージファイルに基づいて、機能モジュール及び関連機能モジュールを起動する。

【0122】

エッジサーバ 1620 は、イメージファイル更新部 1621、イメージファイル分割部 1622、及び分割イメージファイル送信部 1623 を有する。イメージファイル更新部 1621 は、機能モジュール及び関連機能モジュールのそれぞれに対応するイメージファイルを生成する。イメージファイル分割部 1622 は、生成されたイメージファイルを分割した分割イメージファイルを生成する。分割イメージファイル送信部 1623 は、生成された分割イメージファイルをストレージデバイス 1630 へ送信する。

【0123】

ストレージデバイス 1630 は、分割イメージファイル受信部 1631、及び分割イメージファイル送信部 1632 を有する。分割イメージファイル受信部 1631 は、エッジサーバ 1620 から分割イメージファイルを受信して、格納する。分割イメージファイル送信部 1632 は、通信端末 1610 からの要求に応じて、機能モジュール及び関連機能モジュールに対応する分割イメージファイルを通信端末 1610 へ送信する。

【0124】

上述した各装置の各処理部は、例えば、プログラムに従って動作するコンピュータの CPU (Central Processing Unit)、および、そのコンピュータの通信インタフェースによって実現される。例えば、CPU が、そのコンピュータのプログラム記憶装置等のプログラム記録媒体からプログラムを読み込み、そのプログラムに従って、必要に応じて通信

10

＜2.2. 動作例＞

次に、第2の実施形態における動作例について説明する。

【0125】

第2の実施形態によれば、通信端末 1610 は、異常動作状態にある機能モジュールを検知し、エッジサーバ 1620 へ異常動作状態を通知する。エッジサーバ 1620 は、機能モジュール及び関連機能モジュールのそれぞれに対応するイメージファイルを生成し、生成されたイメージファイルを分割した分割イメージファイルを生成して、ストレージデバイス 1630 へ送信する。ストレージデバイス 1630 は、分割イメージファイルを格納し、通信端末 1610 からの要求に応じて、機能モジュール及び関連機能モジュールに対応する分割イメージファイルを通信端末 1610 へ送信する。通信端末 1610 は、ストレージデバイス 1630 から取得した分割イメージファイルを結合してイメージファイルを生成し、生成されたイメージファイルに基づいて機能モジュール及び関連機能モジュールを起動する。

20

【0126】

－第1の実施形態との関係

一例として、第2の実施形態における通信端末 1610、エッジサーバ 1620、およびストレージデバイス 1630 はそれぞれ、第1の実施形態における通信端末 101、エッジサーバ 103、及びストレージデバイス 102 である。この場合に、第1の実施形態についての説明は、第2の実施形態にも適用され得る。

30

【0127】

なお、第2の実施形態は、この例に限定されない。

【0128】

以上、本発明の実施形態を説明したが、本発明はこれらの実施形態に限定されるものではない。これらの実施形態は例示にすぎないということ、及び、本発明のスコップ及び精神から逸脱することなく様々な変形が可能であるということは、当業者に理解されるであろう。

【0129】

例えば、本明細書に記載されている処理は、必ずしも上述した順序に沿って時系列に実行されなくてよい。例えば、各処理は、上述した順序と異なる順序で実行されても、並列的に実行されてもよい。また、処理の一部が削除されてもよく、さらなる処理が追加されてもよい。

40

【0130】

また、本明細書において説明した分散システムの構成要素を備える装置（例えば、分散システムを構成する複数の装置（又はユニット）のうちの1つ以上の装置（又はユニット）、又は上記複数の装置（又はユニット）のうちの1つのためのモジュール）が提供されてもよい。また、上記構成要素の処理を含む方法が提供されてもよく、上記構成要素の処理をプロセッサに実行させるためのプログラムが提供されてもよい。また、当該プログラムを記録したコンピュータに読み取り可能な非一時的記録媒体（Non-transitory computer readable medium）が提供されてもよい。当然ながら、このような装置、モジュ

50

ール、方法、プログラム、及びコンピュータに読み取り可能な非一時的記録媒体も本発明に含まれる。

【0131】

上記実施形態の一部又は全部は、以下の付記のようにも記載され得るが、以下には限られない。

【0132】

(付記1)

1以上の通信端末と1以上のストレージデバイスとエッジサーバとがネットワークを介して通信する分散システムであって、

前記通信端末は、異常動作状態にある機能モジュールを検知し、前記エッジサーバへ前記異常動作状態を通知し、

前記エッジサーバは、前記機能モジュール及び関連機能モジュールのそれぞれに対応するイメージファイルを生成し、前記生成されたイメージファイルを分割した複数の分割イメージファイルを生成して、前記複数の分割イメージファイルを前記ストレージデバイスへ送信し、

前記ストレージデバイスは、前記分割イメージファイルを格納し、前記通信端末からの要求に応じて、前記機能モジュール及び前記関連機能モジュールに対応する分割イメージファイルを前記通信端末へ送信し、

前記通信端末は、前記ストレージデバイスから取得した前記複数の分割イメージファイルを結合して前記イメージファイルを生成し、前記生成されたイメージファイルに基づいて前記機能モジュール及び前記関連機能モジュールを起動する、
ことを特徴とする分散システム。

【0133】

(付記2)

前記通信端末は、前記異常動作状態にある機能モジュールを検知すると、前記機能モジュール及び前記関連機能モジュールの動作を停止させ、前記機能モジュール及び前記関連機能モジュールを廃棄することを特徴とする付記1に記載の分散システム。

【0134】

(付記3)

前記通信端末は、前記異常動作状態にある機能モジュールを検知すると、前記異常動作状態の内容を示すインシデントレポートを前記エッジサーバへ送信することを特徴とする付記1または2に記載の分散システム。

【0135】

(付記4)

前記エッジサーバは、前記インシデントレポートの内容にマッチする更新ポリシーに応じて、前記イメージファイルを生成することを特徴とする付記3に記載の分散システム。

【0136】

(付記5)

前記通信端末は、前記複数のストレージデバイスのうち、前記通信端末の近隣に存在するストレージデバイスから、前記分割イメージファイルを取得することを特徴とする付記1乃至4のいずれか1項に記載の分散システム。

【0137】

(付記6)

前記近隣のストレージデバイスは、前記通信端末と通信リンクを直接確立することができるストレージデバイスであることを特徴とする付記5に記載の分散システム。

【0138】

(付記7)

前記近隣のストレージデバイスは、前記通信端末に対するホップ数に応じて決定されることを特徴とする付記5に記載の分散システム。

【0139】

10

20

30

40

50

(付記 8)

前記エッジサーバは、前記複数の分割イメージファイルを、予め設定されたグループ内に含まれる複数のストレージデバイスに送信することを特徴とする付記 1 乃至 7 のいずれか 1 項に記載の分散システム。

【0140】

(付記 9)

前記通信端末は、前記複数の分割イメージファイルのそれぞれを並列でダウンロードすることを特徴とする付記 1 乃至 8 のいずれか 1 項に記載の分散システム。

【0141】

(付記 10)

分散システムを構成する通信端末であって、

複数の機能モジュールの動作状態を診断し、異常動作状態にある機能モジュールを検知するモジュール診断手段と、

前記異常動作状態にある機能モジュールの動作を停止させ、前記機能モジュールを廃棄するモジュール廃棄手段と、

前記機能モジュールに対応し、前記異常動作状態を解消するように生成されたイメージファイルを分割した複数の分割イメージファイルを取得し、前記複数の分割イメージファイルを結合する分割イメージファイル結合手段と、

前記複数の分割イメージファイルを結合して生成されたイメージファイルに基づいて、前記機能モジュールを起動するモジュール起動手段と

を備えることを特徴とする通信端末。

【0142】

(付記 11)

1 以上の通信端末と 1 以上のストレージデバイスとエッジサーバとがネットワークを介して通信する分散システムの機能復旧方法であって、

前記通信端末が、異常動作状態にある機能モジュールを検知し、前記エッジサーバへ前記異常動作状態を通知する通知ステップと、

前記エッジサーバが、前記機能モジュール及び関連機能モジュールのそれぞれに対応するイメージファイルを生成し、前記生成されたイメージファイルを分割した複数の分割イメージファイルを生成して、前記複数の分割イメージファイルを前記ストレージデバイスへ送信する第 1 の送信ステップと、

前記ストレージデバイスが、前記分割イメージファイルを格納し、前記通信端末からの要求に応じて、前記機能モジュール及び前記関連機能モジュールに対応する分割イメージファイルを前記通信端末へ送信する第 2 の送信ステップと、

前記通信端末が、前記ストレージデバイスから取得した前記複数の分割イメージファイルを結合して前記イメージファイルを生成し、前記生成されたイメージファイルに基づいて前記機能モジュール及び前記関連機能モジュールを起動する起動ステップとを含むことを特徴とする機能復旧方法。

【0143】

(付記 12)

コンピュータを付記 10 に記載の通信端末として機能させるためのプログラム。

【産業上の利用可能性】

【0144】

本発明の一実施形態は、スマートシティなどの社会基盤となるサイバーフィジカルシステムへ適用することが考えられる。また、本発明の一実施形態は、敵対者からのサイバー攻撃が想定されるミッションクリティカルなネットワークシステムへ適用することが考えられる。

【符号の説明】

【0145】

100 分散システム

10

20

30

40

50

- 101 通信端末
- 102 ストレージデバイス
- 103 エッジサーバ
- 104 障害物
- 105 クラウドサーバ

【図面】

【図 1】

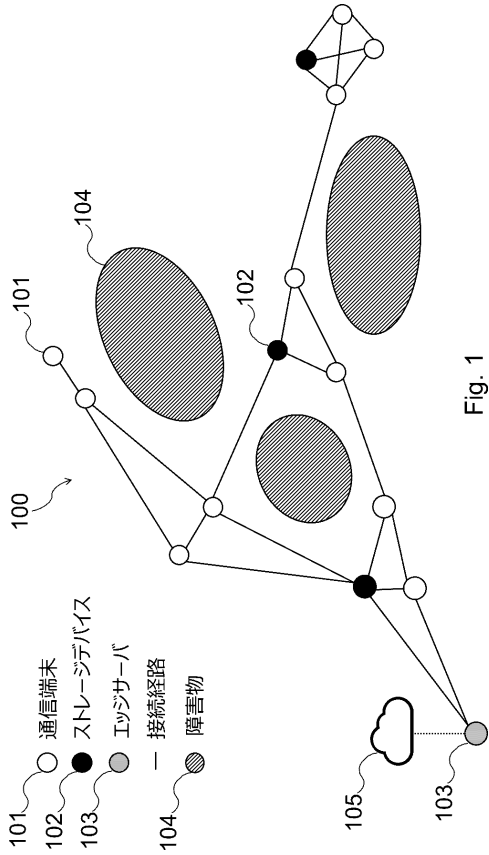


Fig. 1

【図 2】

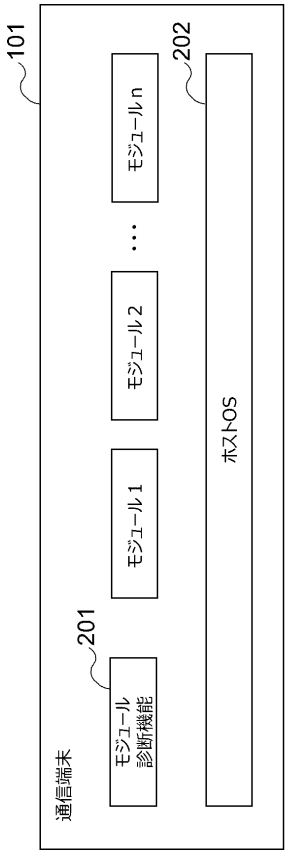


Fig. 2

10

20

30

40

50

【図 3】

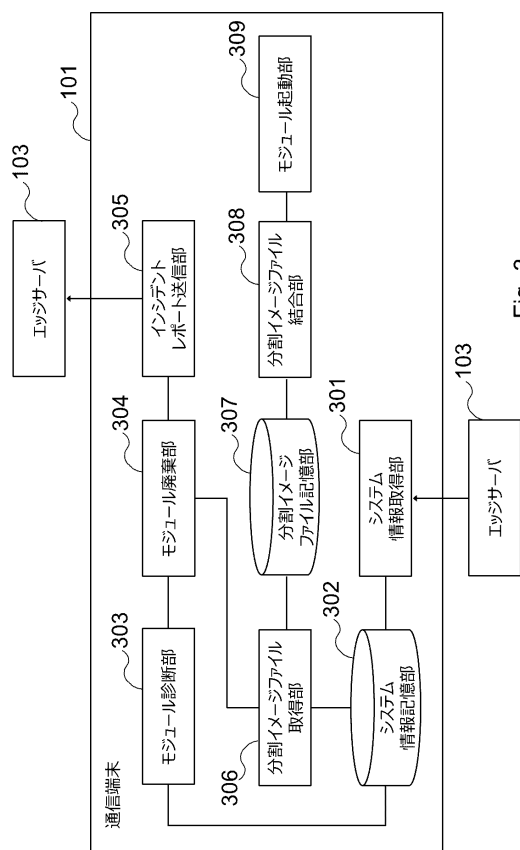


Fig. 3

【図 4】

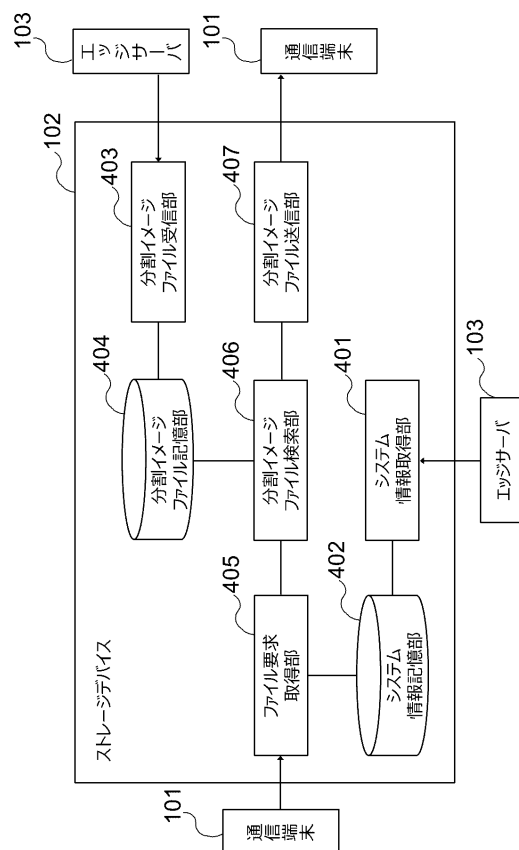


Fig. 4

【図 5】

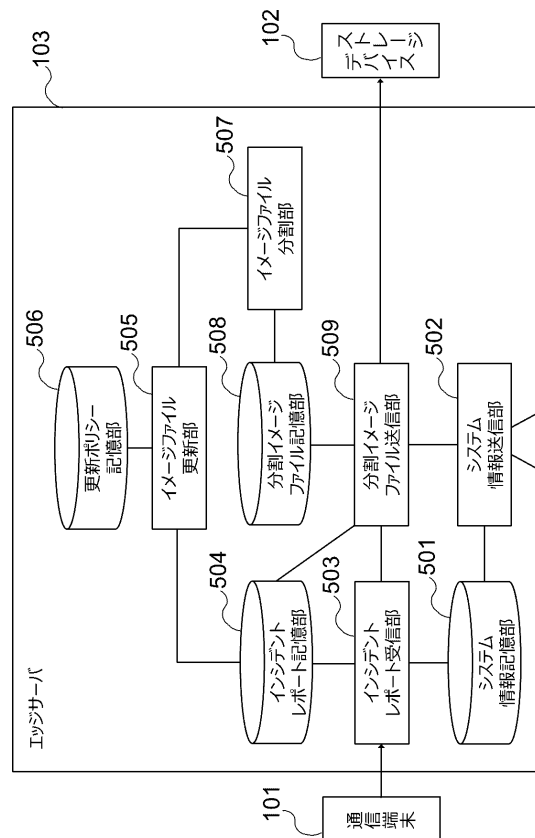


Fig. 5

【図 6】

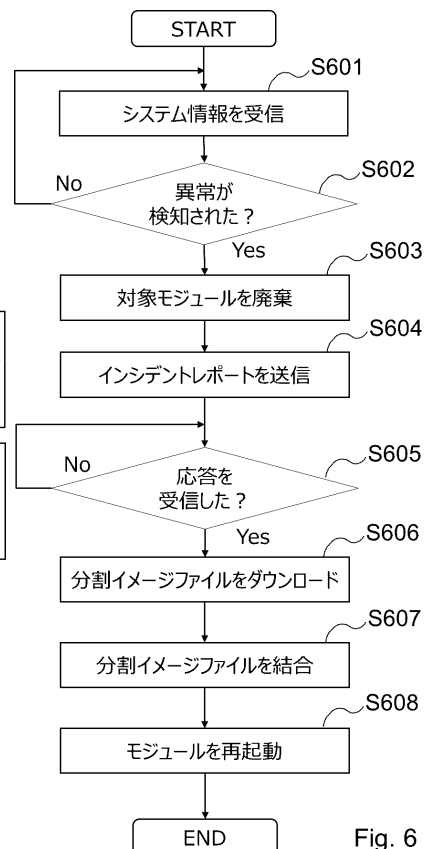


Fig. 6

【図 7】

端末ID	端末タイプ
e001	エッジサーバ
s001	ストレージデバイス
s002	ストレージデバイス
d001	通信端末
d002	通信端末
⋮	⋮

(a)

自身の端末ID
d001

(b)

送信先端末ID	次に転送すべき端末ID
s001	d001
s002	d002
e001	d002
⋮	⋮

(c)

Fig. 7

【図 8】

モジュールID	モジュールバージョン	分割数
login	3.8.5	128
camera	2.4.3	36
detect-person	0.1.1	521
⋮	⋮	⋮

(a)

モジュールID	モジュールバージョン	連携モジュールID	連携モジュールバージョン
camera	2.4.3	detect-person	0.1.1
camera	2.4.3	login	3.8.5
⋮	⋮	⋮	⋮

(b)

Fig. 8

【図 9】

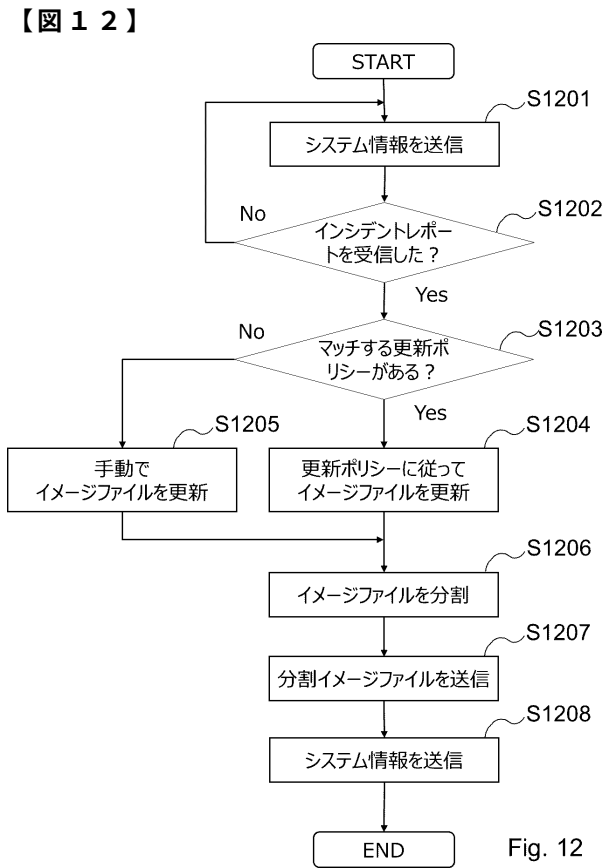
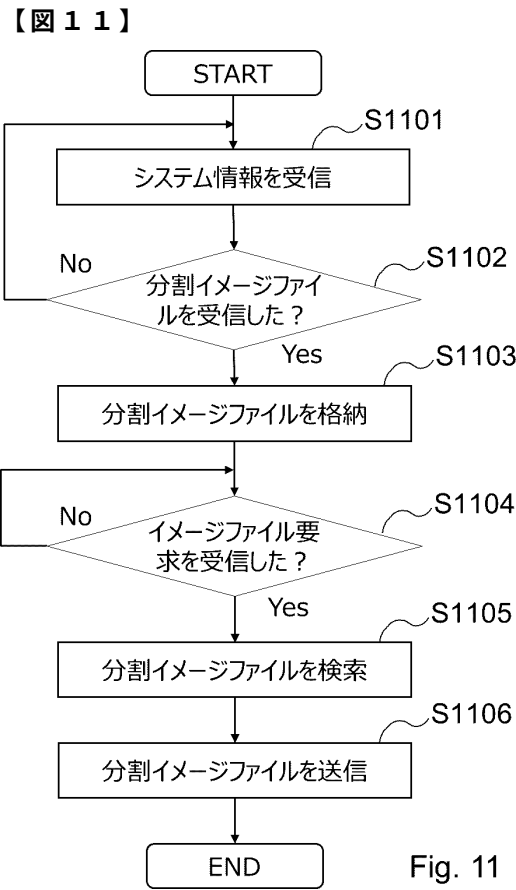
モジュールID	モジュールバージョン	ポリシータイプ	値
login	3.8.5	valid_account	userA
login	3.8.5	login_from	192.168.24.0/24
camera	2.4.3	ave_trans_rate	3Mbps
detect-person	0.1.1	file_hash	/etc/conf, 79a9e9766e8007d6c341c7e238045ae5
⋮	⋮	⋮	⋮

Fig. 9

【図 10】

モジュールID	モジュールバージョン	フラグメントナンバー
login	3.8.5	1
login	3.8.5	2
login	3.8.5	3
⋮	⋮	⋮
camera	2.4.3	1
camera	2.4.3	2
⋮	⋮	⋮

Fig. 10



【図 1 3】

受信日時	送信元端末ID	モジュールID	モジュールバージョン	違反ポリシータイプ	ログ
2020/01/24 02:08:32+09:00	d001	login	3.8.5	valid_account	"login trial was detected to invalid account 'userC'."
2020/01/24 02:08:34+09:00	d001	login	3.8.5	login_from	"login trial succeeded from '192.168.33.24' to 'userA'."
...	...	...	...	...	...

Fig. 13

【図 1 4】

モジュールID	該当バージョン	違反ポリシータイプ	対処方法
login	>= 3.8.0	valid_account	なにもしない
login	>= 1.0.0	login_from	ログインが成功したアカウントを無効化する
...	...	...	...

Fig. 14

10

20

30

40

50

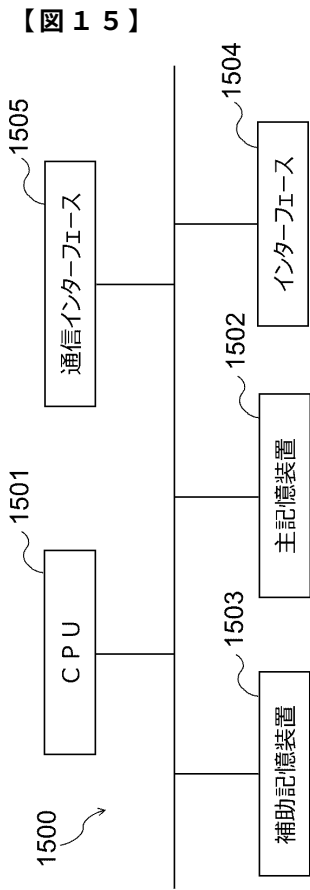


Fig. 15

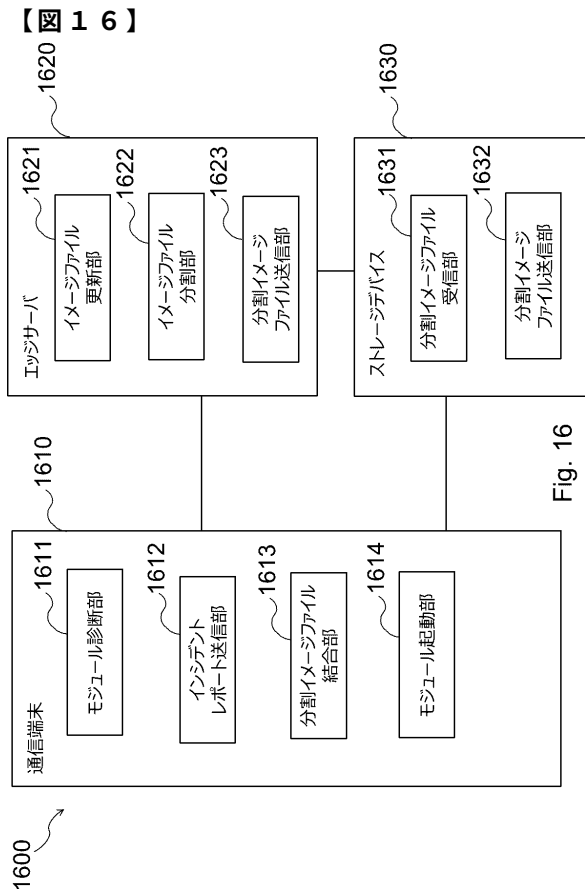


Fig. 16

10

20

30

40

50

フロントページの続き

- (56)参考文献 坂田 浩二、鈴木 薫、井上 博之、前田 香織、移動体デジタルサイネージシステムの遠隔監視、第3回インターネットと運用技術シンポジウム（I O T S 2 0 1 0），日本，情報処理学会，2010年12月02日，2010巻，pp.89-96
- (58)調査した分野 (Int.Cl.，D B名)
- G 0 6 F 2 1 / 5 5
- G 0 6 F 1 1 / 0 7