

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2020-136701

(P2020-136701A)

(43) 公開日 令和2年8月31日(2020.8.31)

(51) Int.Cl.			F I			テーマコード (参考)		
HO4L	12/66	(2006.01)	HO4L	12/66	B	5B089		
HO4L	12/24	(2006.01)	HO4L	12/24		5K030		
HO4L	12/28	(2006.01)	HO4L	12/28	200Z	5K033		
GO6F	13/00	(2006.01)	HO4L	12/28	200M			
			GO6F	13/00	351Z			

審査請求 未請求 請求項の数 7 O L (全 15 頁)

(21) 出願番号 特願2019-23052 (P2019-23052)
 (22) 出願日 平成31年2月12日 (2019.2.12)

(71) 出願人 000004226
 日本電信電話株式会社
 東京都千代田区大手町一丁目5番1号
 (74) 代理人 110002147
 特許業務法人酒井国際特許事務所
 (72) 発明者 野村 公輝
 東京都千代田区大手町一丁目5番1号 日
 本電信電話株式会社内
 (72) 発明者 永淵 幸雄
 東京都千代田区大手町一丁目5番1号 日
 本電信電話株式会社内
 (72) 発明者 張 一凡
 東京都千代田区大手町一丁目5番1号 日
 本電信電話株式会社内

最終頁に続く

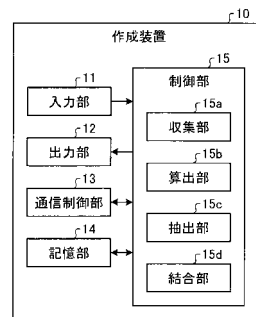
(54) 【発明の名称】 作成装置、作成システム、作成方法および作成プログラム

(57) 【要約】

【課題】IoTゲートウェイに適用するホワイトリストを、容量を抑えて迅速に作成する。

【解決手段】収集部15aが、IoTゲートウェイに接続されているIoT機器の情報と、IoTゲートウェイが記憶する、IoT機器ごとに許可される通信の内容を指定するホワイトリストとを収集する。算出部15bが、収集されたIoT機器情報に基づいて、IoTゲートウェイごとのIoT機器の通信の特徴を示す特徴量と、IoTゲートウェイ間の該特徴量の類似度とを算出する。抽出部15cが、算出された類似度が所定の閾値以上である場合に、各IoTゲートウェイが記憶するホワイトリストに含まれる各IoT機器のホワイトリスト情報から、各ホワイトリストを相互に補完するIoT機器のホワイトリスト情報を抽出する。結合部15dが、抽出されたホワイトリスト情報と、各IoTゲートウェイが記憶するホワイトリストとを結合する。

【選択図】図3



【特許請求の範囲】**【請求項 1】**

I o T (Internet of Things) ゲートウェイに接続されている I o T 機器の情報と、I o T ゲートウェイが記憶する、I o T 機器ごとに許可される通信の内容を指定するホワイトリストとを収集する収集部と、

収集された前記 I o T 機器の情報に基づいて、I o T ゲートウェイごとの I o T 機器の通信の特徴を示す特徴量と、I o T ゲートウェイ間の該特徴量の類似度とを算出する算出部と、

算出された前記類似度が所定の閾値以上である場合に、各 I o T ゲートウェイが記憶するホワイトリストに含まれる各 I o T 機器のホワイトリスト情報から、各ホワイトリストを相互に補完する I o T 機器のホワイトリスト情報を抽出する抽出部と、

を備えることを特徴とする作成装置。

【請求項 2】

前記算出部は、前記 I o T ゲートウェイごとの前記 I o T 機器の機種ごとの台数と、該機種ごとの通信の特徴とに基づいて、前記特徴量を算出することを特徴とする請求項 1 に記載の作成装置。

【請求項 3】

前記算出部は、ベクトル間の類似度の算出手法に基づいて、前記特徴量の類似度を算出することを特徴とする請求項 1 に記載の作成装置。

【請求項 4】

さらに、抽出された前記ホワイトリスト情報と、各 I o T ゲートウェイが記憶するホワイトリストとを結合する結合部を備えることを特徴とする請求項 1 に記載の作成装置。

【請求項 5】

作成装置と、I o T (Internet of Things) ゲートウェイとを有する作成システムであって、

前記作成装置は、

I o T ゲートウェイに接続されている I o T 機器の情報と、I o T ゲートウェイが記憶する、I o T 機器ごとに許可される通信の内容を指定するホワイトリストとを収集する収集部と、

収集された前記 I o T 機器の情報に基づいて、I o T ゲートウェイごとの I o T 機器の通信の特徴を示す特徴量と、I o T ゲートウェイ間の該特徴量の類似度とを算出する算出部と、

算出された前記類似度が所定の閾値以上である場合に、各 I o T ゲートウェイが記憶するホワイトリストに含まれる各 I o T 機器のホワイトリスト情報から、各ホワイトリストを相互に補完する I o T 機器のホワイトリスト情報を抽出する抽出部と、を備え、

前記 I o T ゲートウェイは、

抽出された前記ホワイトリスト情報と、自装置が記憶するホワイトリストとを結合する結合部を備える

ことを特徴とする作成システム。

【請求項 6】

作成装置で実行される作成方法であって、

I o T (Internet of Things) ゲートウェイに接続されている I o T 機器の情報と、I o T ゲートウェイが記憶する、I o T 機器ごとに許可される通信の内容を指定するホワイトリストとを収集する収集工程と、

収集された前記 I o T 機器の情報に基づいて、I o T ゲートウェイごとの I o T 機器の通信の特徴を示す特徴量と、I o T ゲートウェイ間の該特徴量の類似度とを算出する算出工程と、

算出された前記類似度が所定の閾値以上である場合に、各 I o T ゲートウェイが記憶するホワイトリストに含まれる各 I o T 機器のホワイトリスト情報から、各ホワイトリストを相互に補完する I o T 機器のホワイトリスト情報を抽出する抽出工程と、

10

20

30

40

50

を含んだことを特徴とする作成方法。

【請求項 7】

IoTゲートウェイに接続されているIoT機器の情報と、IoTゲートウェイが記憶する、IoT機器ごとに許可される通信の内容を指定するホワイトリストとを収集する収集ステップと、

収集された前記IoT機器の情報に基づいて、IoTゲートウェイごとのIoT機器の通信の特徴を示す特徴量と、IoTゲートウェイ間の該特徴量の類似度とを算出する算出ステップと、

算出された前記類似度が所定の閾値以上である場合に、各IoTゲートウェイが記憶するホワイトリストに含まれる各IoT機器のホワイトリスト情報から、各ホワイトリストを相互に補完するIoT機器のホワイトリスト情報を抽出する抽出ステップと、

をコンピュータに実行させるための作成プログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、作成装置、作成システム、作成方法および作成プログラムに関する。

【背景技術】

【0002】

カメラや温湿度センサー等の機器をIoT (Internet of Things) 機器として通信ネットワークにつなげるIoTゲートウェイが知られている(非特許文献1参照)。IoT機器はパソコンと比較してリソースが少ないため、セキュリティ対策ソフトウェアを導入することは困難な場合がある。

【0003】

そこで、IoT機器のセキュリティ対策として、許可する通信をリスト化したホワイトリストをIoTゲートウェイに適用し、ホワイトリストにない通信をアクセス不可にするアクセス制御が行われる。

【先行技術文献】

【非特許文献】

【0004】

【非特許文献1】“エッジゲートウェイ”、[online]、NEC、[2018年2月2日検索]、インターネット<URL:<http://jpn.nec.com/iot/platform/egw/index.html>>

【発明の概要】

【発明が解決しようとする課題】

【0005】

しかしながら、IoTゲートウェイに適用するホワイトリストの作成には、時間がかかるといった問題があった。一般に、ホワイトリストの作成には、機械学習が有効であるが、機械学習によるホワイトリストの作成には、数日程度の期間を要する場合がある。この機械学習によるホワイトリスト作成期間にも、IoT機器が危険なサイトにアクセスする可能性があるため、セキュリティ対策が不可欠である。

【0006】

本発明は、上記に鑑みてなされたものであって、IoTゲートウェイに適用するホワイトリストを、容量を抑えて迅速に作成すること目的とする。

【課題を解決するための手段】

【0007】

上述した課題を解決し、目的を達成するために、本発明に係る作成装置は、IoT (Internet of Things) ゲートウェイに接続されているIoT機器の情報と、IoTゲートウェイが記憶する、IoT機器ごとに許可される通信の内容を指定するホワイトリストとを収集する収集部と、収集された前記IoT機器の情報に基づいて、IoTゲートウェイごとのIoT機器の通信の特徴を示す特徴量と、IoTゲートウェイ間の該特徴量の類似度とを算出する算出部と、算出された前記類似度が所定の閾値以上である場合に、各IoT

10

20

30

40

50

Tゲートウェイが記憶するホワイトリストに含まれる各IoT機器のホワイトリスト情報から、各ホワイトリストを相互に補完するIoT機器のホワイトリスト情報を抽出する抽出部と、を備えることを特徴とする。

【発明の効果】

【0008】

本発明によれば、IoTゲートウェイに適用するホワイトリストを、容量を抑えて迅速に作成することができる。

【図面の簡単な説明】

【0009】

【図1】図1は、本実施形態に係る作成システムの概要構成を例示する模式図である。 10

【図2】図2は、本実施形態に係る作成装置の処理概要を説明するための図である。

【図3】図3は、作成装置の概略構成を例示する模式図である。

【図4】図4は、算出部の処理を説明するための図である。

【図5】図5は、抽出部の処理を説明するための図である。

【図6】図6は、作成装置による作成処理手順を示すフローチャートである。

【図7】図7は、作成プログラムを実行するコンピュータの一例を示す図である。

【発明を実施するための形態】

【0010】

以下、図面を参照して、本発明の一実施形態を詳細に説明する。なお、この実施形態により本発明が限定されるものではない。また、図面の記載において、同一部分には同一の符号を付して示している。 20

【0011】

[作成システムの構成]

図1は、本実施形態に係る作成システムの概略構成を例示する模式図である。図1に例示するように、作成システム1は、IoTゲートウェイ2と作成装置10とを有する。IoT機器3は、例えば、カメラやセンサー等の通常はネットワークNに接続されていない機器であり、Bluetooth（登録商標）や無線LAN等でIoTゲートウェイ2に接続される。

【0012】

IOTゲートウェイ2は、配下のIoT機器3をネットワークNに接続するネットワーク装置であり、NP（Network Processor）やFPGA（Field Programmable Gate Array）等で実現される。 30

【0013】

各IoTゲートウェイ2は、自装置の配下のIoT機器3の情報を定期的に収集している。例えば、図1に例示するように、各IoTゲートウェイ2は、IoT機器3の機種と、それぞれの機種の台数と、自IoTゲートウェイ2との間の通信の特徴とを収集している。

【0014】

また、本実施形態において、通信の特徴は、例えば、通信頻度と通信容量との組み合わせで表される。例えば、通信頻度は定期、不定期のいずれかで表される。また、通信容量は、大容量、中容量、または小容量のいずれかで表される。 40

【0015】

図1には、IoT-GW(A)の配下に、IoT機器(a)が3台接続され、このIoT機器(a)の通信特徴が「定期/中容量」であることが例示されている。また、このIoT-GW(A)の配下には、IoT機器(b)が1台接続され、このIoT機器(b)の通信特徴が「不定期/大容量」であることが例示されている。

【0016】

また、各IoTゲートウェイ2は、ホワイトリストを記憶している。ホワイトリストとは、配下のIoT機器3の機種ごとに、アクセス可能なサイト等の許可される通信の内容を指定する情報である。各IoTゲートウェイ2のホワイトリストは、配下の各IoT機 50

器3のホワイトリスト情報の集合である。

【0017】

図1に示す例では、IoT-GW(A)のホワイトリストには、配下のIoT機器(a)のホワイトリスト情報と、IoT機器(b)のホワイトリスト情報が含まれていることが例示されている。また、図1には、このIoT機器(a)のホワイトリスト情報は、URL(a1)およびURL(a2)へのアクセスを許可するものであることが例示されている。また、図1には、このIoT機器(b)のホワイトリスト情報は、URL(b1)およびURL(b2)へのアクセスを許可するものであることが例示されている。

【0018】

作成装置10は、ネットワークNに接続されている全てのIoTゲートウェイ2のうち、配下のIoT機器3の通信特徴が類似しているIoTゲートウェイ2間でIoT機器3のホワイトリスト情報を共有させる。これにより、各IoTゲートウェイ2には、自IoTゲートウェイ2に接続される可能性の高いIoT機器3のホワイトリスト情報のみを含む最新のホワイトリストが適用可能となる。

10

【0019】

ここで、図2は、本実施形態に係る作成システム1の処理概要を説明するための説明図である。図2に例示するように、作成システム1において、作成装置10は、各IoTゲートウェイ2が記憶する既存のホワイトリストと、各IoTゲートウェイ2の配下のIoT機器情報とを収集する(ステップ(1))。

【0020】

具体的には、作成装置10は、各IoTゲートウェイ2の配下のIoT機器情報として、IoT機器3の機種とそれぞれの機種の台数と自IoTゲートウェイ2との間の通信の特徴とを収集している。

20

【0021】

そして、作成装置10は、IoTゲートウェイ2ごとに、配下のIoT機器3の通信の特徴を示す特徴量と、IoTゲートウェイ2間での特徴量の類似度とを算出する(ステップ(2))。

【0022】

また、作成装置10は、IoTゲートウェイ2ごとおよびIoT機器3ごとに、ホワイトリスト情報を集計する(ステップ(3))。そして、作成装置10は、IoTゲートウェイ2間の類似度を参照し、類似度が所定の閾値以上に高い場合に、各IoTゲートウェイのホワイトリストを補完するIoT機器3のホワイトリスト情報を抽出し、暫定的なホワイトリストとする(ステップ(4)~(5))。

30

【0023】

図2に示す例では、類似度が60%以上の場合に、IoTゲートウェイ2の特徴量が類似するものとされている。そして、作成装置10は、特徴量が類似するIoTゲートウェイ2間で所望のIoT機器3のホワイトリスト情報が同一になるように、それぞれのIoTゲートウェイ2に対する暫定的なホワイトリストを作成する。つまり、暫定的なホワイトリストとは、それぞれのIoTゲートウェイ2の既存のホワイトリストを補完するためのIoT機器3のホワイトリスト情報の集合である。

40

【0024】

図2に示す例では、IoT-GW(A)とIoT-GW(C)との間で所望のIoT機器3のホワイトリスト情報が同一になるように、暫定的なホワイトリストが作成されている。例えば、IoT-GW(C)に対して、既存のホワイトリストを補完するために、IoT機器(a)のホワイトリスト情報を含む暫定的なホワイトリストが作成されている。

【0025】

各IoTゲートウェイ2では、既存のホワイトリストと暫定的なホワイトリストとを最新のホワイトリストとして適用する(ステップ(6))。これにより、類似度が高いIoTゲートウェイ2間でホワイトリストを共有することができる。各IoTゲートウェイ2では、新規のIoT機器3に対して、暫定的なホワイトリストを用いてアクセス制御が可

50

能となる。図2に示す例では、I o T - G W (C) では、暫定的なホワイトリストにより、新規のI o T 機器 (a) のアクセス制御が可能となっている。

【 0 0 2 6 】

また、作成装置 1 0 は、各 I o T ゲートウェイ 2 に接続される可能性が低い I o T 機器 3 のホワイト情報を除外して暫定的なホワイトリストを作成することができる。図2に示す例では、I o T - G W (C) との類似度が低い I o T - G W (B) との間では、ホワイトリストは共有されない。例えば、I o T 機器 (c) のホワイトリスト情報は、I o T - G W (B) のホワイトリストに含まれているが、I o T - G W (C) の既存のホワイトリストにも暫定的なホワイトリストにも含まれていない。これにより、作成装置 1 0 は、容量を抑えて暫定的なホワイトリストを作成することが可能となる。

10

【 0 0 2 7 】

[作成装置の構成]

図3は、作成装置 1 0 の概略構成を例示する模式図である。図3に例示するように、作成装置 1 0 は、パソコン等の汎用コンピュータで実現され、入力部 1 1、出力部 1 2、通信制御部 1 3、記憶部 1 4、および制御部 1 5 を備える。

【 0 0 2 8 】

入力部 1 1 は、キーボードやマウス等の入力デバイスによって実現され、操作者による入力操作に対応して、制御部 1 5 に対して処理開始などの各種指示情報を入力する。出力部 1 2 は、液晶ディスプレイなどの表示装置、プリンター等の印刷装置等によって実現される。

20

【 0 0 2 9 】

通信制御部 1 3 は、N I C (Network Interface Card) 等で実現され、L A N (Local Area Network) やインターネット等の電気通信回線を介した I o T ゲートウェイ 2 等の外部の装置と制御部 1 5 との通信を制御する。

【 0 0 3 0 】

記憶部 1 4 は、R A M (Random Access Memory)、フラッシュメモリ (Flash Memory) 等の半導体メモリ素子、または、ハードディスク、光ディスク等の記憶装置によって実現される。記憶部 1 4 には、作成装置 1 0 を動作させる処理プログラムや、処理プログラムの実行中に使用されるデータなどが予め記憶され、あるいは処理の都度一時的に記憶される。例えば、記憶部 1 4 には、後述する作成処理において I o T ゲートウェイ 2 から収集された I o T 機器情報やホワイトリスト等が記憶される。なお、記憶部 1 4 は、通信制御部 1 3 を介して制御部 1 5 と通信する構成でもよい。

30

【 0 0 3 1 】

制御部 1 5 は、C P U (Central Processing Unit) 等によって実現され、メモリに記憶された処理プログラムを実行する。これにより、制御部 1 5 は、図4に例示するように、収集部 1 5 a、算出部 1 5 b、抽出部 1 5 c および結合部 1 5 d として機能する。なお、これらの機能部は、それぞれ、あるいは一部が異なるハードウェアに実装されてもよい。例えば、結合部 1 5 d は、I o T ゲートウェイ 2 に実装されてもよい。

【 0 0 3 2 】

収集部 1 5 a は、I o T ゲートウェイ 2 に接続されている I o T 機器 3 の情報と、I o T ゲートウェイ 2 が記憶する、I o T 機器 3 ごとに許可される通信の内容を指定するホワイトリストとを収集する。具体的には、収集部 1 5 a は、ネットワーク N に接続されている全ての I o T ゲートウェイ 2 から、各 I o T ゲートウェイ 2 が定期的に収集している I o T 機器情報と、各 I o T ゲートウェイ 2 が記憶する既存のホワイトリストとを収集する。

40

【 0 0 3 3 】

図2に示した例では、収集部 1 5 a は、I o T - G W (A) から、I o T 機器 (a)、I o T 機器 (b) 等の配下の I o T 機器 3 の機種ごとの台数と、通信特徴とを含む I o T 機器情報を収集する。また、収集部 1 5 a は、I o T - G W (B) から、I o T 機器 (a)、I o T 機器 (c) 等の配下の I o T 機器 3 の機種ごとの台数と、通信特徴とを含む I

50

IoT機器情報を収集する。

【0034】

そして、収集部15aは、各IoTゲートウェイ2から収集したIoT機器情報を、IoTゲートウェイ2ごとおよびIoT機器3ごとに集約する。図2に示した例では、例えば、IoT-GW(A)の配下に、通信特徴「定期/中容量」であるIoT機器(a)が3台存在することが示されている。

【0035】

また、収集部15aは、IoT-GW(A)から、IoT機器(a)のURL(a1)およびURL(a2)へのアクセスを許可するホワイトリスト情報、IoT機器(b)のURL(b1)およびURL(b3)へのアクセスを許可するホワイトリスト情報等を含むホワイトリストを収集している。また、収集部15aは、IoT-GW(B)から、IoT機器(a)のURL(a1)およびURL(a3)へのアクセスを許可するホワイトリスト情報、IoT機器(c)のURL(c1)およびURL(c2)へのアクセスを許可するホワイトリスト情報等を含むホワイトリストを収集している。

10

【0036】

図3の説明に戻る。算出部15bは、収集されたIoT機器3の情報に基づいて、IoTゲートウェイ2ごとのIoT機器3の通信の特徴を示す特徴量と、IoTゲートウェイ2間の該特徴量の類似度とを算出する。

【0037】

例えば、算出部15bは、IoTゲートウェイ2ごとのIoT機器3の機種ごとの台数と、該機種ごとの通信の特徴とに基づいて特徴量を算出する。また、算出部15bは、例えば、機種ごとの台数と通信の頻度と容量とに基づいて特徴量を算出する。

20

【0038】

ここで、図4は、算出部15bの処理を説明するための図である。図4に示す例では、算出部15bは、特徴量として、各IoTゲートウェイ2の配下のIoT機器3の通信特徴ごとの台数の割合を用いて、通信特徴のベクトルを算出している。

【0039】

具体的には、算出部15bは、まず、図4(1)に示すように、収集部15aが収集したIoT機器情報をIoTゲートウェイ2ごとおよびIoT機器3ごとに集約する。図4に示す例では、各IoT機器3の通信特徴は、通信特徴1および通信特徴2の組み合わせで表されている。通信特徴1は、通信頻度であり、定期、不定期のいずれかで表されている。また、通信特徴2は、通信容量であり、大容量、中容量、小容量のいずれかで表されている。例えば、図4(1)には、IoT-GW(A)の配下には、通信特徴1「定期」、通信特徴2「中容量」のIoT機器(a)が3台存在することが示されている。

30

【0040】

そして、算出部15bは、図4(2)に示すように、IoTゲートウェイ2ごとの通信特徴のベクトルを算出する。図4に示す例では、通信特徴のベクトルは、各通信特徴のIoTゲートウェイ2での台数の割合の要素としたベクトルである。

【0041】

例えば、通信特徴のベクトルの1番目の要素は、通信特徴1が「定期」であるIoT機器3の各IoTゲートウェイ2での割合である。図4(2)に示す例では、IoT-GW(A)についての通信特徴のベクトルAの1番目の要素は、配下の5台のIoT機器3のうち通信特徴1が「定期」であるIoT機器3は4台であるので、0.8と算出されている。

40

【0042】

また、例えば、通信特徴のベクトルの5番目の要素は、通信特徴2が「小容量」であるIoT機器3のIoTゲートウェイ2での割合である。図4(2)に示す例では、IoT-GW(A)についての通信特徴のベクトルAの5番目の要素は、配下の5台のIoT機器3のうち通信特徴2が「小容量」であるIoT機器3は1台であるので、0.2と算出されている。

50

【 0 0 4 3 】

次に、算出部 1 5 b は、図 4 (3) および (4) に示すように、I o T ゲートウェイ 2 間での通信特徴のベクトルの類似度を算出する。類似度の算出手法は特に限定されず、算出部 1 5 b は、例えば、ベクトル間のコサイン類似度や、一般化 J a c c a r d 類似度等を算出する。算出部 1 5 b は、類似度として、複数の算出手法による類似度の平均値を算出してよい。図 4 (3) に示す例では、算出部 1 5 b は、類似度として、ベクトル間のコサイン類似度を算出している。そして、算出部 1 5 b は、図 4 (4) に示すように、I o T ゲートウェイ 2 間の通信特徴のベクトルの類似度を算出する。

【 0 0 4 4 】

図 3 の説明に戻る。抽出部 1 5 c は、算出された類似度が所定の閾値以上である場合に、各 I o T ゲートウェイ 2 が記憶するホワイトリストに含まれる各 I o T 機器 3 のホワイトリスト情報から、各ホワイトリストを相互に補完する I o T 機器 3 のホワイトリスト情報を抽出する。また、抽出部 1 5 c は、抽出したホワイトリスト情報を用いて、各 I o T ゲートウェイ 2 に適用する暫定的なホワイトリストを作成する。

10

【 0 0 4 5 】

ここで、図 5 は、抽出部 1 5 c の処理を説明するための図である。図 5 の例では、抽出部 1 5 c は、類似度が 6 0 % 以上の I o T ゲートウェイ 2 の組み合わせを対象としている。そして、抽出部 1 5 c は、対象の I o T ゲートウェイ 2 間で所望の I o T 機器 3 のホワイトリスト情報が同一になるように、各 I o T ゲートウェイ 2 の既存のホワイトリストを補完する暫定的なホワイトリストを作成する。

20

【 0 0 4 6 】

例えば、抽出部 1 5 c は、収集部 1 5 a が収集した、図 5 (1) に例示する I o T ゲートウェイ 2 の既存のホワイトリストを、図 5 (2) に示すように、I o T 機器 3 ごとに集計する。そして、抽出部 1 5 c は、算出部 1 5 b が算出した、図 5 (3) に例示する I o T ゲートウェイ 2 間の類似度を参照し、類似度が 6 0 % 以上の I o T ゲートウェイ 2 の組み合わせを選定する。図 5 (3) に示す例では、I o T - G W (A) と I o T - G W (B) との組み合わせが 7 8 % であることから、相互に類似する I o T ゲートウェイ 2 として選定される。

【 0 0 4 7 】

そして、抽出部 1 5 c は、図 5 (4) に示すように、類似する I o T ゲートウェイ 2 間で所望の I o T 機器 3 のホワイトリスト情報が同一になるように、相互に補完する I o T 機器 3 のホワイトリスト情報を抽出する。図 5 (4) に示す例では、例えば、I o T - G W (B) に対して、I o T - G W (A) の既存のホワイトリストに含まれていて I o T - G W (B) の既存のホワイトリストに含まれていない I o T 機器 (b) のホワイトリスト情報が抽出されている。ここでは、他ではなく I o T - G W (A) で現に機能している I o T 機器 (b) の U R L (b 1) および U R L (b 3) へのアクセスを許可するホワイトリスト情報が抽出される。

30

【 0 0 4 8 】

同様に、I o T - G W (B) に対して、I o T 機器 (c) のホワイトリスト情報が抽出される。このように、I o T - G W (B) に対して、I o T 機器 (b) のホワイトリスト情報と I o T 機器 (c) のホワイトリスト情報が抽出される。抽出部 1 5 c は、I o T G W (B) に対して、I o T 機器 (b) のホワイトリスト情報と I o T 機器 (c) のホワイトリスト情報とを含む暫定的なホワイトリストを作成する。

40

【 0 0 4 9 】

図 3 の説明に戻る。結合部 1 5 d は、抽出されたホワイトリスト情報と、各 I o T ゲートウェイ 2 が記憶するホワイトリストとを結合する。具体的には、結合部 1 5 d は、抽出されたホワイトリスト情報を用いて作成された暫定的なホワイトリストと、各 I o T ゲートウェイ 2 が記憶するホワイトリストとを結合して、各 I o T ゲートウェイ 2 に適用するホワイトリストを作成する。

【 0 0 5 0 】

50

すなわち、結合部 15 d は、各 I o T ゲートウェイ 2 の既存のホワイトリストと、抽出部 15 c が作成した暫定的なホワイトリストとを結合して、各 I o T ゲートウェイ 2 に適用する最新のホワイトリストを作成する。各 I o T ゲートウェイ 2 は、既存の I o T 機器 3 には、既存のホワイトリストを適用し、新規の I o T 機器 3 には暫定的なホワイトリストを適用する。

【 0 0 5 1 】

例えば、図 5 に示した例では、I o T - G W (B) は、I o T 機器 (a) および I o T 機器 (d) に対しては、既存のホワイトリストによりアクセス制御を行う。また、I o T - G W (B) は、新規の I o T 機器 (b) および I o T 機器 (c) に対しては、暫定的なホワイトリストでアクセス制御を行う。

10

【 0 0 5 2 】

同様に、I o T - G W (A) は、I o T 機器 (a)、I o T 機器 (b) および I o T 機器 (c) に対しては、既存のホワイトリストによりアクセス制御を行う。また、I o T - G W (A) は、新規の I o T 機器 (d) に対しては、暫定的なホワイトリストでアクセス制御を行う。

【 0 0 5 3 】

このように、作成装置 1 0 により、類似する I o T ゲートウェイ 2 間でホワイトリストを共有することができる。各 I o T ゲートウェイ 2 では、新規の I o T 機器 3 に対して、暫定的なホワイトリストを用いてアクセス制御が可能となる。また、各 I o T ゲートウェイ 2 に接続される可能性が低い I o T 機器 3 のホワイト情報が除外された、容量を抑えた暫定的なホワイトリストが作成される。

20

【 0 0 5 4 】

なお、結合部 15 d は、I o T ゲートウェイ 2 に実装されてもよい。その場合には、作成装置 1 0 は、抽出部 15 c が作成した暫定的なホワイトリストを、通信制御部 1 3 を介して各 I o T ゲートウェイ 2 に配信する。

【 0 0 5 5 】

[作成処理]

図 6 は、本実施形態に係る作成装置 1 0 による作成処理手順を示すフローチャートである。図 6 のフローチャートは、例えば、開始を指示する操作入力があったタイミングで開始される。

30

【 0 0 5 6 】

まず、収集部 15 a が、ネットワーク N に接続されている全ての I o T ゲートウェイ 2 から、各 I o T ゲートウェイ 2 が定期的に収集している I o T 機器情報と、各 I o T ゲートウェイ 2 が記憶する既存のホワイトリストとを収集する (ステップ S 1)。例えば、I o T 機器情報には、I o T 機器 3 の機種とそれぞれの機種の台数と自 I o T ゲートウェイ 2 との間の通信の特徴とが含まれる。

【 0 0 5 7 】

次に、算出部 15 b が、収集された I o T 機器情報に基づいて、I o T ゲートウェイ 2 ごとに配下の I o T 機器 3 の通信の特徴を示す特徴量と、I o T ゲートウェイ 2 間の該特徴量の類似度とを算出する (ステップ S 2)。例えば、算出部 15 b は、各 I o T ゲートウェイ 2 の配下の I o T 機器 3 の通信特徴ごとの台数の割合に基づいて、特徴量を算出する。

40

【 0 0 5 8 】

次に、抽出部 15 c が、算出された類似度が所定の閾値以上である場合に、各 I o T ゲートウェイ 2 が記憶するホワイトリストに含まれる各 I o T 機器 3 のホワイトリスト情報から、各ホワイトリストを相互に補完する I o T 機器 3 のホワイトリスト情報を抽出する。また、抽出部 15 c は、各 I o T ゲートウェイ 2 に対して、抽出したホワイトリスト情報を含む暫定的なホワイトリストを作成する (ステップ S 3)。

【 0 0 5 9 】

すなわち、抽出部 15 c は、類似する I o T ゲートウェイ 2 間で所望の I o T 機器 3 の

50

ホワイトリスト情報が同一になるように、それぞれのIoTゲートウェイ2に対する暫定的なホワイトリストを作成する。

【0060】

また、結合部15dが、各IoTゲートウェイ2の既存のホワイトリストと、抽出部15cが作成した暫定的なホワイトリストとを結合して、各IoTゲートウェイ2に適用する最新のホワイトリストを作成する(ステップS4)。これにより、一連の作成処理が終了する。

【0061】

以上、説明したように、本実施形態の作成装置10において、収集部15aが、IoTゲートウェイ2に接続されているIoT機器3の情報と、IoTゲートウェイ2が記憶する、IoT機器3ごとに許可される通信の内容を指定するホワイトリストとを収集する。算出部15bが、収集されたIoT機器情報に基づいて、IoTゲートウェイ2ごとのIoT機器3の通信の特徴を示す特徴量と、IoTゲートウェイ2間の該特徴量の類似度とを算出する。抽出部15cが、算出された類似度が所定の閾値以上である場合に、各IoTゲートウェイ2が記憶するホワイトリストに含まれる各IoT機器3のホワイトリスト情報から、各ホワイトリストを相互に補完するIoT機器3のホワイトリスト情報を抽出する。

10

【0062】

これにより、ネットワークNに接続されている全てのIoTゲートウェイ2のうち、配下のIoT機器3の通信特徴が類似しているIoTゲートウェイ2間で、現に機能しているIoT機器3のホワイトリスト情報を共有することができる。したがって、各IoTゲートウェイ2に接続される可能性の高いIoT機器3のホワイトリスト情報のみを含む最新のホワイトリストを適用することが可能となる。

20

【0063】

このように、作成装置10は、機械学習によるホワイトリスト作成期間にも、IoTゲートウェイ2に適用するホワイトリストを迅速に作成することができる。また、自IoTゲートウェイ2に接続される可能性が低いIoT機器3のホワイト情報を除外することにより、容量を抑えてホワイトリストを作成することが可能となる。

【0064】

また、算出部15bは、例えば、IoTゲートウェイ2ごとのIoT機器3の機種ごとの台数と、該機種ごとの通信の特徴とに基づいて特徴量を算出する。また、算出部15bは、例えば、機種ごとの台数と通信の頻度と容量とに基づいて特徴量を算出する。これにより、IoTゲートウェイ2の配下のIoT機器3の通信の特徴を端的に表すことが可能となる。

30

【0065】

また、結合部15dが、抽出されたホワイトリスト情報と、各IoTゲートウェイ2が記憶するホワイトリストとを結合する。この結合部15dは、作成装置10に実装されてもよいし、IoTゲートウェイ2に実装されてもよい。これにより、柔軟にシステムを構成することが可能となる。

【0066】

40

[プログラム]

上記実施形態に係る作成装置10が実行する処理をコンピュータが実行可能な言語で記述したプログラムを作成することもできる。一実施形態として、作成装置10は、パッケージソフトウェアやオンラインソフトウェアとして上記の作成処理を実行する作成プログラムを所望のコンピュータにインストールさせることによって実装できる。例えば、上記の作成プログラムを情報処理装置に実行させることにより、情報処理装置を作成装置10として機能させることができる。ここで言う情報処理装置には、デスクトップ型またはノート型のパーソナルコンピュータが含まれる。また、その他にも、情報処理装置にはスマートフォン、携帯電話機やPHS(Personal Handyphone System)などの移動体通信端末、さらには、PDA(Personal Digital Assistant)などのスレート端末などがその

50

範疇に含まれる。また、作成装置 10 の機能を、クラウドサーバに実装してもよい。

【0067】

図7は、作成プログラムを実行するコンピュータの一例を示す図である。コンピュータ1000は、例えば、メモリ1010と、CPU1020と、ハードディスクドライブインタフェース1030と、ディスクドライブインタフェース1040と、シリアルポートインタフェース1050と、ビデオアダプタ1060と、ネットワークインタフェース1070とを有する。これらの各部は、バス1080によって接続される。

【0068】

メモリ1010は、ROM(Read Only Memory)1011およびRAM1012を含む。ROM1011は、例えば、BIOS(Basic Input Output System)等のブートプログラムを記憶する。ハードディスクドライブインタフェース1030は、ハードディスクドライブ1031に接続される。ディスクドライブインタフェース1040は、ディスクドライブ1041に接続される。ディスクドライブ1041には、例えば、磁気ディスクや光ディスク等の着脱可能な記憶媒体が挿入される。シリアルポートインタフェース1050には、例えば、マウス1051およびキーボード1052が接続される。ビデオアダプタ1060には、例えば、ディスプレイ1061が接続される。

10

【0069】

ここで、ハードディスクドライブ1031は、例えば、OS1091、アプリケーションプログラム1092、プログラムモジュール1093およびプログラムデータ1094を記憶する。上記実施形態で説明した各情報は、例えばハードディスクドライブ1031

20

【0070】

また、作成プログラムは、例えば、コンピュータ1000によって実行される指令が記述されたプログラムモジュール1093として、ハードディスクドライブ1031に記憶される。具体的には、上記実施形態で説明した作成装置10が実行する各処理が記述されたプログラムモジュール1093が、ハードディスクドライブ1031に記憶される。

【0071】

また、作成プログラムによる情報処理に用いられるデータは、プログラムデータ1094として、例えば、ハードディスクドライブ1031に記憶される。そして、CPU1020が、ハードディスクドライブ1031に記憶されたプログラムモジュール1093やプログラムデータ1094を必要に応じてRAM1012に読み出して、上述した各手順を実行する。

30

【0072】

なお、作成プログラムに係るプログラムモジュール1093やプログラムデータ1094は、ハードディスクドライブ1031に記憶される場合に限られず、例えば、着脱可能な記憶媒体に記憶されて、ディスクドライブ1041等を介してCPU1020によって読み出されてもよい。あるいは、作成プログラムに係るプログラムモジュール1093やプログラムデータ1094は、LANやWAN(Wide Area Network)等のネットワークを介して接続された他のコンピュータに記憶され、ネットワークインタフェース1070を介してCPU1020によって読み出されてもよい。

40

【0073】

以上、本発明者によってなされた発明を適用した実施形態について説明したが、本実施形態による本発明の開示の一部をなす記述および図面により本発明は限定されることはない。すなわち、本実施形態に基づいて当業者等によりなされる他の実施形態、実施例および運用技術等は全て本発明の範疇に含まれる。

【符号の説明】

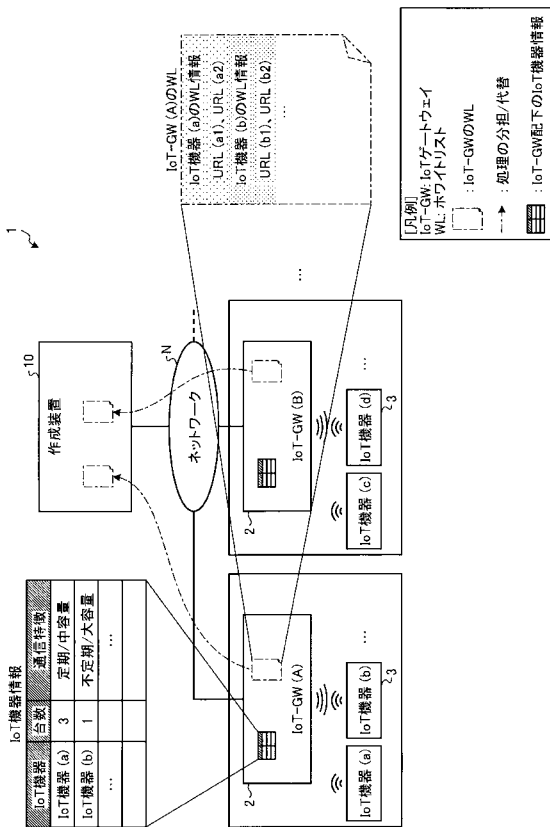
【0074】

- 1 作成システム
- 2 I o T ゲートウェイ
- 3 I o T 機器

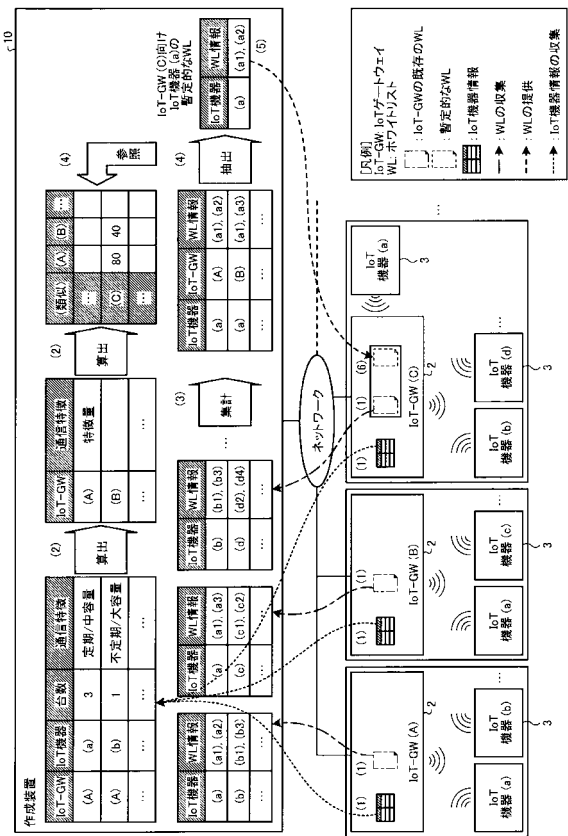
50

- 1 0 作成装置
- 1 1 入力部
- 1 2 出力部
- 1 3 通信制御部
- 1 4 記憶部
- 1 5 制御部
- 1 5 a 収集部
- 1 5 b 算出部
- 1 5 c 抽出部
- 1 5 d 結合部
- N ネットワーク

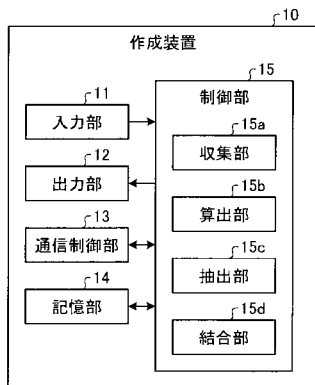
【図 1】



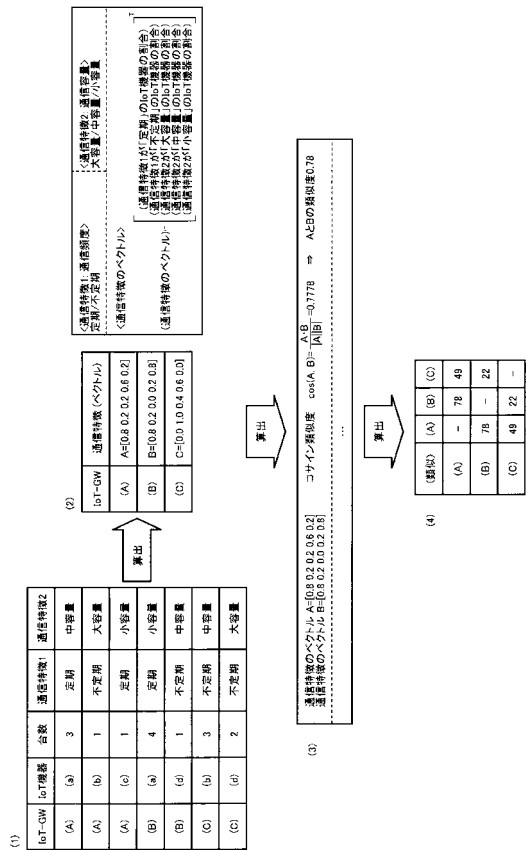
【図 2】



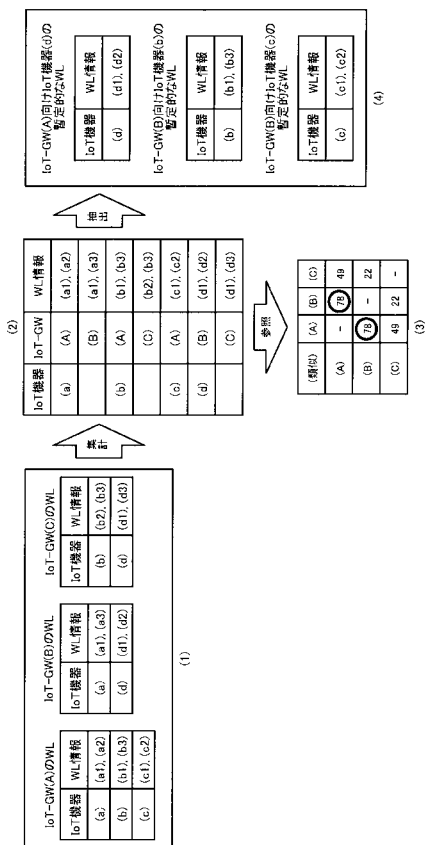
【図3】



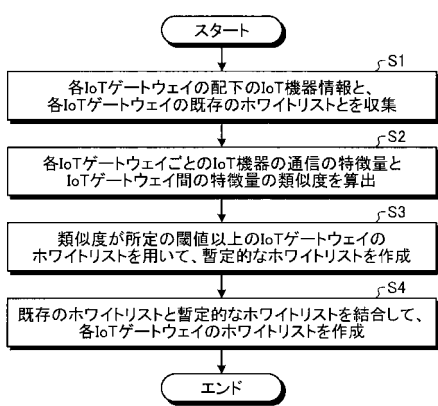
【図4】



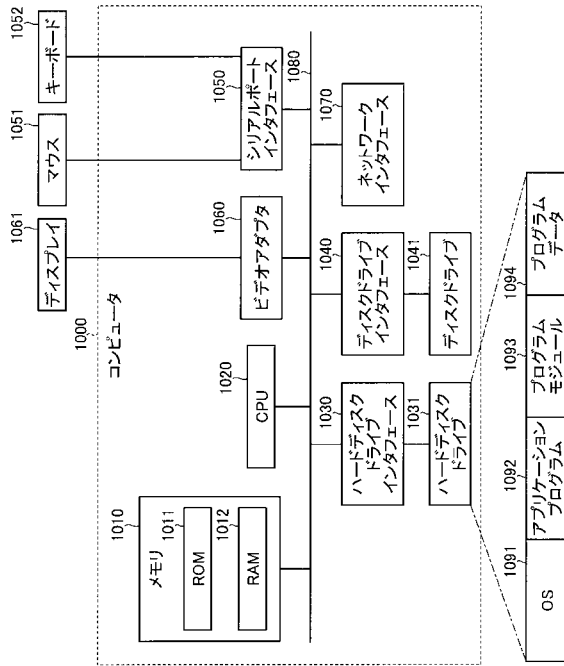
【図5】



【図6】



【 図 7 】



フロントページの続き

- (72)発明者 村田 哲彦
東京都千代田区大手町一丁目5番1号 日本電信電話株式会社内
- (72)発明者 森下 幸治
東京都千代田区大手町一丁目5番1号 日本電信電話株式会社内
- (72)発明者 太田 賢治
東京都千代田区大手町一丁目5番1号 日本電信電話株式会社内
- (72)発明者 向山 明夫
東京都千代田区大手町一丁目5番1号 日本電信電話株式会社内
- (72)発明者 温品 貴大
東京都千代田区大手町一丁目5番1号 日本電信電話株式会社内
- (72)発明者 長山 弘樹
東京都千代田区大手町一丁目5番1号 日本電信電話株式会社内
- (72)発明者 谷川 真樹
東京都千代田区大手町一丁目5番1号 日本電信電話株式会社内

Fターム(参考) 5B089 GA01 GA21 GA31 GB01 HA10 HB02 JB16 KA17 KB04 KC15
KC57 MC03
5K030 GA14 GA15 HD03 JA10 JT09 KA04 KA06 LD20
5K033 AA08 DA01 DB12 DB20