

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7535309号
(P7535309)

(45)発行日 令和6年8月16日(2024.8.16)

(24)登録日 令和6年8月7日(2024.8.7)

(51)国際特許分類

F I

G O 6 N 20/00 (2019.01)

G O 6 N 20/00

G O 6 N 3/02 (2006.01)

G O 6 N 3/02

請求項の数 17 (全36頁)

(21)出願番号	特願2021-507273(P2021-507273)	(73)特許権者	519094721
(86)(22)出願日	令和2年3月12日(2020.3.12)		株式会社Geek Guild
(86)国際出願番号	PCT/JP2020/010806		京都府京都市西京区御陵大原1番地36
(87)国際公開番号	WO2020/189496		京大桂ベンチャープラザ北館 310号室
(87)国際公開日	令和2年9月24日(2020.9.24)	(74)代理人	100098899
審査請求日	令和5年2月1日(2023.2.1)		弁理士 飯塚 信市
(31)優先権主張番号	特願2019-49137(P2019-49137)	(74)代理人	100163865
(32)優先日	平成31年3月15日(2019.3.15)		弁理士 飯塚 健
(33)優先権主張国・地域又は機関	日本国(JP)	(72)発明者	尾藤 美紀
(31)優先権主張番号	特願2019-49138(P2019-49138)		京都府京都市下京区中堂寺栗田町93
(32)優先日	平成31年3月15日(2019.3.15)		KRP4号館3階 KRP BIZNEX
(33)優先権主張国・地域又は機関	日本国(JP)	(72)発明者	T 株式会社Geek Guild内
			花村 慎介
			京都府京都市下京区中堂寺栗田町93
			KRP4号館3階 KRP BIZNEX
			最終頁に続く

(54)【発明の名称】 変換システム、方法及びプログラム

(57)【特許請求の範囲】

【請求項1】

クライアント装置と、前記クライアント装置とネットワークを介して接続されたサーバとを含み、機械学習により得られた学習済モデルに基づいて入力データに対する変換処理を行って出力データを生成する、変換システムであって、

前記クライアント装置は、

前記学習済モデルの入力段階から第1の中間段階へと至る前記学習済モデルの一部であって、前記入力データに基づいて変換処理を行うことにより前記学習済モデルの前記第1の中間段階における第1の中間出力を生成する、入力側変換処理部と、

前記第1の中間出力を前記サーバへと送信する、クライアント側送信部と、

前記第1の中間出力に由来して前記サーバにおいて生成され、前記学習済モデルの前記第1の中間段階より出力側に近い第2の中間段階における変換出力である、第2の中間出力を前記サーバから受信する、クライアント側受信部と、

前記学習済モデルの前記第2の中間段階から出力段階へと至る前記学習済モデルの一部であって、前記第2の中間出力に基づいて変換処理を行うことにより前記出力データを生成する、出力側変換処理部と、を備え、

前記クライアント装置は、さらに、

前記第1の中間出力と前記第2の中間出力との対応関係を表すキャッシュテーブルを記憶した、キャッシュテーブル記憶部と、

前記キャッシュテーブル中に前記第1の中間出力と対応する前記第2の中間出力が存在

するか否かを判定する、判定部と、

前記判定部において前記キャッシュテーブル中に前記第1の中間出力と対応する前記第2の中間出力が存在すると判定された場合には、前記クライアント側送信部と前記クライアント側受信部とを動作させることに代えて前記キャッシュテーブルから対応する前記第2の中間出力を取得し、一方、前記判定部において前記キャッシュテーブル中に前記第1の中間出力と対応する前記第2の中間出力が存在しないと判定された場合には、前記クライアント側送信部と前記クライアント側受信部とを動作させることにより前記クライアント側受信部において受信された前記第2の中間出力を取得する、選択的取得部と、を備える変換システム。

【請求項2】

前記クライアント装置は、さらに、

前記クライアント側受信部において受信された前記第2の中間出力を対応する前記第1の中間出力と対応付けて前記キャッシュテーブルへと記憶させるキャッシュテーブル記憶部を備える、請求項1に記載の変換システム。

【請求項3】

前記クライアント装置は、さらに、

前記第1の中間出力を暗号化して第1の暗号化中間出力を生成する暗号化部と、

前記サーバにより暗号化された第2の中間出力である第2の暗号化中間出力を復号化する復号化部と、を備え、

前記クライアント側送信部は、前記第1の暗号化中間出力を前記サーバへと送信し、

前記サーバは、受信した前記第1の暗号化中間出力を復号化して前記第1の中間出力を復元すると共に、前記第2の中間出力を暗号化して前記第2の暗号化中間出力を生成して前記クライアント装置へと送信し、

前記クライアント側受信部は、前記第2の暗号化中間出力を受信する、請求項1に記載の変換システム。

【請求項4】

前記クライアント装置は、さらに、

前記第1の暗号化中間出力をハッシュ化して第1のハッシュ値を生成する、ハッシュ化処理部を備え、

前記キャッシュテーブルにおける前記第1の中間出力は、前記第1のハッシュ値であり、

前記判定部は、前記第1のハッシュ値に基づいて、対応する前記第2の中間出力が存在するか否かを判定する、請求項3に記載の変換システム。

【請求項5】

前記クライアント装置は、さらに、

前記第1の中間出力を丸め処理して第1の丸め中間出力を生成する、値丸め処理部を備える、請求項4に記載の変換システム。

【請求項6】

前記クライアント装置は、さらに、

前記キャッシュテーブルに基づいて、近似関数を生成する近似関数生成部と、

前記第1の中間出力を入力として前記近似関数に基づいて前記第2の中間出力を生成する、近似変換処理部と、を備える、請求項1に記載の変換システム。

【請求項7】

前記近似関数は、誤差逆伝播法を適用可能な関数である、請求項6に記載の変換システム。

【請求項8】

前記近似関数は、バイパス関数を含むものである、請求項6に記載の変換システム。

【請求項9】

前記近似関数は、複数の異なる近似関数の重み付き和により構成される、請求項6に記載の変換システム。

【請求項10】

10

20

30

40

50

前記クライアント装置は複数から成り、

前記キャッシュテーブルは、複数の前記クライアント装置により共有される、請求項 1 に記載の変換システム。

【請求項 1 1】

前記サーバは、さらに、

前記第 1 の中間段階から前記第 2 の中間段階へと至る前記学習済モデルの一部であって、前記第 1 の中間出力に基づいて変換処理を行うことにより前記第 2 の中間段階における前記第 2 の中間出力を生成する、中間変換処理部を備える請求項 1 に記載の変換システム。

【請求項 1 2】

前記サーバは、ネットワークを介して接続された多段のサーバで構成され、

各サーバは、前記第 1 の中間段階と前記第 2 の中間段階との間の学習済モデルを分割した部分モデルをそれぞれ保持し、各サーバの各部分モデルに基づいて順に変換処理を行うことにより前記第 2 の中間出力を生成する、請求項 1 に記載の変換システム。

【請求項 1 3】

前記クライアント装置は、さらに、

前記入力データと、前記入力データと対応する前記出力データとの関係性を表す入出力データテーブルを記憶する入出力データテーブル記憶部を備える、請求項 1 に記載の変換システム。

【請求項 1 4】

ネットワークを介してサーバと接続され、機械学習により得られた学習済モデルに基づいて入力データに対する変換処理を行って出力データを生成する、クライアント装置であって、

前記学習済モデルの入力段階から第 1 の中間段階へと至る前記学習済モデルの一部であって、前記入力データに基づいて変換処理を行うことにより前記学習済モデルの前記第 1 の中間段階における第 1 の中間出力を生成する、入力側変換処理部と、

前記第 1 の中間出力を前記サーバへと送信する、クライアント側送信部と、

前記第 1 の中間出力に基づいて前記サーバにおいて生成され、前記学習済モデルの前記第 1 の中間段階より出力側に近い第 2 の中間段階における変換出力である第 2 の中間出力を前記サーバから受信する、クライアント側受信部と、

前記学習済モデルの前記第 2 の中間段階から出力段階へと至る前記学習済モデルの一部であって、前記第 2 の中間出力に基づいて変換処理を行うことにより前記出力データを生成する、出力側変換処理部と、を備え、

前記クライアント装置は、さらに、

前記第 1 の中間出力と前記第 2 の中間出力との対応関係を表すキャッシュテーブルを記憶した、キャッシュテーブル記憶部と、

前記キャッシュテーブル中に前記第 1 の中間出力と対応する前記第 2 の中間出力が存在するか否かを判定する、判定部と、

前記判定部において前記キャッシュテーブル中に前記第 1 の中間出力と対応する前記第 2 の中間出力が存在すると判定された場合には、前記クライアント側送信部と前記クライアント側受信部とを動作させることに代えて前記キャッシュテーブルから対応する前記第 2 の中間出力を取得し、一方、前記判定部において前記キャッシュテーブル中に前記第 1 の中間出力と対応する前記第 2 の中間出力が存在しないと判定された場合には、前記クライアント側送信部と前記クライアント側受信部とを動作させることにより前記クライアント側受信部において受信された前記第 2 の中間出力を取得する、選択的取得部と、を備える、クライアント装置。

【請求項 1 5】

ネットワークを介してサーバと接続されたクライアント装置において実行され、機械学習により得られた学習済モデルに基づいて入力データに対する変換処理を行って出力データを生成する、変換方法であって、

前記学習済モデルの入力段階から第 1 の中間段階へと至る前記学習済モデルの一部を用

10

20

30

40

50

いて、前記入力データに基づいて変換処理を行うことにより前記学習済モデルの前記第 1 の中間段階における第 1 の中間出力を生成する、入力側変換処理ステップと、

前記第 1 の中間出力を前記サーバへと送信する、クライアント側送信ステップと、

前記第 1 の中間出力に基づいて前記サーバにおいて生成され、前記学習済モデルの前記第 1 の中間段階より出力側に近い第 2 の中間段階における変換出力である第 2 の中間出力を前記サーバから受信する、クライアント側受信ステップと、

前記学習済モデルの前記第 2 の中間段階から出力段階へと至る前記学習済モデルの一部を用いて、前記第 2 の中間出力に基づいて変換処理を行うことにより前記出力データを生成する、出力側変換処理ステップと、

前記第 1 の中間出力と前記第 2 の中間出力との対応関係を表すキャッシュテーブルを記憶する、キャッシュテーブル記憶ステップと、

前記キャッシュテーブル中に前記第 1 の中間出力と対応する前記第 2 の中間出力が存在するか否かを判定する、判定ステップと、

前記判定ステップにおいて前記キャッシュテーブル中に前記第 1 の中間出力と対応する前記第 2 の中間出力が存在すると判定された場合には、前記クライアント側送信ステップと前記クライアント側受信ステップとを実行することに代えて前記キャッシュテーブルから対応する前記第 2 の中間出力を取得し、一方、前記判定ステップにおいて前記キャッシュテーブル中に前記第 1 の中間出力と対応する前記第 2 の中間出力が存在しないと判定された場合には、前記クライアント側送信ステップと前記クライアント側受信ステップとを実行することにより前記クライアント側受信ステップにおいて受信された前記第 2 の中間出力を取得する、選択的取得ステップと、を備える、変換方法。

【請求項 16】

ネットワークを介してサーバと接続され、機械学習により得られた学習済モデルに基づいて入力データに対する変換処理を行って出力データを生成する、クライアント装置の制御プログラムであって、

前記学習済モデルの入力段階から第 1 の中間段階へと至る前記学習済モデルの一部を用いて、前記入力データに基づいて変換処理を行うことにより前記学習済モデルの前記第 1 の中間段階における第 1 の中間出力を生成する、入力側変換処理ステップと、

前記第 1 の中間出力を前記サーバへと送信する、クライアント側送信ステップと、

前記第 1 の中間出力に基づいて前記サーバにおいて生成され、前記学習済モデルの前記第 1 の中間段階より出力側に近い第 2 の中間段階における変換出力である第 2 の中間出力を前記サーバから受信する、クライアント側受信ステップと、

前記学習済モデルの前記第 2 の中間段階から出力段階へと至る前記学習済モデルの一部であって、前記第 2 の中間出力に基づいて変換処理を行うことにより前記出力データを生成する、出力側変換処理ステップと、

前記第 1 の中間出力と前記第 2 の中間出力との対応関係を表すキャッシュテーブルを記憶する、キャッシュテーブル記憶ステップと、

前記キャッシュテーブル中に前記第 1 の中間出力と対応する前記第 2 の中間出力が存在するか否かを判定する、判定ステップと、

前記判定ステップにおいて前記キャッシュテーブル中に前記第 1 の中間出力と対応する前記第 2 の中間出力が存在すると判定された場合には、前記クライアント側送信ステップと前記クライアント側受信ステップとを実行することに代えて前記キャッシュテーブルから対応する前記第 2 の中間出力を取得し、一方、前記判定ステップにおいて前記キャッシュテーブル中に前記第 1 の中間出力と対応する前記第 2 の中間出力が存在しないと判定された場合には、前記クライアント側送信ステップと前記クライアント側受信ステップとを実行することにより前記クライアント側受信ステップにおいて受信された前記第 2 の中間出力を取得する、選択的取得ステップと、を備える、制御プログラム。

【請求項 17】

クライアント装置と、前記クライアント装置とネットワークを介して接続されたサーバとを含み、機械学習により得られた学習済モデルに基づいて入力データに対する変換処理

10

20

30

40

50

を行って出力データを生成する、変換システムであって、

前記クライアント装置は、

前記機械学習モデルの入力段階から第1の中間段階へと至る前記機械学習モデルの一部であって、前記機械学習モデルへの前記入力データに基づいて変換処理を行うことにより前記機械学習モデルの前記第1の中間段階における第1の中間出力を生成する、入力側変換処理部と、

前記第1の中間段階より出力側に近い第2の中間段階から出力段階へと至る前記機械学習モデルの一部であって、第2の中間段階に対する入力に基づいて変換処理を行うことにより前記機械学習モデルの前記出力データを生成する、出力側変換処理部と、

前記機械学習モデルにおける前記第1の中間出力と前記第2の中間出力との対応関係を表すサンプル情報に基づいて生成された近似関数に基づいて変換処理を行って、前記第1の中間出力に基づいて前記第2の中間出力を生成する、中間変換処理部と、を備え、

前記出力データは、前記入力データを前記入力側変換処理部の入力として前記入力側変換処理部、前記中間変換処理部及び前記出力側変換処理部を動作させることにより生成され、

前記クライアント装置は、さらに、

前記第1の中間出力を前記サーバへと送信する、クライアント側送信部と、

前記第1の中間出力に由来して前記サーバにおいて生成され、前記学習済モデルの前記第1の中間段階より出力側に近い第2の中間段階における変換出力である、第2の中間出力を前記サーバから受信する、クライアント側受信部と、

前記第1の中間出力と前記第2の中間出力との対応関係を表すキャッシュテーブルを記憶した、キャッシュテーブル記憶部と、

前記キャッシュテーブル中に前記第1の中間出力と対応する前記第2の中間出力が存在するか否かを判定する、判定部と、

前記判定部において前記キャッシュテーブル中に前記第1の中間出力と対応する前記第2の中間出力が存在すると判定された場合には、前記クライアント側送信部と前記クライアント側受信部とを動作させることに代えて前記キャッシュテーブルから対応する前記第2の中間出力を取得し、一方、前記判定部において前記キャッシュテーブル中に前記第1の中間出力と対応する前記第2の中間出力が存在しないと判定された場合には、前記クライアント側送信部と前記クライアント側受信部とを動作させることにより前記クライアント側受信部において受信された前記第2の中間出力を取得する、選択的取得部と、を備え、

前記サンプル情報は、前記キャッシュテーブルである、変換システム。

【発明の詳細な説明】

【技術分野】

【0001】

この発明は、機械学習技術を利用した変換システム、方法、プログラム等に関する。

【背景技術】

【0002】

近年、AI (Artificial Intelligence)、特に、機械学習技術が注目を集めており、様々な用途や課題解決への機械学習技術の適用が試みられている。例えば、製造業者や製造ラインの自動化業者等が、工場内等に設置される産業用ロボットに機械学習技術を適用し、より適切な制御を行おうとすること等が試みられている (例えば、特許文献1)。

【先行技術文献】

【特許文献】

【0003】

【文献】特開2017-030014号公報

【発明の概要】

【発明が解決しようとする課題】

10

20

30

40

50

【0004】

ところで、機械学習技術は未だ普く浸透しているとは言い難い。そのため、特定の対象へと機械学習技術を適用する場合には、機械学習技術に関する専門的知見を保有する事業者等が、機械学習技術に関する知見は持たないものの特定の課題を抱える利用者へと、機械学習技術を提供する形式で行われる場合が多い。

【0005】

しかしながら、このとき、機械学習技術の提供者は、一般に、機械学習に関するコンピュータプログラム等を利用者へと提供することには慎重である。当該プログラムの意図しない転用や流出、リバースエンジニアリング等のリスクが存在するためである。

【0006】

一方、機械学習技術の利用者としては、機械学習を行うために自らの保有する様々なデータ、特に生データを機械学習技術の提供者を含む第三者へと提供することには慎重となる。それらのデータは個人情報や営業秘密等に該当する場合が多く、非常に繊細な取扱いが必要となる情報であるためである。

【0007】

すなわち、従前、機械学習技術の利用者と提供者のそれぞれの事情により、機械学習技術の利用が十分に進まない場合があった。

【0008】

本発明は、上述の技術的背景の下になされたものであり、その目的とするところは、機械学習技術の利用者と提供者の双方の要求を満たすことができるセキュアなシステムを提供することにある。

【0009】

本発明のさらに他の目的並びに作用効果については、明細書の以下の記述を参照することにより、当業者であれば容易に理解されるであろう。

【課題を解決するための手段】

【0010】

上述の技術的課題は、以下の構成を有する変換システム等により解決することができる。

【0011】

すなわち、本発明に係る変換システムは、クライアント装置と、前記クライアント装置とネットワークを介してサーバと接続され、機械学習により得られた学習済モデルに基づいて入力データに対する変換処理を行って出力データを生成する、変換システムであって、前記クライアント装置は、前記学習済モデルの入力段階から第1の中間段階へと至る前記学習済モデルの一部であって、前記入力データに基づいて変換処理を行うことにより前記学習済モデルの前記第1の中間段階における第1の中間出力を生成する、入力側変換処理部と、前記第1の中間出力を前記サーバへと送信する、クライアント側送信部と、前記第1の中間出力に由来して前記サーバにおいて生成され、前記学習済モデルの前記第1の中間段階より出力側に近い第2の中間段階における変換出力である、第2の中間出力を前記サーバから受信する、クライアント側受信部と、前記学習済モデルの前記第2の中間段階から出力段階へと至る前記学習済モデルの一部であって、前記第2の中間出力に基づいて変換処理を行うことにより前記出力データを生成する、出力側変換処理部と、を備えている。

【0012】

このような構成によれば、機械学習を用いた変換処理を行う上で、クライアント装置とサーバとの間では、抽象化された中間出力のみが送受信され、生データが通信されることはない。従って、クライアント装置のユーザは、個人情報や営業秘密等の情報を確実に保護することができる。また、学習済モデルの提供者にとっては、クライアント装置側へと学習済モデルの全体を提供する必要がない。従って、アルゴリズムやそのアルゴリズムを実装したプログラムの漏洩等のリスクを低減することができる。すなわち、学習済モデルの利用者側と提供者側の双方の要求を満たすことができるセキュアな変換システムを提供することができる。

10

20

30

40

50

【0013】

なお、ここで、第1の中間出力及び第2の中間出力の語は、いずれも、学習済モデルの各段階の単なる出力値のみならず、当該出力値を暗号化するなどの所定の変換を行った値も含むものである。

【0014】

前記クライアント装置は、さらに、前記第1の中間出力と前記第2の中間出力との対応関係を表すキャッシュテーブルを記憶した、キャッシュテーブル記憶部と、前記キャッシュテーブル中に前記第1の中間出力と対応する前記第2の中間出力が存在するか否かを判定する、判定部と、前記判定部において前記キャッシュテーブル中に前記第1の中間出力と対応する前記第2の中間出力が存在すると判定された場合には、前記クライアント側送信部と前記クライアント側受信部とを動作させることに代えて前記キャッシュテーブルから対応する前記第2の中間出力を取得し、一方、前記判定部において前記キャッシュテーブル中に前記第1の中間出力と対応する前記第2の中間出力が存在しないと判定された場合には、前記クライアント側送信部と前記クライアント側受信部とを動作させることにより前記クライアント側受信部において受信された前記第2の中間出力を取得する、選択的取得部と、を備えてもよい。

10

【0015】

前記クライアント装置は、さらに、前記クライアント側受信部において受信された前記第2の中間出力を対応する前記第1の中間出力と対応付けて前記キャッシュテーブルへと記憶させるキャッシュテーブル記憶部を備えてもよい。

20

【0016】

前記クライアント装置は、さらに、前記第1の中間出力を暗号化して第1の暗号化中間出力を生成する暗号化部と、前記サーバにより暗号化された第2の中間出力である第2の暗号化中間出力を復号化する復号化部と、を備え、前記クライアント側送信部は、前記第1の暗号化中間出力を前記サーバへと送信し、前記サーバは、受信した前記第1の暗号化中間出力を復号化して前記第1の中間出力を復元すると共に、前記第2の中間出力を暗号化して前記第2の暗号化中間出力を生成して前記クライアント装置へと送信し、前記クライアント側受信部は、前記第2の暗号化中間出力を受信する、ものであってもよい。

【0017】

前記クライアント装置は、さらに、前記第1の暗号化中間出力をハッシュ化して第1のハッシュ値を生成する、ハッシュ化処理部を備え、前記キャッシュテーブルにおける前記第1の中間出力は、前記第1のハッシュ値であり、前記判定部は、前記第1のハッシュ値に基づいて、対応する前記第2の中間出力が存在するか否かを判定する、ものであってもよい。

30

【0018】

前記クライアント装置は、さらに、前記第1の中間出力を丸め処理して第1の丸め中間出力を生成する、値丸め処理部を備える、ものであってもよい。

【0019】

前記クライアント装置は、さらに、前記キャッシュテーブルに基づいて、近似関数を生成する近似関数生成部と、前記第1の中間出力を入力として前記近似関数に基づいて前記第2の中間出力を生成する、近似変換処理部と、を備えるものであってもよい。

40

【0020】

前記近似関数は、誤差逆伝播法を適用可能な関数である、ものであってもよい。

【0021】

前記近似関数は、バイパス関数を含むものであってもよい。

【0022】

前記近似関数は、複数の異なる近似関数の重み付き和により構成される、ものであってもよい。

【0023】

前記クライアント装置は複数から成り、前記キャッシュテーブルは、複数の前記クライ

50

アント装置により共有される、ものであってもよい。

【0024】

前記サーバは、さらに、前記第1の中間段階から前記第2の中間段階へと至る前記学習済モデルの一部であって、前記第1の中間出力に基づいて変換処理を行うことにより前記第2の中間段階における前記第2の中間出力を生成する、中間変換処理部を備えるものであってもよい。

【0025】

前記サーバは、ネットワークを介して接続された多段のサーバで構成され、各サーバは、前記第1の中間段階と前記第2の中間段階との間の学習済モデルを分割した部分モデルをそれぞれ保持し、各サーバの各部分モデルに基づいて順に変換処理を行うことにより前記第2の中間出力を生成する、ものであってもよい。

【0026】

前記クライアント装置は、さらに、前記入力データと、前記入力データと対応する前記出力データとの関係性を表す入出力データテーブルを記憶する入出力データテーブル記憶部を備える、ものであってもよい。

【0027】

本発明は、クライアント装置としても観念することができる。すなわち、本発明に係るクライアント装置は、ネットワークを介してサーバと接続され、機械学習により得られた学習済モデルに基づいて入力データに対する変換処理を行って出力データを生成する、クライアント装置であって、前記学習済モデルの入力段階から第1の中間段階へと至る前記学習済モデルの一部であって、前記入力データに基づいて変換処理を行うことにより前記学習済モデルの前記第1の中間段階における第1の中間出力を生成する、入力側変換処理部と、前記第1の中間出力を前記サーバへと送信する、クライアント側送信部と、前記第1の中間出力に基づいて前記サーバにおいて生成され、前記学習済モデルの前記第1の中間段階より出力側に近い第2の中間段階における変換出力である第2の中間出力を前記サーバから受信する、クライアント側受信部と、前記学習済モデルの前記第2の中間段階から出力段階へと至る前記学習済モデルの一部であって、前記第2の中間出力に基づいて変換処理を行うことにより前記出力データを生成する、出力側変換処理部と、を備えるクライアント装置。

【0028】

本発明は、変換方法としても観念することができる。すなわち、本発明に係る変換方法は、ネットワークを介してサーバと接続され、機械学習により得られた学習済モデルに基づいて入力データに対する変換処理を行って出力データを生成する、変換方法であって、前記学習済モデルの入力段階から第1の中間段階へと至る前記学習済モデルの一部を用いて、前記入力データに基づいて変換処理を行うことにより前記学習済モデルの前記第1の中間段階における第1の中間出力を生成する、入力側変換処理ステップと、前記第1の中間出力を前記サーバへと送信する、クライアント側送信ステップと、前記第1の中間出力に基づいて前記サーバにおいて生成され、前記学習済モデルの前記第1の中間段階より出力側に近い第2の中間段階における変換出力である第2の中間出力を前記サーバから受信する、クライアント側受信ステップと、前記学習済モデルの前記第2の中間段階から出力段階へと至る前記学習済モデルの一部を用いて、前記第2の中間出力に基づいて変換処理を行うことにより前記出力データを生成する、出力側変換処理ステップと、を備えている。

【0029】

本発明は、制御プログラムとしても観念することができる。すなわち、本発明に係る制御プログラムは、ネットワークを介してサーバと接続され、機械学習により得られた学習済モデルに基づいて入力データに対する変換処理を行って出力データを生成する、クライアント装置の制御プログラムであって、前記学習済モデルの入力段階から第1の中間段階へと至る前記学習済モデルの一部を用いて、前記入力データに基づいて変換処理を行うことにより前記学習済モデルの前記第1の中間段階における第1の中間出力を生成する、入力側変換処理ステップと、前記第1の中間出力を前記サーバへと送信する、クライアント

10

20

30

40

50

側送信ステップと、前記第 1 の中間出力に基づいて前記サーバにおいて生成され、前記学習済モデルの前記第 1 の中間段階より出力側に近い第 2 の中間段階における変換出力である第 2 の中間出力を前記サーバから受信する、クライアント側受信ステップと、前記学習済モデルの前記第 2 の中間段階から出力段階へと至る前記学習済モデルの一部であって、前記第 2 の中間出力に基づいて変換処理を行うことにより前記出力データを生成する、出力側変換処理ステップと、を備えている。

【0030】

本発明は、サーバとしても観念することができる。すなわち、本発明に係るサーバは、クライアント装置とネットワークを介して接続され、機械学習により得られた学習済モデルに基づいて入力データに対する変換処理を行って出力データを生成する、サーバであって、前記クライアント装置は、前記学習済モデルの入力段階から第 1 の中間段階へと至る前記学習済モデルの一部であって、前記入力データに基づいて変換処理を行うことにより前記学習済モデルの前記第 1 の中間段階における第 1 の中間出力を生成する、入力側変換処理部と、前記第 1 の中間出力を前記サーバへと送信する、クライアント側送信部と、前記第 1 の中間出力に基づいて前記サーバにおいて生成され、前記学習済モデルの前記第 1 の中間段階より出力側に近い第 2 の中間段階における変換出力である第 2 の中間出力を前記サーバから受信する、クライアント側受信部と、前記学習済モデルの前記第 2 の中間段階から出力段階へと至る前記学習済モデルの一部であって、前記第 2 の中間出力に基づいて変換処理を行うことにより前記出力データを生成する、出力側変換処理部と、を備えている。

【0031】

別の側面から見た本発明に係る変換システムは、機械学習により得られた学習済モデルに基づいて入力データに対する変換処理を行って出力データを生成する、変換システムであって、前記機械学習モデルの入力段階から第 1 の中間段階へと至る前記機械学習モデルの一部であって、前記機械学習モデルへの前記入力データに基づいて変換処理を行うことにより前記機械学習モデルの前記第 1 の中間段階における第 1 の中間出力を生成する、入力側変換処理部と、前記第 1 の中間段階より出力側に近い第 2 の中間段階から出力段階へと至る前記機械学習モデルの一部であって、第 2 の中間段階に対する入力に基づいて変換処理を行うことにより前記機械学習モデルの前記出力データを生成する、出力側変換処理部と、前記機械学習モデルにおける前記第 1 の中間出力と前記第 2 の中間出力との対応関係を表すサンプル情報に基づいて生成された近似関数に基づいて変換処理を行って、前記第 1 の中間出力に基づいて前記第 2 の中間出力を生成する、中間変換処理部と、を備え、前記出力データは、前記入力データを前記入力側変換処理部の入力として前記入力側変換処理部、前記中間変換処理部及び前記出力側変換処理部を動作させることにより生成される、ものである。

【0032】

このような構成によれば、既に得られている中間出力の対応関係に関するサンプル情報に基づいて近似関数を生成して変換処理を行うことができるので、サーバ等への問い合わせを行うことなく変換処理を行うことができる。このような構成によれば、よりクライアント装置等の変換装置又はシステムの自律性と変換時間の短縮化を図ることができる。なお、このような構成を、サーバへの問い合わせを行う上述の変換システムと適宜に組み合わせて利用してもよく、例えば、通信環境又はネットワークの利用可否等に応じて、変換処理のアルゴリズムを適宜切り替えてもよい。

【発明の効果】

【0033】

本発明によれば、機械学習技術の利用者側と提供者側の双方の要求を満たすことができるセキュアな予測システムを提供することができる。

【図面の簡単な説明】

【0034】

【図 1】 図 1 は、システムの全体構成図（第 1 の実施形態）である。

- 【図 2】図 2 は、サーバのハードウェア構成図である。
- 【図 3】図 3 は、ロボットのハードウェア構成図である。
- 【図 4】図 4 は、ロボットに関する機能ブロック図（第 1 の実施形態）である。
- 【図 5】図 5 は、サーバに関する機能ブロック図（第 1 の実施形態）である。
- 【図 6】図 6 は、ロボットにおける予測処理（第 1 の実施形態）（その 1）である。
- 【図 7】図 7 は、ロボットにおける予測処理（第 1 の実施形態）（その 2）である。
- 【図 8】図 8 は、サーバにおける予測処理（第 1 の実施形態）である。
- 【図 9】図 9 は、予測処理に関する概念図（第 1 の実施形態）である。
- 【図 10】図 10 は、システムの全体構成図（第 2 の実施形態）である。
- 【図 11】図 11 は、中間サーバのハードウェア構成図である。
- 【図 12】図 12 は、中間サーバに関する機能ブロック図（第 2 の実施形態）である。
- 【図 13】図 13 は、中間サーバにおける予測処理（第 2 の実施形態）（その 1）である。
- 【図 14】図 14 は、中間サーバにおける予測処理（第 2 の実施形態）（その 2）である。
- 【図 15】図 15 は、最終サーバにおける予測処理（第 2 の実施形態）である。
- 【図 16】図 16 は、予測処理に関する概念図（第 2 の実施形態）である。
- 【図 17】図 17 は、ロボットに関する機能ブロック図（第 3 の実施形態）である。
- 【図 18】図 18 は、中間サーバに関する機能ブロック図（第 3 の実施形態）である。
- 【図 19】図 19 は、最終サーバに関する機能ブロック図（第 3 の実施形態）である。
- 【図 20】図 20 は、ロボットにおける学習処理（第 3 の実施形態）である。
- 【図 21】図 21 は、近似データに関する概念図である。
- 【図 22】図 22 は、中間サーバにおける記憶処理（第 3 の実施形態）である。
- 【図 23】図 23 は、中間サーバにおける学習処理（第 3 の実施形態）である。
- 【図 24】図 24 は、最終サーバにおける記憶処理（第 3 の実施形態）である。
- 【図 25】図 25 は、最終サーバにおける学習処理（第 3 の実施形態）である。
- 【図 26】図 26 は、学習処理に関する概念図（第 3 の実施形態）である。
- 【図 27】図 27 は、システムの全体構成図（変形例）である。
- 【図 28】図 28 は、バイパス関数を利用する例に関する概念図である。
- 【図 29】図 29 は、バイパス関数の概念図である。
- 【図 30】図 30 は、サブ近似関数を利用した近似の概念図である。

【発明を実施するための形態】

【0035】

以下、本発明に係るシステム等の実施の一形態を、添付の図面を参照しつつ、詳細に説明する。なお、以下の実施形態においては、予測処理の語を用いることがある。当業者には明らかな通り、予測処理の語は、学習済モデルの順方向演算処理を意味し、従って、例えば、単に変換処理、推論処理等といった語と置換することができる。

【0036】

< 1. 第 1 の実施形態 >

< 1. 1 システムの構成 >

まず、図 1～図 5 を参照しつつ、本実施形態におけるシステム 10 の構成について説明する。

【0037】

図 1 は、本実施形態に係るシステム 10 の全体構成図である。同図から明らかな通り、通信機能を有するサーバ 1 と、通信機能を有する複数（N 個）のロボット 3 とが、サーバ・クライアントシステムを構成しており、それらは互いに、WAN（Wide Area Network）及び LAN（Local Area Network）を介して接続されている。なお、WAN は例えばインターネットであり、LAN は例えば工場内等に設置されている。

【0038】

図 2 は、サーバ 1 のハードウェア構成について示す図である。同図から明らかな通り、サーバ 1 は、制御部 11、記憶部 12、I/O 部 13、通信部 14、表示部 15、入力部

10

20

30

40

50

16を備え、それらはシステムバス等を介して互いに接続されている。制御部11は、CPU又はGPU等のプロセッサで構成されており各種プログラムの実行処理を行う。記憶部12は、ROM、RAM、ハードディスク、フラッシュメモリ等の記憶装置であり、各種データや動作プログラム等を記憶している。I/O部13は、外部装置との入出力等を行うものである。通信部14は、例えば所定の通信規格に基づいて通信を行う通信ユニットであり、本実施形態におけるクライアント装置であるロボット3との通信を行う。表示部15は、ディスプレイ等と接続され所定の表示を行う。入力部16は、例えばキーボードやマウス等により管理者からの入力を受け付けるものである。

【0039】

図3は、ロボット3のハードウェア構成について示す図である。ロボット3は、例えば、工場内等に配置される産業用ロボットである。同図から明らかな通り、ロボット3は、制御部31、記憶部32、I/O部33、通信部34、表示部35、検知部36及び駆動部37を備え、それらはシステムバス等を介して互いに接続されている。制御部31は、CPU又はGPU等のプロセッサで構成されており各種プログラムの実行処理を行う。記憶部32は、ROM、RAM、ハードディスク、フラッシュメモリ等の記憶装置であり、各種データや動作プログラム等を記憶している。I/O部33は、外部装置との入出力等を行うものである。通信部34は、例えば所定の通信規格に基づいて通信を行う通信ユニットであり、本実施形態ではサーバ1との通信を行う。表示部35は、ディスプレイ等と接続され所定の表示を行う。検知部36は、センサと接続されセンサ情報をデジタルデータとして検出する。駆動部37は、制御部からの指令に応じて、接続される（図示しない）モータ等を駆動する。

【0040】

図4は、ロボット3の制御部31に関する機能ブロック図である。同図から明らかな通り、制御部31は、センサ情報取得部311、予測処理部312、暗号化処理部319、ハッシュ化処理部313、情報取得要否判定部314、キャッシュ情報取得処理部315、サーバ情報取得処理部316、復号化部317及び駆動指令部318を備えている。

【0041】

センサ情報取得部311は、検知部36にて取得されたセンサ情報を取得する。予測処理部312は、ニューラルネットワークを教師有り学習することにより生成された予測モデル（学習済モデル）の構成等に関する基本情報や重み情報等を読み込むと共に、入力されたデータに基づいて所定の予測出力を生成する。暗号化処理部319は、入力されたデータを公開鍵等により暗号化する処理を行う。ハッシュ化処理部313は、入力された情報をハッシュ化して対応するハッシュ値、すなわち、規則性の無い固定長の値を生成する。情報取得要否判定部314は、所定のデータに対して既にそれと対応するデータが所定のテーブル中に記憶されているか否かを判定する。キャッシュ情報取得処理部315は、情報取得要否判定部314において所定のデータに対応するデータが存在すると判断された場合にその対応するデータを取得する。サーバ情報取得処理部316は、サーバ1へと所定のデータを送信して当該データに対応するデータを受信する。復号化部317は、公開鍵等により暗号化されたデータを暗号鍵にて復号化処理する。駆動指令部318は、出力データに基づいてモータ等を駆動する。

【0042】

図5は、サーバ1の制御部11に関する機能ブロック図である。同図から明らかな通り、制御部11は、データ入力受付部111、復号化処理部112、予測処理部113、暗号化処理部114及びデータ送信部115を備えている。

【0043】

データ入力受付部111は、ロボット3から送信されるデータ入力を受け付ける。復号化処理部112は、公開鍵等により暗号化されたデータを暗号鍵等により復号化する。予測処理部113は、ニューラルネットワークを教師有り学習することにより生成された予測モデル（学習済モデル）の構成等の基本情報や重み情報等を読み込むと共に、入力されたデータに基づいて所定の予測出力を生成する。暗号化処理部114は、入力されるデー

10

20

30

40

50

タを公開鍵等により暗号化する。データ送信部は、送信対象データをロボット3へと送信する処理を行う。

【0044】

＜1.2 システムの動作＞

次に、図6～図9を参照しつつ、システム10の動作について説明する。

【0045】

図6及び図7を参照しつつ、本実施形態におけるロボット3の予測処理動作について説明する。本実施形態において、ロボット3は、取得したセンサ情報に基づいて所定の予測処理を行いモータ等の動作部を駆動するものである。

【0046】

ロボット3において、予測処理が開始すると、センサ情報取得部311を介してセンサ情報(I)を取得する処理が行われる(S1)。続いて、このセンサ情報(I)を予測処理部312へと入力して入力段階から第1の中間層まで予測処理を行い入力側中間層データ(X1)を生成する(S3)。

【0047】

生成された入力側中間層データ(X1)は、暗号化処理部319において公開鍵により暗号化され暗号化入力側中間層データ(X1')が生成される(S5)。暗号化入力側中間層データ(X1')は、その後、ハッシュ化処理部313によりハッシュ化され、ハッシュ値(Y1)が生成される(S7)。

【0048】

続いて、情報取得要否判定処理部314は、ハッシュテーブルを読み出し、生成されたハッシュ値(Y1)に対応する暗号化出力側中間層データ(Z1')がハッシュテーブル中に存在するか否かを判定する(S9)。出力側中間層データ(Z1)は、後述するように、第1の中間層より出力層寄りの第2の中間層出力を表しており、暗号化出力側中間層データ(Z1')は、サーバ1において公開鍵により暗号化された第2の中間層の出力を表している。

【0049】

判定(S9)の結果、ハッシュ値(Y1)に対応する暗号化出力側中間層データ(Z1')がハッシュテーブル中に存在する場合(S11YES)、キャッシュ情報取得処理部315は、当該暗号化出力側中間層データ(Z1')をキャッシュ情報として取得する処理を行う(S13)。

【0050】

一方、判定の結果、ハッシュ値(Y1)に対応する暗号化出力側中間層データ(Z1')がハッシュテーブル中に存在しない場合(S11NO)、サーバ情報取得処理部316は、暗号化入力側中間層データ(X1')をサーバ1へと送信し(S15)、その後所定の待機状態(S17NO)へと移行する。この待機状態において、サーバ1より暗号化出力側中間層データ(Z1')を受信すると、待機状態が解除され(S17YES)、受信した暗号化出力側中間層データ(Z1')を前記ハッシュ値(Y1)と対応付けて保存する処理が行われる(S19)。なお、この間のサーバ1の動作は図8において詳述する。

【0051】

復号化部317は、取得した暗号化出力側中間層データ(Z1')を秘密鍵により復号化することで出力側中間層データ(Z1)を生成する(S21)。その後、予測処理部312は、生成された出力側中間層データ(Z1)に基づいて、第2の中間層から出力層までの予測処理を行い最終出力(O)を生成する(S23)。その後、駆動指令部318は、最終出力(O)に基づいてモータ等の駆動部へと駆動指令を行う(S25)。この駆動処理が完了すると、再度、センサ情報の取得処理が行われ(S1)、以後、一連の処理(S1～S25)が繰り返される。

【0052】

次に、図8を参照しつつ、サーバ1の予測処理動作について説明する。

【0053】

10

20

30

40

50

サーバ１において予測処理が開始すると、サーバ１は、データ入力受付部１１１により所定の待機状態へと移行する（Ｓ３１ＮＯ）。この状態において、ロボット３からの暗号化入力側中間層データ（Ｘ１'）を受信すると待機状態が解除され（Ｓ３１ＮＯ）、復号化処理部１１２により、受信した暗号化入力側中間層データ（Ｘ１'）を秘密鍵により復号化して入力側中間層データ（Ｘ１）を生成する処理が行われる（Ｓ３３）。その後、予測処理部１１３は、この入力側中間層データ（Ｘ１）を入力として第１の中間層から第２の中間層までの予測処理を行い、出力側中間層データ（Ｚ１）を生成する（Ｓ３５）。

【００５４】

暗号化処理部１１４は、この出力側中間層データ（Ｚ１）を公開鍵を用いて暗号化して、暗号化出力側中間層データ（Ｚ１'）を生成する（Ｓ３７）。その後、データ送信部１１５は、暗号化出力側中間層データ（Ｚ１'）をロボット３へと送信する（Ｓ３９）。この送信処理が終了すると、サーバ１は、再び受信待機状態（Ｓ３１）へと戻り、以後、一連の処理（Ｓ３１～Ｓ３９）が繰り返される。

【００５５】

図９は、本実施形態に係るシステム１により実現される予測処理の概念図である。同図において、上段は、ロボット３において行われる予測処理の概念図であり、下段は、サーバ１において行われる予測処理の概念図である。また、同図の左側が入力側、右側が出力側を示している。

【００５６】

同図から明らかな通り、ロボット３においてセンサ情報（Ｉ）が入力されると、予測処理部３１２は、入力段階から第１の中間層までの間の予測処理を行い、入力側中間層データ（Ｘ１）を生成する。その後、入力側中間層データ（Ｘ１）は、暗号化を経てサーバ１へと送信され、サーバ１において復号化される。

【００５７】

サーバ１において、予測処理部１１３は、入力側中間層データ（Ｘ１）を入力として、第１の中間層から第２の中間層までの予測処理を行い、出力側中間層データ（Ｚ１）を生成する。その後、出力側中間層データ（Ｚ１）は、暗号化を経てロボット３へと送信され、ロボット３において復号化される。

【００５８】

ロボット３において、予測処理部３１２は、第２の中間層から出力層までの間の予測処理を行い、最終出力（Ｏ）を生成する。

【００５９】

このような構成によれば、機械学習を用いた予測処理を行う上で、クライアント装置（ロボット３）とサーバとの間では、抽象化された中間出力のみが送受信され、生データを送受信する必要がない。従って、クライアント装置のユーザは、個人情報や営業秘密等の情報を確実に保護することができる。また、予測モデルの提供者にとっては、クライアント装置側へと予測モデルの全体を提供する必要がない。従って、アルゴリズムやそのアルゴリズムを実装したプログラムの漏洩等のリスクを低減することができる。すなわち、予測モデルの利用者側と提供者側の双方の要求を満たすことができるセキュアな予測システムを提供することができる。

【００６０】

また、ハッシュテーブルへと記憶されているデータに関してはサーバへの問合せが不要となるので、サーバ利用コストを削減することができ、また、予測処理の高速化を実現することができる。また、システムを継続的に利用してハッシュテーブルへと十分な情報の蓄積を行えば、クライアント装置をほぼ自律的に動作させることも可能となる。

【００６１】

さらに、クライアント装置とサーバとの間で通信される中間出力については暗号化処理がなされている。そのため、一層のデータの安全が図られている。

【００６２】

加えて、上述の実施形態においては、ハッシュ化処理がなされている。これにより、デ

10

20

30

40

50

一タの安全性が向上すると共に、ハッシュテーブルにおける検索処理の高速化により、判定処理の高速化を実現することができる。

【0063】

＜2．第2の実施形態＞

本実施形態では、システム20において、サーバが多段階に配置される。

【0064】

＜2．1 システムの構成＞

図10～図12を参照しつつ、本実施形態に係るシステム20の構成について説明する。本実施形態においては、サーバ5、6が多段階で構成されている。

【0065】

図10は、本実施形態に係るシステム20の全体構成図である。同図から明らかな通り、本実施形態に係るシステム20は、サーバ5とクライアント装置としての複数のロボット7（7-1～7-N）とがネットワークを介して通信により接続される点において第1の実施形態と同一である。しかしながら、本実施形態は、ロボット7と最終サーバ5との間に中間サーバ6が介在する点において第1の実施形態と相違する。この中間サーバ6は、例えば機械学習技術のベンダ（AIベンダ）等により運用される。

【0066】

図11は、ロボット7と最終サーバ5との間に介在する中間サーバ6のハードウェア構成について示す図である。同図から明らかな通り、中間サーバ6は、制御部61、記憶部62、I/O部63、通信部64、表示部65、入力部66を備え、それらはシステムバス等を介して互いに接続されている。制御部61は、CPU又はGPU等のプロセッサで構成されており各種プログラムの実行処理を行う。記憶部62は、ROM、RAM、ハードディスク、フラッシュメモリ等の記憶装置であり、各種データや動作プログラム等を記憶している。I/O部63は、外部装置との入出力等を行うものである。通信部64は、例えば所定の通信規格に基づいて通信を行う通信ユニットであり、最終サーバ5及びクライアント装置としてのロボット7との通信を行う。表示部65は、ディスプレイ等と接続され所定の表示を行う。入力部66は、例えばキーボードやマウス等により管理者からの入力を受け付けるものである。

【0067】

図12は、中間サーバ6の制御部61に関する機能ブロック図である。同図から明らかな通り、制御部61は、データ入力受付部611、復号化処理部612、予測処理部613、暗号化処理部614、ハッシュ化処理部615、情報取得要否判定部616、キャッシュ情報取得処理部617、サーバ情報取得処理部618及びデータ送信部619を備えている。

【0068】

データ入力受付部611は、ロボット3又は最終サーバ5から送信されるデータ入力を受け付ける。復号化処理部612は、公開鍵等により暗号化されたデータを暗号鍵等により復号化する。予測処理部613は、ニューラルネットワークを教師有り学習することにより生成された予測モデル（学習済モデル）の構成等の基本情報や重み情報等を読み込むと共に、入力されたデータに基づいて所定の予測出力を生成する。暗号化処理部614は、入力されるデータを公開鍵等により暗号化する。ハッシュ化処理部615は、入力された情報をハッシュ化して対応するハッシュ値、すなわち、規則性の無い固定長の値を生成する。情報取得要否判定部616は、所定のデータに対して既にそれと対応するデータが所定のテーブル中に記憶されているか否かを判定する。キャッシュ情報取得処理部617は、情報取得要否判定部616において所定のデータに対応するデータが存在すると判断された場合にその対応するデータを取得する。サーバ情報取得処理部618は、最終サーバ5へと所定のデータを送信して当該データに対応するデータを受信する。データ送信部619は、送信対象データをロボット3又は最終サーバ5へと送信する処理を行う。

【0069】

なお、最終サーバ5とロボット7のハードウェア構成は、第1の実施形態のサーバ1と

10

20

30

40

50

ロボット 3 の構成と略同一であるので、ここでは記載を省略する。

【 0 0 7 0 】

< 2 . 2 システムの動作 >

次に、図 1 3 ~ 図 1 6 を参照しつつ、本実施形態に係るシステム 2 0 の動作について説明する。

【 0 0 7 1 】

ロボット 7 の動作は、第 1 の実施形態と略同一である。すなわち、図 6 及び図 7 において示した通り、情報取得要否判定処理部 3 1 4 における判定 (S 9) の結果、ハッシュ値 (Y 1) に対応する暗号化出力側中間層データ (Z 1 ') がハッシュテーブル中に存在しない場合 (S 1 1 N O) 、サーバ情報取得処理部 3 1 6 は、第 1 の暗号化入力側中間層データ (X 1 ') を中間サーバ 6 へと送信し (S 1 5) 、その後所定の待機状態 (S 1 7 N O) へと移行する。この待機状態において、サーバ 1 より第 1 の暗号化出力側中間層データ (Z 1 ') を受信すると、待機状態が解除され (S 1 7 Y E S) 、受信した第 1 の暗号化出力側中間層データ (Z 1 ') を前記ハッシュ値 (Y 1) と対応付けて保存する処理が行われる (S 1 9) 。

【 0 0 7 2 】

図 1 3 及び図 1 4 は、中間サーバ 6 の予測処理動作に関するフローチャートである。中間サーバ 6 は、予測処理が開始すると、データ入力受付部 6 1 1 により所定の待機状態に移行する (S 5 1 N O) 。その後、ロボット 7 から第 1 の暗号化入力側中間層データ (X 1 ') を受信すると (S 5 1 Y E S) 、待機状態が解除される。その後、復号化処理部 6 1 2 は、受信した第 1 の暗号化入力側中間層データ (X 1 ') を秘密鍵により復号化処理し、第 1 の入力側中間層データ (X 1) を生成する (S 5 3) 。

【 0 0 7 3 】

予測処理部 6 1 3 は、復号化した第 1 の入力側中間層データ (X 1) に基づいて、第 1 の中間層から第 3 の中間層までの予測処理を行って第 2 の入力側中間層データ (X 2) を生成する (S 5 5) 。暗号化処理部 6 1 4 は、第 2 の入力側中間層データ (X 2) を公開鍵で暗号化して第 2 の暗号化入力側中間層データ (X 2 ') を生成する (S 5 7) 。また、ハッシュ化処理部 6 1 5 は、第 2 の暗号化入力側中間層データ (X 2 ') をハッシュ化処理して第 2 のハッシュ値 (Y 2) を生成する (S 5 9) 。

【 0 0 7 4 】

その後、情報取得要否判定部 6 1 6 は、中間サーバ 6 に記憶された第 2 のハッシュテーブルを読み出し、生成された第 2 のハッシュ値 (Y 2) に対応する第 2 の暗号化出力側中間層データ (Z 2 ') が第 2 のハッシュテーブル中に存在するか否かを判定する (S 6 1) 。この判定 (S 9) の結果、第 2 のハッシュ値 (Y 2) に対応する第 2 の暗号化出力側中間層データ (Z 2 ') がハッシュテーブル中に存在する場合 (S 6 3 Y E S) 、キャッシュ情報取得処理部 6 1 7 は、当該第 2 の暗号化出力側中間層データ (Z 2 ') をキャッシュ情報として取得する処理を行う (S 6 5) 。

【 0 0 7 5 】

一方、判定の結果、第 2 のハッシュ値 (Y 2) に対応する第 2 の暗号化出力側中間層データ (Z 2 ') が第 2 のハッシュテーブル中に存在しない場合 (S 6 3 N O) 、サーバ情報取得処理部 6 1 8 は、第 2 の暗号化入力側中間層データ (X 2 ') をサーバ 1 へと送信し (S 6 7) 、その後所定の待機状態 (S 6 9 N O) へと移行する。この待機状態において、最終サーバ 5 より第 2 の暗号化出力側中間層データ (Z 2 ') を受信すると、待機状態が解除され (S 6 9 Y E S) 、受信した第 2 の暗号化出力側中間層データ (Z 2 ') を前記第 2 のハッシュ値 (Y 2) と対応付けて保存する処理が行われる (S 7 1) 。なお、この間の最終サーバ 5 の動作は図 1 5 において後述する。

【 0 0 7 6 】

復号化処理部 6 1 2 は、取得した第 2 の暗号化出力側中間層データ (Z 2 ') を秘密鍵により復号化することで第 2 の出力側中間層データ (Z 2) を生成する (S 7 3) 。その後、予測処理部 6 1 3 は、生成された第 2 の出力側中間層データ (Z 2) に基づいて、第 4

の中間層から第2の中間層までの予測処理を行い、第1の出力側中間層データ（Z1）を生成する（S75）。暗号化処理部614は、第1の出力側中間層データ（Z1）に暗号化処理を行い第1の暗号化出力側中間層データ（Z1'）を生成する（S77）。その後、データ送信部619は、第1の暗号化出力側中間層データ（Z1'）をロボット7へと送信する。この送信処理が終了すると、中間サーバ6は再び受信待機状態（S51NO）へと戻り、以後、一連の処理（S51～S79）が繰り返される。

【0077】

図15は、最終サーバ5の予測処理動作に関するフローチャートを示している。

【0078】

予測処理が開始すると、最終サーバ5は、データ入力受付部111により所定の待機状態へと移行する（S81NO）。この状態において、中間サーバ6からの第2の暗号化入力側中間層データ（X2'）を受信すると待機状態が解除される（S81YES）。復号化処理部112は、受信した第2の暗号化入力側中間層データ（X2'）を秘密鍵により復号化する処理を行い、第2の入力側中間層データ（X2）を生成する（S83）。その後、予測処理部113は、この第2の入力側中間層データ（X2）を入力として第3の中間層から第4の中間層までの予測処理を行い、第2の出力側中間層データ（Z2）を生成する（S85）。

【0079】

暗号化処理部114は、この第2の出力側中間層データ（Z2）を公開鍵を用いて暗号化して、第2の暗号化出力側中間層データ（Z2'）を生成する（S87）。その後、データ送信部115は、第2の暗号化出力側中間層データ（Z2'）を中間サーバ6へと送信する（S89）。この送信処理が終了すると、最終サーバ5は再度受信待機状態（S81）へと戻り、以後、一連の処理（S81～S89）が繰り返される。

【0080】

図16は、本実施形態に係るシステム20により実現される予測処理の概念図である。同図において、上段は、ロボット7において行われる予測処理の概念図であり、中段は、中間サーバ6において行われる予測処理の概念図であり、下段は、最終サーバ5において行われる予測処理の概念図である。また、同図において左側が入力側、右側が出力側を示している。

【0081】

同図から明らかな通り、ロボット3においてセンサ情報（I）が入力されると、予測処理部312は、入力段階から第1の中間層までの間の予測処理を行い、第1の入力側中間層データ（X1）を生成する。その後、第1の入力側中間層データ（X1）は、暗号化を経て中間サーバ6へと送信され、中間サーバ6において復号化される。

【0082】

中間サーバ6において、予測処理部613は、第1の中間層から第3の中間層までの間の予測処理を行い、第2の入力側中間層データ（X2）を生成する。その後、第2の入力側中間層データ（X2）は、暗号化を経て最終サーバ5へと送信され、最終サーバ5において復号化される。

【0083】

最終サーバ5において、予測処理部113は、第2の入力側中間層データ（X2）を入力として、第3の中間層から第4の中間層までの予測処理を行い、第2の出力側中間層データ（Z2）を生成する。その後、第2の出力側中間層データ（Z2）は、暗号化を経て中間サーバ6へと送信され、中間サーバ6において復号化される。

【0084】

中間サーバ6において、予測処理部613は、第4の中間層から第2の中間層までの間の予測処理を行い、第1の出力側中間層データ（Z1）を生成する。その後、第1の出力側中間層データ（Z1）は、暗号化を経てロボット7へと送信され、ロボット7において復号化される。

【0085】

10

20

30

40

50

ロボット 7 において、予測処理部 3 1 2 は、第 2 の中間層から出力層までの間の予測処理を行い、最終出力（O）を生成する。

【0086】

このような構成によれば、サーバが多段に設けられていることから、クライアント装置及び各サーバにおける個々の装置の処理負担を軽減できると同時に、多段化によるスケールメリットによりクライアント装置における予測性能の向上も見込むことができる。しかも、このように多段化を行っても、各サーバはキャッシュ情報に基づいた予測処理も行うことから処理の低速化が生じにくい。なお、予測モデルが分散配置されるのでよりシステムの安全性の向上等も見込まれ、また、複数の管理者による各サーバの分担管理も可能となる。

10

【0087】

＜3. 第3の実施形態＞

本実施形態では、システム 3 0 が予測処理に加えて学習処理を行う。

【0088】

＜3. 1 システムの構成＞

本実施形態に係るシステム 3 0 の構成は、第 2 の実施形態において示したものと略同一である。尤も、ロボット 7、中間サーバ 6 及び最終サーバ 5 の各制御部が、予測処理に加えて学習処理のための機能ブロックを有する点において相違する。

【0089】

図 1 7 は、ロボット 7 の制御部 7 1 0 の機能ブロック図である。

20

【0090】

同図において、予測処理部 7 1 0 1 の内容は、図 4 において示した構成と略同一であるので詳細な説明は省略する。ただし、予測処理部 7 1 0 1 は、さらにキャッシュテーブル追加処理部 7 1 0 9 を備える点において異なる。キャッシュテーブル追加処理部 7 1 0 9 は、図 7 において復号化処理（S 2 1）を行って出力側中間層データ（Z 1）を生成した後に、当該出力側中間層データ（Z 1）を、対応する入力側中間層データ（X 1）と共に、キャッシュテーブルへと追加記憶させる処理を行う。このキャッシュテーブルは後述の学習処理に用いられる。

【0091】

制御部 7 1 0 は、さらに、学習処理部 7 1 0 2 を有している。学習処理部 7 1 0 2 は、データ読出部 7 1 0 2、近似関数生成処理部 7 1 1 6、予測処理部 7 1 1 7、誤差逆伝播処理部 7 1 1 8、パラメータ更新処理部 7 1 1 9、暗号化処理部 7 1 2 0、及びデータ送信処理部 7 1 2 1 を備えている。

30

【0092】

データ読出部 7 1 1 5 は、ロボット 7 内に記憶されている種々のデータの読出処理を行う。近似関数生成処理部 7 1 1 6 は、所定の入出力の対応関係に関するキャッシュテーブルに基づき、後述の手法にて近似関数を生成する。予測処理部 7 1 1 7 は、ニューラルネットワークを教師有り学習することにより生成された予測モデル（学習済モデル）の構成等の基本情報や重み情報等を読み込むと共に、入力されたデータに基づいて所定の予測出力を生成する。

40

【0093】

誤差逆伝播処理部 7 1 1 8 は、予測モデルの出力と教師データとを比較して得られた誤差をモデルの出力側から入力側へと伝播させる処理（Back Propagation）を行う。パラメータ更新処理部 7 1 1 9 は、予測モデルの出力と教師データとの誤差を小さくするよう重み等のモデルのパラメータを更新する処理を行う。暗号化処理部 7 1 2 0 は、所定の対象データを公開鍵等により暗号化する処理を行う。データ送信処理部 7 1 2 1 は、所定の対象データを中間サーバ 6 へと送信する処理を行う。

【0094】

図 1 8 は、中間サーバ 6 の制御部 6 1 0 の機能ブロック図である。

【0095】

50

同図において、予測処理部 6 1 0 1 の内容は、図 1 2 において示した構成と略同一であるので詳細な説明は省略する。ただし、予測処理部 6 1 0 1 は、さらにキャッシュテーブル追加処理部 6 1 1 2 を備える点において異なる。キャッシュテーブル追加処理部 6 1 1 2 は、図 1 4 において復号化処理 (S 7 5) を行って第 2 の出力側中間層データ (Z 2) を生成した後に、当該第 2 の出力側中間層データ (Z 2) を、対応する第 2 の入力側中間層データ (X 2) と共に、キャッシュテーブルへと追加記憶させる処理を行う。このキャッシュテーブルは後述の学習処理に用いられる。

【0096】

制御部 6 1 0 は、さらに、学習処理部 6 1 0 2 を有している。学習処理部 6 1 0 2 は、データ入力受付部 6 1 2 3、データ読出部 6 1 1 5、サンプリング処理部 6 1 1 6、近似関数生成処理部 6 1 1 7、予測処理部 6 1 1 8、誤差逆伝播処理部 6 1 1 9、パラメータ更新処理部 6 1 2 0、暗号化処理部 6 1 2 1、及びデータ送信処理部 6 1 2 2 を備えている。

10

【0097】

データ入力受付部 6 1 2 3 は、ロボット 7 から受信する第 1 のキャッシュテーブル等の種々のデータを受信して復号化し記憶する処理を行う。データ読出部 6 1 1 5 は、中間サーバ 6 内に記憶されている種々のデータの読出処理を行う。サンプリング処理部 6 1 1 6 は、キャッシュテーブルから学習対象となるデータセットを選択する処理を行う。近似関数生成処理部 6 1 1 7 は、所定の入出力の対応関係に関するキャッシュテーブルに基づき、後述の手法にて、近似関数を生成する。予測処理部 6 1 1 8 は、ニューラルネットワークを教師有り学習することにより生成された予測モデル (学習済モデル) の構成等の基本情報や重み情報等を読み込むと共に、入力されたデータに基づいて所定の予測出力を生成する。

20

【0098】

誤差逆伝播処理部 6 1 1 9 は、予測モデルの出力と教師データとを比較して得られた誤差をモデルの出力側から入力側へと伝播させる処理 (Back Propagation) を行う。パラメータ更新処理部 6 1 2 0 は、予測モデルの出力と教師データとの誤差を小さくするよう重み等のモデルのパラメータを更新する処理を行う。暗号化処理部 6 1 2 1 は、所定の対象データを公開鍵等により暗号化する処理を行う。データ送信処理部 6 1 2 2 は、所定の対象データをロボット 7 又は最終サーバ 5 へと送信する処理を行う。

30

【0099】

図 1 9 は、最終サーバ 5 の制御部 5 1 0 の機能ブロック図である。

【0100】

同図において、予測処理部 5 1 0 1 の内容は、図 5 において示した構成と略同一であるので詳細な説明は省略する。

【0101】

制御部 5 1 0 は、さらに、学習処理部 5 1 0 2 を有している。学習処理部 5 1 0 2 は、データ入力受付部 5 1 1 5、データ読出部 5 1 1 0、サンプリング処理部 5 1 1 1、予測処理部 5 1 1 2、誤差逆伝播処理部 5 1 1 3、及びパラメータ更新処理部 5 1 1 4 を備えている。

40

【0102】

データ入力受付部 5 1 1 5 は、中間サーバ 6 から受信する第 2 のキャッシュテーブル等の種々のデータを受信して復号化し記憶する処理を行う。データ読出部 5 1 1 0 は、最終サーバ 5 内に記憶されている種々のデータの読出処理を行う。サンプリング処理部 5 1 1 1 は、第 2 のキャッシュテーブルから学習対象となるデータセットを選択する処理を行う。予測処理部 5 1 1 2 は、ニューラルネットワークを教師有り学習することにより生成された予測モデル (学習済モデル) の構成等の基本情報や重み情報等を読み込むと共に、入力されたデータに基づいて所定の予測出力を生成する。

【0103】

誤差逆伝播処理部 5 1 1 3 は、予測モデルの出力と教師データとを比較して得られた誤

50

差をモデルの出力側から入力側へと伝播させる処理（Back Propagation）を行う。パラメータ更新処理部 5114 は、予測モデルの出力と教師データとの誤差を小さくするよう重み等のモデルのパラメータを更新する処理を行う。

【0104】

＜3.2 システムの動作＞

続いて、図20～図26を参照しつつ、システム30の動作について説明する。なお、予測処理動作については第2の実施形態と略同一であるのでここでは説明を省略する。

【0105】

図20は、ロボット7における学習処理動作のフローチャートである。同図から明らかな通り、学習処理動作が開始すると、データ読出部7115は、ロボット7内に記憶され教師データに相当する入出力データテーブルから一対の入出力対（X0、Z0）を読み出す（S101）。この読み出しを行うと、予測処理部7117は、入力データX0に基づいて、予測モデルの入力層から第1の中間層へと至る区間において予測処理を行ない入力側中間層データ（X1-s1）を生成する（S103）。

10

【0106】

一方、これら（S101～S103）と並行して、データ読出部7115は、予測処理時にロボット7へと蓄積された第1の入力側中間層データ（X1）と第1の出力側中間層データ（Z1）との対応関係を含む第1のキャッシュテーブルを読み出す処理を行う（S105）。第1のキャッシュテーブルを読み出した後、この第1のキャッシュテーブルに基づいて、近似関数を生成する処理が行われる（S107）。

20

【0107】

ここで、近似関数の生成処理について詳細に説明する。第1の入力側中間層（説明の便宜上、仮にX層とする）のデータ（X1）を入力として、第1の出力側中間層（説明の便宜上、仮にZ層とする）のデータ（Z1）を生成するデータ変換（キャッシュ変換）は、以下のように表すことができる。

【数1】

$$\vec{z} = S(\vec{x})$$

30

【0108】

ここで、n個のニューロンから成るX層のデータを表すベクトルは以下のように表すことができる。

【数2】

$$\vec{x} = (x_1, \dots, x_m, \dots, x_n)$$

【0109】

同様に、N個のニューロンから成るZ層のデータを表すベクトルは以下のように表すことができる。

40

【数3】

$$\vec{z} = (z_1, \dots, z_k, \dots, z_N)$$

【0110】

また、Z層のk番目の値zkは数式（1）より、他のN-1個の値と独立して計算が可能であるから、以下の通り表すことができる。

【数4】

50

$$z_k = S_k(\vec{x})$$

【0111】

このとき、変換関数 S_k は、キャッシュ変換の性質により、 X 層のデータベクトルの各成分値の組み合わせが第1のキャッシュテーブル内に存在しなければ、対応する Z 層の k 番目の値へと変換することができない。そのため、次のような1次方程式である数式(5)により近似する。

【数5】

$$z_k = (\sum_m^n w_{km} x_m) + b$$

10

【0112】

なお、数式(5)の変数は、下記の $n+1$ 個である。

【数6】

$$w_{k1}, \dots, w_{kn}, b$$

20

【0113】

従って、数式(5)の解を求めるためには、数式(4)から $n+1$ 個のデータを抽出して、以下の $n+1$ 元1次連立方程式を解けばよいこととなる。

【数7】

$$\begin{cases} z_{k1} = w_{k1}x_{1,1} + \dots + w_{km}x_{m,1} + \dots + w_{kn}x_{n,1} + b \\ \dots \\ z_{kj} = w_{k1}x_{1,j} + \dots + w_{km}x_{m,j} + \dots + w_{kn}x_{n,j} + b \\ \dots \\ z_{k,n+1} = w_{k1}x_{1,n+1} + \dots + w_{km}x_{m,n+1} + \dots + w_{kn}x_{n,n+1} + b \end{cases}$$

30

【0114】

なお、この $n+1$ 個のデータを抽出する際には、近似値を得たい点の近傍のキャッシュデータを選出することが好ましい。近似値を得たい点の近傍のキャッシュデータを可能な限り抽出することで、近似誤差の変動を抑制することができるためである。このようなキャッシュデータの抽出に関する概念図が図21に示されている。

40

【0115】

ここで、以下の通り、定義することができる。

【数8】

50

$$\beta_k = (z_{k,1}, \dots, z_{k,j}, \dots, z_{k,n+1})$$

$$A = \begin{pmatrix} x_{1,1} & \cdots & x_{m,1} & \cdots & x_{n,1} & 1 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ x_{1,j} & \cdots & x_{m,j} & \cdots & x_{n,j} & 1 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ x_{1,n+1} & \cdots & x_{m,n+1} & \cdots & x_{n,n+1} & 1 \end{pmatrix}$$

10

$$v_k = (w_{k1}, \dots, w_{km}, \dots, w_{kn}, b)$$

【 0 1 1 6 】

そうすると、数式（ 7 ）は、下記の通り簡潔に表現することができる。

【数 9 】

$$Av_k = \beta_k$$

20

【 0 1 1 7 】

$n + 1$ 次の正方行列である A が正則行列であれば、数式（ 9 ）は一意に以下の解 v_k をもつ。

【数 1 0 】

$$v_k = \hat{v}_k = (\hat{w}_{k1}, \dots, \hat{w}_{km}, \dots, \hat{w}_{kn}, \hat{b})$$

【 0 1 1 8 】

30

すなわち、数式（ 9 ）をガウスの消去法等のアルゴリズムに則り、コンピュータで演算することで、数式（ 1 0 ）の解 v_k を得ることができる。この解 v_k を代入することで、数式（ 5 ）は以下のように表すことができる。

【数 1 1 】

$$z_k = \left(\sum_m^n \hat{w}_{km} x_m \right) + \hat{b}$$

【 0 1 1 9 】

40

すなわち、この数式（ 1 1 ）が近似式となる。なお、同数式から明らかな通り、 X 層のデータベクトルの各成分について近似的に偏微分が可能であるので、例えば、 Z 層から X 層への誤差逆伝播等も容易に行うことができる。すなわち、キャッシュテーブルが対応する学習モデル部分の前後、すなわち、例えば入力側・出力側の各機械学習モデルが多階層ニューラルネットワークモデルであっても、誤差逆伝播法を用いて高速に学習処理を行うことができる。

【 0 1 2 0 】

図 2 0 のフローチャートに戻り、第 1 の入力側中間層データ（ $X_1 - s_1$ ）の生成処理（ $S_1 0 3$ ）と近似関数の生成処理（ $S_1 0 7$ ）が完了すると、予測処理部 7 1 1 7 により、第 1 の入力側中間層データ（ X_1 ）と近似関数に基づいて、第 1 の中間層から第 2 の

50

中間層へと至る区間の予測処理が行われ出力側中間層データ（Z1-s1）が生成される（S109）。また、その後、予測処理部7117は、出力側中間層データ（Z1-s1）を入力として、第2の中間層から出力層へと至る区間の予測処理を行い、最終出力（Z0-s1）を生成する（S111）。

【0121】

誤差逆伝播処理部6119は、教師データに係る教師出力（Z0）と最終出力（Z0-s1）との誤差を生成し、当該誤差又はそれに基づく所定の値（例えば、二乗平均誤差等）を、例えば、最急降下法等の手法により出力側から入力側へと伝播する（S113）。

【0122】

その後、パラメータ更新処理部7119は、逆伝播された誤差等に基づいて、学習モデルのうち、近似関数部分を除く、入力層から第1の中間層へと至る区間と、第2の中間層から出力層へと至る区間の重み等のパラメータを更新する処理を行う（S115）。

【0123】

その後、ロボット7は、第1のキャッシュテーブルを送信することが許可されているかを所定の設定情報から確認する（S117）。その結果、送信許可がない場合には、学習終了判定（S121）を行い、終了しない場合（S121NO）には、再度すべての処理（S101～S121）を繰り返す。一方、終了する場合（S121YES）には、学習処理は終了する。

【0124】

一方、キャッシュテーブルの送信許可がある場合（S117YES）には、データ送信処理部7121は、暗号化処理部7120による暗号化を施した第1のキャッシュテーブルを中間サーバ6へと送信する処理を行う（S119）。なお、その後、学習終了判定（S121）が行われる。

【0125】

次に、中間サーバ6の学習処理動作について説明する。

【0126】

図22は、ロボット7から送信される第1のキャッシュテーブルの受信及び記憶処理に関するフローチャートである。同図から明らかな通り、中間サーバ6において学習処理が開始すると、データ入力受付部6123は、データ受信待機状態へと移行する（S131）。この状態において、暗号化された第1のキャッシュテーブルに相当するデータを受信すると（S131YES）、データ受信待機状態は解除され、受信した第1のキャッシュデータを秘密鍵等により復号化し（S133）、記憶部へと記憶する処理（S135）が行われる。この記憶処理が終了すると、再び中間サーバ6は受信待機状態（S131NO）へと移行する。

【0127】

図23は、図22に示した第1のキャッシュテーブルの受信処理と平行して実行される、中間サーバ6における学習処理動作に関するフローチャートである。同図から明らかな通り、学習処理が開始すると、データ読出部6115は、中間サーバ6内に記憶され教師データに相当する入出力データテーブルから入出力対（X1-s1、Z1-s1）を読み出す（S141）。入出力対が読み出されると、サンプリング処理部6116は、学習に使用する入出力対を抽出する（S143）。この抽出処理の後、予測処理部6118は、入力データ（X1-s1）に基づいて、予測モデルの第1の中間層から第3の中間層へと至る区間において予測処理を行なって、第2の入力側中間層データ（X2-s2）を生成する（S145）。

【0128】

一方、これら（S141～S145）と並行して、データ読出部6115は、予測処理時に中間サーバ6へと蓄積された第2の入力側中間層データ（X2）と第1の出力側中間層データ（Z2）との対応関係を含む第2のキャッシュテーブル（X2、Z2）を読み出す処理を行う（S147）。第2のキャッシュテーブルを読み出した後、この第2のキャッシュテーブルに基づいて、第2の入力側中間層データ（X2）に基づいて第2の出力側

10

20

30

40

50

中間層データ（ Z_2 ）を生成するような近似関数を生成する処理が行われる（ $S149$ ）。なお、近似関数の生成処理はロボット7における近似関数生成と同様である。

【0129】

第2の入力側中間層データ（ $X_2 - s_2$ ）の生成処理（ $S145$ ）と近似関数の生成処理（ $S149$ ）が完了すると、予測処理部6118により、第2の入力側中間層データ（ $X_2 - s_2$ ）と近似関数に基づいて、第3の中間層から第4の中間層へと至る区間の予測処理が行われ第2の出力側中間層データ（ $Z_2 - s_2$ ）が生成される（ $S151$ ）。また、その後、予測処理部6118は、第2の出力側中間層データ（ $Z_2 - s_2$ ）を入力として、第4の中間層から第2の中間層へと至る区間の予測処理を行い、第2の出力側予測出力（ $Z_1 - s_2$ ）を生成する（ $S153$ ）。

10

【0130】

誤差逆伝播処理部6119は、教師データ（ $Z_1 - s_1$ ）と第2の出力側予測出力（ $Z_1 - s_2$ ）との誤差を生成し、当該誤差又はそれに基づく所定の値（例えば、二乗平均誤差等）を、例えば、最急降下法等の手法により出力側から入力側へと伝播する（ $S155$ ）。

【0131】

その後、パラメータ更新処理部6120は、逆伝播された誤差等に基づいて、学習モデルのうち、近似関数部分を除く、第1の中間層から第3の中間層へと至る区間と、第4の中間層から第2の中間層へと至る区間の重み等のパラメータを更新する処理を行う（ $S157$ ）。

20

【0132】

その後、中間サーバ6は、第2のキャッシュテーブル（ $X_2 - s_2$ 、 $Z_2 - s_2$ ）を送信することが許可されているか否かを所定の設定情報から確認する（ $S159$ ）。その結果、送信許可がない場合には、学習終了判定（ $S163$ ）を行い、終了しない場合（ $S163NO$ ）には、再度すべての処理（ $S141 \sim S163$ ）を繰り返す。一方、終了する場合（ $S163YES$ ）には、学習処理は終了する。

【0133】

一方、キャッシュテーブルの送信許可がある場合（ $S159YES$ ）には、データ送信処理部6122は、暗号化処理部6121による暗号化を施した第2のキャッシュテーブルを最終サーバ5へと送信する処理を行う（ $S161$ ）。なお、その後、学習終了判定（ $S163$ ）が行われる。

30

【0134】

次に、最終サーバ5の学習処理動作について説明する。

【0135】

図24は、中間サーバ6から送信される第2のキャッシュテーブル（ $X_2 - s_2$ 、 $Z_2 - s_2$ ）の受信及び記憶処理に関するフローチャートである。同図から明らかな通り、最終サーバ5において学習処理が開始すると、データ入力受付部5115は、データ受信待機状態へと移行する（ $S171$ ）。この状態において、暗号化された第2のキャッシュテーブルに相当するデータを受信すると（ $S171YES$ ）、データ受信待機状態は解除され、受信した第2のキャッシュデータを秘密鍵等により復号化し（ $S173$ ）、記憶部へと記憶する処理（ $S175$ ）が行われる。この記憶処理が終了すると、再び最終サーバ5は受信待機状態（ $S171NO$ ）へと移行する。

40

【0136】

図25は、図24に示した第2のキャッシュテーブルの受信処理と平行して実行される、最終サーバ5における学習処理動作に関するフローチャートである。学習処理が開始すると、データ読出部5110は、キャッシュテーブルを読み出す処理を行う（ $S181$ ）。その後、サンプリング処理部（ $S5111$ ）は、キャッシュテーブルから学習対象となる入出力対を抽出する（ $S183$ ）。

【0137】

予測処理部5112は、読み出された第2の入力側中間層データ（ $X_2 - s_2$ ）に基づ

50

き、第3の中間層から第4の中間層までの予測処理を行い、第2の出力側中間層データ（ $Z2-s3$ ）を生成する（ $S185$ ）。誤差逆伝播処理部5113は、第2の出力側中間層データ（ $Z2-s3$ ）と教師データ（ $Z2-s2$ ）との誤差を生成し、当該誤差又はそれに基づく所定の値（例えば、二乗平均誤差等）を、例えば、最急降下法等の手法により出力側から入力側へと伝播する（ $S187$ ）。

【0138】

その後、パラメータ更新処理部5114は、逆伝播された誤差等に基づいて、学習モデルの重み等のパラメータを更新する処理を行う（ $S189$ ）。パラメータの更新処理が行われると、学習の終了判定が行われ、所定の終了条件が満たされていない場合（ $S191NO$ ）には、再度一連の処理（ $S181\sim S189$ ）が行われる。一方、所定の終了条件が満たされた場合（ $S191YES$ ）には、学習処理は終了する。

【0139】

図26は、本実施形態に係るシステム30により実現される学習処理の概念図である。同図において、上段は、ロボット7において行われる学習処理の概念図であり、中段は、中間サーバ6において行われる学習処理の概念図であり、下段は、最終サーバ5において行われる学習処理の概念図である。また、同図において左側が入力側、右側が出力側を示している。

【0140】

同図から明らかな通り、ロボット7において入力情報（ $X0$ ）が入力されると、予測処理部7117は、入力段階から第1の中間層までの間の予測処理を行い、第1の入力側中間層データ（ $X1-s1$ ）を生成する。一方、近似関数生成処理部7116により、第1のキャッシュテーブル（ $X1$ 、 $Z1$ ）に基づいて近似関数（ $F(x)$ ）が生成される。予測処理部7117は、第1の入力側中間層データ（ $X1-s1$ ）と近似関数（ $F(x)$ ）に基づいて、第1の出力側中間層データ（ $Z1-s1$ ）を生成する。また、第1の出力側中間層データ（ $Z1-s1$ ）に基づいて最終出力データ（ $Z0-s1$ ）が生成される。誤差逆伝播処理部7118は、この最終出力データ（ $Z0-s1$ ）と教師データ（ $Z0$ ）との間の誤差を最終出力段階から近似関数を経て入力段階まで逆伝播させる。その後、パラメータ更新処理部7119は、最終出力段階から第2の中間層、第1の中間層から入力段階までの間の重みを含むパラメータが更新される。また、このとき生成された第1のキャッシュテーブル（ $X1-s1$ 、 $Z1-s1$ ）は、所定条件下で中間サーバ6へと提供される。

【0141】

また、同図から明らかな通り、中間サーバ6において第1の入力側中間層データ（ $X1-s1$ ）が入力されると、予測処理部6118は、第1の中間層から第3の中間層までの間の予測処理を行い、第2の入力側中間層データ（ $X2-s2$ ）を生成する。一方、近似関数生成処理部6117により、第1のキャッシュテーブル（ $X1-s1$ 、 $Z1-s1$ ）に基づいて近似関数（ $G(x)$ ）が生成される。予測処理部6118は、第2の入力側中間層データ（ $X2-s2$ ）と近似関数（ $G(x)$ ）に基づいて、第2の出力側中間層データ（ $Z2-s2$ ）を生成する。また、第2の出力側中間層データ（ $Z2-s2$ ）に基づいて第1の出力側中間層データ（ $Z1-s2$ ）が生成される。誤差逆伝播処理部6119は、この最終出力データ（ $Z1-s2$ ）と教師データ（ $Z1-s1$ ）との間の誤差を第2の中間層から近似関数を経て第1の中間層まで逆伝播させる。その後、パラメータ更新処理部6120は、第2の中間層から第4の中間層、第3の中間層から第1の中間層までの間の重みを含むパラメータを更新する。また、このとき生成された第2のキャッシュテーブル（ $X2-s2$ 、 $Z2-s2$ ）は、所定条件下で最終サーバ5へと提供される。

【0142】

さらに、同図から明らかな通り、最終サーバ5において第2の入力側中間層データ（ $X2-s2$ ）が入力されると、予測処理部5112は、第3の中間層から第4の中間層までの間の予測処理を行い、第2の出力側中間層データ（ $Z2-s3$ ）を生成する。誤差逆伝播処理部5113は、この第2の出力側中間層データ（ $Z2-s3$ ）と教師データ（ $Z2$

ー s 2) との間の誤差を第 4 の中間層から第 3 の中間層まで逆伝播させる。その後、パラメータ更新処理部 5 1 1 4 は、第 4 の中間層から第 4 の中間層までの間の重みを含むパラメータが更新される。

【0 1 4 3】

< 4. 変形例 >

本発明は上述の実施形態の構成・動作に限定されるものではなく、様々に変形することが可能である。

【0 1 4 4】

第 3 の実施形態において、キャッシュテーブルから生成される近似関数は学習処理の際のみ使用されるものとして記載した。しかしながら、本発明はこのような構成に限定されない。例えば、予測処理の目的で、それまでに得られているキャッシュテーブルに基づいて近似関数を生成し、第 1 の入力側中間層データ (X 1) と近似関数とに基づいて、第 1 の中間層から第 2 の中間層へと至る区間の予測処理を行い出力側中間層データ (Z 1) を生成してもよい。このような構成によれば、例えば一定程度ハッシュテーブルへとデータが蓄積された後においては、サーバ側への問合せ頻度を大幅に減らすか又は問い合わせを行うことなく予測処理を行うことが可能となる。

【0 1 4 5】

上述の実施形態においては、入力側中間層データ (X) (例えば X 1 又は X 2) を暗号化、ハッシュ化した後に、当該ハッシュ値をキーとしてハッシュテーブル検索処理を行っている (例えば、図 6 の S 1 1、図 1 3 の S 5 5 など)。しかしながら、本発明はこのような構成に限定されない。従って、例えば、入力側中間層データ (X) について丸め処理を行った後に暗号化及び／又はハッシュ化し、ハッシュテーブル検索してもよい。丸め処理とは、入力側中間層データ (X) が属する集合を U としたときに、集合 U に属する特定の入力側中間層データにつき同じ値 (X_u) (代表値) を持つものとみなす処理である。例えば、入力側中間層データ (X) の一部のノード値 (ニューロン発火値) につき、数値の切り上げ又は切り下げ処理等を行って整数値に離散化させ複数の整数値の集合を形成してもよい。このような構成によれば、過去に得られたハッシュ値との一致性を向上させ、処理の高速化等を実現することができる。

【0 1 4 6】

上述の実施形態においては、クライアント装置としてのロボット 7 は中間サーバ 6 又はサーバ 1 との間で直接通信する構成とした。しかしながら、このような構成に限定されない。図 2 7 は、変形例に係るシステム 4 0 の全体構成図である。同構成においてはシステム 4 0 は、予測処理を行うサーバ 2 と、サーバ 2 と WAN を介して接続され、かつ、LAN に接続された仲介サーバ 8 と、LAN に接続されたクライアント装置としてのロボット 9 とから構成されている。本変形例においては、サーバ 2 とクライアント装置 9 との間の情報のやり取りは仲介サーバ 8 を介して行われることとなる。

【0 1 4 7】

上述の実施形態では、機械学習アルゴリズムとして、ニューラルネットワーク (又はディープラーニング) を用いた教師あり学習を例示した。しかしながら、本発明はそのような構成に限定されない。従って、例えば、他の分割可能であって、同様な形式で中間値を取り扱うことが可能な機械学習アルゴリズムを利用してもよい。また、教師あり学習のみならず、例えば、GAN (Generative Adversarial Networks) や VAE (Variational Auto Encoder)、SOM (Self-Organizing Map) 等の教師なし学習や、強化学習を利用してもよい。なお、強化学習を行う場合には、例えば、シミュレータ上での予測処理等を利用してもよい。

【0 1 4 8】

上述の実施形態における学習処理においては、近似関数を式 5 において示した 1 次方程式により近似することで生成した。しかしながら、近似手法はこのような例に限定されず、他の手法により近似を行ってもよい。

10

20

30

40

50

【0149】

例えば、近似関数としてバイパス関数を利用してもよい。図28は、バイパス関数を利用する例に関する概念図である。同図において、 $H(x)$ は、式5等で示された1次方程式による近似関数を表し、 $J(x)$ は、バイパス関数を表し、全体として近似関数を形成している。同図から明らかな通り、バイパス関数である $J(x)$ は、1次方程式による近似関数 $H(x)$ を迂回（バイパス）するように並列的に配置されている。なお、いずれの関数も誤差逆伝播法を適用可能である。

【0150】

図29は、バイパス関数 $J(x)$ の概念図である。同図の例にあつては、入力側中間層のノード数の方が出力側中間層のノード数より大きい場合が示されている。入力側中間層からデータが入力されると、バイパス関数 $J(x)$ は、より少ないノード数（例えば、入力側中間層のノード数の半分程度）のプーリング層によりデータ圧縮を行う。その後、プーリング層におけるノード出力は、出力側中間層へと提供される。このとき、プーリング層から出力側中間層への結合が存在しないノードに対してはゼロ（0）が提供される（ゼロパディング）。

【0151】

例えば、入力側中間層のノード数 n_x が32個、出力側中間層のノード数 n_z が20個の場合、プーリング層のノード数は入力側中間層のノード数 n_x の半分の16個となる。このとき、プーリング手法としては、隣り合うノード値との平均を採る平均プーリング等を利用することができる。その後、プーリング層からの16個の出力は出力側中間層へと提供される。このとき、プーリング層のノードと対応付かない4個の出力側中間層のノードに対しては、ゼロ（0）が提供される。なお、本変形例ではプーリング層を利用しているが、必ずしもプーリング層を利用する必要はなく、例えば、そのままデータを素通りさせる迂回路を形成してもよい。

【0152】

このような構成によれば、キャッシュテーブルに基づいて生成される近似関数を迂回することで誤差逆伝播が促進され、その結果、学習の効率化を行うことができる。

【0153】

また、例えば、近似関数として、複数のサブ近似関数の和を用いてもよい。図30は、サブ近似関数の和を利用した近似の概念図である。同図から明らかな通り、近似関数の出力は、複数の異なる近似関数 $K_1(x)$ 、 $K_2(x)$ 、 $K_3(x)$ 、 $\dots$ 、 $K_n(x)$ （以下、便宜上、これらの関数をサブ近似関数と呼ぶ）にそれぞれ寄与係数 a_1 、 a_2 、 a_3 、 $\dots$ 、 a_n を掛け合わせた値の総和（重み付き和）となる。なお、このとき、寄与係数 a_i （ $i=1, 2, \dots, n$ ）はそれぞれ0以上1以下の値をとり、 a_i の総和は1、すなわち、 $a_1 + a_2 + \dots + a_n = 1$ となる。この寄与係数は固定値であってもよいし、順方向演算や誤差逆伝播の度に異なる値を与える等変動させてもよい。各サブ近似関数は、キャッシュテーブルに基づいて生成される近似関数であり、ニューラルネットワークや上述の実施形態において利用した1次方程式による近似関数等である。なお、いずれのサブ近似関数も誤差逆伝播法を適用可能に構成されている。

【0154】

このような構成によれば、近似関数前後の階層とのアンサンブル効果により近似精度の向上が見込まれ、その結果、キャッシュテーブルにおけるデータ蓄積が不十分な場合であっても近似精度の維持又は向上を見込むことができる。

【0155】

上述の実施形態においては、ロボット、中間サーバ、最終サーバ等はすべての単一の装置として例示した。しかしながら、本発明はそのような構成に限定されない。従って、例えば、装置構成の一部を外部装置として別に設けてもよい。例えば、外部の大容量記憶ストレージを設置しサーバ等の装置と接続してもよい。また、単一の装置でなく、複数の装置を用いて分散処理等を行ってもよい。さらに、仮想化技術等を用いてもよい。

【0156】

上述の実施形態においては、一つのクライアント装置が1つのハッシュテーブルを保持するものとしたが、本発明はこのような構成に限定されない。従って、例えば、複数のクライアント装置間でハッシュテーブルを共有してもよい。これにより、各クライアント装置においてそれぞれ行われた予測処理のキャッシュが共有のものとして蓄積されていくので、より迅速に、サーバ利用コストの低減、処理の高速化、クライアント装置の自律的な動作などを実現することができる。なお、ハッシュテーブルの共有は、例えば、図27のシステムにおける仲介サーバ8を用いて行われてもよいし、分散ハッシュテーブル等の技術を用いてサーバ等を介さずに直接各クライアント装置間で互いに情報の照会をすることにより行われてもよい。

【0157】

上述の実施形態においては学習処理を逐次的に行う例を示したが、このような構成に限定されない。従って、例えば、複数の入出力対に対応する誤差を一定程度蓄積させた後にバッチ的にパラメータ更新を行うような構成としてもよい。また、予測処理と平行して学習処理を行うような所謂オンライン学習を行ってもよい。

【0158】

上述の実施形態においては、クライアント装置としてロボットを例示した。しかしながら、本発明はこのような構成に限定されない。クライアント装置は、物理的動作を伴うかを問わず、あらゆる装置を含むものとして解釈されるべきである。例えば、クライアント装置には、スマートフォン、タブレット端末、パーソナルコンピュータ、スマートスピーカ、ウェアラブル端末などあらゆる情報処理装置を含むことに留意されたい。

【0159】

上述の実施形態においては、ロボットの動作情報（センサ信号やモータ信号）を学習対象としたが本発明はこのような構成に限定されない。従って、例えば、学習対象データは、撮像信号、音声信号、画像信号、動画像信号、言語情報、文字情報などあらゆる情報を含み、例えば、音声認識処理、画像信号処理、自然言語処理等など様々な目的の処理を行ってもよい。

【0160】

上述の実施形態においては、クライアント装置は、入力側中間層（X）と出力側中間層（Z）との間の演算をサーバ側に演算させる構成としているものの、本発明はこのような構成に限定されない。従って、例えば、クライアント装置も所定の分割された中間層を一部保持し、複数回、サーバと部分的な予測結果の送受信を行うことで予測処理を行ってもよい。

【0161】

上述の実施形態においては、誤差逆伝播法により逆伝播された誤差に基づいて学習モデルのうち近似関数を除いた部分について重み等のパラメータ更新処理を行った（例えば、S115、S157など）。しかしながら、本発明はこのような構成に限定されない。従って、例えば、近似関数部分のパラメータについても更新処理を行ってもよい。

【産業上の利用可能性】

【0162】

本発明は、機械学習技術を利用するすべての産業において利用可能である。

【符号の説明】

【0163】

- 1 サーバ
- 3 ロボット
- 5 最終サーバ
- 6 中間サーバ
- 7 ロボット
- 8 仲介サーバ
- 10 システム

10

20

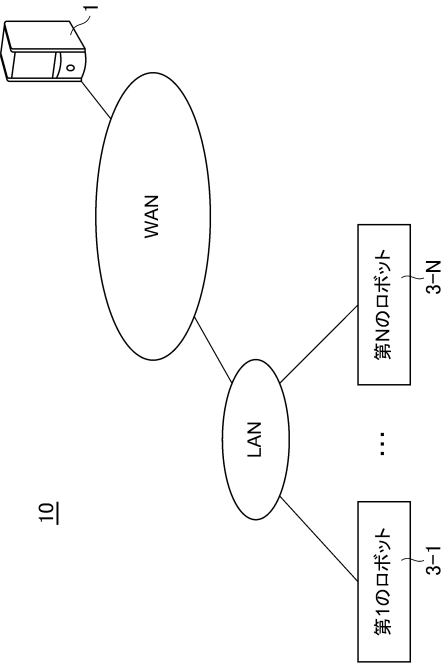
30

40

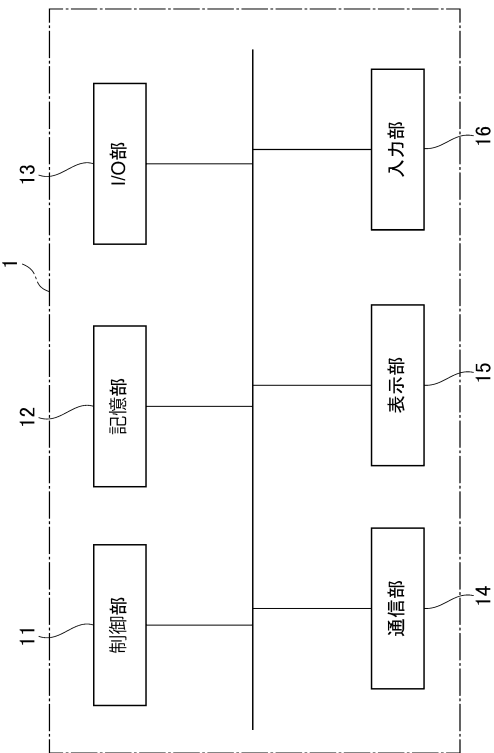
50

【図面】

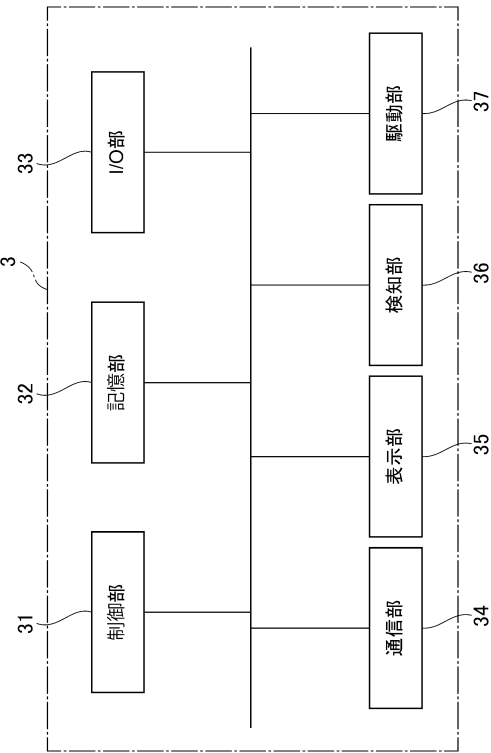
【図 1】



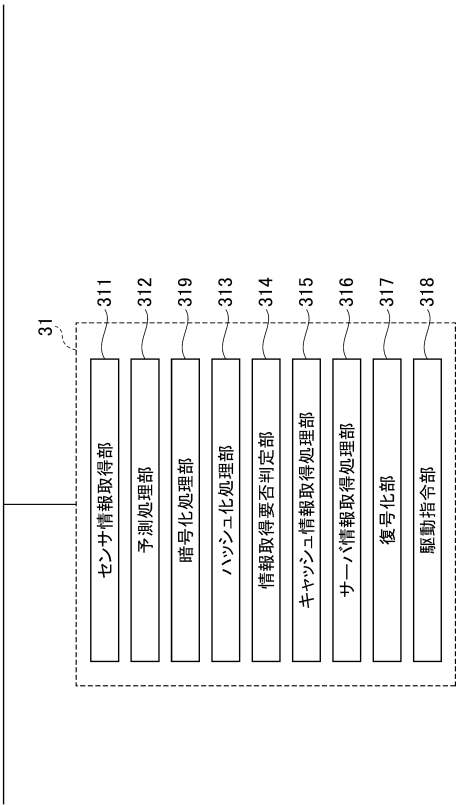
【図 2】



【図 3】



【図 4】



10

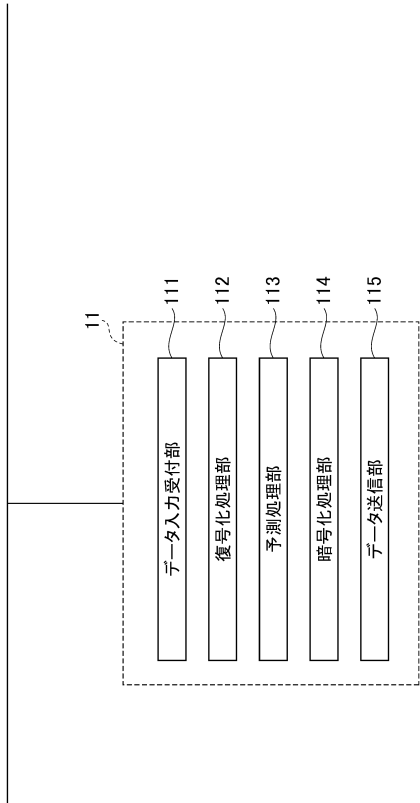
20

30

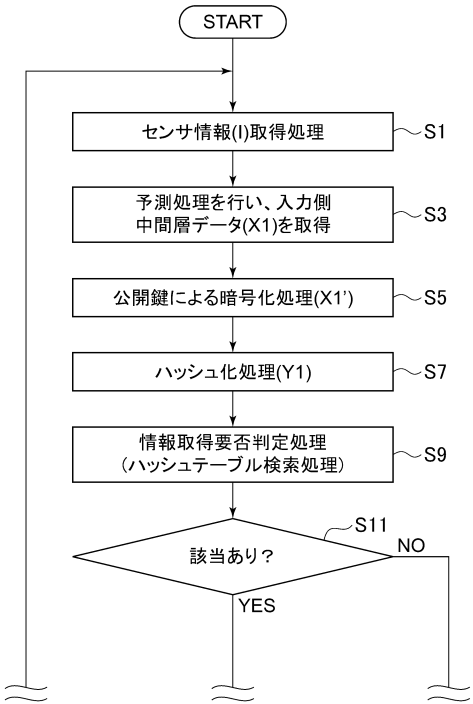
40

50

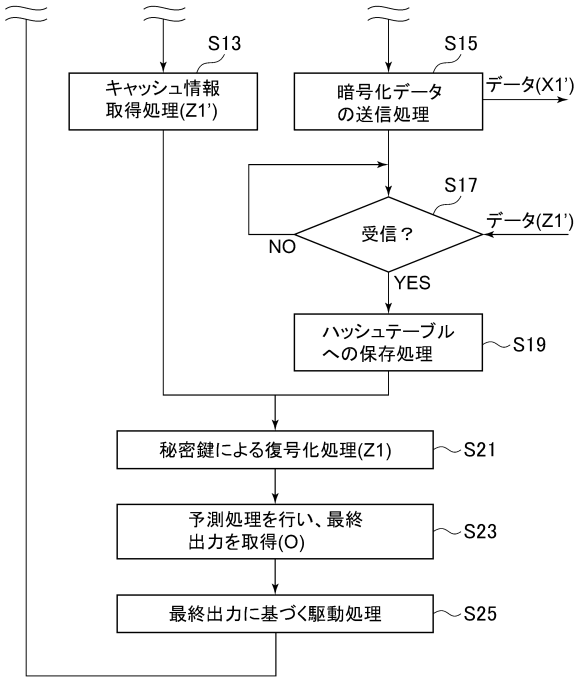
【図 5】



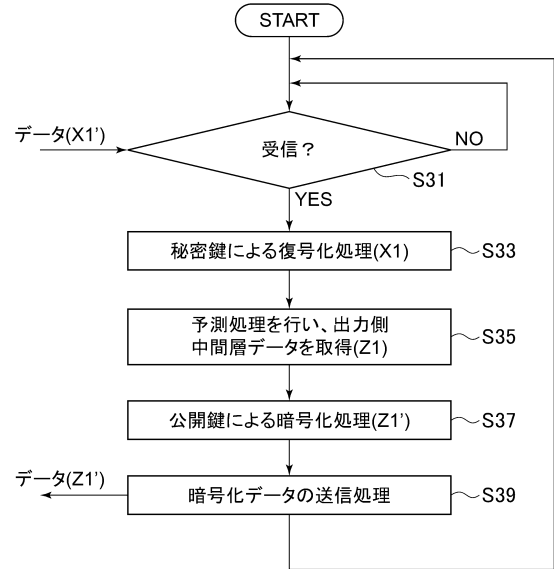
【図 6】



【図 7】



【図 8】



10

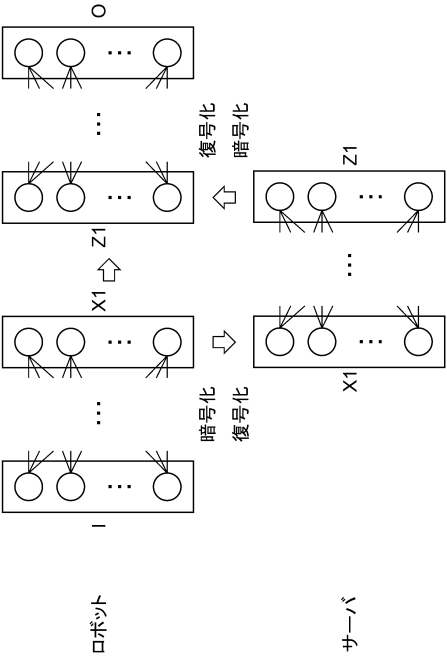
20

30

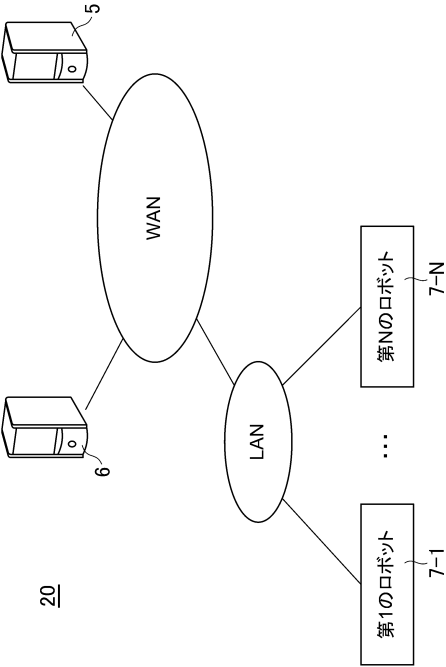
40

50

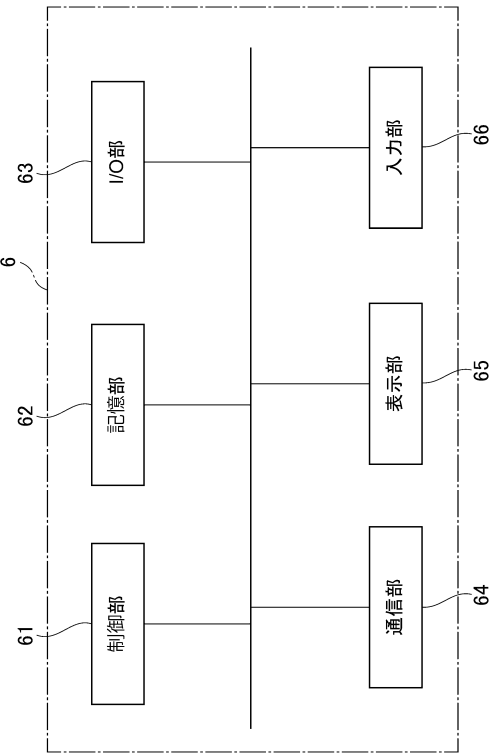
【図 9】



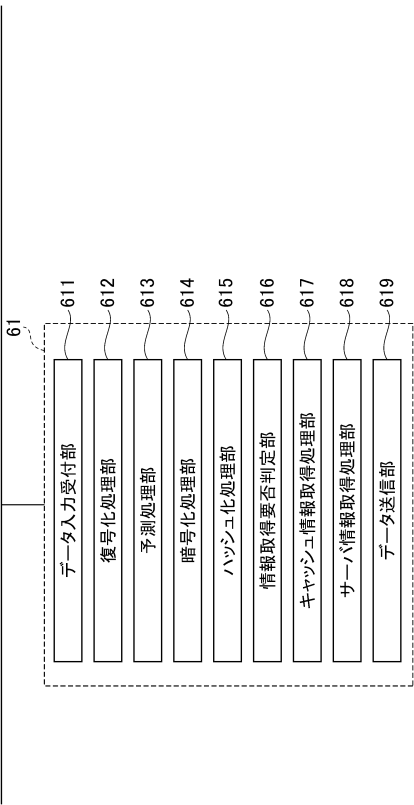
【図 10】



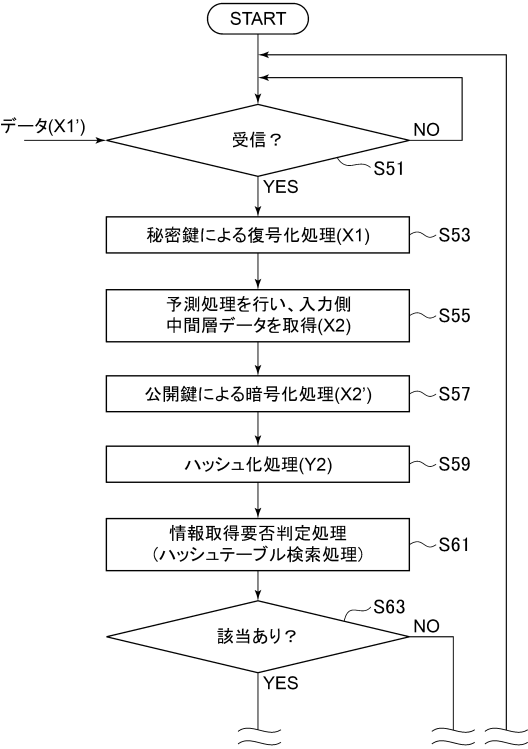
【図 11】



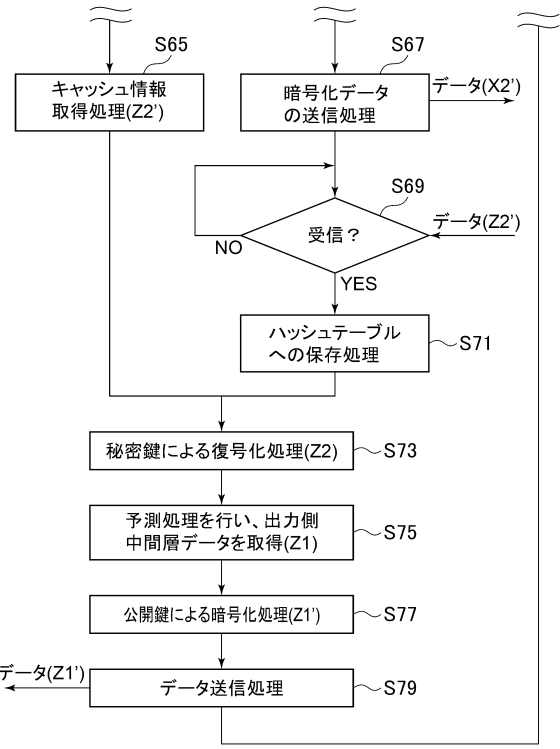
【図 12】



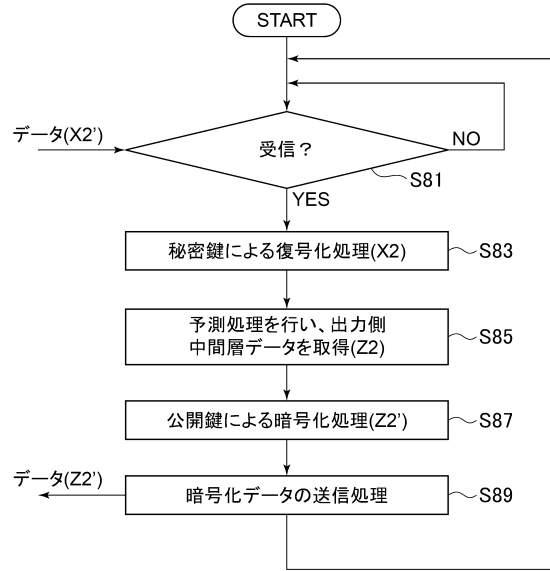
【図 1 3】



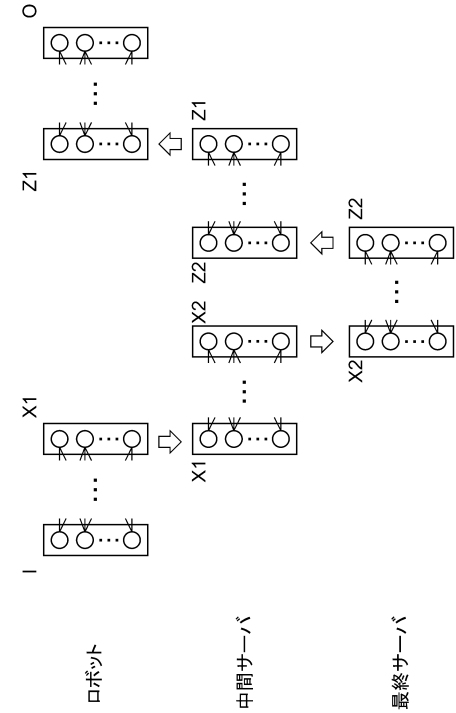
【図 1 4】



【図 1 5】



【図 1 6】



10

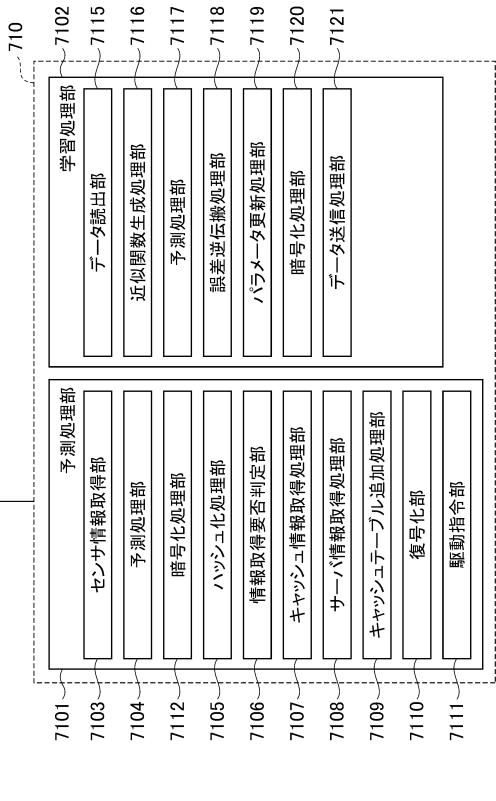
20

30

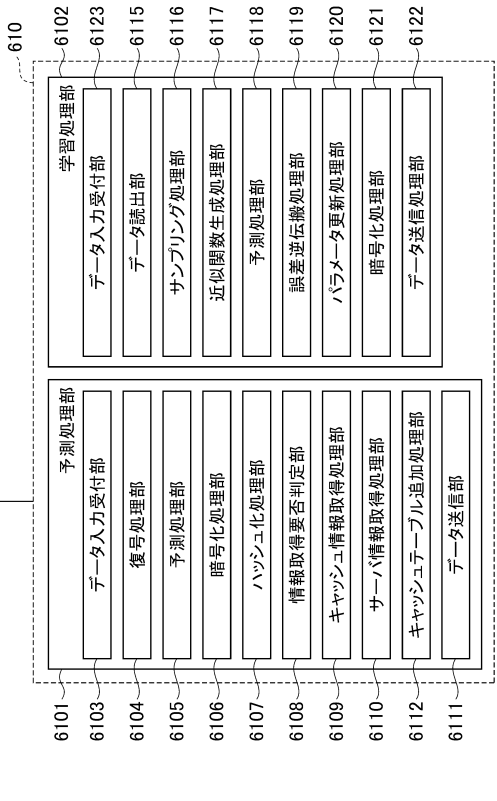
40

50

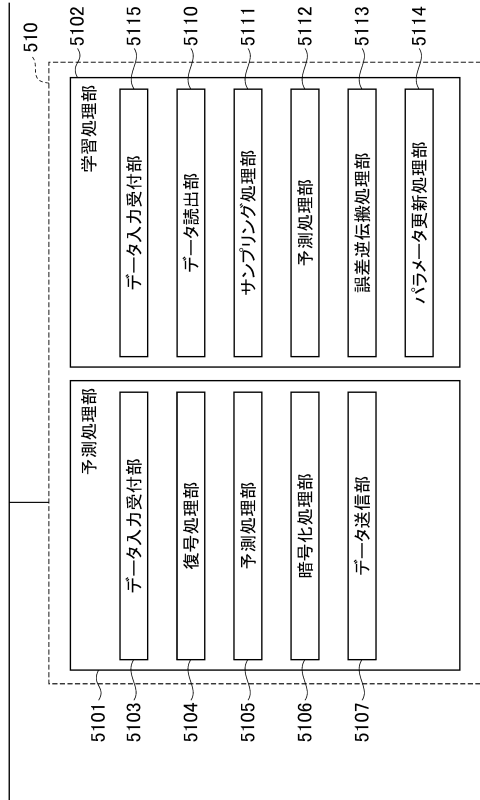
【図 1 7】



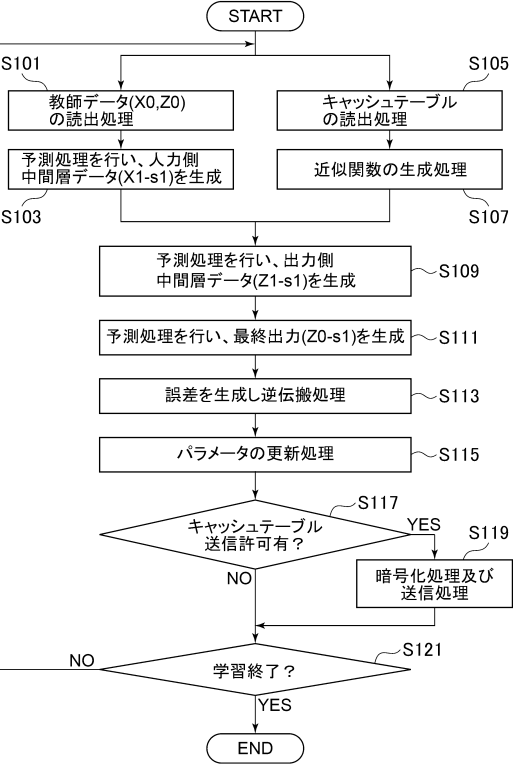
【図 1 8】



【図 1 9】



【図 2 0】



10

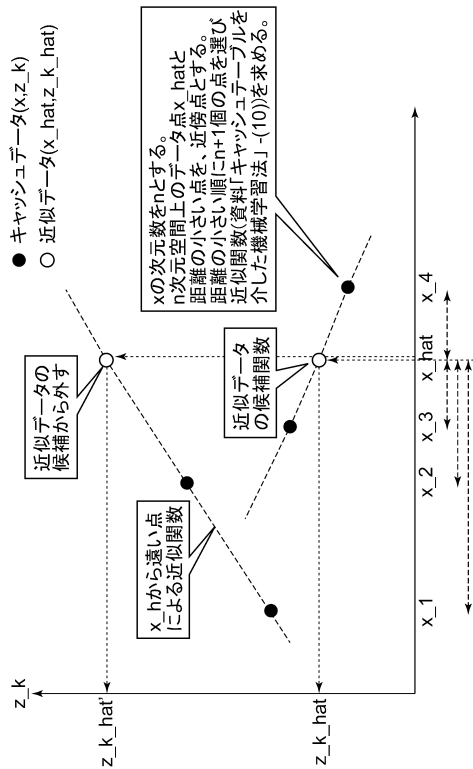
20

30

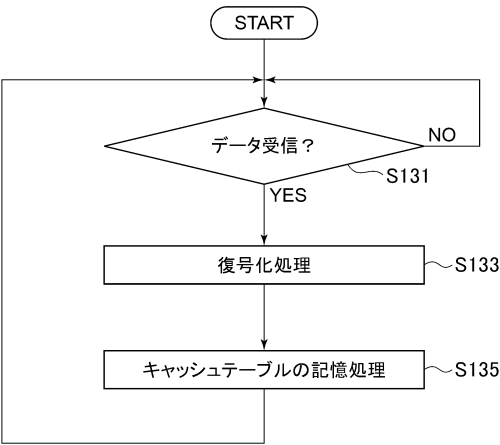
40

50

【図 2 1】



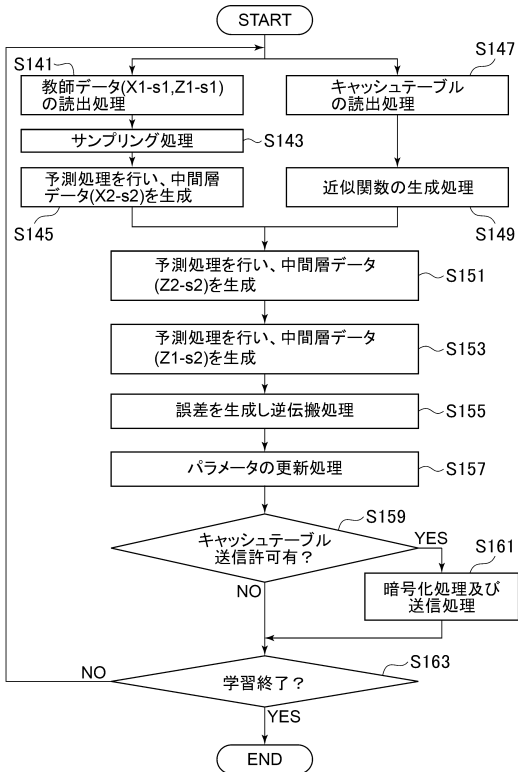
【図 2 2】



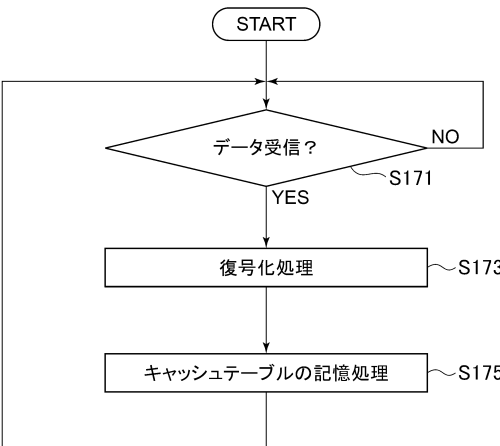
10

20

【図 2 3】



【図 2 4】

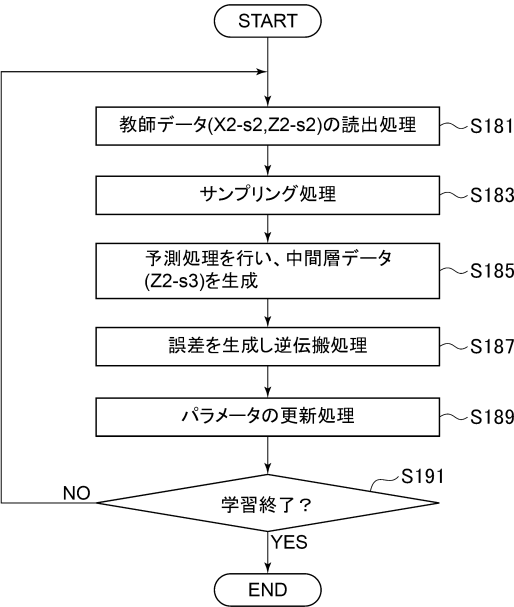


30

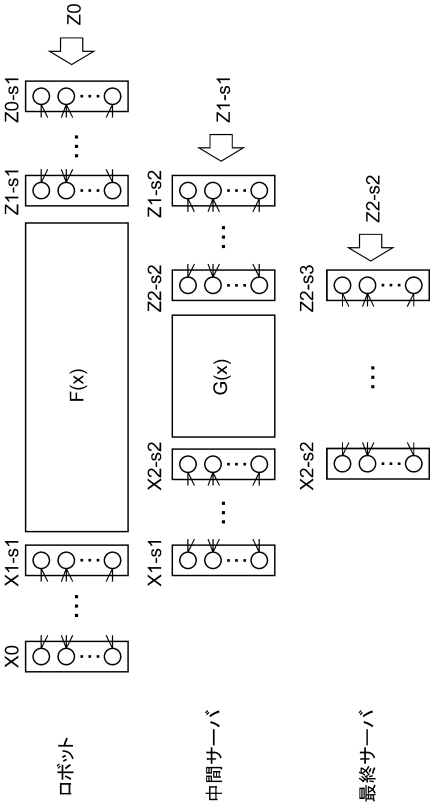
40

50

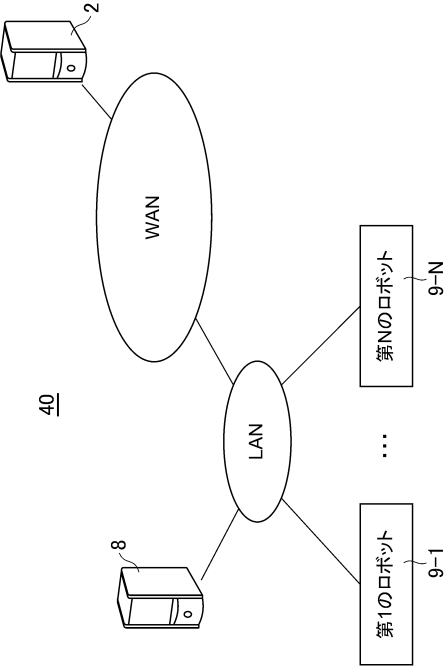
【図 2 5】



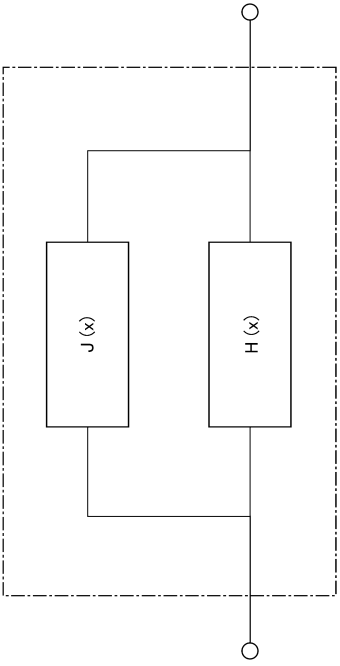
【図 2 6】



【図 2 7】



【図 2 8】



10

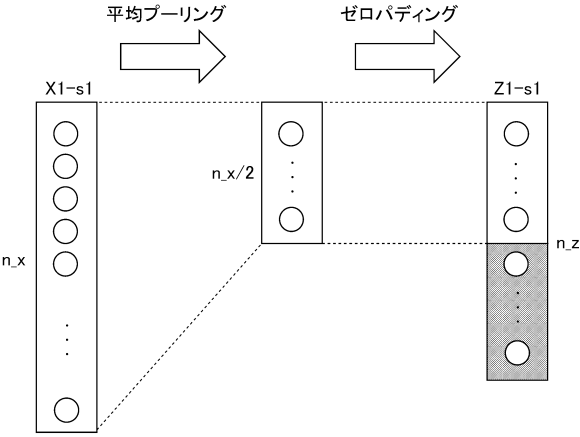
20

30

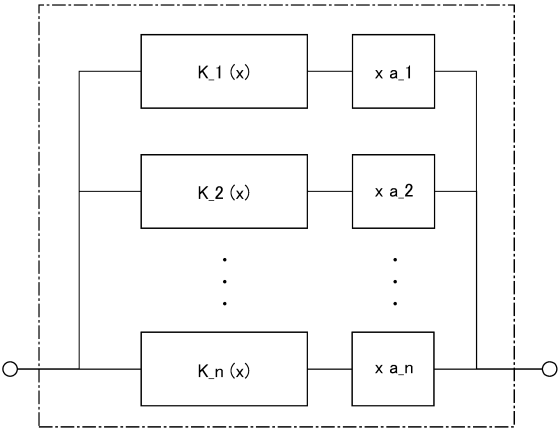
40

50

【図 29】



【図 30】



10

20

30

40

50

フロントページの続き

 T 株式会Geek Guild内
 審査官 渡辺 順哉
(56)参考文献 特許第5816771 (JP, B1)
 特開2018-163623 (JP, A)
 特開2018-097612 (JP, A)
(58)調査した分野 (Int.Cl., DB名)
 G06N 3/00-99/00