(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2018-190239
(P2018-190239A)
(43)公開日　平成30年11月29日(2018.11.29)

(51)Int.Cl.		F I		テーマコード（参考）
G06N 99/00	(2010.01)	G06N	99/00	150
G06F 9/48	(2006.01)	G06F	9/46	457
G06F 21/62	(2013.01)	G06F	21/62	318

審査請求 未請求　請求項の数 13　ＯＬ　（全 20 頁）

(21)出願番号　特願2017-93205(P2017-93205)
(22)出願日　平成29年5月9日(2017.5.9)

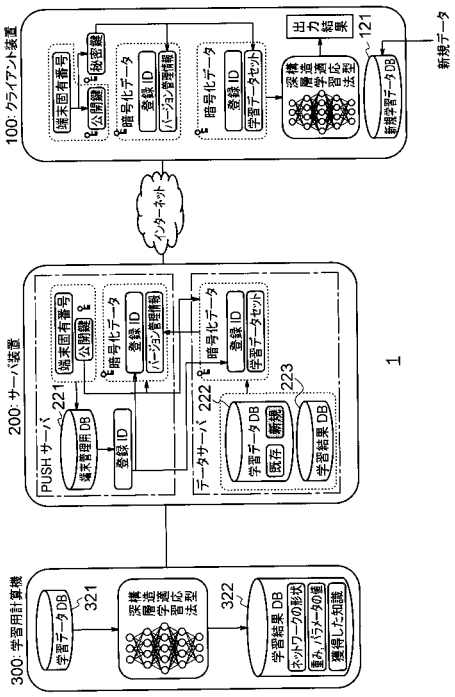
（出願人による申告）平成２８年度、総務省、戦略的情報通信研究開発推進委託事業、産業技術力強化法第１９条の適用を受ける特許出願

(71)出願人　507234438
公立大学法人県立広島大学
広島県広島市南区宇品東１丁目１番７１号
(74)代理人　100091982
弁理士　永井　浩之
(74)代理人　100091487
弁理士　中村　行孝
(74)代理人　100082991
弁理士　佐藤　泰和
(74)代理人　100105153
弁理士　朝倉　悟
(74)代理人　100152205
弁理士　吉田　昌司

最終頁に続く

(54)【発明の名称】深層学習自動学習システム、クライアント装置およびサーバ装置

(57)【要約】
【課題】クライアント装置とサーバ装置間の通信を深層学習が完了するまで保持する必要がなく、最新の学習結果をサーバ装置からクライアント装置にインターネットを通じてセキュアに提供する。
【解決手段】実施形態による深層学習自動学習システム１は、インターネットを介して接続されたクライアント装置１００とサーバ装置２００を備え、サーバ装置２００は、バージョン管理情報を暗号化した暗号化学習バージョンデータをクライアント装置１００にプッシュ通知するプッシュ通知部２１４を有し、クライアント装置１００は、暗号化学習バージョンデータを復号化してバージョン管理情報を取得するバージョン管理情報取得部１１３と、バージョン管理情報に対応する学習結果データを既に取得しているか否かを判定し、取得していない場合はサーバ装置２００に対して学習結果データの送信を要求するデータ要求部１１４と、を有する。
【選択図】図１



【特許請求の範囲】
【請求項１】
インターネットを介して接続されたクライアント装置およびサーバ装置を備える深層学習自動学習システムであって、
前記クライアント装置は、
前記クライアント装置の識別情報に基づいて公開鍵および秘密鍵を生成する鍵生成部と、
前記サーバ装置に新規学習データを送信する新規学習データ送信部と、を有し、
前記サーバ装置は、
前記公開鍵を用いて、前記新規学習データに基づく学習結果データを暗号化して、暗号化学習結果データを生成する学習結果データ暗号化部と、
前記公開鍵を用いて、前記学習結果データを識別するためのバージョン管理情報を暗号化して、暗号化学習バージョンデータを生成するバージョン管理情報暗号化部と、
前記クライアント装置に前記暗号化学習バージョンデータをプッシュ通知するプッシュ通知部と、を有し、
前記クライアント装置は、
前記サーバ装置からプッシュ通知された前記暗号化学習バージョンデータを、前記秘密鍵を用いて復号化して、前記バージョン管理情報を取得するバージョン管理情報取得部と、
前記バージョン管理情報に対応する学習結果データを既に取得しているか否かを判定し、取得していない場合は前記サーバ装置に対して前記学習結果データの送信を要求するデータ要求部と、
前記データ要求部の要求に応じて前記サーバ装置から前記クライアント装置に送信された前記暗号化学習結果データを、前記秘密鍵を用いて復号化して、前記学習結果データを取得する学習結果データ取得部と、をさらに有することを特徴とする深層学習自動学習システム。
【請求項２】
前記サーバ装置は、前記クライアント装置の前記識別情報に基づいて登録ＩＤを発行する登録ＩＤ発行部をさらに有し、
前記プッシュ通知部は、前記登録ＩＤを用いて、前記クライアント装置に前記暗号化学習バージョンデータをプッシュ通知することを特徴とする請求項１に記載の深層学習自動学習システム。
【請求項３】
前記学習結果データ暗号化部は、前記学習結果データおよび前記登録ＩＤを暗号化して前記暗号化学習結果データを生成し、
前記バージョン管理情報暗号化部は、前記バージョン管理情報および前記登録ＩＤを暗号化して前記暗号化学習バージョンデータを生成することを特徴とする請求項２に記載の深層学習自動学習システム。
【請求項４】
前記クライアント装置は、前記暗号化学習バージョンデータを復号化して得られた登録ＩＤと、前記暗号化学習結果データを復号化して得られた登録ＩＤとが一致する場合に、前記学習結果データを用いて構造適応型深層学習法による推論を行う推論部をさらに有することを特徴とする請求項３に記載の深層学習自動学習システム。
【請求項５】
前記サーバ装置は、
前記クライアント装置から受信した前記新規学習データを学習データＤＢに保存する新規学習データ保存部と、
前記学習データＤＢの学習データが所定の基準を満たす場合に、前記学習データを学習用計算機に送信する学習データ送信部と、をさらに有することを特徴とする請求項１～４のいずれかに記載の深層学習自動学習システム。

【請求項６】
前記所定の基準は、一定量のデータが溜まった場合、または、前記新規学習データと既存学習データとの誤差が閾値を超えた場合であることを特徴とする請求項５に記載の深層学習自動学習システム。
【請求項７】
前記学習用計算機は、前記学習データを用いて構造適応型深層学習法により学習を行う深層学習実行部を有することを特徴とする請求項５または６に記載の深層学習自動学習システム。
【請求項８】
前記クライアント装置は、
前記学習結果データが取得された後、前記サーバ装置に対して前記暗号化学習結果データを消去するよう要求するデータ消去要求部をさらに備えることを特徴とする請求項１～７のいずれかに記載の深層学習自動学習システム。
【請求項９】
前記クライアント装置は、
前記学習結果データを用いて行われた推論の結果を出力する出力部と、
をさらに備えることを特徴とする請求項１～８のいずれかに記載の深層学習自動学習システム。
【請求項１０】
前記サーバ装置は、
前記クライアント装置から前記学習結果データの送信要求を受信すると、前記暗号化学習結果データを前記クライアント装置に送信する学習結果データ送信部をさらに備えることを特徴とする請求項１～９のいずれかに記載の深層学習自動学習システム。
【請求項１１】
前記サーバ装置は、
前記クライアント装置から前記暗号化学習結果データの消去リクエストを受信すると、前記暗号化学習結果データを消去するデータ消去部をさらに備えることを特徴とする請求項１～１０のいずれかに記載の深層学習自動学習システム。
【請求項１２】
インターネットを介してサーバ装置に接続されたクライアント装置であって、
前記クライアント装置の識別情報に基づいて公開鍵および秘密鍵を生成する鍵生成部と、
前記サーバ装置に新規学習データを送信する新規学習データ送信部と、
前記サーバ装置からプッシュ通知された暗号化学習バージョンデータを、前記秘密鍵を用いて復号化して、学習結果データを識別するためのバージョン管理情報を取得するバージョン管理情報取得部と、
前記バージョン管理情報に対応する学習結果データを既に取得しているか否かを判定し、取得していない場合は前記サーバ装置に対して前記学習結果データの送信を要求するデータ要求部と、
前記データ要求部の要求に応じて前記サーバ装置から前記クライアント装置に送信された暗号化学習結果データを、前記秘密鍵を用いて復号化して、前記学習結果データを取得する学習結果データ取得部と、
を備えることを特徴とするクライアント装置。
【請求項１３】
インターネットを介してクライアント装置に接続されたサーバ装置であって、
前記クライアント装置から受信した公開鍵を用いて、学習結果データを暗号化して暗号化学習結果データを生成する学習結果データ暗号化部と、
前記公開鍵を用いて、前記学習結果データを識別するためのバージョン管理情報を暗号化して暗号化学習バージョンデータを生成するバージョン管理情報暗号化部と、
前記クライアント装置に前記暗号化学習バージョンデータをプッシュ通知するプッシュ

通知部と、
を備えることを特徴とするサーバ装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、深層学習自動学習システム、クライアント装置およびサーバ装置に関し、より詳しくは、クライアント装置からサーバ装置に送信された学習データに基づいて深層学習を行い、最新の学習結果をサーバ装置からクライアント装置にインターネットを通じてセキュアに提供する深層学習自動学習システム、ならびに、当該深層学習自動学習システムが備えるクライアント装置およびサーバ装置に関する。
【背景技術】
【０００２】
センサー等の外部装置から得られた学習データを用いて深層学習を行うシステムが活発に研究されている。深層学習は、多層構造のニューラルネットワークを用いた機械学習の一種である。深層学習の一手法として、構造適応型深層学習法が知られている（非特許文献１参照）。この構造適応型深層学習法は、ＤＢＮ（Ｄｅｅｐ　Ｂｒｉｅｆ　Ｎｅｔｗｏｒｋ）において、最適な隠れニューロン数および層の数を学習中に自動で求めるための手法である。
【０００３】
なお、特許文献１には、クライアントコンピュータが生成した診断データをベンダーコンピュータシステムにより解析して推奨データを生成し、クライアントに対し推奨データを伝達する方法が記載されている。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２００４－３４８７３０号公報
【非特許文献】
【０００５】
【非特許文献１】鎌田真、市村匠、原章、“ニューロン生成／消滅アルゴリズムによる構造適応型Ｒｅｓｔｒｉｃｔｅｄ　Ｂｏｌｔｚｍａｎｎ　Ｍａｃｈｉｎｅ”、計測自動制御学会第８回コンピューテーショナル・インテリジェンス研究会、ｐｐ．９０－９６（２０１５）
【発明の概要】
【発明が解決しようとする課題】
【０００６】
深層学習を利用するための情報処理システムとして、インターネットを介して接続されたクライアント装置とサーバ装置を備えるシステムであって、クライアント装置が学習データをサーバ装置に送信し、当該学習データに基づく深層学習が行われた後、サーバ装置が学習結果をクライアント装置に送信するシステムが考えられる。深層学習を実行する学習用計算機の性能にもよるが、一般的に深層学習は比較的長い時間（例えば数時間程度）を要する。
【０００７】
しかしながら、深層学習が終了するまでクライアント装置とサーバ装置間の通信（セッション）を保持することは、セッションがタイムアウトするため困難である。また、セッションのタイムアウト時間を深層学習に要する時間より長くすることは、セキュリティ維持の観点から望ましくない。
【０００８】
そこで、本発明は、クライアント装置とサーバ装置間の通信を深層学習が完了するまで保持する必要がなく、最新の学習結果をサーバ装置からクライアント装置にインターネットを通じてセキュアに提供することができる深層学習自動学習システム、クライアント装

置およびサーバ装置を提供することを目的とする。
【課題を解決するための手段】
【０００９】
本発明に係る深層学習自動学習システムは、
インターネットを介して接続されたクライアント装置およびサーバ装置を備える深層学習自動学習システムであって、
前記クライアント装置は、
前記クライアント装置の識別情報に基づいて公開鍵および秘密鍵を生成する鍵生成部と、
前記サーバ装置に新規学習データを送信する新規学習データ送信部と、を有し、
前記サーバ装置は、
前記公開鍵を用いて、前記新規学習データに基づく学習結果データを暗号化して、暗号化学習結果データを生成する学習結果データ暗号化部と、
前記公開鍵を用いて、前記学習結果データを識別するためのバージョン管理情報を暗号化して、暗号化学習バージョンデータを生成するバージョン管理情報暗号化部と、
前記クライアント装置に前記暗号化学習バージョンデータをプッシュ通知するプッシュ通知部と、を有し、
前記クライアント装置は、
前記サーバ装置からプッシュ通知された前記暗号化学習バージョンデータを、前記秘密鍵を用いて復号化して、前記バージョン管理情報を取得するバージョン管理情報取得部と、
前記バージョン管理情報に対応する学習結果データを既に取得しているか否かを判定し、取得していない場合は前記サーバ装置に対して前記学習結果データの送信を要求するデータ要求部と、
前記データ要求部の要求に応じて前記サーバ装置から前記クライアント装置に送信された前記暗号化学習結果データを、前記秘密鍵を用いて復号化して、前記学習結果データを取得する学習結果データ取得部と、をさらに有することを特徴とする。
【００１０】
本発明に係るクライアント装置は、
インターネットを介してサーバ装置に接続されたクライアント装置であって、
前記クライアント装置の識別情報に基づいて公開鍵および秘密鍵を生成する鍵生成部と、
前記サーバ装置に新規学習データを送信する新規学習データ送信部と、
前記サーバ装置からプッシュ通知された暗号化学習バージョンデータを、前記秘密鍵を用いて復号化して、学習結果データを識別するためのバージョン管理情報を取得するバージョン管理情報取得部と、
前記バージョン管理情報に対応する学習結果データを既に取得しているか否かを判定し、取得していない場合は前記サーバ装置に対して前記学習結果データの送信を要求するデータ要求部と、
前記データ要求部の要求に応じて前記サーバ装置から前記クライアント装置に送信された暗号化学習結果データを、前記秘密鍵を用いて復号化して、前記学習結果データを取得する学習結果データ取得部と、
を備えることを特徴とする。
【００１１】
本発明に係るサーバ装置は、
インターネットを介してクライアント装置に接続されたサーバ装置であって、
前記クライアント装置から受信した公開鍵を用いて、学習結果データを暗号化して暗号化学習結果データを生成する学習結果データ暗号化部と、
前記公開鍵を用いて、前記学習結果データを識別するためのバージョン管理情報を暗号化して暗号化学習バージョンデータを生成するバージョン管理情報暗号化部と、

前記クライアント装置に前記暗号化学習バージョンデータをプッシュ通知するプッシュ通知部と、
を備えることを特徴とする。
【発明の効果】
【００１２】
本発明に係る深層学習自動学習システムでは、サーバ装置は、学習結果データを識別するためのバージョン管理情報を暗号化した暗号化学習バージョンデータをクライアント装置にプッシュ通知することにより深層学習が終了したことを通知し、クライアント装置に新しい学習結果データをダウンロードすることを促す。プッシュ通知を受信したクライアント装置は、バージョン管理情報に対応する学習結果データを既に取得しているか否かを判定し、取得していない場合、サーバ装置に対して学習結果データの送信を要求する。要求を受けたサーバ装置は、学習結果データを暗号化した暗号化学習結果データをクライアント装置に送信する。このようにすることで、クライアント装置は、サーバ装置との通信を深層学習が完了するまで保持することなく、最新の学習結果データを取得することができる。
【００１３】
さらに、本発明に係る深層学習自動学習システムでは、バージョン管理情報および学習結果データは、公開鍵を用いて暗号化されてからクライアント装置に送信されるため、サーバ装置からクライアント装置にデータをセキュアに配信することができる。
【００１４】
よって、本発明によれば、クライアント装置とサーバ装置間の通信を深層学習が完了するまで保持する必要がなく、最新の学習結果をサーバ装置からクライアント装置にインターネットを通じてセキュアに提供することができる。
【図面の簡単な説明】
【００１５】
【図１】実施形態に係る深層学習自動学習システムの概略的な構成図である。
【図２】実施形態に係るクライアント装置の概略的な構成図である。
【図３】実施形態に係るサーバ装置の概略的な構成図である。
【図４】実施形態に係る端末管理用データベースの一例を示す図である。
【図５】実施形態に係る学習用計算機の概略的な構成図である。
【図６】実施形態に係るクライアント装置とサーバ装置間のフローチャートである。
【図７】実施形態に係るサーバ装置と学習用計算機間のフローチャートである。
【図８】実施形態に係るサーバ装置とクライアント装置間のフローチャートである。
【図９】図８に続く、実施形態に係るサーバ装置とクライアント装置間のフローチャートである。
【図１０】図９に続く、実施形態に係るサーバ装置とクライアント装置間のフローチャートである。
【図１１】実施形態に係るプッシュ通知の設定画面の一例である。
【図１２】実施形態に係るプッシュ通知の画面例である。
【発明を実施するための形態】
【００１６】
以下、本発明に係る実施形態について図面を参照しながら説明する。
【００１７】
＜深層学習自動学習システム＞
まず、図１を参照して、本発明の実施形態に係る深層学習自動学習システム１の概略的な構成について説明する。なお、深層学習自動学習システム１の各構成の内部構成・処理等については、図２以降の図面を参照して説明する。
【００１８】
深層学習自動学習システム１は、クライアント装置１００、サーバ装置２００および学習用計算機３００を備える。クライアント装置１００とサーバ装置２００は、インターネ

ットを介して接続されている。なお、図１では１台のクライアント装置１００のみがサーバ装置２００に接続されているが、複数のクライアント装置１００がサーバ装置２００に接続されてもよい。

【００１９】

クライアント装置１００は、各種センサー等を有するＩＯＴ機器等の外部装置から新規学習データを入力する。ここで、新規学習データとは、深層学習に用いるためのデータであり、深層学習にまだ用いられていないデータである。なお、クライアント装置１００は、具体的には、パソコン、タブレット端末、組み込みボード等である。

【００２０】

クライアント装置１００は、当該クライアント装置１００を識別するための識別情報を有する。この識別情報は、例えば、クライアント装置１００のＭＡＣアドレスやシリアル番号等の端末固有番号である。

【００２１】

サーバ装置２００は、Ｗｅｂデータサーバまたはクラウドサーバとも呼ばれ、図１に示すように、ＰＵＳＨサーバおよびデータサーバを有する。このサーバ装置２００は、学習用計算機３００に通信可能に接続されており、学習用計算機３００に学習データを送信し、学習用計算機３００から学習結果データを受信する。ここで、学習結果データとは、深層学習により得られたデータであって、クライアント装置でニューラルネットワークを再構成するために必要となるデータである。学習結果データは、具体的には、ニューラルネットワークの形状、重み、その他のパラメータ値である。なお、学習結果データは、深層学習により蓄積された知識（ＩＦ－ＴＨＥＮルールなど）を含んでもよい。

【００２２】

学習用計算機３００は、サーバ装置２００から受信した学習データを用いて学習を行う。この学習用計算機３００は、例えば、既述の構造適応型深層学習法により深層学習を行う。なお、学習用計算機３００は、ＧＰＵ（Ｇｒａｐｈｉｃｓ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔｓ）計算機と呼ばれることもある。

【００２３】

深層学習自動学習システム１では、後ほど詳しく説明するように、クライアント装置１００からサーバ装置２００に新規学習データがアップロードされ、サーバ装置２００からクライアント装置１００に学習結果データがダウンロードされる。

【００２４】

なお、本発明に係る深層学習自動学習システムは、図１に示す構成に限られない。例えば、サーバ装置２００のＰＵＳＨサーバとデータサーバは、通信装置を介して接続された別個のサーバ装置として構成されてもよい。また、サーバ装置２００は、学習用計算機３００を含むように構成されてもよい。すなわち、サーバ装置２００と学習用計算機３００は一つの情報処理装置として構成されてもよい。

【００２５】

次に、クライアント装置１００、サーバ装置２００および学習用計算機３００の各々について、さらに詳しく説明する。まず、クライアント装置１００の詳細について説明する。

【００２６】

＜クライアント装置＞

図２に示すように、クライアント装置１００は、制御部１１０と、記憶部１２０と、通信部１３０とを有している。

【００２７】

制御部１１０は、クライアント装置１００内のプロセッサが所定のプログラムを実行することにより実現される。この制御部１１０は、鍵生成部１１１と、新規学習データ送信部１１２と、バージョン管理情報取得部１１３と、データ要求部１１４と、学習結果データ取得部１１５と、データ消去要求部１１６と、推論部１１７と、出力部１１８とを有している。各部の詳細については後ほど説明する。

【００２８】
記憶部１２０は、新規学習データＤＢ１２１を有する。新規学習データＤＢ１２１は、ＩＯＴ機器等の外部装置から入力された新規学習データを記憶する。なお、記憶部１２０は、例えばハードディスク、半導体メモリ（ＳＳＤ等）から構成される。
【００２９】
通信部１３０は、クライアント装置１００がインターネットを介してサーバ装置２００との間で情報を送受信するためのインターフェースである。
【００３０】
ここで、制御部１１０の各部の詳細について説明する。
【００３１】
鍵生成部１１１は、クライアント装置１００の識別情報に基づいて公開鍵および秘密鍵を生成する。公開鍵はデータを暗号化する際に用いるキーであり、秘密鍵はデータを復号化する際に用いるキーである。なお、鍵の生成方法は特に限定されず、公知の鍵生成手法を用いることが可能である。
【００３２】
新規学習データ送信部１１２は、新規学習データＤＢ１２１に保存された新規学習データをサーバ装置２００に送信する。なお、本実施形態では、新規学習データは、ｈｔｔｐｓを用いてサーバ装置２００にセキュアに送信される。
【００３３】
バージョン管理情報取得部１１３は、サーバ装置２００からプッシュ通知された暗号化学習バージョンデータを、鍵生成部１１１により生成された秘密鍵を用いて復号化して、バージョン管理情報を取得する。ここで、バージョン管理情報は、学習結果データを識別するための情報である。また、暗号化学習バージョンデータは、少なくともバージョン管理情報を公開鍵で暗号化して得られるデータのことである。なお、本実施形態では、暗号化学習バージョンデータは、バージョン管理情報と登録ＩＤ（Ｒｅｇｉｓｔｒａｔｉｏｎ　ＩＤ）を公開鍵で暗号化して得られるデータである。
【００３４】
データ要求部１１４は、バージョン管理情報に対応する学習結果データを既に取得しているか否かを判定し、取得していない場合はサーバ装置２００に対して学習結果データの送信を要求する。なお、データ要求部１１４は、学習結果データの送信を要求する際、バージョン管理情報のバージョンをサーバ装置２００に送信してもよい。これにより、サーバ装置２００は、クライアント装置１００に送信すべき学習結果データを把握することができる。
【００３５】
学習結果データ取得部１１５は、データ要求部１１４の要求に応じてサーバ装置２００からクライアント装置１００に送信された暗号化学習結果データを、鍵生成部１１１により生成された秘密鍵を用いて復号化して学習結果データを取得する。なお、学習結果データは、深層学習に用いた学習データを含んでいてもよい。すなわち、学習結果データ取得部１１５は、学習結果データとして、学習データセットを取得してもよい。ここで、「学習データセット」とは、深層学習に用いた学習データと、学習結果データとの組合せ（データセット）のことである。
【００３６】
暗号化学習結果データは、少なくとも学習結果データを公開鍵で暗号化して得られるデータである。なお、本実施形態では、暗号化学習結果データは、学習結果データと登録ＩＤを公開鍵で暗号化して得られるデータである。
【００３７】
データ消去要求部１１６は、学習結果データ取得部１１５により学習結果データが取得された後、サーバ装置２００に対して、サーバ装置２００が有する暗号化学習結果データを消去するよう要求する。これにより、クライアント装置１００にダウンロード済みの暗号化学習結果データがサーバ装置２００から消去され、サーバ装置２００のメモリを節約

することができる。
【００３８】
推論部１１７は、学習結果データ取得部１１５により取得された学習結果データを用いて推論を行う。本実施形態では、構造適応型深層学習法による推論を行う。
【００３９】
なお、推論部１１７は、暗号化学習バージョンデータを復号化して得られた登録ＩＤと、暗号化学習結果データを復号化して得られた登録ＩＤとが一致する場合に、学習結果データを用いて構造適応型深層学習法による推論を行うことが好ましい。これにより、意図しない別バージョンの学習結果データを用いて推論を行うという事態を防止できる。
【００４０】
出力部１１８は、推論部１１７により行われた推論の結果を出力する。推論結果の出力先は、クライアント装置１００のディスプレイ、プリンタ（図示せず）、記憶部１２０、あるいはクライアント装置１００に接続された他の装置等である。
【００４１】
＜サーバ装置＞
次に、サーバ装置２００の詳細について説明する。
【００４２】
図３に示すように、サーバ装置２００は、制御部２１０と、記憶部２２０と、通信部２３０とを有している。
【００４３】
制御部２１０は、サーバ装置２００内のプロセッサが所定のプログラムを実行することにより実現される。この制御部２１０は、登録ＩＤ発行部２１１と、学習結果データ暗号化部２１２と、バージョン管理情報暗号化部２１３と、プッシュ通知部２１４と、新規学習データ保存部２１５と、学習データ送信部２１６と、学習結果データ送信部２１７と、データ消去部２１８とを有している。各部の詳細については後ほど説明する。
【００４４】
なお、本実施形態では、登録ＩＤ発行部２１１、バージョン管理情報暗号化部２１３およびプッシュ通知部２１４はＰＵＳＨサーバに設けられており、学習結果データ暗号化部２１２、新規学習データ保存部２１５、学習データ送信部２１６、学習結果データ送信部２１７およびデータ消去部２１８はデータサーバに設けられている。
【００４５】
記憶部２２０は、端末管理用ＤＢ２２１と、学習データＤＢ２２２と、学習結果ＤＢ２２３とを有する。この記憶部２２０は、例えばハードディスク、半導体メモリ（ＳＳＤ等）から構成される。
【００４６】
端末管理用ＤＢ２２１は、図４に示すように、クライアント装置１００から受信した端末固有番号（より一般的には識別情報）と公開鍵を関連付けて記憶するデータベースである。なお、端末管理用ＤＢ２２１は、図４に示すように、端末固有番号および公開鍵と関連付けて登録ＩＤを記憶してもよい。
【００４７】
学習データＤＢ２２２は、クライアント装置１００から受信した新規学習データが蓄積されるデータベースである。この学習データＤＢ２２２には、既存学習データおよび新規学習データの両方が保存される。ここで、既存学習データは、学習用計算機３００で既に深層学習に用いられたデータである。
【００４８】
学習結果ＤＢ２２３は、学習用計算機３００から受信した学習結果データが蓄積されるデータベースである。
【００４９】
通信部２３０は、サーバ装置２００がインターネットを介してクライアント装置１００との間で情報を送受信し、また、学習用計算機３００との間で情報を送受信するためのイ

ンターフェースである。
【００５０】
ここで、制御部２１０の各部の詳細について説明する。
【００５１】
登録ＩＤ発行部２１１は、クライアント装置１００の識別情報に基づいて登録ＩＤ（Ｒｅｇｉｓｔｒａｔｉｏｎ　ＩＤ）を発行する。登録ＩＤは、プッシュ通知部２１４がクライアント装置１００に対してプッシュ通知を行うために必要な情報であり、クライアント装置１００に固有のＩＤである。登録ＩＤには、クライアント装置１００とサーバ装置２００間の通信経路に関する情報等が含まれる。
【００５２】
なお、クライアント装置１００とサーバ装置２００間の通信のセキュリティを確保する観点から、登録ＩＤ発行部２１１は、必要なときにのみ登録ＩＤを発行し、不要になれば登録ＩＤを削除することが好ましい。また、登録ＩＤ発行部２１１は、一定の期間ごとに登録ＩＤを再発行（リフレッシュ）するようにしてもよい。
【００５３】
学習結果データ暗号化部２１２は、クライアント装置１００から受信した公開鍵を用いて、新規学習データに基づく学習結果データを暗号化して、暗号化学習結果データを生成する。本実施形態では、学習結果データ暗号化部２１２は、学習用計算機３００から受信した学習結果データと、登録ＩＤ発行部２１１により発行された登録ＩＤとを暗号化することにより、暗号化学習結果データを生成する。
【００５４】
なお、学習結果データ暗号化部２１２は、学習データセットを暗号化することにより暗号化学習結果データを生成してもよい。
【００５５】
バージョン管理情報暗号化部２１３は、クライアント装置１００から受信した公開鍵を用いて、学習用計算機３００から受信した学習結果データのバージョン管理情報を暗号化して、暗号化学習バージョンデータを生成する。本実施形態では、バージョン管理情報暗号化部２１３は、バージョン管理情報および登録ＩＤを暗号化して暗号化学習バージョンデータを生成する。
【００５６】
プッシュ通知部２１４は、クライアント装置１００に暗号化学習バージョンデータをプッシュ通知する。本実施形態では、プッシュ通知部２１４によるプッシュ通知は登録ＩＤを用いて行われる。なお、登録ＩＤ以外のデバイストークンを用いてプッシュ通知を行ってもよい。
【００５７】
新規学習データ保存部２１５は、クライアント装置１００から受信した新規学習データを学習データＤＢ２２２に保存する。
【００５８】
学習データ送信部２１６は、学習データＤＢ２２２の学習データが所定の基準を満たす場合に、学習データを学習用計算機３００に送信する。本実施形態では、学習データＤＢ２２２に蓄積された学習データのうち新規増加分のみが学習用計算機３００に送信される。すなわち、学習用計算機３００の学習データＤＢ３２１に保存されている学習データと、学習データＤＢ２２２に保存されている学習データとの差分が学習用計算機３００に送信される。なお、これに限らず、学習データ送信部２１６は、学習データＤＢ２２２に保存された新規学習データおよび既存学習データの両方を学習用計算機３００に送信するようにしてもよい。
【００５９】
「所定の基準が満たす場合」とは、例えば、学習データＤＢ２２２に所定量の新規学習データが蓄積された場合、および／または、新規学習データと既存学習データとの誤差が閾値を超えた場合である。「誤差が閾値を超えた場合」とは、例えば、既存学習データの

統計量と新規学習データの統計量との差が所定値よりも大きくなった場合、あるいは、既存学習データの統計量と全データ（既存学習データと新規学習データ）の統計量との差が所定値よりも大きくなった場合である。統計量としては例えば平均値が用いられるが、それ以外の統計量であってもよい。

【００６０】

学習結果データ送信部２１７は、クライアント装置１００から学習結果データの送信要求（送信リクエスト）を受信すると、学習結果データ暗号化部２１２により生成された暗号化学習結果データをクライアント装置１００に送信する。

【００６１】

データ消去部２１８は、サーバ装置２００が有する暗号化学習結果データを消去するようクライアント装置１００から要求されると（すなわち、消去リクエストを受信すると）、暗号化学習結果データを消去する。

【００６２】

＜学習用計算機＞

次に、学習用計算機３００の詳細について説明する。

【００６３】

学習用計算機３００は、図５に示すように、制御部３１０と、記憶部３２０と、通信部３３０とを有している。

【００６４】

制御部３１０は、学習用計算機３００内のプロセッサが所定のプログラムを実行することにより実現される。この制御部３１０は、深層学習実行部３１１を有する。

【００６５】

深層学習実行部３１１は、学習データＤＢ３２１に蓄積された学習データを用いて深層学習を行う。この深層学習実行部３１１は、例えば構造適応型深層学習法により深層学習を行う。

【００６６】

記憶部３２０は、学習データＤＢ３２１と、学習結果ＤＢ３２２とを有する。学習データＤＢ３２１は、サーバ装置２００から受信した学習データ（既存学習データおよび新規学習データ）が蓄積されるデータベースである。学習結果ＤＢ３２２は、深層学習実行部３１１の出力（学習結果データ）が蓄積されるデータベースである。すなわち、学習結果ＤＢ３２２には、学習により得られたニューラルネットワークの形状、重み、その他のパラメータ値の他、深層学習により蓄積された知識（ＩＦ－ＴＨＥＮルールなど）が蓄積される。

【００６７】

なお、記憶部３２０は、例えばハードディスク、半導体メモリ（ＳＳＤ等）から構成される。

【００６８】

通信部３３０は、学習用計算機３００がサーバ装置２００との間で情報を送受信するためのインターフェースである。

【００６９】

＜深層学習自動学習システムの動作＞

次に、図６～図１２を参照して、上記の構成を有する深層学習自動学習システム１の処理動作の一例について説明する。

【００７０】

まず、図６を参照して、公開鍵のサーバ装置への登録、および新規学習データのサーバ装置へのアップロード等の工程について説明する。

【００７１】

クライアント装置１００の鍵生成部１１１は、自身の（すなわち、クライアント装置１００の）端末固有番号に基づいて、公開鍵および秘密鍵を生成する（ステップＳ１１）。本ステップは、例えば、図１１に示す画面でトグルボタンを操作し、「プッシュ通知有効

化」をオンにすると実行される。なお、プッシュ通知の有効化処理が完了すると、登録ＩＤの情報が登録情報ウィンドウＷに表示される。

【００７２】

公開鍵および秘密鍵が生成された後、クライアント装置１００は、プッシュ通知に必要な登録ＩＤをサーバ装置２００に発行してもらうために、通信部１３０を介して、端末固有番号および公開鍵をサーバ装置２００（ＰＵＳＨサーバ）に送信する（ステップＳ１２）。

【００７３】

サーバ装置２００は、クライアント装置１００から端末固有番号および公開鍵を受信すると、端末管理用ＤＢ２２１に端末固有番号および公開鍵を関連付けて保存する（ステップＳ２１）。その後、登録ＩＤ発行部２１１は、端末固有番号に基づいて登録ＩＤを発行し、発行された登録ＩＤを端末管理用ＤＢ２２１に端末固有番号と関連付けて保存する（ステップＳ２２）。

【００７４】

クライアント装置１００の新規学習データ送信部１１２は、外部装置から入力し、新規学習データＤＢ１２１に保存された新規学習データをサーバ装置２００（データサーバ）にアップロードする（ステップＳ１３）。本ステップは、例えば、サーバ装置２００から登録ＩＤが発行されたこと（すなわち、プッシュ通知の有効化処理が完了したこと）が通知された後に行われる。

【００７５】

サーバ装置２００の新規学習データ保存部２１５は、クライアント装置１００から新規学習データを受信すると、受信した新規学習データを学習データＤＢ２２２に保存する（ステップＳ２３）。

【００７６】

次に、図７を参照して、学習データの蓄積および自動学習等の工程について説明する。

【００７７】

サーバ装置２００の学習データ送信部２１６は、学習データＤＢ２２２に蓄積された学習データが所定の基準を満たすか否かを判定する（ステップＳ３１）。そして、学習データが所定の基準を満たす場合に（Ｓ３１：Ｙｅｓ）、学習データ送信部２１６は、新規増加分の学習データを学習用計算機３００に送信する（ステップＳ３２）。学習用計算機３００は、サーバ装置２００から学習データを受信すると、受信した学習データを学習データＤＢ３２１に保存する。

【００７８】

学習用計算機３００は、学習データＤＢ３２１に蓄積された学習データが所定の基準を満たすか否かを判定する（ステップＳ４１）。本ステップで用いる基準は、例えば、学習データＤＢ３２１に蓄積された学習データの数が予め定められた数に達した場合である。なお、本ステップにおける基準は、ステップＳ３１における基準と同じ基準であってもよいし、異なる基準であってもよい。

【００７９】

学習データＤＢ３２１の学習データが所定の基準を満たす場合（Ｓ４１：Ｙｅｓ）、深層学習実行部３１１は、学習データＤＢ３２１に蓄積された学習データを用いて深層学習を行う（ステップＳ４２）。本ステップでは、例えば構造適応型深層学習法による深層学習が行われる。

【００８０】

深層学習実行部３１１は、学習終了後、学習結果ＤＢ３２２に学習結果データを保存する（ステップＳ４３）。その後、学習用計算機３００は、ステップＳ４２で得られた学習結果データをサーバ装置２００に送信する（ステップＳ４４）。

【００８１】

サーバ装置２００は、学習用計算機３００から学習結果データを受信すると、学習用計算機３００から受信した学習結果データを学習結果ＤＢ２２３にバージョン管理情報とと

もに保存する（ステップＳ３３）。なお、学習結果データは学習データを含んでもよい。本実施形態では、サーバ装置２００は、学習データセットをバージョン管理情報とともに学習結果ＤＢ２２３に保存する。

【００８２】

次に、図８を参照して、暗号化データの生成およびプッシュ通知等の工程について説明する。

【００８３】

学習結果データが学習結果ＤＢ２２３に保存されると、サーバ装置２００の学習結果データ暗号化部２１２は、クライアント装置１００から受信した公開鍵を用いて、登録ＩＤと学習データセットを暗号化して、暗号化学習結果データを生成する（ステップＳ５１）。

【００８４】

サーバ装置２００のバージョン管理情報暗号化部２１３は、クライアント装置１００から受信した公開鍵を用いて、登録ＩＤおよびバージョン管理情報を暗号化して、暗号化学習バージョンデータを生成する（ステップＳ５２）。

【００８５】

サーバ装置２００のプッシュ通知部２１４は、ステップＳ５２で生成された暗号化学習バージョンデータをクライアント装置１００にプッシュ通知する（ステップＳ５３）。プッシュ通知は、ステップＳ２２で発行された登録ＩＤを用いて行われる。より詳しくは、ステップＳ２２で発行された登録ＩＤに対応するクライアント装置１００に対してプッシュ通知が行われる。

【００８６】

クライアント装置１００のバージョン管理情報取得部１１３は、ステップＳ１１で生成された秘密鍵を用いて、サーバ装置２００からプッシュ通知された暗号化学習バージョンデータを復号化して、登録ＩＤおよびバージョン管理情報を取得する（ステップＳ６１）。このようにして取得されたバージョン管理情報は、学習データセットのバージョンを示す。図１２は、プッシュ通知されたクライアント装置１００の画面例を示している。この例では、学習データセットがサーバ装置２００において更新されたことを示すとともに、更新された学習データセットのバージョンも示している。

【００８７】

続いて、図９を参照して、学習結果データの送信リクエストおよびダウンロード等の工程について説明する。

【００８８】

クライアント装置１００のデータ要求部１１４は、ステップＳ６１で取得されたバージョン管理情報に対応する学習データセットが取得済みであるか否かを判定する（ステップＳ６２）。そして、バージョン管理情報に対応する学習データセットをまだ取得していない場合（Ｓ６２：Ｙｅｓ）、データ要求部１１４は、サーバ装置２００に対して学習データセットの送信を要求する（ステップＳ６３）。なお、本ステップでは、バージョン管理情報がサーバ装置２００に送信される。

【００８９】

サーバ装置２００の学習結果データ送信部２１７は、クライアント装置１００から送信リクエストを受信すると、クライアント装置１００から受信したバージョン管理情報のバージョンに対応する暗号化学習結果データをクライアント装置１００に送信する（ステップＳ５４）。クライアント装置１００は、サーバ装置２００から暗号化学習結果データをダウンロードする。

【００９０】

暗号化学習結果データのダウンロードが完了すると、クライアント装置１００の学習結果データ取得部１１５は、ステップＳ１１で生成された秘密鍵を用いて暗号化学習結果データを復号化して、登録ＩＤと学習データセットを取得する（ステップＳ６４）。なお、本ステップの完了後、クライアント装置１００のディスプレイに新しい学習データセット

を取得した旨を表示してもよい。例えば、「新しい学習データセットが利用可能になりました。」というメッセージがプッシュ通知されるようにしてもよい。

【００９１】

続いて、図１０を参照して、暗号化データの消去および推論実行等の工程について説明する。

【００９２】

クライアント装置１００により学習データセットが取得されると、データ消去要求部１１６は、サーバ装置２００に対して暗号化学習結果データの消去を要求する（ステップＳ６５）。

【００９３】

クライアント装置１００から消去リクエストを受信すると、サーバ装置２００のデータ消去部２１８は、暗号化学習結果データを消去する（ステップＳ５５）。

【００９４】

その後、クライアント装置１００の推論部１１７は、ステップＳ６１で暗号化学習バージョンデータを復号化して得られた登録ＩＤと、ステップＳ６４で暗号化学習結果データを復号化して得られた登録ＩＤとが一致するか否かを判定する（ステップＳ６６）。

【００９５】

推論部１１７は、２つの登録ＩＤが一致する場合（Ｓ６６：Ｙｅｓ）、ステップＳ６４で取得された学習データセットを用いて推論を行う（ステップＳ６７）。このように登録ＩＤが一致する場合にのみ推論を行うようにすることで、確実に最新バージョンの学習データセットを用いた推論を行うことができる。

【００９６】

推論が完了すると、クライアント装置１００の出力部１１８は、推論部１１７により行われた推論の結果を出力する（ステップＳ６８）。

【００９７】

なお、上記処理フローは一例に過ぎず、他にも様々な処理フローが想定される。例えば、上記処理フローではステップＳ５１において暗号化学習結果データを生成したが、これに限らず、クライアント装置１００から送信リクエストを受信した後に暗号化学習結果データを生成するようにしてもよい。また、上記処理フローでは送信リクエストが自動的に送信されたが、これに限らず、クライアント装置１００のユーザの承認を経た後に送信リクエストがサーバ装置２００に送信されるようにしてもよい。

【００９８】

なお、上記処理フローによる学習結果データのクライアント装置への配信と同様の手法によって、クライアント装置の動作アルゴリズムやセキュリティソフト等のソフトウェア（以下、「ソフトウェア等」という。）が最新のバージョンに自動でアップデートされるようにしてもよい。具体的には、前述の処理フローと同様に、サーバ装置（データサーバ）は、ソフトウェア等が更新された旨をクライアント装置にプッシュ通知し、クライアント装置からの送信リクエストに応じてソフトウェア等のアップデートに必要なデータを暗号化してクライアント装置に送信する。クライアント装置は、サーバ装置から受信した暗号化データをダウンロードし、秘密鍵を用いて復号化することで、ソフトウェア等のアップデートに必要なデータを入手する。このようにすることで、クライアント装置は、ソフトウェア等の自動アップデートをセキュアに行うことができる。

【００９９】

以上説明したように、深層学習自動学習システム１では、サーバ装置２００は、クライアント装置１００に暗号化学習バージョンデータをプッシュ通知することにより、新たな学習結果データ（学習データセット）が得られたことを通知する。プッシュ通知を受信したクライアント装置１００は、バージョン管理情報に対応する学習結果データを既に取得しているか否かを判定し、取得していない場合、サーバ装置２００に送信リクエストを送信する。送信リクエストを受信したサーバ装置２００は、クライアント装置１００に暗号化学習結果データを送信する。このようにすることで、クライアント装置１００は、サー

バ装置２００との通信を深層学習が完了するまで保持することなく、最新の学習結果データを取得することができる。

【０１００】

また、深層学習自動学習システム１では、バージョン管理情報および学習結果データは、公開鍵を用いて暗号化されてからクライアント装置１００に送信されるため、サーバ装置からクライアント装置にデータをセキュアに配信することができる。

【０１０１】

さらに、深層学習自動学習システム１では、サーバ装置２００が暗号化学習バージョンデータおよび暗号化学習結果データを、登録ＩＤが発行されたクライアント装置１００（すなわち、認証されたクライアント装置）にのみ送信することから、最新の学習結果をサーバ装置からクライアント装置にインターネットを通じてさらにセキュアに提供することができる。

【０１０２】

よって、本実施形態によれば、クライアント装置とサーバ装置間の通信を深層学習が完了するまで保持する必要がなく、最新の学習結果をサーバ装置からクライアント装置にインターネットを通じてセキュアに提供することができる。

【０１０３】

また、深層学習自動学習システム１では、サーバ装置は、自身の学習データＤＢ２２２の学習データが所定の基準を満たす場合に学習データを学習用計算機に送信するように構成され、学習用計算機は、自身の学習データＤＢ３２１の学習データが所定の基準を満たす場合に当該学習データに基づいて深層学習を行うように構成されている。このため、本実施形態によれば、新規学習データの蓄積に応じて自動的に深層学習を行うことができる。

【０１０４】

上記の記載に基づいて、当業者であれば、本発明の追加の効果や種々の変形を想到できるかもしれないが、本発明の態様は、上述した実施形態に限定されるものではない。特許請求の範囲に規定された内容及びその均等物から導き出される本発明の概念的な思想と趣旨を逸脱しない範囲で種々の追加、変更及び部分的削除が可能である。

【０１０５】

上述した実施形態で説明した深層学習自動学習システムの少なくとも一部は、ハードウェアで構成してもよいし、ソフトウェアで構成してもよい。ソフトウェアで構成する場合には、深層学習自動学習システムの少なくとも一部の機能を実現するプログラムをフレキシブルディスクやＣＤ－ＲＯＭ等の記録媒体に収納し、コンピュータに読み込ませて実行させてもよい。記録媒体は、磁気ディスクや光ディスク等の着脱可能なものに限定されず、ハードディスク装置やメモリなどの固定型の記録媒体でもよい。

【０１０６】

また、深層学習自動学習システムの少なくとも一部の機能を実現するプログラムを、インターネット等の通信回線（無線通信も含む）を介して頒布してもよい。さらに、同プログラムを暗号化したり、変調をかけたり、圧縮した状態で、インターネット等の有線回線や無線回線を介して、あるいは記録媒体に収納して頒布してもよい。

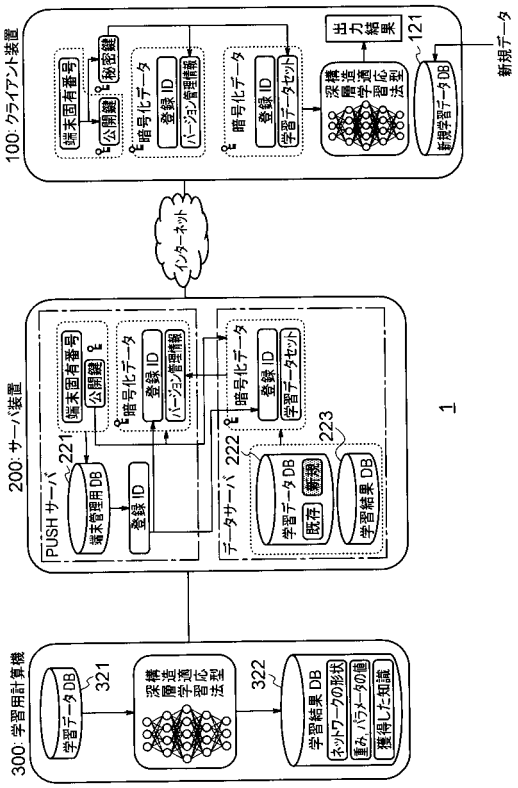
【符号の説明】

【０１０７】

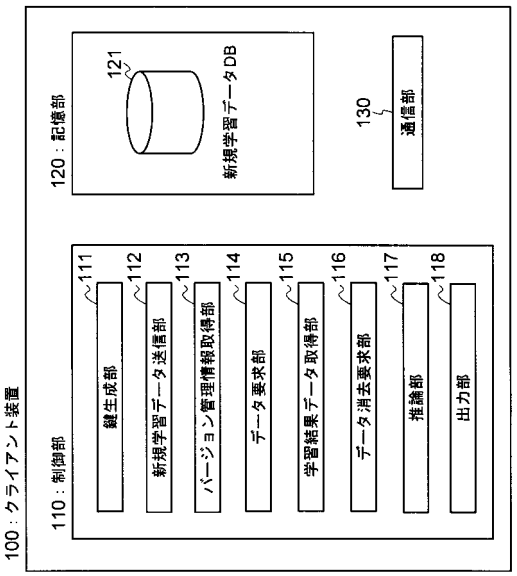
１　深層学習自動学習システム
１００　クライアント装置
１１０　制御部
１１１　鍵生成部
１１２　新規学習データ送信部
１１３　バージョン管理情報取得部
１１４　データ要求部
１１５　学習結果データ取得部

１１６　データ消去要求部
１１７　推論部
１１８　出力部
１２０　記憶部
１２１　新規学習データＤＢ
１３０，２３０，３３０　通信部
２００　サーバ装置
２１０　制御部
２１１　登録ＩＤ発行部
２１２　学習結果データ暗号化部
２１３　バージョン管理情報暗号化部
２１４　プッシュ通知部
２１５　新規学習データ保存部
２１６　学習データ送信部
２１７　学習結果データ送信部
２１８　データ消去部
２２０　記憶部
２２１　端末管理用ＤＢ
２２２　学習データＤＢ
２２３　学習結果ＤＢ
３００　学習用計算機
３１０　制御部
３１１　深層学習実行部
３２０　記憶部
３２１　学習データＤＢ
３２２　学習結果ＤＢ

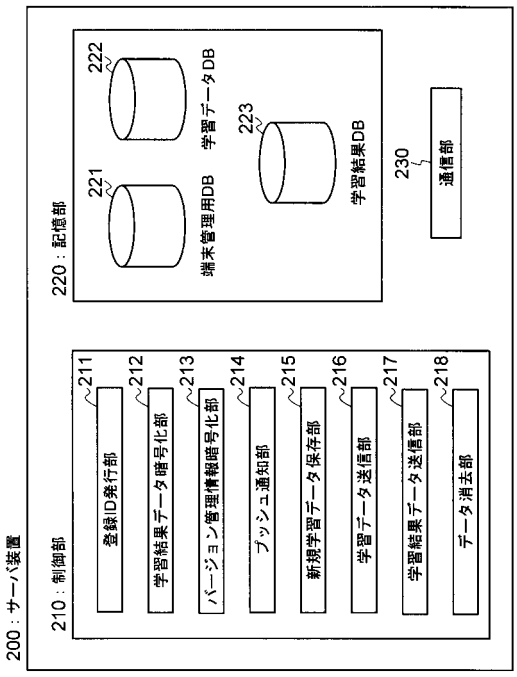
【図１】



【図２】



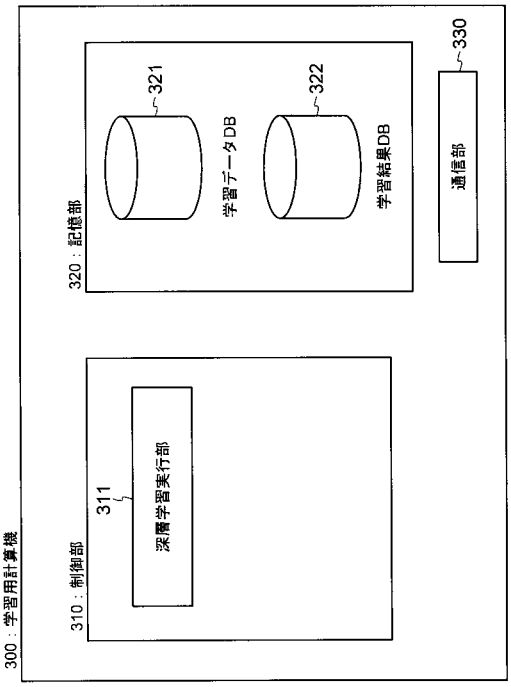
【図３】



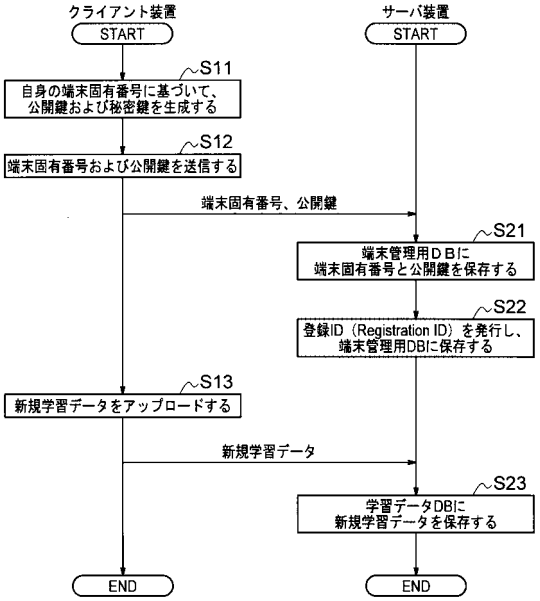
【図４】

No.	端末固有番号	公開鍵	登録ID
1			
2			
3			
：			

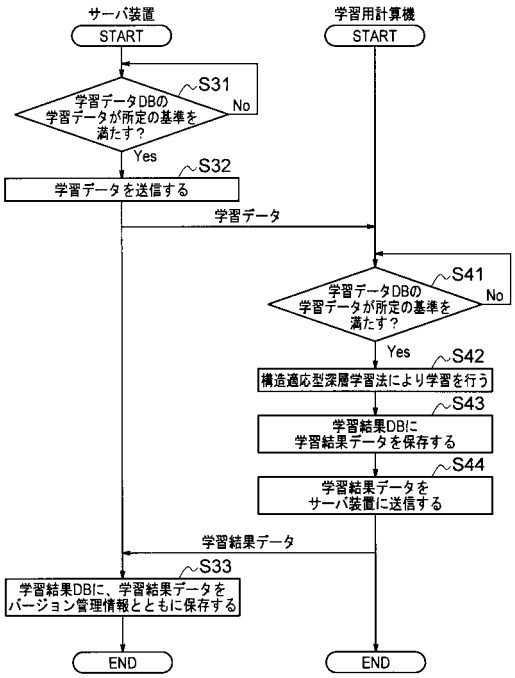
【図５】


300：学習用計算機
310：制御部
311
深層学習実行部
320：記憶部
321
学習データDB
322
学習結果DB
330
通信部

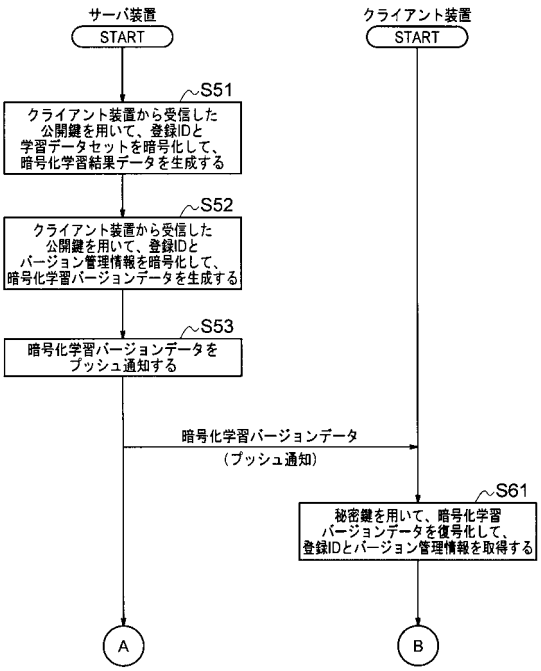
【図６】


クライアント装置
START
サーバ装置
START
S11
自身の端末固有番号に基づいて、公開鍵および秘密鍵を生成する
S12
端末固有番号および公開鍵を送信する
端末固有番号、公開鍵
S21
端末管理用ＤＢに端末固有番号と公開鍵を保存する
S22
登録ID（Registration ID）を発行し、端末管理用DBに保存する
S13
新規学習データをアップロードする
新規学習データ
S23
学習データDBに新規学習データを保存する
END
END

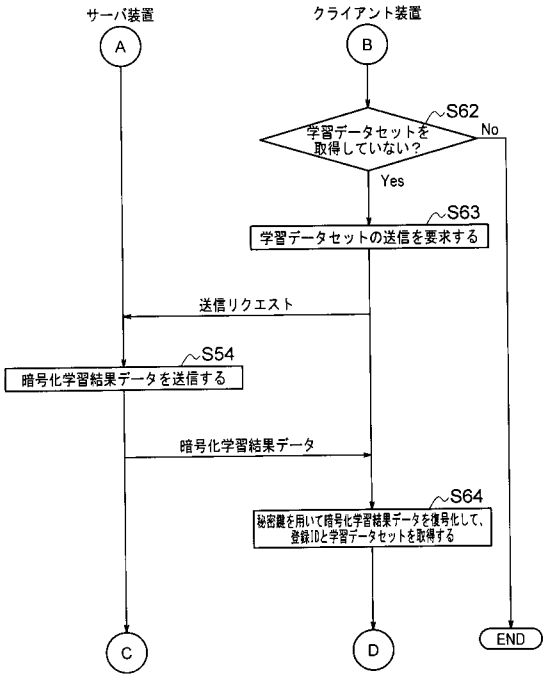
【図７】


サーバ装置
START
学習用計算機
START
S31
学習データDBの学習データが所定の基準を満たす？
No
Yes
S32
学習データを送信する
学習データ
S41
学習データDBの学習データが所定の基準を満たす？
No
Yes
S42
構造適応型深層学習法により学習を行う
S43
学習結果DBに学習結果データを保存する
S44
学習結果データをサーバ装置に送信する
学習結果データ
S33
学習結果DBに、学習結果データをバージョン管理情報とともに保存する
END
END

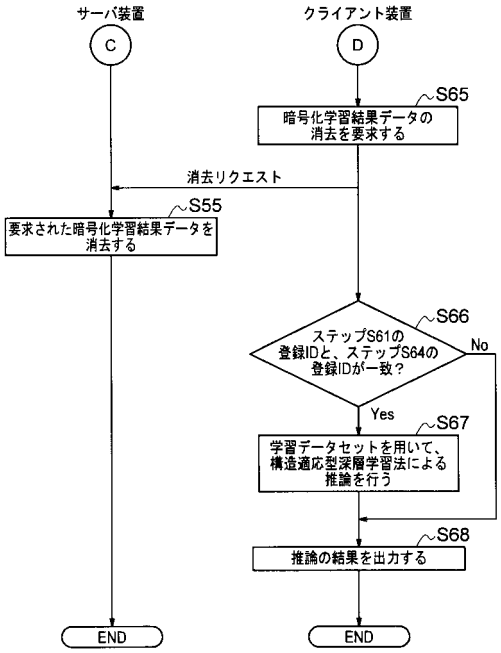
【図８】


サーバ装置
START
クライアント装置
START
S51
クライアント装置から受信した公開鍵を用いて、登録IDと学習データセットを暗号化して、暗号化学習結果データを生成する
S52
クライアント装置から受信した公開鍵を用いて、登録IDとバージョン管理情報を暗号化して、暗号化学習バージョンデータを生成する
S53
暗号化学習バージョンデータをプッシュ通知する
暗号化学習バージョンデータ
（プッシュ通知）
S61
秘密鍵を用いて、暗号化学習バージョンデータを復号化して、登録IDとバージョン管理情報を取得する
A
B

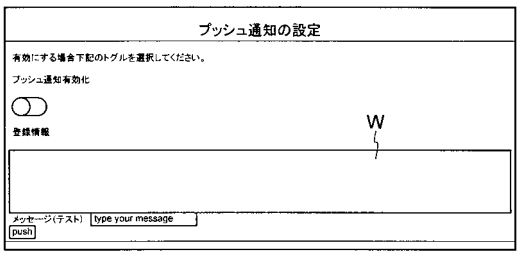
【図９】



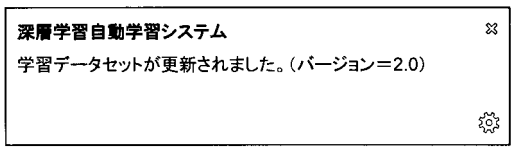
【図１０】



【図１１】



【図１２】



フロントページの続き

(72)発明者　市　村　　匠
広島県広島市南区宇品東一丁目１番７１号　公立大学法人県立広島大学内
(72)発明者　鎌　田　　真
広島県広島市南区宇品東一丁目１番７１号　公立大学法人県立広島大学内