(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7089303号
(P7089303)

(45)発行日　令和4年6月22日(2022.6.22)

(24)登録日　令和4年6月14日(2022.6.14)

(51)国際特許分類

Ｈ０４Ｌ　9/08　(2006.01)	Ｈ０４Ｌ	9/08	Ｂ
Ｇ０６Ｆ　21/60　(2013.01)	Ｇ０６Ｆ	21/60	３２０
Ｇ０６Ｎ　3/02　(2006.01)	Ｇ０６Ｎ	3/02	

ＦＩ

請求項の数　15　（全38頁）

(21)出願番号　特願2020-550013(P2020-550013)
(86)(22)出願日　令和1年8月21日(2019.8.21)
(86)国際出願番号　PCT/JP2019/032598
(87)国際公開番号　WO2020/075396
(87)国際公開日　令和2年4月16日(2020.4.16)
審査請求日　令和3年3月17日(2021.3.17)
(31)優先権主張番号　特願2018-191672(P2018-191672)
(32)優先日　平成30年10月10日(2018.10.10)
(33)優先権主張国・地域又は機関
日本国(JP)

(73)特許権者　398034168
株式会社アクセル
東京都千代田区外神田四丁目１４番１号
(74)代理人　100085660
弁理士　鈴木 均
(72)発明者　客野 一樹
東京都千代田区外神田四丁目１４番１号
株式会社アクセル内
審査官　松平 英

最終頁に続く

(54)【発明の名称】　推論装置、処理システム、推論方法及び推論プログラム

(57)【特許請求の範囲】
【請求項１】
ニューラルネットワークの学習済みモデルの内容を表す情報を出力する出力部と、
前記学習済みモデルが暗号化された暗号化学習済みモデルが入力されたか否かを判定する判定部と、
前記暗号化学習済みモデルが入力されたとき、前記出力部による出力処理を停止する停止部と、
前記暗号化学習済みモデルが入力されたとき、前記暗号化学習済みモデルを復号する復号部と、
復号された前記学習済みモデルを用いて推論をする推論部と、
を備えることを特徴とする推論装置。
【請求項２】
前記推論装置に含まれる機器を識別する第１機器識別子を含む許諾情報の発行要求を、学習済みモデルを生成する学習装置に送信する送信部と、
前記第１機器識別子を含む許諾情報を前記学習装置から取得する取得部と、
を備え、
前記復号部は、
前記暗号化学習済みモデルが入力されたとき、前記第１機器識別子と、前記推論装置に含まれるいずれかの機器を識別する第２機器識別子とが一致する場合、前記暗号化学習済みモデルを復号する

ことを特徴とする請求項１に記載の推論装置。
【請求項３】
前記許諾情報は、さらに、
前記暗号化学習済みモデルを復号する復号鍵を含み、
前記復号部は、
前記復号鍵を用いて前記暗号化学習済みモデルを復号する
ことを特徴とする請求項２に記載の推論装置。
【請求項４】
前記許諾情報は、さらに、
前記暗号化学習済みモデルの有効期限を含み、
前記復号部は、
前記暗号化学習済みモデルを復号するときの時刻が前記有効期限内に含まれるとき、前記暗号化学習済みモデルを復号する
ことを特徴とする請求項２または３に記載の推論装置。
【請求項５】
前記推論装置は、さらに、
前記許諾情報が格納された処理装置と着脱可能に接続される接続部
を備え、
前記取得部は、
前記接続部に前記処理装置が接続されているとき、前記処理装置から許諾情報を取得する
ことを特徴とする請求項２から４のいずれか一つに記載の推論装置。
【請求項６】
前記暗号化学習済みモデルは、
前記学習済みモデルが暗号化されているか否かを識別する暗号化識別子が付与され、
前記判定部は、
前記暗号化識別子を参照することにより、前記暗号化学習済みモデルが入力されたか否かを判定する
ことを特徴とする請求項１から５のいずれか一つに記載の推論装置。
【請求項７】
ニューラルネットワークの学習済みモデルの内容を表す情報を出力する出力部と、
前記学習済みモデルに含まれる１以上の層の第１演算に対応する第１データが暗号化された第１暗号化データが入力されたか否かを判定する判定部と、
前記第１暗号化データが入力されたとき、前記出力部による出力処理を停止する停止部と、
前記学習済みモデルから前記１以上の層を除いた層の第２演算に対応する第２データが記憶され、かつ前記第２データを用いて前記第２演算を実行する処理装置と着脱可能に接続される接続部と、
前記第１暗号化データが入力されたとき、前記第１暗号化データを復号する復号部と、
前記第１データを用いて前記第１演算を実行し、かつ前記処理装置に前記第２演算を実行させることにより推論をする推論部と、
を備えることを特徴とする推論装置。
【請求項８】
前記処理装置は、さらに、
前記第１暗号化データを復号する機能を有し、
前記推論装置は、前記復号部に代えて、
前記第１暗号化データが入力されたとき、前記処理装置に前記第１暗号化データを復号させることにより、前記第１データを取得する取得部
を備えることを特徴とする請求項７に記載の推論装置。
【請求項９】
前記第２演算は、
ニューラルネットワークに含まれる連続する３層以上の演算を含む

ことを特徴とする請求項７または８に記載の推論装置。
【請求項１０】
学習装置と推論装置とを含む処理システムであって、
前記学習装置は、
ニューラルネットワークの学習をする学習部と、
前記学習部により学習された学習済みモデルを符号化する符号化部と、
符号化された前記学習済みモデルを暗号化する暗号化部と、
前記推論装置は、
前記学習済みモデルの内容を表す情報を出力する出力部と、
前記学習済みモデルが暗号化された暗号化学習済みモデルが入力されたか否かを判定する判定部と、
前記暗号化学習済みモデルが入力されたとき、前記出力部による出力処理を停止する停止部と、
前記暗号化学習済みモデルが入力されたとき、前記暗号化学習済みモデルを復号する復号部と、
復号された前記学習済みモデルを用いて推論をする推論部と、
を備えることを特徴とする処理システム。
【請求項１１】
プロセッサにより実行される推論方法であって、
前記プロセッサは、
ニューラルネットワークの学習済みモデルの内容を表す情報を出力し、
前記学習済みモデルが暗号化された暗号化学習済みモデルが入力されたか否かを判定し、
前記暗号化学習済みモデルが入力されたとき、前記情報の出力を停止し、
前記暗号化学習済みモデルが入力されたとき、前記暗号化学習済みモデルを復号し、
復号された前記学習済みモデルを用いて推論をする
ことを特徴とする推論方法。
【請求項１２】
ニューラルネットワークの学習済みモデルの内容を表す情報を出力し、
前記学習済みモデルが暗号化された暗号化学習済みモデルが入力されたか否かを判定し、
前記暗号化学習済みモデルが入力されたとき、前記情報の出力を停止し、
前記暗号化学習済みモデルが入力されたとき、前記暗号化学習済みモデルを復号し、
復号された前記学習済みモデルを用いて推論をする
処理をプロセッサに実行させることを特徴とする推論プログラム。
【請求項１３】
学習装置と保存装置と処理装置と推論装置とを含む処理システムであって、
前記学習装置は、
ニューラルネットワークの学習をする学習部と、
前記処理装置と着脱可能に接続される第１接続部と、
前記学習部により学習された学習済みモデルに含まれる１以上の層の第１演算に対応する第１データを暗号化する暗号化部と、
前記第１データが暗号化された第１暗号化データを前記保存装置に出力する第１出力部と、
前記学習済みモデルから前記１以上の層を除いた層の第２演算に対応する第２データを前記処理装置に書き込む書込部と、
を備え、
前記保存装置は、
前記第１暗号化データを記憶する第１記憶部
を備え、
前記処理装置は、
前記第２データを記憶する第２記憶部と、
前記第２データを用いて前記第２演算を実行する推論部と、

前記学習装置及び前記推論装置と着脱可能に接続される第２接続部と、
を備え、
前記推論装置は、
前記学習済みモデルの内容を表す情報を出力する第２出力部と、
前記保存装置から前記第１暗号化データを取得する取得部と、
前記第１暗号化データが入力されたか否かを判定する判定部と、
前記第１暗号化データが入力されたとき、前記第２出力部による出力処理を停止する停止部と、
前記処理装置と着脱可能に接続される第３接続部と、
前記第１暗号化データが入力されたとき、前記第１暗号化データを復号する第１復号部と、
前記第１データを用いて前記第１演算を実行し、かつ前記処理装置に前記第２データを用いて前記第２演算を実行させることにより推論をする推論部と、
を備えることを特徴とする処理システム。
【請求項１４】
前記処理装置は、前記第１復号部に代えて、
前記推論装置から前記第１暗号化データが入力されたとき、前記第１暗号化データを復号する第２復号部と、
前記第２復号部で復号された前記第１データを前記推論装置に出力する第３出力部と、
を備え、
前記推論装置において、
前記取得部は、
前記第１暗号化データが入力されたとき、前記処理装置に前記第１暗号化データを復号させることにより、復号された前記第１データを取得する
ことを特徴とする請求項１３に記載の処理システム。
【請求項１５】
前記第２演算は、
ニューラルネットワークに含まれる連続する３層以上の演算を含む
ことを特徴とする請求項１３または１４のいずれか一つに記載の処理システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、推論装置、推論方法及び推論プログラムに関する。
【背景技術】
【０００２】
画像認識、音声認識、及び文字認識などのアプリケーションにおいて、入力層、中間層、及び出力層を含むニューラルネットワーク（Ｎｅｕｒａｌ　Ｎｅｔｗｏｒｋ：ＮＮ）を用いた推論処理が用いられている。なお、ニューラルネットワークは、入力層、中間層、及び出力層の各層に演算機能を有する複数のユニット（ニューロン）を含む。また、ニューラルネットワークの各層に含まれるユニットは、それぞれが隣り合う層に含まれるユニットと重み付きのエッジで結合されている。
【０００３】
ニューラルネットワークを用いた推論処理では、中間層を多層にしたニューラルネットワークを用いることにより、推論の制度を向上する技術が知られている。なお、中間層を多層にしたニューラルネットワークを用いた機械学習は、ディープラーニングと呼ばれている。以下の説明では、中間層を多層にしたニューラルネットワークのことを、単にニューラルネットワークともいう。
【０００４】
ディープラーニングでは、ニューラルネットワークが多数のユニットとエッジとを含み演算の規模が大きくなるため、高性能の情報処理装置が必要とされる。また、ディープラーニングは、設定するパラメータの数が多いため、ユーザがパラメータを適宜設定して、情

報処理装置に機械学習を実行させ、推論の精度が高い学習済みモデルを得るのは困難である。学習済みモデルとは、ニューラルネットワークのネットワーク構造、重み、及びバイアスを含む、ネットワーク構造に機械学習済みのパラメータが設定されたニューラルネットワークである。重みとは、ニューラルネットワークに含まれるユニット間のエッジに設定される重み係数のことである。バイアスとは、ユニットの発火の閾値である。また、ニューラルネットワークのネットワーク構造のことを、単にネットワーク構造ともいう。

【０００５】

このため、ニューラルネットワークを用いた推論処理を利用するアプリケーションの開発者が、ディープラーニングを実行することにより得られた学習済みモデルをユーザに配布することが行われている。これにより、ユーザは、所有するエッジ側の端末で学習済みモデルを用いた推論処理を実行することができる。なお、エッジ側の端末とは、例えば、ユーザが所有する携帯電話、及びパソコンなどの情報処理装置のことである。以下の説明では、エッジ側の端末のことを、単にエッジ端末ともいう。

【０００６】

関連する技術として、携帯端末と、携帯端末に接続するサーバを有する、携帯端末を用いた察知エージェントシステムがある。携帯端末は、ユーザから取得する情報に含まれる特徴ベクトルを暗号化し、次いで、暗号化された特徴ベクトルをニューラルネットワークの入力層としてサーバに送信する。サーバは、暗号化された特徴ベクトルを受信して、ニューラルネットワークの入力層から隠れ層を計算し、隠れ層の計算結果を携帯端末に送信する。携帯端末は更に、サーバからの隠れ層の計算結果から出力層の計算を行う技術が知られている。

【０００７】

関連する他の技術として、ユーザから学習データを取得し、サーバ側で機械学習することにより得られた学習済みモデルを、ユーザが所有するエッジ端末に配信することにより、エッジ端末で推論処理を実行可能にする技術がある。エッジ端末に学習済みモデルを配信するとき、学習済みモデルは、暗号化された状態で、かつ暗号化された通信経路を経由してエッジ端末に配信される。さらに、エッジ端末が学習済みモデルを利用できる有効期限を設定することにより、学習済みモデルを保護する技術が知られている（例えば、特許文献１及び非特許文献１）。

【先行技術文献】

【特許文献】

【０００８】

【文献】特開２０１８－４５６７９号公報

【非特許文献】

【０００９】

【文献】FUJITSU Cloud Service for OSS「Zinraiプラットフォームサービス」ご紹介インターネット＜http://jp.fujitsu.com/solutions/cloud/k5/document/pdf/k5-zinrai-platform-function-overview.pdf＞

【発明の概要】

【発明が解決しようとする課題】

【００１０】

開発者側で学習した学習済みモデルは、ネットワーク構造、重み、及びバイアスが開示されると、開発者のノウハウとして保護したい学習方法が第三者に推測されることがある。このため、推論技術の分野では、学習済みモデルの内容を秘密状態のまま、学習済みモデルをユーザに利用させる技術が求められている。

【００１１】

前述した推論技術では、暗号化された学習済みモデルは、復号されたあとにエッジ端末側のフレームワークに読み込まれるので、ユーザ側で閲覧及びコピーすることが可能となり、学習済みモデルに含まれるネットワーク構造及び重みが漏洩することがある。

本発明は、一側面として、学習済みモデルに含まれるネットワーク構造及び重みの漏洩を

防止する技術を提供する。
【課題を解決するための手段】
【００１２】
本明細書で開示する推論装置のひとつに、出力部と、判定部と、停止部と、複合部と、推論部とを備える推論装置がある。出力部は、ニューラルネットワークの学習済みモデルの内容を表す情報を出力する。判定部は、学習済みモデルが暗号化された暗号化学習済みモデルが入力されたか否かを判定する。停止部は、暗号化学習済みモデルが入力されたとき、出力部による出力処理を停止する。複合部は、暗号化学習済みモデルが入力されたとき、暗号化学習済みモデルを復号する。推論部は、復号された学習済みモデルを用いて推論をする。
【発明の効果】
【００１３】
１実施態様によれば、学習済みモデルに含まれるネットワーク構造及び重みの漏洩を防止することができる。
【図面の簡単な説明】
【００１４】
【図１】実施形態１のニューラルネットワークを用いた処理システムの一例を示す図である。
【図２】実施形態１の顧客装置の一実施例を示す機能ブロック図である。
【図３】ライセンス情報の一例を示す図である。
【図４】実施形態１の顧客装置が実行する処理の一実施例を説明する図である。
【図５】実施形態１の開発装置の一実施例を示す機能ブロック図である。
【図６】顧客管理情報の一例を示す図である。
【図７】プロダクト情報の一例を示す図である。
【図８】実施形態１の開発装置の実行する処理の一実施例を説明する図である。
【図９】実施形態１の管理装置の一実施例を示す機能ブロック図である。
【図１０】製品管理情報の一例を示す図である。
【図１１】実施形態１の処理システムにおいて実行される処理の一例を示すシーケンス図（その１）である。
【図１２】実施形態１の処理システムにおいて実行される処理の一例を示すシーケンス図（その２）である。
【図１３】実施形態２のニューラルネットワークを用いた処理システムの一例を示す図である。
【図１４】実施形態２の顧客装置の一実施例を示す機能ブロック図である。
【図１５】実施形態２の開発装置の一実施例を示す機能ブロック図である。
【図１６】実施形態２の開発装置が実行する処理の一例を説明する図である。
【図１７】実施形態２の処理装置の一実施例を示す機能ブロック図である。
【図１８】実施形態２の処理システムにおいて実行される処理の一例を示すシーケンス図である。
【図１９】実施形態３のニューラルネットワークを用いた処理システムの一例を示す図である。
【図２０】実施形態３の顧客装置の一実施例を示す機能ブロック図である。
【図２１】実施形態３の顧客装置が実行する処理の一例を説明する図である。
【図２２】実施形態３の処理装置の一実施例を示す機能ブロック図である。
【図２３】実施形態３の処理システムにおいて実行される処理の一例を示すシーケンス図である。
【図２４】実施形態４のニューラルネットワークを用いた処理システムの一例を示す図である。
【図２５】実施形態４の顧客装置の一実施例を示す機能ブロック図である。
【図２６】畳み込みニューラルネットワークの構造を示す図である。

【図２７】実施形態４の開発装置の一実施例を示す機能ブロック図である。
【図２８】実施形態４の処理装置の一実施例を示す機能ブロック図である。
【図２９】実施形態４の処理システムにおいて実行される処理の一例を示すシーケンス図である。
【図３０】コンピュータ装置の一実施例を示すブロック図である。
【図３１】ＤＨ鍵交換を用いた暗号処理システムの一実施例を示す図である。
【図３２】公開鍵暗号方式を用いた暗号処理システムの一実施例を示す図である。
【図３３】暗号化学習済みモデルの暗号化ヘッダの一実施例を示す図である。
【発明を実施するための形態】
【００１５】
［実施形態１］
実施形態１のニューラルネットワークを用いた処理について説明する。
図１は、実施形態１のニューラルネットワークを用いた処理システムの一例を示す図である。
図１を参照して、ニューラルネットワークを用いた処理の概要を説明する。
【００１６】
処理システム２００は、例えば、顧客装置１ａ、１ｂ、１ｃと、開発装置２と、管理装置３と、保存装置４とを備える。そして、顧客装置１ａ、１ｂ、１ｃと、開発装置２と、管理装置３と、保存装置４とは、ネットワーク３００を介して通信可能に接続される。また、顧客装置１ａ、１ｂ、１ｃと、開発装置２と、管理装置３と、保存装置４とは、例えば、後述するコンピュータ装置である。以下の説明では、顧客装置１ａと、顧客装置１ｂと、顧客装置１ｃとを特に区別しないとき、単に顧客装置１ともいう。
【００１７】
顧客装置１は、例えば、ユーザが所有する情報処理装置である。顧客装置１は、推論処理を用いたアプリケーションを実行する推論装置及びエッジ端末の一例である。開発装置２は、例えば、学習済みモデルの生成とアプリケーションの作成とをする情報処理装置である。開発装置２は、開発者が所有する学習装置の一例である。学習済みモデルは、ネットワーク構造と、重み及びバイアスとを別々のデータとして含んでもよい。
【００１８】
管理装置３は、例えば、管理者が所有する情報処理装置である。そして、管理装置３は、学習済みモデルの使用を許諾するライセンス情報を生成する。保存装置４は、例えば、開発者が所有する情報処理装置である。なお、保存装置４は、開発者が所有する情報処理装置に限らず、例えば、データの保存及び配信を実行する、第三者が運営するサーバ装置などの情報処理装置でもよい。
【００１９】
開発装置２は、開発者が設定したネットワーク構造を用いてディープラーニングを実行することにより、学習済みモデルを生成する。また、開発装置２は、推論処理を実行する推論ＤＬＬ（Ｄｙｎａｍｉｃ　Ｌｉｎｋ　Ｌｉｂｒａｒｙ：　ＤＬＬ）を呼び出して利用するアプリケーションを作成する。そして、開発装置２は、学習済みモデルのプロダクト情報の登録を管理装置３に要求する。なお、アプリケーションには、スタブプログラムの始点を指し示すエントリーポイント、及びアプリケーションの実行時にアプリケーションの始点を指し示すとともに推論ＤＬＬを呼び出すスタブプログラムが付与されてもよい。推論ＤＬＬは、例えば、管理者から開発者に提供される。
【００２０】
管理装置３は、開発装置２から学習済みモデルのプロダクト情報の登録の要求を受信すると、共通鍵を含むプロダクト情報を生成し、プロダクト情報を記憶する。そして、管理装置３は、開発装置２にプロダクト情報を送信する。共通鍵は、暗号化鍵及び復号鍵の一例である。
【００２１】
開発装置２は、管理装置３からプロダクト情報を受信すると、プロダクト情報に含まれる

共通鍵を用いて、学習済みモデルを暗号化する。そして、開発装置２は、暗号化学習済みモデルと、推論ＤＬＬと、アプリケーションとを含む推論情報４ａを保存装置４に送信する。保存装置４は、推論情報４ａを受信すると、推論情報４ａを記憶する。

【００２２】

顧客装置１は、ユーザからの要求に応じて、保存装置４から推論情報４ａを取得する。ユーザは、取得した推論情報４ａに含まれる学習済みモデルが暗号化されている場合、顧客装置１を用いて、開発装置２に学習済みモデルの使用を許諾するライセンス情報の発行を要求する。

【００２３】

開発装置２は、顧客装置１からライセンス情報の発行の要求を受信すると、管理装置３にライセンス情報の生成を要求する。管理装置３は、開発装置２からライセンス情報の生成の要求を受信すると、学習済みモデルに対応する、プロダクト情報に含まれる共通鍵を付与したライセンス情報を生成し、開発装置２に送信する。

【００２４】

開発装置２は、管理装置３からライセンス情報を受信すると、顧客装置１にライセンス情報を送信する。顧客装置１は、開発装置２からライセンス情報を受信すると、ライセンス情報に含まれる共通鍵を用いて、推論情報４ａに含まれる暗号化学習済みモデルを復号し、推論処理を実行する。具体的には、顧客装置１は、ニューラルネットワークのフレームワークに暗号化学習済みモデルを読み込んだとき、学習済みモデルが暗号化されていると判定し、自動的にライセンスファイルを読み込む。そして、顧客装置１は、ライセンス情報に含まれる共通鍵を用いて、暗号化学習済みモデルを復号する。学習済みモデルが暗号化されているか否かの判定は、フレームワークの機能の一部として実装してもよい。以下の説明では、ニューラルネットワークのフレームワークのことを、単にフレームワークともいう。

【００２５】

以上のように、顧客装置１は、フレームワークに学習済みモデルを読み込むことにより、学習済みモデルが暗号化されているか否かを判定する。そして、顧客装置１は、学習済みモデルが暗号化されている場合には、ライセンス情報を読み込み、ライセンス情報に含まれる共通鍵を用いて暗号化学習済みモデルを復号する。したがって、顧客装置１は、学習済みモデルをユーザ側で閲覧及びコピーすることを困難にし、学習済みモデルに含まれるネットワーク構造及び重みの漏洩を防止することができる。

実施形態１の処理システムについて、より具体的に説明する。

【００２６】

以下の説明では、学習済みモデルが暗号化されている場合について説明する。なお、本発明の顧客装置１は、暗号化されていない学習済みモデルを取得した場合には、学習済みモデルが暗号化されていないことを判定し、学習済みモデルを用いた推論処理を自動的に実行する。

【００２７】

図２は、実施形態１の顧客装置の一実施例を示す機能ブロック図である。

図２を参照して、顧客装置１で実行される処理について説明する。

顧客装置１は、制御部１０と、記憶部２０とを備える。そして、顧客装置１は、各種情報を表示する表示装置３０と接続される。なお、顧客装置１は、表示装置３０を含む構成でもよい。

【００２８】

制御部１０は、取得部１１と、判定部１２と、復号部１３と、推論部１４と、出力部１５と、停止部１６とを含む。記憶部２０は、開発装置２から取得したライセンス情報２１を記憶する。ライセンス情報２１は、管理装置３で生成される許諾情報の一例である。

ライセンス情報２１は、例えば、図３に示すように、プロダクト名と、難読化共通鍵と、顧客名と、有効期限と、機器識別子と、電子署名とを含む。

プロダクト名は、開発装置２が生成した学習済みモデルを識別する識別子である。

【００２９】
難読化共通鍵は、例えば、管理装置３が生成したプロダクト名で識別される学習済みモデルを暗号化及び復号する共通鍵を所定の演算により暗号化した暗号文である。難読化共通鍵は、管理装置３で生成される。
【００３０】
難読化共通鍵は、例えば、ライセンス情報２１に含まれるプロダクト名、顧客名、有効期限、及び機器識別子の少なくとも一つと共通鍵との排他的論理和の演算を行うことにより、得られる値でもよい。難読化共通鍵は、例えば、ライセンス情報２１に含まれる顧客名、有効期限、及び機器識別子の少なくとも一つと共通鍵との加減算の演算を行うことにより、得られる値でもよい。また、難読化共通鍵は、例えば、公開鍵暗号の秘密鍵で、共通鍵を暗号化した値でもよい。
【００３１】
顧客名は、顧客装置１を利用するユーザを識別する識別子である。例えば、顧客装置１ａに記憶される顧客名Ａは、顧客装置１ａのユーザを識別する識別子である。
有効期限は、学習済みモデルの利用を許諾する期限を示す情報である。
【００３２】
機器識別子は、例えば、顧客装置１に含まれるいずれかの装置を識別する識別子である。顧客装置１に含まれる装置とは、例えば、ＣＰＵ、及びＨＤＤなどである。識別子は、例えば、ＣＰＵ、及びＨＤＤなどの機器ＩＤでもよい。ライセンス情報２１に含まれる機器識別子は、第１機器識別子の一例である。
【００３３】
電子署名は、ライセンス情報２１の内容が改ざんされていないことを証明するために用いられる情報である。電子署名は、例えば、ライセンス情報２１に含まれるプロダクト名、顧客名、有効期限、及び機器識別子の少なくとも一つを用いて得られる電子署名用の値を求め、電子署名用の値を公開鍵暗号の秘密鍵で暗号化した値でもよい。電子署名は、管理装置３０で生成される。
【００３４】
図２を参照して説明する。
取得部１１は、保存装置４から、学習済みモデルが暗号化されているか否かを識別する暗号化識別子が付与された暗号化学習済みモデルと、推論ＤＬＬと、アプリケーションとを含む推論情報４ａを取得する。
また、取得部１１は、ユーザからの要求に応じて、ライセンス情報２１の発行を開発装置２に要求することにより、ライセンス情報２１を取得する。ライセンス情報２１の発行の要求には、使用許諾を要求する学習済みモデルのプロダクト名と、ユーザの顧客名と、希望する有効期限と、顧客装置１に含まれる機器の機器識別子とが含まれる。暗号化識別子は、開発装置２により、学習済みモデルに付与される情報である。機器識別子は、ユーザが顧客装置１に含まれる任意の装置の機器ＩＤを設定してもよいし、ライセンス情報２１の発行の要求をするときに、顧客装置１が選択した装置の機器ＩＤでもよい。
【００３５】
判定部１２は、ニューラルネットワークの構造及びニューラルネットワークに含まれるエッジの重みの少なくとも一つを含む学習済みモデル（データ）が暗号化された、暗号化学習済みモデルが入力されたか否かを判定する。このとき、判定部１２は、暗号化学習済みモデルに付与されている暗号化識別子を参照することにより、暗号化学習済みモデルが入力されたか否かを判定してもよい。
【００３６】
復号部１３は、暗号化学習済みモデルが入力されたとき、暗号化学習済みモデルを復号する。復号部１３は、ラインセンス情報２１に含まれる難読化共通鍵を復号し、復号した共通鍵を用いて暗号化学習済みモデルを復号してもよい。復号部１３は、例えば、難読化共通鍵を生成したときと逆の演算をすることにより、難読化共通鍵を復号する。
【００３７】

また、復号部１３は、ライセンス情報２１に含まれる有効期限を参照し、学習済みモデルを復号するときの時刻が有効期限内に含まれるとき、暗号化学習済みモデルを復号してもよい。復号部１３は、ライセンス情報２１に含まれる機器識別子と、顧客装置に含まれるいずれかの機器を識別する機器識別子とが一致するとき、学習済みモデルを復号してもよい。顧客装置に含まれる機器を識別する機器識別子は、第２機器識別子の一例である。
推論部１４は、復号された学習済みモデルを用いて推論を実行する。

【００３８】

出力部１５は、学習済みモデルに含まれる情報を出力する。学習済みモデルに含まれる情報とは、ニューラルネットワークのネットワーク構造、重み、及びバイアスなどである。
出力部１５は、学習済みモデルに含まれる情報を、例えば、表示装置３０に表示させてもよい。

【００３９】

停止部１６は、暗号化学習済みモデルが入力されたとき、出力部１５による出力処理を停止する。出力処理は、例えば、フレームワークの機能の一部であり、学習済みモデルに含まれる、ネットワーク構造、重み、及びバイアスを表示装置３０に表示する機能である。また、出力処理は、例えば、フレームワークの機能の一部であり、学習済みモデルに含まれる、ネットワーク構造、重み、及びバイアスを記録媒体などに出力する機能でもよい。すなわち、停止部１６は、暗号化学習済みモデルが入力されたとき、顧客によるネットワーク構造の閲覧及び取得を禁止する。
より具体的には、停止部１６は、例えば、ニューラルネットワークの各レイヤーの名称、レイヤーの出力データの名称、レイヤーの出力データのサイズ、ネットワークのサマリー、及びネットワークのプロファイル情報についての、出力部１５による出力処理を停止する。ネットワークのサマリーとは、例えば、レイヤーの名称とレイヤーのサイズとを羅列した情報である。また、ネットワークのプロファイル情報とは、各レイヤーの処理時間を含む情報である。

【００４０】

図４は、実施形態１の顧客装置の実行する処理の一実施例を説明する図である。
図４を参照して、推論処理についてより詳細に説明する。図４に示すように、顧客装置１において、推論処理は、推論ＤＬＬを制御部１０が実行することにより処理される。推論ＤＬＬは、例えば、制御部１０によって実行されることにより、復号部１３と、推論部１４として機能する。

【００４１】

ユーザによりアプリケーションが実行されると、判定部１２は、取得部１１が取得した学習済みモデルに付与されている暗号化識別子を参照し、学習済みモデルが暗号化されているか否かを判定する。なお、推論部１４は、学習済みモデルが暗号化されていないとき、取得した学習済みモデルを用いて推論処理を実行する。
判定部１２は、取得した学習済みモデルが暗号化されているとき、復号部１３と推論部１４とを含む推論ＤＬＬを呼び出す。

【００４２】

復号部１３は、ライセンス情報２１に含まれる電子署名の検証をする。例えば、復号部１３は、電子署名を生成したときに用いた公開鍵暗号に対応する公開鍵を用いて、電子署名を復号する。また、復号部１３は、ライセンス情報２１に含まれるプロダクト名、顧客名、有効期限、及び機器識別子の少なくとも一つを用いて、電子署名を生成したときと同じ演算をして電子署名用の値を求める。そして、復号部１３は、電子署名を復号した値と、求めた電子署名用の値とが一致するとき、電子署名の検証を承認する。これにより、復号部１３は、ライセンス情報２１が改ざんされていないことを確認する。

【００４３】

復号部１３は、電子署名を承認すると、ライセンス情報２１に含まれる難読化共通鍵を復号する。そして、復号部１３は、復号した共通鍵を用いて暗号化学習済みモデルを復号する。

推論部１４は、復号された学習済みモデルを用いて、推論処理を実行する。そして、推論部１４は、推論結果をアプリケーションに出力する。

【００４４】

図５は、実施形態１の開発装置の一実施例を示す機能ブロック図である。

図５を参照して、開発装置２で実行される処理について説明する。

開発装置２は、制御部４０と、記憶部５０とを備える。

制御部４０は、取得部４１と、学習部４２と、符号化部４３と、暗号化部４４と、付与部４５と、生成部４６と、出力部４７とを含む。記憶部５０は、顧客装置１から取得した顧客管理情報５１と、管理装置３から取得したプロダクト情報５２とを記憶する。

【００４５】

顧客管理情報５１は、顧客からライセンス情報２１の発行の要求とともに受信する情報であり、例えば、図６に示すように、プロダクト名と、顧客名と、有効期限と、機器識別子とを含む。

プロダクト名は、顧客装置１から使用の許諾を要求された学習済みモデルを識別する識別子である。

顧客名は、ライセンス情報２１の発行を要求したユーザを識別する識別子である。

有効期限は、学習済みモデルの利用を許諾する期限を示す情報である。

機器識別子は、例えば、顧客装置１に含まれるいずれかの装置を識別する識別子である。

【００４６】

プロダクト情報５２は、管理装置３にプロダクト情報５２の登録の要求をすることにより、管理装置３から取得する情報であり、例えば、図７に示すように、プロダクト名と、開発者名と、難読化共通鍵とを含む。

プロダクト名は、管理装置３にプロダクト情報５２の登録を要求した学習済みモデルを識別する識別子である。

開発者名は、プロダクト情報５２の登録を要求した開発者を識別する識別子である。

難読化共通鍵は、管理装置３で生成された、学習済みモデルを暗号化及び復号する処理に用いる共通鍵を暗号化した情報である。

【００４７】

図５を参照して説明する。

取得部４１は、顧客装置１からプロダクト名と、顧客名と、有効期限と、機器識別子とを含む顧客情報を取得し、顧客管理情報５１に格納する。取得部４１は、管理装置３にプロダクト情報の登録を要求する。そして、取得部４１は、管理装置３で生成されたプロダクト情報５２を取得し、記憶部５０に記憶させる。プロダクト情報の登録の要求には、学習済みモデルのプロダクト名と学習済みモデルを生成した開発者名とが含まれる。

また、取得部４１は、ライセンス情報２１の生成の要求を管理装置３に送信する。そして、取得部４１は、管理装置３で生成されたライセンス情報を取得する。

【００４８】

学習部４２は、開発者が設定したネットワーク構造及び学習のパラメータを用いて、ニューラルネットワークの重みを調整する。学習のパラメータとは、例えば、フレームワークを用いたディープラーニングの学習時に設定する、ユニット数、荷重減衰、スパース正則化、ドロップアウト、学習率、及びオプティマイザーなどを設定するハイパーパラメータである。

【００４９】

符号化部４３は、ネットワーク構造、重み及びバイアスの少なくとも一つを含む学習済みモデルを符号化する。これにより、符号化部４３は、学習済みモデルが符号化された符号化学習済みモデルを生成する。符号化学習済みモデルは、符号化データの一例である。

暗号化部４４は、符号化学習済みモデルを暗号化する。これにより、暗号化部４４は、符号化学習済みモデルが暗号化された暗号化学習済みモデルを生成する。

【００５０】

付与部４５は、学習済みモデルが暗号化されていることを識別する暗号化識別子を、符号

化学習済みモデルが暗号化された暗号化学習済みモデルに付与する。付与部４５は、学習済みモデルが暗号化されていないとき、学習済みモデルが暗号化されていないことを識別する暗号化識別子を、学習済みモデルに付与する。

【００５１】

なお、付与部４５は、学習済みモデルがネットワーク構造と、重み及びバイアスとを別々のデータとして含むとき、例えば、暗号化されたネットワーク構造に暗号化識別子を付与してもよい。また、付与部４５は、学習済みモデルがネットワーク構造と、重み及びバイアスとを別々のデータとして含むとき、例えば、暗号化された重み及びバイアスに暗号化識別子を付与してもよい。

【００５２】

生成部４６は、暗号化学習済みモデルと、推論ＤＬＬと、アプリケーションとを含む推論情報４ａを生成する。アプリケーションは、学習済みモデルを用いた推論処理の結果を用いて、画像認識、音声認識、及び文字認識などの各種処理を実行するプログラムであり、開発者によって作成される。

【００５３】

出力部４７は、保存装置４に推論情報４ａを出力する。すなわち、出力部４７は、符号化学習済みモデルが暗号化された暗号化学習済みモデルを出力する。なお、出力部４７は、推論情報４ａを、例えば、記録媒体に出力してもよい。この場合には、ユーザは、開発者から記録媒体を受けとり、記録媒体から推論情報４ａを読み込ませることにより、取得部１１に推論情報４ａを取得させてもよい。

また、出力部４７は、管理装置３から取得したライセンス情報２１を、顧客装置１に出力する。

【００５４】

図８は、実施形態１の開発装置の実行する処理の一実施例を説明する図である。

図８を参照して、開発装置２で実行される暗号化処理についてより詳細に説明する。開発装置２において、暗号化処理は、制御部４０が暗号化ツールを実行することにより処理される。暗号化ツールとは、例えば、開発者が学習済みモデルを暗号化するときに用いられるプログラムであり、管理者３から提供される。暗号化ツールは、例えば、制御部４０によって実行されることにより、符合化部４３と、暗号化部４４と、付与部４５として機能する。

【００５５】

取得部４１は、学習部４２により学習済みモデルが生成されると、管理装置３に学習済みモデルに対応するプロダクト情報５２の登録を要求する。そして、取得部４２は、管理装置３から、管理装置３で生成されたプロダクト情報５２を取得し、記憶部５０に記憶する。

【００５６】

開発者は、プロダクト情報５２が記憶部５０に記憶されたあと、プロダクト情報５２に含まれるプロダクト名に対応する学習済みモデルの暗号化を開発装置２に要求する。開発装置２は、学習済みモデルの暗号化が要求されると、符号化部４３と、暗号化部４４と、付与部４５とを含む暗号化ツールを起動する。

【００５７】

符号化部４３は、学習済みモデルを符号化する。符号化部４３は、例えば、学習済みモデルに含まれる重み及びバイアスの少なくとも一つを符号化する。このとき、符号化部４３は、符号化のアルゴリズムとして、量子化及びランレングス符号化の少なくとも一つを用いてもよい。

【００５８】

暗号化部４４は、プロダクト情報５２に含まれる難読化共通鍵を生成したときと逆の演算をして難読化共通鍵を復号する。そして、暗号化部４４は、共通鍵を用いて符号化された学習済みモデルを暗号化する。付与部４５は、暗号化学習済みモデルに暗号化されていることを識別する暗号化識別子を付与する。以上のように、開発装置２は、暗号化処理を実行することにより、学習済みモデルを暗号化した暗号化学習済みモデルを生成する。暗号

化部４４は、暗号化のアルゴリズムとして、Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ　（ＤＥＳ）、及びＡｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ（ＡＥＳ）などを適宜選択して使用してもよい。

【００５９】

図９は、実施形態１の管理装置の一実施例を示す機能ブロック図である。

図９を参照して、管理装置３で実行される処理について説明する。

管理装置３は、制御部６０と、記憶部７０とを備える。

制御部６０は、割当部６１と、難読化部６２と、生成部６３と、出力部６４とを含む。記憶部７０は、開発装置２から取得したプロダクト名に共通鍵を割り当てた製品管理情報７１を記憶する。

【００６０】

製品管理情報７１は、学習済みモデルのプロダクト名に対する、共通鍵の割り当てを示す情報である。製品管理情報７１は、例えば、図１０に示すように、プロダクト名と、開発者名と、難読化共通鍵とを含む。

プロダクト名は、プロダクト情報５２の登録を要求された学習済みモデルを識別する識別子である。

開発者名は、プロダクト情報５２の登録を要求した開発者を識別する識別子である。

【００６１】

難読化共通鍵は、プロダクト名に対応する学習済みモデルに割り当てた共通鍵を難読化した情報である。なお、共通鍵は、難読化しない状態で、製品管理情報７１に格納されてもよい。この場合には、顧客装置１は、管理装置３から暗号化されていない共通鍵を、開発装置２を介して受信し、暗号化学習済みモデルの復号を実行してもよい。また、開発装置２は、暗号化されていない共通鍵を管理装置３から受信し、学習済みモデルの暗号化を実行してもよい。以下の説明では、共通鍵は、難読化されている状態で製品管理情報７１に格納されているものとして説明する。共通鍵を難読化した状態で製品管理情報７１に格納するのは、管理装置３がハッキングされるなどして、製品管理情報７１に格納されている情報が盗難された場合において、共通鍵の不正利用を防止するためである。

【００６２】

図９を参照して説明する。

割当部６１は、開発装置２からのプロダクト情報の登録の要求に含まれるプロダクト名及び開発者名に共通鍵を割り当てる。

難読化部６２は、所定の演算を施すことにより、共通鍵を難読化する。

生成部６３は、プロダクト名、開発者名、及び難読化共通鍵を対応付けたプロダクト情報５２を製品管理情報７１に格納する。

【００６３】

出力部６４は、開発装置２からのプロダクト名と開発者名とを含むプロダクト情報５２の取得要求に応じて、対応するプロダクト情報５２を開発装置２に出力する。なお、出力部６４は、プロダクト情報５２を、例えば、記録媒体に出力してもよい。この場合には、開発者は、管理者から記録媒体を受けとり、取得部４２に記録媒体からプロダクト情報５２を読み込ませることにより、プロダクト情報５２を取得してもよい。

【００６４】

図１１、図１２は、実施形態１の処理システムにおいて実行される処理の一例を示すシーケンス図である。

図１１、図１２を参照して実施形態１の処理システムにおいて実行される処理を説明する。以下の説明において、説明の簡単化のため、顧客装置１の制御部１０、開発装置２の制御部４０、及び管理装置３の制御部６０が実行する処理のことを、顧客装置１、開発装置２、及び管理装置３が実行する処理と記載する。

【００６５】

図１１を参照して説明する。

開発装置２は、開発者からニューラルネットワークのネットワーク構造の設定の入力を受

け付ける（Ｓ１０１）。開発装置２は、機械学習を実行することにより、ニューラルネットワークに含まれるエッジの重み及びバイアスを調整する（Ｓ１０２）。さらに、開発装置２は、調整した重み及びバイアスを符号化する（Ｓ１０３）。そして、開発装置２は、ネットワーク構造と、符合化した重み及びバイアスと、を含む学習済みモデルを生成する（Ｓ１０４）。

【００６６】

開発装置２は、学習済みモデルのプロダクト名と開発者名とを含むプロダクト情報５２の登録要求情報を生成する（Ｓ１０５）。そして、開発装置２は、登録要求情報を管理装置３に送信することにより、管理装置３にプロダクト情報５２の登録要求をする（Ｓ１０６）。

【００６７】

管理装置３は、開発装置２から登録要求情報を受信すると、共通鍵を生成し、登録要求情報に含まれるプロダクト名と開発者名とに、共通鍵を割り当てる（Ｓ１０７）。また、管理装置３は、プロダクト名と開発者名とに割り当てた共通鍵を難読化する（Ｓ１０８）。そして、管理装置３は、プロダクト名と開発者名と難読化共通鍵とを関連付けたプロダクト情報５２を生成し、製品管理情報７１に格納する（Ｓ１０９）。管理装置３は、生成したプロダクト情報５２を開発装置２に送信する（Ｓ１１０）。

【００６８】

開発装置２は、管理装置３からプロダクト情報５２を受信すると、プロダクト情報５２に含まれる難読化共通鍵を復号する（Ｓ１１１）。そして、開発装置２は、復号した共通鍵を用いて、プロダクト情報５２に含まれるプロダクト名に対応する学習済みモデルを暗号化する（Ｓ１１２）。開発装置２は、暗号化した学習済みモデルを保存装置４に送信し、保存装置４に暗号化学習済みモデルを記憶させる（Ｓ１１３）。このとき、開発装置２は、暗号化学習済みモデルと、アプリケーションと、推論ＤＬＬとを含む推論情報４ａを生成し、推論情報を保存装置４に記憶させてもよい。

【００６９】

図１２を参照して説明する。

顧客装置１は、ユーザからの要求に応じて保存装置４から学習済みモデルを取得する（Ｓ１１４）。このとき、顧客装置１は、暗号化学習済みモデルと、アプリケーションと、推論ＤＬＬとを含む推論情報を保存装置４から取得することにより、推論情報４ａに含まれる学習済みモデルを取得してもよい。

【００７０】

顧客装置１は、取得した学習済みモデルが暗号化されているか否かを判定する（Ｓ１１５）。顧客装置１は、取得した学習済みモデルが暗号化されていない場合、学習済みモデルを用いて推論処理を実行する。

【００７１】

顧客装置１は、取得した学習済みモデルが暗号化されているとき、プロダクト名と、顧客名と、有効期限と、機器識別子とを含む顧客情報を生成する（Ｓ１１６）。そして、顧客装置１は、生成した顧客情報を含むライセンス情報２１の発行要求を開発装置２に送信する（Ｓ１１７）。

【００７２】

開発装置２は、ライセンス情報２１の発行要求を受信すると、ライセンス情報２１の発行要求に含まれる顧客情報を顧客管理情報５１に格納する（Ｓ１１８）。そして、開発装置２は、顧客情報を含むライセンス情報２１の生成要求を管理装置３に送信する（Ｓ１１９）。

【００７３】

管理装置３は、ライセンス情報２１の生成要求を受信すると、顧客情報に含まれるプロダクト名に対応するレコードを製品管理情報７１から抽出し、ライセンス情報２１の発行要求に含まれる顧客情報を用いて電子署名を生成する。また、管理装置３は、抽出したレコードに含まれる難読化共通鍵と、生成した電子署名と、受信した顧客情報とを含むライセ

ンス情報２１を生成する（Ｓ１２０）。そして、管理装置３は、生成したライセンス情報２１を開発装置２に送信する（Ｓ１２１）。

【００７４】

開発装置２は、管理装置３からライセンス情報２１を受信すると、ライセンス情報２１を顧客装置１に送信する（Ｓ１２２）。

顧客装置１は、開発装置２からライセンス情報２１を受信すると、ライセンス情報２１に含まれる電子署名を検証する（Ｓ１２３）顧客装置１は、電子署名が承認できないとき、処理を終了する。

【００７５】

顧客装置１は、電子署名を承認すると、難読化共通鍵を復号する（Ｓ１２４）。また、顧客装置１は、復号した共通鍵を用いて暗号化学習済みモデルを復号する（Ｓ１２５）。さらに、顧客装置１は、暗号化学習済みモデルの情報を出力する機能を停止する（Ｓ１２６）。そして、顧客装置１は、推論処理を実行する（Ｓ１２７）。

【００７６】

以上のように、実施形態１の顧客装置１は、取得した学習済みモデルが暗号化されているか否かを判定する。そして、顧客装置１は、学習済みモデルが暗号化されているとき、自動的に学習済みモデルを復号し、復号した学習済みモデルを用いた推論処理を実行する。したがって、顧客装置１は、復号した学習済みモデルを出力することなく、推論処理を実行するので、学習済みモデルに含まれるネットワーク構造及び重みの漏洩を防止することができる。

【００７７】

実施形態１の顧客装置１は、暗号化学習済みモデルが入力されたとき、フレームワークの機能の一部である学習済みモデルを出力する処理を停止するので、学習済みモデルに含まれるネットワーク構造及び重みの漏洩を防止することができる。

【００７８】

実施形態１の学習済みモデルは、ネットワーク構造または重みの情報に暗号化されているか否かを識別する暗号化識別子を含む。これにより、顧客装置１は、学習済みモデルが暗号化されているか否かを判定し、自動的に学習済みモデルを復号して、復号した学習済みモデルを用いた推論処理を実行する。したがって、顧客装置１は、復号した学習済みモデルを出力することなく、推論処理を実行するので、学習済みモデルに含まれるネットワーク構造及び重みの漏洩を防止することができる。

【００７９】

実施形態１の顧客装置１は、ライセンス情報２１を取得し、ライセンス情報２１に応じて暗号化学習済みモデルを復号して利用するので、ライセンス情報２１を保有していないユーザの学習済みモデルの利用を拒絶することができる。したがって、顧客装置１は、学習済みモデルの不正利用を防止することができる。

【００８０】

実施形態１の開発装置２は、学習によって調整した重み及びバイアスを符合化したあとに暗号化し、暗号化学習済みモデルを生成する。すなわち、開発装置２は、暗号化対象の学習済みモデルのサイズを小さくしてから、暗号化処理を実行する。したがって、開発装置２は、暗号処理の負荷を低減し、かつ暗号化学習済みモデルのサイズを小さくすることができる。

【００８１】

実施形態１の開発装置２は、ネットワーク構造または重みの情報に暗号化されているか否かを識別する暗号化識別子を含む暗号化学習済みモデルを生成する。また、実施形態１では、顧客装置１で実行するフレームワークの機能に、暗号化識別子を参照することにより、学習済みモデルが暗号化されているか否かを判定する機能と、暗号化学習済みモデルを復号する機能とを付与する。これにより、顧客装置１は、暗号化識別子を参照することにより、学習済みモデルが暗号化されているか否かを判定する。したがって、顧客装置１は、フレームワークに読み込んだ学習済みモデルが暗号化されているとき、自動的に学習済

みモデルを復号可能となり、学習済みモデルに含まれるネットワーク構造及び重みの漏洩を防止することができる。

【００８２】

実施形態１のライセンス情報２１は、プロダクト名、顧客名、有効期限、及び機器識別子の少なくとも一つを用いて共通鍵を難読化した情報を含む。これにより、実施形態１の処理システム２００は、ライセンス情報２１が盗難されても、共通鍵の利用を困難にし、学習済みモデルの不正利用、及びネットワーク構造及び重みの漏洩を防止することができる。

【００８３】

実施形態１のライセンス情報２１は、有効期限を含む。これにより、顧客装置１は、有効期限が切れたときに、暗号化学習済みモデルの利用を拒絶する。したがって、顧客装置１は、例えば、学習済みモデルを評価版としてユーザに提供したときなどにおいて、学習済みモデルを利用可能な期間を設定することができる。

【００８４】

実施形態１の電子署名は、ライセンス情報２１に含まれるプロダクト名、顧客名、有効期限、及び機器識別子の少なくとも一つを用いて生成される。これにより、顧客装置１は、ライセンス情報２１に含まれる情報が書き換えられたとき、ライセンス情報２１に不正な改ざんがされたものと判定し、暗号化学習済みモデルの利用を拒絶することができる。

【００８５】

実施形態１の処理システム２００では、学習済みモデルの開発者が学習済みモデルを用いるアプリケーションを作成するものとして説明したが、アプリケーションは、学習済みモデルの開発者とは別のアプリ開発者が作成してもよい。この場合において、ライセンス情報２１と、暗号化学習済みモデルとは、アプリ開発者を介して、学習済みモデルの開発者から顧客に提供されてもよい。

【００８６】

ライセンス情報２１と暗号化学習済みモデルとをアプリ開発者を介して顧客に提供する場合においても、難読化共通鍵の復号は、推論ＤＬＬ内で難読化共通鍵を生成したときと逆の演算をすることにより、自動的に行なわれる。すなわち、アプリ開発者及び顧客は、学習済みモデルの内容を知ることなくアプリケーションの開発及び利用をする。これにより、処理システム２００において、学習済みモデルの内容は、学習済みモデルの開発者以外に知られることなく利用される。以上により、処理システム２００は、学習済みモデルを無断で流用されるなどのリスクを抑制して、学習済みモデルの開発者と、アプリ開発者との協業を促進することができる。

【００８７】

［実施形態２］

実施形態２の処理システムについて説明する。

図１３は、実施形態２のニューラルネットワークを用いた処理システムの一例を示す図である。

図１３を参照して、ニューラルネットワークを用いた処理の概要を説明する。

実施形態２の処理システム４００の構成は、図１で説明した実施形態１の処理システム２００と同じ構成であるので説明を省略する。以下の説明では、処理システム４００において、処理システム２００と異なる機能を有する顧客装置５ａ、５ｂ、５ｃの構成と、開発装置６Ａの構成とを説明する。また、処理システム２００と同じ構成については、実施形態１と同じ符号を付し、説明を省略する。顧客装置５ａと、顧客装置５ｂと、顧客装置５ｃとを特に区別しないとき、単に顧客装置５Ａともいう。

【００８８】

図１４は、実施形態２の顧客装置の一実施例を示す機能ブロック図である。

図１４を参照して、顧客装置５Ａで実行される処理について説明する。

顧客装置５Ａは、制御部８０ａと、記憶部２０と、接続部８４とを含む。顧客装置５Ａの構成は、実施形態１の顧客装置１の構成に、接続部８４が追加された構成である。以下の説明では、接続部８４と、接続部８４の追加にともない機能が一部変更された取得部８１

と、判定部８２と、復号部８３との変更された機能との説明をし、その他の説明を省略する。

【００８９】

接続部８４は、ライセンス情報２１が格納された処理装置７と着脱可能に接続される。処理装置７は、開発装置６によりライセンス情報２１が格納された装置であり、例えば、制御回路、記憶装置、及び入出力インターフェイスを含むＵＳＢドングルなどである。

【００９０】

取得部８１は、ユーザからの要求に応じて、ライセンス情報２１の発行を開発装置６Ａに要求する。これにより、ユーザは、開発装置６Ａによりライセンス情報２１が格納された処理装置７を開発者から提供される。また、取得部８１は、接続部８４に処理装置７が接続されたとき、処理装置７からライセンス情報２１を取得する。

そして、判定部８２と、復号部８３とは、処理装置７に格納されたライセンス情報２１を用いて判定処理と復号処理とを実行する。

【００９１】

図１５は、実施形態２の開発装置の一実施例を示す機能ブロック図である。

図１５を参照して、開発装置６Ａで実行される処理について説明する。

開発装置６Ａは、制御部９０ａと、記憶部５０と、接続部９１とを備える。開発装置６Ａの構成は、実施形態１の開発装置２の構成に、書込部９２と、接続部９１とが追加された構成である。以下の説明では、接続部９１と、書込部９２と、機能が一部変更された出力部９３の変更された機能との説明をし、その他の説明を省略する。

【００９２】

接続部９１は、処理装置７と着脱可能に接続される。書込部９２は、図１６に示すように、管理装置３から取得したライセンス情報２１を、接続部９１を介して処理装置７に書き込みをする。なお、実施形態２において、出力部９３は、管理装置３から取得したライセンス情報２１を、顧客装置１に出力しなくてもよい。

【００９３】

図１７は、実施形態２の処理装置の一実施例を示す機能ブロック図である。

図１７を参照して、処理装置７で実行される処理について説明する。

処理装置７は、制御部１００と、記憶部１１０と、接続部１０３とを備える。制御部１００は、取得部１０１と、出力部１０２とを含む。記憶部１１０は、ライセンス情報２１を記憶する。

【００９４】

接続部１０３は、顧客装置５Ａ及び開発装置６Ａと着脱可能に接続される。取得部１０１は、接続部１０３が開発装置６Ａと接続されたとき、開発装置６Ａから接続部１０３を介してライセンス情報２１を取得し、記憶部１１０にライセンス情報２１を記憶する。出力部１０２は、接続部１０３が顧客装置５Ａと接続されたとき、接続部１０３を介して顧客装置５Ａにライセンス情報２１を出力する。

【００９５】

図１８は、実施形態２の処理システムにおいて実行される処理の一例を示すシーケンス図である。

図１８を参照して、実施形態２の処理システムにおいて実行される処理を説明する。以下の説明において、説明の簡単化のため、顧客装置５Ａの制御部８０ａ、開発装置６Ａの制御部９０ａ、及び管理装置３の制御部６０が実行する処理のことを、顧客装置５Ａ、開発装置６Ａ、及び管理装置３が実行する処理と記載する。

【００９６】

実施形態２の処理システム４００は、実施形態１の処理システム２００で実行される処理のＳ１２２からＳ１２４に代えて、下記で説明するＳ２０１からＳ２０４が追加された処理である。以下の説明では、Ｓ２０１からＳ２０４の処理を説明し、その他の処理の説明を省略する。

【００９７】

開発装置６Ａは、Ｓ１２２において、管理装置３からライセンス情報２１を受信すると、ライセンス情報２１を処理装置７に書き込む（Ｓ２０１）。そして、開発者は、ユーザに処理装置７を提供する。

【００９８】

顧客装置５Ａは、例えば、ユーザにより処理装置７が接続される（Ｓ２０２）と、処理装置７からライセンス情報２１を取得し、取得したライセンス情報２１に含まれる電子署名を検証する（Ｓ２０３）。顧客装置５Ａは、電子署名が承認できないとき、処理を終了する。

【００９９】

顧客装置５Ａは、電子署名を承認すると、処理装置７から取得したライセンス情報２１に含まれる難読化共通鍵を復号する（Ｓ２０４）。そして、顧客装置５Ａは、復号した共通鍵を用いて暗号化学習済みモデルを復号する（Ｓ１２５）。なお、難読化共通鍵の復号は、推論情報４ａに含まれる推論ＤＬＬを用いて、顧客装置５Ａが管理装置３における共通鍵の難読化と逆の処理を行うことにより実行されてもよい。

【０１００】

以上のように、実施形態２の顧客装置５Ａは、処理装置７に記憶されたラインセンス情報２１を用いて暗号化学習済みモデルを復号するため、処理装置７を提供されたユーザのみが学習済みモデルを復号可能にする。したがって、顧客装置５Ａは、学習済みモデルに含まれるネットワーク構造及び重みの漏洩を防止することができる。

【０１０１】

実施形態２の処理システム４００では、学習済みモデルの開発者が学習済みモデルを用いるアプリケーションを作成するものとして説明したが、アプリケーションは、学習済みモデルの開発者とは別のアプリ開発者が作成してもよい。この場合において、暗号化学習済みモデルは、アプリ開発者を介して、学習済みモデルの開発者から顧客に提供されてもよい。

【０１０２】

暗号化学習済みモデルを、アプリ開発者を介して顧客に提供する場合においても、難読化共通鍵の復号は、推論ＤＬＬ内で難読化共通鍵を生成したときと逆の演算をすることにより、自動的に行なわれる。すなわち、アプリ開発者及び顧客は、学習済みモデルの内容を知ることなくアプリケーションの開発及び利用をする。これにより、処理システム４００において、学習済みモデルの内容は、学習済みモデルの開発者以外に知られることなく利用される。以上により、処理システム４００は、学習済みモデルを無断で流用されるなどのリスクを抑制して、学習済みモデルの開発者と、アプリ開発者との協業を促進することができる。

【０１０３】

［実施形態３］

実施形態３の処理システムについて説明する。

図１９は、実施形態３のニューラルネットワークを用いた処理システムの一例を示す図である。

図１９を参照して、ニューラルネットワークを用いた処理の概要を説明する。

【０１０４】

実施形態３の処理システム５００の構成は、図１３で説明した実施形態２の処理システム４００と同じ構成であるので説明を省略する。以下の説明では、処理システム５００において、処理システム４００と異なる機能を有する顧客装置５ｄ、５ｅ、５ｆの構成と、処理装置９の構成とを説明する。また、処理システム４００と同じ構成については、実施形態２と同じ符号を付し、説明を省略する。顧客装置５ｄと、顧客装置５ｅと、顧客装置５ｆとを特に区別しないとき、単に顧客装置５Ｂともいう。

【０１０５】

図２０は、実施形態３の顧客装置の一実施例を示す機能ブロック図である。

図２０を参照して、顧客装置５Ｂで実行される処理について説明する。

顧客装置５Ｂは、制御部８０ｂと、記憶部２０と、接続部８４とを含む。
以下の説明では、機能が一部変更された取得部８５の変更された機能の説明をし、その他の説明を省略する。
【０１０６】
接続部８４は、暗号化学習済みモデルを復号する機能を有し、かつライセンス情報２１が格納された処理装置８と着脱可能に接続される。処理装置８は、開発装置６によりライセンス情報２１が格納された装置であり、例えば、制御回路、記憶装置、及び入出力インターフェイスを含むＵＳＢドングルなどである。
【０１０７】
取得部８５は、図２１に示すように、暗号化学習済みモデルが入力されたとき、接続部８４に処理装置８が接続されている場合、処理装置８に暗号化学習済みモデルを復号させることにより、学習済みモデルを取得する。
推論部１４は、復号された学習済みモデルを用いて、アプリケーションから入力される推論の対象の対象データを用いて、推論処理を実行する。
【０１０８】
図２２は、実施形態３の処理装置の一実施例を示す機能ブロック図である。
図２２を参照して、処理装置８で実行される処理について説明する。
実施形態３の処理装置８は、制御部１２０と、記憶部１１０と、接続部１０１とを備える。処理装置８の構成は、実施形態２の処理装置７の構成に、復号部１２１が追加された構成である。以下の説明では、復号部１２１の説明をし、その他の説明を省略する。なお、処理装置８は、暗号化識別子を参照することにより、顧客装置５Ｂから入力される暗号化学習済みモデルが暗号化されているか否かを判定する判定部を備えてもよい。
【０１０９】
復号部１２１は、顧客装置５Ｂを介して暗号化学習済みモデルが入力されると、ライセンス情報２１に含まれる難読化共通鍵を復号する。また、復号部１２１は、復号した共通鍵を用いて暗号化学習済みモデルを復号する。そして、出力部１０３は、接続部１０１を介して顧客装置５Ａに復号された暗号化学習済みモデルを出力する。
【０１１０】
図２３は、実施形態３の処理システムにおいて実行される処理の一例を示すシーケンス図である。
図２３を参照して、実施形態３の処理システム５００において実行される処理を説明する。以下の説明において、説明の簡単化のため、顧客装置５Ｂの制御部８０ｂ、開発装置６Ａの制御部９０ａ、及び管理装置３の制御部６０が実行する処理のことを、顧客装置５Ｂ、開発装置６Ａ、及び管理装置３が実行する処理と記載する。
【０１１１】
実施形態３の処理システム５００は、実施形態２の処理システム４００で実行される処理のＳ２０４、Ｓ１２５に代えて、下記で説明するＳ３０１、Ｓ３０２が追加された処理である。以下の説明では、Ｓ３０１とＳ３０２の処理を説明し、その他の処理の説明を省略する。
【０１１２】
顧客装置５Ｂは、例えば、ユーザにより処理装置８が接続される（Ｓ２０２）と、処理装置８からライセンス情報２１を取得し、取得したライセンス情報２１に含まれる電子署名を検証する（Ｓ２０３）。顧客装置５Ｂは、電子署名が承認できないとき、処理を終了する。
【０１１３】
顧客装置５Ｂは、電子署名を承認すると、処理装置７に暗号化学習済みモデルを出力する（Ｓ３０１）。これにより、顧客装置５Ｂは、処理装置８に暗号化学習済みモデルを復号させる。そして、顧客装置５Ｂは、処理装置８から復号された学習済みモデルを取得する（Ｓ３０２）。
【０１１４】

以上のように、実施形態３の顧客装置５Ｂは、処理装置８に暗号化学習済みモデルを復号させるため、処理装置８を提供されたユーザのみが学習済みモデルを復号可能にする。したがって、顧客装置５Ｂは、学習済みモデルに含まれるネットワーク構造及び重みの漏洩を防止することができる。

【０１１５】

実施形態３の処理システム５００では、学習済みモデルの開発者が学習済みモデルを用いるアプリケーションを作成するものとして説明したが、アプリケーションは、学習済みモデルの開発者とは別のアプリ開発者が作成してもよい。この場合において、暗号化学習済みモデルは、アプリ開発者を介して、学習済みモデルの開発者から顧客に提供されてもよい。

【０１１６】

暗号化学習済みモデルを、アプリ開発者を介して顧客に提供する場合においても、難読化共通鍵の復号は、推論ＤＬＬ内で難読化共通鍵を生成したときと逆の演算をすることにより、自動的に行なわれる。すなわち、アプリ開発者及び顧客は、学習済みモデルの内容を知ることなくアプリケーションの開発及び利用をする。これにより、処理システム５００において、学習済みモデルの内容は、学習済みモデルの開発者以外に知られることなく利用される。以上により、処理システム５００は、学習済みモデルを無断で流用されるなどのリスクを抑制して、学習済みモデルの開発者と、アプリ開発者との協業を促進することができる。

【０１１７】

［実施形態４］

実施形態４の処理システムについて説明する。

図２４は、実施形態４のニューラルネットワークを用いた処理システムの一例を示す図である。

図２４を参照して、ニューラルネットワークを用いた処理の概要を説明する。

【０１１８】

実施形態４の処理システム６００の構成は、図１９で説明した実施形態３の処理システム５００と同じ構成であるので説明を省略する。以下の説明では、処理システム６００において、処理システム５００と異なる機能を有する５ｇ、５ｈ、５ｉの構成と、開発装置６Ｂの構成と、処理装置９の構成とを説明する。また、処理システム５００と同じ構成については、実施形態３と同じ符号を付し、説明を省略する。顧客装置５ｇと、顧客装置５ｈと、顧客装置５ｉとを特に区別しないとき、単に顧客装置５Ｃともいう。

【０１１９】

図２５は、実施形態４の顧客装置の一実施例を示す機能ブロック図である。

図２５を参照して、顧客装置５Ｃで実行される処理について説明する。

顧客装置５Ｃは、制御部８０ｂと、記憶部２０と、接続部８４とを含む。以下の説明では、機能が一部変更された取得部８６と、判定部８７と、推論部８８との変更された機能との説明をし、その他の説明を省略する。

【０１２０】

接続部８４は、ニューラルネットワークに属する一部の層の演算（後述する第２演算）を実行する機能と暗号化学習済みモデルを復号する機能とを有し、かつライセンス情報２１と層情報１４１とが格納された処理装置９と着脱可能に接続される。層情報１４１とは、例えば、図２６に示す畳み込みニューラルネットワーク７００に含まれる連続する３層以上の層７３０のネットワーク構成、重み、及びバイアスを含む情報である。

【０１２１】

上述の層情報１４１は、一例であり、畳み込みニューラルネットワーク、またはその他のニューラルネットワークに含まれる任意の１以上の層でもよい。以下の説明において、ニューラルネットワークの構造は、図２６に示す畳み込みニューラルネットワークであるものとして説明する。

【０１２２】

取得部８６は、層情報１４１を除く暗号化学習済みモデルを保存装置４から取得する。判定部８７は、層情報１４１を除く暗号化学習済みモデルが入力されたか否かを判定する。層情報１４１を除く暗号化学習済みモデルとは、例えば、図２６に示す層７３０のネットワーク構造、重み、及びバイアスを示す情報を、畳み込みニューラルネットワーク７００の学習済みモデルから除いた情報である。

【０１２３】

すなわち、層情報１４１を除く暗号化学習済みモデルとは、１以上の層を含む第１演算と、１以上の他の層を含む第２演算と、を含むニューラルネットワークの第１演算の構造及び重みを含む第１学習済みモデルを暗号化した情報である。第１演算とは、例えば、図２６に示す、アプリケーションから推論の対象データ７０１が入力される入力層７１０、畳み込み層７２０、及び畳み込み層７４０から出力層７８０に含まれるネットワーク構造、重み、バイアスに対応する演算である。第２演算とは、例えば、図２６に示す、プーリング層７３１からプーリング層７３３を含む層７３０に含まれるネットワーク構造、重み、バイアスに対応する演算である。

【０１２４】

取得部８６は、層情報１４１を除く暗号化学習済みモデルが入力されたとき、層情報１４１を除く暗号化学習済みモデルを処理装置９に出力する。これにより、取得部８６は、処理装置９に層情報１４１を除く暗号化学習済みモデルを復号させる。

【０１２５】

取得部８６は、処理装置９から層情報１４１を除く学習済みモデルを取得する。推論部８８は、層情報１４１を除く学習済みモデルを用いて、図２６に示す畳み込み層７２０までの処理を実行する。そして、取得部８６は、畳み込み層７２０の出力データを処理装置９に出力する。これにより、取得部８６は、処理装置９に層情報１４１を用いて第２演算を実行させる。以下の説明では、層情報１４１を用いた第２演算のことを、層情報１４１の演算ともいう。

【０１２６】

取得部８６は、処理装置９から層情報１４１の演算結果を取得する。推論部８８は、層情報１４１の演算結果を用いて、図２６に示す畳み込み層７３０から出力層７８０までの層に対応する演算を実行する。

【０１２７】

図２７は、実施形態４の開発装置の一実施例を示す機能ブロック図である。

図２７を参照して、開発装置６Ｂで実行される処理について説明する。

開発装置６Ｂは、制御部９０ｂと、記憶部５０と、接続部９９とを含む。以下の説明では、機能が一部変更された書込部９４と、暗号化部９５、生成部９６、出力部９７との変更された機能との説明をし、その他の説明を省略する。

【０１２８】

接続部９１は、処理装置９と着脱可能に接続される。書込部９４は、学習部４２及び符合化部４３により生成された学習済みモデルの一部である層情報１４１を、接続部９１を介して処理装置９に書き込みをする。実施形態４において、暗号化部９５は、層情報１４１を除く学習済みモデルを暗号化する。生成部９６は、層情報１４１を除く暗号化学習済みモデルと、推論ＤＬＬと、アプリケーションとを含む推論情報４ｂを生成する。出力部９７は、推論情報４ｂを保存装置４に出力する。なお、暗号化部９５は、層情報１４１を暗号化してもよい。そして、書込部９４は、暗号化された層情報１４１を処理装置９に書き込んでもよい。また、出力部９７は、推論情報４ａを保存装置４に出力してもよい。

【０１２９】

図２８は、実施形態４の処理装置の一実施例を示す機能ブロック図である。

図２８を参照して、処理装置９で実行される処理について説明する。

実施形態４の処理装置９は、制御部１３０と、記憶部１４０と、接続部１０１とを備える。処理装置９の構成は、実施形態３の処理装置８の構成に、推論部１３１と、層情報１４１とが追加された構成である。以下の説明では、推論部１３１と、層情報１４１と、推論

部１３１及び層情報１４１の追加にともない機能が一部変更された取得部１３２と、出力部１３３と、復号部１３４との変更された機能との説明をし、その他の説明を省略する。なお、処理装置９は、暗号化識別子を参照することにより、顧客装置５Ｃから入力される暗号化学習済みモデルが暗号化されているか否かを判定する判定部を備えてもよい。

【０１３０】

推論部１３１は、顧客装置５Ｃから層情報１４１に入力する入力データを取得すると、層情報１４１の演算を実行する。そして、出力部１０１は、層情報１４１の演算結果を顧客装置５Ｃに出力する。層情報１４１に入力する入力データとは、例えば、図２６に示す畳み込み層７２０の出力データである。層情報１４１の演算結果とは、例えば、図２６に示すプーリング層７３３の出力データである。なお、層情報１４１が暗号化されている場合には、復号部１３３は、層情報１４１を復号する。そして、推論部１３１は、復号された層情報１４１を用いて、層情報１４１の演算を実行する。

取得部１３２は、開発装置６Ｂから層情報１４１を取得し、記憶部１４０に記憶する。

【０１３１】

復号部１３４は、顧客装置５Ｃから層情報１４１を除く暗号化学習済みモデルが入力されると、ライセンス情報２１に含まれる難読化共通鍵を復号する。また、復号部１３４は、復号した共通鍵を用いて層情報１４１を除く暗号化学習済みモデルを復号する。そして、出力部１３３は、復号された層情報１４１を除く暗号化学習済みモデルを顧客装置５Ｃに出力する。

【０１３２】

以上のように、処理装置９には、１以上の層を含む第１演算と、１以上の他の層を含む第２演算と、を含むニューラルネットワークの第２演算の構造及び重みを含む第２学習済みモデルが記憶されている。そして、処理装置９は、第２学習済みモデルを用いて第２演算を実行する。

【０１３３】

図２９は、実施形態４の処理システムにおいて実行される処理の一例を示すシーケンス図である。

図２９を参照して、実施形態４の処理システム６００において実行される処理を説明する。以下の説明において、説明の簡単化のため、顧客装置５Ｃの制御部８０ｃ、開発装置６Ｂの制御部９０ｂ、及び管理装置３の制御部６０が実行する処理のことを、顧客装置５Ｃ、開発装置６Ｂ、及び管理装置３が実行する処理と記載する。

【０１３４】

実施形態４の処理システム６００は、実施形態３の処理システム５００で実行される処理のＳ１２７、Ｓ３０１、Ｓ３０２に代えて、下記で説明するＳ４０１からＳ４０６が追加された処理である。以下の説明では、Ｓ４０１からＳ４０６の処理を説明し、その他の処理の説明を省略する。

【０１３５】

顧客装置５Ｃは、例えば、ユーザにより処理装置９が接続される（Ｓ２０２）と、処理装置９からライセンス情報２１を取得し、取得したライセンス情報２１に含まれる電子署名を検証する（Ｓ２０３）。顧客装置５Ｃは、電子署名が承認できないとき、処理を終了する。

【０１３６】

顧客装置５Ｃは、電子署名を承認すると、処理装置９に層情報１４１を除く暗号化学習済みモデルを出力する（Ｓ４０１）。これにより、顧客装置５Ｃは、処理装置９に層情報１４１を除く暗号化学習済みモデルを復号させる。

【０１３７】

顧客装置５Ｃは、処理装置８から復号された層情報１４１を除く学習済みモデルを取得する（Ｓ４０２）。顧客装置５Ｃは、暗号化学習済みモデルの情報を出力する機能を停止する（Ｓ１２６）。

【０１３８】

顧客装置５Ｃは、層情報１４１を除く学習済みモデルを用いて、層情報１４１の前段の層までの推論処理を実行する（Ｓ４０３）。そして、顧客装置５Ｃは、処理装置９に層情報１４１の前段の層までの演算結果を処理装置９に出力する（Ｓ４０４）。これにより、顧客装置５Ｃは、処理装置９に層情報１４１の演算を実行させる。

【０１３９】

顧客装置５Ｃは、層情報１４１の演算結果を処理装置９から取得する（Ｓ４０５）。顧客装置５Ｃは、層情報１４１の演算結果を用いて、層情報１４１の後段の層から出力層までの演算を実行する（Ｓ４０６）。

【０１４０】

以上のように、実施形態４の顧客装置５Ｃは、処理装置９に推論処理の演算の一部を実行させるため、処理装置９から一部の層のネットワーク構造と、重みと、バイアスとを含む情報を出力することなく推論処理の実行を可能にする。したがって、顧客装置５Ｃは、学習済みモデルに含まれるネットワーク構造及び重みの漏洩を防止することができる。

【０１４１】

また、実施形態４の処理装置９は、ニューラルネットワークに含まれる連続する３層以上に対応する層情報１４１の演算を内部で実行する。したがって、顧客装置５Ｃは、層７３０の少なくとも１以上の層の入出力の情報を隠した状態で推論処理が実行可能になる。これにより、顧客装置５Ｃは、学習済みモデルに含まれるネットワーク構造及び重みの漏洩を防止することができる。

【０１４２】

上述の説明において、顧客装置５Ｃは、層情報１４１を除く暗号化学習済みモデルを処理装置９に復号させているが、復号部８３が層情報１４１を除く暗号化学習済みモデルを復号してもよい。この場合には、推論部８８は、復号部８３で復号された層情報１４１を除く学習済みモデルを用いて、推論処理を実行する。

【０１４３】

上述の説明において、顧客装置５Ｃは、層情報１４１を除く暗号化学習済みモデルを取得しているが、取得部８６は、層情報１４１を除く学習済みモデルを取得してもよい。この場合には、推論部８８は、層情報１４１を除く学習済みモデルが入力されたとき、層情報１４１を除く学習済みモデルを用いて第１演算を実行し、かつ処理装置９に層情報１４１を用いて第２演算を実行させることにより推論をする。

【０１４４】

上述の説明において、処理装置９は、ニューラルネットワークに含まれる連続する３層以上の演算を実行しているが、これに限らず、ニューラルネットワークに含まれる任意の１層以上の演算を実行してもよい。これにより、処理装置９は、演算能力に応じた量の演算を実行することができるので、処理装置９の演算速度に起因する推論処理の速度の低下を抑制することができる。

【０１４５】

実施形態４の処理システム６００では、学習済みモデルの開発者が学習済みモデルを用いるアプリケーションを作成するものとして説明したが、アプリケーションは、学習済みモデルの開発者とは別のアプリ開発者が作成してもよい。この場合において、暗号化学習済みモデルは、アプリ開発者を介して、学習済みモデルの開発者から顧客に提供されてもよい。

【０１４６】

暗号化学習済みモデルを、アプリ開発者を介して顧客に提供する場合においても、難読化共通鍵の復号は、推論ＤＬＬ内で難読化共通鍵を生成したときと逆の演算をすることにより、自動的に行なわれる。すなわち、アプリ開発者及び顧客は、学習済みモデルの内容を知ることなくアプリケーションの開発及び利用をする。これにより、処理システム６００において、学習済みモデルの内容は、学習済みモデルの開発者以外に知られることなく利用される。以上により、処理システム６００は、学習済みモデルを無断で流用されるなどのリスクを抑制して、学習済みモデルの開発者と、アプリ開発者との協業を促進すること

ができる。
【０１４７】
図３０は、コンピュータ装置の一実施例を示すブロック図である。
図３０を参照して、コンピュータ装置８００の構成について説明する。
図３０において、コンピュータ装置８００は、制御回路８０１と、記憶装置８０２と、読書装置８０３と、記録媒体８０４と、通信インターフェイス８０５と、入出力インターフェイス８０６と、入力装置８０７と、表示装置８０８とを含む。また、通信インターフェイス８０５は、ネットワーク８０９と接続される。そして、各構成要素は、バス８１０により接続される。顧客装置１、５Ａ、５Ｂ、５Ｃと、開発装置２、６Ａ、６Ｂと、管理装置３と、処理装置７、８，９とは、コンピュータ装置８００に記載の構成要素の一部または全てを適宜選択して構成することができる。
【０１４８】
制御回路８０１は、コンピュータ装置８００全体の制御をする。そして、制御回路８０１は、例えば、Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ（ＣＰＵ）、及びＦｉｅｌｄ　Ｐｒｏｇｒａｍｍａｂｌｅ　Ｇａｔｅ　Ａｒｒａｙ（ＦＰＧＡ）などのプロセッサである。そして、制御回路８０１は、例えば、上述した各装置の制御部として機能する。
【０１４９】
記憶装置８０２は、各種データを記憶する。そして、記憶装置８０２は、例えば、Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ（ＲＯＭ）及びＲａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ（ＲＡＭ）、及びＨａｒｄ　Ｄｉｓｋ（ＨＤ）などである。記憶装置８０２は、例えば、上述した各装置の記憶部として機能する。
【０１５０】
また、ＲＯＭは、ブートプログラムなどのプログラムを記憶している。ＲＡＭは、制御回路８０１のワークエリアとして使用される。ＨＤは、ＯＳ、アプリケーションプログラム、ファームウェアなどのプログラム、及び各種データを記憶している。記憶装置８０２は、制御回路８０１を、上述した各装置の制御部として機能させるプログラムを記憶してもよい。上述した各装置の制御部として機能させるプログラムとは、例えば、上述したフレームワーク、暗号化ツール、推論ＤＬＬ、及びアプリケーションなどである。そして、フレームワーク、暗号化ツール、推論ＤＬＬ、及びアプリケーションのそれぞれは、制御回路８０１を上述した各装置の制御部として機能させるプログラムの全てまたは一部を含んでもよい。
【０１５１】
なお、上述の各プログラムは、制御回路８０１が通信インターフェイス８０５を介してアクセス可能であれば、ネットワーク８０９上のサーバが有する記憶装置に記憶されていても良い。
【０１５２】
読書装置８０３は、制御回路８０１に制御され、着脱可能な記録媒体８０４のデータのリード／ライトを行なう。そして、読書装置８０３は、例えば、各種Ｄｉｓｋ　Ｄｒｉｖｅ（ＤＤ）及びＵｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ（ＵＳＢ）などである。
【０１５３】
記録媒体８０４は、各種データを保存する。記録媒体８０４は、例えば、上述した各装置の制御部として機能させるプログラムを記憶する。さらに、記録媒体８０４は、図１、図１３、図１９に示す、推論情報４ａ、及び図２４に示す、推論情報４ｂの少なくとも一つを記憶しても良い。そして、記録媒体８０４は、読書装置８０３を介してバス８１０に接続され、制御回路８０１が読書装置８０３を制御することにより、データのリード／ライトが行なわれる。
【０１５４】
また、記録媒体８０４は、例えば、ＳＤ　Ｍｅｍｏｒｙ　Ｃａｒｄ（ＳＤメモリーカード）、Ｆｌｏｐｐｙ　Ｄｉｓｋ（ＦＤ）、Ｃｏｍｐａｃｔ　Ｄｉｓｃ（ＣＤ）、Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｋ（ＤＶＤ）、Ｂｌｕ－ｒａｙ（登録商標）　Ｄｉｓｋ（ＢＤ

）、及びフラッシュメモリなどの非一時的記録媒体である。
【０１５５】
通信インターフェイス８０５は、ネットワーク８０９を介してコンピュータ装置８００と他の装置とを通信可能に接続する。また、通信インターフェイス８０５は、無線ＬＡＮの機能を有するインターフェイス、及び近距離無線通信機能を有するインターフェイスを含んでも良い。ＬＡＮは、Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋの略である。
【０１５６】
入出力インターフェイス８０６は、例えば、キーボード、マウス、及びタッチパネルなどの入力装置８０７と接続され、接続された入力装置８０７から各種情報を示す信号が入力されると、バス８１０を介して入力された信号を制御回路８０１に出力する。また、入出力インターフェイス８０６は、制御回路８０１から出力された各種情報を示す信号がバス８１０を介して入力されると、接続された各種装置にその信号を出力する。
入力装置８０７は、例えば、学習用のフレームワークのハイパーパラメータの設定の入力を受け付けても良い。
【０１５７】
表示装置８０８は、各種情報を表示する。表示装置８０８は、タッチパネルでの入力を受け付けるための情報を表示しても良い。表示装置８０８は、例えば、顧客装置１、５Ａ、５Ｂ、５Ｃに接続される、表示装置３０として機能する。
入出力インターフェイス８０６、入力装置８０７、及び表示装置８０８は、ＧＵＩとして機能してもよい。
ネットワーク８０９は、例えば、ＬＡＮ、無線通信、またはインターネットなどであり、コンピュータ装置８００と他の装置を通信接続する。
【０１５８】
なお、本実施形態は、以上に述べた実施形態に限定されるものではなく、本実施形態の要旨を逸脱しない範囲内で種々の構成または実施形態を取ることができる。
以下の説明では、顧客装置１、５Ａ、５Ｂ、５Ｃのことを特に区別しないとき、単に顧客装置ともいう。また、開発装置２、６Ａ、６Ｂのことを特に区別しないとき、単に開発装置ともいう。さらに、管理装置３のことを、単に管理装置ともいう。そして、保存装置４のことを、単に保存装置ともいう。また、処理装置７、８，９のことを特に区別しないとき、単に処理装置ともいう。
【０１５９】
実施形態１から実施形態４において、共通鍵は、難読化して顧客装置に提供されるものとして説明したが、管理装置で生成された秘密鍵と公開鍵とを用いて顧客装置に提供されてもよい。
【０１６０】
後述する図３１の構成に対応する第１の例として、管理装置は、第１生成部により、第１秘密鍵と、第１秘密鍵に対応する第１公開鍵とを生成する。開発装置は、学習部により、学習済みモデルの重みを調整する学習をする。また、開発装置は、第２生成部により、第２秘密鍵と、第１公開鍵と第２秘密鍵とを用いる共通鍵と、第２秘密鍵に対応する第２公開鍵とを生成する。そして、開発装置は、第２生成部で生成された共通鍵を用いて学習済みモデルを暗号化する。
【０１６１】
顧客装置は、判定部により、暗号化学習済みモデルが入力されたか否かを判定する。また、顧客装置は、図示しない第３生成部により、第１秘密鍵と第２公開鍵とを用いて共通鍵を生成する。顧客装置は、学習済みモデルが入力されたとき、復号部により、第３生成部で生成された共通鍵を用いて学習済みモデルを復号する。そして、顧客装置は、推論部により、復号部により復号された学習済みモデルを用いて推論をする。なお、第３生成部は、例えば、顧客装置の制御部に含まれる。
【０１６２】
図３１は、ＤＨ鍵交換を用いた処理システムの一実施例を示す図である。

図３１を参照して、ＤＨ鍵交換（Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ鍵交換）を用いた共通鍵の提供処理を説明する。以下の説明において、生成元ｇと素数ｎとは、管理装置が設定したあと、開発装置と顧客装置とにそれぞれ共有されているものとして説明する。暗号化ツール及び推論ＤＬＬは、それぞれ、破線で囲まれる情報を含み、破線で囲まれる処理を実行するものとする。また、アプリ開発装置は、アプリ開発者が利用する情報処理装置であり、例えば、上述した図３０に示すコンピュータ装置である。なお、アプリ開発者とは、アプリケーションを開発する開発者のことである。アプリケーションとは、例えば、開発装置で開発された学習済みモデルを用いて、推論処理を実行するソフトウェアのことである。

【０１６３】

管理装置は、秘密鍵ｓを生成して、推論ＤＬＬに秘密鍵ｓを付与する（Ｓ１１）。Ｓ１１において、管理装置は、さらに、推論ＤＬＬに生成元ｇと素数ｎとを付与することにより、生成元ｇ及び素数ｎを顧客装置と共有してもよい。以下の説明では、管理装置が、推論ＤＬＬに生成元ｇと素数ｎとを付与したものとして説明する。

さらに、管理装置は、生成元ｇと素数ｎとを設定し、下記式（１）に生成元ｇと、素数ｎと、秘密鍵ｓとを代入して、公開鍵ａを求める（Ｓ１２）。

公開鍵$a = g^{s} \bmod n$・・・（１）

【０１６４】

そして、管理装置は、暗号化ツールに公開鍵ａを付与する（Ｓ１３）。Ｓ１３において、管理装置は、さらに、暗号化ツールに生成元ｇと素数ｎとを付与することにより、生成元ｇと素数ｎとを開発装置と共有してもよい。以下の説明では、管理装置が、暗号化ツールに生成元ｇと素数ｎとを付与したものとして説明する。

【０１６５】

開発装置は、暗号化ツールを実行することにより、秘密鍵ｐを生成し、暗号化ツールに付与されている公開鍵ａと、秘密鍵ｐとを下記式（２）に代入して、共通鍵ｄｈを求める（Ｓ１４）。

共通鍵$dh = a^{p} \bmod n$・・・（２）

そして、開発装置は、共通鍵ｄｈを用いて、学習済みモデルを暗号化する（Ｓ１５）。

さらに、開発装置は、暗号化ツールに付与されている生成元ｇ及び素数ｎと、秘密鍵ｐとを下記式（３）に代入して、公開鍵ｂを求める（Ｓ１６）。

公開鍵$b = g^{p} \bmod n$・・・（３）

【０１６６】

アプリ開発装置は、開発装置から暗号化学習済みモデルと公開鍵ｂとを取得し、学習済みモデルを用いて推論処理を実行するアプリケーションを作成する。以下の説明では暗号化学習済みモデルと公開鍵ｂとは、アプリ開発者から顧客にアプリケーションとともに提供されるものとして説明するが、暗号化学習済みモデルと公開鍵ｂとは学習済みモデルの開発者から顧客に直接提供されてもよい。

【０１６７】

また、図３３に示すように、公開鍵ｂは、開発装置により、暗号化学習済みモデルに付与される暗号化ヘッダに格納されて、顧客に提供されてもよい。さらに、暗号化ヘッダには、例えば、ライセンス情報２１に含まれるプロダクト名と、暗号化共通鍵と、顧客名と、有効期限と、機器識別子と、電子署名と、著作者情報との少なくとも一つを格納してもよい。さらに、暗号化ヘッダには、暗号化識別子を格納してもよい。この場合には、暗号化ヘッダに含まれる情報は、ライセンスファイルまたはドングルに代えて、暗号化ヘッダを媒体として顧客に提供される。なお、著作者情報とは、例えば、学習済みモデルの開発者を識別する情報である。また、実施形態１から実施形態４においても、ライセンスファイルに代えて、ライセンス情報２１に含まれる情報の少なくとも一つを暗号化ヘッダに格納してもよい。この場合にも、暗号化ヘッダに含まれる情報は、ライセンスファイルまたはドングルに代えて、暗号化ヘッダを媒体として顧客に提供される。

【０１６８】

顧客装置は、公開鍵ｂが入力されると、推論ＤＬＬに付与されている秘密鍵ｓ、生成元ｇ及び素数ｎと、公開鍵ｂとを下記式（４）に代入して、共通鍵ｄｈを求める。
共通鍵ｄｈ＝ｂｓｍｏｄ　ｎ・・・（４）
そして、顧客装置は、暗号化学習済みモデルが入力されると、共通鍵を用いて暗号化学習済みモデルを復号して、学習済みモデルを得る。

【０１６９】

後述する図３２の構成に対応する第２の例として、管理装置は、第１生成部により、秘密鍵と、秘密鍵に対応する公開鍵とを生成する。開発装置は、学習部により、学習済みモデルの重みを調整する。また、開発装置は、第２生成部により、共通鍵を生成する。そして、開発装置は、暗号化部により、公開鍵を用いて共通鍵を暗号化し、共通鍵を用いて学習済みモデルを暗号化する。

【０１７０】

顧客装置は、判定部により、暗号化学習済みモデルが入力されたか否かを判定する。また、顧客装置は、復号部により、秘密鍵を用いて開発装置の暗号化部により暗号化された暗号化共通鍵を復号し、復号した共通鍵を用いて暗号化学習済みモデルを復号する。そして、顧客装置は、推論部により、復号部により復号された学習済みモデルを用いて推論をする。

【０１７１】

図３２は、公開鍵暗号方式を用いた暗号処理システムの一実施例を示す図である。
図３２を参照して、公開鍵暗号方式を用いた共通鍵の提供処理を説明する。暗号化ツール及び推論ＤＬＬは、それぞれ、破線で囲まれる情報を含み、破線で囲まれる処理を実行するものとする。

【０１７２】

管理装置は、秘密鍵ｘを生成して、推論ＤＬＬに秘密鍵ｘを付与する（Ｓ２１）。また、管理装置は、秘密鍵ｘを用いて、秘密鍵ｘに対応する公開鍵ｙを生成し、暗号化ツールに公開鍵ｙを付与する（Ｓ２２）。

【０１７３】

開発装置は、共通鍵ｚを設定し、共通鍵ｚを用いて、学習済みモデルを暗号化する（Ｓ２３）。また、開発装置は、暗号化ツールに付与されている公開鍵ｙを用いて、共通鍵ｚを暗号化する（Ｓ２４）。

【０１７４】

アプリ開発装置は、開発装置から暗号化学習済みモデルと、暗号化共通鍵ｅｚとを取得し、学習済みモデルを用いて推論処理を実行するアプリケーションを作成する。以下の説明では、暗号化学習済みモデルと暗号化共通鍵ｅｚとは、アプリ開発者から顧客にアプリケーションとともに提供されるものとして説明するが、暗号化学習済みモデルと暗号化共通鍵ｅｚとは学習済みモデルの開発者から顧客に直接提供されてもよい。

【０１７５】

また、図３３に示すように、公開鍵ｅｚは、開発装置により、暗号化学習済みモデルに付与される暗号化ヘッダに格納されて、顧客に提供されてもよい。さらに、暗号化ヘッダには、例えば、ライセンス情報２１に含まれるプロダクト名と、暗号化共通鍵と、顧客名と、有効期限と、機器識別子と、電子署名と、著作者情報との少なくとも一つを格納してもよい。さらに、暗号化ヘッダには、暗号化識別子を格納してもよい。この場合には、暗号化ヘッダに含まれる情報は、ライセンスファイルまたはドングルに代えて、暗号化ヘッダを媒体として顧客に提供される。

【０１７６】

顧客装置は、暗号化共通鍵ｅｚが入力されると、推論ＤＬＬに付与されている秘密鍵ｘを用いて暗号化共通鍵ｅｚを復号し、共通鍵ｚを得る。そして、顧客装置は、暗号化学習済みモデルが入力されると、共通鍵ｚを用いて暗号化学習済みモデルを復号して、学習済みモデルを得る。

【０１７７】

以上の構成により、推論ＤＬＬに含まれる秘密鍵が流出しない限り、暗号化共通鍵が復号されることがないので、共通鍵の漏洩を防止することができる。
また、暗号化共通鍵の復号は、推論ＤＬＬ内で秘密鍵を用いて自動的に行なわれる。すなわち、アプリ開発者及び顧客は、学習済みモデルの内容を知ることなくアプリケーションの開発及び利用をする。これにより、図３１、図３２に示す処理システムにおいて、学習済みモデルの内容は、学習済みモデルの開発者以外に知られることなく利用される。以上により、図３１、図３２に示す処理システムは、学習済みモデルを無断で流用されるなどのリスクを抑制して、学習済みモデルの開発者と、アプリ開発者との協業を促進することができる。

【０１７８】

なお、上記の説明では、図３１、図３２に示す処理システムで得られる効果を具体的にするため、アプリ開発者は、学習済みモデルの開発者とは別の開発者であるものとして説明したが、アプリ開発者と、学習済みモデルの開発者とは、同一の開発者であってもよい。

【０１７９】

図３３は、暗号化学習済みモデルの暗号化ヘッダの一実施例を示す図である。
図３３を参照して、暗号化学習済みモデルの変形例を説明する。
実施形態１から実施形態４において、ライセンス情報２１は、ライセンスファイルまたはドングルに書き込むものとして説明したが、図３３に示すように、学習済みモデルに付与される暗号化ヘッダに格納してもよい。すなわち、ライセンス情報２１に含まれるプロダクト名と、難読化共通鍵と、顧客名と、有効期限と、機器識別子と、電子署名と、暗号化識別子と、著作者情報との少なくとも一つを学習済みモデルに付与する暗号化ヘッダに含ませてもよい。

【０１８０】

より具体的には、開発装置は、暗号化学習済みモデルに付与される暗号化ヘッダにライセンス情報２１と、暗号化識別子とを格納して、保存装置に保存する。そして、顧客装置は、開発装置に暗号化学習済みモデルの取得要求をする。開発装置は、取得要求に応じて、保存装置に保存した暗号化学習済みモデルを顧客装置に提供する。このとき、開発装置は、暗号化ヘッダに格納されている有効期限と、電子署名とを書き換えてもよい。なお、処理システムにおいて、保存装置が有効期限と、電子署名との書き換えを実行してもよい。この場合には、保存装置は、顧客装置からの暗号化学習済みモデルの取得要求を受け付け、暗号化ヘッダに格納されている有効期限と、電子署名とを書き換えて、暗号化学習済みモデルを顧客装置に提供してもよい。

【０１８１】

以上の構成により、実施形態の処理システムは、顧客装置の取得要求に応じた有効期限を、顧客装置が暗号化学習済みモデルを取得するときに設定することができる。これにより、実施形態の処理システムは、学習済みモデルの配信サービスに適した運用が可能となる。なお、学習済みモデルの配信サービスにおいて、顧客装置による暗号化学習済みモデルの取得は、例えば、開発装置を介して行われてもよいし、保存装置から暗号化学習済みモデルを直接ダウンロードすることにより行われてもよい。

【符号の説明】

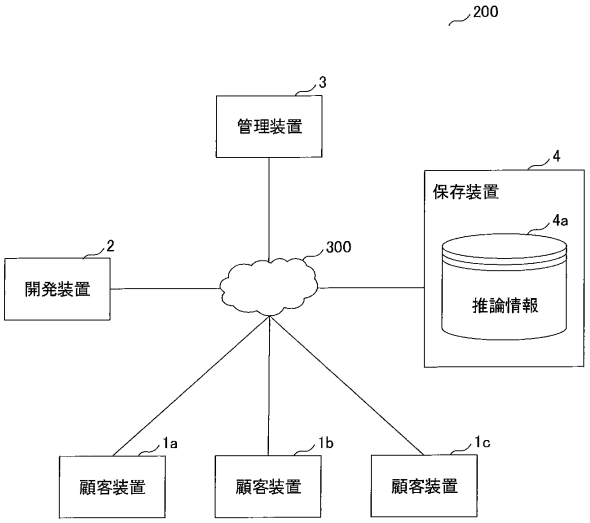
【０１８２】

１、５Ａ、５Ｂ、５Ｃ　顧客装置
２、６Ａ、６Ｂ　開発装置
３　管理装置
４　保存装置
７、８，９　処理装置
８００　コンピュータ装置
８０１　制御回路
８０２　記憶装置
８０３　読書装置

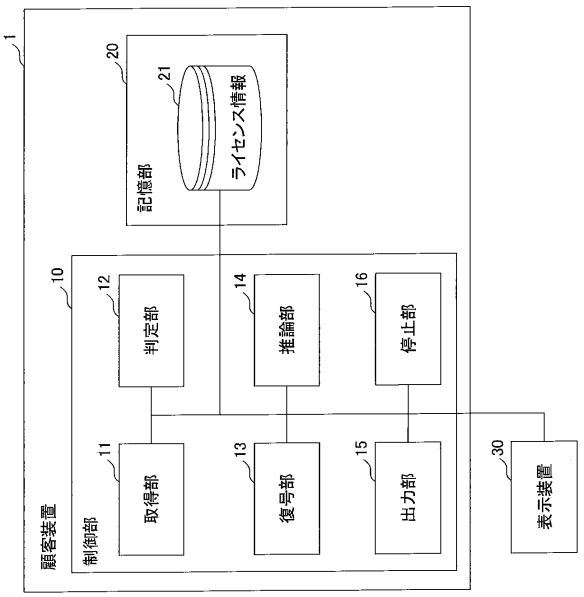
８０４　　記録媒体
８０５　　通信Ｉ/Ｆ
８０６　　入出力Ｉ/Ｆ
８０７　　入力装置
８０８　　表示装置
８０９　　ネットワーク
８１０　　バス

【図面】

【図１】



【図２】

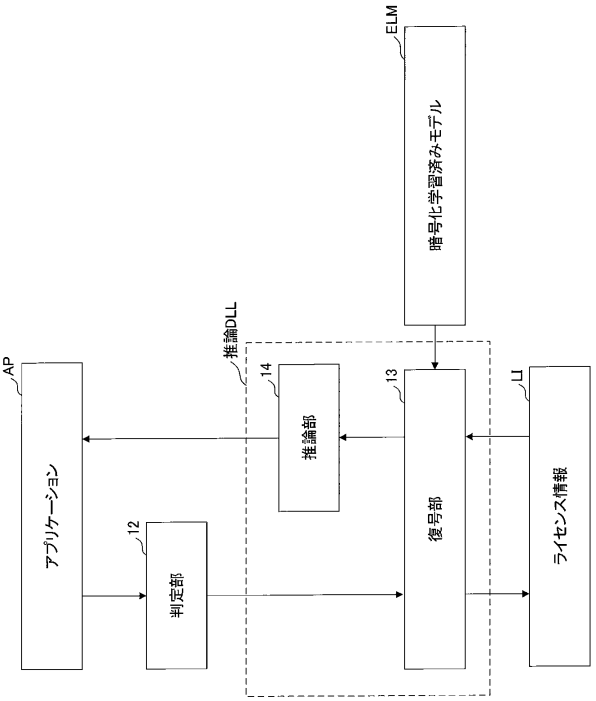


【図３】

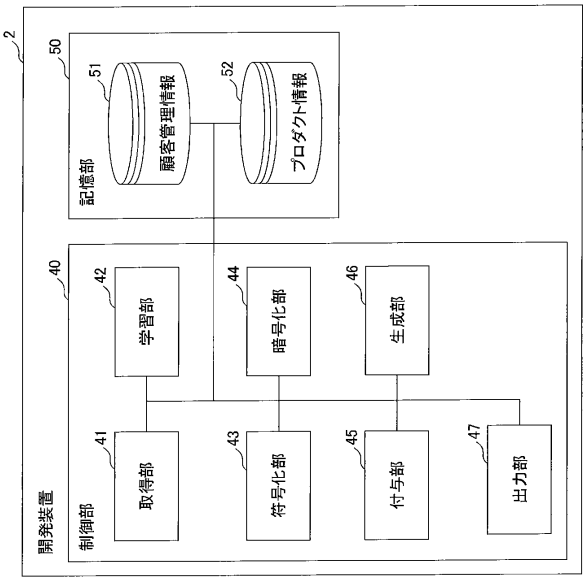
21

プロダクト名	難読化共通鍵	顧客名	有効期限	機器識別子	電子署名
PRODUCT0	EK1	A	20xx/aa/bb	a	EA

【図４】



【図５】



【図６】

51

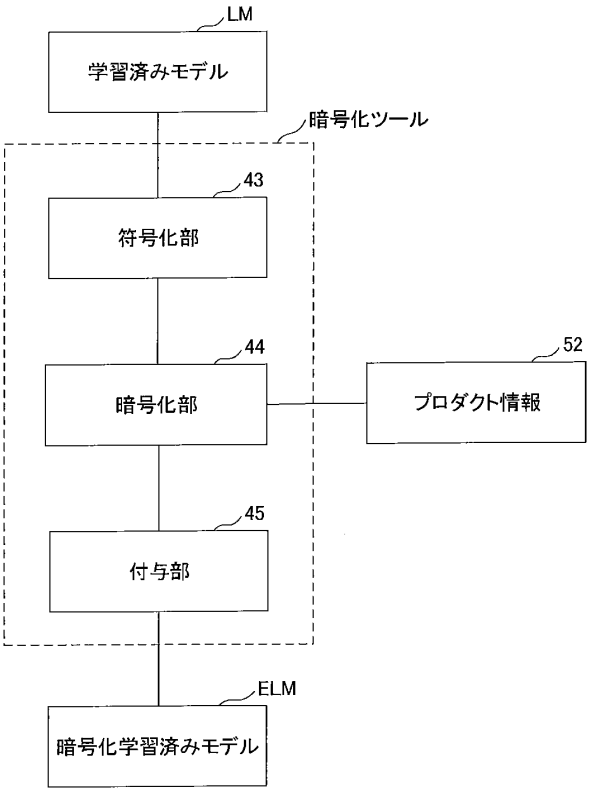
プロダクト名	顧客名	有効期限	機器識別子
PRODUCT0	A	20xx/aa/bb	a
PRODUCT1	B	20yy/cc/dd	b
PRODUCT2	C	20zz/ee/ff	c
PRODUCT3	D	20vv/gg/hh	d

【図７】

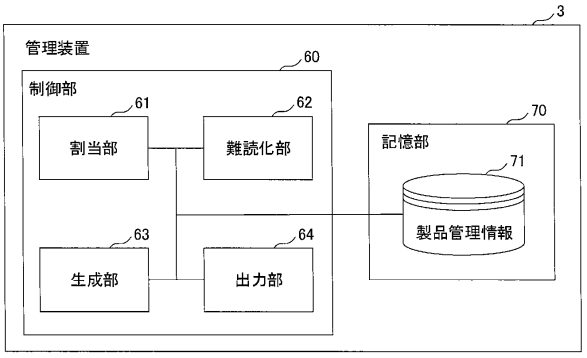
52

プロダクト名	開発者名	難読化共通鍵
PRODUCT0	E	EK1

【図８】



【図９】

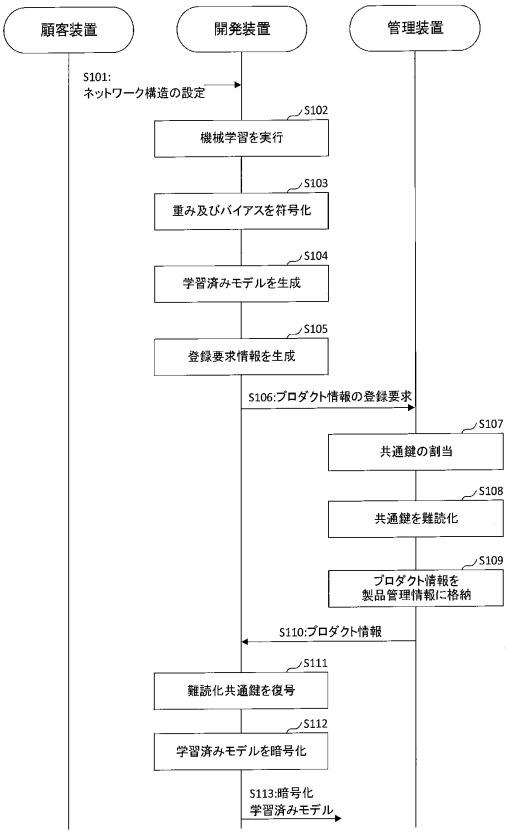


【図１０】

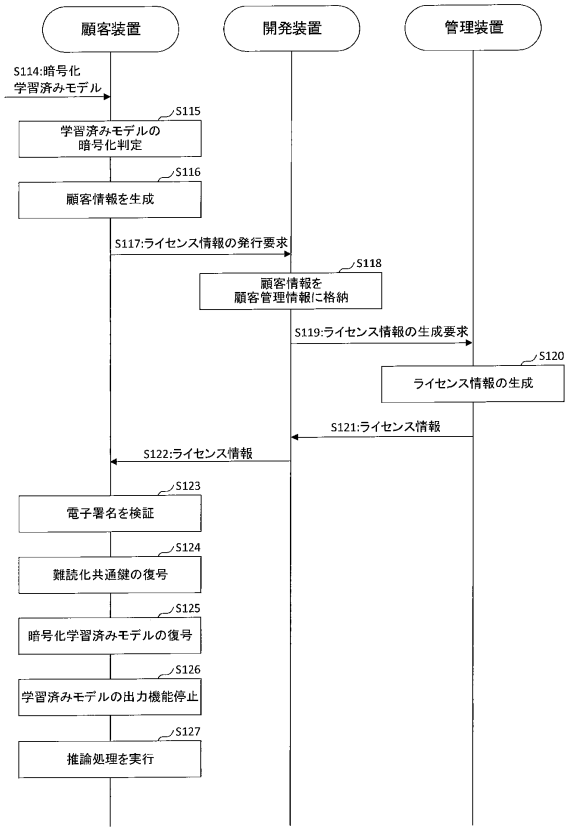
71

プロダクト名	開発者名	難読化共通鍵
PRODUCT0	E	K1
PRODUCT1	F	K2
PRODUCT2	G	K3
PRODUCT3	H	K4

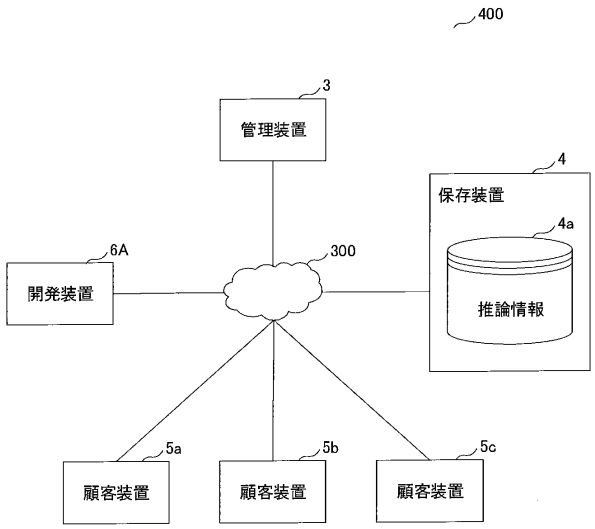
【図１１】



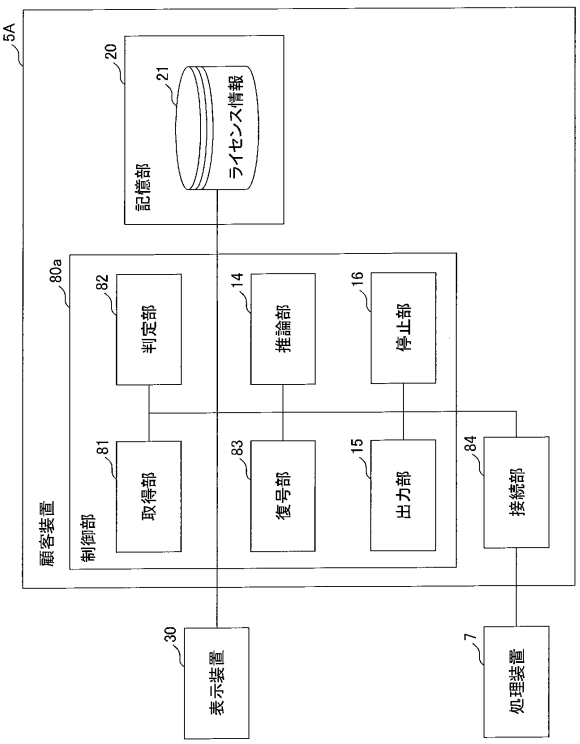
【図１２】



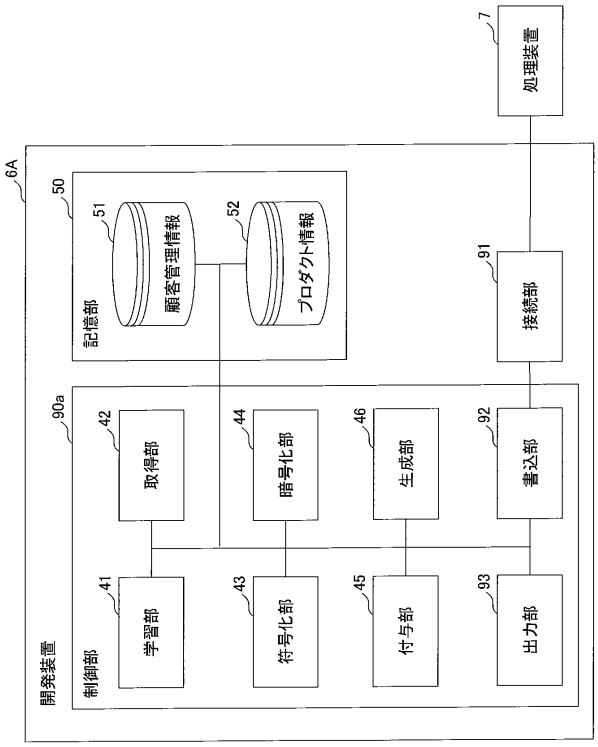
【図１３】



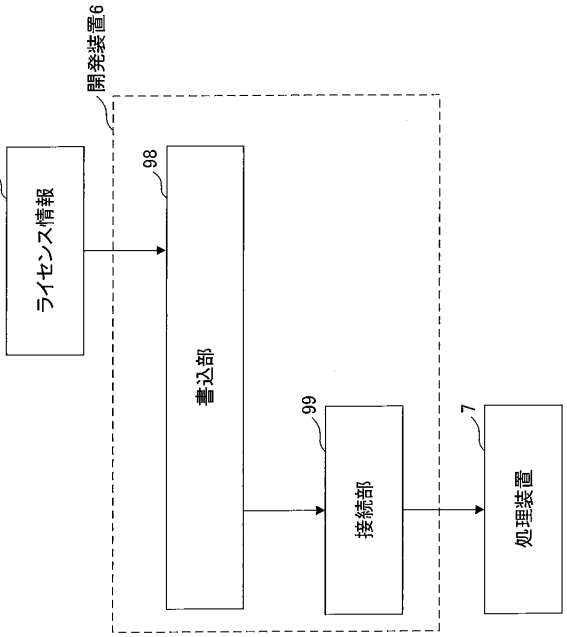
【図１４】



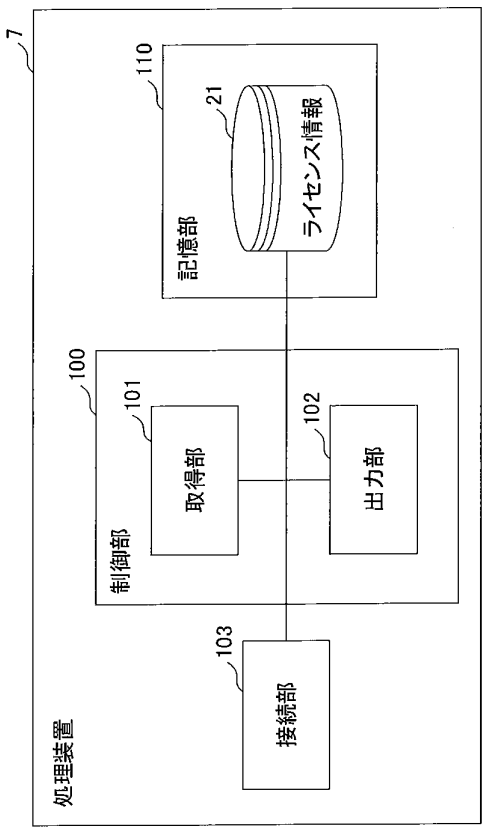
【図１５】



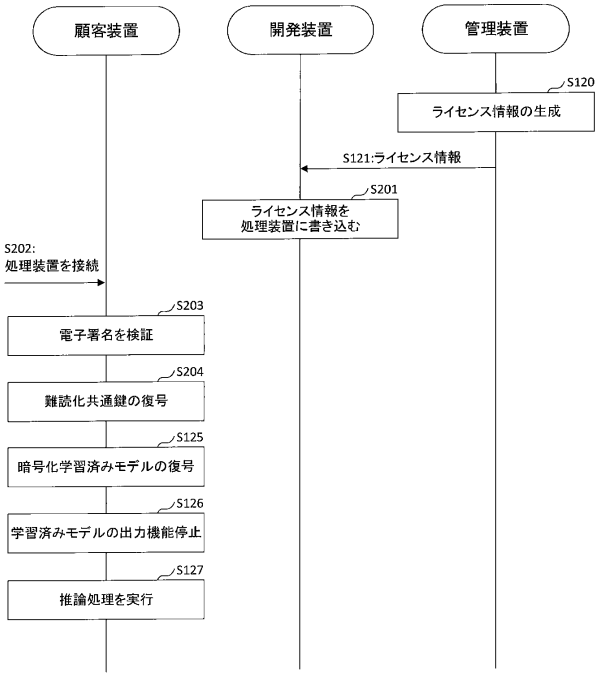
【図１６】



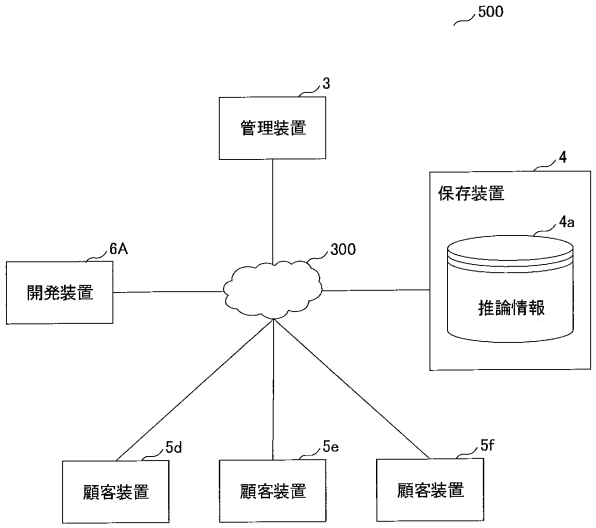
【図１７】



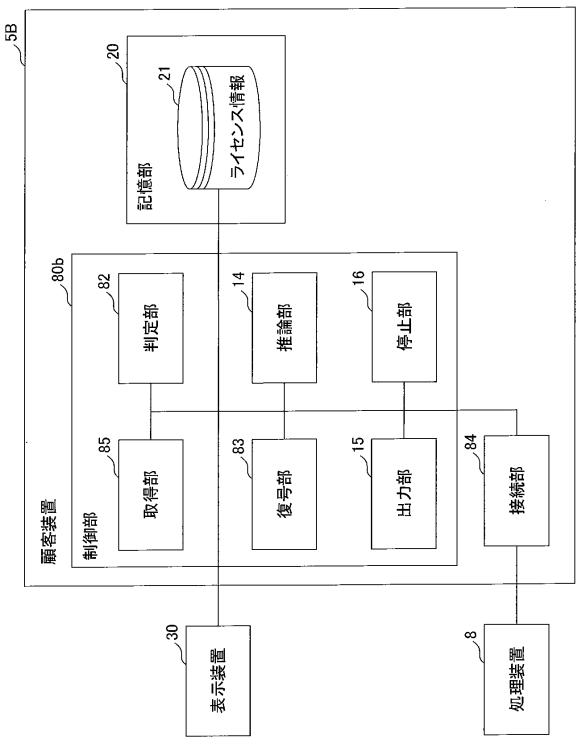
【図１８】



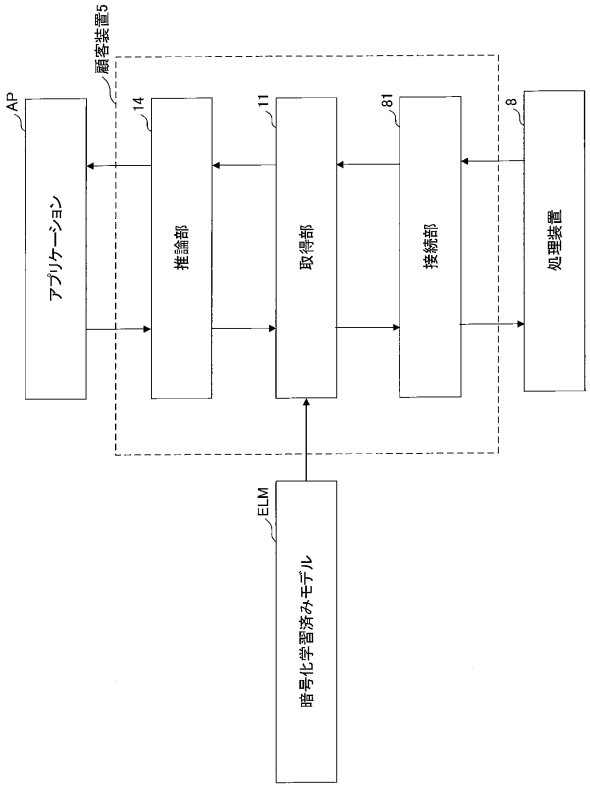
【図１９】



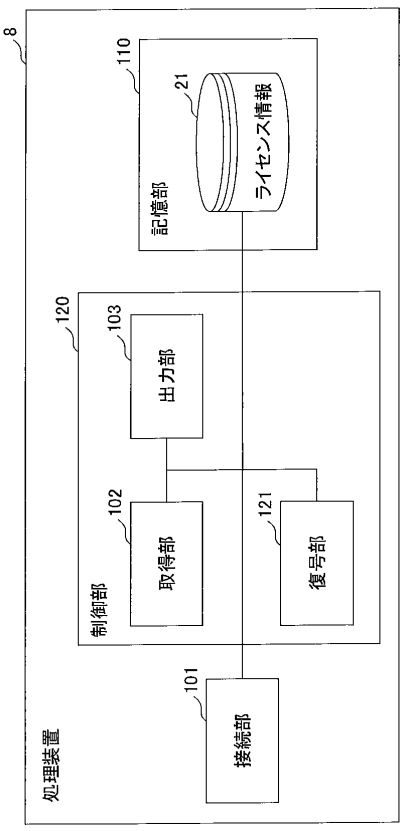
【図２０】



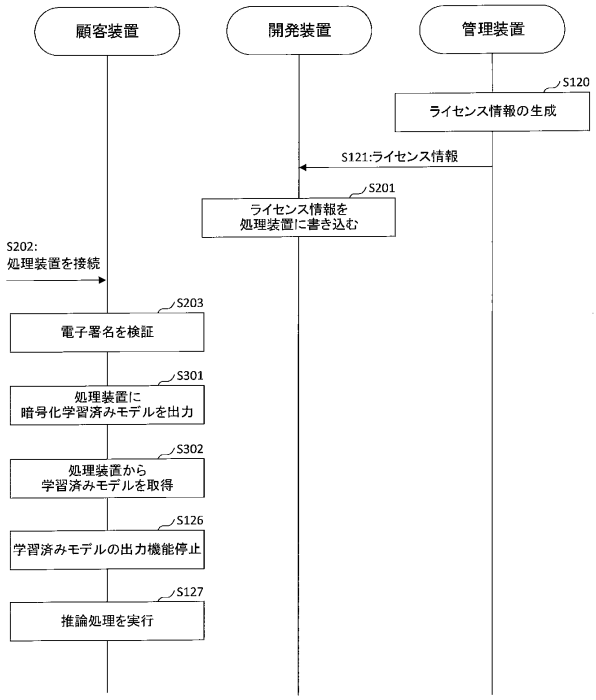
【図２１】



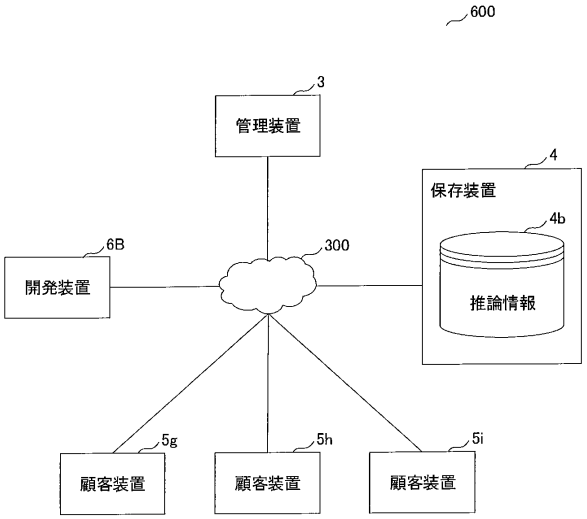
【図２２】



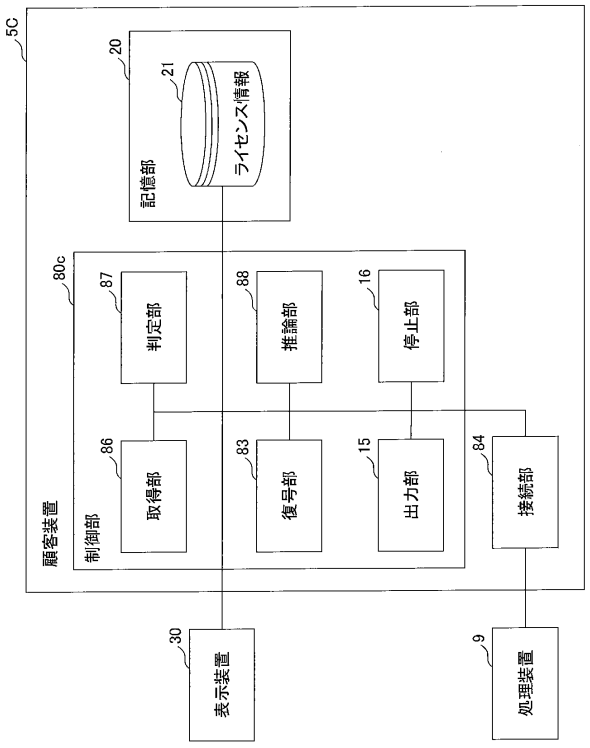
【図２３】



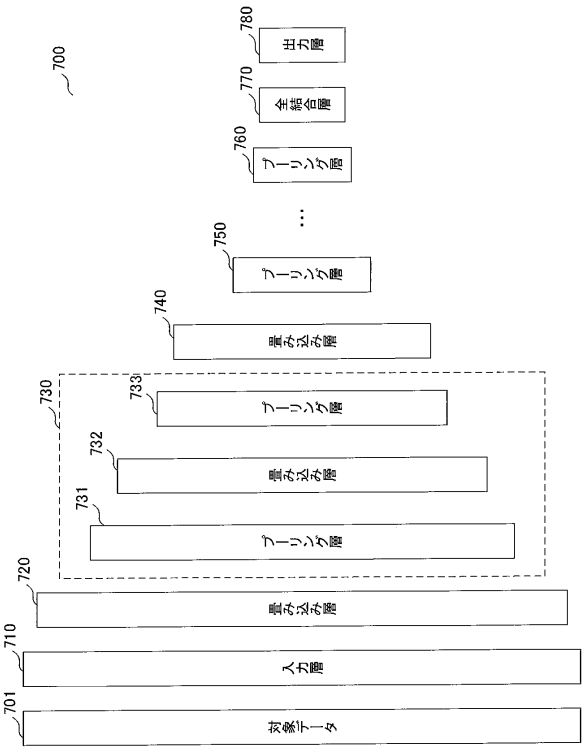
【図２４】



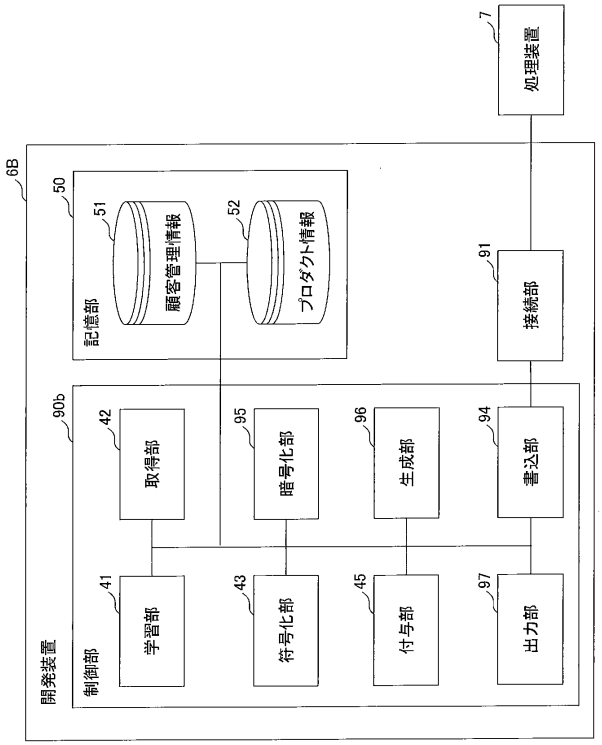
【図２５】



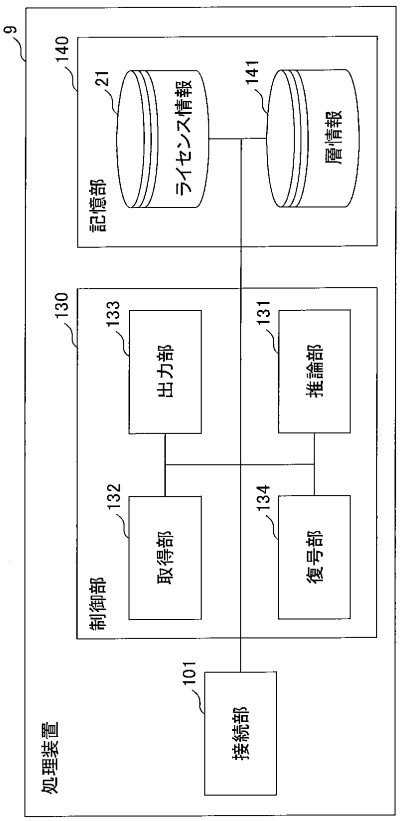
【図２６】



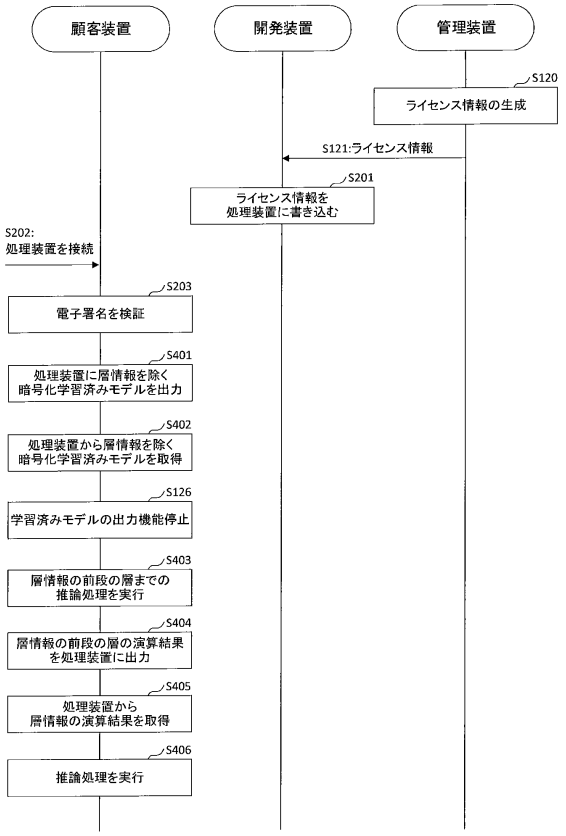
【図２７】



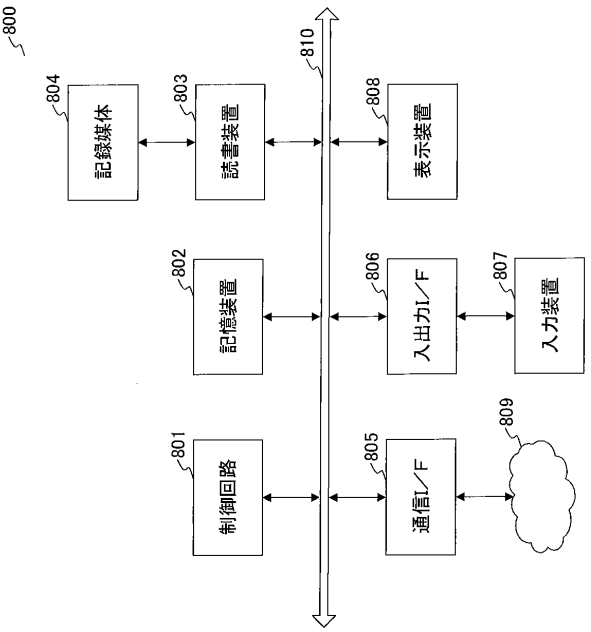
【図２８】



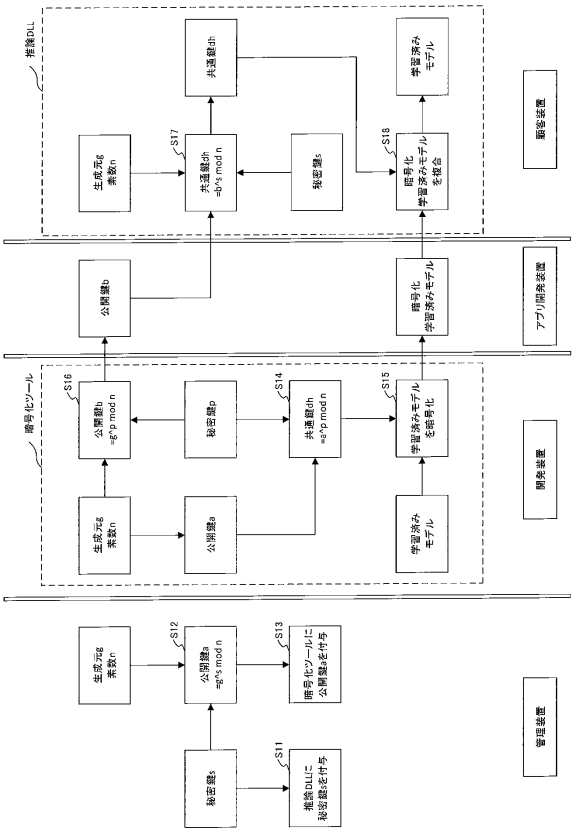
【図２９】



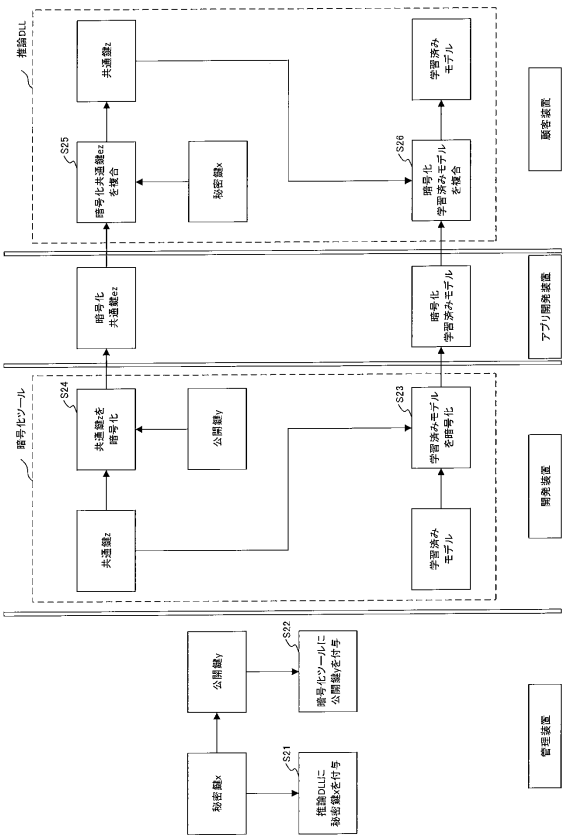
【図３０】



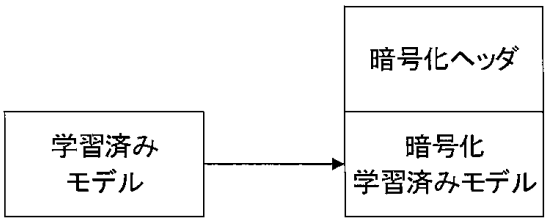
【図３１】


推論DLL
生成元g
素数n
共通鍵dh
S17
共通鍵dh
=b^s mod n
秘密鍵s
S16
暗号化
学習済みモデル
を複合
学習済み
モデル
顧客装置
公開鍵b
暗号化
学習済みモデル
アプリ開発装置
暗号化ツール
S16
公開鍵b
=g^b mod n
秘密鍵b
S14
共通鍵dh
=a^b mod n
S15
学習済みモデル
を暗号化
生成元g
素数n
公開鍵a
学習済み
モデル
開発装置
生成元g
素数n
S12
公開鍵a
=g^s mod n
S13
暗号化ツールに
公開鍵aを付与
秘密鍵s
S11
推論DLLに
秘密鍵sを付与
管理装置

【図３２】


推論DLL
共通鍵z
S25
暗号化共通鍵ez
を複合
秘密鍵x
S26
暗号化
学習済みモデル
を複合
学習済み
モデル
顧客装置
暗号化
共通鍵ez
暗号化
学習済みモデル
アプリ開発装置
暗号化ツール
S24
共通鍵zを
暗号化
公開鍵y
S23
学習済みモデル
を暗号化
共通鍵z
学習済み
モデル
開発装置
公開鍵y
S22
暗号化ツールに
公開鍵yを付与
秘密鍵x
S21
推論DLLに
秘密鍵xを付与
管理装置

【図３３】


学習済み
モデル
暗号化ヘッダ
暗号化
学習済みモデル

フロントページの続き

(56)参考文献 特開平０７－２７１５９４（ＪＰ，Ａ）
特開平１０－１５４９７６（ＪＰ，Ａ）
特開平１１－０３１１３１（ＪＰ，Ａ）
特開２００２－０２６８９２（ＪＰ，Ａ）
特開２００４－２８２７１７（ＪＰ，Ａ）
国際公開第２０１６／１９９３３０（WO，Ａ１）
中国特許出願公開第１０８５４０４４４（ＣＮ，Ａ）

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ８／００－８／３８
８／６０－８／７７
９／４４－９／４４５
９／４５１
１２／１４
２１／００－２１／８８
Ｇ０６Ｎ ３／００－３／１２
７／０８－９９／００
Ｇ０９Ｃ １／００－５／００
Ｈ０４Ｋ １／００－３／００
Ｈ０４Ｌ ９／００－９／４０