

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2020年12月24日(24.12.2020)



(10) 国際公開番号

WO 2020/255342 A1

(51) 国際特許分類:
H04L 29/02 (2006.01)

蔵野市緑町三丁目9番11号 NTT 知的財産センタ内 Tokyo (JP).

(21) 国際出願番号: PCT/JP2019/024539

(74) 代理人: 杉村 憲司 (SUGIMURA Kenji);
〒1000013 東京都千代田区霞が関三丁目2番1
号 霞が関コモンゲート西館36階 Tokyo (JP).

(22) 国際出願日: 2019年6月20日(20.06.2019)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

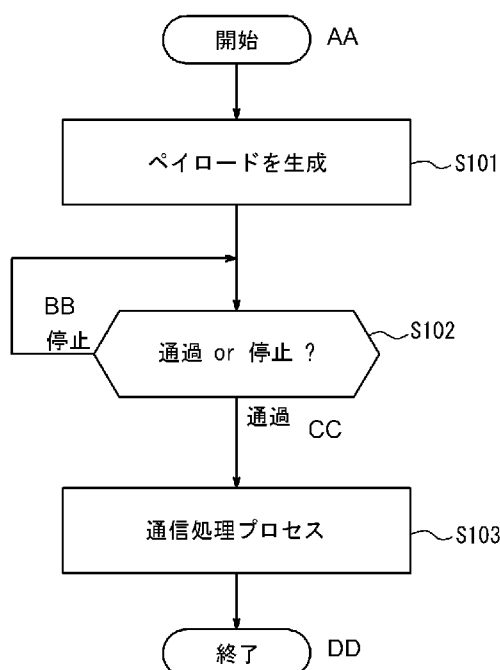
(71) 出願人: 日本電信電話株式会社 (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) [JP/JP]; 〒1008116 東京都千代田区大手町一丁目5番1号 Tokyo (JP).

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,

(72) 発明者: 新井 健一 (ARAI Kenichi); 〒1808585 東京都武蔵野市緑町三丁目9番11号 NTT 知的財産センタ内 Tokyo (JP). 吉田 尊彦 (YOSHIDA Takahiko); 〒1808585 東京都武

(54) Title: TRANSMISSION CONTROL METHOD, AND PROGRAM

(54) 発明の名称: 送信制御方法、およびプログラム



S101 Payload generation
S102 Pass or stop?
S103 Communication processing process
AA Start
BB Stop
CC Pass
DD End

(57) Abstract: Provided is a transmission control method for a transmission device compliant with an OSI reference model. The transmission control method comprises: a generation step S101 of generating a payload in an upper layer; and a communication processing process step S103 of executing or stopping a communication processing process of the payload in a lower layer on the basis of inputted control information.

[続葉有]

SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA,
UG, US, UZ, VC, VN, ZA, ZM, ZW.

- (84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

- 一 国際調査報告(条約第21条(3))

(57) 要約: 送信制御方法は、OSI参照モデルに準拠した送信装置の送信制御方法であって、上位層においてペイロードを生成する生成ステップS101と、入力された制御情報に基づいて、下位層において前記ペイロードの通信処理プロセスを実行又は停止する通信処理プロセスステップS103と、を含む。

明 細 書

発明の名称：送信制御方法、およびプログラム

技術分野

[0001] 本発明は、送信制御方法、およびプログラムに関する。

背景技術

[0002] 従来、国際標準化機構により策定され、異機種間でのデータ通信を実現するための統一規格として、OSI (Open System Interconnection) 参照モデルが知られている。OSI参照モデルは、通信機器における通信機能が、第7層（アプリケーション層）、第6層（プレゼンテーション層）、第5層（セッション層）、第4層（トランスポート層）、第3層（ネットワーク層）、第2層（データリンク層）、第1層（物理層）、という7つの階層構造に分割されたモデルである（例えば、非特許文献1参照）。

[0003] 近年、IoT (Internet of Things) システムの普及に伴って、IoTデバイスがマルウェアに感染するという事象が増加している。IoTデバイスは、CPU (Central Processing Unit) やメモリを搭載し、アプリケーションが導入されているため、マルウェアに感染する可能性が高い。しかし、IoTデバイスは、企業システムなどとは異なり、運用監視が適切に行われていないのが現状である。そのため、IoTデバイスがマルウェアに感染しても、IoTデバイスの管理者は、気付かない場合が多い。

[0004] また、IoTデバイスは、悪意のある第三者による乗っ取りによって、改ざんの対象となり易い。しかし、IoTデバイスは、企業システムなどとは異なり、野外に設置されている場合もある。その場合には、悪意のある第三者がIoTデバイスを開箱し、PC (personal computer) などを直接IoTデバイスに接続させて、IoTデバイスを物理的に乗っ取ることが容易である。

先行技術文献

非特許文献

[0005] 非特許文献1：「OSI参照モデル」、[online]、[2019年6月14日検索]、インターネット<<https://ja.wikipedia.org/wiki/OSI参照モデル>>

発明の概要

発明が解決しようとする課題

[0006] OSI参照モデルに準拠した送信装置（例えば、IoTデバイス）において、外部機器（例えば、サーバ）へのデータ送信の実行又は停止を、任意に制御する方法は知られていない。

[0007] そのため、受信側にとって不要な通信が送信側から送信されてきた場合には、受信側では受信した不要な通信を手動又は自動に廃棄処理していた。特に、マルウェアに感染したIoTデバイス、悪意のある第三者に物理的に乗っ取られたIoTデバイス、災害などによって所在不明になったIoTデバイスなどによって、受信側にとって不要な通信がされてきた場合、受信側では受信した不要な通信を手動又は自動で廃棄処理していた。

[0008] また、マルウェアに感染したIoTデバイス、又は悪意のある第三者に物理的に乗っ取られたIoTデバイスから送信される、受信側にとって不要な通信を停止させるためには、該IoTデバイスが設置されている現場まで出向き、該IoTデバイスの通信を強制的に停止させたり、該IoTデバイスを排除させたりするなど物理的に解決させるしかなかった。

[0009] また、災害などによって所在不明になったIoTデバイスから、受信側にとって不要な通信がされてきた場合には、所在不明になったIoTデバイスの所在が特定され、排除されるまでは、受信側にとって不要な通信を受信せざるを得なかった。

[0010] かかる事情に鑑みてなされた本発明の目的は、OSI参照モデルに準拠した送信装置において、外部機器へのデータ送信の実行又は停止を、任意に制御することが可能な送信制御方法、およびプログラムを提供することにある。

課題を解決するための手段

[0011] 上記課題を解決するため、本発明に係る送信制御方法は、OSI参照モデ

ルに準拠した送信装置の送信制御方法であって、上位層においてペイロードを生成する生成ステップと、入力された制御情報に基づいて、下位層において前記ペイロードの通信処理プロセスを実行又は停止する通信処理プロセスステップと、を含むことを特徴とする。

[0012] また、上記課題を解決するため、本発明に係るプログラムは、コンピュータに、上記送信制御方法を実行させることを特徴とする。

発明の効果

[0013] 本発明によれば、OS参照モデルに準拠した送信装置において、外部機器へのデータ送信の実行又は停止を、任意に制御することが可能となる。

図面の簡単な説明

[0014] [図1]本発明の第1実施形態に係る送信装置の構成の一例を示すブロック図である。

[図2]本発明の第1実施形態に係る送信装置の概念図の一例を示す図である。

[図3]本発明の第1実施形態に係る送信制御方法の一例を示すフローチャートである。

[図4]本発明の第2実施形態に係る通信システムの構成の一例を示すブロック図である。

[図5]本発明の第2実施形態に係る送信制御方法の一例を示すフローチャートである。

[図6]本発明の第3実施形態に係る通信システムの構成の一例を示すブロック図である。

[図7]本発明の第3実施形態に係る送信制御方法の一例を示すフローチャートである。

発明を実施するための形態

[0015] 以下、本発明の一実施形態について、図面を参照して詳細に説明する。

[0016] <第1実施形態>

[送信装置]

図1及び図2を参照して、第1実施形態に係る送信装置100について説

明する。図 1 は、第 1 実施形態に係る送信装置 100 の構成の一例を示す図である。図 2 は、第 1 実施形態に係る送信装置 100 の概念図の一例を示す図である。

[0017] 図 1 に示すように、送信装置 100 は、ペイロード生成部 110 と、判定部 120 と、通信処理プロセス部 130 と、を備える。送信装置 100 は、OS 参照モデルに準拠した装置であれば、その構成が特に限定されるものではなく、例えば、パーソナルコンピュータ、スマートフォン、タブレット端末などであってよい。

[0018] ペイロード生成部 110 は、ユーザデータが内包されるペイロードを生成する。ペイロードは、上位層（例えば、アプリケーション層）において生成される。ペイロード生成部 110 は、生成したペイロードを、判定部 120 へ出力する。

[0019] 判定部 120 は、入力される制御情報に基づいて、上位層から下位層（例えば、プレゼンテーション層）へペイロードを通過させるか否かを判定する（図 2 参照）。制御情報とは、送信装置 100 において、外部機器へのデータ送信の実行又は停止を制御するための情報である。例えば、「通過」を示す制御情報が判定部 120 に入力されると、上位層から下位層へペイロードが通過し、下位層においてペイロードの通信処理プロセスが実行される。すなわち、送信装置 100 は、外部機器へのデータ送信を実行し、送信装置 100 と外部機器との通信を実行するように制御される。例えば、「停止」を示す制御情報が判定部 120 に入力されると、上位層から下位層へペイロードが通過せず、下位層においてペイロードの通信処理プロセスが実行されない。すなわち、送信装置 100 は、外部機器へのデータ送信を停止し、送信装置 100 と外部機器との通信を停止するように制御される。

[0020] 制御情報（「通過」又は「停止」）は、送信装置 100 の内部で生成され、判定部 120 へ入力されてもよいし、送信装置 100 の外部から判定部 120 へ入力されてもよい。例えば、判定部 120 が制御情報を生成してもよいし、外部機器で制御情報が生成され、外部機器から判定部 120 へ制御情

報が入力されてもよい。

- [0021] 判定部 120 は、入力される制御情報（「通過」）に基づいて、上位層から下位層へペイロードを通過させると判定した場合、上位層から下位層へペイロードを通過させる。この場合、下位層においてペイロードの通信処理プロセスが実行される。一方、判定部 120 は、入力される制御情報（「停止」）に基づいて、上位層から下位層へペイロードを通過させないと判定した場合、上位層でペイロードを停止させる。この場合、下位層においてペイロードの通信処理プロセスが実行されない。
- [0022] 通信処理プロセス部 130 は、送信装置 100 に入力される制御情報に基づいて、下位層においてペイロードの通信処理プロセスを実行又は停止する。すなわち、通信処理プロセス部 130 は、上位層から下位層へペイロードが通過したか、上位層から下位層へペイロードが通過していないか、に基づいて、下位層においてペイロードの通信処理プロセスを実行又は停止する。
- [0023] 通信処理プロセス部 130 は、上位層から下位層へペイロードが通過した場合、下位層においてペイロードの通信処理プロセスを実行する。この場合、送信装置 100 は、外部機器へのデータ送信を行う。一方、通信処理プロセス部 130 は、上位層から下位層へペイロードが通過していない場合、下位層においてペイロードの通信処理プロセスを停止する。この場合、送信装置 100 は、外部機器へのデータ送信を行わない。
- [0024] 通信処理プロセス部 130 は、下位層においてペイロードの通信処理プロセスを実行する場合、プレゼンテーション層→セッション層→トランスポート層→ネットワーク層→データリンク層→物理層、の順番で、ペイロードの通信処理プロセスを実行する。ペイロードは、各層（第 6 層～第 1 層）において順番に処理されることで、送信装置 100 と外部機器との通信で必要とされるヘッダやフッタが付加される。
- [0025] 第 1 実施形態に係る送信装置 100 によれば、ペイロード生成部 110 と通信処理プロセス部 130 との間に設けられる判定部 120 が、入力される制御情報に基づいて、上位層から下位層へペイロードを通過させるか否かを

判定し、通信処理プロセス部 130 が、判定部 120 による判定に基づいて、下位層においてペイロードの通信処理プロセスを実行又は停止する。すなわち、OS 1 参照モデルに準拠した送信装置において、既存の OS 1 参照モデルに手を加えることなく、判定部 120 が、入力される制御情報に基づいて、通信処理プロセスの実行又は停止を制御し、外部機器へのデータ送信の実行又は停止を、任意に制御することが可能となる。

[0026] 〔送信制御方法〕

次に、図 3 を参照して、第 1 実施形態に係る送信制御方法について説明する。図 3 は、送信制御方法の一例を示すフローチャートである。

[0027] ステップ S 101 において、ペイロード生成部 110 は、ユーザデータが内包されるペイロードを生成する。

[0028] ステップ S 102 において、判定部 120 は、入力される制御情報に基づいて、上位層から下位層へペイロードを通過させるか否かを判定する。判定部 120 が、「通過」を示す制御情報に基づいて、上位層から下位層へペイロードを通過させると判定した場合、ステップ S 103 の処理が行われる。判定部 120 が、「停止」を示す制御情報に基づいて、上位層から下位層へペイロードを通過させないと判定した場合、ステップ S 102 の処理が行われる。

[0029] ステップ S 103 において、通信処理プロセス部 130 は、送信装置 100 と外部機器との通信で必要とされるヘッダやフッタをペイロードに付加する通信処理プロセスを実行する。

[0030] 第 1 実施形態に係る送信制御方法によれば、OS 1 参照モデルに準拠した送信装置において、外部機器へのデータ送信の実行又は停止を、任意に制御することが可能となる。

[0031] 第 1 実施形態に係る送信制御方法を、例えば、マルウェアに感染した IoT デバイス、悪意のある第 3 者に物理的に乗っ取られた IoT デバイス、災害などによって所在不明となった IoT デバイスなどに適用することで、外部機器の管理者は、外部機器が不要なデータを受信した場合、不要なデータ

を自動又は手動で廃棄処理しなければならないという従来の問題を解消できる。

[0032] また、第1実施形態に係る送信制御方法を、マルウェアに感染したIoTデバイスや悪意のある第3者に物理的に乗っ取られたIoTデバイスに適用することで、外部機器の管理者は、外部機器が不要なデータを受信した場合、これらのデバイスが設置される現場まで出向き、これらのデバイスの通信を強制的に停止又は排除しなければならないという従来の問題を解消できる。

[0033] また、第1実施形態に係る送信制御方法を、災害などによって所在不明となったIoTデバイスに適用することで、外部機器の管理者は、外部機器が不要なデータを受信した場合、これらのデバイスを特定して排除しなければならないという従来の問題を解消できる。

[0034] <第2実施形態>

[通信システム]

図4を参照して、第2実施形態に係る通信システム1について説明する。

図4は、第2実施形態に係る通信システム1の構成の一例を示す図である。

[0035] 図4に示すように、通信システム1は、送信装置100と、受信装置200と、を備える。送信装置100は、ペイロード生成部110と、判定部120と、通信処理プロセス部130と、通信部140と、を備える。受信装置200は、制御部210と、通信部220と、を備える。送信装置100と受信装置200とは、ネットワーク2によって相互に接続される。

[0036] 送信装置100は、OS参照モデルに準拠した装置であれば、その構成が特に限定されるものではなく、例えば、パーソナルコンピュータ、スマートフォン、タブレット端末などであってよい。受信装置200は、OS参照モデルに準拠した装置であれば、その構成が特に限定されるものではなく、例えば、サーバなどであってよい。なお、第2実施形態に係る送信装置が、第1実施形態に係る送信装置と異なる点は、第1実施形態に係る送信装置は、内部又は外部から制御情報が入力されてもよいのに対して、第2実施形

態に係る送信装置は、受信装置から制御情報が入力される点である。その他の構成は、同じであるため、重複した説明を省略する場合がある。

[0037] ペイロード生成部 110 は、ユーザデータが内包されるペイロードを生成する。ペイロードは、上位層（例えば、アプリケーション層）において生成される。ペイロード生成部 110 は、生成したペイロードを、判定部 120 へ出力する。

[0038] 判定部 120 は、送信装置 100 の通信部 140 がネットワーク 2 を介して受信装置 200 の通信部 220 から受信し、この通信部 140 から入力される制御情報に基づいて、上位層から下位層（例えば、プレゼンテーション層）へペイロードを通過させるか否かを判定する。制御情報とは、送信装置 100 において、受信装置 200 へのデータ送信の実行又は停止を制御するための情報である。例えば、「i=0：通過」を示す制御情報が判定部 120 に入力されると、上位層から下位層へペイロードが通過し、下位層においてペイロードの通信処理プロセスが実行される。すなわち、送信装置 100 は、受信装置 200 へのデータ送信を実行し、送信装置 100 と受信装置 200 との通信を実行するように制御される。例えば、「i=1：停止」を示す制御情報が判定部 120 に入力されると、上位層から下位層へペイロードが通過せず、下位層においてペイロードの通信処理プロセスが実行されない。すなわち、送信装置 100 は、受信装置 200 へのデータ送信を停止し、送信装置 100 と受信装置 200 との通信を停止するように制御される。

[0039] 判定部 120 は、通信部 140 から入力される制御情報（「i=0：通過」）に基づいて、上位層から下位層へペイロードを通過させると判定した場合、上位層から下位層へペイロードを通過させる。この場合、下位層においてペイロードの通信処理プロセスが実行される。一方、判定部 120 は、通信部 140 から入力される制御情報（「i=1：停止」）に基づいて、上位層から下位層へペイロードを通過させないと判定した場合、上位層でペイロードを停止させる。この場合、下位層においてペイロードの通信処理プロセスが実行されない。

- [0040] 通信処理プロセス部 130 は、送信装置 100 の通信部 140 がネットワーク 2 を介して受信装置 200 の通信部 220 から受信した制御情報に基づいて、下位層においてペイロードの通信処理プロセスを実行又は停止する。すなわち、通信処理プロセス部 130 は、上位層から下位層へペイロードが通過したか、上位層から下位層へペイロードが通過していないか、に基づいて、下位層においてペイロードの通信処理プロセスを実行又は停止する。
- [0041] 通信処理プロセス部 130 は、上位層から下位層へペイロードが通過した場合、下位層においてペイロードの通信処理プロセスを実行する。この場合、送信装置 100 は、受信装置 200 へのデータ送信を行う。一方、通信処理プロセス部 130 は、上位層から下位層へペイロードが通過していない場合、下位層においてペイロードの通信処理プロセスを停止する。この場合、送信装置 100 は、受信装置 200 へのデータ送信を行わない。
- [0042] 通信部 140 は、ネットワーク 2 を介して、受信装置 200 の通信部 220 と通信する。通信部 140 は、ネットワーク 2 を介して、受信装置 200 の通信部 220 から、例えば、制御情報などの各種の情報を受信する。通信部 140 は、ネットワーク 2 を介して、受信装置 200 の通信部 220 へ、例えば、通信処理プロセス後のデータ（ヘッダやフッタが付加されたペイロード）などの各種の情報を送信する。
- [0043] 例えば、通信部 140 は、ネットワーク 2 を介して、受信装置 200 の通信部 220 から制御情報（「i=0：通過」）を受信すると、制御情報（「i=0：通過」）を判定部 120 へ出力する。例えば、通信部 140 は、ネットワーク 2 を介して、受信装置 200 の通信部 220 から制御情報（「i=1：停止」）を受信すると、制御情報（「i=1：停止」）を判定部 120 へ出力する。
- [0044] 制御部 210 は、制御情報（「i=0：通過」又は「i=1：停止」）を生成する。制御部 210 は、生成した制御情報（「i=0：通過」又は「i=1：停止」）を、通信部 220 へ出力する。制御部 210 が制御情報を生成することで、送信装置 100 と受信装置 200 との通信の実行又は停止を、受信装置 200 が、任意に制御することが可能となる。

- [0045] 制御部210は、例えば、送信装置100からデータを受信したくない場合、すなわち、送信装置100から送信されるデータが不要なデータであると判定する場合、制御情報として、「i=1：停止」を生成し、通信部220へ出力する。通信部220へ出力された制御情報（「i=1：停止」）は、ネットワーク2を介して、送信装置100の通信部140へ送信される。判定部120は、送信装置100の通信部140から入力される制御情報（「i=0：通過」）に基づいて、上位層から下位層へペイロードを通過させるという判定を行う。
- [0046] 制御部210は、例えば、送信装置100からデータを受信したい場合、すなわち、送信装置100から送信されるデータが不要なデータではないと判定する場合、制御情報として、「i=0：通過」を生成し、通信部220へ出力する。通信部220へ出力された制御情報（「i=0：通過」）は、ネットワーク2を介して、送信装置100の通信部140へ送信される。判定部120は、送信装置100の通信部140から入力される制御情報（「i=0：通過」）に基づいて、上位層から下位層へペイロードを通過させないという判定を行う。
- [0047] 通信部220は、ネットワーク2を介して、送信装置100の通信部140と通信する。通信部220は、ネットワーク2を介して、送信装置100の通信部140へ、例えば、制御情報（「i=0：通過」又は「i=1：停止」）などの各種の情報を送信する。通信部220は、ネットワーク2を介して、送信装置100の通信部140から、例えば、通信処理プロセス後のデータ（ヘッダやフッタが付加されたペイロード）などの各種の情報を受信する。
- [0048] 例えば、通信部220は、制御部210から入力される制御情報（「i=0：通過」）を、ネットワーク2を介して送信装置100の通信部140へ送信すると、通信処理プロセス部130は、下位層においてペイロードの通信処理プロセスを実行する。そして、通信部220は、通信処理プロセス後のデータを、ネットワーク2を介して送信装置100の通信部140から受信する。すなわち、下位層においてペイロードの通信処理プロセスが実行された

場合、送信装置１００と受信装置２００とは通信を実行する。

[0049] 例えば、通信部２２０は、制御部２１０から入力される制御情報（「i=1：停止」）を、ネットワーク２を介して送信装置１００の通信部１４０へ送信すると、通信処理プロセス部１３０は、下位層においてペイロードの通信処理プロセスを停止する。すなわち、下位層においてペイロードの通信処理プロセスが停止された場合、送信装置１００と受信装置２００とは通信を停止する。

[0050] 第２実施形態に係る通信システム１によれば、ＯＳＩ参照モデルに準拠した送信装置１００において、受信装置２００へのデータ送信の実行又は停止を、受信装置２００が、任意に制御することが可能となる。また、第２実施形態に係る通信システム１によれば、送信装置１００と受信装置２００との通信の実行又は停止を、受信装置２００が、任意に制御することが可能となる。

[0051] 〔送信制御方法〕

次に、図５を参照して、第２実施形態に係る送信制御方法について説明する。図５は、送信制御方法の一例を示すフローチャートである。

[0052] ステップＳ２０１において、送信装置１００は、ユーザデータが内包されるペイロードを生成する。

[0053] ステップＳ２０２において、送信装置１００は、ネットワーク２を介して、受信装置２００から、制御情報（「i=0：通過」又は「i=1：停止」）を受信する。

[0054] ステップＳ２０３において、送信装置１００は、受信装置２００から入力される制御情報に基づいて、上位層から下位層へペイロードを通過させるか否かを判定する。送信装置１００が、「i=0：通過」を示す制御情報に基づいて、上位層から下位層へペイロードを通過させると判定した場合、ステップＳ２０４の処理が行われる。送信装置１００が、「i=1：停止」を示す制御情報に基づいて、上位層から下位層へペイロードを通過させないと判定した場合、ステップＳ２０２の処理が行われる。

- [0055] ステップS204において、送信装置100は、送信装置100と受信装置200との通信で必要とされるヘッダやフッタをペイロードに付加する通信処理プロセスを実行する。
- [0056] ステップS205において、送信装置100は、ネットワーク2を介して、通信処理プロセス後のデータを受信装置200へ送信する。なお、送信装置100が通信処理プロセスを実行しない場合、送信装置100と受信装置200とは通信を停止する。
- [0057] 第2実施形態に係る送信制御方法によれば、OS1参照モデルに準拠した送信装置において、受信装置200へのデータ送信の実行又は停止を、受信装置200が、任意に制御することが可能となる。また、第2実施形態に係る送信制御方法によれば、送信装置100と受信装置200との通信の実行又は停止を、受信装置200が、任意に制御することが可能となる。
- [0058] 第2実施形態に係る送信制御方法を、例えば、マルウェアに感染したIoTデバイス、悪意のある第3者に物理的に乗っ取られたIoTデバイス、災害などによって所在不明となったIoTデバイスなどに適用することで、受信装置200の管理者は、受信装置200が不要なデータを受信した場合、不要なデータを自動又は手動で廃棄処理しなければならないという従来の問題を解消できる。
- [0059] また、第2実施形態に係る送信制御方法を、マルウェアに感染したIoTデバイスや悪意のある第3者に物理的に乗っ取られたIoTデバイスに適用することで、受信装置200の管理者は、受信装置200が不要なデータを受信した場合、これらのデバイスが設置される現場まで出向き、これらのデバイスの通信を強制的に停止又は排除しなければならないという従来の問題を解消できる。
- [0060] また、第2実施形態に係る送信制御方法を、災害などによって所在不明となったIoTデバイスに適用することで、受信装置200の管理者は、受信装置200が不要なデータを受信した場合、これらのデバイスを特定して排除しなければならないという従来の問題を解消できる。

[0061] <第3実施形態>

図6を参照して、第3実施形態に係る通信システム1Aについて説明する。図6は、第3実施形態に係る通信システム1Aの構成の一例を示す図である。

[0062] 第3実施形態に係る通信システム1Aが、第2実施形態に係る通信システム1と異なる点は、第3実施形態に係る通信システム1Aは、第2実施形態に係る送信装置100の構成に加えて復号部150を備え、第2実施形態に係る受信装置200の構成に加えて暗号化部230を備える点である。なお、その他の構成は、第2実施形態に係る通信システム1と同じであるため、以下の説明では、異なる点のみについて説明し、同じ点については重複した説明を省略する。

[0063] 図6に示すように、通信システム1Aは、送信装置100Aと、受信装置200Aと、を備える。送信装置100Aは、ペイロード生成部110と、判定部120と、通信処理プロセス部130と、通信部140と、復号部150と、を備える。受信装置200Aは、制御部210と、通信部220と、暗号化部230と、を備える。送信装置100Aと受信装置200Aとは、ネットワーク2によって相互に接続される。

[0064] 暗号化部230は、制御部210から入力される制御情報（「i=0：通過」又は「i=1：停止」）、記憶部などに記憶されるID（identification：識別子）およびPW（password：パスワード）を暗号化処理し、暗号化データを生成する。制御部210は、暗号化部230により生成された暗号化データを、通信部220へ出力する。通信部220へ出力された暗号化データは、通信部220からネットワーク2を介して、送信装置100Aへ送信される。なお、IDは、管理者などによって予め設定されてよい。また、PWは、管理者などによって予め設定されてもよいし、公知のPW自動生成機能を用いて生成されてもよい。

[0065] 暗号化処理の方式は、特に限定されるものではなく、例えば、暗号化と復号に同じ鍵を用いる共通鍵暗号方式を採用してもよいし、暗号化と復号に異

なる鍵を用いる公開鍵暗号方式を採用してもよい。共通鍵暗号方式の代表的な規格としては、例えば、DES (Data Encryption Standard)、AES (Advanced Encryption Standard) などが挙げられる。

[0066] 通信部220は、ネットワーク2を介して、送信装置100Aの通信部140と通信する。通信部220は、ネットワーク2を介して、送信装置100Aの通信部140へ、例えば、暗号化データなどの各種の情報を送信する。通信部220は、ネットワーク2を介して、送信装置100Aの通信部140から、例えば、通信処理プロセス後のデータなどの各種の情報を受信する。

[0067] 通信部140は、ネットワーク2を介して、受信装置200Aの通信部220と通信する。通信部140は、ネットワーク2を介して、受信装置200Aの通信部220から、例えば、暗号化データなどの各種の情報を受信する。また、通信部140は、ネットワーク2を介して、受信装置200Aの通信部220へ、例えば、通信処理プロセス後のデータなどの各種の情報を送信する。

[0068] 復号部150は、通信部140が受信した暗号化データを復号処理し、復号した制御情報（「i=0：通過」又は「i=1：停止」）、ID、およびPWを取得する。復号部150は、復号した制御情報（「i=0：通過」又は「i=1：停止」）、ID、およびPWを、判定部120へ出力する。

[0069] 判定部120は、復号部150から入力されるIDに基づいて、IDの照合処理を行って、IDが正しいか否かを判定する。判定部120は、IDが正しいと判定する場合、復号部150から入力されるPWに基づいて、PWの照合処理を行う。一方、判定部120は、IDが誤っていると判定する場合、PWの照合処理を行わない。

[0070] 判定部120は、復号部150から入力されるPWに基づいて、PWの照合処理を行って、PWが正しいか否かを判定する。判定部120は、PWが正しいと判定する場合、復号部150から入力される制御情報に基づいて、上位層から下位層へペイロードを通過させるか否かを判定する。一方、判定

部 1 2 0 は、PW が誤っていると判定する場合、判定処理を行わない。

[0071] 判定部 1 2 0 は、復号部 1 5 0 から入力される制御情報に基づいて、上位層から下位層へペイロードを通過させるか否かを判定する。判定部 1 2 0 は、復号部 1 5 0 から入力される制御情報（「i=0：通過」）に基づいて、上位層から下位層へペイロードを通過させると判定した場合、上位層から下位層へペイロードを通過させる。この場合、下位層においてペイロードの通信処理プロセスが実行される。一方、判定部 1 2 0 は、復号部 1 5 0 から入力される制御情報（「i=1：停止」）に基づいて、上位層から下位層へペイロードを通過させないと判定した場合、上位層でペイロードを停止させる。この場合、下位層においてペイロードの通信処理プロセスが実行されない。

[0072] 第 3 実施形態に係る通信システム 1 A によれば、暗号化復号処理を用いてセキュリティ機能を強化しつつ、OS I 参照モデルに準拠した送信装置 1 0 0 A において、受信装置 2 0 0 A へのデータ送信の実行又は停止を、受信装置 2 0 0 A が、任意に制御することが可能となる。また、第 3 実施形態に係る通信システム 1 A によれば、送信装置 1 0 0 A と受信装置 2 0 0 A との通信の実行又は停止を、受信装置 2 0 0 A が、任意に制御することが可能となる。

[0073] [送信制御方法]

次に、図 7 を参照して、第 3 実施形態に係る送信制御方法について説明する。図 7 は、送信制御方法の一例を示すフローチャートである。

[0074] ステップ S 3 0 1 において、送信装置 1 0 0 A は、ユーザデータが内包されるペイロードを生成する。

[0075] ステップ S 3 0 2 において、送信装置 1 0 0 A は、ネットワーク 2 を介して、受信装置 2 0 0 A から、暗号化された制御情報（「i=0：通過」又は「i=1：停止」）、ID および PW を受信する。

[0076] ステップ S 3 0 3 において、送信装置 1 0 0 A は、暗号化された制御情報（「i=0：通過」又は「i=1：停止」）、ID および PW を復号する。

[0077] ステップ S 3 0 4 において、送信装置 1 0 0 A は、復号した ID を照合し

、IDが正しいか否かを判定する。送信装置100Aが、IDが正しいと判定する場合、ステップS305の処理が行われる。送信装置100Aが、IDが誤っていると判定する場合、ステップS302の処理が行われる。

[0078] ステップS305において、送信装置100Aは、復号したPWを照合し、PWが正しいか否かを判定する。送信装置100Aが、PWが正しいと判定する場合、ステップS306の処理が行われる。送信装置100Aが、PWが誤っていると判定する場合、ステップS302の処理が行われる。

[0079] ステップS306において、送信装置100Aは、復号した制御情報に基づいて、上位層から下位層へペイロードを通過させるか否かを判定する。送信装置100Aが、「i=0：通過」を示す制御情報に基づいて、上位層から下位層へペイロードを通過させると判定した場合、ステップS307の処理が行われる。送信装置100Aが、「i=1：停止」を示す制御情報に基づいて、上位層から下位層へペイロードを通過させないと判定した場合、ステップS302の処理が行われる。

[0080] ステップS307において、送信装置100Aは、送信装置100Aと受信装置200Aとの通信で必要とされるヘッダやフッタをペイロードに付加する通信処理プロセスを実行する。

[0081] ステップS308において、送信装置100Aは、ネットワーク2を介して、通信処理プロセス後のデータを受信装置200Aへ送信する。なお、送信装置100Aが通信処理プロセスを実行しない場合、送信装置100Aと受信装置200Aとは通信を停止する。

[0082] 第3実施形態に係る送信制御方法によれば、暗号化復号処理を用いてセキュリティ機能を強化しつつ、OS参照モデルに準拠した送信装置100Aにおいて、受信装置200Aへのデータ送信の実行又は停止を、受信装置200Aが、任意に制御することが可能となる。また、第3実施形態に係る送信制御方法によれば、送信装置100Aと受信装置200Aとの通信の実行又は停止を、受信装置200Aが、任意に制御することが可能となる。

[0083] 第3実施形態に係る送信制御方法を、例えば、マルウェアに感染したI/O

IoTデバイス、悪意のある第三者に物理的に乗っ取られたIoTデバイス、災害などによって所在不明となったIoTデバイスなどに適用することで、受信装置200Aの管理者は、受信装置200Aが不要なデータを受信した場合、不要なデータを自動又は手動で廃棄処理しなければならないという従来の問題を解消でき、更にセキュリティ機能を強化できる。

[0084] また、第3実施形態に係る送信制御方法を、マルウェアに感染したIoTデバイスや悪意のある第三者に物理的に乗っ取られたIoTデバイスに適用することで、受信装置200Aの管理者は、受信装置200Aが不要なデータを受信した場合、これらのデバイスが設置される現場まで出向き、これらのデバイスの通信を強制的に停止又は排除しなければならないという従来の問題を解消でき、更にセキュリティ機能を強化できる。

[0085] また、第3実施形態に係る送信制御方法を、災害などによって所在不明となったIoTデバイスに適用することで、受信装置200Aの管理者は、受信装置200Aが不要なデータを受信した場合、これらのデバイスを特定して排除しなければならないという従来の問題を解消でき、更にセキュリティ機能を強化できる。

[0086] <変形例>

本発明は上記の実施形態及び変形例に限定されるものではない。例えば、上述の各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。その他、本発明の趣旨を逸脱しない範囲で適宜変更が可能である。

[0087] <プログラム及び記録媒体>

また、上記の実施形態及び変形例で説明した各装置における各種の処理機能をコンピュータによって実現してもよい。その場合、各装置が有すべき機能の処理内容はプログラムによって記述される。そして、このプログラムをコンピュータで実行することにより、上記各装置における各種の処理機能がコンピュータ上で実現される。

- [0088] この処理内容を記述したプログラムは、コンピュータで読み取り可能な記録媒体に記録しておくことができる。コンピュータで読み取り可能な記録媒体としては、例えば、磁気記録装置、光ディスク、光磁気記録媒体、半導体メモリ等のようなものでもよい。
- [0089] また、このプログラムの流通は、例えば、そのプログラムを記録したDVD、CD-ROM等の可搬型記録媒体を販売、譲渡、貸与等することによって行う。さらに、このプログラムをサーバコンピュータの記憶装置に格納しておき、ネットワークを介して、サーバコンピュータから他のコンピュータにそのプログラムを転送することにより、このプログラムを流通させてもよい。
- [0090] このようなプログラムを実行するコンピュータは、例えば、まず、可搬型記録媒体に記録されたプログラムもしくはサーバコンピュータから転送されたプログラムを、一旦、自己の記憶部に格納する。そして、処理の実行時、このコンピュータは、自己の記憶部に格納されたプログラムを読み取り、読み取ったプログラムに従った処理を実行する。また、このプログラムの別の実施形態として、コンピュータが可搬型記録媒体から直接プログラムを読み取り、そのプログラムに従った処理を実行することとしてもよい。さらに、このコンピュータにサーバコンピュータからプログラムが転送されるたびに、逐次、受け取ったプログラムに従った処理を実行することとしてもよい。また、サーバコンピュータから、このコンピュータへのプログラムの転送は行わず、その実行指示と結果取得のみによって処理機能を実現する、いわゆるASP（Application Service Provider）型のサービスによって、上述の処理を実行する構成としてもよい。なお、プログラムには、電子計算機による処理の用に供する情報であってプログラムに準ずるもの（コンピュータに対する直接の指令ではないがコンピュータの処理を規定する性質を有するデータ等）を含むものとする。
- [0091] また、コンピュータ上で所定のプログラムを実行させることにより、各装置を構成することとしたが、これらの処理内容の少なくとも一部をハードウ

エア的に実現することとしてもよい。

[0092] 上述の実施形態は代表的な例として説明したが、本発明の趣旨及び範囲内で、多くの変更及び置換ができることは当業者に明らかである。したがって、本発明は、上述の実施形態によって制限するものと解するべきではなく、特許請求の範囲から逸脱することなく、種々の変形や変更が可能である。例えば、実施形態の構成図に記載の複数の構成ブロックを1つに組み合わせたり、あるいは1つの構成ブロックを分割したりすることが可能である。

符号の説明

[0093]	1, 1 A	通信システム
	2	ネットワーク
	1 0 0, 1 0 0 A	送信装置
	1 1 0	ペイロード生成部
	1 2 0	判定部
	1 3 0	通信処理プロセス部
	1 4 0	通信部
	1 5 0	復号部
	2 0 0, 2 0 0 A	受信装置
	2 1 0	制御部
	2 2 0	通信部
	2 3 0	暗号化部

請求の範囲

- [請求項1] OS I 参照モデルに準拠した送信装置の送信制御方法であって、
上位層においてペイロードを生成する生成ステップと、
入力された制御情報に基づいて、下位層において前記ペイロードの
通信処理プロセスを実行又は停止する通信処理プロセスステップと、
を含む、送信制御方法。
- [請求項2] 前記制御情報に基づいて、前記上位層から前記下位層へ前記ペイロ
ードを通過させるか否かを判定する判定ステップを更に含み、
前記通信処理プロセスステップは、
前記判定ステップにより、前記上位層から前記下位層へ前記ペイロ
ードを通過させると判定された場合、前記下位層において前記ペイロ
ードの通信処理プロセスを実行し、
前記判定ステップにより、前記上位層から前記下位層へ前記ペイロ
ードを通過させないと判定された場合、前記下位層において前記ペイロ
ードの通信処理プロセスを停止する、
請求項1に記載の送信制御方法。
- [請求項3] OS I 参照モデルに準拠した受信装置から前記制御情報を受信する
受信ステップと、
前記通信処理プロセスステップにより、前記下位層において前記ペ
イロードの通信処理プロセスが実行された場合、通信処理プロセス後
のデータを前記受信装置へ送信する送信ステップと、
前記通信処理プロセスステップにより、前記下位層において前記ペ
イロードの通信処理プロセスが停止された場合、前記送信装置と前記
受信装置とが通信を停止する停止ステップと、
を更に含む、請求項1又は2に記載の送信制御方法。
- [請求項4] OS I 参照モデルに準拠した受信装置から暗号化された制御情報、
ID、およびPWを受信する受信ステップと、
前記暗号化された制御情報、ID、およびPWを復号する復号ステ

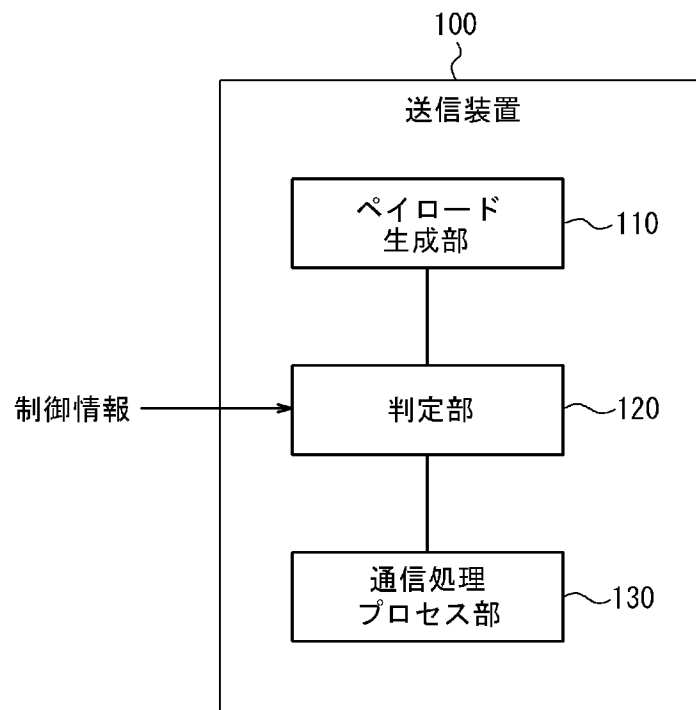
ップと、

復号した前記 I D および P W が正しいか否かを判定する照合ステップと、を更に含み、

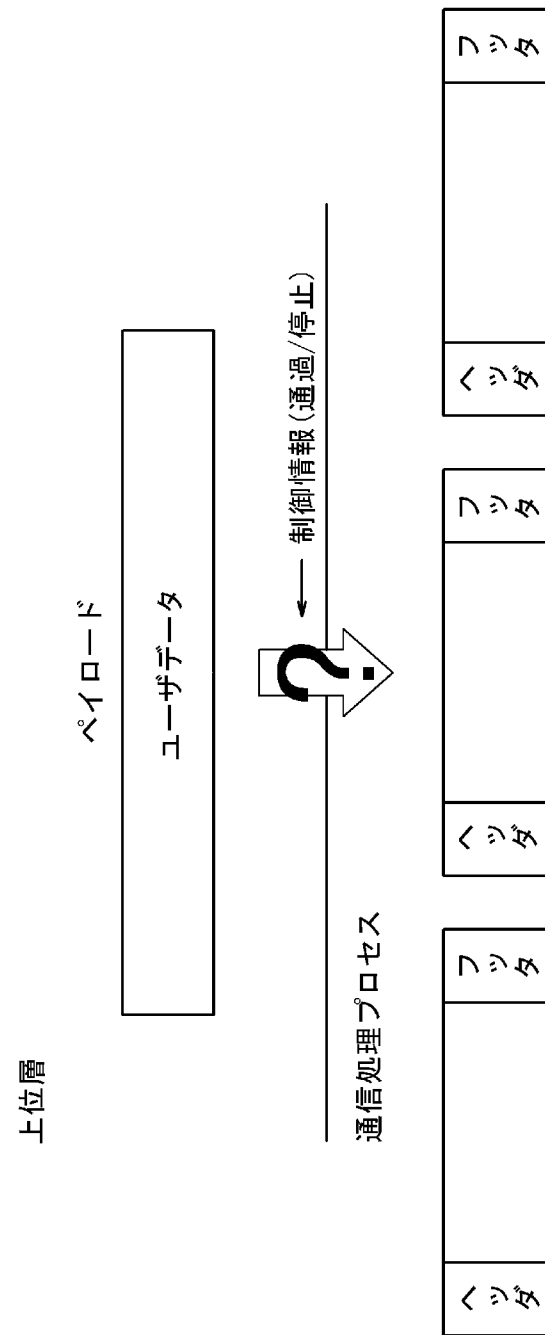
前記通信処理プロセスステップは、前記照合ステップにより、前記 I D および P W が正しいと判定された場合に、前記ペイロードの通信処理プロセスを実行する、請求項 1 から 3 のいずれか一項に記載の送信制御方法。

[請求項5] コンピュータに、請求項 1 から 4 のいずれか一項に記載の送信制御方法を実行させるためのプログラム。

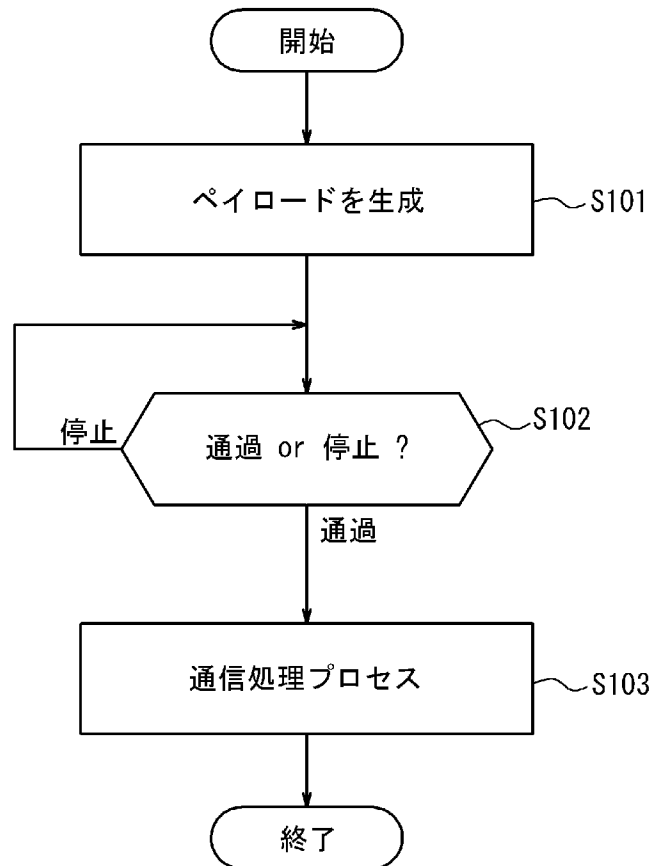
[図1]



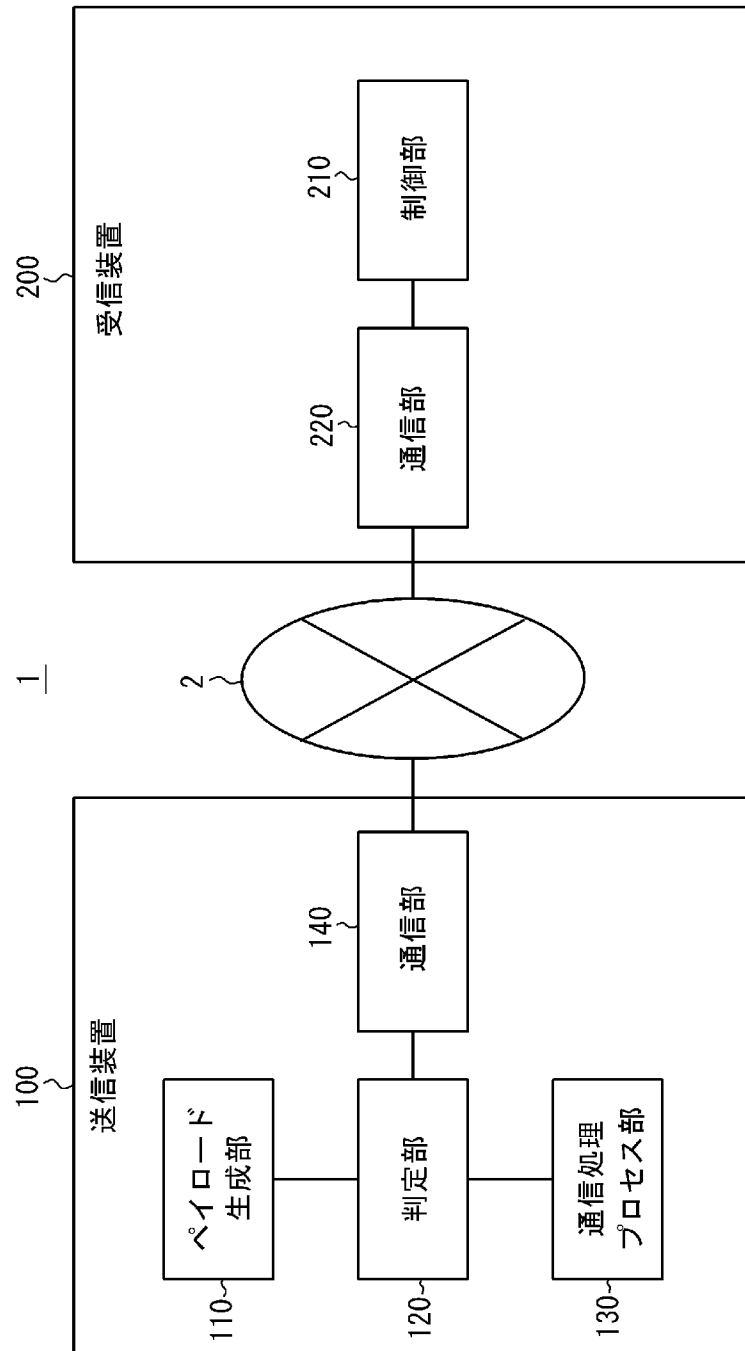
[図2]



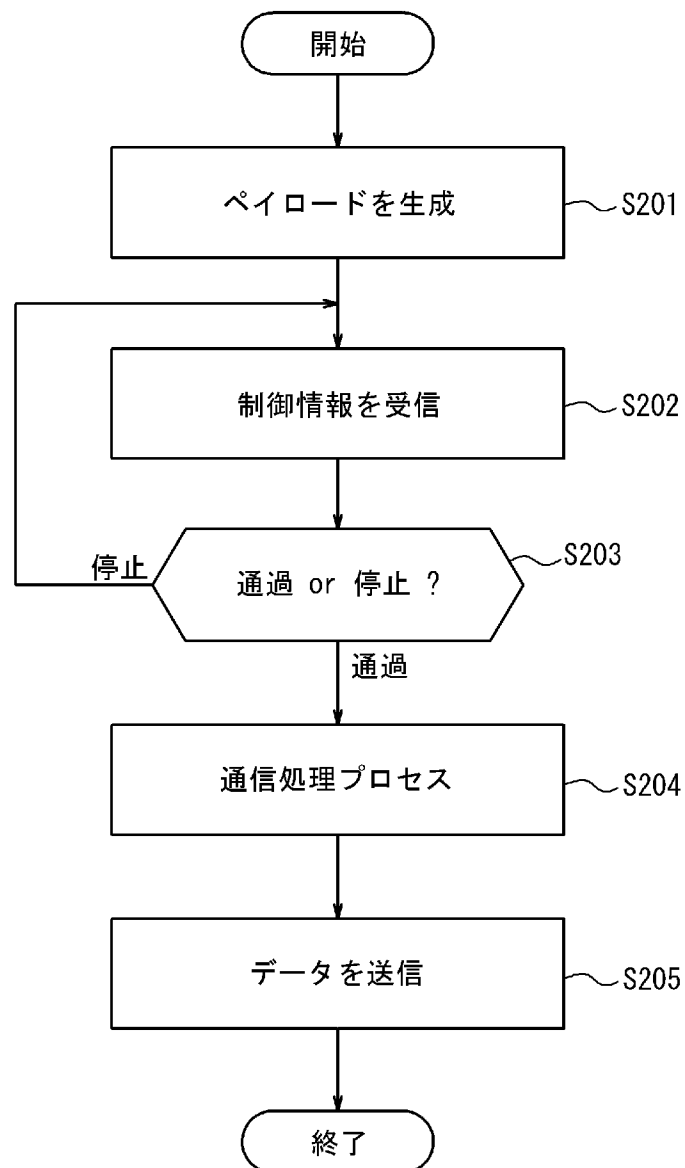
[図3]



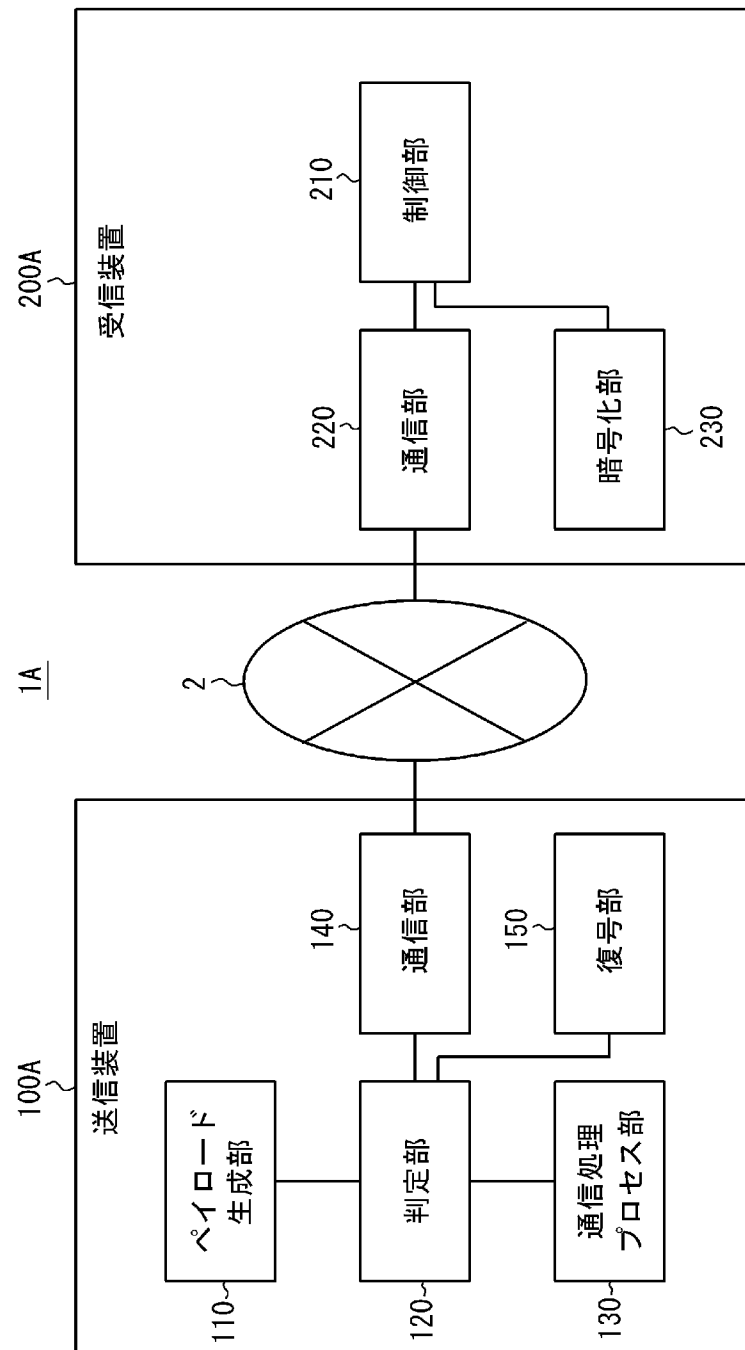
[図4]



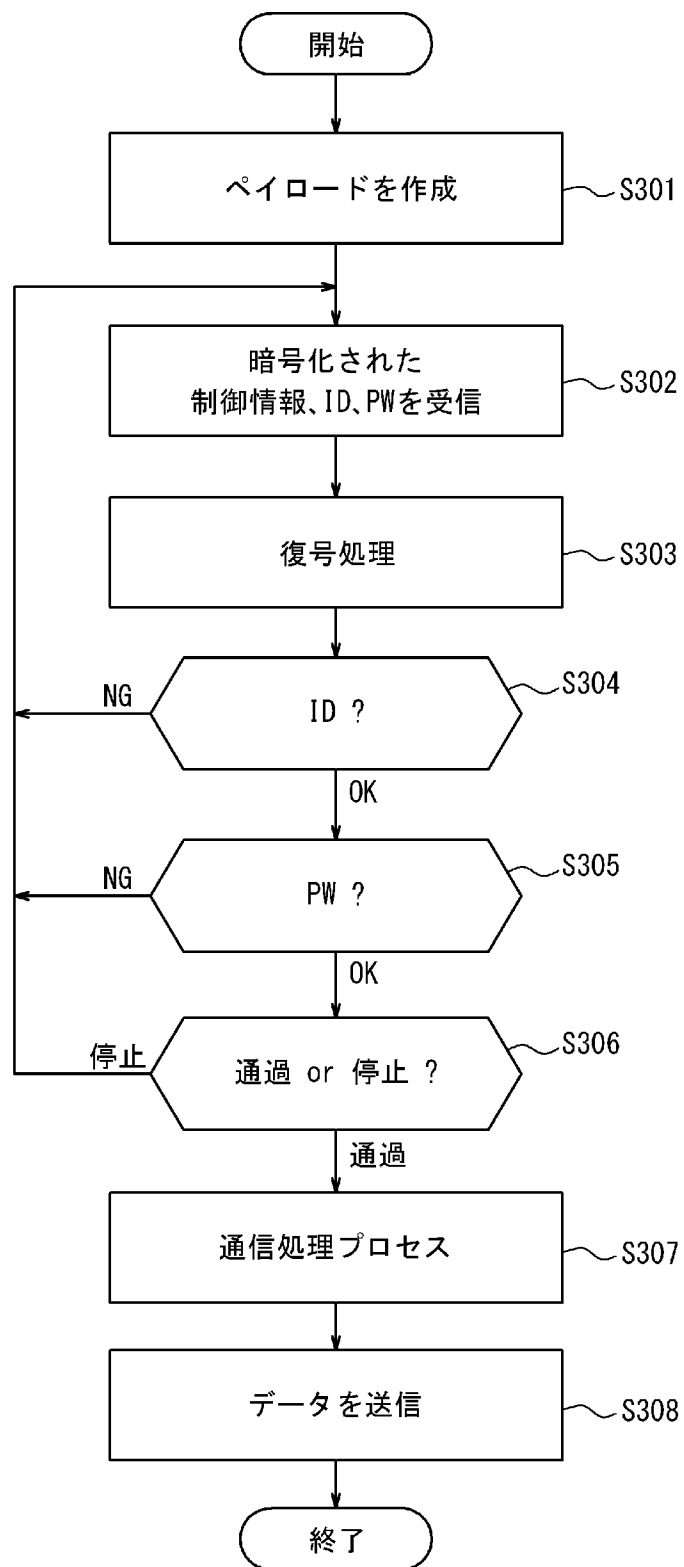
[図5]



[図6]



[図7]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2019/024539

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. H04L29/02 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int. Cl. H04L29/00-29/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Published examined utility model applications of Japan 1922-1996

Published unexamined utility model applications of Japan 1971-2019

Registered utility model specifications of Japan 1996-2019

Published registered utility model applications of Japan 1994-2019

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2012-14278 A (LENOVO SINGAPORE PTE. LTD.) 19	1-3
Y	January 2012, paragraphs [0039]-[0051], [0068]-[0074] & US 2011/0321145 A1, paragraphs [0038]-[0050], [0067]-[0073]	4
Y	JP 2010-157068 A (VISIONERE CORP.) 15 July 2010, claim 6, paragraphs [0049]-[0060] (Family: none)	4
Y	JP 2008-176725 A (SONY CORP.) 31 July 2008, paragraphs [0118]-[0120] (Family: none)	4

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
03.10.2019

Date of mailing of the international search report
15.10.2019

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int.Cl. H04L29/02(2006.01)i

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int.Cl. H04L29/00-29/08

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2019年
日本国実用新案登録公報	1996-2019年
日本国登録実用新案公報	1994-2019年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
X Y	JP 2012-14278 A (レノボ・シンガポール・プライベート・リミテッド) 2012.01.19, [0039]-[0051], [0068]-[0074] & US 2011/0321145 A1 [0038]-[0050], [0067]-[0073]	1-3 4
Y	JP 2010-157068 A (ヴィジョネア株式会社) 2010.07.15, 請求項 6, [0049]-[0060] (ファミリーなし)	4
Y	JP 2008-176725 A (ソニー株式会社) 2008.07.31, [0118]-[0120] (ファミリーなし)	4

C欄の続きにも文献が列挙されている。

パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日

03.10.2019

国際調査報告の発送日

15.10.2019

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

玉木 宏治

5 X

3047

電話番号 03-3581-1101 内線 3596