(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9月10日(10.09.2020)

WIPO | PCT

(10) 国際公開番号
WO 2020/179709 A1

(51) 国際特許分類:
H04L 9/08 (2006.01) *H04L 12/22* (2006.01)
H04L 9/14 (2006.01) *G06F 21/44* (2013.01)
H04L 9/32 (2006.01) *G06F 21/60* (2013.01)

(21) 国際出願番号： PCT/JP2020/008471

(22) 国際出願日： 2020年2月28日(28.02.2020)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

(30) 優先権データ：
特願 2019-038379 2019年3月4日(04.03.2019) JP

(71) 出願人: 株式会社 東芝 (**KABUSHIKI KAISHA TOSHIBA**) [JP/JP]; 〒1050023 東京都港区芝浦一丁目1番1号 Tokyo (JP). 東芝インフラシステムズ株式会社 (**TOSHIBA INFRASTRUCTURE SYSTEMS & SOLUTIONS CORPORATION**) [JP/JP]; 〒2120013 神奈川県川崎市幸区堀川町72番地34 Kanagawa (JP).

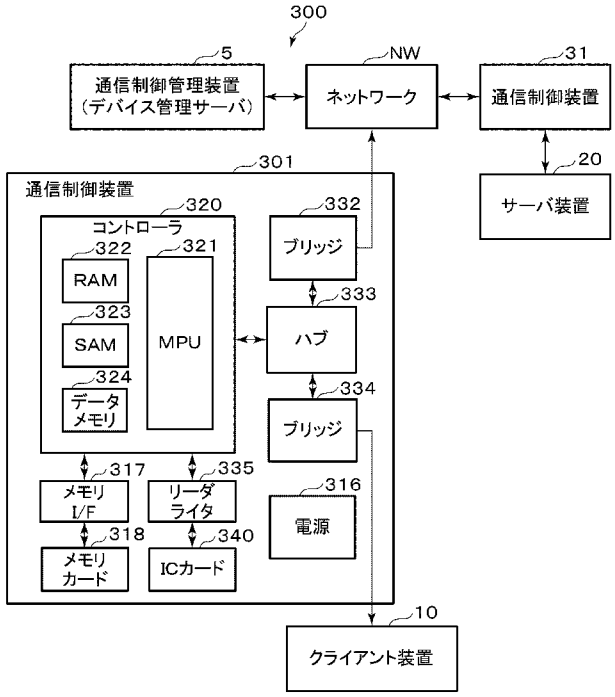
(72) 発明者: 友枝 裕樹 (**TOMOEDA, Yuuki**); 〒2120013 神奈川県川崎市幸区堀川町72番地34 東芝インフラシステムズ株式会社内 Kanagawa (JP).

(74) 代理人: 蔵田 昌俊, 外 (**KURATA, Masatoshi** et al.); 〒1050014 東京都港区芝三丁目23番1号 セレスティン芝三井ビルディング11階 鈴榮特許綜合事務所内 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,

(54) **Title:** COMMUNICATION CONTROL DEVICE AND COMMUNICATION SYSTEM

(54) 発明の名称： 通信制御装置および通信システム



5 Communication control management device (device management server)
10 Client device
20 Server device
31, 301 Communication control device
316 Power source
317 Memory interface
318 Memory card
320 Controller
324 Data memory
332, 334 Bridge
333 Hub
335 Reader/writer
340 IC card
NW Network

(57) **Abstract:** According to an embodiment, a communication control device has a controller and a memory. By using a first device and an issued secret key, and a common key in which a client certificate is used and that is determined by mutual authentication processing with a second communication control device that is connected between a second server device and a network communication network, the controller transmits, to the second communication control device, information obtained by encrypting information transmitted from the first device to the second device, and transmits, to

WO 2020/179709 A1

[続葉有]

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, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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:

— 国際調査報告 (条約第21条(3))

the first device, information obtained by decrypting information transmitted from the second device to the first device. The memory stores analysis information of a communication amount of data communication that is performed through a communication interface. The controller further executes self-diagnosis at an execution time that is set on the basis of the analysis information of the communication amount stored in the memory, and transmits the execution result of the self-diagnosis to a device management server that collects information indicating an operation state.

(57) 要約:実施形態によれば、通信制御装置は、コントローラとメモリとを有する。コントローラは、第１の装置および発行された秘密鍵、及びクライアント証明書を用いた第２のサーバ装置とネットワーク通信網との間に接続される第２の通信制御装置との相互認証処理により決定された共通鍵を用いて、第１の装置から第２の装置へ送信される情報を暗号化した情報を前記第２の通信制御装置に送信し、第２の装置から第１の装置へ送信される情報を復号した情報を第１の装置に送信する。メモリは、通信インターフェースを介してデータ通信した通信量の分析情報を記憶する。コントローラは、さらに、メモリに記憶する通信量の分析情報に基づいて設定される実行時刻に自己診断を実行し、自己診断の実行結果を動作状態を示す情報を収集するデバイス管理サーバへ送信する。

明　細　書

発明の名称 ： 通信制御装置および通信システム

技術分野

[0001] 本発明の実施形態は、通信制御装置および通信システムに関する。

背景技術

[0002] 通信システムは、取り扱うデータおよび機器の制御情報をマルウェア等の攻撃から防御される必要がある。例えば、社会インフラとして設置される監視カメラ等の機器は、通信するデータの安全性を確保することが必要である。しかしながら、監視カメラなどの社会インフラを構築する各機器は、一旦設置されると、頻繁に置換えることが難しいため、安全対策が不十分になってしまうという問題がある。

先行技術文献

特許文献

[0003] 特許文献1：日本国特開２００９－１１７８８７号公報

発明の概要

発明が解決しようとする課題

[0004] 本発明が解決しようとする課題は、社会インフラシステムなどに用いる通信の安全性を向上させることができる通信制御装置および通信システムを提供することである。

課題を解決するための手段

[0005] 実施形態によれば、通信制御装置は、コントローラとメモリとを有する。コントローラは、第１の装置および発行された秘密鍵、及びクライアント証明書を用いた第２のサーバ装置とネットワーク通信網との間に接続される第２の通信制御装置との相互認証処理により決定された共通鍵を用いて、第１の装置から第２の装置へ送信される情報を暗号化した情報を前記第２の通信制御装置に送信し、第２の装置から第１の装置へ送信される情報を復号した情報を第１の装置に送信する。メモリは、通信インターフェースを介してデ

ータ通信した通信量の分析情報を記憶する。コントローラは、さらに、メモリに記憶する通信量の分析情報に基づいて設定される実行時刻に自己診断を実行し、自己診断の実行結果を動作状態を示す情報を収集するデバイス管理サーバへ送信する。

図面の簡単な説明

[0006] [図1]図１は、各実施形態に係る通信システムの基本構成例を示す図である。

[図2]図２は、各実施形態に係るクライアント装置およびサーバ装置の機能構成例を示すブロック図である。

[図3]図３は、各実施形態に係るクライアント側の通信制御装置およびサーバ側の通信制御装置における機能構成例を示すブロック図である。

[図4]図４は、各実施形態に係る通信制御装置における認証部の構成例としてのＩＣカードのハードウェア構成例を示す図である。

[図5]図５は、各実施形態に係る通信制御装置における認証部の構成例としてのＣカードにおける機能構成例を示すブロック図である。

[図6]図６は、各実施形態に係る通信制御管理装置における機能構成例を示すブロック図である。

[図7]図７は、図１に示す通信システムが行う処理の一例を示すシーケンスである。

[図8]図８は、第１の実施形態に係る通信システムの第１の構成例を示す図である。

[図9]図９は、第１の実施形態に係る通信システムの第１の構成例における通信制御装置の構成例を示すブロック図である。

[図10]図１０は、第１の実施形態の第１の構成例に係る通信システムの動作例を説明するためのシーケンスである。

[図11]図１１は、第１の実施形態に係る通信システムの第２の構成例を示す図である。

[図12]図１２は、第１の実施形態に係る通信システムの第２の構成例における通信制御装置の構成例を示すブロック図である。

[図13]図１３は、第１の実施形態の第２の構成例に係る通信システムの動作例を説明するためのシーケンスである。

[図14]図１４は、第２の実施形態に係る通信システムの構成例を示す図である。

[図15]図１５は、第２の実施形態に係る通信システムの構成例における通信制御装置の構成例を示すブロック図である。

[図16]図１６は、第２の実施形態に係る通信システムにおける分散制御器の動作例を説明するためのフローチャートである。

[図17]図１７は、第３の実施形態に係る通信システムの構成例を示すブロック図である。

[図18]図１８は、第３の実施形態に係る通信システムの第１の動作例を説明するためのシーケンスである。

[図19]図１９は、第３の実施形態に係る通信システムの第２の動作例を説明するためのシーケンスである。

[図20]図２０は、第４の実施形態に係る通信システムの第１の動作例を説明するためのシーケンスである。

[図21]図２１は、第４の実施形態に係る通信システムの第２の動作例を説明するためのシーケンスである。

[図22]図２２は、第４の実施形態に係る通信システムの第３の動作例を説明するためのシーケンスである。

実施形態

[0007] 以下、各実施形態について、図面を参照して説明する。

まず、各実施形態に係る通信システムのベースとなる基本的な構成例および動作例について説明する。

図１は、各実施形態に係る通信システムのベースとなる構成を有する通信システム１の構成例を示す図である。

通信システム１は、クライアント装置１０（１０－１～１０－Ｎ）と、サーバ装置２０と、クライアント側の通信制御装置３０（３０－１～３０－Ｎ

）（「第１の通信制御装置」の一例）と、サーバ側の通信制御装置３１（「第１の通信制御装置」の一例）と、通信制御管理装置５（「プライベート認証局」の一例）と、ネットワーク６と、ゲートウェイ７と、を備える。以下の説明においては、ネットワーク６と、ネットワーク６とクライアント装置１０等とを接続するゲートウェイ７と、をまとめて「ネットワークＮＷ」とも称する。

[0008] クライアント装置１０は、クライアント側の通信制御装置３０を介してネットワークＮＷと接続する。サーバ装置２０は、サーバ側の通信制御装置３１を介してネットワークＮＷと接続する。なお、クライアント装置１０、およびサーバ装置２０の構成の詳細については後述する。

[0009] クライアント側の通信制御装置３０は、クライアント装置１０とネットワークＮＷとの間に接続され、クライアント装置１０とサーバ装置２０との間の通信を仲介する。クライアント側の通信制御装置３０は、クライアント装置１０によりサーバ装置２０に対して送信されるデータを取得し、取得したデータをサーバ装置２０に対して出力する。ここで、クライアント側の通信制御装置３０は、サーバ装置２０に対してデータを送信する際に、クライアント装置１０から取得したデータを暗号化し、暗号化したデータをサーバ装置２０に対して送信する。

[0010] また、クライアント側の通信制御装置３０は、サーバ装置２０によりクライアント装置１０に対して送信されるデータを取得し、取得したデータをクライアント装置１０に対して出力する。ここで、クライアント側の通信制御装置３０が取得するデータは暗号化されたデータである。クライアント側の通信制御装置３０は、クライアント装置１０にデータを出力する際に、サーバ装置２０からサーバ側の通信制御装置３１を介して取得したデータを復号し、復号したデータをクライアント装置１０に出力する。

[0011] サーバ側の通信制御装置３１は、サーバ装置２０とネットワークＮＷとの間に接続され、クライアント装置１０とサーバ装置２０との間の通信を仲介する。サーバ側の通信制御装置３１は、サーバ装置２０によりクライアント

装置１０に対して送信されるデータを取得し、取得したデータをクライアント装置１０に対して送信する。ここで、サーバ側の通信制御装置３１は、クライアント装置１０に対してデータを送信する際に、サーバ装置２０から取得したデータを暗号化し、暗号化したデータをクライアント装置１０に対して送信する。

[0012] また、サーバ側の通信制御装置３１は、クライアント装置１０によりサーバ装置２０に対して送信されるデータを取得し、取得したデータをサーバ装置２０に対して出力する。ここで、サーバ側の通信制御装置３１が取得するデータは暗号化されたデータである。サーバ側の通信制御装置３１は、サーバ装置２０にデータを出力する際に、クライアント装置１０からクライアント側の通信制御装置３０を介して取得したデータを復号し、復号したデータをサーバ装置２０に出力する。

[0013] クライアント側の通信制御装置３０およびサーバ側の通信制御装置３１が行うデータの暗号化には、例えば、ＳＳＬ（Secure Socket Layer）／ＴＬＳ（Trans port Layer Security）のプロトコルによる暗号化が行われる。クライアント側の通信制御装置３０およびサーバ側の通信制御装置３１は、例えば、ＳＳＬ／ＴＬＳプロトコルを、ＨＴＴＰと組み合わせることで、ＨＴＴＰに含まれるデータを暗号化し、安全性を向上させたＨＴＴＰＳ（HTTP Secure）に置き換える。

[0014] なお、クライアント側の通信制御装置３０およびサーバ側の通信制御装置３１が行うデータの暗号化は、ＨＴＴＰをＨＴＴＰＳとすることに限定されない。クライアント側の通信制御装置３０およびサーバ側の通信制御装置３１は、ＳＳＬ／ＴＬＳプロトコルを種々の通信プロトコルと組み合わせることにより、安全性を向上させたセキュアな通信プロトコルに置き換えてもよい。例えば、クライアント側の通信制御装置３０およびサーバ側の通信制御装置３１は、ＦＴＰ（File Transfer Protocol）をＦＴＰＳ（FTP Secure）に置き換えてもよい。

[0015] 通信システム１において、クライアント側の通信制御装置３０、またはサ

ーバ側の通信制御装置３１により暗号化されたデータがネットワークＮＷに出力される。換言すると、通信システム１におけるネットワークＮＷを流れるデータは、暗号化されたデータであり。このため、ネットワークＮＷで送受信されるデータに対し、外部から悪意をもってアクセスされデータが盗聴されてしまうような危険を回避し、安全性を向上させる。なお、ここでいうデータの盗聴とは、「データを盗み見る行為」または「データを抜き取る行為」をいう。

[0016] 通信制御管理装置５は、クライアント側の通信制御装置とサーバ側の通信制御装置とを用いた通信を管理するための通信管理サーバである。例えば、通信制御管理装置５は、クライアント側の通信制御装置３０に対し、クライアント証明書、および秘密鍵を発行する。図１に示す構成例において、通信制御管理装置５は、クライアント側の通信制御装置３０に装着するＩＣカードに記憶するクライアント証明書、および秘密鍵を発行する。また、通信制御管理装置５は、ＩＣカードが装着されたクライアント側の通信制御装置３０に対し、ＩＣカードに記憶させるクライアント証明書、および秘密鍵を、ネットワークＮＷを介して送信する。

[0017] また、通信制御管理装置５は、サーバ側の通信制御装置３１に対し、サーバ証明書、および秘密鍵を発行する。例えば、通信制御管理装置５は、ＩＣカードに記憶するサーバ証明書、および秘密鍵を発行する。また、通信制御管理装置５は、ＩＣカードが装着されたサーバ側の通信制御装置３１に対し、ＩＣカードに記憶させるサーバ証明書、および秘密鍵を、ネットワークＮＷを介して送信する。クライアント証明書、サーバ証明書、および秘密鍵のそれぞれは、クライアント側の通信制御装置３０とサーバ側の通信制御装置３１とが暗号化通信を行う場合に用いる共通鍵（セッション鍵）を決定するために必要な情報である。

[0018] ここでは、クライアント装置１０、およびサーバ装置２０の構成について説明する。クライアント装置１０とサーバ装置２０とは、例えば、社会インフラシステムを構築する構成要素（コンポーネント）である。社会インフラ

とは、道路交通網、発電設備、配送電設備、水処理設備、又はガス配給設備等などの社会基盤を整えるために必要な設備である。社会インフラシステムとは、例えば、社会インフラを監視し、状況の変化を把握し、その変化に対応することにより、社会インフラを安定的に動作させる仕組みである。以下においては、クライアント装置１０とサーバ装置とは、道路や公共設備などを監視する監視システムのコンポーネントである場合を例に説明する。この場合、クライアント装置１０は、道路の状況等が撮像された撮像データを、ネットワークＮＷを介して送信する装置（ネットワーク監視カメラ）である。サーバ装置２０は、クライアント装置１０により送信された撮像データを、ネットワークＮＷを介して受信する装置である。

[0019] なお、クライアント装置１０とサーバ装置２０とは、監視システムのコンポーネントに限定されることはない。例えば、クライアント装置１０とサーバ装置とは、発電設備や配送電設備における電力状況をモニタリングするシステムのコンポーネントであってもよいし、物流センタにおける配送状況を取得するシステム、あるいは工場や研究機関における設備の稼働状況を取得するシステム等のコンポーネントであってもよい。

[0020] 図２は、図１に示すクライアント装置１０、およびサーバ装置２０の機能構成例を示すブロック図である。

クライアント装置１０は、ＮＷ（ネットワーク）通信部１１と、クライアント制御部１２と、撮像部１３とを備える。ＮＷ通信部１１は、例えば、クライアント装置１０のイーサネット（登録商標）のポートである。ＮＷ通信部１１は、クライアント側の通信制御装置３０に接続され、クライアント装置１０からサーバ装置２０に対して送信されるデータをクライアント側の通信制御装置３０に出力する。なお、ＮＷ通信部１１は、従来のシステムであれば、ネットワークＮＷに接続され、ネットワークＮＷを介して、サーバ装置２０と通信を行う機能部に相当する。

[0021] クライアント制御部１２は、例えば、ＣＰＵなどを含むプロセッサであり、クライアント装置１０を統括的に制御する。クライアント制御部１２は、

例えば、サーバ装置２０からの制御に従い、撮像部１３に撮像を開始または停止させたり、撮像部１３に対し撮像するカメラの方向や、撮像する際の倍率等の撮像条件を設定したりする。

撮像部１３は、クライアント制御部１２の指示に従い、所定箇所における風景を撮像する。撮像部１３は、撮像したデータ（撮像データ）を、クライアント制御部１２に出力する。

[0022] サーバ装置２０は、ＮＷ（ネットワーク）通信部２１と、サーバ制御部２２と、撮像データ記憶部２３とを備える。ＮＷ通信部２１は、例えば、サーバ装置２０のイーサネット（登録商標）のポートである。ＮＷ通信部２１は、サーバ側の通信制御装置３１に接続され、サーバ装置２０からクライアント装置１０に対して送信されるデータをサーバ側の通信制御装置３１に出力する。なお、ＮＷ通信部２１は、従来のシステムであれば、ネットワークＮＷに接続され、ネットワークＮＷを介して、クライアント装置１０と通信を行う機能部に相当する。

[0023] サーバ制御部２２は、例えば、ＣＰＵなどを含むプロセッサであり、サーバ装置２０を統括的に制御する。サーバ制御部２２は、例えば、クライアント装置１０により撮像された撮像データを、撮像データ記憶部２３に記憶させる。撮像データ記憶部２３は、サーバ制御部２２の指示に従い、撮像データを記憶する。

[0024] クライアント装置１０とサーバ装置２０とが、互いのＮＷ通信部およびネットワークＮＷを介して接続された場合、クライアント装置とサーバ装置２０との間の通信には、ネットワーク監視カメラにおける一般的な通信プロトコルであるＨＴＴＰが用いられることがある。

[0025] この場合、クライアント装置１０、またはサーバ装置２０によりネットワークＮＷに出力された、暗号化されていない情報（いわゆる、平文）がネットワークＮＷを流れる。この場合、外部から悪意をもってネットワークＮＷ上のデータが取得されてしまうと、容易に撮像データが盗聴されたり、改ざんされたりする危険性がある。このような不正な攻撃に対する対策として、

クライアント装置１０には撮像データを暗号化させてネットワークＮＷに出力させることが考えられる。例えば、クライアント装置１０のクライアント制御部１２は、撮像データを暗号化し、暗号化した撮像データをネットワークＮＷに出力する。

[0026] しかしながら、そもそも監視カメラが備えるＣＰＵ等のプロセッサは、撮像データの圧縮や符号化の用途に用いられるために用いられる用途で用いられることが一般的であるため、さらに暗号化のための処理を行うだけの資源（リソース）を備えていないことが多い。このような場合、クライアント制御部１２が元々有するＣＰＵでは、撮像データを暗号化させることができない。クライアント制御部１２に撮像データを暗号化させる場合には、撮像データを暗号化するためのプロセッサを、更にクライアント制御部１２に搭載させる等、クライアント制御部１２のハードウェア構成の変更や置換えが必要となることが考えられる。クライアント装置１０は、監視カメラ等の社会インフラを構成するコンポーネントであるため、ハードウェア構成を変更したり置換えたりすることが容易にはできない。このような事情を鑑みると、クライアント装置１０変更を加えることなく、撮像データが暗号化されてネットワークＮＷに出力されることが望ましい。

[0027] 通信システム１は、クライアント装置１０とネットワークＮＷとの間に接続されたクライアント側の通信制御装置３０が、クライアント装置１０が送信するデータを暗号化してネットワークＮＷに出力する。また、サーバ装置２０とネットワークＮＷとの間に接続されたサーバ側の通信制御装置３１は、サーバ装置２０が送信する制御データを暗号化してネットワークＮＷに出力する。これにより、クライアント装置１０、およびサーバ装置２０を変更することなく、ネットワークＮＷを流れる撮像データの安全性を向上させる。

[0028] ここでは、クライアント側の通信制御装置３０、およびサーバ側の通信制御装置３１の構成について図３を用いて説明する。図３は、図１に示すクライアント側の通信制御装置３０、およびサーバ側の通信制御装置３１の機能

構成例を示すブロック図である。クライアント側の通信制御装置３０、およびサーバ側の通信制御装置３１の機能構成は同じである。このため、以下では、一方（例えば、クライアント側の通信制御装置３０）の構成について説明し、他方（例えば、サーバ側の通信制御装置３１）の構成については説明を省略する。また、以下では、クライアント側の通信制御装置３０とサーバ側の通信制御装置３１とを区別しない場合には、単に、通信制御装置３０（３１）などと称する。

[0029] 図３に示すように、通信制御装置３０（３１）は、ＮＷ（ネットワーク）通信部３２と、制御部３３と、装置通信部３４と、リーダライタ３５と、ＩＣカード４０とを備える。

ここで、ＩＣカード４０は、「認証部」の一例である。認証部は、リーダライタ３５およびＩＣカード４０で実現するものに限定されない。認証部は、制御部３３が実現しても良いし、認証処理用の処理回路で実現しても良い。

ＮＷ通信部３２は、ネットワークＮＷに接続され、ネットワークＮＷを介して、他方の通信制御装置３０（３１）と通信を行う。

[0030] 制御部３３は、例えば、ＣＰＵなどを含むプロセッサであり、通信制御装置３０（３１）を統括的に制御する。制御部３３は、例えば、リーダライタ３５を介して、ＩＣカード４０にコマンドを送信するとともに、ＩＣカード４０からレスポンスを受信する。また、制御部３３は、ＩＣカード４０から受信したレスポンスに基づく情報を、ＮＷ通信部３２を介して、他方の通信制御装置３０（３１）に送信する。また、制御部３３は、ＮＷ通信部３２を介して、他方の通信制御装置３０（３１）から受信した情報に基づいて、ＩＣカード４０にコマンドを送信する。

[0031] 装置通信部３４は、装置（クライアント装置１０、またはサーバ装置２０）に接続され、装置と通信を行う。具体的には、クライアント側の通信制御装置３０の装置通信部３４は、クライアント装置１０に接続され、クライアント装置１０からの撮像データを取得するとともに、復号された制御データ

をクライアント装置１０に出力する。また、サーバ側の通信制御装置３１の装置通信部３４は、サーバ装置２０に接続され、サーバ装置２０からの制御データを取得するとともに、復号された撮像データをサーバ装置２０に出力する。

[0032] リーダライタ３５は、コンタクト部３６を介してＩＣカード４０に接続し、ＩＣカード４０との間の通信を行う。

ＩＣカード４０は、例えば、プラスチックのカード基材に、ＩＣモジュール４１を実装して形成されている。すなわち、ＩＣカード４０は、ＩＣモジュール４１と、ＩＣモジュール４１が埋め込まれたカード基材とを備える。また、ＩＣカード４０は、通信制御装置３０（３１）に着脱可能に装着され、コンタクト部３６を介して通信制御装置３０（３１）と通信可能である。

[0033] ＩＣカード４０は、例えば、通信制御装置３０（３１）が送信したコマンド（処理要求）を、コンタクト部３６を介して受信し、受信したコマンドに応じた処理（コマンド処理）を実行する。そして、ＩＣカード４０は、コマンド処理の実行結果であるレスポンス（処理応答）を通信制御装置３０（３１）にコンタクト部３６を介して送信する。

[0034] ＩＣモジュール４１は、コンタクト部３６とＩＣチップ４２とを備える。コンタクト部３６は、ＩＣカード４０が動作するために必要な各種信号の端子を有している。ここで、各種信号の端子は、電源電圧、クロック信号、リセット信号などを通信制御装置３０（３１）から供給を受ける端子、及び、通信制御装置３０（３１）と通信するためのシリアルデータ入出力端子（ＳＩＯ端子）を有する。ＩＣチップ４２は、例えば、１チップのマイクロプロセッサなどのＬＳＩ（Large Scale Integration）である。

[0035] ここでは、ＩＣカード４０のハードウェア構成について図４を用いて説明する。図４は、図３に示すＩＣカード４０のハードウェア構成例を示す図である。

ＩＣカード４０は、コンタクト部３６と、ＩＣチップ４２とを備えたＩＣモジュール４１を備えている。そして、ＩＣチップ４２は、ＵＡＲＴ（Unive

rsal Asynchronous Receiver Transmitter）４３と、ＣＰＵ４４と、ＲＯＭ（Read Only Memory）４５と、ＲＡＭ（Random Access Memory）４６と、ＥＥＰＲＯＭ（登録商標）（Electrically Erasable Programmable ROM）４７とを備える。また、各構成（４３から４７）は、内部バスＢＳを介して接続されている。

[0036] ＵＡＲＴ４３は、上述したＳＩＯ端子を介して、通信制御装置３０（３１）とシリアルデータ通信を行う。ＵＡＲＴ４３は、ＳＩＯ端子を介して受信したシリアルデータ信号をパラレル変換したデータ（例えば、１バイトのデータ）を内部バスＢＳに出力する。また、ＵＡＲＴ４３は、内部バスＢＳを介して取得したデータをシリアル変換して、ＳＩＯ端子を介して通信制御装置３０（３１）に出力する。ＵＡＲＴ４３は、例えば、ＳＩＯ端子を介してコマンドを通信制御装置３０（３１）から受信する。また、ＵＡＲＴ４３は、ＳＩＯ端子を介してレスポンスを通信制御装置３０（３１）に送信する。

[0037] ＣＰＵ４４は、ＲＯＭ４５又はＥＥＰＲＯＭ４７に記憶されているプログラムを実行して、ＩＣカード４０の各種処理を行う。ＣＰＵ４４は、例えば、コンタクト部３６を介して、ＵＡＲＴ４３が受信したコマンドに応じたコマンド処理を実行する。

[0038] ＲＯＭ４５は、例えば、マスクＲＯＭなどの不揮発性メモリであり、ＩＣカード４０の各種処理を実行するためのプログラム、及びコマンドテーブルなどのデータを記憶する。ＲＡＭ４６は、例えば、ＳＲＡＭ（Static RAM）などの揮発性メモリであり、ＩＣカード４０の各種処理を行う際に利用されるデータを一時記憶する。ＥＥＰＲＯＭ４７は、例えば、電気的に書き換え可能な不揮発性メモリである。ＥＥＰＲＯＭ４７は、ＩＣカード４０が利用する各種データを記憶する。ＥＥＰＲＯＭ４７は、例えば、ＩＣカード４０を利用した各種サービス（アプリケーション）に使用される情報を記憶する。

[0039] 次に、ＩＣカード４０の構成について、図５を用いて説明する。図５は、図４に示すＩＣカード４０の機能構成例を示すブロック図である。ＩＣカー

ド４０は、通信部５０と、制御部５１と、記憶部５４とを備える。ここで、図５に示されるＩＣカード４０の各部は、図４に示されるＩＣカード４０のハードウェアを用いて実現される。

[0040] 通信部５０は、例えば、ＵＡＲＴ４３と、ＣＰＵ４４と、ＲＯＭ４５に記憶されているプログラムとにより実現され、コンタクト部３６を介して、例えば、通信制御装置３０（３１）との間でコマンド及びレスポンスの送受信を行う。すなわち、通信部５０は、所定の処理を要求するコマンド（処理要求）を通信制御装置３０（３１）から受信するとともに、コマンドに対するレスポンス（処理応答）を通信制御装置３０（３１）に送信する。通信部５０は、ＵＡＲＴ４３を介して通信制御装置３０（３１）から受信した受信データをＲＡＭ４６に記憶させる。また、通信部５０は、ＲＡＭ４６に記憶されている送信データを、ＵＡＲＴ４３を介して通信制御装置３０（３１）に送信する。

[0041] 制御部５１は、例えば、ＣＰＵ４４と、ＲＡＭ４５と、ＲＯＭ４６又はＥＥＰＲＯＭ４７とにより実現され、ＩＣカード４０を統括的に制御する。制御部５１は、コマンド処理部５２と暗号化復号部５３とを備える。

ここで、コマンド処理部５２が行う処理は、「認証処理」の一例である。また、暗号化復号部５３が行う処理は、「暗号化復号処理」の一例である。

[0042] コマンド処理部５２は、各種コマンド処理を実行する。コマンド処理部５２は、例えば、後述するＨＴＴＰＳリクエストを要求するコマンド処理として、ＳＳＬ／ＴＬＳハンドシェイクを行う。ＳＳＬ／ＴＬＳハンドシェイクでは、暗号化された通信に必要な鍵情報等の交換、および通信先の装置との相互認証を行う。ここで、相互認証とは、クライアント側の通信制御装置３０とサーバ側の通信制御装置３１とが、通信を行う前に、互いに正当に認証された装置であることを相互に確認する認証処理である。

[0043] 暗号化復号部５３は、データを暗号化する処理、および暗号化されたデータを復号する処理を実行する。暗号化復号部５３は、通信部５０を介して取得した装置（クライアント装置１０、またはサーバ装置２０）により出力さ

れたデータを暗号化する。また、暗号化復号部５３は、通信部５０を介して取得したネットワークＮＷからの暗号化されたデータを復号する。

[0044] 記憶部５４は、例えば、ＥＥＰＲＯＭ４７により構成された記憶部であり、証明書情報記憶部５５と、秘密情報記憶部５６とを備える。証明書情報記憶部５５は、通信制御管理装置５が発行した装置（クライアント装置１０、またはサーバ装置２０）に対する証明書を記憶する。具体的には、クライアント側の通信制御装置３０に装着されるＩＣカード４０の証明書情報記憶部５５には、クライアント証明書を示す情報が記憶される。また、サーバ側の通信制御装置３１に装着されるＩＣカード４０の証明書情報記憶部５５には、サーバ証明書を示す情報が記憶される。

[0045] 秘密情報記憶部５６は、通信制御管理装置５が発行した装置（クライアント装置１０、またはサーバ装置２０）に対する秘密鍵を記憶する。具体的には、クライアント側の通信制御装置３０に装着されるＩＣカード４０の秘密情報記憶部５６には、クライアント側の通信制御装置３０に対して発行された秘密鍵を示す情報が記憶される。また、サーバ側の通信制御装置３１に装着されるＩＣカード４０の証明書情報記憶部５５には、サーバ側の通信制御装置３１に対して発行された秘密鍵を示す情報が記憶される。

[0046] ここでは、通信制御管理装置５の構成について、図６を用いて説明する。図６は、図１に示す通信制御管理装置５の構成例を示すブロック図である。通信制御管理装置５は、例えば、ＮＷ（ネットワーク）通信部６０と、制御部６１と、記憶部６６とを備える。

ＮＷ通信部６０は、ネットワークＮＷに接続され、ネットワークＮＷを介して、通信制御装置３０（３１）と通信を行う。

[0047] 制御部６１は、例えば、ＣＰＵなどのプロセッサを含む。制御部６１は、プロセッサがプログラムを実行することにより種々の処理を実現する。制御部６１は、通信制御管理装置５を統括的に制御する。また、制御部６１は、主に通信制御装置３０（３１）の正当性を認めるプライベート認証局として動作する。図６に示す例では、制御部６１は、プロセッサがプログラムを実

行することにより、鍵生成部６２、証明書発行部６３、証明書更新部６４、証明書管理部６５および管理部６９としての機能を実現するための処理を実行する。

[0048] 鍵生成部６２は、例えば、通信制御装置３０（３１）からの認証申請に基づいて、後述する証明書に含まれる公開鍵に対応する秘密鍵の発行を行う。

[0049] 証明書発行部６３は、例えば、通信制御装置３０（３１）からの認証申請に基づいて、通信制御装置３０（３１）の正当性を認める証明書の発行を行う。証明書には、公開鍵と、通信制御装置３０（３１）の所有者を示す情報が含まれる。

[0050] 証明書更新部６４は、有効期限が渡過した証明書に対して新たな有効期限を設定することにより、証明書の更新を行う。証明書更新部６４は、例えば、通信制御装置３０（３１）からの更新申請に基づいて、当該通信制御装置３０（３１）に対して発行した証明書の有効期限を延長させた証明書を発行し、発行した証明書を通信制御装置３０（３１）に対して送信する。発行した証明書を示す情報が通信制御装置３０（３１）により受信され、通信制御装置３０（３１）のＩＣカード４０の証明書情報記憶部４０５に記憶されることで、通信制御装置３０（３１）の証明書の有効期限が延長される。

[0051] 証明書管理部６５は、既に発行済みの証明書に対する管理を行う。証明書管理部６５は、例えば、通信制御装置３０（３１）に装着されたＩＣカード４０の改ざん、または盗難等により相互認証において互いの正当性が証明されない場合に、通信制御装置３０（３１）に対して発行した証明書を無効化する処理を行う。また、証明書管理部６５は、通信制御装置３０（３１）からの問い合わせに基づいて、通信制御装置３０（３１）、および他の通信装置に対して発行した証明書が証明書管理部６５により発行されたものか否か応答するようにしてもよい。また、証明書管理部６５は、定期的に、発行済みの証明書が正当な通信制御装置３０（３１）に使用されているかを確認するようにしてもよい。

[0052] 管理部６９は、通信制御装置３０（３１）を管理する。例えば、管理部６

９は、通信制御装置３０（３１）が行う相互認証を、ネットワークＮＷを介して遠隔制御する。

記憶部６６は、例えば、鍵情報記憶エリア６７と、証明書情報記憶エリア６８とを備える。鍵情報記憶エリア６７は、例えば既に発行済みの公開鍵や、秘密鍵を示す情報を記憶する。証明書情報記憶エリア６８は、例えば既に発行済みの証明書を示す情報を記憶する。鍵情報記憶エリア６７と、証明書情報記憶エリア６８とは、例えば、鍵生成部６２が秘密鍵を発行する際、証明書発行部６３が証明書を発行する際などに参照される。また、鍵情報記憶エリア６７には、鍵生成部６２が発行した秘密鍵を示す情報が記憶される。また、証明書情報記憶エリア６８には、証明書発行部６３が発行した証明書を示す情報が記憶される。

[0053] ここでは、通信システム１が行う処理の流れについて、図７を用いて説明する。

[0054] 図７は、通信システム１が行う処理の一例を示すシーケンスチャートである。

[0055] クライアント装置１０は、撮像データをサーバ装置２０に送信する場合、まずサーバ装置２０に対するＨＴＴＰリクエストを送信する（ステップＳ１）。クライアント装置１０が送信したＨＴＴＰリクエストは、クライアント側の通信制御装置３０により取得される（ステップＳ２）。

[0056] クライアント側の通信制御装置３０は、クライアント装置１０により送信されたＨＴＴＰリクエストを取得すると、サーバ側の通信制御装置３１に対して、ＨＴＴＰＳのリクエスト（Client Hello）を送信する（ステップＳ３）。これにより、クライアント側の通信制御装置３０とサーバ側の通信制御装置３１との間のハンドシェイクが開始される（ステップＳ４）。

[0057] 具体的には、クライアント側の通信制御装置３０が送信するClient Helloには、例えば、ＴＬＳのバージョン、および通信に用いる暗号方式やアルゴリズムのリストを示す情報が含まれる。サーバ側の通信制御装置３１は、Client Helloに対する応答として、クライアント側の通信制御装置３０に対しＨ

ＴＴＰＳのレスポンス（Server Hello）を送信する。サーバ側の通信制御装置３１が送信するServer Helloには、例えばClient Helloで提示された選択肢の中でサーバ装置２０が選択した情報が含まれる。換言すると、クライアント側の通信制御装置３０からの提示に対し、サーバ側の通信制御装置３１が選択を行うことで、通信における具体的な暗号化アルゴリズムが決定される。

[0058] そして、サーバ側の通信制御装置３１は、暗号化通信に用いる共通鍵に必要な情報を送る。共通鍵に必要な情報には、例えば、サーバ装置２０に対して発行された公開鍵とその証明書を示す情報、およびクライアント装置１０の公開鍵とその証明書を送ることを要求する情報が含まれる。クライアント側の通信制御装置３０は、サーバ側の通信制御装置３１に対して、自装置に対して発行された公開鍵とその証明書、及び暗号化通信に用いる共通鍵に必要な情報を送る。

[0059] クライアント側の通信制御装置３０とサーバ側の通信制御装置３１との間の相互認証は、例えば次のように行われる。クライアント側の通信制御装置３０は、今までに受信したServer Hello等から署名を生成し、サーバ側の通信制御装置３１に送信する。サーバ側の通信制御装置３１は、クライアント側の通信制御装置３０から受信した署名を、クライアント側の通信制御装置３０から受信した証明書に基づいて検証する。サーバ側の通信制御装置３１は、検証が成功すると、その証明書が間違いなくクライアント側の通信制御装置３０のものであると判定する。また、サーバ側の通信制御装置３１は、今までに受信したClient Hello等から署名を生成し、クライアント側の通信制御装置３０に送信する。クライアント側の通信制御装置３０は、サーバ側の通信制御装置３１から受信した署名を、サーバ側の通信制御装置３１から受信した証明書に基づいて検証する。クライアント側の通信制御装置３０は、検証が成功すると、その証明書が間違いなくサーバ側の通信制御装置３１のものであると判定する。

[0060] クライアント側の通信制御装置３０とサーバ側の通信制御装置３１との間

の相互認証が正しく行われると、クライアント側の通信制御装置３０とサーバ側の通信制御装置３１とは、それぞれ暗号化に用いる共通鍵を生成して交換する。

[0061] サーバ側の通信制御装置３１から送付されたサーバ装置２０に対して発行された公開鍵とその証明書が、クライアント側の通信制御装置３０に許容される証明書であれば、サーバ側の通信制御装置３１は、クライアント側の通信制御装置３０から送付された公開鍵とその証明書が、サーバ側の通信制御装置３１に許容される証明書であれば、ハンドシェイクを終了する。

[0062] サーバ側の通信制御装置３１は、クライアント側の通信制御装置３０とのハンドシェイクが確立されると、サーバ装置２０に対し、ＨＴＴＰリクエストを送信する（ステップＳ５）。ＨＴＴＰリクエストは、ステップＳ１においてクライアント装置１０から送信されるＨＴＴＰリクエストである。

[0063] サーバ側の通信制御装置３１により送信されたＨＴＴＰリクエストは、サーバ装置２０により受信される（ステップＳ６）。このとき、サーバ装置２０は、クライアント装置１０からＨＴＴＰリクエストが要求されたと認識する。このため、サーバ装置２０は、クライアント装置１０に対しするＨＴＴＰレスポンスを応答する（ステップＳ７）。サーバ装置２０が送信したＨＴＴＰレスポンスは、サーバ側の通信制御装置３１により取得される（ステップＳ８）。

[0064] サーバ側の通信制御装置３１は、取得したサーバ装置２０からのＨＴＴＰレスポンスを、ステップＳ４のハンドシェイクにおいて決定された共通鍵を用いて暗号化する（ステップＳ９）。サーバ側の通信制御装置３１により暗号化されたＨＴＴＰレスポンスは、ネットワークＮＷを介してクライアント側の通信制御装置３０に受信される（ステップＳ１０）。クライアント側の通信制御装置３０は、受信したＨＴＴＰレスポンスを、共通鍵を用いて復号する（ステップＳ１１）。クライアント側の通信制御装置３０により復号されたＨＴＴＰレスポンスは、クライアント装置１０に取得される（ステップＳ１２）。クライアント装置１０は、復号されたＨＴＴＰレスポンスを受信

する（ステップＳ１３）。このとき、クライアント装置１０は、サーバ装置２０からＨＴＴＰレスポンスが応答されたと認識する。このため、クライアント装置１０は、サーバ装置２０に対し、撮像データを送信する（ステップＳ１４）。

[0065] クライアント装置１０が送信した撮像データは、クライアント側の通信制御装置３０により取得される（ステップＳ１５）。クライアント側の通信制御装置３０は、クライアント装置１０により送信された撮像データを、共通鍵を用いて暗号化する（ステップＳ１６）。クライアント側の通信制御装置３０により暗号化された撮像データは、ネットワークＮＷを介してサーバ側の通信制御装置３１に受信される（ステップＳ１７）。

[0066] サーバ側の通信制御装置３１は、受信した撮像データを、共通鍵を用いて復号する（ステップＳ１８）。サーバ側の通信制御装置３１により復号された撮像データは、サーバ装置２０にとり取得される（ステップＳ１９）。サーバ装置２０は、復号された撮像データを受信する（ステップＳ２０）。このとき、サーバ装置２０は、クライアント装置１０からの撮像データを受信したと認識する。

[0067] なお、上記フローチャートのステップＳ４において、クライアント側の通信制御装置３０とサーバ側の通信制御装置３１との間の相互認証が正しく行われなかった場合、クライアント側の通信制御装置３０は、通信先との通信を許可しない。具体的には、クライアント側の通信制御装置３０は、通信先から送信された情報をクライアント装置１０に出力しない。相互認証が正しく行われなかった場合、通信先がサーバ側の通信制御装置３１に見せかけた不正な通信装置である可能性があるためである。この場合、クライアント側の通信制御装置３０は、例えば、相互認証が正しく行われなかった場合の通信記録を通信制御管理装置５に送信するようにしてもよい。これより、通信制御管理装置５は相互認証が正しく行われなかった場合の通信記録を取得することができ、管理下にあるクライアント側の通信制御装置３０に対する不正な通信のパターンや頻度を把握することで、ネットワークの異常を監視す

ることができる。

[0068] また、クライアント側の通信制御装置３０は、上記フローチャートのステップＳ４において行われるハンドシェイクにおいて相互認証の代わりにクライアント装置１０に対する通信を許可する通信機器の情報を示す送信先リストに基づいて、通信先との通信を許可するか否かを判定するようにしてもよい。送信先リストに示される通信機器の情報は、例えばＵＲＬ（Uniform Resource Locator）である。クライアント側の通信制御装置３０の制御部３３は、通信先のＵＲＬが送信先リストに登録されているＵＲＬである場合に当該通信先との通信を許可し、送信先リストに登録されていない場合には通信を許可しない。

[0069] また、制御部３３は、送信先リストを更新するようにしてもよい。制御部３３は、例えば、一定期間にクライアント装置１０に対する通信を許可された通信先のＵＲＬ、および許可されなかった通信先ＵＲＬを記憶させる。そして、制御部３３は、例えば、送信先リストに登録されたＵＲＬのうち、一定期間に通信が行われた通信先のＵＲＬを再度登録する等することにより送信先リストを更新する。あるいは、クライアント側の通信制御装置３０は、一定期間に通信を許可された通信先ＵＲＬ、および許可されなかった通信先ＵＲＬを通信制御管理装置５に送信するようにしてもよい。この場合、例えば、通信制御管理装置５は、クライアント側の通信制御装置３０と通信を行った通信先ＵＲＬに基づいて、送信先リストを更新するようにしてもよい。通信制御管理装置５により送信先リストが更新されることで、通信制御管理装置５が管理下にあるクライアント側の通信制御装置３０と通信する通信機器を一括して管理することができる。

[0070] また、クライアント側の通信制御装置３０は、ステップＳ４において行われるハンドシェイクが確立した後にクライアント装置１０に対して送信された情報（例えば、ファームウェアの更新プログラム）の内容が正しいか否かの検証を行うようにしてもよい。例えば、クライアント側の通信制御装置３０の制御部３３は、ネットワークＮＷを介してクライアント装置１０のファ

ームウェアの更新プログラムが送信された場合、検証用の鍵（検証鍵）を用いて検証する。この場合、通信制御管理装置５は、例えば、クライアント側の通信制御装置３０およびサーバ側の通信制御装置３１それぞれに検証鍵を送信するようにしてもよい。

[0071] 例えば、サーバ側の通信制御装置３１は、クライアント装置１０へ送信する情報（平文）からハッシュ値を生成し、生成したハッシュ値を検証鍵で暗号化する。そして、サーバ側の通信制御装置３１は、平文と暗号化したハッシュ値をさらに秘密鍵で暗号してクライアント装置１０へ送信する。また、クライアント側の通信制御装置３０は共通鍵を用いて情報を復号化し、平文と暗号化されたハッシュ値とを取得する。

[0072] また、クライアント側の通信制御装置３０は、取得した平文からハッシュ値を生成するとともに、暗号化されたハッシュ値を検証鍵で復号する。クライアント側の通信制御装置３０は、平文から生成したハッシュ値と、復号化したハッシュ値とが等しい値である場合、クライアント装置１０に対して送信された情報は正しい内容であると判定する。この場合、クライアント側の通信制御装置３０は、復号した情報（平文）をクライアント装置１０に出力する。一方、クライアント側の通信制御装置３０は、平文から生成したハッシュ値と復号化したハッシュ値が等しい値でない場合、クライアント装置１０に対して送信された情報は、サーバ装置２０またはサーバ側の通信制御装置３１に見せかけた不正な通信装置から送信された不正な情報である可能性があると判定する。この場合、クライアント側の通信制御装置３０は、復号した情報（平文）をクライアント装置１０に出力しない。

[0073] これにより、クライアント装置１０は、検証済みである正しい内容であることが検証された情報のみを受け取ることができる。また、通常、クライアント装置１０がファームウェアを更新する際の更新プログラムの内容が正しいか否かの判定を行うと考えられるが、クライアント装置１０に代わりサーバ側の通信制御装置３１がクライアント装置１０に対して送信された情報の内容を検証することにより、クライアント装置１０の処理負担を軽減させる

ことが可能となる。

[0074] 以上説明したように、通信システム１は、クライアント装置１０とネットワークＮＷとの間に接続されるクライアント側の通信制御装置３０と、サーバ装置２０とネットワークＮＷとの間に接続されるサーバ側の通信制御装置３１と、を備える。クライアント側の通信制御装置３０は、クライアント装置１０からの情報を暗号化してネットワークＮＷ経由でサーバ側の通信制御装置３１へ送信し、ネットワークＮＷからの情報（通信制御装置３１で暗号化されたサーバ装置２０からの情報）を復号してクライアント装置１０へ送信する。サーバ側の通信制御装置３１は、サーバ装置２０からの情報を暗号化してネットワークＮＷ経由でクライアント側の通信制御装置３０へ送信し、ネットワークＮＷからの情報（通信制御装置３０で暗号化されたクライアント装置からの情報）を復号してサーバ装置２０に送信する。

[0075] これにより、通信システム１は、社会インフラシステムを変更することなく、社会インフラシステムの安全性を向上させることができる。クライアント装置１０からサーバ装置２０に対して送信されたＨＴＴＰプロトコルの撮像データ（いわゆる平文）が、クライアント側の通信制御装置３０により、例えば、ＳＳＬ／ＴＬＳプロトコルと組み合わされて、安全性が向上されたＨＴＴＰＳに置き換えられるためである。また、サーバ装置２０かクライアント装置１０らに対して送信された制御データは、暗号化されるが、クライアント側の通信制御装置３０により復号されて、クライアント装置１０に受信されるため、クライアント装置１０に復号させる処理を行わせる必要がなく、既存の装置を変更することなくそのまま利用することができる。

[0076] また、通信システム１では、クライアント側の通信制御装置３０とサーバ側の通信制御装置３１とが相互認証を行うため、いずれか一方方向のみの認証を行う場合よりも安全性を向上させることができる。一般的なクライアント端末とサーバ装置とにおいては、サーバ装置に対して不特定多数のクライアント端末が通信を行うため、当該不特定多数のクライアント端末に対して正当なクライアント証明書を発行して管理し続けることは現実的ではない。

しかしながら、通信システムを適用する社会インフラシステムなどにおいては、クライアント装置１０とサーバ装置２０との関係は明確に特定されている。このため、クライアント側の通信制御装置３０とサーバ側の通信制御装置３１とが相互認証を行うことが可能であり、安全性を向上させることができる。

[0077] 一般に、クライアント証明書を有していないクライアント端末では、サーバ装置と通信を行うために、サーバ装置が発行したＩＤやパスワードの入力を求められることがある。このようなパスワード認証においては、安全性を維持するために、パスワードに対し文字と数字を組合せた長文の文字列が要求されたり、定期的なパスワードの変更等が求められたりすることがある。しかしながら、覚えなければならないパスワードが増えると、管理が面倒になってしまい、パスワードをメモに残したり、ウェブブラウザに記録させたりするなど、かえってパスワードが漏洩してしまう場合があった。

[0078] これに対し、通信システム１では、クライアント側の通信制御装置３０がクライアント証明書を有することにより、サーバ装置２０との間で確実に相互認証を行うことができる。このため、パスワード認証が不要となる。このため、パスワードを入力する手間や定期的に変更して管理する手間がなくなり、ユーザの利便性が向上する。つまり、ユーザに負担をかけることなく安全性を維持することができる。

[0079] また、クライアント証明書を有していないクライアント端末がＩＤやパスワードによる認証に基づいてサーバ装置と通信を行うシステムでは、ＩＤとパスワードが正しく入力できてしまえば、だれでもサーバ装置末と通信することができてしまう。このため、クライアント端末を不正に乗っ取り、サーバ装置へ不正にアクセスすることが可能となってしまう。例えば、不正に乗っ取られたサーバ装置によってクライアント端末の機能が制限され、解除するために身代金が要求されるといったランサムウェアに感染する可能性がある。

[0080] これに対し、上述した通信システム１では、クライアント装置１０とサー

バ装置２０との間で、通信制御装置３０（３１）を介した相互認証が行われることにより、クライアント装置１０やサーバ装置２０が不正に乗っ取られることがない。つまり、通信システム１では、ランサムウェアに対する対策も可能となる。

[0081] また、例えば、ネットワーク内に管理者が不在の端末（野良デバイスともいう）がある場合、その端末が不正に乗っ取られることにより、その端末がマルウェア等の攻撃を行う不正な端末として利用されてしまう場合がある。これに対し、上述した通信システム１では、クライアント装置１０とサーバ装置２０との間で、通信制御装置３０（３１）を介した相互認証が行われることにより、ネットワークＮＷの内部にある管理者が不在の端末が不正に乗っ取られて攻撃に利用された場合であっても、マルウェア等に感染することを防止することができる。

[0082] また、上述した通信システム１では、サーバ装置２０がサーバ側の通信制御装置３１に接続されており、サーバ装置２０の内部で認証処理を行わない。このため、サーバ装置２０の内部で証明書等を保持する必要がなく、サーバ側の通信制御装置３１に接続されたサーバ装置２０が通信制御管理装置５の管理下であることが明確となる。サーバ装置２０がすでにサーバ側の通信制御装置３１に相当する機能部を有している場合には、必ずしもサーバ装置２０とネットワークＮＷとの間にサーバ側の通信制御装置３１が物理的に接続される必要はない。この場合、サーバ装置２０が元々有するサーバ側の通信制御装置３１に相当する機能部により、クライアント側の通信制御装置３０との間の認証処理が行われる。

[0083] また、通信システム１では、ＩＣカード４０の制御部４０１において、相互認証と暗号化復号処理とのうち少なくともいずれか一方を行わせる。このため、通信制御装置３０（３１）の装置コストを抑制することができる。

[0084] また、通信システム１においては、通信制御装置３０（３１）に装着されたＩＣカード４０が相互認証と暗号化復号処理とのうち少なくともいずれか一方の処理を行う例を説明したが、通信システム１は、相互認証および暗号

化複合化処理を行う構成がＩＣカードに限定されるものではない。また、上述したＩＣカード４０としては、秘密鍵およびクライアント証明書（あるいは、サーバ証明書）を記憶する記憶機能と、相互認証と暗号化復号処理とのうち少なくともいずれか一方を行う処理機能を有している機能部であればよく、例えば、ＩＣチップが搭載されたＳＩＭカードであってもよいし、カードの形態を採用しなくてもよい。

[0085] また、通信システム１においては、クライアント側の通信制御装置３０のＩＣカード４０は、クライアント側の通信制御装置３０に対して着脱可能に装着される。これにより、通信システム１においては、ＩＣカード４０とクライアント側の通信制御装置３０とが分離可能であるため、どちらか一方を交換する場合には、当該一方のデバイスを交換すればよい。例えば、ＩＣカード４０とクライアント側の通信制御装置３０とが一体化された場合には、ＩＣカード４０に相当する部分を交換する場合には、クライアント側の通信制御装置３０全体を交換しなければならないが、この場合と比較して、通信システム１では、クライアント側の通信制御装置３０が有するＩＣカード４０等の特定の部分を交換する場合のメンテナンスコストを抑制することができる。

[0086] また、通信システム１は、通信制御管理装置５を更に備え、通信制御管理装置５は、クライアント側の通信制御装置３０に装着されたＩＣカード４０に記憶させる秘密鍵、及びクライアント証明書をクライアント側の通信制御装置３０に送信し、サーバ側の通信制御装置３１に装着されたＩＣカード４０に記憶させる秘密鍵、及びサーバ証明書をサーバ側の通信制御装置３１に送信する。これにより、通信システム１は、通信制御管理装置５により発行された正当な秘密鍵、証明書を用いて、ハンドシェイクを行い、共通鍵を決定することができ、上述した効果を奏する他、社会インフラシステムの安全性を更に向上させることができる。

[0087] なお、通信システム１の構成は、上述した例に限定されない。例えば、通信制御装置３０（３１）は、処理の負荷に基づき、ハードウェアにより通信

制御装置３０（３１）の機能を実現するＨＳＭ（Hardware Security Module）を用いてもよい。つまり、通信制御装置３０（３１）は、セキュアな処理が可能な限り、必ずしもＩＣカードを装着する構成に限らず、上記通信制御装置３０（３１）の機能を実現できるＩＣチップやＩＣモジュールを用いた構成としてもよい。

[0088] また、通信システム１においては、ＳＳＬ／ＴＬＳプロトコルを用いたセキュアな通信を常時行うようにしてもよいし、ＳＳＬ／ＴＬＳプロトコルを用いた通信を行うか否かを選択可能にしてもよい。また、クライアント装置１０とサーバ装置２０との間における双方向の通信のうち一方の方向の通信のみをＳＳＬ／ＴＬＳプロトコルを用いた通信としてもよい。また、ＳＳＬ／ＴＬＳプロトコルを用いたセキュアな通信を常時行うようにしてもよいし、ＳＳＬ／ＴＬＳプロトコルを用いた通信を行うか否かを選択可能にしてもよい。

[0089] ＳＳＬ／ＴＬＳプロトコルを用いた通信を常時行うようにすることで、通信制御装置３０（３１）により認証された正当な通信制御装置３０（３１）とは異なる装置からの通信を遮断することができる。このため、クライアント装置１０やサーバ装置２０に対する不正なアクセスや、クライアント装置１０やサーバ装置２０がマルウェアに感染することを抑止することができる。

[0090] また、通信システム１においては、ＳＳＬ／ＴＬＳプロトコルを用いた通信を常時行い、クライアント装置１０やサーバ装置２０に対する不正なアクセスを記憶するようにしてもよい。この場合、通信制御管理装置５に不正なアクセスの記録が送信されるようにしてもよい。通信制御管理装置５は、不正なアクセスの有無を認識することができ、システム全体に対する大規模攻撃が開始される前の予兆の段階を検出して対策することが可能となる。

[0091] また、通信システム１においては、通信制御装置３０（３１）は、定期的に、自装置が接続されているクライアント装置１０またはサーバ装置２０との接続が維持されているか否かを確認するようにしてもよい。この場合、通

信制御管理装置５に接続状態を示す情報が送信されるようにしてもよい。通信制御管理装置５は、通信制御装置３０（３１）から接続状態を示す情報が受信できない場合などには、通信制御装置３０（３１）がクライアント装置１０またはサーバ装置２０から切り離された判断し、当該切り離された通信制御装置３０（３１）を無効とする。こうすることで通信制御管理装置５は、切り離された通信制御装置３０（３１）が不正な装置に接続されてなりすましに悪用されることを抑制する。

[0092] また、通信システム１においては、通信制御装置３０（３１）に装着するＩＣカード４０に、ＣＣ（Common Criteria/ISO15408）認証を取得したセキュアエレメントと呼ばれる耐タンパ性の高いチップを搭載してもよい。このチップを用いて、秘密鍵や公開鍵を含む証明書を記憶させることにより、非常に高い安全性を維持することができる。

[0093] また、通信システム１においては、サーバ装置２０や通信制御管理装置５等から、通信制御装置３０（３１）を介して、クライアント装置１０のプログラムを更新させるようにしてもよい。通信制御装置３０（３１）を介してプログラムの更新（ファームウェアのアップデート）が行われることにより、安全にクライアント装置１０の機能を更新させることができる。このようにサーバ装置２０からクライアント装置１０に対してファームウェアが送信される場合、サーバ装置２０から送信されるファームウェアには、例えばサーバ側の通信制御装置３１により暗号化されたサーバ装置２０の署名が付与される。この場合、クライアント装置１０では、クライアント側の通信制御装置３０により署名が復号されることにより、送信されたファームウェアが間違いなくサーバ装置２０から送信されたファームウェアであると判定することができる。これにより、あたかもサーバ装置２０であるかのように装う不正な端末から、不正なファームウェアがクライアント装置１０に送信されてしまった場合であっても、クライアント装置１０に対し不正なファームウェアに基づく誤った更新がなされてしまうことを排除することができる。

[0094] また、このように通信制御装置３０（３１）を介して通信が行われること

により、サーバ装置２０や通信制御管理装置５等からクライアント装置１０にファームウェアを安全に更新することができるため、作業員が複数のクライアント装置１０に対して物理的に各々のクライアント装置１０が設置されている場所まで移動してファームウェアのアップデート作業を行う場合と比較して、作業コストを低減させることも可能である。

[0095] また、通信システム１においては、サーバ装置２０や通信制御管理装置５等から、通信制御装置３０（３１）を介して、クライアント装置１０の起動や停止を行ってもよい。通信制御装置３０（３１）を介して起動や停止（リモートアクティベーション）が行われることにより、安全にクライアント装置１０の機能を更新させることができ、セキュアな遠隔制御を実現させることができる。

[0096] また、通信システム１においては、クライアント装置１０、およびサーバ装置２０が有線により通信する場合を例に説明したが、これに限定されることはない。クライアント装置１０、およびサーバ装置２０のうち少なくともいずれかが無線ＬＡＮ等により無線通信を行う装置であってもよい。例えば、クライアント装置１０が無線通信によりサーバ装置２０と通信を行う場合、クライアント側の通信制御装置３０は、無線による通信機能を有し、クライアント装置１０により送信されるデータを暗号化し、暗号化したデータを、無線通信によりサーバ装置２０に送信する。

[0097] なお、上述した通信システム１において、クライアント側の通信制御装置３０がサーバ側の通信制御装置３１と通信を行う例を説明したが、クライアント側の通信制御装置３０の通信先はこれに限定されることはない。例えば、クライアント側の通信制御装置３０－１は、クライアント側の通信制御装置３０－２と通信を行ってもよい。クライアント側の通信制御装置３０－１は、クライアント側の通信制御装置３０－２から通信開始の合図を受信した場合、まずクライアント側の通信制御装置３０－２との間で相互認証を行い、クライアント側の通信制御装置３０－２が正当な通信端末であることを確認する。そして、相互認証が正しく行われた場合、クライアント側の通信制

御装置３０－１は、クライアント側の通信制御装置３０－２から受信した情報をクライアント装置１０に出力する。暗号を使用して送信データに認証子が付与されることにより、通信情報の改ざんの検出及び送信者の特定が可能となる。このため、通信システム１においては、クライアント側の通信制御装置３０とサーバ側の通信制御装置３１との通信、及びクライアント側の通信制御装置３０同士の通信において、「正しい相手から」、「改ざんされていないデータを受け取る」ことを確実にすることができる。

[0098] （第１の実施形態）

次に、第１の実施形態に係る通信システムについて説明する。

図８は、第１の実施形態に係る通信システム１００の第１構成例を示す図である。図８に示す通信システム１００は、図１に示すシステム構成において通信制御装置３０を通信制御装置１０１に置き換えたものである。また、図８に示す構成例において、通信制御装置１０１は、ネットワークＮＷとクライアント装置１０との間に、並列に設けた複数の通信デバイス１１１Ａ、１１１Ｂを有する。

[0099] 図８に示す構成において、通信システム１００における通信制御装置１０１以外の各装置は、図１に示す装置と同様な構成で実現することができる。このため、以下、通信制御装置１０１以外の構成については、詳細な説明を省略するものとする。

なお、通信システム１００においては、通信制御装置３１についても、通信制御装置１０１と同様に、ネットワークＮＷとサーバ装置２０との間に、並列に設けた複数の通信デバイスを具備する構成としても良い。

図９は、第１の実施形態に係る通信システム１００の第１の構成例における通信制御装置１０１の構成例を示すブロック図である。

図９に示す構成例において、通信制御装置１０１は、複数の通信デバイス１１１として並列に配置した第１通信デバイス１１１Ａと第２通信デバイス１１１Ｂとを有する。第１通信デバイス１１１Ａと第２通信デバイス１１１Ｂとは、通信制御装置１０１において、ネットワークＮＷ側に接続するハブ

１１４とクライアント側に接続するハブ１１５との間に並列に接続する。第１通信デバイス１１１Ａおよび第２通信デバイス１１１Ｂは、それぞれが上述した図１に示す通信制御装置３０と同等の通信処理を実行する構成を有する。

[0100] また、図９に示す構成例において、通信制御装置１０１は、第１通信デバイス１１１Ａと第２通信デバイス１１１Ｂとが共用する電源１１６およびメモリＩ／Ｆ１１７とを有するものとする。電源１１６は、外部電源に接続され、外部電源からの電力を各通信デバイス１１１Ａ、１１１Ｂへ供給する。メモリＩ／Ｆ１１７は、メモリカードなどのメモリデバイス１１８をセットするインターフェースである。例えば、メモリＩ／Ｆ１１７には、初期設定情報などの通信デバイス１１１Ａ、１１１Ｂに適用する情報を記憶したメモリデバイス１１８がセットされる。メモリＩ／Ｆ１１７にセットするメモリデバイス１１８は、通信デバイス１１１Ａ、１１１Ｂから供給されるデータ（例えば、ログデータ）を記憶するようにしても良い。

[0101] ただし、第１実施形態に係る通信制御装置１０１は、通信制御装置３０と同様な構成を有する複数の通信デバイスを並列に配置したシステムとして実現しても良い。このようなシステムでは、各通信デバイスがそれぞれ電源およびメモリＩ／Ｆなどを具備する構成として良い。また、通信制御装置１０１において、第１通信デバイス１１１Ａと第２通信デバイス１１１Ｂとは、ネットワークＮＷとクライアント装置１０との間に並列に配置するものであれば良い。例えば、通信制御装置１０１は、ハブ１１４及び１１５を設けずに、第１通信デバイス１１１Ａと第２通信デバイス１１１Ｂとが、それぞれネットワークＮＷおよびクライアント装置１０に接続するインターフェースを具備した構成であっても良い。

[0102] 各通信制御装置１０１において、第１通信デバイス１１１Ａおよび第２通信デバイス１１１Ｂは、ネットワークＮＷとクライアント装置１０との間に並列に配置され、何れか一方が通常通信モード（第１の通信モード）による通信処理を実行する。通信制御装置１０１は、通常通信モードで通信する通

信デバイス１１１Ａ、１１１Ｂを切り替えることによりネットワークＮＷとクライアント装置１０との間における通信制御を実現する。

[0103] ここで、通常通信モードは、上述したようなサーバ側の通信制御装置３１との相互認証に基づく共通鍵を用いた送受信データの暗号化および復号化を伴う通信を行う動作モードであるものとする。また、本実施形態において、通信制御装置１０１は、通常通信モードにおいて、後述するホワイトリストにある宛先との通信を許可するホワイトリスト運用モードで通信を実行するものとする。

[0104] なお、通信制御装置１０１において並列に設ける第１通信デバイス１１１Ａおよび第２通信デバイス１１１Ｂは、それぞれが独立した２つの通信処理用のソフトウエアで実現するものであっても良い。この場合、ハードウエアとしては１つの通信デバイスを２つのソフトウエアで実現する並列に配置した２つの通信デバイスとして動作するようにしても良い。

[0105] 各通信デバイス１１１（第１通信デバイス１１１Ａおよび１１１Ｂ）は、自身の故障、不正アクセス、あるいは、マルウエア感染などを検知する機能を有する。例えば、通信デバイス１１１は、故障、不正アクセス又はマルウエア感染などを示す故障や通信障害などの不具合を示す情報を通信制御管理装置（デバイス管理サーバ）５へ送信する。また、各通信デバイス１１１は、通信制御管理装置５からの指示に応じて動作モードを切り替える。例えば、各通信デバイス１１１は、通信制御管理装置５からの指示に応じて未通信状態から通常通信モードに切り替えたり、通常通信モードから未通信状態に切り替えたりする。

[0106] 各通信デバイス１１１（１１１Ａ、１１１Ｂ）は、図９に示すように、コントローラ１２０、ブリッジ１３２、ハブ１３３、ブリッジ１３４、リーダライタ１３５およびＩＣカード１４０を有する。

コントローラ１２０は、通信デバイス１１１を制御するものである。図９に示す構成例において、コントローラ１２０は、ＭＰＵ１２１、ＲＡＭ１２２、ＳＡＭ１２３およびデータメモリ１２４などを有する。

[0107] ＭＰＵ１２１は、コントローラ１２０の制御を司るプロセッサの一例である。ＭＰＵ１２１は、データメモリ１２４などに記憶したプログラムを実行することで種々の処理を実現する。例えば、コントローラ１２０は、ＭＰＵ１２１がプログラムを実行することにより、通信制御、故障検知、通信障害の検知、自己診断、および、ログ情報の収集などの処理を実行する。

[0108] また、コントローラ１２０は、ＭＰＵ１２１がプログラムを実行することにより、サーバ側の通信制御装置３１との相互認証処理、クライアント装置１０からネットワークＮＷへ送出するデータの暗号化処理、ネットワークＮＷを経由してクライアント装置へ送信される暗号化されたデータの復号化処理などを行うようにしても良い。また、コントローラ１２０は、リーダライタ１３５を介して接続するＩＣカード１４０に対して、相互認証処理、暗号化処理および復号化処理の少なくとも何れか１つを依頼するようにしても良い。

[0109] ＲＡＭ１２２は、ランダムアクセスメモリである。ＲＡＭ１２２は、作業用のデータを保持するワーキングメモリとして機能する。ＳＡＭ１２３は、シリアルアクセスメモリである。データメモリ１２４は、書き換え可能な不揮発性のメモリである。

データメモリ１２４は、プログラムおよび設定情報などを記憶する。例えば、データメモリ１２４は、通信を許可する宛先のリストを示すホワイトリストを記憶する。コントローラ１２０は、通信モードがホワイトリストにある宛先との通信を行うホワイトリスト運用モード（通常通信モード、第１の通信モード）である場合、データメモリ１２４に記憶するホワイトリストを参照して通信を実行する。また、コントローラ１２０は、データメモリ１２４にあるホワイトリストを通信制御管理装置５からの指示に応じて書き換えるようにしても良い。例えば、通信デバイス１１１は、ホワイトリストにある宛先をすべて削除することにより未通信状態とするようにしても良い。また、データメモリ１２４は、当該通信デバイスの動作状態を示すログ情報を記憶するようにしても良い。データメモリ１２４に蓄積したログ情報は、通

信制御管理装置（デバイス管理サーバ）５へ送ったり、自己診断処理などに用いたりする。

[0110] ブリッジ１３２、１３４は、通信インターフェース（通信部）として機能する。ブリッジ１３２おおよび１３４は、ハブ１３３を介してコントローラ１２０に接続される。

ブリッジ１３２は、通信デバイス１１１におけるネットワークＮＷ側の通信を実行する。ブリッジ１３２は、図３に示すＮＷ通信部３２としての通信を実現する。ブリッジ１３２は、ネットワークＮＷから受信するデータをハブ１３３を介してコントローラ１２０へ供給する。また、ブリッジ１３４は、コントローラ１２０またはＩＣカード１４０で暗号化したデータをネットワークＮＷへ送出する。

[0111] ブリッジ１３４は、通信デバイス１１１におけるクライアント装置１０側の通信を実行する。ブリッジ１３４は、図３に示す装置通信部３４としての通信を実現する。ブリッジ１３４は、クライアント装置１０からのデータをハブ１３３を介してコントローラ１２０へ供給する。例えば、ブリッジ１３４は、ネットワークＮＷからの暗号化されたデータをコントローラ１１０またはＩＣカード１４０で復号化したデータをクライアント装置１０へ送出する。

[0112] リーダライタ１３５およびＩＣカード１４０は、上述した図３に示すリーダライタ３５およびＩＣカード４０に相当するものである。ＩＣカード１４０は、上述した図４に示すＩＣカード４０と構成を有するもので実現できる。また、ＩＣカード１４０は、上述した図５に示すＩＣカード４０と同様な処理機能を有し、通信制御装置１０１における認証部の一例として機能する。

[0113] 次に、第１の実施形態に係る図８に示す構成の通信システム１００における第１の動作例について説明する。

図１０は、図８に示す構成の通信システム１００における動作例を説明するためのシーケンスである。

まず、通信制御装置１０１は、第１通信デバイス１１１Ａがホワイトリストに基づく通常の運用モード（通常通信モード、第１の通信モード）で通信を実行し（ステップＳ１０１）、第２通信デバイス１１１Ｂが未通信状態であるものとする（ステップＳ１０２）。

[0114] 第１通信デバイス１１１Ａのコントローラ１２０は、通常通信モードにおいて、通信データ量、通信速度、通信時間、エラーの検出頻度などの動作状態を監視し、当該第１通信デバイスにおける故障または通信障害の有無を検知する（ステップＳ１０３）。また、コントローラ１２０は、設定されたタイミングで自己診断を実行することにより当該通信デバイス１１１Ａ内における不具合の有無を検知するようにしても良い。また、各通信デバイス１１１は、不具合を検知する検知器を設け、検知器による検知結果をコントローラ１２０が取得する構成としても良い。

[0115] 第１通信デバイス１１１Ａのコントローラ１２０は、不具合を検知しなければ（ステップＳ１０３、ＮＯ）、通常通信モードでの通信を継続して実行する。また、第１通信デバイス１１１Ａのコントローラ１２０は、通常通信モードで通信を実行中に不具合を検知すると（ステップＳ１０３、ＹＥＳ）、不具合を示す情報を通信制御管理装置５へ送信する。

[0116] 通信制御装置１０１の第１通信デバイス１１１Ａが送信した不具合を示す情報は、通信制御管理装置５により取得される（ステップＳ１０５）。通信制御管理装置５の制御部６１は、通信制御装置１０１の第１通信デバイス１１１Ａからの不具合を示す情報に応じて、当該通信制御装置１０１の第２通信デバイス１１１Ｂを通常通信モードとし、第１通信デバイス１１１Ａを未通信状態するように制御する。

[0117] すなわち、第１通信デバイス１１１Ａからの不具合を示す情報を受信すると、通信制御管理装置５の制御部６１は、不具合を示す情報の発信元である通信制御装置１０１の第２通信デバイス１１１Ｂに対して通常通信モードへの切替を指示する（ステップＳ１０６）。この通信制御管理装置５からの通常通信モードへの切替を指示は、不具合を示す情報の発信元である通信制御

装置１０１の第２通信デバイス１１１Ｂにより取得される（ステップＳ１０７）。これにより、第２通信デバイス１１１Ｂのコントローラ１２０は、通信制御管理装置５からの通常通信モードへの切替指示に応じて動作モードを通常通信モードに切り替える（ステップＳ１０８）。

[0118] また、第１通信デバイス１１１Ａからの不具合を示す情報を受信すると、通信制御管理装置５の制御部６１は、不具合を示す情報の発信元である通信制御装置１０１の第１通信デバイス１１１Ａに対して未通信状態となることを指示する（ステップＳ１０９）。この通信制御管理装置５からの未通信状態への切替指示は、不具合を示す情報の発信元である第１通信デバイス１１１Ｂにより取得される（ステップＳ１１０）。これにより、第１通信デバイス１１１Ａのコントローラ１２０は、通信制御管理装置５からの未通信状態への切替指示に応じて動作モードを未通信状態に切り替える（ステップＳ１１１）。

[0119] ここで、第１通信デバイスと第２通信デバイスとの動作モードの切り替えは、通信制御装置１０１としての通信が途切れることが無いように切り替えられる。例えば、通信制御管理装置（デバイス管理サーバ）５は、第２通信デバイス１１１Ｂにおける通常通信モードへの切り替えが完了した後に第１通信デバイス１１１Ａを未通信状態にするようにする。これにより、通信制御管理装置５は、通信制御装置１０１における通信の可用性を確実に確保することができる。

[0120] なお、通信制御装置１０１は、通常通信モードで通信を実行中の一方の通信デバイスに不具合が発生した場合に、他方の通信デバイスで通常通信モードでの通信を実行するように切り替える制御を通信制御装置１０１内で実現するようにしても良い。例えば、通常通信モードで通信を実行中の第１通信デバイスが不具合を検知した場合、第１通信デバイス１１１Ａのコントローラ１２０が第２通信デバイス１１１Ｂに対して通常通信モードへの切替を要求するようにしても良い。これにより、第２通信デバイス１１１Ｂは要求に応じて通常通信モードで起動し、第１通信デバイス１１１Ａが未通信状態に

遷移するようにできる。この場合、第１通信デバイスと第２通信デバイスとは互いのアドレスによって通信することが可能である。

[0121] 次に、第１の実施形態に係る通信システムの第２の構成例について説明する。

図１１は、第１の実施形態に係る通信システム１００´の第２の構成例を示す図である。図１１に示す通信システム１００´は、図１に示すシステム構成において通信制御装置３０を通信制御装置１０１´に置き換えたものである。また、図１１に示す構成例において、通信制御装置１０１´は、ネットワークＮＷとクライアント装置１０との間に、直列に配置した複数の通信デバイス１１１Ｃ、１１１Ｄを有する。

[0122] 図１１に示す構成において、通信システム１００´における通信制御装置１０１´以外の各装置は、図１に示す装置と同様な構成で実現することができる。このため、以下、通信制御装置１０１´以外の各装置の構成については、詳細な説明を省略するものとする。

なお、通信システム１００´においては、通信制御装置３１についても、通信制御装置１０１´と同様に、ネットワークＮＷとサーバ装置２０との間に、直列に配置した複数の通信デバイスを具備する構成としても良い。

図１２は、第１の実施形態に係る通信システム１００´の第２の構成例における通信制御装置１０１´の構成例を示すブロック図である。

図１２に示す構成例において、通信制御装置１０１´は、複数の通信デバイス１１１として、直列に配置した第１通信デバイス１１１Ｃと第２通信デバイス１１１Ｄとを有する。図１２に示す例では、通信制御装置１０１´において、ネットワークＮＷに接続する第１通信デバイス１１１Ｃとクライアント装置１０に接続する第２通信デバイス１１１Ｄとが直列に接続される。

[0123] また、図１２に示す構成例において、通信制御装置１０１´は、第１通信デバイス１１１Ｃと第２通信デバイス１１１Ｄとが共用する電源１１６およびメモリＩ／Ｆ１１７とを有するものとする。電源１１６は、図９と同様に、外部電源に接続され、外部電源からの電力を各通信デバイス１１１Ｃ、１

１１Ｄへ供給するものである。また、メモリＩ／Ｆ１１７は、図９と同様に、メモリカードなどのメモリデバイス１１８をセットするインターフェースである。

ただし、通信制御装置１０１´は、通信制御装置３０と同様な構成を有する複数の通信デバイスを直列に配置したシステムとして実現しても良い。このようなシステムでは、複数の通信デバイス１１１´がそれぞれ電源およびメモリＩ／Ｆなどの構成を具備するものとして良い。

[0124] 第１通信デバイス１１１Ｃおよび第２通信デバイス１１１Ｄは、それぞれが上述した図１に示す通信制御装置３０と同等の通信処理を実行する構成を有する。すなわち、各通信制御装置１０１内において、ネットワークＮＷとクライアント装置１０との間に直列に配置された第１通信デバイス１１１Ｃおよび第２通信デバイス１１１Ｄは、何れか一方が通常通信モード（第１の通信モード）による通信を行い、他方がパススルーモード（第２の通信モード）で通信を行う。

[0125] ここで、パススルーモード（第２の通信モード）は、入力する情報をそのまま通過させて出力する通信モードである。また、通常通信モードは、上述したようにサーバ側の通信制御装置３１との相互認証に基づく共通鍵を用いた送受信データの暗号化および復号化を伴う通信を行う動作モードであるものとする。また、本実施形態において、通信制御装置１０１´は、通常運用モードにおいて、上述したようなホワイトリストにある宛先との通信を許可するホワイトリスト運用モードで通信を実行するものとする。

[0126] なお、通信制御装置１０１´において直列に設ける第１通信デバイス１１１Ｃおよび第２通信デバイス１１１Ｄは、それぞれが独立した２つの通信処理用のソフトウエアで実現するものであっても良い。この場合、ハードウエアとしては１つの通信デバイスを２つのソフトウエアで実現する並列に配置した２つの通信デバイスとして動作するようにしても良い。

[0127] 各通信デバイス１１１´（第１通信デバイス１１１Ｃおよび１１１Ｄ）は、自身の故障、不正アクセス、あるいは、マルウエア感染などを検知する機

能を有する。例えば、通信デバイス１１１´は、故障、不正アクセス又はマルウエア感染などを示す故障や通信障害などの不具合を示す情報を通信制御管理装置（デバイス管理サーバ）５へ通知する。また、各通信デバイス１１１´は、通信制御管理装置５からの指示に応じて動作モードを切り替える。例えば、各通信デバイス１１１´は、通信制御管理装置５からの指示に応じてパススルーモードから通常通信モードに切り替えたり、通常通信モードからパススルーモードに切り替えたりする。

[0128] 図１２に示すように、各通信デバイス１１１´（１１１Ｃ、１１１Ｄ）は、図９に示す構成と同様に、コントローラ１２０、ブリッジ１３２、ハブ１３３、ブリッジ１３４、リーダライタ１３５およびＩＣカード１４０などを有するものとする。また、コントローラ１２０は、ＭＰＵ１２１、ＲＡＭ１２２、ＳＡＭ１２３およびデータメモリ１２４などを有するものとする。これらの各構成は、図９に示す各構成と同様なもので実現できるため、詳細な説明を省略するものとする。

[0129] 次に、第１の実施形態に係る図１１に示す構成の通信システム１００´における動作例（第２の動作例）について説明する。

図１３は、図１１に示す構成の通信システム１００´における動作例を説明するためのシーケンスである。

まず、通信制御装置１０１´は、第１通信デバイス１１１Ｃがホワイトリストに基づく通常の運用モード（通常通信モード）で通信を実行し（ステップＳ１２１）、第２通信デバイス１１１Ｄがパススルーモードで動作するものとする（ステップＳ１２２）。

[0130] 第１通信デバイス１１１Ｃのコントローラ１２０は、通常通信モードにおいて、通信データ量、通信速度、通信時間、エラーの検出頻度などの動作状態を監視し、当該第１通信デバイスにおける故障または通信障害の有無を検知する（ステップＳ１２３）。また、コントローラ１２０は、設定されたタイミングで自己診断を実行することにより当該通信デバイス１１１Ａ内における不具合の有無を検知するようにしても良い。また、各通信デバイス１１

１は、不具合を検知する検知器を設け、検知器による検知結果をコントローラ１２０が取得する構成としても良い。

[0131] 第１通信デバイス１１１Ｃのコントローラ１２０は、不具合を検知しなければ（ステップＳ１２３、ＮＯ）、通常通信モードでの通信を継続して実行する。また、第１通信デバイス１１１Ｃのコントローラ１２０は、通常通信モードで通信を実行中に不具合を検知すると（ステップＳ１２３、ＹＥＳ）、不具合を示す情報を通信制御管理装置５へ通知する（ステップＳ１２４）。

[0132] 通信制御装置１０１´の第１通信デバイス１１１Ｃが通知する不具合を示す情報は、通信制御管理装置５により取得される（ステップＳ１２５）。通信制御管理装置５の制御部６１は、通信制御装置１０１´の第１通信デバイス１１１Ｃからの不具合を示す情報に応じて、当該通信制御装置１０１´の第２通信デバイス１１１Ｄを通常通信モードとし、第１通信デバイス１１１Ｃをパススルーモードとするように制御する。

[0133] すなわち、第１通信デバイス１１１Ｃからの不具合を示す情報を受信すると、通信制御管理装置５の制御部６１は、不具合を示す情報の発信元である通信制御装置１０１´の第２通信デバイス１１１Ｄに対して通常通信モードへの切替を指示する（ステップＳ１２６）。この通信制御管理装置５からの通常通信モードへの切替を指示は、不具合を示す情報の発信元である通信制御装置１０１´における第２通信デバイス１１１Ｄにより取得される（ステップＳ１２７）。これにより、第２通信デバイス１１１Ｄのコントローラ１２０は、通信制御管理装置５からの通常通信モードへの切替指示に応じて動作モードを通常通信モードに切り替える（ステップＳ１２８）。

[0134] また、第１通信デバイス１１１Ｃからの不具合を示す情報を受信すると、通信制御管理装置５の制御部６１は、不具合を示す情報の発信元である通信制御装置１０１´の第１通信デバイス１１１Ｃに対してパススルーモードとなることを指示する（ステップＳ１２９）。この通信制御管理装置５からのパススルーモードへの切替指示は、不具合を示す情報の発信元である第１通

信デバイス１１１Ｃにより取得される（ステップＳ１３０）。これにより、第１通信デバイス１１１Ｃのコントローラ１２０は、通信制御管理装置５からのパススルーモードへの切替指示に応じて動作モードをパススルーモードに切り替える（ステップＳ１３１）。

[0135] 以上のような第１の実施形態に係る通信システムによれば、通信制御装置において複数の通信デバイスを設けた冗長構成とする。これにより、第１の実施形態によれば、ネットワークを介したデータ通信におけるセキュリティ性を確保するための通信制御装置に故障や通信障害が発生しても通信が途切れることなく継続することができるような確実な可用性をもった通信の運用を実現できる。

[0136] （第２の実施形態）

次に、第２の実施形態に係る通信システムについて説明する。

図１４は、第２の実施形態に係る通信システム２００の構成例を示す図である。図１４に示す通信システム２００は、図１に示すシステム構成においてクライアント側の通信制御装置３０を通信制御装置２０１に置き換えたものである。また、図１４に示す構成例において、通信制御装置２０１は、ネットワークＮＷとクライアント装置１０との間に、分散制御器２１２Ａおよび２１２Ｂを介して並列に配置した複数の通信デバイス２１１Ａ、２１１Ｂ、２１１Ｃを有する。

[0137] 図１４に示す構成において、通信システム２００における通信制御装置２０１以外の各装置は、図１に示す装置と同様な構成で実現することができる。このため、通信制御装置２００以外の構成については、詳細な説明を省略するものとする。

なお、通信システム２００においては、サーバ側の通信制御装置３１についても、通信制御装置２０１と同様に、ネットワークＮＷとサーバ装置２０との間に、分散制御器を介して並列に配置した複数の通信デバイスを具備する構成としても良い。

[0138] 図１５は、第２の実施形態に係る通信システム２００の構成例における通

信制御装置２０１の構成例を示すブロック図である。

図１５に示す構成例において、通信制御装置２０１は、複数の通信デバイス２１１として並列に配置した３つの通信デバイス２１１Ａ、２１１Ｂ、２１１Ｃを有する。複数の通信デバイス２１１Ａ～２１１Ｃは、通信制御装置２０１において、ネットワークＮＷに接続する分散制御器２１２Ａとクライアント装置１０に接続する分散制御器２１２Ｂとの間に並列に接続する。複数の通信デバイス２１１Ａ～２１１Ｃは、それぞれが上述した図１に示す通信制御装置３０と同等の通信処理を実行する構成を有する。また、分散制御器２１２Ａ、２１２Ｂは、通信処理の負荷を複数の通信デバイス２１１Ａ～２１１Ｃに分散する制御を行う。したがって、暗号化復号処理や、証明書による相互認証処理も、それぞれの通信デバイス２１１Ａ～２１１Ｃが有するコントローラが処理を行うことができる。

[0139] また、図１５に示す構成例において、通信制御装置２０１は、複数の通信デバイス２１１Ａ～２１１Ｃ、分散制御器２１２Ａ、２１２Ｂが共用する電源２１６を有する。また、通信制御装置２０１は、複数の通信デバイス２１１Ａ～２１１Ｃが共用するおよびメモリＩ／Ｆ２１７も有する。電源２１６は、外部電源に接続され、外部電源からの電力を各通信デバイス２１１Ａ～２１１Ｃおよび分散制御器２１２Ａ、２１２Ｂへ供給する。メモリＩ／Ｆ２１７は、メモリカードなどのメモリデバイス２１８をセットするインターフェースである。例えば、メモリＩ／Ｆ２１７には、各通信デバイス２１１に対する設定情報などを記憶したメモリデバイス２１８がセットされる。

[0140] なお、第２の実施形態に係る通信制御装置２０１において、並列に配置される通信デバイス２１１の個数は、３個に限定されるものではく、複数であれば良い。また、通信制御装置２０１において、並列に配置される各通信デバイス２１１は、同内容の通信処理を行うものであれば良く、処理能力が異なるものであっても良い。さらには、通信制御装置２０１において、並列に配置される各通信デバイス２１１は、処理能力が異なるもの置き換えても良い。

[0141] また、第２の実施形態に係る通信制御装置２０１は、通信制御装置３０と同様な構成を有する複数の通信デバイスを２つの分散制御器２１２Ａ、２１２Ｂ間に並列に配置した分散デバイスシステムとして実現しても良い。この場合、分散デバイスシステムを構成する各通信デバイスは、それぞれ電源およびメモリＩ／Ｆなどを具備し、独立して動作することができる装置として構成されるものとして良い。

[0142] 各通信デバイス２１１（２１１Ａ～２１１Ｃ）は、図１５に示すように、コントローラ２２０、ブリッジ２３２、ハブ２３３、ブリッジ２３４、リーダライタ２３５およびＩＣカード２４０を有する。

コントローラ２２０は、通信デバイス２１１を制御するものである。図１５に示す構成例において、コントローラ２２０は、ＭＰＵ２２１、ＲＡＭ２２２、ＳＡＭ２２３およびデータメモリ２２４などを有する。

[0143] ＭＰＵ２２１は、コントローラ２２０の制御を司るプロセッサの一例である。ＭＰＵ２２１は、データメモリ２２４などに記憶したプログラムを実行することで種々の処理を実現する。例えば、コントローラ２２０は、ＭＰＵ２２１がプログラムを実行することにより、通信制御、故障検知、通信障害の検知、通信状態の監視、自己診断、および、ログ情報の取集などの処理を実行する。

[0144] また、コントローラ２２０は、ＭＰＵ２２１がプログラムを実行することにより、サーバ側の通信制御装置３１との相互認証処理、クライアント装置１０からネットワークＮＷへ送出するデータの暗号化処理、ネットワークＮＷを経由してクライアント装置へ送信される暗号化されたデータの復号化処理などを行うようにしても良い。また、コントローラ２２０は、相互認証処理、暗号化処理および復号化処理の少なくとも何れか１つをＩＣカード２４０に対して依頼するようにして良い。

[0145] ＲＡＭ２２２は、ランダムアクセスメモリである。ＲＡＭ２２２は、作業用のデータを保持するワーキングメモリとして機能する。ＳＡＭ２２３は、シリアルアクセスメモリである。データメモリ２２４は、書き換え可能な不

揮発性のメモリである。

データメモリ２２４は、プログラムおよび設定情報などを記憶する。例えば、データメモリ２２４は、通信を許可する宛先のリストを示すホワイトリストを記憶する。コントローラ２２０は、データメモリ２２４に記憶するホワイトリストを参照して通常通信モード（第１の通信モード）での通信を実行する。また、データメモリ２２４は、当該通信デバイスの動作状態を示すログ情報を記憶するようにしても良い。また、データメモリ２２４は、当該通信デバイスにおける通信量を示す情報を記憶するようにしても良い。また、データメモリ２２４は、ログデータの分析などによる自己診断処理などを実行したりする。

[0146] ブリッジ２３２、２３４は、通信インターフェース（通信部）として機能する。ブリッジ２３２および２３４は、ハブ２３３を介してコントローラ２２０に接続される。

ブリッジ２３２は、通信デバイス２１１におけるネットワークＮＷ側の通信を実行する。ブリッジ２３２は、図３に示すＮＷ通信部３２としての通信を実現する。ブリッジ２３２は、ネットワークＮＷから受信するデータをハブ２３３を介してコントローラ２２０へ供給する。また、ブリッジ２３４は、コントローラ２２０またはＩＣカード２４０で暗号化したデータをネットワークＮＷへ送出する。

[0147] ブリッジ２３４は、通信デバイス２１１におけるクライアント装置１０側の通信を実行する。ブリッジ２３４は、図３に示す装置通信部３４としての通信を実現する。ブリッジ２３４は、クライアント装置１０からのデータをハブ２３３を介してコントローラ２２０へ供給する。また、ブリッジ２３４は、ネットワークＮＷからの暗号化されたデータをコントローラ２２０またはＩＣカード２４０で復号化したデータをクライアント装置１０へ送出する。

[0148] リーダライタ２３５およびＩＣカード２４０は、上述した図３に示すリーダライタ３５およびＩＣカード４０に相当するものである。ＩＣカード２４

０は、上述した図４に示すＩＣカード４０と構成を有するもので実現できる。また、ＩＣカード２４０は、上述した図５に示すＩＣカード４０と同様な処理機能を有し、通信制御装置２０１における認証部の一例として機能する。

[0149] 各分散制御器２１２（２１２Ａ、２１２Ｂ）は、図１５に示すように、コントローラ２５１、メモリ２５２、ハブ２５３およびインターフェース（Ｉ／Ｆ）２５４を有する。

コントローラ２５１は、分散制御器２１２を制御するものである。コントローラ２５１は、プロセッサおよび各種のメモリなどを有する。コントローラ２５１においては、プロセッサがプログラムを実行することで種々の処理を実現する。例えば、コントローラ２５１は、プロセッサがプログラムを実行することにより各通信デバイス２１１Ａ～２１１Ｃへの通信負荷の分散制御を行う。

[0150] メモリ２５２は、設定情報などを記憶する。例えば、メモリ２５２は、通信負荷の分散を判断するための閾値などを記憶する。コントローラ２５１は、メモリ２５２に記憶した閾値などの設定情報に基づいて通信負荷に応じて複数の通信デバイスから通信処理を実行させる通信デバイスを決定する。

ハブ２５３は、ネットワークＮＷまたはクライアント装置１０と複数の通信デバイス２１１Ａ～２１１Ｃとを接続させるインターフェースである。ハブ２５３は、コントローラ２５１によって接続先する通信デバイスが制御される。

[0151] インターフェース２５４は、設定情報などを取得するためのインターフェースである。閾値などの設定情報を通信制御管理装置（デバイス管理サーバ）５から取得する運用形態とする場合、インターフェース２５４は、通信制御管理装置５と通信するための通信部として構成される。また、インターフェース２５４は、閾値などの設定情報を記憶したメモリカードなどのメモリデバイスから情報を読み取るメモリリーダで構成しても良い。また、インターフェース２５４は、閾値などの設定情報を供給する外部装置を接続するた

めのインターフェースであっても良い。

[0152] 次に、第２実施形態に係る図１４及び図１５に示す構成の通信システム２００の動作例について説明する。

図１６は、図１４及び図１５に示す構成の通信システム２００における分散制御器２１２（２１２Ａ、２１２Ｂ）の動作例を説明するためのフローチャートである。

まず、分散制御器２１２は、インターフェース２５４などにより入力される複数の通信デバイス２１１Ａ～２１１Ｃによる分散処理のための設定情報を受け付ける（Ｓ２０１）。分散処理のための設定情報を取得した場合（ステップＳ２０１、ＹＥＳ）、分散制御器２１２（２１２Ａ又は２１２Ｂ）のコントローラ２５１は、入力される設定情報に基づいて複数の通信デバイス２１１Ａ～２１１Ｃによる分散処理を決定するための閾値を設定する（ステップＳ２０２）。ここでは、１つの通信制御装置２０１において並列に配置される通信デバイスが３つである場合を想定するものとし、コントローラ２５１は、第１閾値と第２閾値とをメモリ２５２に保存するものとする。

[0153] 例えば、第１閾値は、通信処理を１つの通信デバイスで実施するか否かを判定するための通信制御装置２０１全体での処理の負荷に対する判定基準値である。分散制御器２１２のコントローラ２５１は、通信制御装置２０１全体での処理の負荷が第１閾値未満であれば１つの通信デバイスで通信処理を実行し、第１閾値以上であれば複数の通信デバイスで分散して通信処理を実行するものとする。

[0154] さらに、第２閾値は、通信処理を３つの通信デバイスで実施するか否かを判定するための通信制御装置２０１全体での処理の負荷に対する判定基準値である。分散制御器２１２のコントローラ２５２は、通信制御装置２０１全体での処理の負荷が第２閾値以上であれば３つの通信デバイスで分散して通信処理を実行し、第１閾値以上かつ第２閾値未満であれば２つの通信デバイスで分割して通信処理を実行するものとする。分散処理を実施するための設定情報としての閾値は、適宜設定できるようにしても良い。

[0155] また、分散制御器２１２Ａ、２１２Ｂのコントローラ２５１は、通信量などに基づく通信デバイスにおける処理の負荷を監視する（ステップＳ２０３）。例えば、ネットワークＮＷ側から入力する情報に対して通信デバイス２１１が復号化処理を実行するため、分散制御器２１２Ａのコントローラ２５１は、ネットワークＮＷ側から入力するデータ量を処理の負荷として監視する。また、クライアント装置１０から入力する情報に対しては通信デバイス２１１が暗号化処理を実行するため、分散制御器２１２Ｂのコントローラ２５１は、クライアント装置１０から入力するデータ量を処理の負荷として監視する。

[0156] 分散制御器２１２のコントローラ２５１は、監視している処理の負荷が第１閾値未満であれば（ステップＳ２０４、ＹＥＳ）、１つの通信デバイス２１１により通信処理を実行させる（ステップＳ２０５）。

例えば、複数の通信デバイスが動作している状態であれば、コントローラ２５１は、監視している処理の負荷が第１閾値未満となった場合に１つの通信デバイスだけで通信を実行し、通信を実行しない通信デバイスを未通信状態（スリープ状態）へ遷移させる。

これにより、分散制御器２１２は、処理の負荷が第１閾値未満である場合に、１つの通信デバイスだけで通信処理を実行し、その他の通信デバイスを未通信状態とすることで無駄な電力消費を抑制できる。

[0157] また、分散制御器２１２のコントローラ２５１は、監視している処理の負荷が第１閾値以上であれば（ステップＳ２０４、ＮＯ）、処理の負荷が第２閾値未満であるかを判定する（ステップＳ２０６）。コントローラ２５１は、処理の負荷が第１閾値以上かつ第２閾値未満である場合（ステップＳ２０６、ＹＥＳ）、２つの通信デバイスに分散して通信処理を実行させる（ステップＳ２０７）。

[0158] 例えば、１つの通信デバイス２１１Ａだけが動作している状態であれば、コントローラ２５１は、監視している処理の負荷が第１閾値以上かつ第２閾値未満となった場合、２つの目の通信デバイス２１１Ｂを通信可能な状態と

する。通信デバイス２１１Ａに加えて通信デバイス２１１Ｂが通信可能な状態となると、コントローラ２５１は、ハブ２５３から出力する情報を通信デバイス２１１Ａと通信デバイス２１１Ｂとへ振り分ける。

[0159] これにより、分散制御器２１２は、処理の負荷が第１閾値以上かつ第２閾値未満である場合に２つの通信デバイスで分散して処理を実行するようにできる。この結果として、分散制御器２１２は、処理が負荷に応じて動作させる複数の通信デバイスで分散して通信処理を実行でき、処理能力の不足によってデータ遅延などが発生することを防止できる。

[0160] また、分散制御器２１２のコントローラ２５１は、監視している処理の負荷が第２閾値以上であれば（ステップＳ２０６、ＮＯ）、３つの通信デバイスに分散して通信処理を実行させる（ステップＳ２０８）。例えば、２つの通信デバイス２１１Ａ及び２１１Ｂが動作している状態であれば、コントローラ２５１は、監視している処理の負荷が第２閾値以上となった場合、３つの目の通信デバイス２１１Ａを通信可能な状態とする。通信デバイス２１１Ａ及び２１１Ｂに加えて通信デバイス２１１Ｃが通信可能な状態となると、コントローラ２５１は、ハブ２５３から出力する情報を通信デバイス２１１Ａと通信デバイス２１１Ｂと通信デバイス２１１Ｃへ振り分ける。

[0161] これにより、分散制御器２１２は、処理の負荷が第２閾値以上である場合に３つの通信デバイス（最大数の通信デバイス）で分散して処理を実行するようにできる。この結果として、分散制御器２１２は、処理が負荷に応じて動作させる複数の通信デバイスで分散して通信処理を実行でき、処理能力の不足によってデータ遅延などが発生することを防止できる。

[0162] なお、上述した動作例は、複数の通信デバイスが正常に動作することを前提して説明したものであるが、分散制御器は、各通信デバイスにおける故障あるいは通信障害などの不具合を検知し、不具合が発生した通信デバイス以外で上述した分散制御を行うようにしても良い。また、全ての通信デバイスにおいて不具合が発生した場合には、分散制御器は、何れかの１つの通信デバイスをパススルーモードとして動作させてデータ通信を確実に継続させる

ようにしても良い。

[0163] また、上述した通信制御装置は、同等な複数の通信デバイスを並列に配置するものとしたが、処理能力が異なる複数の通信デバイスを並列に配置するようにしても良い。また、１つの通信デバイスをメインの処理デバイスとし、それ以外の通信デバイスをスレーブの処理デバイスとしてメインの通信デバイスの処理を補助するような運用としても良い。さらに、通信デバイスが実施する処理内容を分けて実施するようにしても良い。

[0164] 以上のように、第２実施形態に係る通信システムは、ネットワークとクライアント装置との間に分散制御器を介して複数の通信デバイスを並列に配置した通信制御装置を有する。分散制御器は、通信制御装置における処理の負荷を監視し、処理の負荷に応じた台数の通信デバイスで通信処理を分散して実行する。

[0165] これにより、１つの通信デバイスの最大通信許容量を超えたデータの通信を行う場合であっても、通信制御装置としてデータ遅延を起こす確率を減らすことができる。また、処理の負荷に応じた台数の通信デバイスで通信を実行するように制御するため、負荷が少ない状態で多数の通信デバイスを起動させることがなく、省電力化を図ることもできる。

[0166] （第３の実施形態）

次に、第３の実施形態に係る通信システムについて説明する。

図１７は、第３の実施形態に係る通信システム３００および通信制御装置３０１の構成例を示す図である。図１７に示す通信システム３００は、図１に示すシステム構成においてクライアント側の通信制御装置３０を通信制御装置３０１に置き換えたものである。ただし、通信システム３００において、ネットワークＮＷとサーバ装置２０との間に配置されるサーバ側の通信制御装置３１についても、通信制御装置３０１と同様の構成を有するものとして良い。なお、図１７に示す構成において、通信システム３００における通信制御装置３０１以外の各装置は、図１に示す装置と同様な構成で実現することができるため、詳細な説明を省略するものとする。

[0167] 図１７に示す構成例において、通信制御装置３０１は、電源３１６、メモリＩ／Ｆ３１７、コントローラ３２０、ブリッジ３３２、ハブ３３３、ブリッジ３３４、リーダライタ３３５、ＩＣカード３４０などを有する。

コントローラ３２０は、通信デバイス２１１を制御するものである。図１７に示す構成例において、コントローラ３２０は、ＭＰＵ３２１、ＲＡＭ３２２、ＳＡＭ３２３およびデータメモリ３２４などを有する。

[0168] ＭＰＵ３２１は、コントローラ３２０の制御を司るプロセッサの一例である。ＭＰＵ３２１は、データメモリ３２４などに記憶したプログラムを実行することで種々の処理を実現する。例えば、コントローラ３２０は、ＭＰＵ３２１がプログラムを実行することにより、通信制御、故障検知、通信障害の検知、通信量の分析、自己診断、ログ情報の保存およびログ情報の送信などの処理を実行する。

[0169] また、コントローラ３２０は、ＭＰＵ３２１がプログラムを実行することにより、サーバ側の通信制御装置３１との相互認証処理、クライアント装置１０からネットワークＮＷへ送出するデータの暗号化処理、ネットワークＮＷを経由してクライアント装置１０へ送信される暗号化されたデータの復号化処理などを行うようにしても良い。また、コントローラ３２０は、相互認証処理、暗号化処理および復号化処理の少なくとも何れか１つをＩＣカード３４０に対して依頼するようにして良い。

[0170] ＲＡＭ３２２は、ランダムアクセスメモリである。ＲＡＭ３２２は、作業用のデータを保持するワーキングメモリとして機能する。ＳＡＭ３２３は、シリアルアクセスメモリである。データメモリ３２４は、書き換え可能な不揮発性のメモリである。

データメモリ３２４は、プログラムおよび設定情報などを記憶する。例えば、データメモリ３２４は、通信を許可する宛先のリストを示すホワイトリストを記憶する。コントローラ３２０は、データメモリ３２４に記憶するホワイトリストを参照して通常通信モード（第１の通信モード）での通信を実行する。また、データメモリ３２４は、当該通信制御装置の動作状態を示す

ログ情報を記憶するようにしても良い。また、データメモリ３２４は、コントローラ３２０による当該通信制御装置における通信量の分析情報を記憶する。

[0171] ブリッジ３３２、３３４は、通信インターフェース（通信部）として機能する。ブリッジ３３２および３３４は、ハブ３３３を介してコントローラ３２０に接続される。

ブリッジ３３２は、通信制御装置３０１におけるネットワークＮＷ側の通信を実行する。ブリッジ３３２は、図３に示すＮＷ通信部３２としての通信を実現する。ブリッジ３３２は、ネットワークＮＷから受信するデータをハブ３３３を介してコントローラ３２０へ供給する。また、ブリッジ３３４は、コントローラ３２０またはＩＣカード３４０で暗号化したデータをネットワークＮＷへ送出する。

[0172] ブリッジ３３４は、通信制御装置３０１におけるクライアント装置１０側の通信を実行する。ブリッジ３３４は、図３に示す装置通信部３４としての通信を実現する。ブリッジ３３４は、クライアント装置１０からのデータをハブ３３３を介してコントローラ３２０へ供給する。また、ブリッジ３３４は、ネットワークＮＷからの暗号化されたデータをコントローラ３２０またはＩＣカード３４０で復号化したデータをクライアント装置１０へ送出する。

[0173] リーダライタ３３５およびＩＣカード３４０は、上述した図３に示すリーダライタ３５およびＩＣカード４０に相当するものである。ＩＣカード３４０は、上述した図４に示すＩＣカード４０と構成を有するもので実現できる。また、ＩＣカード３４０は、上述した図５に示すＩＣカード４０と同様な処理機能を有し、通信制御装置３０１における認証部の一例として機能する。

[0174] また、電源３１６は、外部電源に接続され、外部電源からの電力を当該通信制御装置３０１内の各部へ供給する。メモリＩ／Ｆ３１７は、メモリカードなどのメモリデバイス３１８をセットするインターフェースである。例え

ば、メモリＩ／Ｆ３１７には、通信制御装置３０１に対する設定情報などを記憶したメモリデバイス３１８がセットされる。

[0175] 次に、第３実施形態に係る図１７に示す構成の通信システム３００の動作例について説明する。

図１８は、図１７に示す通信システム３００における第１の動作例を説明するためのシーケンスである。

まず、通信制御装置３０１は、通常の運用において通信量を含むログ情報を蓄積する。例えば、通信制御装置３０１のコントローラ３２０は、通信インターフェースとしてのブリッジ３３２および３３４を通過するデータを監視することにより、当該通信制御装置３０１の通信量を示す情報をデータメモリ３２４に保存する。

[0176] 通信制御装置３０１のコントローラ３２０は、データメモリ３２４にログ情報として蓄積する通信量を示す情報を分析し、分析結果としての通信量の分析情報をデータメモリ３２４に記憶する（ステップＳ３０１）。例えば、コントローラ３２０は、所定の周期で通信量の分析を行って通信量の分析情報をデータメモリ３２４に記録する。通信量の分析情報は、例えば、時間当たりの通信量を示すものであっても良いし、時間帯ごとの通信量および通信量の増減傾向などを示すものであっても良いし、通信量が所定閾値未満となる時間帯あるいは通信量が最小となる時間帯を示す情報でも良い。第３の実施形態においては、通信量の分析情報は、当該通信制御装置３０１が自己診断を実施する時刻を決めるための情報であれば良い。

[0177] 通信制御装置３０１のコントローラ３２０は、データメモリ３２４に記憶した通信量の分析情報を通信制御管理装置（デバイス管理サーバ）５へ送信する（ステップＳ３０２）。コントローラ３２０は、例えば、所定のタイミングで通信量の分析情報を送信するようにしても良いし、通信制御管理装置５からの要求に応じて送信するようにしても良い。また、コントローラ３２０は、当該通信制御管理装置５における通信量が少ない時間帯を自己判断し、通信量が少ないと判断した時間帯に通信量の分析情報を通信制御管理装置

５へ送信するようにしても良い。

[0178] 通信制御装置３０１から送信される通信量の分析情報は、通信制御管理装置５に取得される（ステップＳ３０３）。通信制御管理装置５の制御部６１は、ＮＷ通信部６０により受信した通信量の分析情報を送信元の通信制御装置３０１を示す識別情報に対応づけて記憶部６６に記憶する。制御部６１は、受信した通信量の分析情報に基づいて当該通信制御装置３０１が自己診断を実行すべき時刻または時間帯を決定する（ステップＳ３０４）。例えば、制御部３０１は、通信量の分析情報に基づいて通信量が所定閾値未満となる時間帯のうち自己診断処理の要する時間が確保できる時刻を自己診断の実施時刻（実施予定時刻）として特定する。また、夜中等、長時間通信量が低くなるような使用状況下においては、所定閾値未満であるかどうかにかかわらず、自己診断処理の要する時間が確保できる時刻を自己診断の実施時刻（実施予定時刻）として特定してもよい。

[0179] 自己診断の実施時刻を決定した後、制御部６１は、自己診断の実施時刻になると、当該通信制御装置３０１に対して生死確認クエリを送信する（ステップＳ３０５）。生死確認クエリは、正常に動作中であるか否かの応答を要求するものである。通信制御装置３０１のコントローラ３２０は、通信制御管理装置５からの生死確認クエリを受信すると（ステップＳ３０６）、正常動作中であれば正常であることを示す応答を送信する（ステップＳ３０７）。また、通信制御装置３０１は、生死確認クエリに対して前回の自己診断を実施した日時などを応答するようにしても良い。

[0180] 通信制御管理装置５の制御部６１は、通信制御装置３０１からの応答に基づいて自己診断を実施させるか否かを判断する（ステップＳ３０８）。例えば、制御部６１は、通信制御装置から応答がない場合、あるいは、前回の自己診断を実施したに日時から所定期間以上経過している場合、当該通信制御装置３０１に自己診断を実施させるものと判断する。また、制御部６１は、通信制御装置３０１からの応答内容にかかわらず、自己診断を実施させるようにしても良い。自己診断を実施させる場合、通信制御管理装置５の制御部

６１は、当該通信制御装置３０１に対して自己診断の実施を要求する（ステップＳ３０９）。

[0181] 通信制御管理装置５のコントローラ３２０は、通信制御管理装置５からの自己診断の実施要求を受信すると、現在、自身が自己診断を実施できる状況であるかを判断する（ステップＳ３１１）。例えば、コントローラ３２０は、現在の通信量が所定の閾値未満であれば自己診断を実施するものとする。

[0182] これは、通信制御管理装置５が指定する自己診断の実施時刻は、過去の通信量（通信量の分析情報）に基づくものであって、実際には設定した時刻に通信量が多い可能性があるためである。第３実施形態に係るシステムは、通信制御装置や通信システム全体にできるだけ、負荷をかけずに自己診断を実行させるための制御を行うものである。このため、通信制御装置のコントローラは、実際の通信量が多くなっている場合には自己診断を実施しない（延期する）と判断するものとする。

[0183] 自己診断を実施する場合（ステップＳ３１１、ＹＥＳ）、コントローラ３２０は、自己診断を実施し（ステップＳ３１２）、自己診断の実行結果を示す情報を通信制御管理装置５へ送信する。この場合、自己診断の実行結果を示す情報は、通信制御装置３０１から送信され、通信制御管理装置５が取得する（ステップＳ３１３）。

また、自己診断を実施しない場合（ステップＳ３１１、ＮＯ）、コントローラ３２０は、自己診断を実施していないことを示す通知を通信制御管理装置５へ送信する（ステップＳ３１４）。この場合、自己診断を実施していないことを示す通知が、自己診断の実施要求に対する応答として通信制御管理装置５により取得される（ステップＳ３１５）。

[0184] 自己診断の実施要求に対する結果を取得すると、通信制御管理装置５の制御部６１は、自己診断の結果を記憶部６６に保存する（ステップ３１６）。例えば、通信制御装置３０で自己診断が実施された場合、制御部６１は、自己診断の実行結果を示す情報を実施日時と共に当該通信制御装置３０１の識別情報に対応づけて記憶部６６に記憶する。また、通信制御装置３０で自己

診断が実施されなかった場合、制御部６１は、自己診断が実施できなかった旨の情報を当該通信制御装置３０１の識別情報に対応づけて記憶部６６に記憶する。

[0185] また、通信制御管理装置５の制御部６１は、取得した自己診断の実行結果に対して異常の有無を検証する。自己診断の実行結果から異常と判断される項目があれる場合（ステップＳ３１７、ＹＥＳ）、制御部６１は、通信制御装置３０１または通信システム３００に異常があることを示すアラートを報知する（ステップＳ３１８）。また、生死確認クエリに対して通信制御装置３０１から応答がない場合も、制御部６１は、通信制御装置３０１または通信システム３００に異常があることを報知するようにしても良い。

[0186] 以上のように、第３実施形態の第１の動作例では、通信制御装置における通信量の分析情報を通信制御管理装置が取得し、通信制御管理装置が通信量の分析情報に基づいて通信制御装置に自己診断を実施させる時刻を設定する。

これにより、通信制御管理装置は、通信制御装置に対して、通信量が少なく、自己診断を行っても通常の通信処理に影響がない時間に自己診断を実施させることができる。この結果として、通信制御装置の状態を確認したり、故障や通信障害などを早期に発見したりするための自己診断を本来の通信システムに負荷をかけずに効率よく実施させることができる。

[0187] 次に、第３の実施形態に係る通信システム３００の第２の動作例について説明する。

図１９は、図１７に示す通信システム３００における第２の動作例を説明するためのシーケンスである。

通信制御装置３０１のコントローラ３２０は、上述した第１の動作例と同様に、データメモリ３２４にログ情報として蓄積する通信量を示す情報を分析し、分析結果としての通信量の分析情報をデータメモリ３２４に記憶する（ステップＳ３２１）。

[0188] 通信制御装置３０１のコントローラ３２０は、所定のタイミングでデータ

メモリ３２４に記憶した通信量の分析情報に基づいて自己診断を実行する予定の実施予定時刻を決定する（ステップＳ３２２）。例えば、コントローラ３２０は、通信量の分析情報に基づいて通信量が所定閾値未満となる時間帯のうち自己診断処理の要する時間が確保できる時刻を自己診断の実施時刻（実施予定時刻）として特定する。

[0189] 自己診断の実施予定時刻を決定した場合、コントローラ３２０は、自己診断の実施予定時刻を通信制御管理装置５へ通知する（Ｓ３２３）。この場合、通信制御管理装置５の制御部６１は、通信制御装置３０１から通知される自己診断の実施予定時刻を示す情報を当該通信制御装置３０１の識別情報に対応づけて記憶しておくようにしても良い。ただし、コントローラ３２０は、自己診断の実施予定時刻を通信制御管理装置５へ通知しなくても良い。

[0190] 自己診断の実施予定時刻を決定した後、制御部６１は、自己診断の実施予定時刻になると、自身が自己診断を実施できる状況であるかを判断する（ステップＳ３２４）。例えば、コントローラ３２０は、現在の通信量が所定の閾値未満であれば自己診断を実施する。

自己診断を実施する場合（ステップＳ３２４、ＹＥＳ）、コントローラ３２０は、自己診断を実施し（ステップＳ３２５）、自己診断の実行結果を示す情報を通信制御管理装置５へ送信する。自己診断の実行結果を示す情報は、通信制御装置３０１から送信され、通信制御管理装置５が取得する（ステップＳ３２６）。

また、自己診断を実施しない場合（ステップＳ３２４、ＮＯ）、コントローラ３２０は、自己診断を実施していないことを示す通知を通信制御管理装置５へ送信する（ステップＳ３２７）。この場合、自己診断を実施していないことを示す通知が、自己診断の実施要求に対する応答として通信制御管理装置５により取得される（ステップＳ３２８）。

[0191] 自己診断の実施要求に対する結果を取得すると、通信制御管理装置５の制御部６１は、自己診断の結果を記憶部６６に保存する（ステップ３２９）。また、通信制御装置３０で自己診断が実施されなかった場合、制御部６１は

、自己診断が実施できなかった旨の情報を当該通信制御装置３０１の識別情報に対応づけて記憶部６６に記憶する。

[0192] また、通信制御管理装置５の制御部６１は、取得した自己診断の実行結果に対して異常の有無を検証する（ステップＳ３３０）。自己診断の実行結果から異常と判断される項目がある場合（ステップＳ３３０、ＹＥＳ）、制御部６１は、通信制御装置３０１または通信システム３００に異常があることを示すアラートを報知する（ステップＳ３３１）。

[0193] 以上のように、第３実施形態の第２の動作例では、通信制御装置自身が通信量の分析情報に基づいて自己診断を実施する予定時刻を設定する。これにより、通信制御装置は、通信量が少なく自己診断を行っても通常の通信処理に影響がない時間に自己診断を実施するように計画することができる。この結果として、通信制御管理装置が通信制御装置の状態を確認したり故障や通信障害などを早期に発見したりするための自己診断を通信システムに負荷をかけずに効率よく実施させることができる。

[0194] （第４の実施形態）

次に、第４の実施形態に係る通信システムについて説明する。

第４の実施形態に係る通信システムは、上述した第３の実施形態に係る通信システム３００と同様な構成を有するものとする。従って、第４の実施形態については、第３の実施形態で説明した図１７に示す通信システム３００に適用する例として説明する。

[0195] 以下、第４実施形態に係る通信システム３００の動作例として第１～第４の動作例について説明する。

図２０は、第４の実施形態に係る通信システム３００における第１の動作例を説明するためのシーケンスである。

まず、通信制御装置３０１は、動作状態を示すログ情報をデータメモリ３２４に蓄積する。ここで、データメモリ３２４に蓄積するログ情報は、通信制御装置３０１の動作履歴を示す情報である。ただし、不正アクセスなどの緊急に通信制御管理装置５へ通知すべき情報は、ログ情報として保存しても

良いが、直ちに通信制御管理装置５へ通知される。

[0196] また、通常の運用における通信量を示す情報は、ログ情報としてデータメモリ３２４に蓄積するようにしても良い。例えば、通信制御装置３０１のコントローラ３２０は、通信インターフェースとしてのブリッジ３３２および３３４を通過するデータを監視することにより、当該通信制御装置３０１の通信量を示す情報をデータメモリ３２４に保存する。

[0197] 通信制御装置３０１のコントローラ３２０は、データメモリ３２４にログ情報として蓄積する通信量を示す情報を分析し、分析結果としての通信量の分析情報をデータメモリ３２４に記憶する（ステップＳ４０１）。例えば、コントローラ３２０は、所定の周期で通信量の分析を行って通信量の分析情報をデータメモリ３２４に記録する。通信量の分析情報は、例えば、時間当たりの通信量を示すものであっても良いし、時間帯ごとの通信量および通信量の増減傾向などを示すものであっても良いし、通信量が所定閾値未満となる時間帯あるいは通信量が最小となる時間帯を示す情報でも良い。第４の実施形態において、通信量の分析情報は、当該通信制御装置３０１がログ情報を通信制御管理装置（デバイス管理サーバ）５へ送信する時刻を決めるための情報であれば良い。

[0198] 通信制御装置３０１のコントローラ３２０は、データメモリ３２４に記憶した通信量の分析情報を通信制御管理装置（デバイス管理サーバ）５へ送信する（ステップＳ４０２）。コントローラ３２０は、例えば、所定のタイミングで通信量の分析情報を送信するようにしても良いし、通信制御管理装置５からの要求に応じて送信するようにしても良い。また、コントローラ３２０は、当該通信制御管理装置５における通信量が少ない時間帯を自己判断し、通信量が少ないと判断した時間帯に通信量の分析情報を通信制御管理装置５へ送信するようにしても良い。

[0199] 通信制御装置３０１から送信される通信量の分析情報は、通信制御管理装置５に取得される（ステップＳ４０３）。通信制御管理装置５の制御部６１は、ＮＷ通信部６０により受信した通信量の分析情報を送信元の通信制御装

置３０１を示す識別情報に対応づけて記憶部６６に記憶する（ステップＳ４０４）。制御部６１は、記憶部６６に記憶した各通信制御装置３０１からの通信量の分析情報に基づいて、各通信制御装置３０１がログ情報を送信するスケージュール（ログ収集のスケジュール）を決定する（ステップＳ４０５）。例えば、制御部３０１は、当該通信システムにおける各通信制御装置からの通信量の分析情報に基づいて、ネットワークＮＷ全体における通信量が所定閾値未満となるように、各通信制御装置３０１がログ情報を送信できる時刻（時間帯）をスケジューリングする。

[0200] ログ収集のスケジュールを作成すると、制御部６１は、個々の通信制御装置３０１に対してログ情報を送信する時刻（送出時刻）を通知する（ステップＳ４０６）。通信制御装置３０１のコントローラ３２０は、通信制御管理装置５からログ情報の送出時刻の通知を受信すると（ステップＳ４０７）、ログ情報の送出時刻をデータメモリ３２４に記憶する（ステップＳ４０８）。コントローラ３２０は、通信制御管理装置５から指示されたログ情報の送出時刻になると、データメモリ３２４に蓄積したログ情報を通信制御管理装置５へ送信する（ステップＳ４０９）。

[0201] 通信制御装置３０１から送信されるログ情報は、ネットワークＮＷを経由して通信制御管理装置５へ伝送され、通信制御管理装置５に受信される（ステップＳ４１０）。通信制御管理装置５の制御部６１は、通信制御装置３０１から受信したログ情報を記憶部６６に保存する（ステップ４１１）。例えば、制御部６１は、受信したログ情報を実施日時と共に当該通信制御装置３０１の識別情報に対応づけて記憶部６６に記憶する。

[0202] 上述した第４の実施形態に係る第１の動作例は、クライアント装置に接続する通信制御装置が自身の通信量の分析情報を通信制御管理装置へ送信し、通信制御管理装置は、通信システムにおける各通信制御装置からの通信量の分析情報に基づいて、個々の通信制御装置がログ情報を送信する時刻をスケジュールリングする。

[0203] これにより、各通信制御装置３０１が通信量の分析情報に基づいてログ情

報を送信する時刻を判断する必要がなく、通信制御管理装置は、通信システム全体の各通信制御装置における通信量を加味して各通信制御装置がログ情報の送出を決定できる。この結果、個々の通信制御装置だけでなく、ネットワーク全体に発生すると予測される負荷も考慮して各通信制御装置がログ情報を送出する時刻をコントローラできる。

[0204] 次に、第４の実施形態に係る通信システム３００における第２の動作例について説明する。

図２１は、第４の実施形態に係る通信システム３００における第２の動作例を説明するためのシーケンスである。

まず、通信制御装置３０１のコントローラ３２０は、上述の第１の動作例と同様に、データメモリ３２４にログ情報として蓄積する通信量を示す情報を分析し、分析結果としての通信量の分析情報をデータメモリ３２４に記憶する（ステップＳ４２１）。

通信制御装置３０１のコントローラ３２０は、データメモリ３２４に記憶した通信量の分析情報に基づいて、当該通信制御装置３０１がログ情報を送信する送出時刻の候補を選出する（ステップＳ４２２）。送出時刻の候補は、１つであっても良いし、複数であっても良いし、時間帯で示しても良い。

[0205] 例えば、コントローラ３２０は、当該通信制御装置における通信量の分析情報に基づき、通信量が最も少ない時間帯で当該通信制御装置３０１がログ情報を送信できる時刻を送出時刻の候補として選出する。また、制御部３０１は、当該通信制御装置における通信量の分析情報に基づき、通信量が所定閾値未満となる時間帯から当該通信制御装置３０１がログ情報を送信できる時刻（送出時刻）を選出しても良い。

[0206] ログ情報の送出時刻の候補を選出すると、コントローラ３２１０は、選出したログ情報の送出時刻の候補を通信制御管理装置５へ送信する（ステップＳ４２４）。これにより、通信制御装置３０１が選出するログ情報の送出時刻の候補は、通信制御管理装置５が取得する。

[0207] 通信制御管理装置５の制御部６１は、ＮＷ通信部６０により受信したログ

情報の送出時刻の候補を示す情報を送信元の通信制御装置３０１を示す識別情報に対応づけて記憶部６６に記憶する（ステップＳ４２５）。これにより、記憶部６６には、通信システムにおける各通信制御装置３０１からログ情報の送出時刻の候補を示す情報が蓄積される。

[0208] 通信制御管理装置５の制御部６１は、記憶部６６に記憶した各通信制御装置３０１のログ情報の送出時刻の候補に基づいてシステム全体の各通信制御装置３１がロゴ情報を送出する時刻のスケジュール（ログ収集のスケジュール）を作成する（ステップＳ４２６）。例えば、制御部３０１は、ネットワークＮＷ全体における通信量が所定閾値未満となるように、各通信制御装置からのログ情報の送出時刻の候補をスケジューリングする。

[0209] ログ情報の送出時刻のスケジュールを作成すると、制御部６１は、個々の通信制御装置３０１に対してログ情報を送信する送出時刻を通知する（ステップＳ４２７）。通信制御装置３０１のコントローラ３２０は、通信制御管理装置５からログ情報の送出時刻の通知を受信すると（ステップＳ４２８）、ログ情報の送出時刻をデータメモリ３２４に記憶する（ステップＳ４２９）。コントローラ３２０は、通信制御管理装置５から指示されたログ情報の送出時刻になると、データメモリ３２４に蓄積したログ情報を通信制御管理装置５へ送信する（ステップＳ４３０）。

[0210] 通信制御装置３０１から送信されるログ情報は、ネットワークＮＷを経由して通信制御管理装置５へ伝送され、通信制御管理装置５に受信される（ステップＳ４３１）。通信制御管理装置５の制御部６１は、通信制御装置３０１から受信したログ情報を記憶部６６に保存する（ステップ４３２）。例えば、制御部６１は、受信したログ情報を実施日時と共に当該通信制御装置３０１の識別情報に対応づけて記憶部６６に記憶する。

[0211] 以上のように、第４の実施形態に係る第２の動作例は、通信制御装置３０１が自身の通信量の分析情報に基づいてログ情報の送出時刻の候補を選出する。通信制御管理装置５は、通信システム３００における各通信制御装置３０１から取得するログ情報の送出時刻の候補をネットワークＮＷに対する負

荷が少なくなるようにスケジュールリングする。

[0212] これにより、各通信制御装置３０１は、ログ情報を通信制御管理装置へ送信する場合におけるネットワーク全体に対する負荷を軽減することができる。また、ログ情報の送出時刻の候補を各通信制御装置がそれぞれ選出するため、通信制御管理装置５にかかる処理の負荷は軽減できる。この結果として、例えば、通信制御装置の数が大量となるような通信システムにおいても効率良く、各通信制御装置がログ情報を送信する時刻をコントローラできる。

[0213] 次に、第４の実施形態に係る通信システム３００における第３の動作例について説明する。

図２２は、第４の実施形態に係る通信システム３００における第３の動作例を説明するためのシーケンスである。

まず、通信制御装置３０１のコントローラ３２０は、上述の第１の動作例と同様に、データメモリ３２４にログ情報として蓄積する通信量を示す情報を分析し、分析結果としての通信量の分析情報をデータメモリ３２４に記憶する（ステップＳ４４１）。

通信制御装置３０１のコントローラ３２０は、データメモリ３２４に記憶した通信量の分析情報に基づいて、当該通信制御装置３０１がログ情報を送信する送出予定時刻を決定する（ステップＳ４４２）。例えば、コントローラ３２０は、当該通信制御装置における通信量の分析情報に基づき、通信量が最も少ない時間帯で当該通信制御装置３０１がログ情報を送信できる時刻を送出予定時刻として選定する。

[0214] ログ情報の送出予定時刻を選定すると、コントローラ３２０は、選定したログ情報の送出予定時刻になると、ネットワークの混雑度を推定する（ステップＳ４４３）。例えば、コントローラ３２０は、ネットワークの混雑度を確認するための問合せを通信制御管理装置５へ送信してから通信制御管理装置５からの応答を受信するまでの時間からネットワークの混雑度を推定する。ここで、通信制御管理装置５へ送信する問合せは、ネットワークの混雑を推定するためのデータであるため、それ自体がネットワークの負荷とならな

いような小さいサイズのデータとする。

[0215] ネットワークの混雑度が所定の閾値以上であれば（ステップＳ４４４、ＮＯ）、コントローラ３２０は、ログ情報の送信を中止する。ログ情報の送信を中止する場合、コントローラ３２０は、通信量の分析情報から再度ロゴ情報を送信する送出予定時刻を選定するようにする。

[0216] ネットワークの混雑度が所定の閾値未満であれば（ステップＳ４４４、ＹＥＳ）、コントローラ３２０は、ログ情報の送信が可能な状態であると判断し、データメモリ３２４に蓄積しているログ情報を通信制御管理装置５へ送信する（ステップＳ４４５）。

[0217] 通信制御装置３０１から送信されるログ情報は、ネットワークＮＷを経由して通信制御管理装置５へ伝送され、通信制御管理装置５に受信される（ステップＳ４４６）。通信制御管理装置５の制御部６１は、通信制御装置３０１から受信したログ情報を記憶部６６に保存する（ステップ４５７）。

[0218] 以上のように、第４の実施形態に係る第３の動作例は、通信制御装置が自身の通信量の分析情報に基づいてログ情報の送出予定時刻を設定する。通信制御装置は、時間が設定した送出予定時刻になると、ネットワークの混雑度を推定し、ネットワークの混雑度が閾値未満であれば、ログ情報を通信制御管理装置へ送信するものとする。

[0219] これにより、通信制御管理装置は、個々の通信制御装置に対してログ情報の送出時刻を決定する必要がなくなる。また、個々の通信制御装置は、自身が設定した送出予定時刻において、実際のネットワークの混雑度を確認してから、ログ情報を通信制御管理装置へ送信できる。この結果として、例えば、通信制御装置の数が大量となるような通信システムにおいても、通信制御管理装置５にかかる処理が大きくなることがなく、多数の通信制御装置からネットワークに負荷をかけずにログ情報を収集できる。

[0220] 本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、

発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

請求の範囲

[請求項1] 第１の装置とネットワーク通信網との間に接続される第１の通信制御装置と、

第２の装置と前記ネットワーク通信網との間に接続される第２の通信制御装置と、

前記第１の通信制御装置の動作状態を示す情報を収集するデバイス管理サーバと、を備え、

前記第１の通信制御装置は、

前記第１の装置および前記ネットワーク通信網を介して接続される装置と通信する通信インターフェースと、

プライベート認証局により発行された秘密鍵、及びクライアント証明書を用いた前記第２の通信制御装置との相互認証処理により決定された共通鍵を用いて、前記第１の装置から前記第２の装置へ送信される情報を暗号化した情報を前記第２の通信制御装置に送信し、前記第２の装置から前記第１の装置へ送信される情報を復号した情報を前記第１の装置に送信する第１のコントローラと、

前記通信インターフェースを介してデータ通信した通信量の分析情報を記憶するメモリと、を有し、

前記第１のコントローラは、前記メモリに記憶する通信量の分析情報に基づいて設定される実行時刻に自己診断を実行し、自己診断の実行結果を前記デバイス管理サーバへ送信する、

前記第２の通信制御装置は、

前記プライベート認証局により発行された秘密鍵、及びサーバ証明書を用いた相互認証処理により決定された共通鍵を用いて、前記第２の装置から前記第１の装置へ送信される情報を暗号化した情報を前記第１の通信制御装置に送信し、前記第１の装置から前記第２の装置へ送信される情報を復号した情報を前記第２の装置に送信する第２のコントローラを有する、

通信システム。

[請求項2] 前記第１のコントローラは、前記メモリに記憶する通信量の分析情報を前記デバイス管理サーバへ送信し、前記デバイス管理サーバからの指示に応じて自己診断を実行する、

請求項１に記載の通信システム。

[請求項3] 前記第１のコントローラは、前記メモリに記憶する通信量の分析情報に基づいて自己診断の実行予定時刻を決定し、前記実行予定時刻に前記自己診断が実行可能な通信状況であれば前記自己診断を実行し、自己診断の実行結果を前記デバイス管理サーバへ送信する、

請求項１に記載の通信システム。

[請求項4] 第１の装置および発行された秘密鍵、及びクライアント証明書を用いた第２の装置とネットワーク通信網との間に接続される第２の通信制御装置との相互認証処理により決定された共通鍵を用いて、前記第１の装置から前記第２の装置へ送信される情報を暗号化した情報を前記第２の通信制御装置に送信し、前記第２の装置から前記第１の装置へ送信される情報を復号した情報を前記第１の装置に送信するコントローラと、

通信インターフェースを介してデータ通信した通信量の分析情報を記憶するメモリと、を有し、

前記コントローラは、前記メモリに記憶する通信量の分析情報に基づいて設定される実行時刻に自己診断を実行し、自己診断の実行結果を動作状態を示す情報を収集するデバイス管理サーバへ送信する、

通信制御装置。

[請求項5] 前記コントローラは、前記メモリに記憶する通信量の分析情報を前記デバイス管理サーバへ送信し、前記デバイス管理サーバからの指示に応じて自己診断を実行する、

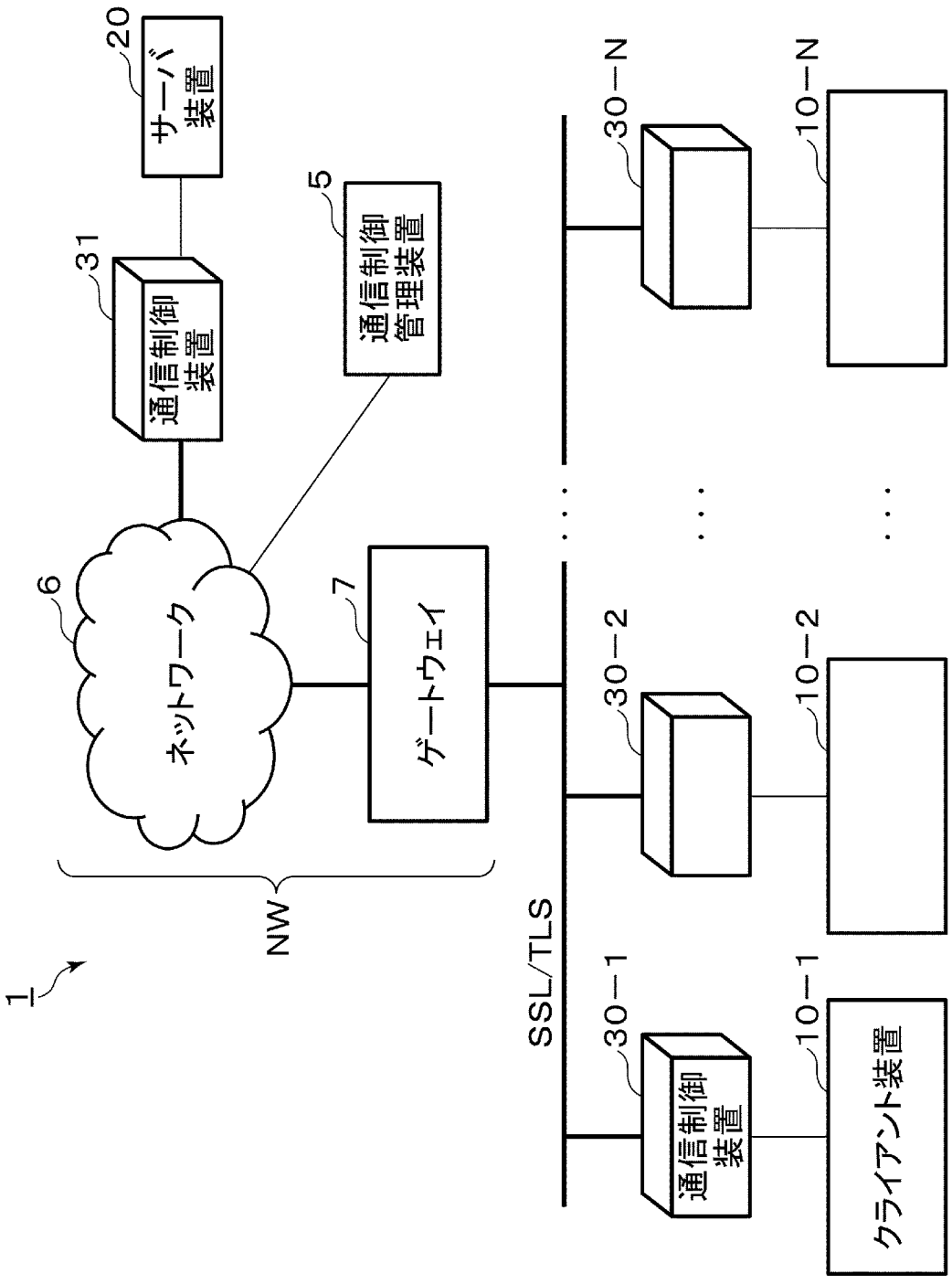
請求項４に記載の通信制御装置。

[請求項6] 前記コントローラは、前記メモリに記憶する通信量の分析情報に基

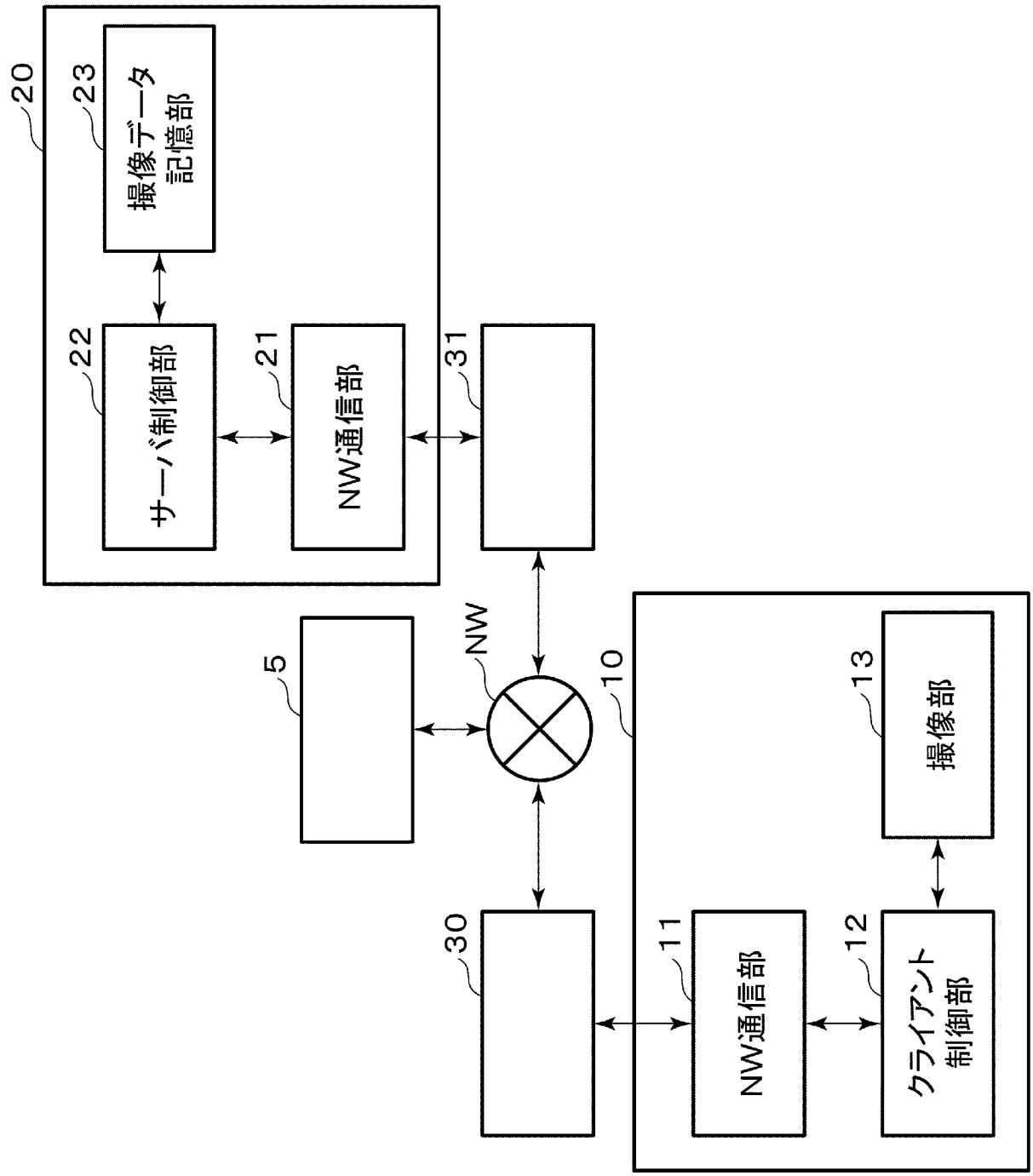
づいて自己診断の実行予定時刻を決定し、前記実行予定時刻に前記自己診断が実行可能な通信状況であれば前記自己診断を実行し、自己診断の実行結果を前記デバイス管理サーバへ送信する、

請求項５に記載の通信制御装置。

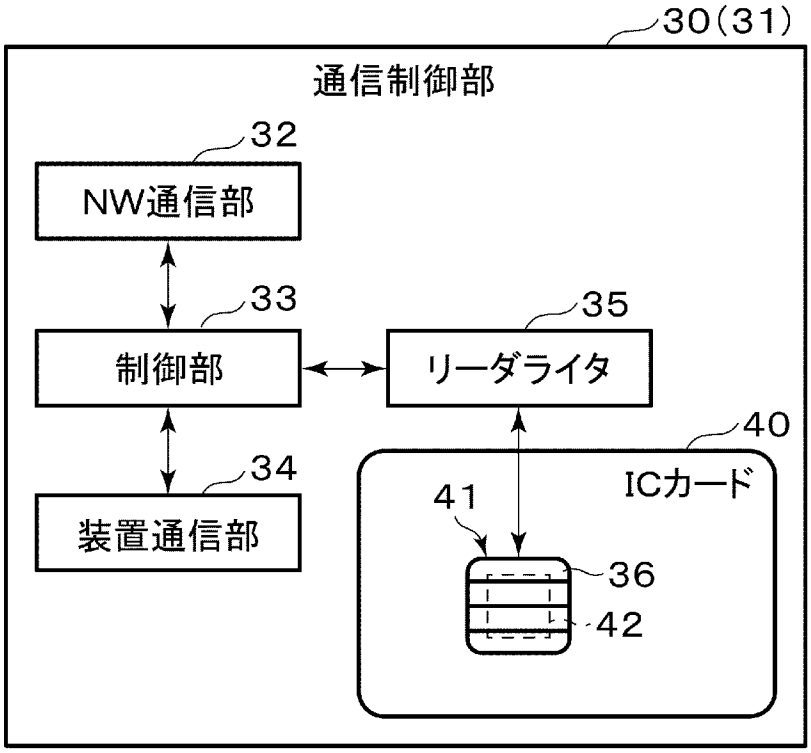
[図1]


1
NW
6
ネットワーク
7
ゲートウェイ
5
通信制御
管理装置
20
サーバ
装置
31
通信制御
装置
SSL/TLS
30－1
通信制御
装置
30－2
30－N
10－1
クライアント装置
10－2
10－N

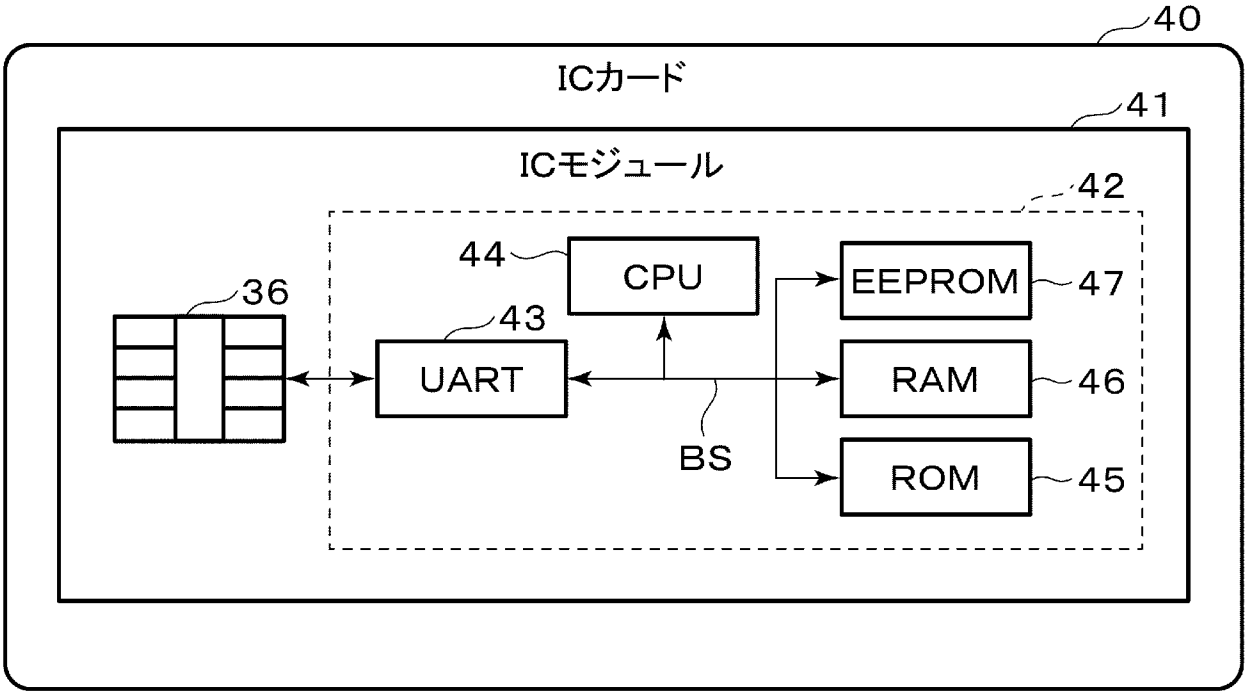
[図2]


20
23
撮像データ記憶部
22
サーバ制御部
21
NW通信部
31
5
NW
10
13
撮像部
30
11
NW通信部
12
クライアント制御部

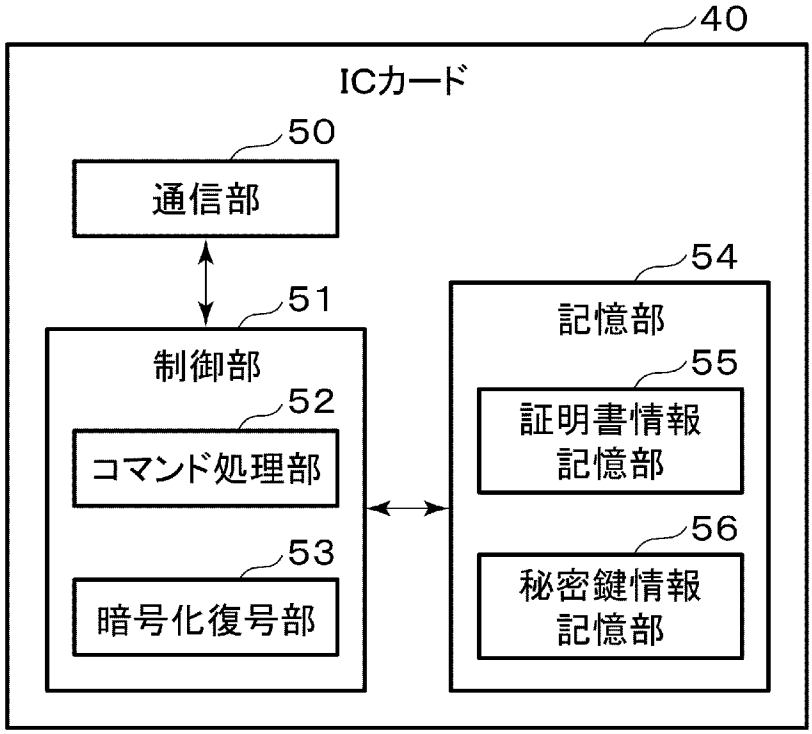
[図3]


30(31)
通信制御部
32
NW通信部
33
制御部
35
リーダライタ
34
装置通信部
40
ICカード
41
36
42

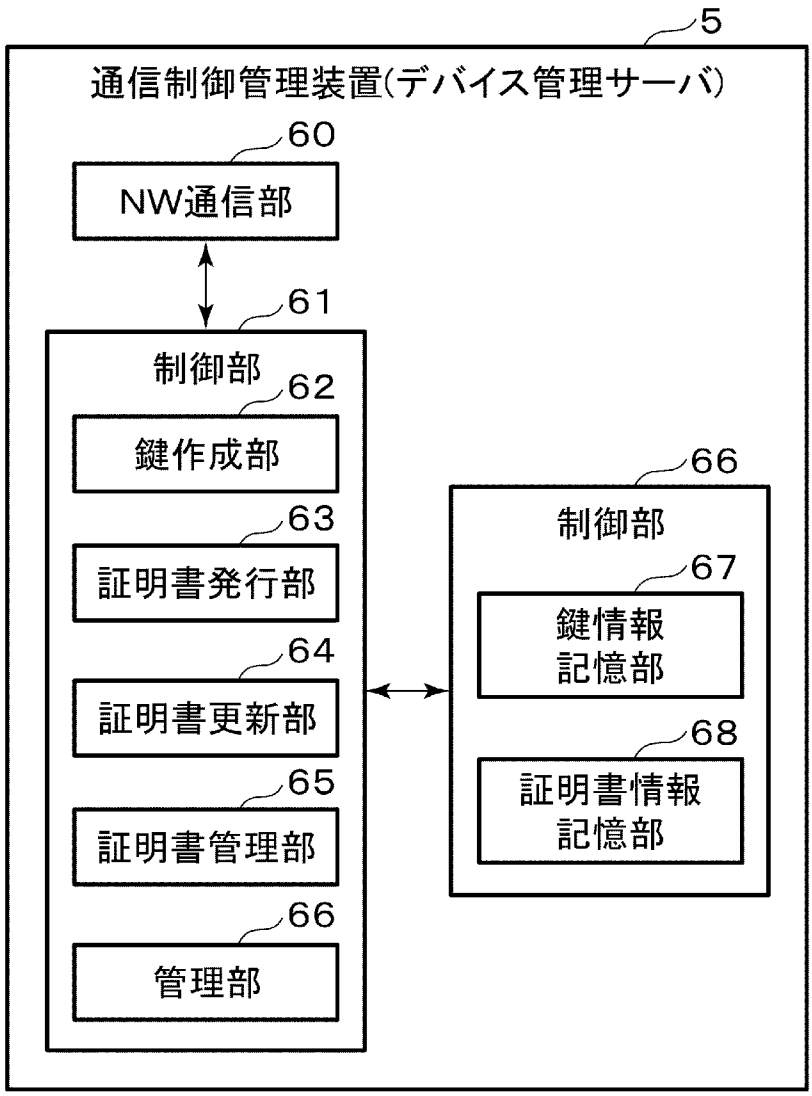
[図4]


40
ICカード
41
ICモジュール
42
44
CPU
36
43
UART
BS
EEPROM
47
RAM
46
ROM
45

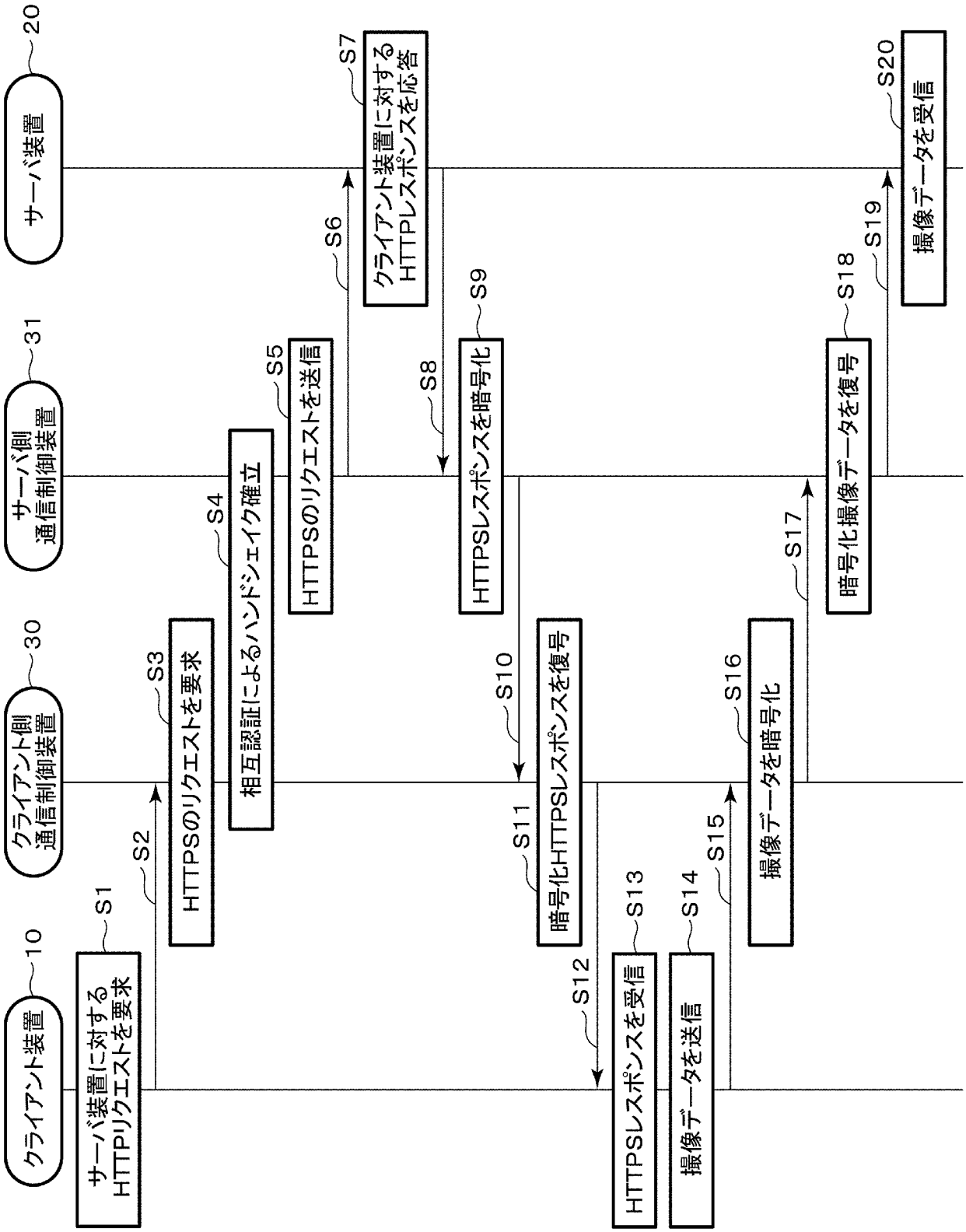
[図5]


40
ICカード
50
通信部
51
制御部
52
コマンド処理部
53
暗号化復号部
54
記憶部
55
証明書情報
記憶部
56
秘密鍵情報
記憶部

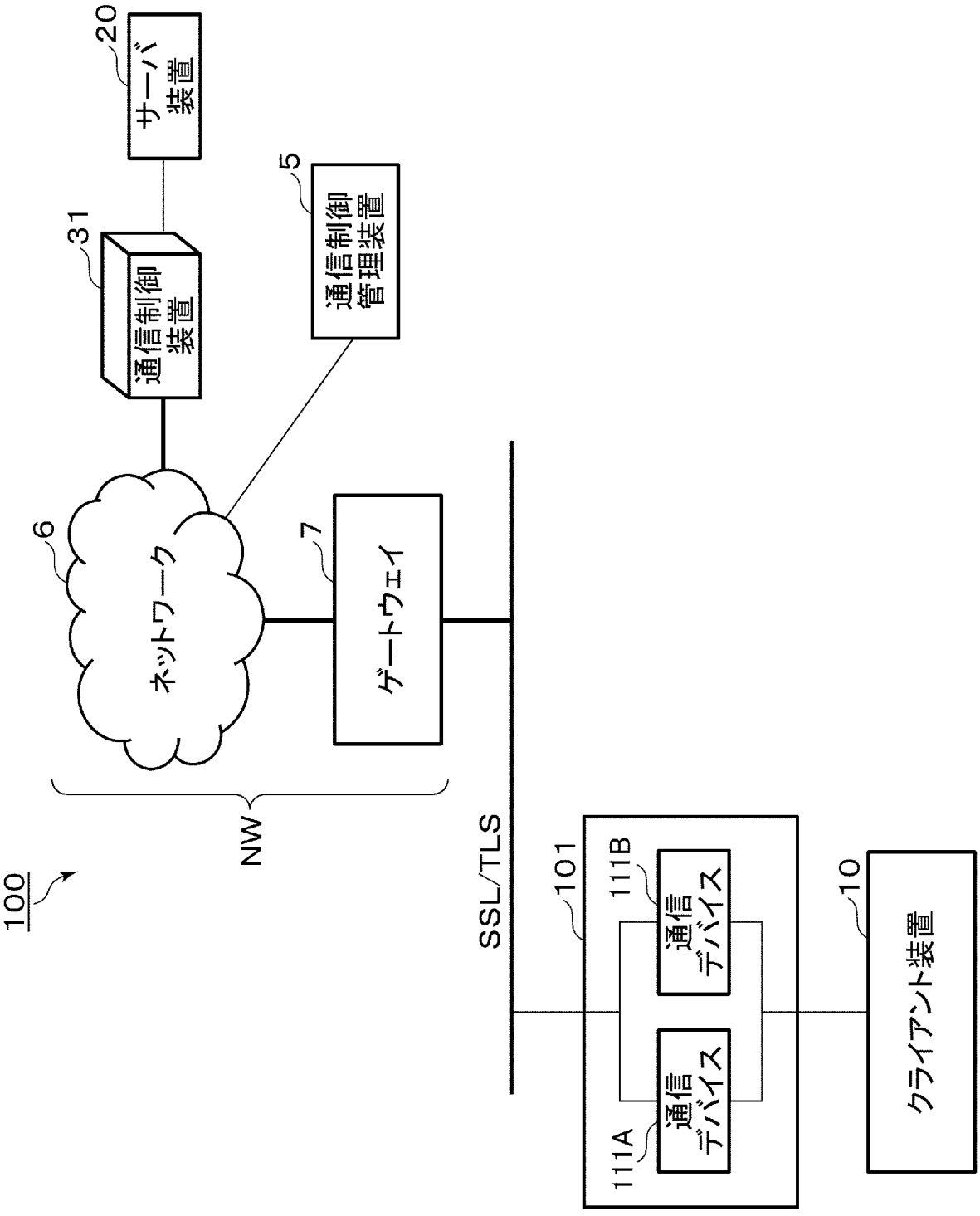
[図6]


5
通信制御管理装置(デバイス管理サーバ)
60
NW通信部
61
制御部
62
鍵作成部
63
証明書発行部
64
証明書更新部
65
証明書管理部
66
管理部
66
制御部
67
鍵情報
記憶部
68
証明書情報
記憶部

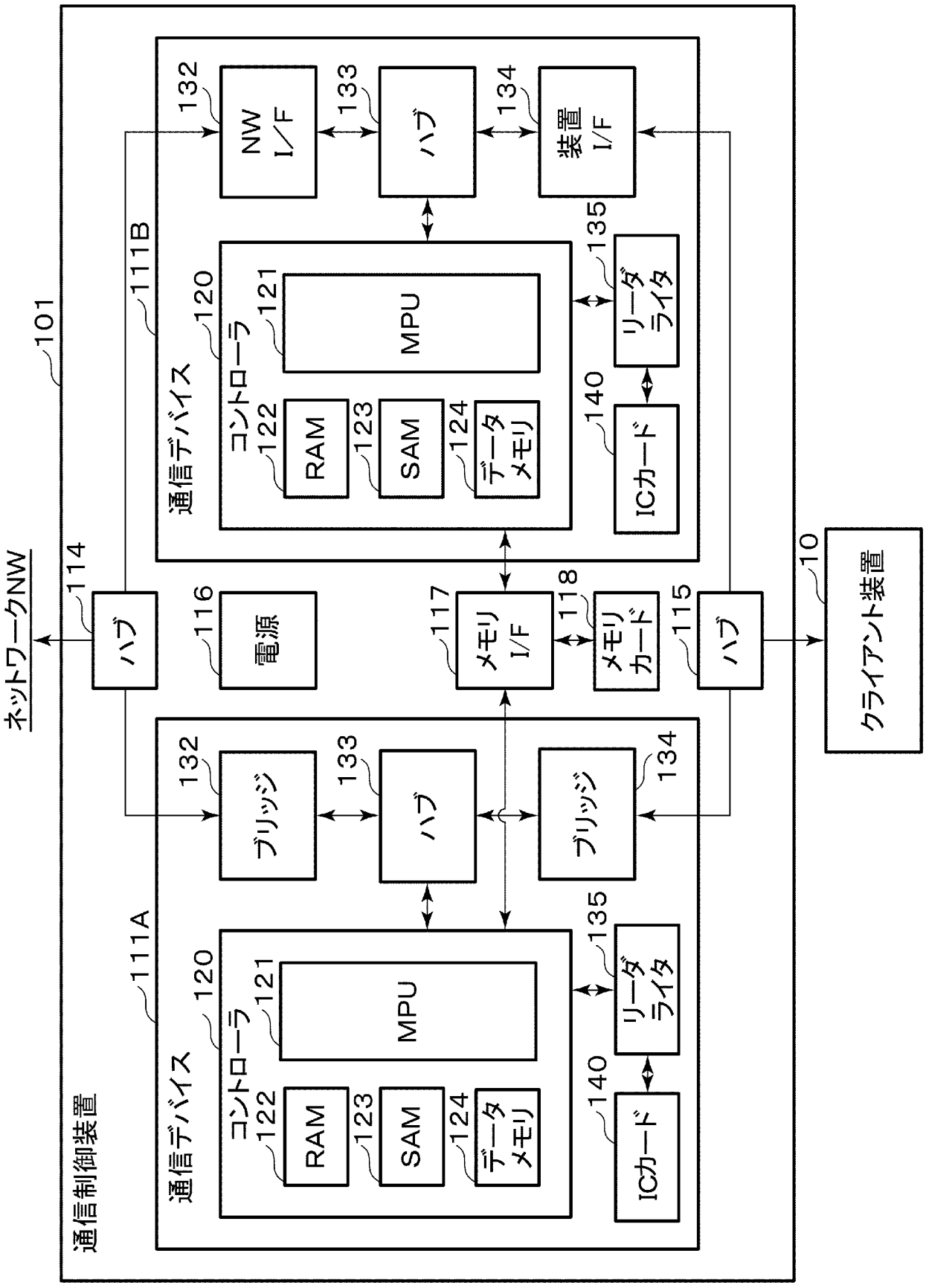
[図7]


クライアント装置
10
サーバ装置
20
クライアント側
通信制御装置
30
サーバ側
通信制御装置
31
S1
サーバ装置に対する
HTTPリクエストを要求
S2
S3
HTTPSのリクエストを要求
S4
相互認証によるハンドシェイク確立
S5
HTTPSのリクエストを送信
S6
S7
クライアント装置に対する
HTTPレスポンスを応答
S8
S9
HTTPSレスポンスを暗号化
S10
S11
暗号化HTTPSレスポンスを復号
S12
S13
HTTPSレスポンスを受信
S14
撮像データを送信
S15
S16
撮像データを暗号化
S17
S18
暗号化撮像データを復号
S19
S20
撮像データを受信

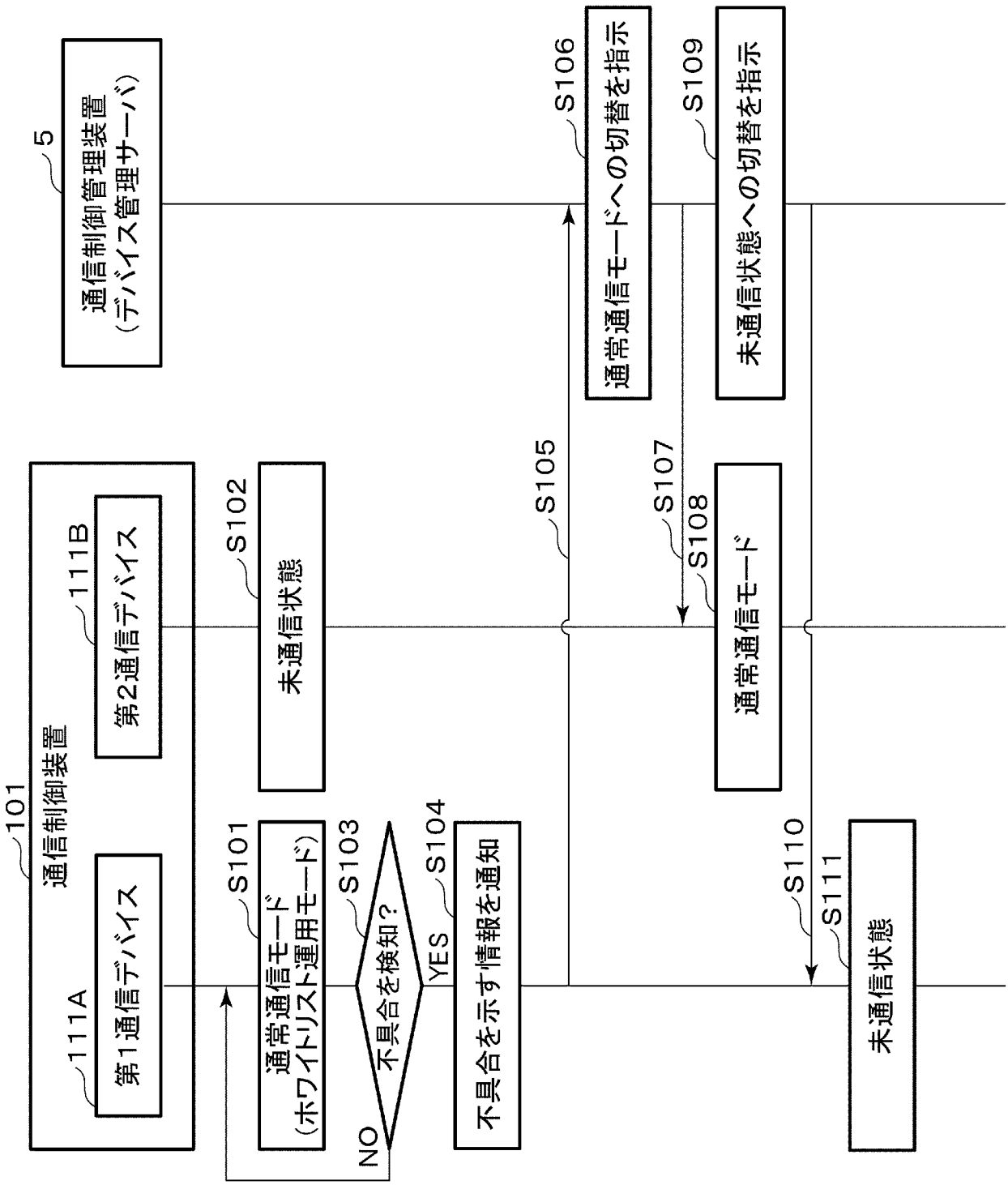
[図8]


100
NW
6
ネットワーク
7
ゲートウェイ
5
通信制御
管理装置
31
通信制御
装置
20
サーバ
装置
SSL/TLS
101
111A
通信
デバイス
111B
通信
デバイス
10
クライアント装置

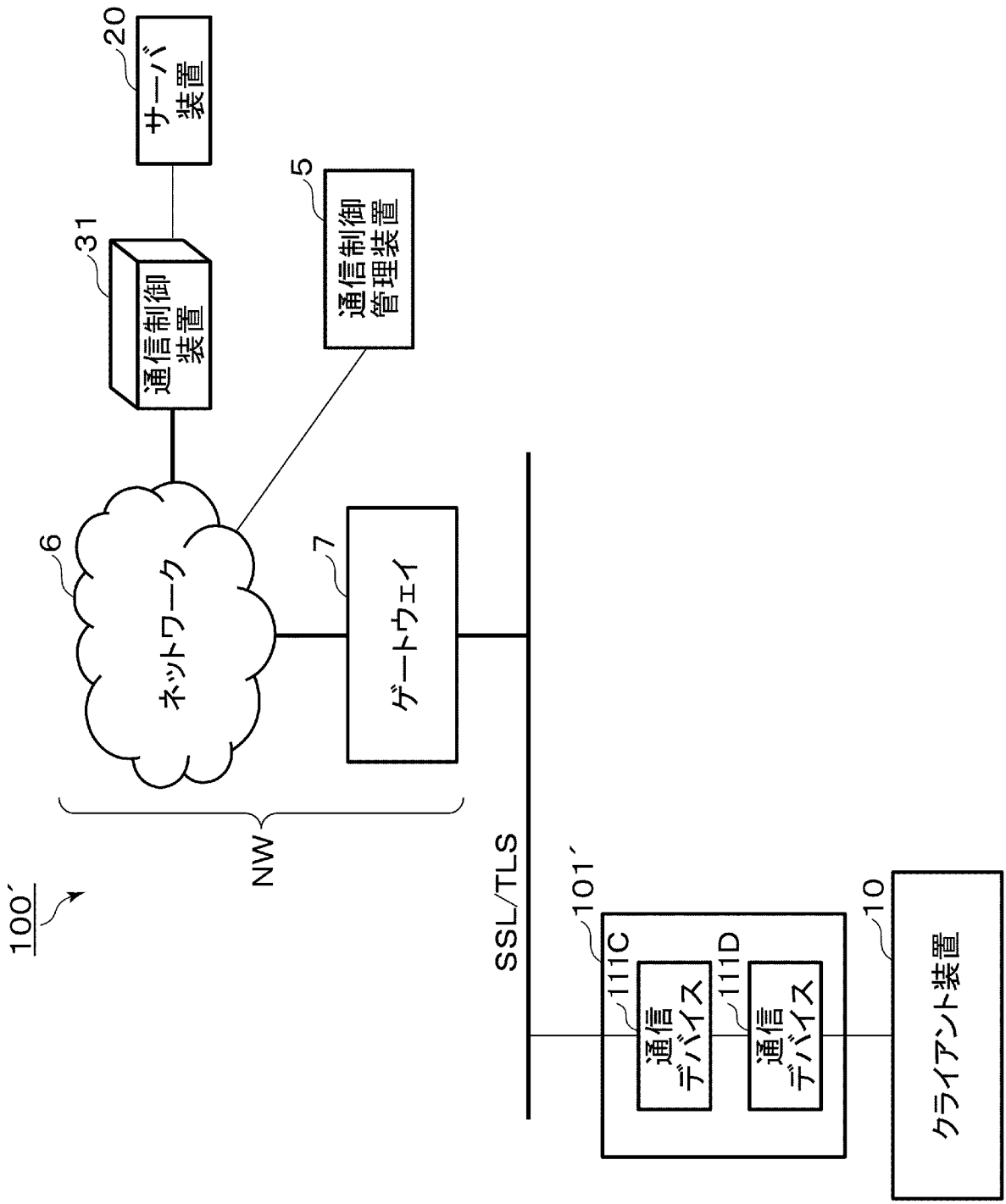
[図9]


101
通信制御装置
ネットワークNW
114
ハブ
116
電源
117
メモリ I/F
118
メモリカード
115
ハブ
10
クライアント装置
111A
111B
通信デバイス
120
コントローラ
121
MPU
122
RAM
123
SAM
124
データメモリ
132
ブリッジ
133
ハブ
134
ブリッジ
135
リーダライタ
140
ICカード
132
NW I/F
133
ハブ
134
装置 I/F
135
リーダライタ
140
ICカード

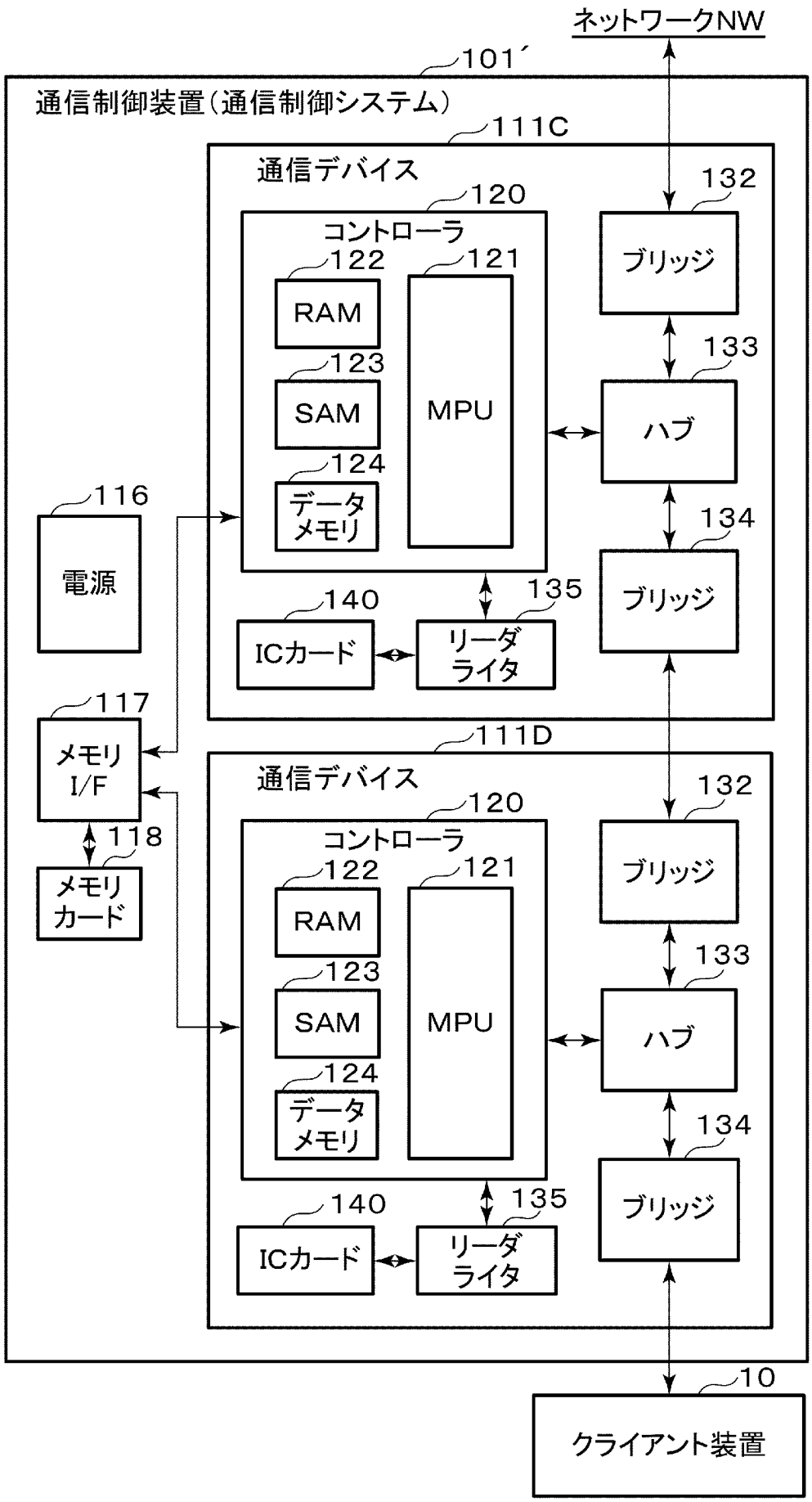
[図10]


5
通信制御管理装置
(デバイス管理サーバ)
101
通信制御装置
111A
第1通信デバイス
111B
第2通信デバイス
S101
通常通信モード
(ホワイトリスト運用モード)
S102
未通信状態
S103
不具合を検知?
NO
YES
S104
不具合を示す情報を通知
S105
S106
通常通信モードへの切替を指示
S107
S108
通常通信モード
S109
未通信状態への切替を指示
S110
S111
未通信状態

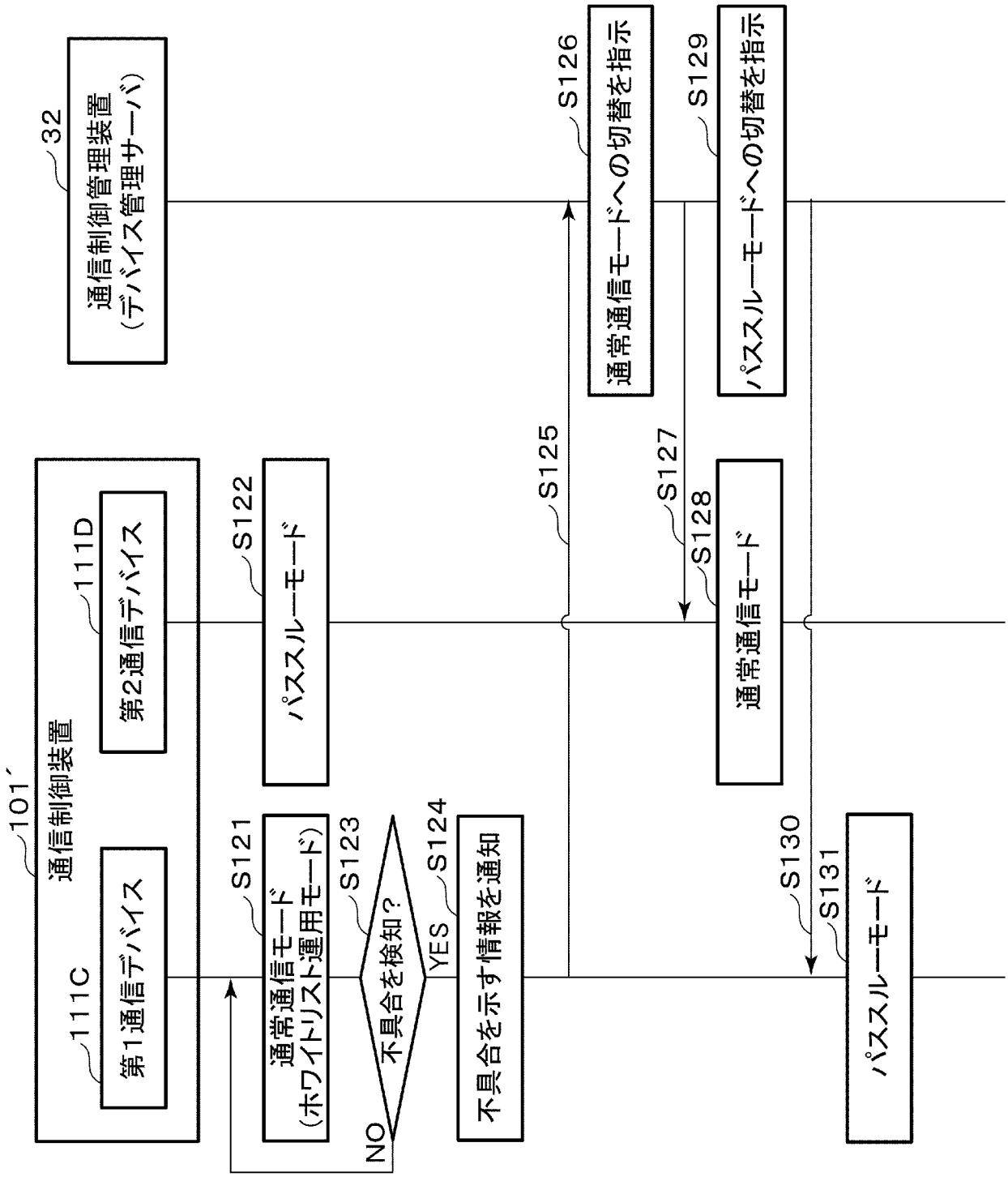
[図11]


100′
NW
6
ネットワーク
7
ゲートウェイ
5
通信制御
管理装置
31
通信制御
装置
20
サーバ
装置
SSL/TLS
101′
111C
通信
デバイス
111D
通信
デバイス
10
クライアント装置

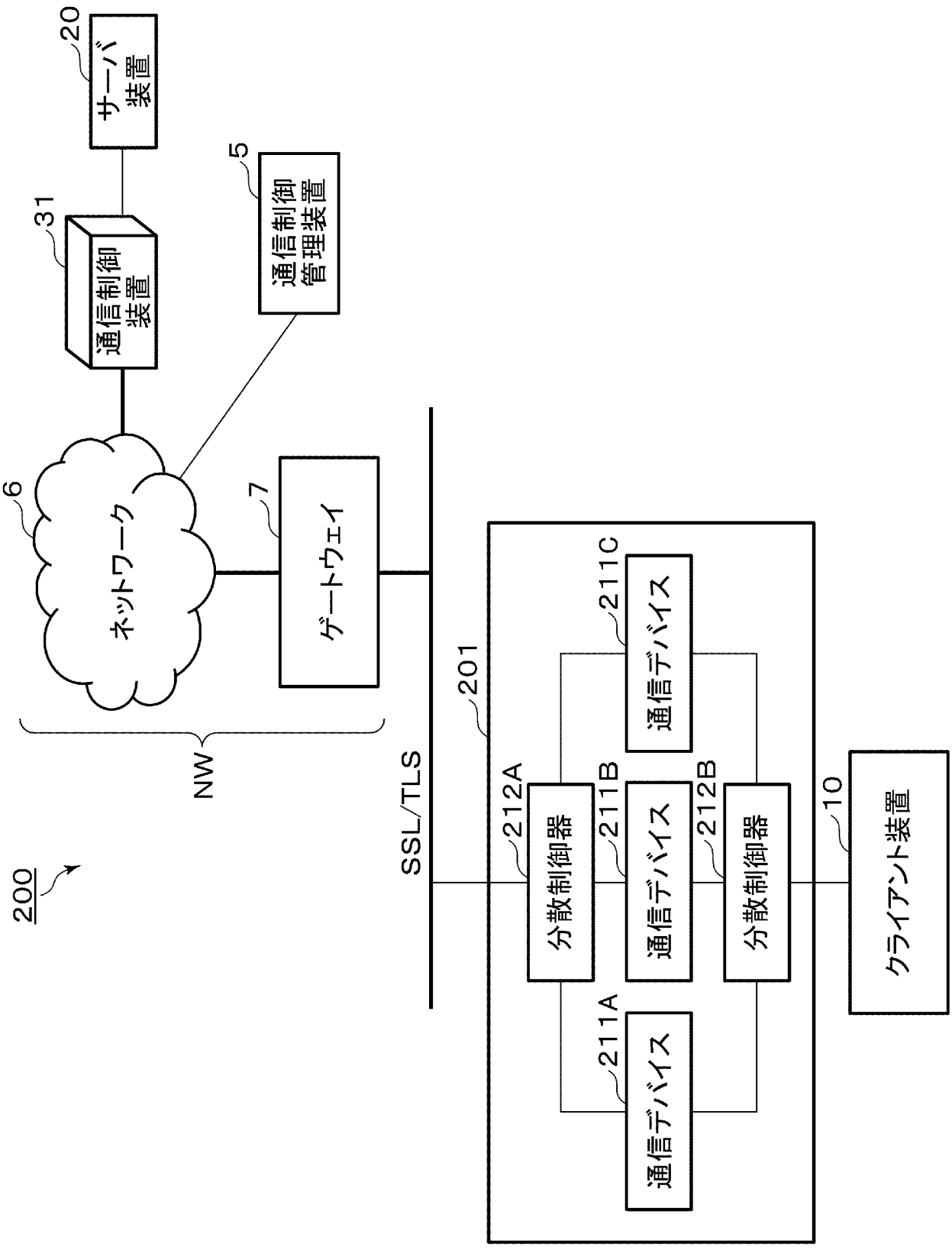
[図12]


ネットワークNW
101´
通信制御装置(通信制御システム)
111C
通信デバイス
120
コントローラ
122
RAM
123
SAM
124
データメモリ
121
MPU
132
ブリッジ
133
ハブ
134
ブリッジ
135
リーダライタ
140
ICカード
116
電源
117
メモリI/F
118
メモリカード
111D
通信デバイス
120
コントローラ
122
RAM
123
SAM
124
データメモリ
121
MPU
132
ブリッジ
133
ハブ
134
ブリッジ
135
リーダライタ
140
ICカード
10
クライアント装置

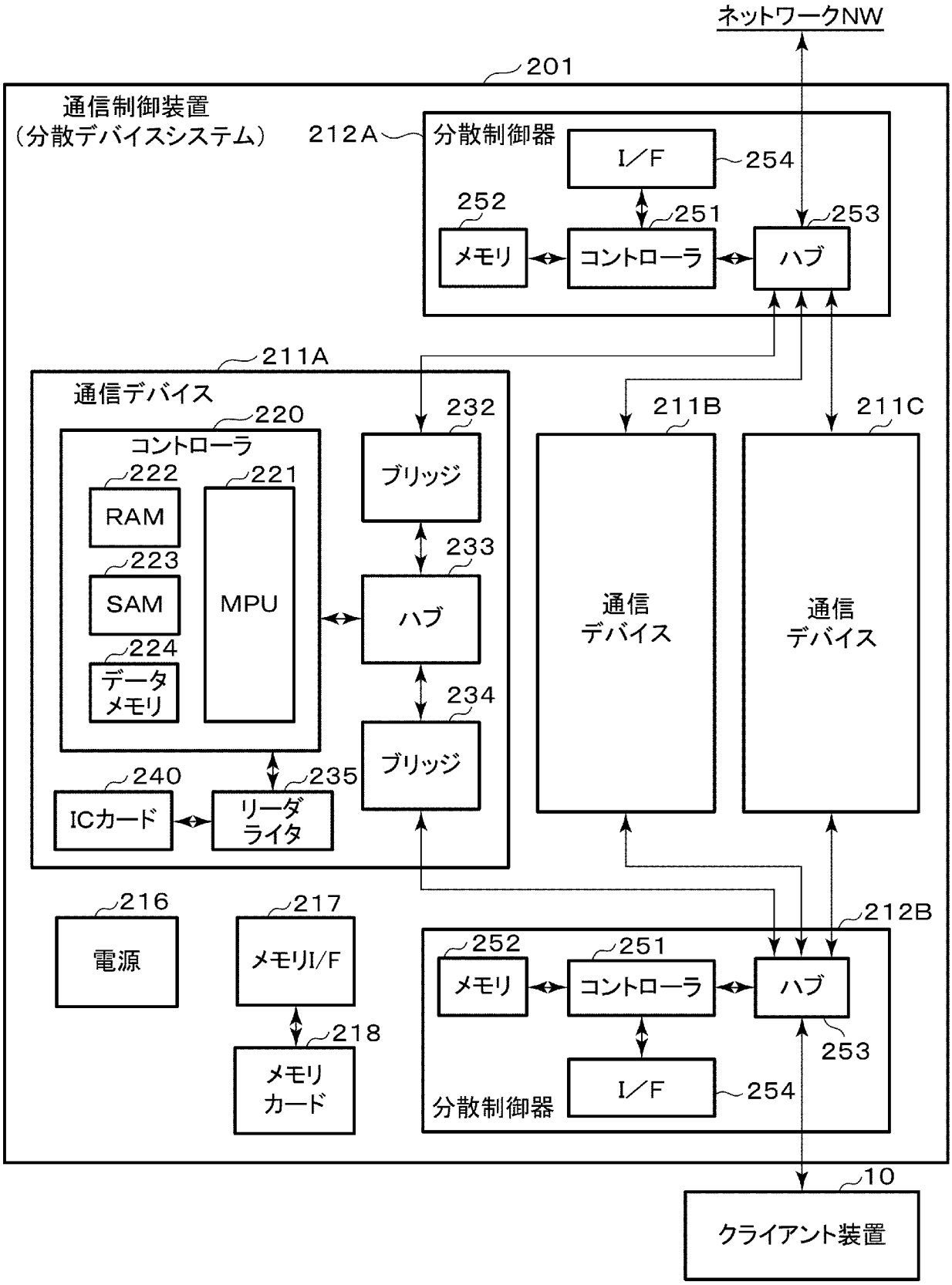
[図13]


101′
通信制御装置
111C
第1通信デバイス
111D
第2通信デバイス
32
通信制御管理装置
(デバイス管理サーバ)
S121
通常通信モード
(ホワイトリスト運用モード)
S122
パススルーモード
S123
不具合を検知?
YES
NO
S124
不具合を示す情報を通知
S125
S126
通常通信モードへの切替を指示
S127
S128
通常通信モード
S129
パススルーモードへの切替を指示
S130
S131
パススルーモード

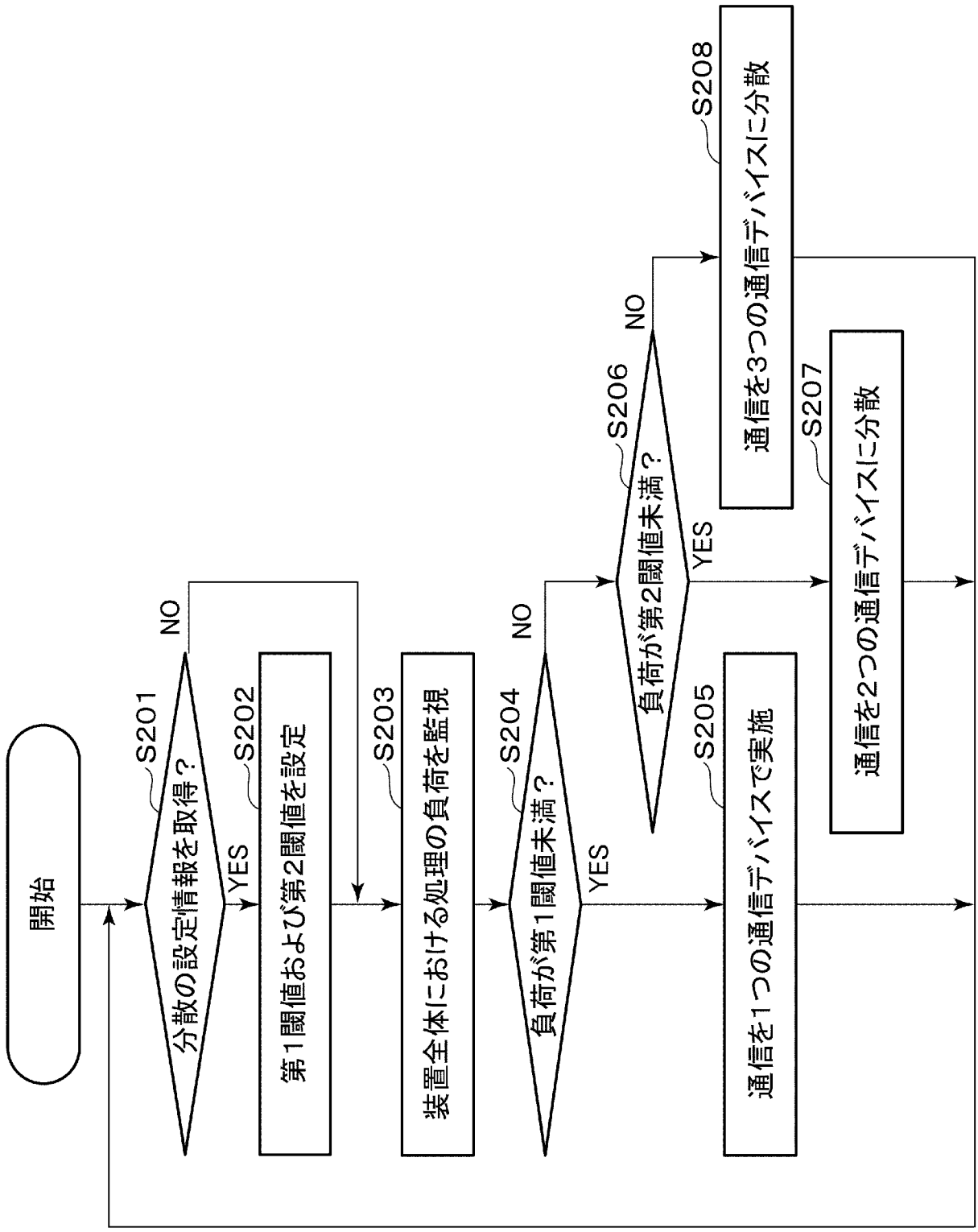
[図14]


200
NW
6
ネットワーク
7
ゲートウェイ
5
通信制御
管理装置
31
通信制御
装置
20
サーバ
装置
SSL/TLS
201
212A
分散制御器
211A
通信デバイス
211B
通信デバイス
211C
通信デバイス
212B
分散制御器
10
クライアント装置

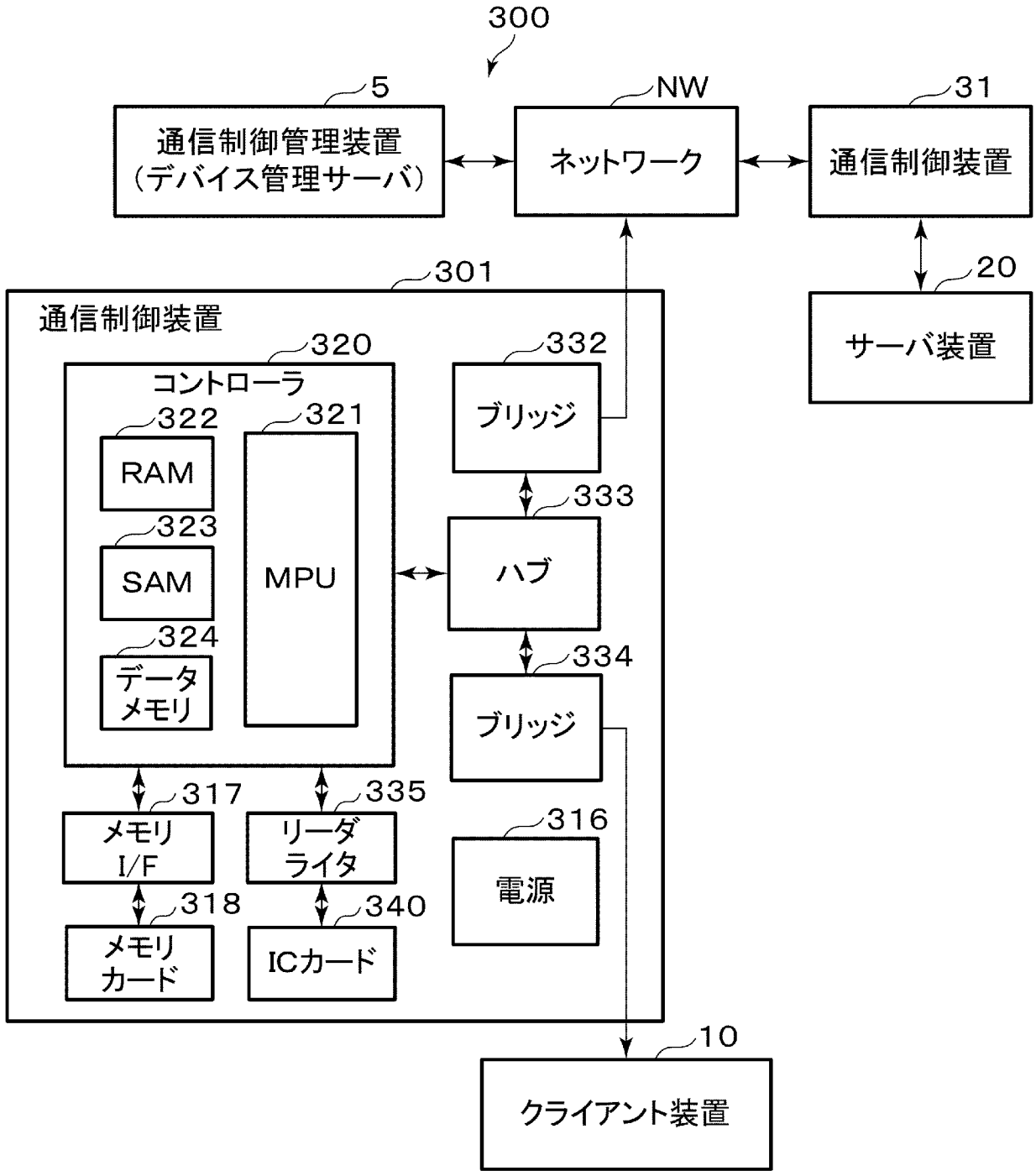
[図15]


ネットワークNW
201
通信制御装置
（分散デバイスシステム）
212A
分散制御器
I／F
254
252
251
253
メモリ
コントローラ
ハブ
211A
通信デバイス
220
コントローラ
222
RAM
223
SAM
224
データ
メモリ
221
MPU
232
ブリッジ
233
ハブ
234
ブリッジ
240
ICカード
235
リーダ
ライタ
211B
通信
デバイス
211C
通信
デバイス
216
電源
217
メモリI/F
218
メモリ
カード
212B
252
メモリ
251
コントローラ
ハブ
253
I／F
254
分散制御器
10
クライアント装置

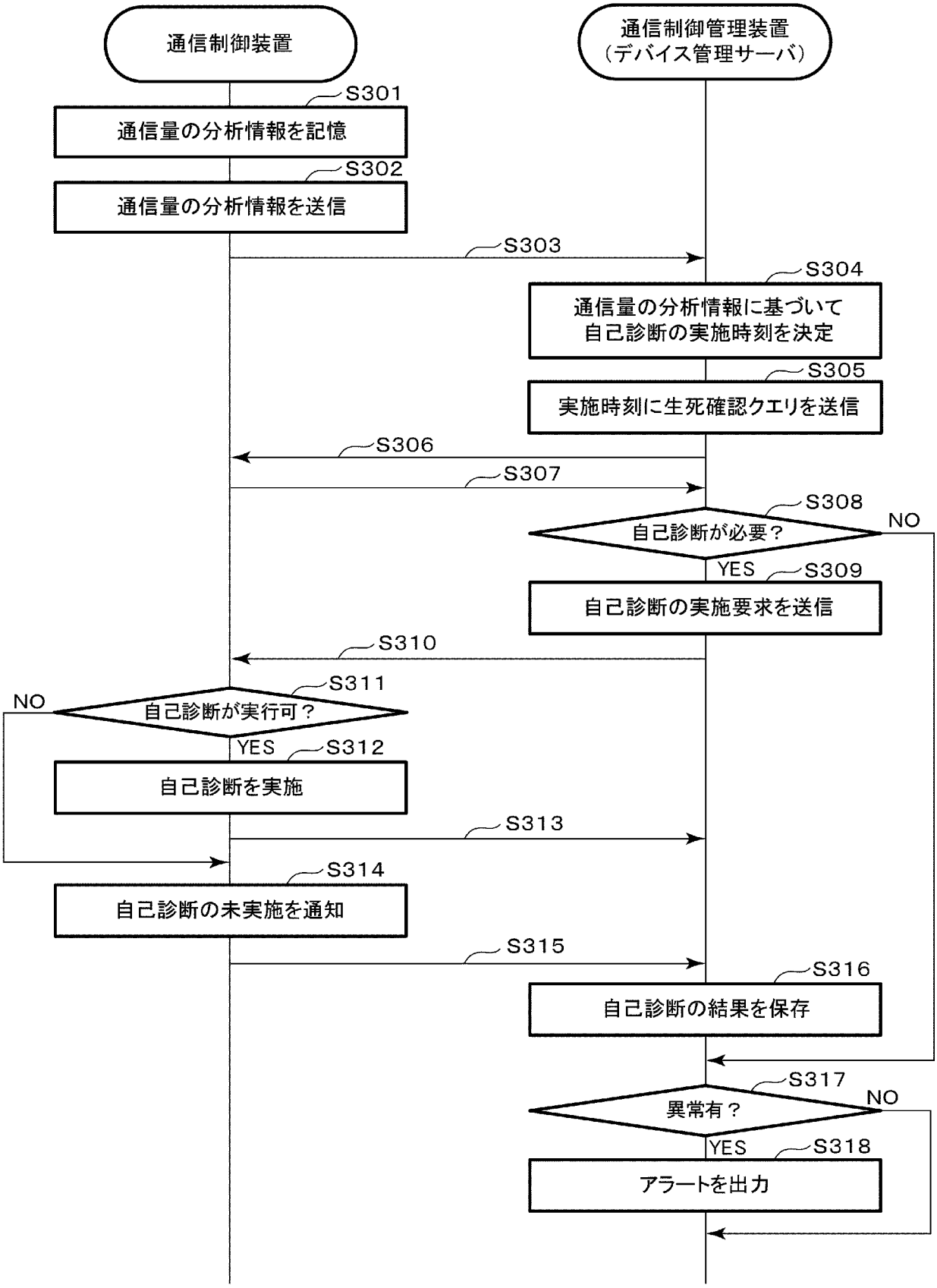
[図16]


開始
S201
分散の設定情報を取得？
NO
YES
S202
第1閾値および第2閾値を設定
S203
装置全体における処理の負荷を監視
S204
負荷が第1閾値未満？
NO
YES
S205
通信を1つの通信デバイスで実施
S206
負荷が第2閾値未満？
NO
YES
S207
通信を2つの通信デバイスに分散
S208
通信を3つの通信デバイスに分散

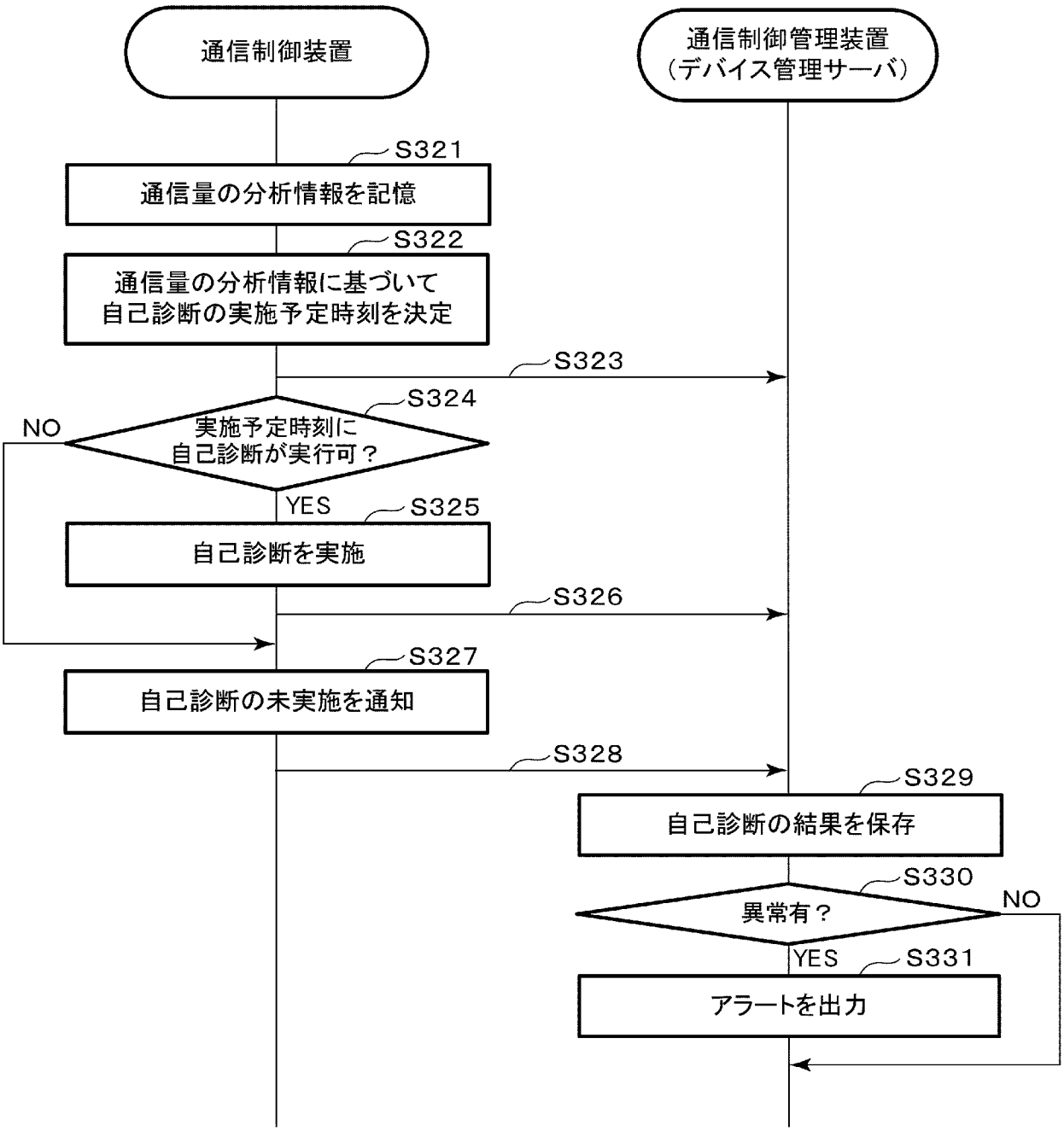
[図17]


300
5
通信制御管理装置
(デバイス管理サーバ)
NW
ネットワーク
31
通信制御装置
20
サーバ装置
301
通信制御装置
320
コントローラ
322
RAM
321
MPU
323
SAM
324
データ
メモリ
332
ブリッジ
333
ハブ
334
ブリッジ
316
電源
317
メモリ
I/F
335
リーダ
ライタ
318
メモリ
カード
340
ICカード
10
クライアント装置

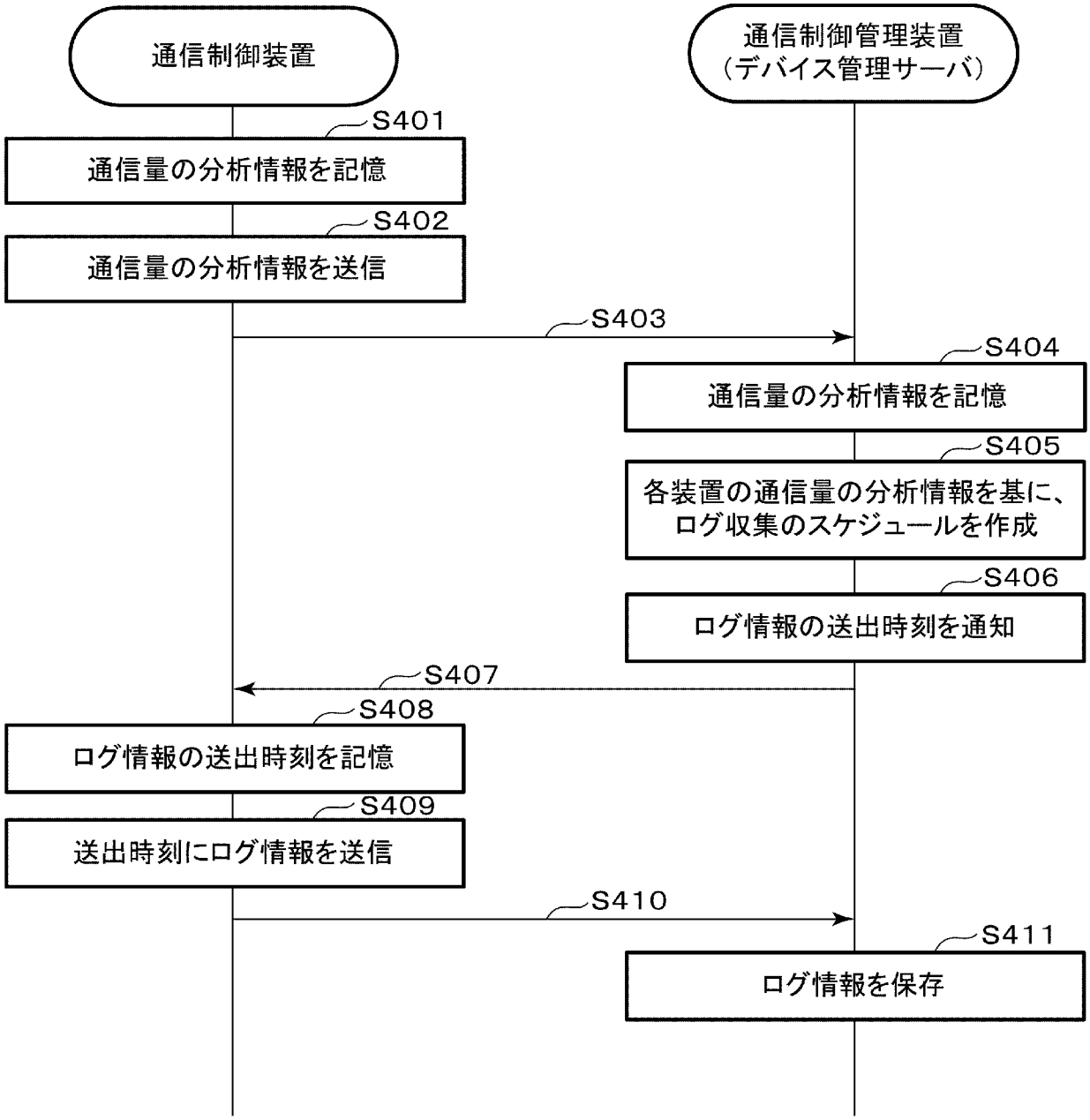
[図18]


通信制御装置
通信制御管理装置
（デバイス管理サーバ）
S301
通信量の分析情報を記憶
S302
通信量の分析情報を送信
S303
S304
通信量の分析情報に基づいて
自己診断の実施時刻を決定
S305
実施時刻に生死確認クエリを送信
S306
S307
S308
自己診断が必要？
NO
YES
S309
自己診断の実施要求を送信
S310
S311
NO
自己診断が実行可？
YES
S312
自己診断を実施
S313
S314
自己診断の未実施を通知
S315
S316
自己診断の結果を保存
S317
異常有？
NO
YES
S318
アラートを出力

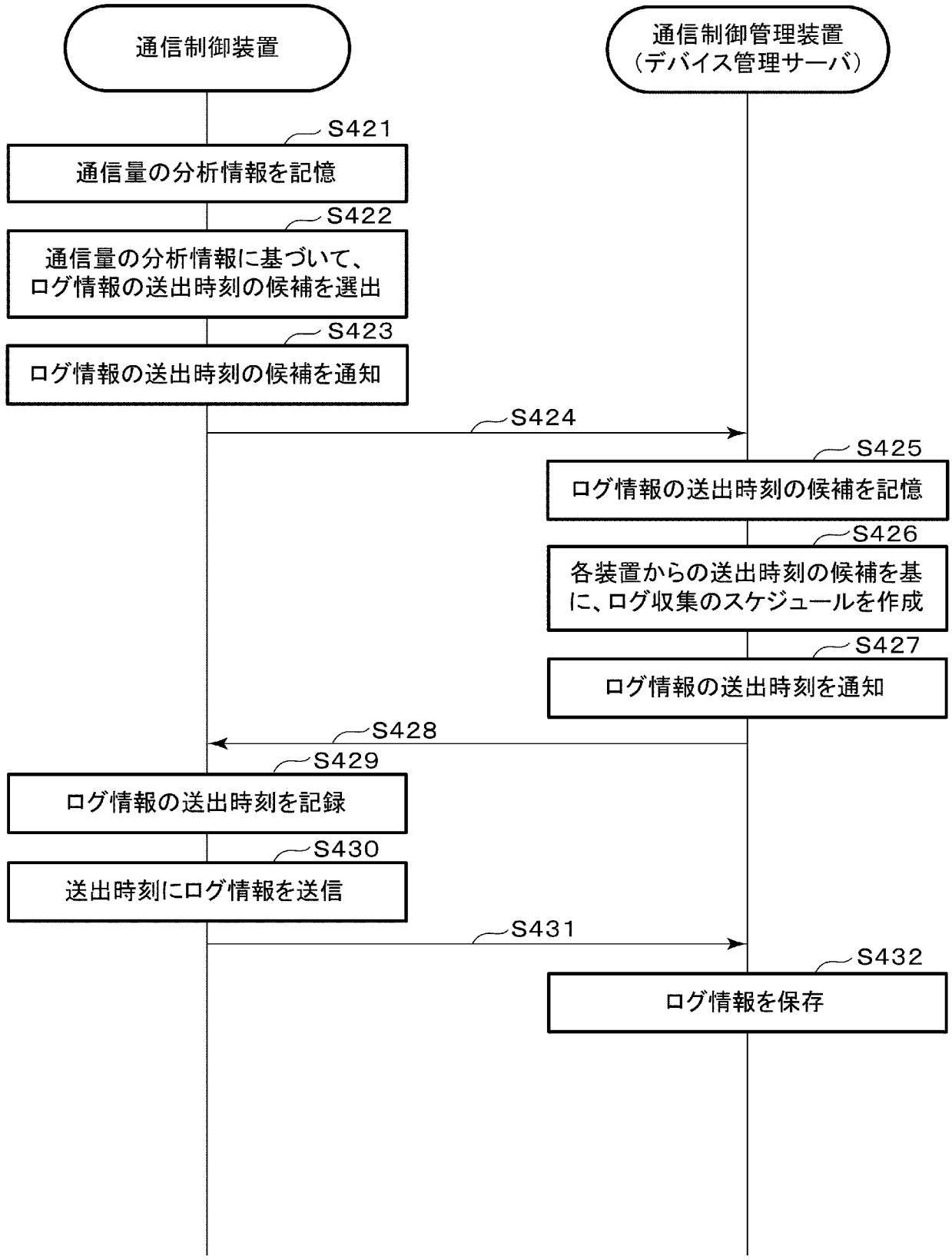
[図19]


通信制御装置
通信制御管理装置
（デバイス管理サーバ）
S321
通信量の分析情報を記憶
S322
通信量の分析情報に基づいて
自己診断の実施予定時刻を決定
S323
S324
実施予定時刻に
自己診断が実行可？
NO
YES
S325
自己診断を実施
S326
S327
自己診断の未実施を通知
S328
S329
自己診断の結果を保存
S330
異常有？
NO
YES
S331
アラートを出力

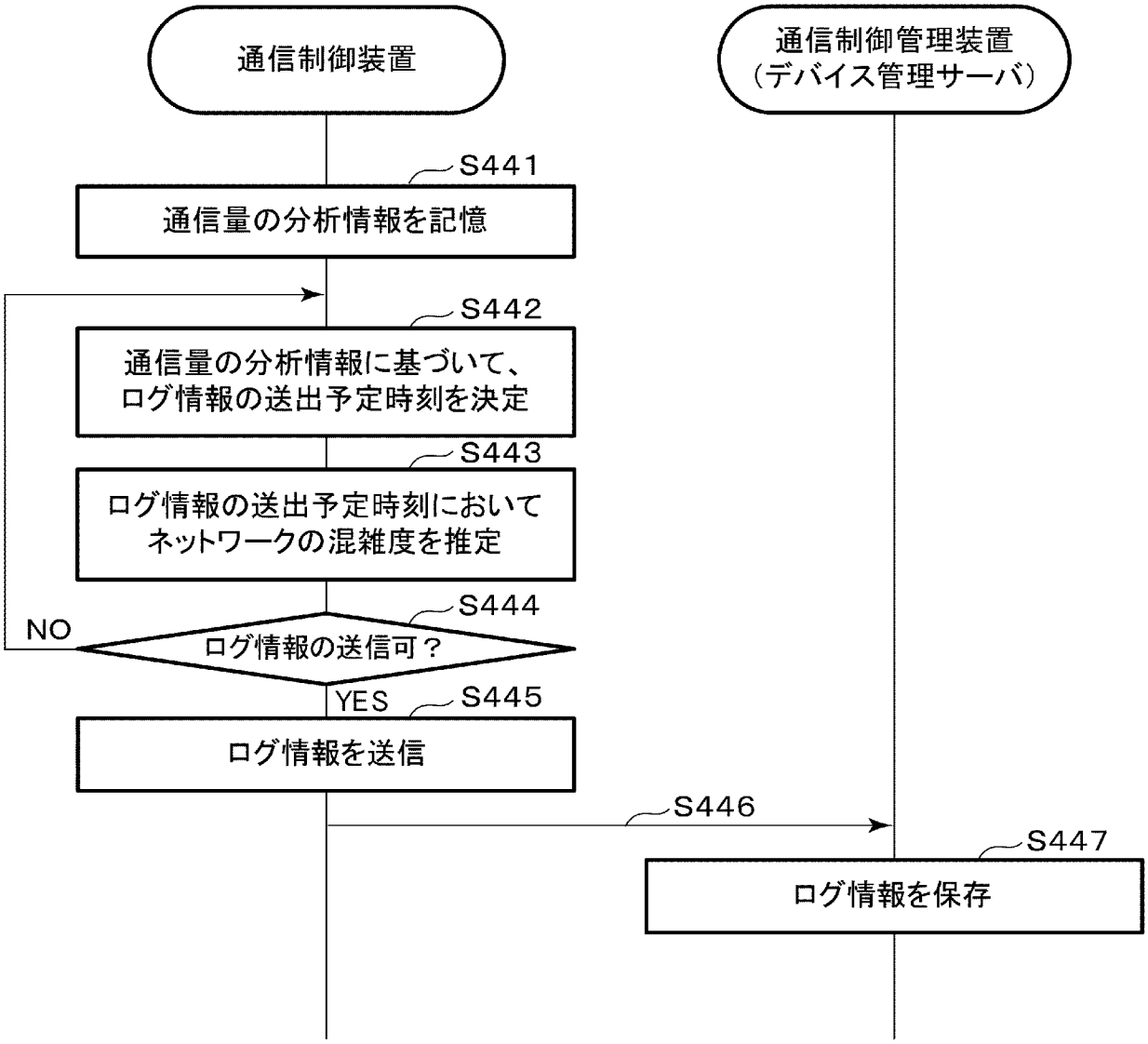
[図20]


通信制御装置
通信制御管理装置
（デバイス管理サーバ）
S401
通信量の分析情報を記憶
S402
通信量の分析情報を送信
S403
S404
通信量の分析情報を記憶
S405
各装置の通信量の分析情報を基に、
ログ収集のスケジュールを作成
S406
ログ情報の送出時刻を通知
S407
S408
ログ情報の送出時刻を記憶
S409
送出時刻にログ情報を送信
S410
S411
ログ情報を保存

[図21]


通信制御装置
通信制御管理装置
（デバイス管理サーバ）
S421
通信量の分析情報を記憶
S422
通信量の分析情報に基づいて、
ログ情報の送出時刻の候補を選出
S423
ログ情報の送出時刻の候補を通知
S424
S425
ログ情報の送出時刻の候補を記憶
S426
各装置からの送出時刻の候補を基
に、ログ収集のスケジュールを作成
S427
ログ情報の送出時刻を通知
S428
S429
ログ情報の送出時刻を記録
S430
送出時刻にログ情報を送信
S431
S432
ログ情報を保存

[図22]


通信制御装置
通信制御管理装置
（デバイス管理サーバ）
S441
通信量の分析情報を記憶
S442
通信量の分析情報に基づいて、
ログ情報の送出予定時刻を決定
S443
ログ情報の送出予定時刻において
ネットワークの混雑度を推定
S444
NO
ログ情報の送信可？
YES
S445
ログ情報を送信
S446
S447
ログ情報を保存

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2020/008471

A. CLASSIFICATION OF SUBJECT MATTER
H04L 9/08(2006.01)i; H04L 9/14(2006.01)i; H04L 9/32(2006.01)i; H04L 12/22(2006.01)i; G06F 21/44(2013.01)i; G06F 21/60(2013.01)i
FI: H04L9/00 601B; H04L9/00 675D; H04L9/00 641; G06F21/44 350; G06F21/60 360; H04L12/22

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)
H04L9/08; H04L9/14; H04L9/32; H04L12/22; G06F21/44; G06F21/60

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	1971-2020
Registered utility model specifications of Japan	1996-2020
Published registered utility model applications of Japan	1994-2020

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.
A	JP 2018-37888 A (TOSHIBA CORP.) 08.03.2018 (2018-03-08) paragraphs [0012]-[0016], [0029]-[0069], fig. 2, 6-7, 11-12	1-6
A	JP 2005-223892 A (RICOH CO., LTD.) 18.08.2005 (2005-08-18) paragraphs [0004]-[0012], [0123]-[0126], fig. 26-27	1-6
A	JP 2013-16041 A (FUJITSU LTD.) 24.01.2013 (2013-01-24) paragraphs [0015]-[0019], fig. 1	1-6

☒ 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	Date of mailing of the international search report
11 May 2020 (11.05.2020)	19 May 2020 (19.05.2020)

Name and mailing address of the ISA/	Authorized officer
Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2020/008471

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	北御門 靖宏 ほか, MOBIKE を応用した IPsecGW 冗長化方式の提案, 電子情報通信学会 2009 年通信ソサイエティ大会講演論文集 2, 01 September 2009, B-6-27, p. 27, in particular, see "3. Proposed method applying MOBIKE", (KITAMIKADO, Yasuhiro et al., "IPsecGW redundancy architecture using MOBIKE", Lecture proceedings 2 of the 2009 communication society conference of IEICE)	1-6

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2020/008471

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
JP 2018-37888 A	08 Mar. 2018	US 2018/0062837 A1 paragraphs [0038]-[0041], [0055]-[0106], fig. 2, 6-7, 11-12 GB 2553388 A	
JP 2005-223892 A	18 Aug. 2005	US 2005/0188196 A1 paragraphs [0009]-[0025], [0231]-[0238], fig. 26-27 JP 2011-160475 A	
JP 2013-16041 A	24 Jan. 2013	(Family: none)	

国際調査報告

国際出願番号
PCT/JP2020/008471

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

H04L 9/08(2006.01)i; H04L 9/14(2006.01)i; H04L 9/32(2006.01)i; H04L 12/22(2006.01)i;
G06F 21/44(2013.01)i; G06F 21/60(2013.01)i
FI: H04L9/00 601B; H04L9/00 675D; H04L9/00 641; G06F21/44 350; G06F21/60 360; H04L12/22

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））

H04L9/08; H04L9/14; H04L9/32; H04L12/22; G06F21/44; G06F21/60

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	１９７１－２０２０年
日本国実用新案登録公報	１９９６－２０２０年
日本国登録実用新案公報	１９９４－２０２０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
A	JP 2018-37888 A (株式会社東芝) 08.03.2018 (2018-03-08) 段落[0012]-[0016],[0029]-[0069], 図2, 6-7, 11-12	1-6
A	JP 2005-223892 A (株式会社リコー) 18.08.2005 (2005-08-18) 段落[0004]-[0012], [0123]-[0126], 図26-27	1-6
A	JP 2013-16041 A (富士通株式会社) 24.01.2013 (2013-01-24) 段落[0015]-[0019], 図1	1-6
A	北御門 靖宏　ほか, ＭＯＢＩＫＥを応用したＩＰｓｅｃＧＷ冗長化方式の提案, 電子情報通信学会２００９年通信ソサイエティ大会講演論文集２, 2009.09.01, B-6-27, p. 27 特に「３．　MOBIKEを応用した提案方式」を参照。	1-6

☐ 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抵触するものではなく、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	国際調査報告の発送日
11.05.2020	19.05.2020

名称及びあて先
日本国特許庁(ISA/JP)
〒100-8915
日本国
東京都千代田区霞が関三丁目４番３号

権限のある職員（特許庁審査官）
青木　重徳 5S 4229

電話番号 03-3581-1101 内線 3546

国際調査報告
パテントファミリーに関する情報

国際出願番号
PCT/JP2020/008471

引用文献	公表日	パテントファミリー文献	公表日
JP 2018-37888 A	08.03.2018	US 2018/0062837 A1 段落[0038]-[0041], [0055]-[0106], FIGs 2, 6-7, 11-12 GB 2553388 A	
JP 2005-223892 A	18.08.2005	US 2005/0188196 A1 段落[0009]-[0025], [0231]-[0238], FIGs 26-27 JP 2011-160475 A	
JP 2013-16041 A	24.01.2013	（ファミリーなし）	