(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2014-42121
(P2014-42121A)
(43)公開日　平成26年3月6日(2014.3.6)

(51)Int.Cl.		F I		テーマコード（参考）
H04L 12/66	(2006.01)	H04L 12/66	B	5K030

審査請求 未請求　請求項の数 10　ＯＬ　（全 18 頁）

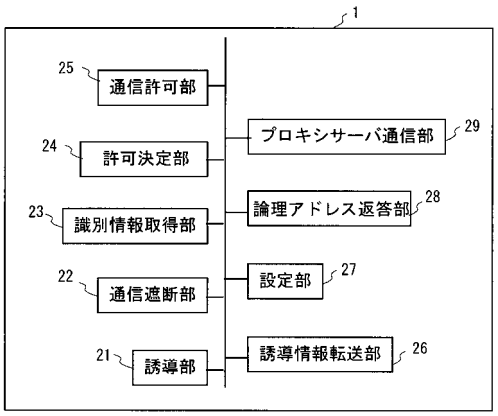
(21)出願番号　特願2012-182654 (P2012-182654)
(22)出願日　平成24年8月21日 (2012.8.21)

(71)出願人　000136136
株式会社ＰＦＵ
石川県かほく市宇野気ヌ９８番地の２
(74)代理人　100113608
弁理士　平川　明
(74)代理人　100105407
弁理士　高田　大輔
(74)代理人　100145838
弁理士　畑添　隆人
(72)発明者　今村　慎哉
石川県かほく市宇野気ヌ９８番地の２　株式会社ＰＦＵ内

Ｆターム(参考)　5K030 GA15　HA08　HD03　LB05　MB09

(54)【発明の名称】通信遮断装置、通信遮断方法、及びプログラム

(57)【要約】
【課題】ネットワークに接続された情報処理装置からの通信について、プロキシサーバを介した通信であっても、適切な許可及び遮断をできる装置を提供することを課題とする。
【解決手段】ネットワークに接続された対象装置２による通信を遮断するセンサー装置１に、対象装置２から送信される情報をセンサー装置１に誘導する誘導部２１と、誘導部２１により誘導された情報で構成される、トランスポート層より上位の所定プロトコルのメッセージから、メッセージの通知先を識別する識別情報を取得する識別情報取得部２３と、少なくとも識別情報取得部２３によって取得された識別情報に基づいて、メッセージによる通信を許可するか否かを決定する許可決定部２４と、許可決定部２４によって許可する決定がされたときに、通信遮断部２２による通信の遮断にかかわらず、メッセージを転送することで、対象装置２による通信を許可する通信許可部２５とを備えた。
【選択図】図２



【特許請求の範囲】
【請求項１】
ネットワークに接続された情報処理装置による通信を遮断する通信遮断装置であって、
前記情報処理装置に対して、他の装置の物理アドレスとして、前記通信遮断装置の物理アドレスを通知することで、前記情報処理装置から送信される情報を前記通信遮断装置に誘導する誘導手段と、
所定の条件を満たす場合に、前記誘導手段によって誘導された情報を転送しないことで、前記情報処理装置による通信を遮断する通信遮断手段と、
前記誘導手段により誘導された情報で構成される、トランスポート層より上位の所定プロトコルのメッセージから、前記メッセージの通知先を識別する識別情報を取得する識別情報取得手段と、
少なくとも前記識別情報取得手段によって取得された前記識別情報に基づいて、前記メッセージによる通信を許可するか否かを決定する許可決定手段と、
前記所定の条件を満たす場合において、前記許可決定手段によって許可する決定がされたときに、前記通信遮断手段による通信の遮断にかかわらず、前記メッセージを転送することで、前記情報処理装置による通信を許可する通信許可手段と、
を備える通信遮断装置。
【請求項２】
前記所定の条件を満たさない場合に、前記誘導手段により誘導された情報を前記他の装置に転送する誘導情報転送手段を更に備える、
請求項１に記載の通信遮断装置。
【請求項３】
前記通信許可手段は、前記他の装置に前記メッセージを転送する、
請求項１又は請求項２に記載の通信遮断装置。
【請求項４】
前記メッセージによる通信の許可される通知先又は前記メッセージによる通信の許可されない通知先の前記識別情報の全部又は一部を設定する設定手段を更に備え、
前記許可決定手段は、前記識別情報取得手段によって取得された前記識別情報が、前記設定手段によって設定された前記識別情報の全部又は一部を含んでいるか否かに基づいて、前記メッセージによる通信を許可するか否かを決定する、
請求項１から３までの何れか一項に記載の通信遮断装置。
【請求項５】
前記誘導手段により誘導された情報が、前記識別情報に対応する論理アドレスの問い合わせを構成する場合に、前記識別情報が識別する通知先の論理アドレスではない所定の論理アドレスを、前記問い合わせに対して返答する論理アドレス返答手段を更に備える、
請求項１から４までの何れか一項に記載の通信遮断装置。
【請求項６】
前記論理アドレス返答手段による前記返答には、前記所定の論理アドレスの有効期間が付加されており、
前記所定の論理アドレスの有効期間は、前記問い合わせに対して前記識別情報が識別する通知先の論理アドレスを返答するサーバによって該返答に付加される、該論理アドレスの有効期間とは異なる有効期間である、
請求項５に記載の通信遮断装置。
【請求項７】
前記所定の論理アドレスの有効期間は、前記問い合わせに対して前記識別情報が識別する通知先の論理アドレスを返答するサーバによって該返答に付加される、該論理アドレスの有効期間よりも短い有効期間である、
請求項６に記載の通信遮断装置。
【請求項８】
前記所定プロトコルの通信の代理をするプロキシサーバと通信するプロキシサーバ通信

手段を更に備え、
前記通信許可手段は、前記誘導手段により誘導された情報が前記所定の論理アドレスを宛先の論理アドレスとする場合において、前記メッセージに前記識別情報を基準とした相対的な情報が含まれるときは、前記メッセージ内の前記相対的な情報を、前記識別情報を基準としない絶対的な情報に変更し、変更したメッセージを、前記プロキシサーバ通信手段を用いて前記プロキシサーバに転送することで、前記情報処理装置による通信を許可する、
請求項５から７までの何れか一項に記載の通信遮断装置。
【請求項９】
ネットワークに接続された情報処理装置による通信を遮断する通信遮断方法であって、
コンピュータによって、
前記情報処理装置に対して、他の装置の物理アドレスとして、前記コンピュータの物理アドレスを通知することで、前記情報処理装置から送信される情報を前記コンピュータに誘導する誘導ステップと、
所定の条件を満たす場合に、前記誘導ステップにおいて誘導された情報を転送しないことで、前記情報処理装置による通信を遮断する通信遮断ステップと、
前記誘導ステップにおいて誘導された情報で構成される、トランスポート層より上位の所定プロトコルのメッセージから、前記メッセージの通知先を識別する識別情報を取得する識別情報取得ステップと、
少なくとも前記識別情報取得ステップにおいて取得された前記識別情報に基づいて、前記メッセージによる通信を許可するか否かを決定する許可決定ステップと、
前記所定の条件を満たす場合において、前記許可決定ステップにおいて許可する決定がされたときに、前記通信遮断ステップにおける通信の遮断にかかわらず、前記メッセージを転送することで、前記情報処理装置による通信を許可する通信許可ステップと、
が実行される、通信遮断方法。
【請求項１０】
コンピュータを、
ネットワークに接続された情報処理装置に対して、他の装置の物理アドレスとして、前記通信遮断装置の物理アドレスを通知することで、前記情報処理装置から送信される情報を前記コンピュータに誘導する誘導手段と、
所定の条件を満たす場合に、前記誘導手段によって誘導された情報を転送しないことで、前記情報処理装置による通信を遮断する通信遮断手段と、
前記誘導手段により誘導された情報で構成される、トランスポート層より上位の所定プロトコルのメッセージから、前記メッセージの通知先を識別する識別情報を取得する識別情報取得手段と、
少なくとも前記識別情報取得手段によって取得された前記識別情報に基づいて、前記メッセージによる通信を許可するか否かを決定する許可決定手段と、
前記所定の条件を満たす場合において、前記許可決定手段によって許可する決定がされたときに、前記通信遮断手段による通信の遮断にかかわらず、前記メッセージを転送することで、前記情報処理装置による通信を許可する通信許可手段と、
として機能させる、プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ネットワークに接続された情報処理装置による通信を遮断する通信遮断装置に関する。
【背景技術】
【０００２】
従来、ネットワーク通信システムにおいて、ネットワークを通じてクライアントから受信された他の機器に対するアクセス要求を受信して宛先ＩＰアドレスを抽出し、そのＩＰ

アドレスを自己のものとして一時登録ＩＰアドレステーブルに登録し、受信したフレームのコピーをネットワークへ再送する通信制御装置が提案されている(特許文献１を参照)。また、アクセス要求装置の要請を受けて代理要求装置が認証処理装置に自己の認証データで要求し、認証処理装置がその要請を受けて認証処理結果に基づくアクセス制御データをアクセス制御装置に配布するネットワークアクセス制御方法が提案されている(特許文献２を参照)。

【先行技術文献】

【特許文献】

【０００３】

【特許文献１】特開２００７－３３６４０１号公報

【特許文献２】国際公開第２００７／１３８６６３号

【発明の概要】

【発明が解決しようとする課題】

【０００４】

例えば、企業内ネットワークにおいては、トラフィックの平準化によるネットワーク負荷の軽減やセキュリティの向上を目的として、プロキシサーバが設置されていることが多い。このネットワークに接続された情報処理装置は、プロキシサーバを介して、インターネット上のＷｅｂサーバ等と通信する必要がある。

【０００５】

また、例えば、企業内ネットワークにおいては、ネットワークの不正利用による情報漏洩やマルウェア等への感染を防ぐため、ネットワークに接続された情報処理装置による通信のうち、セキュリティパッチやセキュリティソフトウェアの定義ファイルのダウンロード、ネットワークの利用申請等を目的とした必要な通信のみを許可し、それ以外の通信を遮断することが行われている。従来、このような通信の許可及び遮断を行う装置やシステムでは、ネットワークを流れるＩＰパケットの宛先ＩＰアドレスや宛先ポート番号に基づいて、許可されるサーバ以外への通信を遮断する方式等が採用されている。

【０００６】

しかし、この方式には、プロキシサーバを介した通信について、適切な許可及び遮断ができないという問題があった。プロキシサーバへ送信されるＩＰパケットの宛先ＩＰアドレス及び宛先ポート番号は、プロキシサーバのＩＰアドレス及びポート番号であり、ＩＰパケットが許可されるサーバとの通信を構成するか否かが判断できないからである。

【０００７】

本発明は、上記の問題に鑑み、ネットワークに接続された情報処理装置からの通信について、プロキシサーバを介した通信であっても、適切な許可及び遮断をできる装置を提供することを課題とする。

【課題を解決するための手段】

【０００８】

本発明では、上記課題を解決するために、以下の手段を採用した。即ち、本発明は、ネットワークに接続された情報処理装置による通信を遮断する通信遮断装置であって、前記情報処理装置に対して、他の装置の物理アドレスとして、前記通信遮断装置の物理アドレスを通知することで、前記情報処理装置から送信される情報を前記通信遮断装置に誘導する誘導手段と、所定の条件を満たす場合に、前記誘導手段によって誘導された情報を転送しないことで、前記情報処理装置による通信を遮断する通信遮断手段と、前記誘導手段により誘導された情報で構成される、トランスポート層より上位の所定プロトコルのメッセージから、前記メッセージの通知先を識別する識別情報を取得する識別情報取得手段と、少なくとも前記識別情報取得手段によって取得された前記識別情報に基づいて、前記メッセージによる通信を許可するか否かを決定する許可決定手段と、前記所定の条件を満たす場合において、前記許可決定手段によって許可する決定がされたときに、前記通信遮断手段による通信の遮断にかかわらず、前記メッセージを転送することで、前記情報処理装置による通信を許可する通信許可手段と、を備える通信遮断装置である。

【０００９】
また、本発明に係る通信遮断装置は、前記所定の条件を満たさない場合に、前記誘導手段により誘導された情報を前記他の装置に転送する誘導情報転送手段を更に備えてもよい。
【００１０】
また、本発明において、前記通信許可手段は、前記他の装置に前記メッセージを転送してもよい。
【００１１】
また、本発明に係る通信遮断装置は、前記メッセージによる通信の許可される通知先又は前記メッセージによる通信の許可されない通知先の前記識別情報の全部又は一部を設定する設定手段を更に備え、前記許可決定手段は、前記識別情報取得手段によって取得された前記識別情報が、前記設定手段によって設定された前記識別情報の全部又は一部を含んでいるか否かに基づいて、前記メッセージによる通信を許可するか否かを決定してもよい。
【００１２】
また、本発明に係る通信遮断装置は、前記誘導手段により誘導された情報が、前記識別情報に対応する論理アドレスの問い合わせを構成する場合に、前記識別情報が識別する通知先の論理アドレスではない所定の論理アドレスを、前記問い合わせに対して返答する論理アドレス返答手段を更に備えてもよい。
【００１３】
また、本発明において、前記論理アドレス返答手段による前記返答には、前記所定の論理アドレスの有効期間が付加されており、前記所定の論理アドレスの有効期間は、前記問い合わせに対して前記識別情報が識別する通知先の論理アドレスを返答するサーバによって該返答に付加される、該論理アドレスの有効期間とは異なる有効期間であってもよい。
【００１４】
また、本発明において、前記所定の論理アドレスの有効期間は、前記問い合わせに対して前記識別情報が識別する通知先の論理アドレスを返答するサーバによって該返答に付加される、該論理アドレスの有効期間よりも短い有効期間であってもよい。
【００１５】
また、本発明に係る通信遮断装置は、前記所定プロトコルの通信の代理をするプロキシサーバと通信するプロキシサーバ通信手段を更に備え、前記通信許可手段は、前記誘導手段により誘導された情報が前記所定の論理アドレスを宛先の論理アドレスとする場合において、前記メッセージに前記識別情報を基準とした相対的な情報が含まれるときは、前記メッセージ内の前記相対的な情報を、前記識別情報を基準としない絶対的な情報に変更し、変更したメッセージを、前記プロキシサーバ通信手段を用いて前記プロキシサーバに転送することで、前記情報処理装置による通信を許可してもよい。
【００１６】
また、本発明は、ネットワークに接続された情報処理装置による通信を遮断する通信遮断方法であって、コンピュータによって、前記情報処理装置に対して、他の装置の物理アドレスとして、前記コンピュータの物理アドレスを通知することで、前記情報処理装置から送信される情報を前記コンピュータに誘導する誘導ステップと、所定の条件を満たす場合に、前記誘導ステップにおいて誘導された情報を転送しないことで、前記情報処理装置による通信を遮断する通信遮断ステップと、前記誘導ステップにおいて誘導された情報で構成される、トランスポート層より上位の所定プロトコルのメッセージから、前記メッセージの通知先を識別する識別情報を取得する識別情報取得ステップと、少なくとも前記識別情報取得ステップにおいて取得された前記識別情報に基づいて、前記メッセージによる通信を許可するか否かを決定する許可決定ステップと、前記所定の条件を満たす場合において、前記許可決定ステップにおいて許可する決定がされたときに、前記通信遮断ステップにおける通信の遮断にかかわらず、前記メッセージを転送することで、前記情報処理装置による通信を許可する通信許可ステップと、が実行される、通信遮断方法であってもよ

い。
【００１７】
また、本発明は、コンピュータを、ネットワークに接続された情報処理装置に対して、他の装置の物理アドレスとして、前記通信遮断装置の物理アドレスを通知することで、前記情報処理装置から送信される情報を前記コンピュータに誘導する誘導手段と、所定の条件を満たす場合に、前記誘導手段によって誘導された情報を転送しないことで、前記情報処理装置による通信を遮断する通信遮断手段と、前記誘導手段により誘導された情報で構成される、トランスポート層より上位の所定プロトコルのメッセージから、前記メッセージの通知先を識別する識別情報を取得する識別情報取得手段と、少なくとも前記識別情報取得手段によって取得された前記識別情報に基づいて、前記メッセージによる通信を許可するか否かを決定する許可決定手段と、前記所定の条件を満たす場合において、前記許可決定手段によって許可する決定がされたときに、前記通信遮断手段による通信の遮断にかかわらず、前記メッセージを転送することで、前記情報処理装置による通信を許可する通信許可手段と、として機能させる、プログラムであってもよい。
【００１８】
また、本発明は、そのようなプログラムをコンピュータその他の装置、機械等が読み取り可能な記録媒体に記録したものでもよい。ここで、コンピュータ等が読み取り可能な記録媒体とは、データやプログラム等の情報を電気的、磁気的、光学的、機械的、又は化学的作用によって蓄積し、コンピュータ等から読み取ることができる記録媒体をいう。
【発明の効果】
【００１９】
本発明によって、ネットワークに接続された情報処理装置からの通信について、プロキシサーバを介した通信であっても、適切な許可及び遮断をすることが可能となる。
【図面の簡単な説明】
【００２０】
【図１】本実施形態に係るセンサー装置を含む通信システムの構成を示す概略図である。
【図２】本実施形態に係るセンサー装置の機能構成の概略を示す図である。
【図３】実施形態１に係るセンサー装置を含む通信システムの通信の例を示すシーケンス図である。
【図４】実施形態１に係るセンサー装置における対象装置からの受信データ処理の流れを示すフローチャートである。
【図５】実施形態１に係るセンサー装置におけるリクエストメッセージ転送先からの受信データ処理の流れを示すフローチャートである。
【図６】実施形態２に係るセンサー装置を含む通信システムの通信の例を示すシーケンス図である。
【図７】実施形態２に係るセンサー装置における対象装置からの受信データ処理の流れを示すフローチャートである。
【図８】実施形態２に係るセンサー装置におけるプロキシサーバからの受信データ処理の流れを示すフローチャートである。
【図９】Ｗｅｂサーバ向けのＨＴＴＰリクエストメッセージのリクエストヘッダの例（一部）である。
【図１０】プロキシサーバ向けのＨＴＴＰリクエストメッセージのリクエストヘッダの例（一部）である。
【発明を実施するための形態】
【００２１】
以下、本発明の実施の形態について、図面に基づいて説明する。本実施形態において、本発明に係る通信遮断装置は、センサー装置として実施され、ネットワークに接続される情報処理装置としての対象装置による通信を遮断する。また、センサー装置は、ＯＳＩ基本参照モデルにおけるトランスポート層より上位の所定プロトコルとしてＨＴＴＰ（Ｈｙｐｅｒ　Ｔｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）のメッセージによる通信を許

可する。なお、以下に説明する実施の形態は、本発明を実施する一例を示すものであって、本発明を以下に説明する具体的構成に限定するものではない。本発明を実施するにあたっては、実施の形態に応じた具体的構成が適宜採用されることが好ましい。

【００２２】

＜構成＞

図１は、本実施形態に係るセンサー装置を含む通信システムの構成を示す概略図である。本実施形態に係る通信システムは、センサー装置１、Ｗｅｂブラウザ等を備える情報処理装置である対象装置２、ＩＰネットワークを構成するネットワークセグメント３、ルータ４、ＨＴＴＰ通信を代理できるプロキシサーバ５、インターネット６、Ｗｅｂサーバ７、及びＷｅｂサーバ７のホスト名に対応するＩＰアドレスを管理して名前解決を行うＤＮＳサーバ８を備える。センサー装置１、対象装置２、ルータ４、及びプロキシサーバ５は、ネットワークセグメント３に接続されている。ネットワークセグメント３は、ルータ４を介してインターネット６と接続されている。Ｗｅｂサーバ７、及びＤＮＳサーバ８は、インターネット６に接続されている。なお、本通信システムは、インターネット６の代わりに、イントラネット、ＷＡＮ（Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）等で構成されてもよい。

【００２３】

ルータ４はプロキシサーバ５からのインターネット６への通信を許可しているため、プロキシサーバ５は、Ｗｅｂサーバ７及びＤＮＳサーバ８と通信をすることができる。一方、ルータ４は対象装置２からのインターネット６への通信を許可していないため、対象装置２は、プロキシサーバ５を介さなければ、Ｗｅｂサーバ７とＨＴＴＰメッセージによる通信をすることができない。また、対象装置２は、ＤＮＳサーバ８と通信することはできない。

【００２４】

センサー装置１は、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）１１、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）１２、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）１３、NIC（Ｎｅｔｗｏｒｋ　Ｉｎｔｅｒｆａｃｅ　Ｃａｒｄ）１４、ＨＤＤ（Ｈａｒｄ　Ｄｉｓｋ　Ｄｒｉｖｅ）等の補助記憶装置１５を備えたコンピュータである。ＣＰＵ１１は、中央処理装置であり、ＲＡＭ１２等に展開された命令及びデータを処理することで、ＲＡＭ１２、ＮＩＣ１４、補助記憶装置１５等を制御する。ＲＡＭ１２は、主記憶装置であり、ＣＰＵ１１によって制御され、各種命令やデータが書き込まれ、読み出される。補助記憶装置１５は、不揮発性の補助記憶装置であり、ＲＡＭ１２にロードされるＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ）や通信の制御プログラム等の各種プログラム等、主にコンピュータの電源を落としても保持したい情報が書き込まれ、読み出される。

【００２５】

また、補助記憶装置１５は、特別にパケットの転送が許可される転送先を示すＩＰアドレスとポート番号の組のリストである転送ＩＰアドレス／ポートリスト、対象装置２からのＨＴＴＰ通信が許可されるＷｅｂサーバ7を示す許可サーバリスト、及びＩＰアドレス、ポート番号、認証情報等のプロキシサーバ５へのアクセス情報を記憶する。

【００２６】

対象装置２は、センサー装置１と同様に、ＣＰＵ、ＲＡＭ、ＲＯＭ、ＮＩＣ、ＨＤＤ等の補助記憶装置１５等を備えたコンピュータである。対象装置２には、Ｗｅｂブラウザ等のプログラムが搭載されており、ＮＩＣを介してＨＴＴＰのメッセージによる通信をすることができる。

【００２７】

図２は、本実施形態に係るセンサー装置１の機能構成の概略を示す図である。センサー装置１は、補助記憶装置１５に記録されているプログラムが、ＲＡＭ１２に読み出され、ＣＰＵ１１によって実行されることで、誘導部２１、通信遮断部２２、識別情報取得部２３、許可決定部２４、通信許可部２５、誘導情報転送部２６、設定部２７、論理アドレス

返答部２８、及びプロキシサーバ通信部２９を備えるコンピュータとして機能する。なお、本実施形態では、コンピュータの備える各機能は、汎用プロセッサであるＣＰＵ１１によって実行されるが、これらの機能の一部又は全部は、１又は複数の専用プロセッサによって実行されてもよい。

【００２８】

本実施形態において、誘導部２１は、ネットワークセグメント３を流れるＭＡＣフレーム（データ）を、その宛先ＭＡＣアドレスがセンサー装置１のＭＡＣアドレスでないものも含めＮＩＣ１４から取得し、送信元ＭＡＣアドレスに基づいて、通信遮断の対象となる対象装置２か否かを判定する。誘導部２１は、取得されたデータが対象装置２から送信されたデータである場合において、そのデータがＡＲＰ要求パケットを構成するときに、送信元の対象装置２に対して、センサー装置１の物理アドレスであるＭＡＣアドレスを、ＡＲＰ応答パケットによって返送する。

【００２９】

ここで、ＡＲＰ応答として、ＡＲＰ要求の送信元へ返送されるＭＡＣアドレスは、デフォルトゲートウェイやネットワークセグメント３内の他の装置のＭＡＣアドレスを、センサー装置１のＭＡＣアドレスで偽装したものである。このため、誘導部２１によれば、ＡＲＰ応答を受信した対象端末２は、ＩＰパケットを送信しようとするネットワークセグメント３内の他の装置のＩＰアドレスと、当該他の装置のＭＡＣアドレスとしてのセンサー１装置のＭＡＣアドレスとを関連付けてＡＲＰテーブルに登録する。このため、誘導部２１は、対象装置２から送信されるＩＰパケットをセンサー装置１に誘導することができる。

【００３０】

通信遮断部２２は、誘導部２１によって誘導されたＩＰパケットをＮＩＣ１４から取得する。通信遮断部２２は、取得されたＩＰパケット中の宛先ＩＰアドレス及び宛先ポート番号が、補助記憶装置１５に記憶された転送ＩＰアドレス／ポートリストに含まれている場合を除き、原則として当該ＩＰパケットの転送を行わない。このため、原則として、誘導されたＩＰパケットは、他の装置に転送されず、対象装置２による他の装置への通信は遮断される。

【００３１】

本実施形態において、通信遮断部２２が通信を遮断する所定の条件は、宛先ＩＰアドレスが、転送ＩＰアドレス／ポートリストに含まれていないことである。なお、通信を遮断する所定の条件は、センサー装置１に誘導されたパケット内の宛先ポート番号に無関係な条件であってもよいし、送信元ＭＡＣアドレス、ＩＰパケットの送信元ＩＰアドレス等のその他の要素に関係する条件であってもよい。

【００３２】

誘導情報転送部２６は、誘導部２１によって誘導されたＩＰパケットをＮＩＣ１４から取得する。誘導情報転送部２６は、取得されたＩＰパケット中の宛先ＩＰアドレス及び宛先ポート番号が、補助記憶装置１５に記憶された転送ＩＰアドレス／ポートリストに含まれている場合に、即ち、通信遮断部２２により通信が遮断されるための所定の条件を満たさない場合に、宛先ＩＰアドレスに対応する、偽装されていないＭＡＣアドレスを有する他の装置へ、ＩＰパケットを転送する。このため、対象装置２は、通信を遮断されることなく、一部の通信を行うことができる。

【００３３】

識別情報取得部２３は、誘導部２１によって誘導されたＩＰパケットを解析し、ＩＰパケットがＨＴＴＰのリクエストメッセージが含まれている場合において、リクエストヘッダ内のＨｏｓｔからリクエストメッセージの通知先を識別する識別情報としてのホスト名を取得する。なお、ホスト名は、リクエストメッセージのリクエスト行のＵＲＩ（Ｕｎｉｆｏｒｍ Ｒｅｓｏｕｒｃｅ Ｉｄｅｎｄｔｉｆｉｅｒ）に基づいて取得されてもよい。

【００３４】

設定部２７は、通信許可部２５によって、通信遮断部２２による通信遮断にかかわらず

、対象装置２からのＨＴＴＰ通信が許可されるＷｅｂサーバ7を設定する。設定は、ドメイン名のリストにより記述され、許可サーバリストとして補助記憶装置１５に記憶される。リストの要素としてのドメイン名は、ＦＱＤＮ（Ｆｕｌｌｙ　Ｑｕａｌｉｆｉｅｄ　Ｄｏｍａｉｎ　Ｎａｍｅ）であるもの、及びＦＱＤＮでないもののいずれの形式でも記述できる。例えば、ＦＱＤＮとして"www.pfu.co.jp"、FQDNでないドメイン名として"pfu.co.jp"を記述できる。ＦＱＤＮは、ホスト名を全部記述したものであり、FQDNでないドメイン名は、ホスト名の一部を記述したものである。ＦＱＤＮでないドメイン名を記述することは、当該ドメイン名が示すドメインに属するすべてのホスト（Ｗｅｂサーバ7）へのＨＴＴＰ通信の許可を設定することを意味する。例えば、"pfu.co.jp"を記述することは、"www.pfu.co.jp"、"web.pfu.co.jp"等の複数のＷｅｂサーバ７へのＨＴＴＰ通信の許可を設定すること意味する。

【００３５】

大規模な通信システムや基幹システム等においては、冗長化や処理能力向上のため複数のサーバが備えられていることが多い。設定部２７によれば、許可されるＷｅｂサーバ７が複数ある場合にも、通信が許可されるＷｅｂサーバ７の設定をドメイン名により一括して記述できるため、１台１台のＷｅｂサーバ７を個別に記述する場合に比べ、システム管理者の作業負担を軽減することができる。また、通信システムのネットワーク構成が変更され、ＩＰアドレスが変更になった場合にも、設定部２７によれば、ドメイン名による記述の設定であるため、設定を変更する必要がなく、システム管理者の作業負担を軽減することができる。なお、対象装置２からのＨＴＴＰ通信が許可されるＷｅｂサーバ７の設定については、許可されないサーバのリストが記述され、記憶されてもよい。また、許可サーバリストの要素は、正規表現やワイルドカードを用いて記述されてもよい。

【００３６】

許可決定部２４は、識別情報取得部２３によって取得されたホスト名と、許可サーバリストの各要素とを、文字列として比較する。ホスト名が許可サーバリスト内のある要素（ホスト名の全部、又は一部に当たるＦＱＤＮではないドメイン名の文字列）を含んでいる場合（ホスト名とある要素が一致する場合も含む）には、許可決定部２４は、対象装置２からのＨＴＴＰ通信を許可する決定をする。許可サーバリスト内の全ての要素が、ホスト名が含まないものである場合は、許可決定部２４は、対象装置２からのＨＴＴＰ通信を許可しない決定をする。なお、許可決定部２４は、識別情報取得部２３によって取得されたホスト名に加え、例えば、リクエストメッセージ中のメソッド名、リソースを示すＵＲＩ等が所定の条件を満たすか否かに基づいて、許可するか否かを決定してもよい。

【００３７】

通信許可部２５は、許可決定部２４によってＨＴＴＰ通信を許可する決定がされたときに、通信遮断部２２により転送を行わないパケットが構成するＨＴＴＰのリクエストメッセージを転送することで、対象装置２によるＨＴＴＰ通信を許可する。通信許可部２５は、リクエストメッセージの転送の際、センサー装置１と転送先との間でＴＣＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｒｏｌ　Ｐｒｏｔｏｃｏｌ）のコネクションを確立する。

【００３８】

プロキシサーバ５を介したＨＴＴＰ通信は、実質的なリソース（Ｗｅｂコンテンツ）を提供するＷｅｂサーバ７が異なっていても、プロキシサーバ５の宛先ＩＰアドレスや宛先ポート番号が用いられるため、トランスポート層以下のプロトコルのメッセージ解析では、通信先のＷｅｂサーバ７が区別できない。本実施形態の識別情報取得部２３、許可決定部２４、及び通信許可部２５によれば、対象装置２からのＨＴＴＰメッセージに含まれる通信先のホスト名に基づいて通信を許可するため、プロキシサーバ５を介した通信についても、一部のＷｅｂサーバ７への通信を許可し、その他のＷｅｂサーバ７への通信を遮断することができる。

【００３９】

論理アドレス返答部２８は、誘導部２１によって誘導されたＩＰパケットが、ホスト名に対応する論理アドレスの問い合わせであるＤＮＳ問い合わせを構成する場合に、問い合

わせられた名前が、設定部２７によって設定された対象装置２からのＨＴＴＰ通信が許可されるＷｅｂサーバ7を示すときは、ＤＮＳ問い合わせに対して、Ｗｅｂサーバ７のＩＰアドレスではなく、所定の論理アドレスとしてのセンサー装置１のＩＰアドレスを返答する。このため、対象装置２は、ＤＮＳサーバ８と通信できない環境であっても、Ｗｅｂサーバ７の名前解決を行うことができる。特に、プロキシサーバ５への通信設定がされていない対象装置２は、通信しようとするＷｅｂサーバ７の名前解決を行おうとするため、論理アドレス返答部２８によって、この名前解決が失敗することを防ぐことができる。なお、論理アドレス返答部２８が返答する所定の論理アドレスは、センサー装置１のＩＰアドレス以外のＩＰアドレスであってもよい。

【００４０】

論理アドレス返答部２８は、ＤＮＳ問い合わせに返答する際、ＤＮＳサーバ８がＷｅｂサーバ７のホスト名の名前解決の際に設定するＴＴＬ（Ｔｉｍｅ　Ｔｏ　Ｌｉｖｅ）値よりも小さい値（例えば、６０秒）を、返答メッセージのＴＴＬ値に設定する。返答メッセージを受信した対象装置２は、このＴＴＬ値をＷｅｂサーバ７のホスト名に対応する論理アドレスであるセンサー装置１のＩＰアドレスの有効期間として扱う。このため、対象装置２は、センサー装置１が設置されていない別のネットワークに接続され、センサー装置１による通信の遮断の作用が及ばなくなった場合に、ＤＮＳサーバ８から、正規のＤＮＳ情報を速やかに取得できる。なお、論理アドレス返答部２８が設定するＴＴＬ値は、ＤＮＳサーバ８がＷｅｂサーバ７のホスト名の名前解決の際に設定するＴＴＬ値以上の値であってもよい。

【００４１】

プロキシサーバ通信部２９は、補助記憶装置１５に記憶されたプロキシサーバ５へのアクセス情報を用いて、ＮＩＣ１５を介してプロキシサーバ５と通信する。

【００４２】

≪実施形態１≫

実施形態１における通信及び処理について図面を用いて説明する。

【００４３】

＜通信システムの通信の流れ＞

実施形態１に係るセンサー装置１を含む通信システムにおける通信の流れについて説明する。実施形態１の通信システムでは、対象装置２からのプロキシサーバ５を介した通信のうち、一部のＷｅｂサーバ７への通信は許可され、その他のサーバへの通信は遮断される。

【００４４】

図３は、実施形態１に係るセンサー装置１を含む通信システムの通信の例を示すシーケンス図である。実施形態１において、対象装置２にはプロキシサーバ５のアクセス情報の設定がされている。また、センサー装置１には、Ｗｅｂサーバ７のホスト名が許可サーバリストに設定されている。図３では、対象装置２によるＷｅｂサーバ７とのＨＴＴＰ通信が、センサー装置１において許可され、センサー装置１とプロキシサーバ５を介して実現される。

【００４５】

ネットワークセグメント３に接続された対象装置２は、プロキシサーバ５と通信を行うために、プロキシサーバ５についてのＡＲＰ要求をブロードキャスト送信する（ステップＳ３０１）。このＡＲＰ要求を受信したセンサー装置１の誘導部２１は、センサー装置１のＭＡＣアドレスを、送信元の対象装置２に対して、ＡＲＰ応答パケットとして返送する（ステップＳ３０２）。ＡＲＰ応答パケットを受信した対象装置２は、プロキシサーバ５のＩＰアドレスに対応するＭＡＣアドレスとしてセンサー装置１のＭＡＣアドレスをＡＲＰテーブルに登録する。

【００４６】

対象装置２は、Ｗｅｂサーバ７と通信するためのＨＴＴＰのリクエストメッセージをプロキシサーバ５宛に送信する（ステップＳ３０３）。この際の送信パケットは、宛先ＭＡ

Ｃアドレスがセンサー装置１のＭＡＣアドレス、宛先ＩＰアドレスがプロキシサーバ５宛であり、リクエストヘッダのＨｏｓｔは、Ｗｅｂサーバ７のホスト名である。リクエストメッセージを受信したセンサー装置１の誘導情報転送部２６は、プロキシサーバ５のＩＰアドレスが転送ＩＰアドレス／ポートリストに含まれていないため、リクエストメッセージを構成するＩＰパケットの転送を行わない。

【００４７】

次に、センサー装置１の識別情報取得部２３がリクエストメッセージからホスト名を取得し、許可決定部２４は、このホスト名に基づいてＨＴＴＰ通信を許可する。センサー装置１の通信許可部２５は、対象装置２から受信されたリクエストメッセージをプロキシサーバ５に転送する（ステップＳ３０４）。なお、Ｗｅｂサーバ７のホスト名が許可サーバリストに設定されていない場合は、識別情報取得部２３がＨＴＴＰ通信を許可しないため、ＨＴＴＰ通信は遮断される。

【００４８】

ステップＳ３０５～Ｓ３０７では、プロキシサーバ５がＷｅｂサーバ７と代理通信する。リクエストメッセージを受信したプロキシサーバ５は、Ｗｅｂサーバ７にリクエストメッセージを代理送信する（ステップＳ３０５）。プロキシサーバ５からリクエストメッセージを受信したＷｅｂサーバ７は、レスポンスメッセージを生成し、プロキシサーバ５に送信する（ステップＳ３０６）。Ｗｅｂサーバ７からレスポンスメッセージを受信したプロキシサーバ５は、レスポンスメッセージを代理送信する（ステップＳ３０７）。

【００４９】

レスポンスメッセージを受信したセンサー装置１は、レスポンスメッセージをリクエストメッセージの送信元の対象装置２に転送する（ステップＳ３０８）。

【００５０】

＜センサー装置の処理の流れ＞

以上の通信の例は、センサー装置１の受信データの処理によって実現される。図４及び図５のフローチャートを用いて、実施形態１に係るセンサー装置１の受信データの処理の流れを説明する。なお、フローチャートに示された処理の具体的な内容及び順序は一例であり、処理内容及び順序には、実施の形態に適したものが適宜採用されることが好ましい。

【００５１】

図４は、実施形態１に係るセンサー装置１における対象装置２からの受信データ処理の流れを示すフローチャートである。対象装置２からの受信データ処理は、センサー装置１が、対象装置２の送信したデータを受信したことを契機に開始される。

【００５２】

ステップＳ４０１及びＳ４０２では、対象装置２からのＡＲＰ要求の処理がされる。まず、誘導部２１は、対象装置２からの受信データが、ＡＲＰ要求であるか否かを判定する（ステップＳ４０１）。ステップＳ４０１において、対象装置２からの受信データがＡＲＰ要求であると判定された場合、誘導部２１は、センサー装置１のＭＡＣアドレスを、送信元の対象装置２に対してＡＲＰ応答パケットとして返送する（ステップＳ４０２）。ステップＳ４０１において、対象装置２からの受信データがＡＲＰ要求でないと判定された場合は、ステップＳ４０３へ処理が進む。

【００５３】

ステップＳ４０３及びＳ４０４では、対象装置２からの受信データの転送についての処理がされる。まず、通信遮断部２２及び誘導情報転送部２６は、対象装置２からの受信データが、転送されるＩＰアドレス、ポート宛か否か、即ち、受信データ内の宛先ＩＰアドレス及び宛先ポート番号が、転送ＩＰアドレス／ポートリストに含まれているかを判定する（ステップＳ４０３）。ステップＳ４０３において、対象装置２からの受信データが、転送されるＩＰアドレス、ポート宛であると判定された場合には、誘導情報転送部２６は、宛先ＩＰアドレスに対応する、偽装されていないＭＡＣアドレスを有する他の装置に、受信データを転送する（ステップＳ４０４）。ステップＳ４０３において、ステップＳ４

０３において、対象装置２からの受信データが、転送されるＩＰアドレス、ポート宛でないと判定された場合は、ステップＳ４０５へ処理が進む。

【００５４】

ステップＳ４０５～Ｓ４０７では、ＨＴＴＰのリクエストメッセージの転送についての処理がされる。まず、識別情報取得部２３は、受信データを解析し、ＨＴＴＰのリクエストメッセージが構成されるか否かを判定する（ステップＳ４０５）。ステップＳ４０５において、ＨＴＴＰのリクエストメッセージが構成されると判定された場合には、識別情報取得部２３は、受信データからリクエストメッセージの通信先のホスト名を取得し、更に、許可決定部２４は、識別情報取得部２３によって取得されたホスト名に基づいて、リクエストメッセージ、通信許可されるＷｅｂサーバ７宛であるか否かを判定する（ステップＳ４０６）。ステップＳ４０６において、リクエストメッセージが通信許可されるＷｅｂサーバ７宛であると判定された場合は、許可決定部２４が、対象装置２からのＨＴＴＰ通信を許可する決定をし、通信許可部２５は、リクエストメッセージを受信データ中の宛先ＩＰアドレス及びポート番号が示す装置に転送する（ステップＳ４０７）。

【００５５】

ステップＳ４０５においてＨＴＴＰのリクエストメッセージが構成されないと判定された場合、又はステップＳ４０６においてリクエストメッセージが通信許可されるＷｅｂサーバ７宛でないと判断された場合には、受信データは破棄され、ＨＴＴＰのリクエストメッセージは転送さない（ステップＳ４０８）。なお、受信データがＨＴＴＰのリクエストメッセージを構成する場合は、ステップＳ４０８において、センサー装置１は、所定のＵＲＬへリダイレクトをするためのレスポンスメッセージを、対象装置２に送信してもよい。この送信によって、センサー装置１は、ＨＴＴＰ通信が遮断される対象装置２に対し、通信システムの利用申請を行うためのＷｅｂページ等の所定の情報の提供することができる。また、受信データがＨＴＴＰのリクエストメッセージを構成する場合は、ステップＳ４０８において、センサー装置１は、リクエストメッセージに関連するコネクションの切断を行ってもよい。

【００５６】

図５は、実施形態１に係るセンサー装置１におけるリクエストメッセージ転送先からの受信データ処理の流れを示すフローチャートである。リクエストメッセージ転送先からの受信データ処理は、センサー装置１が、図４のステップS４０７における通信許可部２５のリクエストメッセージ転送の際に確立したＴＣＰのコネクションから、データを受信したことを契機に開始される。

【００５７】

ステップＳ５０１～Ｓ５０３では、受信されたＨＴＴＰのレスポンスメッセージの転送についての処理がされる。まず、センサー装置１は、受信データがレスポンスメッセージであるか否かを判定する（ステップＳ５０１）。ステップＳ５０１において、受信データがレスポンスメッセージであると判定された場合には、センサー装置１は、リクエストメッセージの転送元である対象装置２に、レスポンスメッセージを転送する（ステップＳ５０２）。ステップＳ５０１において受信データがレスポンスメッセージでないと判定された場合には、センサー装置１は、受信データを破棄する（ステップＳ５０３）。

【００５８】

実施形態１に係るセンサー装置１によれば、ネットワークセグメント３に接続された対象装置２からのＨＴＴＰ通信のうち、プロキシサーバ５を介したＨＴＴＰ通信であっても、その通信先に応じて、一部のＷｅｂサーバ７への通信を許可し、その他のＷｅｂサーバ７への通信を遮断することが可能となる。また、実施形態１に係るセンサー装置１によれば、プロキシサーバ５宛の通信か否かに無関係に、ＨＴＴＰのメッセージによる通信の許可を決定するため、プロキシサーバ５を介さないＨＴＴＰ通信についてもホスト名による設定に基づいて許可及び遮断をすることができる。また、既にプロキシサーバ５が設置され、対象装置２にプロキシサーバ５の設定がされている通信システムに対し、ネットワークの構成やＩＰアドレス等の設定の変更をすることなく、センサー装置１を設置するだけ

で、プロキシサーバ５を介したＨＴＴＰ通信も含めて、対象装置２からのＨＴＴＰ通信の許可及び遮断をすることができる。

【００５９】

なお、実施形態１に係るセンサー装置１は、ＨＴＴＰ通信の許可及び遮断を行うが、例えば、ＳＭＴＰ（Ｓｉｍｐｌｅ Ｍａｉｌ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ）等の通信の許可及び遮断を行ってもよい。

【００６０】

≪実施形態２≫

実施形態２における通信及び処理について図面を用いて説明する。

【００６１】

＜通信システムの通信の流れ＞

実施形態２に係るセンサー装置１を含む通信システムにおける通信の流れについて説明する。実施形態２の通信システムにおいて、プロキシサーバ５のアクセス情報の設定がされていない対象装置２は、通信が許可されたＷｅｂサーバ７とＨＴＴＰ通信をすることができる。

【００６２】

図６は、実施形態２に係るセンサー装置１を含む通信システムの通信の例を示すシーケンス図である。図６では、プロキシサーバ５のアクセス情報の設定がされていない対象装置２によるＷｅｂサーバ７とのＨＴＴＰ通信が、センサー装置１において許可され、センサー装置１とプロキシサーバ５を介して実現される。なお、本通信の例では、センサー装置１の設定部２７によって事前にＷｅｂサーバ７のホスト名が許可サーバリストに設定されている。

【００６３】

ステップＳ６０１及びＳ６０２では、実施形態１と同様に、ＡＲＰ要求及びＡＲＰ応答の送信がされ、センサー装置１のＭＡＣアドレスが対象装置２のＡＲＰテーブルに登録される。

【００６４】

対象装置２は、Ｗｅｂサーバ７のホスト名の名前解決を行うためにＤＮＳ問い合わせを送信する（ステップＳ６０３）。この際の送信パケットは、宛先ＭＡＣアドレスがセンサー装置のＭＡＣアドレスであるため、センサー装置１がＤＮＳ問い合わせを受信する。

【００６５】

ＤＮＳ問い合わせを受信したセンサー装置１の論理アドレス返答部２８は、センサー装置１のＩＰアドレスを対象装置２に返答する（ステップＳ６０４）。

【００６６】

対象装置２は、Ｗｅｂサーバ７と通信するためのＨＴＴＰのリクエストメッセージをセンサー装置１宛に送信する（ステップＳ６０５）。この際の宛先ＩＰアドレスはＤＮＳ問い合わせに対して返答されたセンサー装置１のＩＰアドレスである。

【００６７】

リクエストメッセージを受信したセンサー装置１の識別情報取得部２３は、リクエストメッセージからホスト名を取得し、許可決定部２４は、ホスト名に基づいてＨＴＴＰ通信を許可する。センサー装置１の通信許可部２５は、対象装置２から受信されたリクエストメッセージをプロキシサーバ５向けのリクエストメッセージに変更して、プロキシサーバ５に転送する（ステップＳ６０６）。

【００６８】

ステップＳ６０７～Ｓ６０９では、実施形態１と同様に、プロキシサーバ５がＷｅｂサーバ７と代理通信する。

【００６９】

センサー装置１は、実施形態１と同様に、レスポンスメッセージを、リクエストメッセージの送信元の対象装置２に転送する（ステップＳ６１０）。

【００７０】

＜センサー装置の処理の流れ＞
以上の通信の例は、センサー装置１の受信データの処理によって実現される。図７及び図８のフローチャートを用いて、実施形態２に係るセンサー装置１の受信データの処理の流れを説明する。なお、フローチャートに示された処理の具体的な内容及び順序は一例であり、処理内容及び順序には、実施の形態に適したものが適宜採用されることが好ましい。

【００７１】
図７は、実施形態２に係るセンサー装置１における対象装置２からの受信データ処理の流れを示すフローチャートである。対象装置２からの受信データ処理は、センサー装置１が、対象装置２の送信したデータを受信したことを契機に開始される。

【００７２】
ステップＳ７０１及びＳ７０２では、実施形態１の図４のステップ４０１及び４０２と同様に、対象装置２からのＡＲＰ要求の処理がされる。

【００７３】
ステップＳ７０３～Ｓ７０５では、対象装置２にＤＮＳ問い合わせについての処理がされる。まず、論理アドレス返答部２８は、受信データがＤＮＳ問い合わせを構成するか否かを判定する（ステップＳ７０３）。ステップＳ７０３において、受信データがＤＮＳ問い合わせを構成すると判断された場合は、論理アドレス返答部２８は、問い合わせられた名前がＨＴＴＰ通信の許可されるＷｅｂサーバ7を示すか否かを判定する（ステップＳ７０４）。ステップＳ７０４において、問い合わせられた名前がＨＴＴＰ通信の許可されるＷｅｂサーバ7を示すと判定された場合は、論理アドレス返答部２８は、センサー装置１のＩＰアドレスを返答する（ステップＳ７０５）。ステップＳ７０３において、受信データがＤＮＳ問い合わせを構成しないと判定された場合は、ステップＳ７０６へ処理が進む。ステップＳ７０４において、問い合わせられた名前がＨＴＴＰ通信の許可されるＷｅｂサーバ7を示さないと判定された場合は、ステップＳ７０７へ処理が進む。

【００７４】
ステップＳ７０６及びＳ７０７では、実施形態１の図４のステップＳ４０３及びＳ４０４と同様に、対象装置２からの受信データの転送についての処理がされる。

【００７５】
ステップＳ７０８～Ｓ７１０では、実施形態１の図４のステップＳ４０５、Ｓ４０６、及びＳ４０８と同様に、受信データが破棄される。

【００７６】
ステップＳ７１１～Ｓ７１４では、リクエストメッセージが転送される。まず、通信許可部２５は、受信データの宛先ＩＰアドレスがセンサー装置１のＩＰアドレスであり、かつリクエストメッセージがプロキシサーバ５向けのメッセージであるか否かを判定する（ステップＳ７１１）。リクエストメッセージにホスト名を基準とした相対的な情報が含まれている場合は、プロキシサーバ５向けのメッセージでないと判定される。また、リクエストメッセージにホスト名を基準とした相対的な情報が含まれてない場合は、プロキシサーバ５向けのメッセージであると判定される。

【００７７】
実施形態２では、リクエストメッセージにホスト名を基準とした相対的な情報が含まれている否かは、リクエスト行のＵＲＩが相対的な形式のＵＲＩであるか否かによる。図９は、Ｗｅｂサーバ７向けのＨＴＴＰリクエストメッセージのリクエストヘッダの例（一部）である。図１０は、プロキシサーバ５向けのＨＴＴＰリクエストメッセージのリクエストヘッダの例（一部）である。図９及び図１０のいずれも、"http://www.pfu.co.jp"が示すリソースを取得するためのリクエストヘッダである。図９のＵＲＩは、"/"であり、ホスト名"www.pfu.co.jp"を基準とした相対的な形式のＵＲＩである。図１０のＵＲＩは、"http://www.pfu.co.jp"であり、絶対的な形式のＵＲＩである。

【００７８】
ステップＳ７１１において、受信データの宛先ＩＰアドレスがセンサー装置１のＩＰア

ドレスであり、かつリクエストメッセージがプロキシサーバ５向けのメッセージでないと判定された場合は、通信許可部２５は、リクエストメッセージを、リクエスト行のＵＲＩを上述した絶対的な形式に書き換えることで、プロキシサーバ５向けに変更する（ステップＳ７１２）。次に、通信許可部２５は、プロキシサーバ通信部２９を介して、ステップＳ７１２で変更したリクエストメッセージをプロキシサーバ５に転送する（ステップＳ７１３）。ステップS７１１において、受信データの宛先ＩＰアドレスがセンサー装置１のＩＰアドレスであり、かつリクエストメッセージがプロキシサーバ５向けのメッセージであると判定された場合は、通信許可部２５は、実施形態１の図４のステップＳ４０７と同様に、リクエストメッセージを受信データ中の宛先ＩＰアドレス及びポート番号が示す装置に転送する（ステップＳ７１４）。ステップＳ７１４では、リクエストメッセージはプロキシサーバ５向けに変更されずに転送される。

【００７９】

図８は、実施形態２に係るセンサー装置１におけるプロキシサーバ５からの受信データ処理の流れを示すフローチャートである。プロキシサーバ５からの受信データ処理は、センサー装置１が、図７のＳステップ７１３における通信許可部２５のリクエストメッセージ転送の際に確立したＴＣＰのコネクションから、データを受信したことを契機に開始される。なお、図７のステップＳ７１４における通信許可部２５のリクエストメッセージ転送の際に確立したＴＣＰのコネクションから、データを受信した場合の処理は、図５を用いて説明した、実施形態１と同様の処理であり、ここでは説明を省略する。

【００８０】

まず、センサー装置１は、受信データがレスポンスメッセージであるか否かを判定する（ステップＳ８０１）。ステップＳ８０１において、受信データがレスポンスメッセージであると判定された場合には、リクエストメッセージを対象装置２向けに変更し（ステップＳ８０２）、変更したレスポンスメッセージを、リクエストメッセージの転送元である対象装置２に転送する（ステップＳ８０３）。ステップＳ８０１において、受信データがレスポンスメッセージでないと判定された場合には、受信データは破棄される（ステップＳ８０４）。

【００８１】

携帯端末等にはプロキシサーバ５への通信設定が行えないものがある。従来、このようなプロキシサーバ５への通信設定が行えない情報処理装置やプロキシサーバ５への通信設定を行っていない情報処理装置は、プロキシサーバ５を介した通信を行うことができないという問題があった。このため、特に、企業が新たにクラウドサービスを導入しようとする際、クラウドサービスを利用するための全ての情報処理装置にプロキシサーバ５への通信設定を行う作業が必要とされる不都合や、プロキシサーバ５への通信設定が行えない携帯端末等をクラウドサービスのために利用できないという不都合が生じていた。

【００８２】

実施形態２に係るセンサー装置１によれば、プロキシサーバ５の設定がされていない、あるいはプロキシサーバ５の設定をすることができない対象装置２は、プロキシサーバ５を介したＷｅｂサーバ７との通信を行うことが可能となる。また、実施形態２に係るセンサー装置１によれば、Ｗｅｂサーバ７との通信のためにプロキシサーバ５を介す必要のあるネットワーク環境において、プロキシサーバ５の設定がされていない、あるいはプロキシサーバ５の設定をすることができない対象装置２によるＨＴＴＰ通信のうち、その通信先に応じて、一部のＷｅｂサーバ７への通信を許可し、その他のＷｅｂサーバ７への通信を遮断することが可能となる。更に、プロキシサーバ５の設定がされている対象装置２とプロキシサーバ５の設定がされていない、あるいはプロキシサーバ５の設定をすることができない対象装置２とが、混在してネットワークセグメント３に接続される場合であっても、ＨＴＴＰ通信の許可及び遮断を一つの設定で一元的に管理することができる。

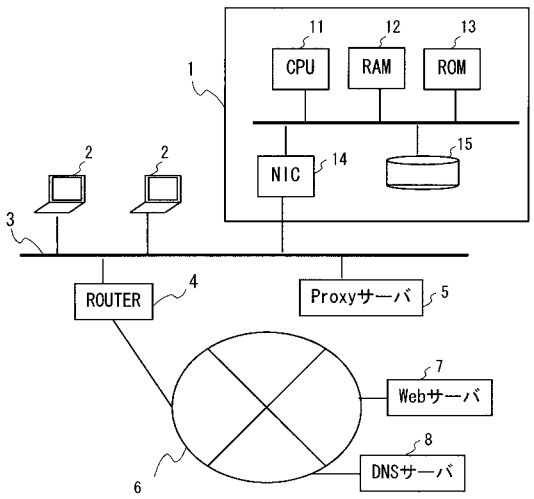
【符号の説明】

【００８３】

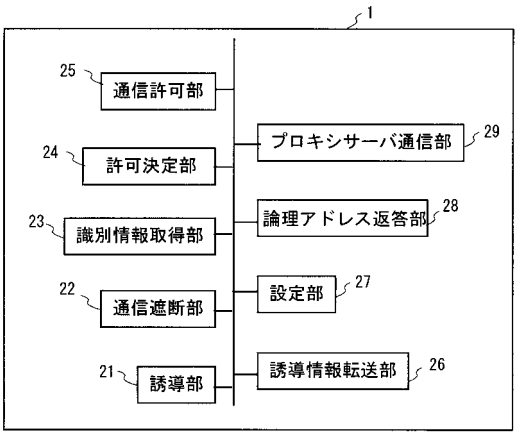
１　センサー装置（通信遮断装置）

２　対象装置（情報処理装置）
３　ネットワークセグメント
４　ルータ
５　プロキシサーバ
６　インターネット
７　Ｗｅｂサーバ
８　ＤＮＳサーバ
２１　誘導部
２２　通信遮断部
２３　識別情報取得部
２４　許可決定部
２５　通信許可部
２６　誘導情報転送部
２７　設定部
２８　論理アドレス返答部
２９　プロキシサーバ通信部

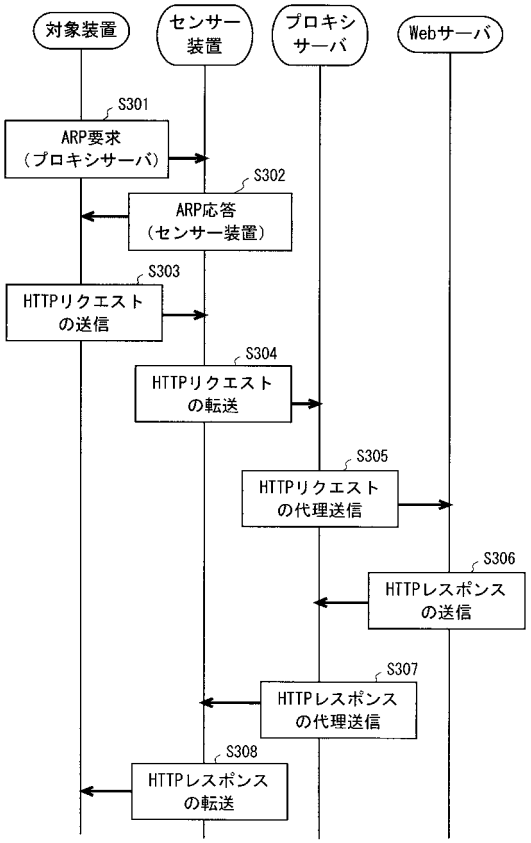
【図１】



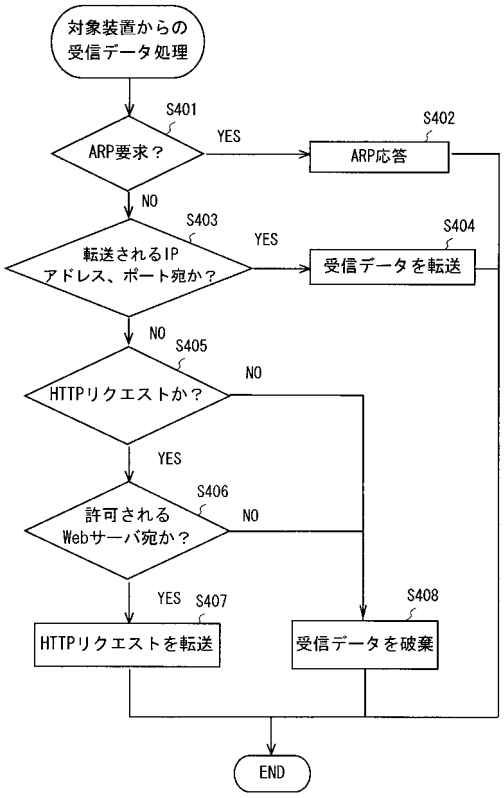
【図２】



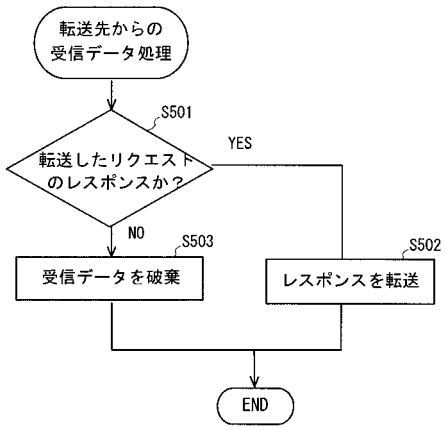
【図３】


対象装置
センサー装置
プロキシサーバ
Webサーバ
S301
ARP要求（プロキシサーバ）
S302
ARP応答（センサー装置）
S303
HTTPリクエストの送信
S304
HTTPリクエストの転送
S305
HTTPリクエストの代理送信
S306
HTTPレスポンスの送信
S307
HTTPレスポンスの代理送信
S308
HTTPレスポンスの転送

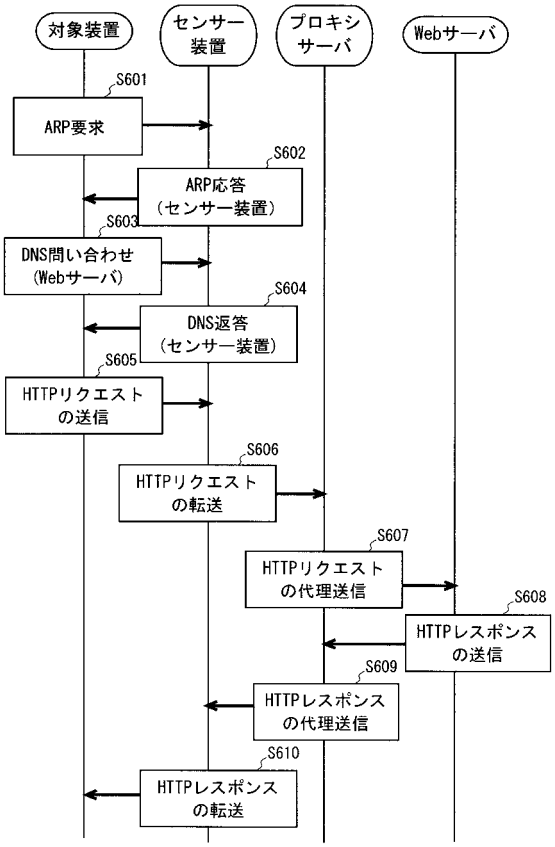
【図４】


対象装置からの受信データ処理
S401
ARP要求？
YES
S402
ARP応答
NO
S403
転送されるIPアドレス、ポート宛か？
YES
S404
受信データを転送
NO
S405
HTTPリクエストか？
NO
YES
S406
許可されるWebサーバ宛か？
NO
YES
S407
HTTPリクエストを転送
S408
受信データを破棄
END

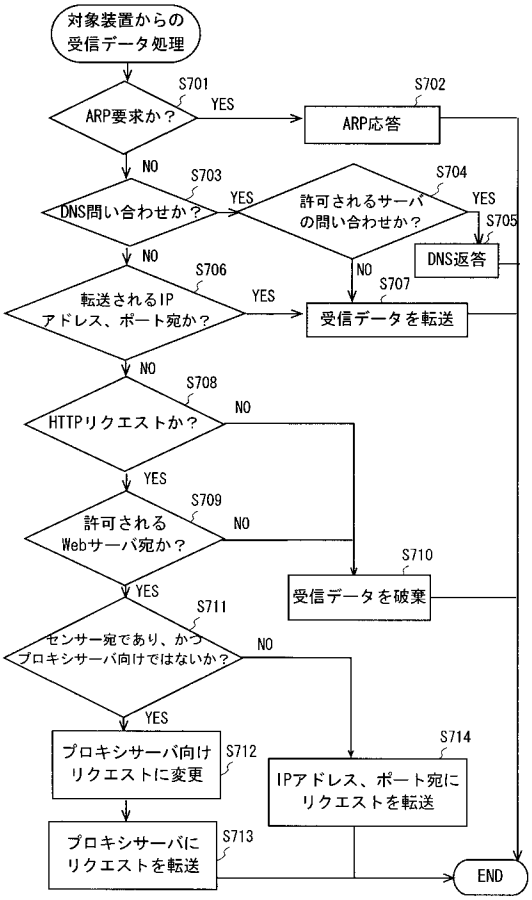
【図５】


転送先からの受信データ処理
S501
転送したリクエストのレスポンスか？
YES
NO
S503
受信データを破棄
S502
レスポンスを転送
END

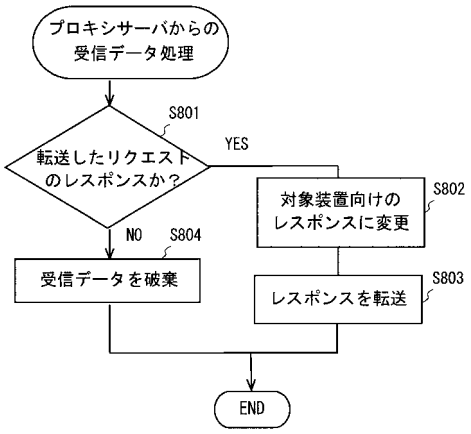
【図６】


対象装置
センサー装置
プロキシサーバ
Webサーバ
S601
ARP要求
S602
ARP応答（センサー装置）
S603
DNS問い合わせ（Webサーバ）
S604
DNS返答（センサー装置）
S605
HTTPリクエストの送信
S606
HTTPリクエストの転送
S607
HTTPリクエストの代理送信
S608
HTTPレスポンスの送信
S609
HTTPレスポンスの代理送信
S610
HTTPレスポンスの転送

【図７】



【図８】



【図９】

```
GET / HTTP/1.0
Host: www.pfu.co.jp
Accept: */*
Accept-Language: ja
UA-CPU: x86
Accept-Encoding: gzip, deflate
・・・・
```

【図１０】

```
GET http://www.pfu.co.jp/ HTTP/1.0
Host: www.pfu.co.jp
Accept: */*
Accept-Language: ja
UA-CPU: x86
Accept-Encoding: gzip, deflate
・・・・
```