

(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2010-220071

(P2010-220071A)

(43) 公開日 平成22年9月30日(2010.9.30)

(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 11 O L (全 21 頁)

(21) 出願番号	特願2009-66685 (P2009-66685)	(71) 出願人	000004237
(22) 出願日	平成21年3月18日 (2009.3.18)		日本電気株式会社
			東京都港区芝五丁目7番1号
		(74) 代理人	100103090
			弁理士 岩壁 冬樹
		(74) 代理人	100124501
			弁理士 塩川 誠人
		(72) 発明者	落丸 直詩
			東京都港区芝五丁目7番1号 日本電気株
			式会社内
		Fターム(参考)	5K030 GA15 HA08 HD03 HD06 JT02
			KA05 LC15

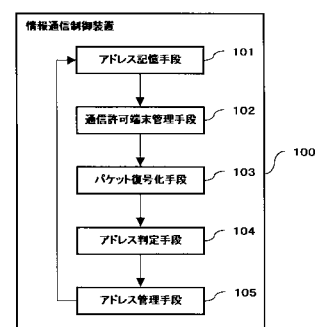
(54) 【発明の名称】 情報通信制御装置、ネットワークインタフェース装置、方法及びプログラム

(57) 【要約】

【課題】 少ない処理で不正アクセスを制限することは困難である。

【解決手段】 通信を許可するアドレスを記憶するアドレス記憶手段と、送信元端末から送信先端末にパケットが送信された際に、送信元端末のアドレスが、アドレス記憶手段に記憶されるアドレスに合致するか否かを判定し、合致すると判定すると送信先端末との通信を許可する通信許可端末管理手段と、合致しないと判定すると、パケットが復号可能か否かを判定し、復号可能であれば予め定められた復号化方法を用いてパケットに含まれる所定の暗号化領域のデータを復号化するパケット復号化手段と、復号化したデータが、送信元端末のアドレスと合致するか否かを判定するアドレス判定手段と、合致すると判定すると、認証に成功したと判定し、復号化したデータによってアドレス記憶手段が記憶するアドレスを更新するアドレス管理手段とを備えたことを特徴とする。

【選択図】 図9



【特許請求の範囲】

【請求項 1】

通信を許可するアドレスを記憶するアドレス記憶手段と、

送信元端末から送信先端末にパケットが送信された際に、前記送信元端末のアドレスが、前記アドレス記憶手段に記憶されるアドレスに合致するか否かを判定し、合致すると判定すると前記送信先端末との通信を許可する通信許可端末管理手段と、

前記通信許可端末管理手段が合致しないと判定すると、前記パケットが復号可能か否かを判定し、復号可能であれば予め定められた復号化方法を用いて前記パケットに含まれる所定の暗号化領域のデータを復号化するパケット復号化手段と、

前記パケット復号化手段が復号化したデータが、前記送信元端末のアドレスと合致するか否かを判定するアドレス判定手段と、

前記アドレス判定手段が合致すると判定すると、認証に成功したと判定し、前記復号化したデータによって前記アドレス記憶手段が記憶するアドレスを更新するアドレス管理手段とを

備えたことを特徴とする情報通信制御装置。

【請求項 2】

アドレス管理手段は、アドレス記憶手段に記憶させたアドレスを、記憶させた時点から所定期間経過すると、前記アドレス記憶手段から消去する

請求項 1 記載の情報通信制御装置。

【請求項 3】

パケット復号化手段によってパケットが復号可能であると判定されると、前記パケットを送信先端末に送信する送信手段と、

前記パケット復号化手段によって前記パケットが復号不可能であると判定されると、前記パケットを破棄するパケット破棄手段とを備えた

請求項 1 又は請求項 2 記載の情報通信制御装置。

【請求項 4】

通信許可端末管理手段が合致しないと判定すると、パケットが ICMP echo パケットであるか否かを判定する ICMP echo パケット判定手段を備え、

パケット復号化手段は、前記 ICMP echo パケット判定手段が ICMP echo パケットであると判定すると、前記パケットが復号可能か否かを判定し、復号可能であれば前記パケットを復号化する

請求項 1 から請求項 3 のうちのいずれか 1 項に記載の情報通信制御装置。

【請求項 5】

パケット復号化手段が復号化したパケットが、前記パケットの暗号化及び復号化に用いる暗号鍵を更新する要求とともに、新たな暗号鍵を含む場合に、当該情報通信制御装置が備える暗号鍵記憶部が記憶する暗号鍵を前記新たな暗号鍵で更新する暗号鍵更新手段を備えた

請求項 1 から請求項 4 のうちのいずれか 1 項に記載の情報通信制御装置。

【請求項 6】

通信を許可するアドレスを記憶するアドレス記憶手段と、

送信元端末から送信先端末にパケットが送信された際に、前記送信元端末のアドレスが、前記アドレス記憶手段に記憶されるアドレスに合致するか否かを判定し、合致すると判定すると前記送信先端末との通信を許可する通信許可端末管理手段と、

前記通信許可端末管理手段が合致しないと判定すると、前記パケットが復号可能か否かを判定し、復号可能であれば予め定められた復号化方法を用いて前記パケットに含まれる所定の暗号化領域のデータを復号化するパケット復号化手段と、

前記パケット復号化手段が復号化したデータが、前記送信元端末のアドレスと合致するか否かを判定するアドレス判定手段と、

前記アドレス判定手段が合致すると判定すると、認証に成功したと判定し、前記復号化したデータによって前記アドレス記憶手段が記憶するアドレスを更新するアドレス管理手

10

20

30

40

50

段とを

備えたことを特徴とするネットワークインタフェース装置。

【請求項 7】

アドレス管理手段は、アドレス記憶手段に記憶させたアドレスを、記憶させた時点から所定期間経過すると、前記アドレス記憶手段から消去する

請求項 6 記載のネットワークインタフェース装置。

【請求項 8】

送信元端末から送信先端末にパケットが送信された際に、前記送信元端末のアドレスが、通信を許可するアドレスを記憶する記憶手段に記憶されるアドレスに合致するか否かを判定し、合致すると判定すると前記送信先端末との通信を許可する通信許可端末管理ステップと、

合致しないと判定すると、前記パケットが復号可能か否かを判定し、復号可能であれば予め定められた復号化方法を用いて前記パケットに含まれる所定の暗号化領域のデータを復号化するパケット復号化ステップと、

復号化したデータが、前記送信元端末のアドレスと合致するか否かを判定するアドレス判定ステップと、

合致すると判定すると、認証に成功したと判定し、前記復号化したデータによって前記アドレス記憶手段が記憶するアドレスを更新するアドレス管理ステップとを

含むことを特徴とする情報通信制御方法。

【請求項 9】

アドレス管理ステップで、アドレス記憶手段に記憶させたアドレスを、記憶させた時点から所定期間経過すると、前記アドレス記憶手段から消去する

請求項 8 記載の情報通信制御方法。

【請求項 10】

通信を許可するアドレスを記憶するアドレス記憶手段を備えたコンピュータに、

前記送信元端末から前記送信先端末にパケットが送信された際に、前記送信元端末のアドレスが、前記アドレス記憶手段に記憶されるアドレスに合致するか否かを判定し、合致すると判定すると前記送信先端末との通信を許可する通信許可端末管理処理と、

合致しないと判定すると、前記パケットが復号可能か否かを判定し、復号可能であれば予め定められた復号化方法を用いて前記パケットに含まれる所定の暗号化領域のデータを復号化するパケット復号化処理と、

復号化したデータが、前記送信元端末のアドレスと合致するか否かを判定するアドレス判定処理と、

合致すると判定すると、認証に成功したと判定し、前記復号化したデータによって前記アドレス記憶手段が記憶するアドレスを更新するアドレス管理処理とを

実行させるための情報通信制御プログラム。

【請求項 11】

コンピュータに、

アドレス管理処理で、アドレス記憶手段に記憶させたアドレスを、記憶させた時点から所定期間経過すると、前記アドレス記憶手段から消去するように実行させる

請求項 10 記載の情報通信制御プログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、情報処理端末間の情報通信を制御する情報通信制御装置、情報通信制御方法及び情報通信制御プログラムに関する。また、本発明は、情報処理端末に装着されるネットワークインタフェース装置に関する。

【背景技術】

【0002】

情報処理端末間の情報通信を制御する機器として、例えば、特許文献 1 には、I C M P

10

20

30

40

50

を用いた情報端末用ネットワークインタフェース装置の一例が記載されている。特許文献 1 に記載された I C M P を用いた情報端末用ネットワークインタフェース装置は、外部ネットワークを介して通信するネットワークインタフェース装置と、I P パケットを処理する装置と、I C M P の宛先到達不能メッセージを検出する装置と、I C M P の宛先到達不能メッセージの頻度に応じて通信をフィルタリングする装置とから構成されている。

【0003】

また、特許文献 2 には、送信情報の送信元アドレスが変化する場合であっても、情報の通過制御を適切に行うことが可能な情報通過制御システムが記載されている。

【先行技術文献】

【特許文献】

10

【0004】

【特許文献 1】特開 2005-51588 号公報

【特許文献 2】特開 2005-159683 号公報

【発明の概要】

【発明が解決しようとする課題】

【0005】

特許文献 1 に記載された I C M P を用いた情報端末用ネットワークインタフェース装置は、ある機器が処理不能な I P パケットを送信された際に、送信元の端末に送信する I C M P の宛先到達不能メッセージを、不正アクセスが行われた回数として記録する。そして、その回数が所定の回数に及んだ時点で、I C M P の宛先到達不能メッセージを生成する原因となっている I P パケットの通信を制限するように動作する。

20

【0006】

このため、特許文献 1 に記載された I C M P を用いた情報端末用ネットワークインタフェース装置には、不正アクセスが所定の回数に及ぶまで、不正アクセスを通過させてしまう課題がある。また、他人の I P アドレスを偽装した成りすましによる不正アクセスが行われた場合、本来制限されるべきでない通信も制限対象としてしまう課題がある。

【0007】

また、特許文献 2 に記載されたシステムでは、復号化したデータが以前に発行した識別情報を含むチケットと一致することを条件としてパケットを通過させるため、事前に識別情報の生成と発行とを行う必要がある。

30

【0008】

そこで、本発明は、少ない処理で不正アクセスを制限することができる情報通信制御装置、ネットワークインタフェース装置、情報通信制御方法及び情報通信制御プログラムを提供することを目的とする。

【課題を解決するための手段】

【0009】

本発明による情報通信制御装置は、通信を許可するアドレスを記憶するアドレス記憶手段と、送信元端末から送信先端末にパケットが送信された際に、送信元端末のアドレスが、アドレス記憶手段に記憶されるアドレスに合致するか否かを判定し、合致すると判定すると送信先端末との通信を許可する通信許可端末管理手段と、通信許可端末管理手段が合致しないと判定すると、パケットが復号可能か否かを判定し、復号可能であれば予め定められた復号化方法を用いてパケットに含まれる所定の暗号化領域のデータを復号化するパケット復号化手段と、パケット復号化手段が復号化したデータが、送信元端末のアドレスと合致するか否かを判定するアドレス判定手段と、アドレス判定手段が合致すると判定すると、認証に成功したと判定し、復号化したデータによってアドレス記憶手段が記憶するアドレスを更新するアドレス管理手段とを備えたことを特徴とする。

40

【0010】

本発明によるネットワークインタフェース装置は、通信を許可するアドレスを記憶するアドレス記憶手段と、送信元端末から送信先端末にパケットが送信された際に、送信元端末のアドレスが、アドレス記憶手段に記憶されるアドレスに合致するか否かを判定し、合

50

致すると判定すると送信先端末との通信を許可する通信許可端末管理手段と、通信許可端末管理手段が合致しないと判定すると、パケットが復号可能か否かを判定し、復号可能であれば予め定められた復号化方法を用いてパケットに含まれる所定の暗号化領域のデータを復号化するパケット復号化手段と、パケット復号化手段が復号化したデータが、送信元端末のアドレスと合致するか否かを判定するアドレス判定手段と、アドレス判定手段が合致すると判定すると、認証に成功したと判定し、復号化したデータによってアドレス記憶手段が記憶するアドレスを更新するアドレス管理手段とを備えたことを特徴とする。

【0011】

本発明による情報通信制御方法は、送信元端末から送信先端末にパケットが送信された際に、送信元端末のアドレスが、通信を許可するアドレスに記憶される記憶手段が記憶するアドレスに合致するか否かを判定し、合致すると判定すると送信先端末との通信を許可する通信許可端末管理ステップと、合致しないと判定すると、パケットが復号可能か否かを判定し、復号可能であれば予め定められた復号化方法を用いてパケットに含まれる所定の暗号化領域のデータを復号化するパケット復号化ステップと、復号化したデータが、送信元端末のアドレスと合致するか否かを判定するアドレス判定ステップと、合致すると判定すると、認証に成功したと判定し、復号化したデータによってアドレス記憶手段が記憶するアドレスを更新するアドレス管理ステップとを含むことを特徴とする。

【0012】

本発明による情報通信制御プログラムは、送信先端末との通信を許可する送信元端末のアドレスを記憶するアドレス記憶手段を備えたコンピュータに、送信元端末から送信先端末にパケットが送信された際に、送信元端末のアドレスが、アドレス記憶手段に記憶されるアドレスに合致するか否かを判定し、合致すると判定すると送信先端末との通信を許可する通信許可端末管理処理と、合致しないと判定すると、パケットが復号可能か否かを判定し、復号可能であればパケットを復号化するパケット復号化処理と、復号化したパケットが含む送信元のアドレスが、送信元端末のアドレスと合致するか否かを判定するアドレス判定処理と、合致すると判定すると、送信元端末のアドレスをアドレス記憶手段に記憶させるアドレス管理処理とを実行させるためのものである。

【発明の効果】

【0013】

本発明によれば、少ない処理で不正アクセスを制限することができる。

【図面の簡単な説明】

【0014】

【図1】本発明による情報通信制御装置を適用したシステムの構成例を示すブロック図である。

【図2】ネットワークインタフェース装置1の構成例を示すブロック図である。

【図3】ICMPパケットのデータ構造の一例を示す説明図である。

【図4】ネットワークインタフェース装置1が、ネットワーク4を介して、遠隔情報端末3からデータを受信した際の動作の一例を示す流れ図である。

【図5】ネットワークインタフェース装置1が、ネットワーク4を介して、遠隔情報端末3からデータを受信した際の動作の一例を示す流れ図である。

【図6】ネットワークインタフェース装置1が、ネットワーク4を介して、遠隔情報端末3からデータを受信した際の動作の一例を示す流れ図である。

【図7】情報端末2からデータ送信をする際の動作の一例を示す流れ図である。

【図8】通信許可端末を示す情報の管理動作の一例を示す流れ図である。

【図9】情報通信制御装置の最小の構成例を示すブロック図である。

【発明を実施するための形態】

【0015】

以下、本発明の実施形態について図面を参照して説明する。図1は、本発明による情報通信制御装置を適用したシステムの構成例を示すブロック図である。図1に示すように、情報通信制御装置を適用したシステムは、ネットワークインタフェース装置1、情報端末

10

20

30

40

50

2 及び遠隔情報端末 3 を含む。また、情報端末 2 と遠隔情報端末 3 とは、ネットワークインタフェース装置 1 及びネットワーク 4 を介して相互に接続される。なお、本実施形態では、情報通信制御装置として、ネットワークインタフェース装置 1 を用いて説明する。

【0016】

図 1 に示すように、ネットワークインタフェース装置 1 は、通信先管理部 11、送信制御部 12、入出力手段 13、ICMP パケット処理部 14、受信制御部 15 及び送受信手段 16 を含む。

【0017】

なお、具体的には、ネットワークインタフェース装置 1 は、パーソナルコンピュータ等の情報処理端末に装備されるインタフェースカードによって実現される。また、情報通信制御装置は、ネットワークインタフェース装置に限らず、例えば、ルータ装置や、ルータ機能を搭載したプログラムに従って動作する情報処理端末であってもよい。

【0018】

ネットワークインタフェース装置 1 は、情報端末 2 が備える一般的な拡張機器スロットに装着可能な装着部を備えている。ネットワークインタフェース装置 1 は、情報端末 2 からの要求に基づいて、送受信手段 16 を介して、ネットワーク 4 と接続される。また、ネットワークインタフェース装置 1 は、情報端末 2 からの要求に基づいて、遠隔情報端末 3 などの外部情報端末との間で送受信するデータの中継を行う機能を備えている。

【0019】

通信先管理部 11 は、送信制御部 12 からの通信許可端末であるか否かを確認する要求（以下、通信許可端末の確認要求）に応じて、通信を許可する端末（以下、通信許可端末）であるか否かを確認する処理を実行する機能を備えている。具体的には、通信先管理部 11 は、送信制御部 12 から渡される（入力される）IP アドレスが、自身が記憶する通信を許可する端末群の IP アドレスと一致する場合、確認処理の結果として、送信制御部 12 に許可する旨を出力する。一方、通信先管理部 11 は、送信制御部 12 から渡される（入力される）IP アドレスが、自身が記憶する通信を許可する端末群の IP アドレスと一致しない場合、確認処理の結果として、送信制御部 12 に不許可である旨を出力する。

【0020】

通信先管理部 11 は、受信制御部 15 からの通信許可端末の確認要求に応じて、通信許可端末であるか否かを確認する処理を実行する機能を備えている。具体的には、通信先管理部 11 は、受信制御部 15 から渡される（入力される）IP アドレスが、自身が記憶する通信を許可する端末群の IP アドレスと一致する場合、確認処理の結果として、受信制御部 15 に許可する旨を出力する。一方、通信先管理部 11 は、受信制御部 15 から渡される（入力される）IP アドレスが、自身が記憶する通信を許可する端末群の IP アドレスと一致しない場合、確認処理の結果として、受信制御部 15 に不許可である旨を出力する。

【0021】

通信先管理部 11 は、ICMP パケット処理部 14 から渡される（入力される）IP アドレスを、通信を許可する端末群の IP アドレスとして記憶する。また、通信先管理部 11 は、記憶してから所定期間が経過すると、記憶した通信を許可する端末群の IP アドレスを消去する機能を備えている。

【0022】

送信制御部 12 は、情報端末 2 からのデータ送信要求に応じて、情報端末 2 が指定する外部情報端末に、送受信手段 16 を介して、データを送信する機能を備えている。

【0023】

送信制御部 12 は、情報端末 2 から受信した送信データから送信先を示す IP アドレスを取得（抽出）する機能を備えている。例えば、送信制御部 12 は、送信するパケットのヘッダに含まれる送信先を示す IP アドレスを抽出する。

【0024】

送信制御部 12 は、取得（抽出）した IP アドレスを通信先管理部 11 に渡して（出力

10

20

30

40

50

して)、通信許可端末の確認要求を行い、通信先管理部 11 から通信許可端末の確認処理の結果を受け取る(入力される)機能を備えている。

【0025】

送信制御部 12 は、通信先管理部 11 が入力した通信許可端末の確認処理の結果が許可を示す場合、送受信手段 16 を用いて、情報端末 2 から受信したデータを、取得(抽出)した送信先に送信する機能を備えている。

【0026】

送信制御部 12 は、通信先管理部 11 が入力した通信許可端末の確認処理の結果が不許可を示す場合、情報端末 2 に送信エラーを示す情報を返却(送信)し、情報端末 2 から受信したデータを廃棄する機能を備えている。

10

【0027】

入出力手段 13 は、情報端末 2 の入出力手段 21 と接続可能な機能を備えている。また、入出力手段 13 は、情報端末 2 の入出力手段 21 と物理的に接続可能な形状に形成されている。

【0028】

入出力手段 13 は、情報端末 2 からネットワークインタフェース装置 1 に対する要求の受け入れ(受信)を行う機能を備えている。入出力手段 13 は、情報端末 2 とネットワークインタフェース装置 1 との間のデータの受け渡し(送受信)を行う機能を備えている。

【0029】

ICMP パケット処理部 14 は、受信制御部 15 から、ICMP パケットが本実施形態で規定する暗号領域を含み、認証が可能であるか否かを判定する処理(以下、ICMP パケット処理)の要求とともに、ICMP echo パケット及び同パケットの送信元を示す IP アドレスを受信する(入力される)機能を備えている。

20

【0030】

ICMP パケット処理部 14 は、受信制御部 15 から受信した(入力された) ICMP echo パケットが、本実施形態で規定する暗号領域を含み、認証処理が可能であるか否かを判定する機能を備えている。また、ICMP パケット処理部 14 は、認証処理の結果を受信制御部 15 に返却(出力)する機能を備えている。なお、ICMP パケット処理部 14 は、例えば、ICMP echo パケットに、予め定めたデータ構造の暗号領域(暗号化したデータを含む領域)が含まれると判定したことに基づいて、復号可能である(認証可能である)と判定する。

30

【0031】

ICMP パケット処理部 14 は、本実施形態で規定する認証処理が可能である ICMP パケットを送信した遠隔情報端末 3 の IP アドレスを記憶するように、通信先管理部 11 に要求を出力する。

【0032】

ICMP パケット処理部 14 は、本実施形態で規定する認証処理が可能である ICMP パケットに、暗号鍵を設定する要求(以下、暗号鍵設定要求)と暗号鍵とが含まれていた場合、自身の暗号鍵記憶領域に、受信した(入力された)暗号鍵を記憶する。

【0033】

40

受信制御部 15 は、送受信手段 16 を用いて、ネットワーク 4 を介して外部から送信されたデータを受信する機能を備えている。受信制御部 15 は、送受信手段 16 が外部から受信したデータの送信元を示す IP アドレスを取得する機能を備えている。例えば、受信制御部 15 は、受信したパケットのヘッダに含まれる送信元を示す IP アドレスを抽出する。

【0034】

受信制御部 15 は、送受信手段 16 が外部から受信したデータが ICMP echo パケットである場合、ICMP パケット処理部 14 に ICMP パケット処理の要求とともに、受信した ICMP echo パケット及び送信元を示す IP アドレスとを出力する機能を備えている。また、受信制御部 15 は、ICMP パケット処理部 14 による ICMP パ

50

ケット処理の要求の結果を受信する機能を備えている。

【0035】

受信制御部15は、ICMPパケット処理部14から受信した（入力された）ICMPパケット処理の要求の結果が成功であった場合、受信したICMP echoパケットを、入出力手段13を用いて、情報端末2に送信する機能を備えている。受信制御部15は、ICMPパケット処理部14から受信した（入力された）ICMPパケット処理の要求の結果が失敗であった場合、受信したICMP echoパケットを破棄する機能を備えている。

【0036】

受信制御部15は、受信したデータがICMP echoパケットでない場合、受信データの送信元IPアドレスとともに、通信許可端末の確認要求を、通信先管理部11に出力する機能を備えている。また、受信制御部15は、通信先管理部11から通信許可端末の確認処理の結果を受信する（入力される）機能を備えている。

【0037】

受信制御部15は、通信先管理部11から受信した（入力された）通信許可端末の確認処理の結果が許可を示す場合、受信したデータを、入出力手段13を用いて、情報端末2に出力する機能を備えている。受信制御部15は、通信先管理部11から受信した（入力された）確認処理の結果が不許可を示す場合、受信したデータを破棄する機能を備えている。

【0038】

送受信手段16は、ネットワーク4と接続する機能を備えている。送受信手段16は、ネットワーク4と物理的に接続可能な形状で形成されている。送受信手段16は、送信制御部12及び受信制御部15と、遠隔情報端末3との間で、ネットワーク4を介して、データの受け渡し（送受信）を行う機能を備えている。

【0039】

情報端末2は、プログラムに従って動作するパーソナルコンピュータ等の情報処理装置によって実現される。情報端末2は、ネットワークインタフェース装置1などの機能を拡張するための機器を物理的に格納可能なスロットを備えている。図1に示すように、情報端末2は、入出力手段21を含む。

【0040】

入出力手段21は、具体的には、プログラムに従って動作する情報処理装置が備えるCPU及びネットワークインタフェース部によって実現される。入出力手段21は、情報端末2への要求やデータの受け渡し（送受信）を行う機能を備えている。

【0041】

情報端末2は、入出力手段21を用いて、遠隔情報端末3などの他の情報端末への自身の所持するデータの送信を、ネットワークインタフェース装置1に要求する機能を備えている。また、情報端末2は、入出力手段21を用いて、他の情報端末が送信したデータの受信を、ネットワークインタフェース装置1に要求する機能を備えている。

【0042】

遠隔情報端末3は、具体的には、プログラムに従って動作するパーソナルコンピュータ等の情報処理装置によって実現される。遠隔情報端末3は、本実施形態で規定するデータ構造及びデータを含むICMPパケットを生成する機能を備えている。

【0043】

図1に示すように、遠隔情報端末3は、送受信手段31を含む。送受信手段31は、具体的には、プログラムに従って動作する情報処理装置のCPU及びネットワークインタフェース部によって実現される。送受信手段31は、ネットワーク4への接続やネットワーク4を介して外部の情報端末と通信を行う機能を備えている。

【0044】

ネットワーク4は、具体的には、LANやインターネット等の通信ネットワークによって実現される。ネットワーク4は、2つ以上の情報端末同士の通信においてデータの経路

10

20

30

40

50

となる。

【0045】

次に、ネットワークインタフェース装置1の詳細について説明する。図2は、ネットワークインタフェース装置1の構成例を示すブロック図である。

【0046】

図2に示すように、通信管理部11は、タイマ111と、通信許可端末記憶部112を含む。タイマ111は、任意の時刻の設定を可能にする機能を通信管理部11に提供する。タイマ111は、設定された任意の時刻になった、又は任意の時刻が過去になったことを通知する機能を通信管理部11に提供する。

【0047】

通信管理部11は、通信許可端末設定部143から受信した（入力された）IPアドレスを、通信許可端末記憶部112に記憶させる。通信管理部11は、通信許可端末記憶部112にIPアドレスを記憶させる際に、その時点の現在時刻を記憶時間として、IPアドレスと関連付けて記憶させる。

【0048】

通信管理部11は、通信許可端末記憶部112からIPアドレスと関連付けられている記憶時間を読み出す機能を備えている。通信管理部11は、通信許可端末記憶部112が記憶するIPアドレスと関連付けられている記憶時間を削除する機能を備えている。

【0049】

図2に示すように、送信制御部12は、送信先監視部121を含む。送信先監視部121は、送信制御部12が送信しようとするデータの送信先を監視し、送信先を示すIPアドレスを取得する機能を送信制御部12に提供する。

【0050】

図2に示すように、ICMPパケット処理部14は、暗号鍵設定部141と、暗号鍵記憶部142と、通信許可端末設定部143と、コマンド処理部144と、復号化・認証処理部145とを含む。

【0051】

暗号鍵設定部141は、コマンド処理部144から暗号鍵を設定する処理（以下、暗号鍵設定）を要求された場合、その要求の契機となった図3に示す構造を備えたICMP echoパケット5が含む復号化されたコマンドのデータ部分513の符号を、新しい暗号鍵として、暗号鍵記憶部142に設定する（記憶させる）機能を備えている。暗号鍵設定部141は、暗号鍵記憶部142に、それまで記憶していた暗号鍵を破棄させ、新たに暗号鍵を記憶させる機能を備えている。

【0052】

なお、暗号鍵記憶部142は、例えば、最初に通信が行われるときには、前もって定められた暗号鍵を予め記憶している。そして、遠隔情報端末3から初めてパケットを受信した場合には、その予め記憶する暗号鍵を用いて復号化を行い、認証を行う。そして、本実施形態で示すように、その後、遠隔情報端末からの要求に応じて暗号鍵の更新が可能である。

【0053】

通信許可端末設定部143は、コマンド処理部144から通信を許可する端末に設定する処理（以下、通信許可端末設定）を要求された場合、その要求の契機となった図3に示す構造を備えたICMP echoパケット5が含む復号化された送信元のIPアドレスデータ511を通信先管理部11に出力する。

【0054】

コマンド処理部144は、復号化・認証処理部145が認証し得ると判定した、図3に示す構造を備えたICMP echoパケット5が含む復号化されたコマンド512の符号を参照し、符号と対応する処理を実行する機能を備えている。

【0055】

コマンド処理部144は、参照したコマンド512の符号に対応する処理が暗号鍵設定

10

20

30

40

50

であった場合に、コマンド処理部 144 に暗号鍵設定を要求する機能を備えている。コマンド処理部 144 は、参照したコマンド 512 の符号に対応する処理が通信許可端末設定であった場合に、通信許可端末設定部 143 に通信許可端末設定を要求する機能を備えている。

【0056】

復号化・認証処理部 145 は、受信制御部 15 から、ICMP パケット処理の要求とともに、ICMP echo パケット及び同パケットの送信元を示す IP アドレスを受信する（入力される）機能を備えている。復号化・認証処理部 145 は、受信した（入力された）ICMP echo パケットが、図 3 に示す ICMP echo パケット 5 と同じ構造であると仮定し、暗号鍵記憶部 142 が記憶する暗号鍵を用いて、echo データ 51

10

【0057】

復号化・認証処理部 145 は、復号化した echo データ 51 の送信元の IP アドレス 511 が、受信制御部 15 から受信した（入力された）パケットの送信元を示す IP アドレスと一致するか否かを判定する機能を備えている。また、復号化・認証処理部 145 は、判定の結果、一致すれば、認証可能である判定し、一致しなければ、認証不可であると判定する機能を備えている。

【0058】

例えば、echo パケットには、ヘッダ等に含まれる送信元のアドレスとは別に、所定の暗号領域に暗号化された状態でアドレスが含まれる。そして、ヘッダ等に含まれるアドレスと復号したアドレスとが合致するか否かを判定することによって、認証の正否を判定できる。従って、本実施形態では、「認証」とは、パケットに送信元のアドレスが予め定められた方式で暗号化された状態で格納されていることを確認し、予め定められた復号方法で復号化したデータが送信元のアドレスと一致するか否かを確認することである。

20

【0059】

復号化・認証処理部 145 は、ICMP echo パケットが認証可能であった場合、復号化した状態の ICMP echo パケットをコマンド処理部 144 に出力し、受信制御部 15 に ICMP パケット処理成功を通知する機能を備えている。また、復号化・認証処理部 145 は、ICMP echo パケットが認証不可であった場合、受信制御部 15 に ICMP パケット処理に失敗した旨を通知する機能を備えている。

30

【0060】

図 2 に示すように、受信制御部 15 は、ICMP パケット識別部 151 と、送信元監視部 152 とを含む。

【0061】

ICMP パケット識別部 151 は、送受信手段 16 が外部から受信したデータが ICMP echo パケットであるか否かを識別する機能を備えている。

【0062】

送信元監視部 152 は、送受信手段 16 が外部から受信したデータから、その送信元を示す IP アドレスを取得（抽出）する機能を備えている。

【0063】

次に、本実施形態で用いる ICMP パケットのデータ構造について説明する。図 3 は、ICMP パケットのデータ構造の一例を示す説明図である。

40

【0064】

図 3 に示す ICMP echo パケット 5 は、図 1 に示す遠隔情報端末 3 などの情報端末が、ネットワークインタフェース装置 1 と接続される情報端末 2 と通信を行う場合に、遠隔情報端末 3 などの情報端末によって生成され、情報端末 2 に送信される。また、ICMP echo パケット 5 は、遠隔情報端末 3 などの情報端末が、ネットワークインタフェース装置 1 が記憶する暗号鍵を変更する場合に、遠隔情報端末 3 などの情報端末によって生成され、情報端末 2 に送信される。

【0065】

50

なお、ICMP echo パケット 5 は、IETF (Internet Engineering Task Force) が RFC (Request for Comments) 791 で定めるところの IP パケットのデータ部分のみを説明しており、実際には直前に IP ヘッダが付随する。

【0066】

ICMP echo パケット 5 は、IETF が RFC 792 で定めるところの Echo or Echo Reply Message に基づくデータ構造を有し、同仕様中の Data 領域に相当する echo データ 51 の領域を有する。

【0067】

図 3 に示すように、echo データ 51 の領域は、送信元の IP アドレス 511 の領域と、コマンド 512 の領域と、コマンドのデータ部分 513 の領域とを含む。 10

【0068】

echo データ 51 の領域は、図 1 に示す遠隔情報端末 3 などの情報端末によって、ICMP echo パケット 5 に格納される直前に暗号化される。具体的には、echo データ 51 の領域は、遠隔情報端末 3 などの情報端末が通信を希望する情報端末 2 と接続されるネットワークインタフェース装置 1 が記憶する暗号鍵と同一の暗号鍵によって、暗号化される。

【0069】

送信元の IP アドレス 511 は、図 1 に示す遠隔情報端末 3 などの情報端末が echo データ 51 を生成する際に、同情報端末によって、同情報端末が保持する IP アドレスデータと等しい符号を設定される。 20

【0070】

コマンド 512 は、図 1 に示す遠隔情報端末 3 などの情報端末が、ネットワークインタフェース装置 1 と接続される情報端末 2 と通信を行う場合に、遠隔情報端末 3 などの情報端末が echo データ 51 を生成する際に、ネットワークインタフェース装置 1 に対して通信許可端末設定を要求する符号を設定される。

【0071】

コマンド 512 は、図 1 に示す遠隔情報端末 3 などの情報端末が、ネットワークインタフェース装置 1 が記憶する暗号鍵を変更する場合に、遠隔情報端末 3 などの情報端末が echo データ 51 を生成する際に、ネットワークインタフェース装置 1 に対して暗号鍵設定を要求する符号を設定される。 30

【0072】

コマンドのデータ部分 513 は、図 1 に示す遠隔情報端末 3 などの情報端末が、ネットワークインタフェース装置 1 と接続される情報端末 2 と通信を行う場合には、何も設定されない。

【0073】

コマンドのデータ部分 513 は、図 1 に示す遠隔情報端末 3 などの情報端末が、ネットワークインタフェース装置 1 が記憶する暗号鍵を変更する場合に、遠隔情報端末 3 などの情報端末が echo データ 51 を生成する際に、設定する新しい暗号鍵のデータが設定される。 40

【0074】

次に、ネットワークインタフェース装置 1 が、ネットワーク 4 を介して、遠隔情報端末 3 からデータを受信した際の動作について説明する。図 4～6 は、ネットワークインタフェース装置 1 が、ネットワーク 4 を介して、遠隔情報端末 3 からデータを受信した際の動作の一例を示す流れ図である。

【0075】

ネットワークインタフェース装置 1 が起動されると、受信制御部 15 は、起動直後より、送受信手段 16 に接続されているネットワーク 4 を介して、外部から送信されるデータを待ち受ける (図 4 のステップ S101)。

【0076】

遠隔情報端末 3 から情報端末 2 にデータを送信するために、ユーザは、遠隔情報端末 3 を用いて、データを送信する操作を行う。すると、送受信手段 3 1 は、ユーザの操作に従って、ネットワーク 4 を介して、ネットワークインタフェース装置 1 にデータを送信する。

【0077】

受信制御部 1 5 は、ネットワーク 4 を介して、遠隔情報端末 3 からデータを受信すると、受信制御部 1 5 が備える送信元監視部 1 5 2 を用いて、遠隔情報端末 3 が保持する I P アドレスを取得する（図 4 のステップ S 1 0 2）。

【0078】

次いで、受信制御部 1 5 は、通信先管理部 1 1 に、取得した I P アドレスとともに、遠隔情報端末 3 が通信を許可する端末であるか否かを確認する要求を出力する。すると、通信先管理部 1 1 は、通信許可端末記憶部 1 1 2 を参照して、受信制御部 1 5 から受信した（入力された）I P アドレスが記憶されているか否かを判定する。

【0079】

そして、記憶されていると判定すると、通信先管理部 1 1 は、受信制御部 1 5 に許可を示す「Y e s」を出力する。一方、ステップ S 1 0 3 において、記憶されていないと判定すると、通信先管理部 1 1 は、受信制御部 1 5 に不許可を示す「N o」を出力する。（図 4 のステップ S 1 0 3）。

【0080】

受信制御部 1 5 は、通信先管理部 1 1 から「Y e s」を受信する（入力される）と、入出力手段 1 3 を用いて、ネットワークインタフェース装置 1 と接続されている情報端末 2 に、受信データを出力する（図 4 のステップ S 1 0 4）。その後、受信制御部 1 5 は、処理をステップ S 1 0 1 に移行する。

【0081】

受信制御部 1 5 は、通信先管理部 1 1 から「N o」を受信する（入力される）と、I C M P パケット識別部 1 5 1 を用いて、受信したデータが I C M P e c h o パケットであるか否かを判定する（図 5 のステップ S 1 0 5）。

【0082】

ステップ S 1 0 5 において、I C M P e c h o パケットであると判定すると、受信制御部 1 5 は、受信した I C M P e c h o パケットとパケットの送信元の I P アドレスとを I C M P パケット処理部 1 4 に出力する。

【0083】

すると、I C M P パケット処理部 1 4 は、復号化・認証処理部 1 4 5 に、受信した I C M P パケットの認証処理を実行するよう要求する。すると、復号化・認証処理部 1 4 5 は、暗号鍵記憶部 1 4 2 から暗号鍵を取得（抽出）し、取得（抽出）した暗号鍵を用いて、I C M P パケットの e c h o データ領域 5 1 を復号化する処理を実行する（図 5 のステップ S 1 0 7）。

【0084】

次いで、復号化・認証処理部 1 4 5 は、復号化した I C M P パケットの e c h o データ領域 5 1 が含む送信元の I P アドレス格納領域 5 1 1 に、パケットの送信元の I P アドレスが含まれているか否かを判定する。

【0085】

そして、含まれていると判定すると、復号化・認証処理部 1 4 5 は、認証が成功したと判定し、I C M P パケット処理部 1 4 に、認証処理が成功した旨を通知する。一方、含まれていないと判定すると、復号化・認証処理部 1 4 5 は、認証が失敗したと判定し、I C M P パケット処理部 1 4 に、認証処理が失敗した旨を通知する。そして、I C M P パケット処理部 1 4 は、処理が失敗した旨を受信制御部 1 5 に通知する（図 5 のステップ S 1 0 8）。

【0086】

受信制御部 1 5 は、ステップ S 1 0 5 において、受信データが I C M P e c h o パケ

10

20

30

40

50

ットでないと判定した場合、又はステップ S 1 0 8 において、認証処理が失敗した場合には、遠隔情報端末 3 から受信したデータを破棄する（図 5 のステップ S 1 0 6）。その後、受信制御部 1 5 は、処理をステップ S 1 0 1 に移行する。

【0087】

I C M P パケット処理部 1 4 は、認証処理が成功すると、コマンド処理部 1 4 4 を用いて、復号化した I C M P パケットのコマンド処理を行う。具体的には、コマンド処理部 1 4 4 は、I C M P パケットの e c h o データ 5 1 が含むコマンド格納領域 5 1 2 を読み出す。そして、コマンド処理部 1 4 4 は、コマンド格納領域 5 1 2 に暗号鍵変更を要求するコマンドが格納されているか否かを判定する（図 5 のステップ S 1 0 9）。

【0088】

ステップ S 1 0 9 において、格納されていると判定すると、コマンド処理部 1 4 4 は、I C M P パケットの e c h o データ 5 1 が含むコマンドのデータ部分の格納領域から読み出しを行い、暗号鍵データとして取得する（図 5 のステップ S 1 1 0）。

【0089】

次いで、コマンド処理部 1 4 4 は、取得した暗号鍵データを暗号鍵設定部 1 4 1 に出力する。すると、暗号鍵設定部 1 4 1 は、暗号鍵記憶部 1 4 2 がそれまで記憶していた暗号鍵を破棄（消去）し、受信した（入力された）暗号鍵データを暗号鍵記憶部 1 4 2 に記憶させることで、暗号鍵を更新する（図 5 のステップ S 1 1 1）。

【0090】

コマンド処理部 1 4 4 は、ステップ S 1 1 1 において、暗号鍵データの更新が完了した後、又はステップ S 1 0 9 において、格納されていないと判定する場合に、通信先管理部 1 1 に I C M P パケットの送信元 I P アドレスを出力する。また、コマンド処理部 1 4 4 は、出力した I P アドレスを記憶するように、通信先管理部 1 1 に要求を出力する。すると、通信先管理部 1 1 は、通信許可端末記憶部 1 1 2 を参照して、コマンド処理部 1 4 4 から受信した（入力された）I P アドレスが記憶されているか否かを判定する（図 6 のステップ S 1 1 2）。

【0091】

ステップ S 1 1 2 において、記憶されていると判定する場合には、通信先管理部 1 1 は、通信許可端末記憶部 1 1 2 が記憶する I P アドレスと、I P アドレスに関連付けられている記憶時間とを削除（消去）する（図 6 のステップ S 1 1 3）。

【0092】

ステップ S 1 1 3 において、記憶されている I P アドレスを削除した後、又はステップ S 1 1 2 において、記憶されていないと判定する場合には、通信先管理部 1 1 は、コマンド処理部 1 4 4 から受信した（入力された）I P アドレスを通信許可端末記憶部 1 1 2 に記憶させる。また、通信先管理部 1 1 は、現在時刻（上記の処理を実行した時刻）を記憶時刻として、I P アドレスと関連付けて通信許可端末記憶部 1 1 2 に記憶させる。その後、通信先管理部 1 1 は、コマンド処理部 1 4 4 に処理完了を通知する（図 6 のステップ S 1 1 4）。

【0093】

ステップ S 1 1 4 において、通信先管理部 1 1 による I P アドレスの記憶処理が完了すると、受信制御部 1 5 は、入出力手段 1 3 を用いて、ネットワークインタフェース装置 1 が接続されている情報端末 2 に、遠隔情報端末 3 から受信したデータである I C M P e c h o パケットを送信する（図 6 のステップ S 1 1 5）。その後、受信制御部 1 5 は、処理をステップ S 1 0 1 に移行する。

【0094】

次に、ネットワークインタフェース装置 1 と接続された情報端末 2 からデータ送信を要求された際の動作について説明する。図 7 は、情報端末 2 からデータ送信をする際の動作の一例を示す流れ図である。

【0095】

ネットワークインタフェース装置 1 が起動されると、送信制御部 1 2 は、起動直後より

10

20

30

40

50

、入出力手段 13 と接続されている情報端末 2 からのデータ送信要求を待ち受ける（図 7 のステップ S 201）。

【0096】

情報端末 2 から遠隔情報端末 3 にデータを送信するために、ユーザは、情報端末 2 を用いて、データを送信する操作を行う。すると、入出力手段 21 は、ユーザの操作に従って、ネットワークインタフェース装置 1 にデータの送信要求とともに、データの送信先を示す情報と送信データとを送信する。

【0097】

すると、送信制御部 12 は、情報端末 2 から、データの送信要求とともに、データの送信先を示す情報と送信データとを受信する（図 7 のステップ S 202）。

10

【0098】

次いで、送信制御部 12 は、通信先管理部 11 に、情報端末 2 から受信したデータの送信先を示す情報である IP アドレスを出力する。また、送信制御部 12 は、通信先管理部 11 に、出力した IP アドレスを保持する遠隔情報端末が通信を許可する端末であるか否かを確認する要求を出力する。

【0099】

すると、通信先管理部 11 は、通信許可端末記憶部 112 を参照して、送信制御部 12 から受信した（入力された）IP アドレスが記憶されているか否かを判定する。そして、記憶されていると判定する場合には、通信先管理部 11 は、送信制御部 12 に許可を示す「Yes」を出力する。一方、記憶されていないと判定する場合には、通信先管理部 11 は、送信制御部 12 に不許可を示す「No」を出力する。（図 7 のステップ S 204）。

20

【0100】

送信制御部 12 は、通信先管理部 11 から「Yes」を受信する（入力される）と、送受信手段 16 を用いて、ネットワーク 4 を介して、データの送信先（すなわち遠隔情報端末 3）に送信データを送信する（図 7 のステップ S 205）。その後、送信制御部 12 は、処理をステップ S 201 に移行する。

【0101】

一方、送信制御部 12 は、通信先管理部 11 から「No」を受信する（入力される）と、情報端末 2 に送信エラーである旨の通知を行う。そして、送信制御部 12 は、情報端末 2 から受信した送信データを破棄する（図 7 のステップ S 203）。その後、送信制御部 12 は、処理をステップ S 201 に移行する。

30

【0102】

次に、ネットワークインタフェース装置 1 が記憶する通信許可端末を示す情報の管理動作について説明する。図 8 は、通信許可端末を示す情報の管理動作の一例を示す流れ図である。

【0103】

ネットワークインタフェース装置 1 が起動されると、通信先管理部 11 は、起動直後に通信許可端末記憶部 112 内の通信許可端末一覧に、1 つ以上の情報が存在するか否かを判定する（図 8 のステップ S 301）。

【0104】

ステップ S 301 において、情報が存在しないと判定した場合、通信先管理部 11 は、再度、通信許可端末一覧に 1 つ以上の情報が存在するか否かを確認し、情報が入力されることを待ち受ける（図 8 のステップ S 301）。

40

【0105】

ステップ S 301 において、情報が存在すると判定した場合、通信先管理部 11 は、記憶している通信許可端末一覧の IP アドレスに関連付けられている記憶時刻から、最も古い時刻を取得（抽出）する（図 8 のステップ S 302）。

【0106】

次いで、通信先管理部 11 は、取得（抽出）した記憶時刻に所定の許可期間（通信を許可する期間を意味する）を加えた時刻を、タイマ 111 に設定する（図 8 のステップ S 3

50

03)。

【0107】

次いで、タイマ111は、設定された時刻になるまで待機する。そして、設定された時刻になったことを検知すると、タイマ111は、通信先管理部11にその旨を通知する（図8のステップS304）。

【0108】

次いで、通信先管理部11は、タイマ111から設定された時刻になった旨の通知を受信する（入力される）と、タイマ111に設定された時刻から所定の許可期間を差し引き、元の記憶時刻を取得（算出）する（図8のステップS305）。

【0109】

次いで、通信先管理部11は、取得（算出）した元の記憶時刻が、通信許可端末記憶部112内の通信許可端末一覧のIPアドレスに関連付けられた記憶時刻と一致するか否かを判定する（図8のステップS306）。

【0110】

ステップS306において、一致すると判定した場合、通信先管理部11は、一致した記憶時刻と記憶時刻が関連付けられているIPアドレスとの組情報を、通信許可端末一覧から削除する（図8のステップS307）。その後、通信先管理部11は、処理をステップS301に移行する。

【0111】

ステップS306において、一致しないと判定した場合、通信先管理部11は、処理をステップS301に移行する。

【0112】

以上のように、本実施形態では、ICMP echoパケットであるか否かを判定する処理を含んでおり、ICMP echoパケットのみを対象として処理を行う。また、特許文献2に記載されたシステムでは、事前に識別情報の生成と発行とを行う必要があるのに対して、本実施形態では、復号化したデータが送信元のIPアドレスと一致することを条件に通信の制御を行っているため、事前に識別情報の生成等を行う必要がない。そのため、処理に必要な手数を少なくすることができる。

【0113】

また、本実施形態では、ネットワークインタフェース装置1は、ICMP echoパケットによる事前の通信許可要求がない通信を通過させないため、不正アクセスを最初から排除することができる。また、本実施形態では、通信を許可する期間を定めているため、通信を許可した端末のIPアドレスを偽装された場合であっても、許可期間が過ぎた時点で排除することができる。

【0114】

本発明の前提である一般的な情報通信制御方法では、以下の課題を有する。

【0115】

第1に、情報端末や、情報端末上で動作するプログラム、情報端末に至る通信経路上の通信装置との通信を許可する端末を、IPアドレスなどの個体識別子によって判別する方法では、あらかじめ複数の個体識別子を記憶させておかなければならない。

【0116】

第2に、情報端末上で動作するプログラムによって認証処理を行う方法では、不特定の端末から多数の不正な通信があった場合に、多数の認証処理により情報端末の負荷が上昇する。また、情報端末上で動作するオペレーティングシステムの種別毎に対応するプログラムが必要となる。

【0117】

第3に、特定の通信プロトコルによる通信のみを許可する方法では、特定の通信プロトコル以外のプロトコルを使用することができない制約が存在する。また、プロトコルの特殊性から、不正アクセスをする者に解析の手がかりを与えやすくなる。

【0118】

10

20

30

40

50

第４に、不正なＩＣＭＰネットワークパケットを受信しないために、全てのＩＣＭＰネットワークパケットを受信しない方法では、正規のＩＣＭＰネットワークパケットも受信できない制約がある。

【０１１９】

以上の課題に対して、本実施形態によれば、以下のような課題解決手段を備えている。

【０１２０】

第１の課題に対して、図１に示す正規の通信を行う遠隔情報端末３と情報端末２とにおいて、遠隔情報端末３は、通信時に本実施形態で規定する暗号化を行った通信許可要求を情報端末２に送信する。すると、情報端末２と接続されたネットワークインタフェース装置１は、受信した通信許可要求が正しく暗号化されているかをＩＣＭＰパケット処理部１４を用いて判断する。そして、要求が正当なものである場合、ＩＣＭＰパケット処理部１４は、要求を送信した端末のＩＰアドレスを、通信先管理部１１に通信を許可する端末のＩＰアドレスとして記憶させる。従って、予め複数の個別識別子を記憶させておかなくてもよい。

10

【０１２１】

第２の課題に対して、図１に示す情報端末２に接続されたネットワークインタフェース装置１は、通信先管理部１１に記憶されていないＩＰアドレスを持つ端末からの通信データを、入出力手段１３から情報端末２に送信しない。従って、不正な通信パケットをネットワークインタフェース装置１で排除することができ、情報端末２の負荷を低減することができる。また、情報端末２のオペレーティングシステムの種別に関わらず、処理を実行することができる。

20

【０１２２】

第３の課題に対して、図１に示す情報端末２に接続されたネットワークインタフェース装置１は、通信先管理部１１が、通信を許可された端末のＩＰアドレスを記憶した時から所定の時間が経過するまでの間、送受信手段１６が受信したＩＰアドレスからの全てのパケットを、入出力手段１３を用いて情報端末２に送信するように制御する。従って、特定の通信プロトコルによる通信に制限することなく、通信制御処理を実行することができる。また、世間一般にありふれたＩＣＭＰパケットを使用し、さらに、データ形式が任意領域であるｅｃｈｏデータ領域を使用することで、一般的なＩＣＭＰパケットであるか、もしくは本実施形態で使用する通信の許可を目的としたＩＣＭＰパケットであるかの区別を難しくすることができる。

30

【０１２３】

第４の課題に対して、図１に示す情報端末２に接続されたネットワークインタフェース装置１は、送受信手段１６が受信したデータが受信制御部１５を用いて、ＩＣＭＰネットワークパケットであるか否かを判定する。また、ネットワークインタフェース装置１は、ＩＣＭＰパケット処理部１４を用いて、パケットが通信を許可する条件を満たすか否かを判定する。そして、ＩＣＭＰネットワークパケットであり、かつ、通信を許可する条件を満たすと判定する場合に、ネットワークインタフェース装置１は、パケットをそのまま入出力手段１３を用いて情報端末２に送信するように制御する。従って、正規であるか不正なＩＣＭＰネットワークパケットを排除するために、ＩＣＭＰネットワークパケットを制限することなく、情報通信をすることができる。

40

【０１２４】

また、本実施形態によれば、以下のような効果を奏する。

【０１２５】

第１の効果は、ＩＣＭＰ　ｅｃｈｏパケットを識別・処理する機能を備えているため、ＩＣＭＰ　ｅｃｈｏパケットを用いて、ネットワークインタフェース装置１の動作を制御することができることである。

【０１２６】

第２の効果は、ＩＣＭＰ　ｅｃｈｏパケットのデータ部を暗号化する機能を備えているため、ＩＣＭＰ　ｅｃｈｏパケットのデータ部の盗聴を防止することができることである

50

。

【0127】

第3の効果は、ICMP echoパケットにより暗号鍵を変更する機能を備えているため、遠隔情報端末から暗号鍵を変更することができることである。

【0128】

第4の効果は、通信許可端末のIPアドレスを記憶する機能と、IPアドレスによって通信の許可の制御を行う機能とを備えているため、プロトコルによらずに通信相手側の端末を制限することができることである。

【0129】

第5の効果は、通信許可端末のIPアドレスを記憶した時刻を管理する機能を備えているため、通信許可時間を所定期間に制限することができることである。

【0130】

以上より、本発明は、以下の特徴を有しているといえる。

【0131】

本発明の第1の特徴として、情報端末と接続されるネットワークインタフェース装置は、本発明で規定したICMPパケットを送信する端末とのみ通信を許可する。これにより、その他の不特定の端末への情報端末の情報漏洩や、不正な通信による負荷上昇の防止を可能としている。

【0132】

本発明の第2の特徴として、通信許可を所定期間としているため、通信の維持にはICMPパケットを定期的を送信する必要がある。これにより、通信を要求する端末が通信要求とICMPによる通信経路の死活確認とを同時に実行することを可能としている。

【0133】

本発明の第3の特徴として、ICMPパケットでデータ形式が任意領域であるechoデータ領域を暗号化している。このことにより、対応する暗号／復号鍵を持つ端末以外の端末が本発明で使用するパケットの区別や内容を参照することを難しくしている。

【0134】

次に、本発明による情報通信制御装置の最小構成について説明する。図9は、情報通信制御装置の最小の構成例を示すブロック図である。図9に示すように、情報通信制御装置100は、最小の構成要素として、IPアドレス記憶手段101と、通信許可端末管理手段102と、パケット復号化手段103と、IPアドレス判定手段104と、IPアドレス管理手段105とを含む。

【0135】

図9に示す最小構成の情報通信制御装置では、通信許可端末管理手段102は、送信元端末から送信先端末にパケットが送信された際に、送信元端末のIPアドレスが、IPアドレス記憶手段101が記憶するIPアドレスに合致するか否かを判定する。そして、パケット復号化手段103は、通信許可端末管理手段102が合致しないと判定すると、パケットが復号可能か否かを判定し、復号可能であればパケットを復号化する。そして、IPアドレス判定手段104は、パケット復号化手段103が復号化したパケットが含む送信元のIPアドレスが、送信元端末のIPアドレスと合致するか否かを判定する。そして、IPアドレス管理手段105は、IPアドレス判定手段104が合致すると判定すると、送信元端末のIPアドレスをIPアドレス記憶手段101に記憶させる。

【0136】

従って、図9に示す最小構成の情報通信制御装置100によれば、事前に識別情報の生成等を行う必要がなく、処理に必要な手数を少なくすることができる。

【0137】

なお、本実施形態では、以下の(1)～(5)に示すような情報通信制御装置の特徴的構成が示されている。

【0138】

(1) 情報通信制御装置（例えば、ネットワークインタフェース装置1によって実現さ

10

20

30

40

50

れる)は、送信先端末(例えば、情報端末2)との通信を許可する送信元端末(例えば、遠隔情報端末3)のアドレスを記憶するアドレス記憶手段(例えば、通信許可端末記憶部112によって実現される)と、送信元端末から送信先端末にパケットが送信された際に、送信元端末のアドレスが、アドレス記憶手段が記憶するアドレスに合致するか否かを判定し、合致すると判定すると送信先端末との通信を許可する通信許可端末管理手段(例えば、通信先管理部11によって実現される)と、通信許可端末管理手段が合致しないと判定すると、パケットが復号可能か否かを判定し、復号可能であれば予め定められた復号化方法を用いてパケットに含まれる所定の暗号化領域のデータを復号化するパケット復号化手段(例えば、復号化・認証処理部145によって実現される)と、パケット復号化手段が復号化したデータ(例えば、送信元のIPアドレス511)が、送信元端末のアドレスと合致するか否かを判定するアドレス判定手段(例えば、復号化・認証処理部145によって実現される)と、アドレス判定手段が合致すると判定すると、認証に成功したと判定し、復号化したデータによってアドレス記憶手段が記憶するアドレスを更新するアドレス管理手段(例えば、通信先管理部11によって実現される)とを備えたことを特徴とする。

10

【0139】

(2)情報通信制御装置において、アドレス管理手段は、アドレス記憶手段に記憶させたアドレスを、記憶させた時点から所定期間経過すると、アドレス記憶手段から消去するように構成されていてもよい。

【0140】

(3)情報通信制御装置は、パケット復号化手段によってパケットが復号可能であると判定されると、パケットを送信先端末に送信する送信手段(例えば、受信制御部15及び入出力手段13によって実現される)と、パケット復号化手段によってパケットが復号不可能であると判定されると、パケットを破棄するパケット破棄手段(例えば、受信制御部15によって実現される)とを備えたことを特徴とする。

20

【0141】

(4)情報通信制御装置において、通信許可端末管理手段が合致しないと判定すると、パケットがICMP echoパケットであるか否かを判定するICMP echoパケット判定手段(例えば、ICMPパケット識別部151によって実現される)を備え、パケット復号化手段は、ICMP echoパケット判定手段がICMP echoパケットであると判定すると、パケットが復号可能か否かを判定し、復号可能であればパケットを復号化するように構成されていてもよい。

30

【0142】

(5)情報通信制御装置は、パケット復号化手段が復号化したパケットが、パケットの暗号化及び復号化に用いる暗号鍵を更新する要求(例えば、コマンド512)とともに、新たな暗号鍵(例えば、コマンドのデータ部分513)を含む場合に、当該情報通信制御装置が備える暗号鍵記憶部(例えば、暗号鍵記憶部142によって実現される)が記憶する暗号鍵を新たな暗号鍵で更新する暗号鍵更新手段(例えば、暗号鍵設定部141によって実現される)を備えたことを特徴とする。

【産業上の利用可能性】

40

【0143】

本発明は、端末間での情報通信を制御する用途に適用可能である。

【符号の説明】

【0144】

- 1 ネットワークインタフェース装置
- 2 情報端末
- 3 遠隔情報端末
- 4 ネットワーク
- 11 通信先管理部
- 12 送信制御部

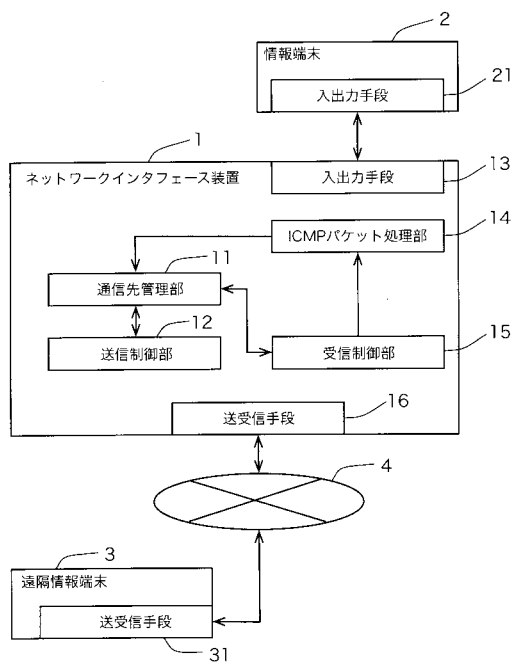
50

- 13, 21 入出力手段
- 14 ICMPパケット処理部
- 15 受信制御部
- 16, 31 送受信手段
- 100 情報通信制御装置
- 101 アドレス記憶手段
- 102 通信許可端末管理手段
- 103 パケット復号化手段
- 104 アドレス判定手段
- 105 アドレス管理手段
- 111 タイマ
- 112 通信許可端末記憶部
- 121 送信先監視部
- 141 暗号鍵設定部
- 142 暗号鍵記憶部
- 143 通信許可端末設定部
- 144 コマンド処理部
- 145 復号化・認証処理部
- 151 ICMPパケット認識部
- 152 送信元監視部

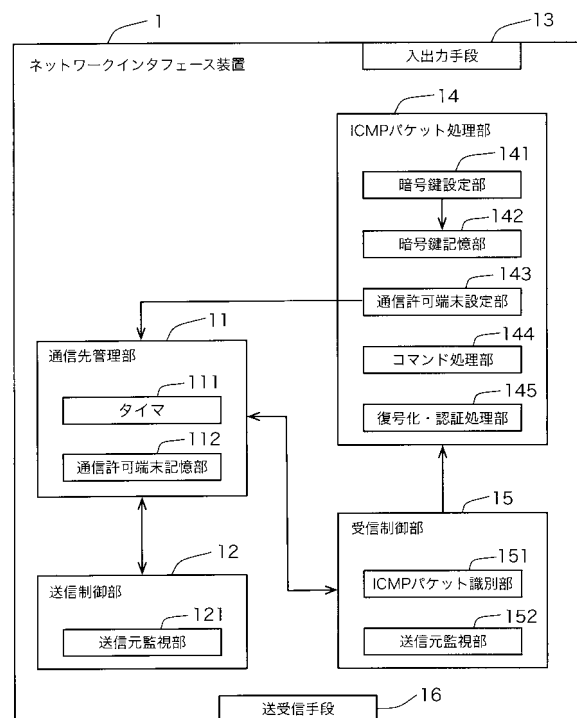
10

20

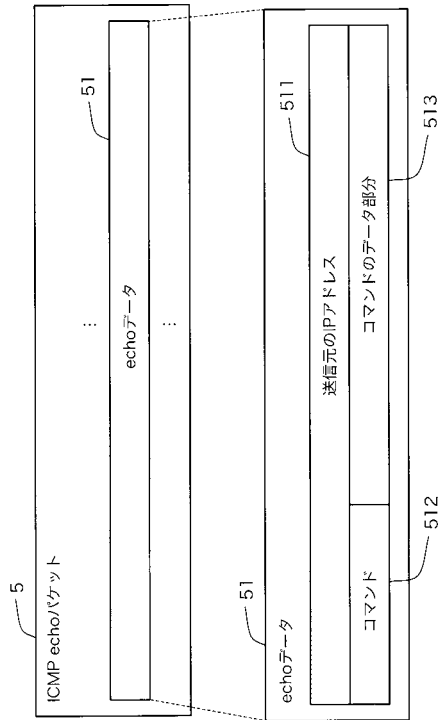
【図 1】



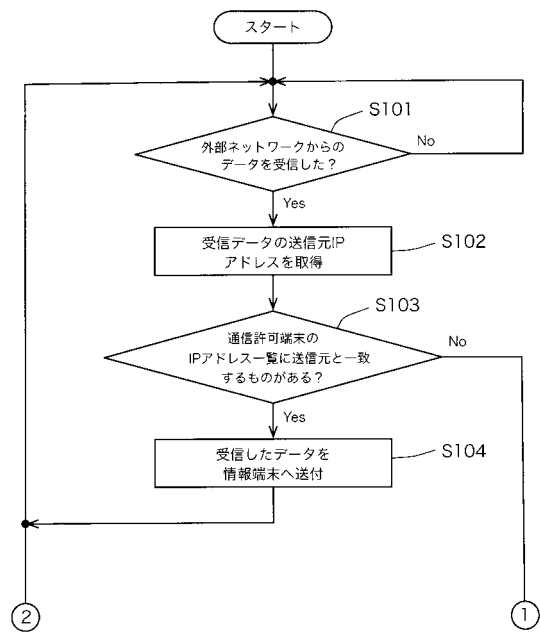
【図 2】



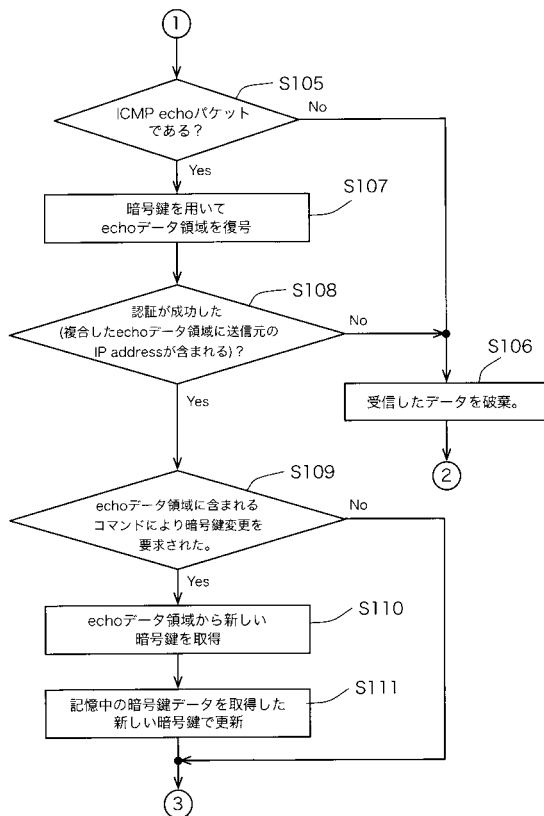
【図 3】



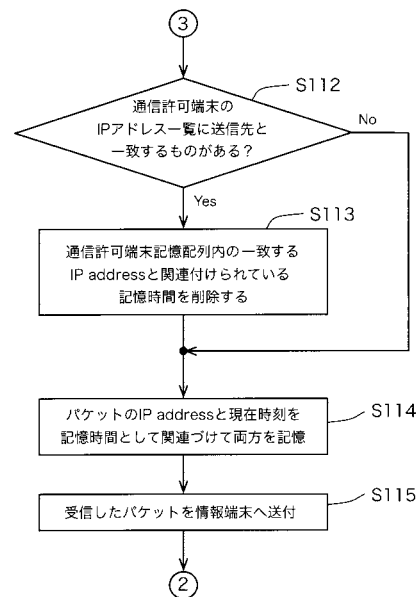
【図 4】



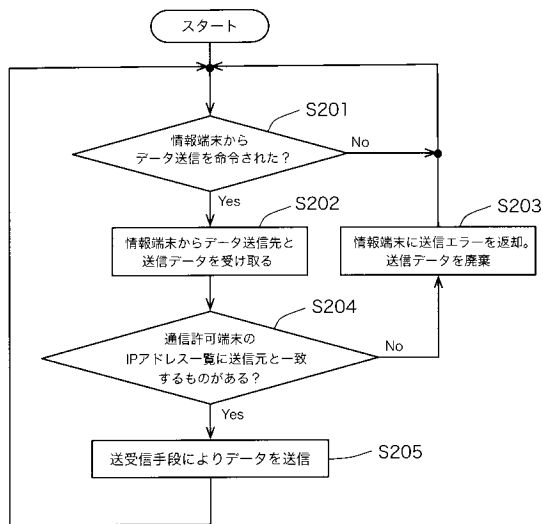
【図 5】



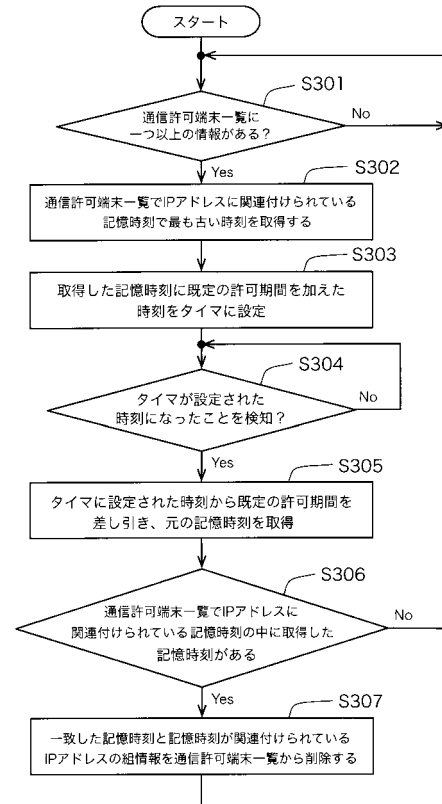
【図 6】



【図 7】



【図 8】



【図 9】

