

(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2012-178169

(P2012-178169A)

(43) 公開日 平成24年9月13日(2012.9.13)

(51) Int.Cl.		F I		テーマコード (参考)
G06F 21/20	(2006.01)	G06F 21/20	1 4 4 C	5 J 1 0 4
G06F 21/24	(2006.01)	G06F 21/24	1 6 3 G	
H04L 9/32	(2006.01)	H04L 9/00	6 7 3 D	

審査請求 有 請求項の数 12 O L (全 28 頁)

(21) 出願番号	特願2012-102371 (P2012-102371)	(71) 出願人	000002185
(22) 出願日	平成24年4月27日 (2012. 4. 27)		ソニー株式会社
(62) 分割の表示	特願2010-248717 (P2010-248717) の分割	(74) 代理人	100082131
原出願日	平成16年6月24日 (2004. 6. 24)		弁理士 稲本 義雄
(31) 優先権主張番号	特願2003-281348 (P2003-281348)	(74) 代理人	100121131
(32) 優先日	平成15年7月28日 (2003. 7. 28)		弁理士 西川 孝
(33) 優先権主張国	日本国 (JP)	(72) 発明者	中野 雄彦
			東京都港区港南1丁目7番1号 ソニー株 式会社内
		(72) 発明者	嶋 久登
			東京都港区港南1丁目7番1号 ソニー株 式会社内
		Fターム(参考)	5J104 AA07 AA16 AA32 DA03 EA08 GA03 KA02 KA20 NA38 PA07

(54) 【発明の名称】 情報処理装置、情報処理方法、およびプログラム

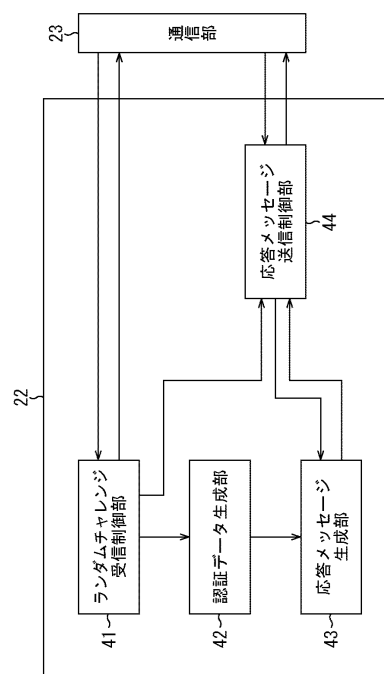
(57) 【要約】

【課題】 所定のコマンドに対する受信機器の応答時間に
基づいて通信距離を判別する。

【解決手段】 ランダムチャレンジ受信制御部は、送信側
の端末からのランダムチャレンジ (RC) を受信し、認証
データ生成部に供給する。ランダムチャレンジ受信制御
部はRCを受信した旨を表すRC受信メッセージを送信側に
送信する。認証データ生成部は、RCに対してハッシュ処
理を施し、その結果得られた認証データを応答メッセー
ジ生成部に供給する。応答メッセージ送信制御部は、送
信側からの応答要求コマンドを受信する前のタイミング
で、応答メッセージ生成部を制御して、認証データを含
む応答メッセージを生成させるとともに、応答要求コマ
ンドを受信したとき、その応答メッセージを送信先の端
末に送信する。本開示は、例えばコンテンツ提供システ
ムに適用できる。

【選択図】 図4

図4



【特許請求の範囲】

【請求項 1】

応答を要求するコマンドを受信装置に送信するコマンド送信部と、

前記受信装置との間で共有する共有データに基づいて、期待値を生成する期待値生成部と、

前記共有データに基づいて生成された認証データを含んだ応答メッセージを前記受信装置から受信する受信部と、

前記期待値生成部により生成された前記期待値と受信部により受信された前記認証データに基づいて、前記受信装置を認証する認証部と、

前記受信装置に対して前記応答を要求するコマンドが送信されたときから、前記受信装置からの応答メッセージが受信されるまでの間の応答時間を計測する計測部と、 10

前記認証部による認証結果、および前記計測部により計測された前記応答時間に基づいて、前記受信装置に対するデータの送信可否を判定する判定部と

を備える情報処理装置。

【請求項 2】

応答を要求するコマンドを受信装置に送信するコマンド送信ステップと、

前記受信装置との間で共有する共有データに基づいて、期待値を生成する期待値生成ステップと、

前記共有データに基づいて生成された認証データを含んだ応答メッセージを前記受信装置から受信する受信ステップと、 20

前記期待値生成ステップの処理で生成された前記期待値と受信ステップの処理で受信された前記認証データに基づいて、前記受信装置を認証する認証ステップと、

前記受信装置に対して前記応答を要求するコマンドが送信されたときから、前記受信装置からの応答メッセージが受信されるまでの間の応答時間を計測する計測ステップと、

前記認証ステップでの認証結果、および前記計測ステップの処理で計測された前記応答時間に基づいて、前記受信装置に対するデータの送信可否を判定する判定ステップと

を含む情報処理方法。

【請求項 3】

応答を要求するコマンドを受信装置に送信するコマンド送信ステップと、

前記受信装置との間で共有する共有データに基づいて、期待値を生成する期待値生成ステップと、 30

前記共有データに基づいて生成された認証データを含んだ応答メッセージを前記受信装置から受信する受信ステップと、

前記期待値生成ステップの処理で生成された前記期待値と受信ステップの処理で受信された前記認証データに基づいて、前記受信装置を認証する認証ステップと、

前記受信装置に対して前記応答を要求するコマンドが送信されたときから、前記受信装置からの応答メッセージが受信されるまでの間の応答時間を計測する計測ステップと、

前記認証ステップでの認証結果、および前記計測ステップの処理で計測された前記応答時間に基づいて、前記受信装置に対するデータの送信可否を判定する判定ステップと

を含む処理をコンピュータに実行させるプログラム。 40

【請求項 4】

送信装置と共有する共有データから生成された認証データに基づく認証結果、および前記送信装置からの所定のコマンドに対する応答時間に基づいてデータの送信可否を判定する前記送信装置と通信可能な情報処理装置において、

前記送信装置から前記コマンドを受信する受信部と、

前記共有データに対して所定の処理を施して、前記認証データを生成する認証データ生成部と、

前記認証データ生成部により生成された前記認証データを含む、前記コマンドに対する応答メッセージを生成する応答メッセージ生成部と、

前記送信装置から送信されてきた前記コマンドが受信されたとき、前記応答メッセージ 50

を前記送信装置に送信する送信部と
を備える情報処理装置。

【請求項 5】

送信装置と共有する共有データから生成された認証データに基づく認証結果、および前記送信装置からの所定のコマンドに対する応答時間に基づいてデータの送信可否を判定する前記送信装置と通信可能な情報処理装置の情報処理方法において、

前記送信装置から前記コマンドを受信する受信ステップと、

前記共有データに対して所定の処理を施して、前記認証データを生成する認証データ生成ステップと、

前記認証データ生成ステップの処理で生成された前記認証データを含む、前記コマンドに対する応答メッセージを生成する応答メッセージ生成ステップと、

前記送信装置から送信されてきた前記コマンドが受信されたとき、前記応答メッセージを前記送信装置に送信する送信ステップと

を含む情報処理方法。

【請求項 6】

送信装置と共有する共有データから生成された認証データに基づく認証結果、および前記送信装置からの所定のコマンドに対する応答時間に基づいてデータの送信可否を判定する前記送信装置と通信可能な情報処理装置の情報処理用のプログラムであって、

前記送信装置から前記コマンドを受信する受信ステップと、

前記共有データに対して所定の処理を施して、前記認証データを生成する認証データ生成ステップと、

前記認証データ生成ステップの処理で生成された前記認証データを含む、前記コマンドに対する応答メッセージを生成する応答メッセージ生成ステップと、

前記送信装置から送信されてきた前記コマンドが受信されたとき、前記応答メッセージを前記送信装置に送信する送信ステップと

を含む処理をコンピュータに実行させるプログラム。

【請求項 7】

受信装置との間で共有するデータをもとに、コマンド認証データと、応答期待値データを生成する認証データ生成部と、

前記コマンド認証データを含み、応答を要求するコマンドを前記受信装置に送信するコマンド送信部と、

前記コマンドに対する受信装置からの応答を受信する応答受信部と、

前記応答期待値と、前記受信装置から受信した前記応答に含まれる応答認証データに基づいて前記受信装置を認証する認証部と、

前記受信装置に対して前記応答を要求するコマンドが送信されたときから、前記受信装置からの応答が受信されるまでの間の応答時間を計測する計測部と、

前記認証部による認証結果、および前記計測部により計測された応答時間に基づいて、前記受信装置に対するデータの送信可否を判定する判定部と

を備える情報処理装置。

【請求項 8】

受信装置との間で共有するデータをもとに、コマンド認証データと、応答期待値データを生成する認証データ生成ステップと、

前記コマンド認証データを含み、応答を要求するコマンドを前記受信装置に送信するコマンド送信ステップと、

前記コマンドに対する受信装置からの応答を受信する応答受信ステップと、

前記応答期待値と、前記受信装置から受信した前記応答に含まれる応答認証データに基づいて前記受信装置を認証する認証ステップと、

前記受信装置に対して前記応答を要求するコマンドが送信されたときから、前記受信装置からの応答が受信されるまでの間の応答時間を計測する計測ステップと、

前記認証ステップによる認証結果、および前記計測ステップの処理で計測された応答時

10

20

30

40

50

間に基づいて、前記受信装置に対するデータの送信可否を判定する判定ステップとを含む情報処理方法。

【請求項 9】

受信装置との間で共有するデータをもとに、コマンド認証データと、応答期待値データを生成する認証データ生成ステップと、

前記コマンド認証データを含み、応答を要求するコマンドを前記受信装置に送信するコマンド送信ステップと、

前記コマンドに対する受信装置からの応答を受信する応答受信ステップと、

前記応答期待値と、前記受信装置から受信した前記応答に含まれる応答認証データに基づいて前記受信装置を認証する認証ステップと、

前記受信装置に対して前記応答を要求するコマンドが送信されたときから、前記受信装置からの応答が受信されるまでの間の応答時間を計測する計測ステップと、

前記認証ステップによる認証結果、および前記計測ステップの処理で計測された応答時間に基づいて、前記受信装置に対するデータの送信可否を判定する判定ステップと

を含む処理をコンピュータに実行させるプログラム。

【請求項 10】

所定のコマンドに対する応答時間に基づいて送信データの送信可否を判定する送信装置と通信可能な情報処理装置において、

前記送信装置との間で共有する共有データから、前記送信装置において前記共有データから生成された前記コマンドの認証データに対応するコマンド期待値データおよび応答認証データを生成する生成部と、

前記送信装置から送信されてきた前記コマンドが受信されたとき、前記コマンドに含まれる前記コマンドの認証データと、前記生成部により生成された前記コマンド期待値データに基づいて前記送信装置を認証する認証部と、

前記認証部による認証結果に基づいて、前記応答認証データを含む応答を前記送信装置に送信する送信部と

を備える情報処理装置。

【請求項 11】

所定のコマンドに対する応答時間に基づいて送信データの送信可否を判定する送信装置と通信可能な情報処理装置の情報処理方法において、

前記送信装置との間で共有する共有データから、前記送信装置において前記共有データから生成された前記コマンドの認証データに対応するコマンド期待値データおよび応答認証データを生成する生成ステップと、

前記送信装置から送信されてきた前記コマンドが受信されたとき、前記コマンドに含まれる前記コマンドの認証データと、前記生成ステップの処理で生成された前記コマンド期待値データに基づいて前記送信装置を認証する認証ステップと、

前記認証ステップの処理での認証結果に基づいて、前記応答認証データを含む応答を前記送信装置に送信する送信ステップと

を備える情報処理方法。

【請求項 12】

所定のコマンドに対する応答時間に基づいて送信データの送信可否を判定する送信装置と通信可能な情報処理装置の情報処理用のプログラムであって、

前記送信装置との間で共有する共有データから、前記送信装置において前記共有データから生成された前記コマンドの認証データに対応するコマンド期待値データおよび応答認証データを生成する生成ステップと、

前記送信装置から送信されてきた前記コマンドが受信されたとき、前記コマンドに含まれる前記コマンドの認証データと、前記生成ステップの処理で生成された前記コマンド期待値データに基づいて前記送信装置を認証する認証ステップと、

前記認証ステップの処理での認証結果に基づいて、前記応答認証データを含む応答を前記送信装置に送信する送信ステップと

10

20

30

40

50

を含む処理をコンピュータに実行させるプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本開示は、情報処理装置、情報処理方法、およびプログラムに関し、特に、通信相手との通信時間を適切に計測することができるようにした情報処理装置、情報処理方法、およびプログラムに関する。

【背景技術】

【0002】

近年、インターネットに代表される公共性のある広域に亘るネットワーク（以下、WAN(Wide Area Network)と称する）や一般家屋等に設けられる局所的なネットワーク（以下、LAN(Local Area Network)と称する）の普及に伴い、それらのネットワークを介した各種データ通信が盛んに行われている。

【0003】

映像や音楽コンテンツなどを、ネットワークを通して伝送する場合は、著作権保護のために、通信相手の機器との間で、認証および鍵交換を行い、コンテンツを暗号化して伝送することが行われている（例えば、非特許文献1参照）。

【先行技術文献】

【非特許文献】

【0004】

【非特許文献1】DTCP Specification Volume 1 Version 1.3 (Information Version) http://www.dtcp.com/daTa/info_20040107_dtcp_Vol_1_1p3.pdf

【発明の概要】

【発明が解決しようとする課題】

【0005】

ここにおいて、著作権の観点からは、家庭内でのコピーや伝送は許可するが、WANで接続された他の家庭との間でのコンテンツの伝送を制限したい場合がある。例えば、テレビジョン放送を録画したコンテンツは、私的利用の範囲（家庭内）で利用できるが、インターネットを通して、他人に伝送するのは著作権を侵害すると考えられるので、このような制限が必要となる。

【0006】

この制限の下では、著作権保護されたコンテンツを送信する機器(送信機器)は、そのコンテンツを受信する通信相手の機器(受信機器)が同一LAN内にあるか、WAN(インターネット)を通して接続されているかを判断する必要がある。

【0007】

例えば、IPアドレスから通信相手が同一サブネット内にあるかどうかを調べることや、IP通信パケットが通過したIPルータの数(Hop Count)を使うことで通信相手がWAN(インターネット)を通して接続されているかを知ることができる。

【0008】

しかしながら、WAN(インターネット)を経由した通信であってもVPN(Virtual Private Network)などの技術を使えば、IPルータを経由せずに接続されている同一サブネットであるかのように接続することが可能である。すなわち不正にコンテンツを入手することが可能である。

【0009】

本開示はこのような状況に鑑みてなされたものであり、所定のコマンドに対する受信機器の応答時間に基づいて通信距離を判別し、例えば送信機器と同一LANに接続されているか否かを判定することを目的とする。

【課題を解決するための手段】

【0010】

本開示の第1の側面の情報処理装置は、応答を要求するコマンドを受信装置に送信する

10

20

30

40

50

コマンド送信部と、前記受信装置との間で共有する共有データに基づいて、期待値を生成する期待値生成部と、前記共有データに基づいて生成された認証データを含んだ応答メッセージを前記受信装置から受信する受信部と、前記期待値生成部により生成された前記期待値と受信部により受信された前記認証データに基づいて、前記受信装置を認証する認証部と、前記受信装置に対して前記応答を要求するコマンドが送信されたときから、前記受信装置からの応答メッセージが受信されるまでの間の応答時間を計測する計測部と、前記認証部による認証結果、および前記計測部により計測された前記応答時間に基づいて、前記受信装置に対するデータの送信可否を判定する判定部とを備える情報処理装置である。

【0011】

本開示の第1の側面の情報処理方法は、応答を要求するコマンドを受信装置に送信するコマンド送信ステップと、前記受信装置との間で共有する共有データに基づいて、期待値を生成する期待値生成ステップと、前記共有データに基づいて生成された認証データを含んだ応答メッセージを前記受信装置から受信する受信ステップと、前記期待値生成ステップの処理で生成された前記期待値と受信ステップの処理で受信された前記認証データに基づいて、前記受信装置を認証する認証ステップと、前記受信装置に対して前記応答を要求するコマンドが送信されたときから、前記受信装置からの応答メッセージが受信されるまでの間の応答時間を計測する計測ステップと、前記認証ステップでの認証結果、および前記計測ステップの処理で計測された前記応答時間に基づいて、前記受信装置に対するデータの送信可否を判定する判定ステップとを含む情報処理方法である。

【0012】

本開示の第1の側面のプログラムは、応答を要求するコマンドを受信装置に送信するコマンド送信ステップと、前記受信装置との間で共有する共有データに基づいて、期待値を生成する期待値生成ステップと、前記共有データに基づいて生成された認証データを含んだ応答メッセージを前記受信装置から受信する受信ステップと、前記期待値生成ステップの処理で生成された前記期待値と受信ステップの処理で受信された前記認証データに基づいて、前記受信装置を認証する認証ステップと、前記受信装置に対して前記応答を要求するコマンドが送信されたときから、前記受信装置からの応答メッセージが受信されるまでの間の応答時間を計測する計測ステップと、前記認証ステップでの認証結果、および前記計測ステップの処理で計測された前記応答時間に基づいて、前記受信装置に対するデータの送信可否を判定する判定ステップとを含む処理をコンピュータに実行させるプログラムである。

【0013】

本開示の第1の側面によれば、応答を要求するコマンドが受信装置に送信され、前記受信装置との間で共有する共有データに基づいて、期待値が生成され、前記共有データに基づいて生成された認証データを含んだ応答メッセージが前記受信装置から受信され、生成された前記期待値と受信された前記認証データに基づいて、前記受信装置が認証され、前記受信装置に対して前記応答を要求するコマンドが送信されたときから、前記受信装置からの応答メッセージが受信されるまでの間の応答時間が計測され、認証結果、および計測された前記応答時間に基づいて、前記受信装置に対するデータの送信可否が判定される。

【0014】

本開示の第2の側面の情報処理装置は、送信装置と共有する共有データから生成された認証データに基づく認証結果、および前記送信装置からの所定のコマンドに対する応答時間に基づいてデータの送信可否を判定する前記送信装置と通信可能な情報処理装置であって、前記送信装置から前記コマンドを受信する受信部と、前記共有データに対して所定の処理を施して、前記認証データを生成する認証データ生成部と、前記認証データ生成部により生成された前記認証データを含む、前記コマンドに対する応答メッセージを生成する応答メッセージ生成部と、前記送信装置から送信されてきた前記コマンドが受信されたとき、前記応答メッセージを前記送信装置に送信する送信部とを備える情報処理装置である。

【0015】

本開示の第2の側面の情報処理方法は、送信装置と共有する共有データから生成された認証データに基づく認証結果、および前記送信装置からの所定のコマンドに対する応答時間に基いてデータの送信可否を判定する前記送信装置と通信可能な情報処理装置の情報処理方法であって、前記送信装置から前記コマンドを受信する受信ステップと、前記共有データに対して所定の処理を施して、前記認証データを生成する認証データ生成ステップと、前記認証データ生成ステップの処理で生成された前記認証データを含む、前記コマンドに対する応答メッセージを生成する応答メッセージ生成ステップと、前記送信装置から送信されてきた前記コマンドが受信されたとき、前記応答メッセージを前記送信装置に送信する送信ステップとを含む情報処理方法である。

【0016】

本開示の第2の側面のプログラムは、送信装置と共有する共有データから生成された認証データに基づく認証結果、および前記送信装置からの所定のコマンドに対する応答時間に基いてデータの送信可否を判定する前記送信装置と通信可能な情報処理装置の情報処理用のプログラムであって、前記送信装置から前記コマンドを受信する受信ステップと、前記共有データに対して所定の処理を施して、前記認証データを生成する認証データ生成ステップと、前記認証データ生成ステップの処理で生成された前記認証データを含む、前記コマンドに対する応答メッセージを生成する応答メッセージ生成ステップと、前記送信装置から送信されてきた前記コマンドが受信されたとき、前記応答メッセージを前記送信装置に送信する送信ステップとを含む処理をコンピュータに実行させるプログラムである。

【0017】

本開示の第2の側面によれば、前記送信装置から前記コマンドが受信され、前記共有データに対して所定の処理が施されて、前記認証データが生成され、生成された前記認証データを含む、前記コマンドに対する応答メッセージが生成され、前記送信装置から送信されてきた前記コマンドが受信されたとき、前記応答メッセージが前記送信装置に送信される。

【0018】

本開示の第3の側面の情報処理装置は、受信装置との間で共有するデータをもとに、コマンド認証データと、応答期待値データを生成する認証データ生成部と、前記コマンド認証データを含み、応答を要求するコマンドを前記受信装置に送信するコマンド送信部と、前記コマンドに対する受信装置からの応答を受信する応答受信部と、前記応答期待値と、前記受信装置から受信した前記応答に含まれる応答認証データに基いて前記受信装置を認証する認証部と、前記受信装置に対して前記応答を要求するコマンドが送信されたときから、前記受信装置からの応答が受信されるまでの間の応答時間を計測する計測部と、前記認証部による認証結果、および前記計測部により計測された応答時間に基いて、前記受信装置に対するデータの送信可否を判定する判定部とを備える情報処理装置である。

【0019】

本開示の第3の側面の情報処理方法は、受信装置との間で共有するデータをもとに、コマンド認証データと、応答期待値データを生成する認証データ生成ステップと、前記コマンド認証データを含み、応答を要求するコマンドを前記受信装置に送信するコマンド送信ステップと、前記コマンドに対する受信装置からの応答を受信する応答受信ステップと、前記応答期待値と、前記受信装置から受信した前記応答に含まれる応答認証データに基いて前記受信装置を認証する認証ステップと、前記受信装置に対して前記応答を要求するコマンドが送信されたときから、前記受信装置からの応答が受信されるまでの間の応答時間を計測する計測ステップと、前記認証ステップによる認証結果、および前記計測ステップの処理で計測された応答時間に基いて、前記受信装置に対するデータの送信可否を判定する判定ステップとを含む情報処理方法である。

【0020】

本開示の第3の側面のプログラムは、受信装置との間で共有するデータをもとに、コマンド認証データと、応答期待値データを生成する認証データ生成ステップと、前記コマン

ド認証データを含み、応答を要求するコマンドを前記受信装置に送信するコマンド送信ステップと、前記コマンドに対する受信装置からの応答を受信する応答受信ステップと、前記応答期待値と、前記受信装置から受信した前記応答に含まれる応答認証データに基づいて前記受信装置を認証する認証ステップと、前記受信装置に対して前記応答を要求するコマンドが送信されたときから、前記受信装置からの応答が受信されるまでの間の応答時間を計測する計測ステップと、前記認証ステップによる認証結果、および前記計測ステップの処理で計測された応答時間に基づいて、前記受信装置に対するデータの送信可否を判定する判定ステップとを含む処理をコンピュータに実行させるプログラムである。

【0021】

本開示の第3の側面によれば、受信装置との間で共有するデータをもとに、コマンド認証データと、応答期待値データが生成され、前記コマンド認証データを含み、応答を要求するコマンドが前記受信装置に送信され、前記コマンドに対する受信装置からの応答が受信され、前記応答期待値と、前記受信装置から受信した前記応答に含まれる応答認証データに基づいて前記受信装置が認証され、前記受信装置に対して前記応答を要求するコマンドが送信されたときから、前記受信装置からの応答が受信されるまでの間の応答時間が計測され、認証結果、および計測された応答時間に基づいて、前記受信装置に対するデータの送信可否が判定される。

【0022】

本開示の第4の側面の情報処理装置は、所定のコマンドに対する応答時間に基づいて送信データの送信可否を判定する送信装置と通信可能な情報処理装置において、前記送信装置との間で共有する共有データから、前記送信装置において前記共有データから生成された前記コマンドの認証データに対応するコマンド期待値データおよび応答認証データを生成する生成部と、前記送信装置から送信されてきた前記コマンドが受信されたとき、前記コマンドに含まれる前記コマンドの認証データと、前記生成部により生成された前記コマンド期待値データに基づいて前記送信装置を認証する認証部と、前記認証部による認証結果に基づいて、前記応答認証データを含む応答を前記送信装置に送信する送信部とを備える情報処理装置である。

【0023】

本開示の第4の側面の情報処理方法は、所定のコマンドに対する応答時間に基づいて送信データの送信可否を判定する送信装置と通信可能な情報処理装置の情報処理方法において、前記送信装置との間で共有する共有データから、前記送信装置において前記共有データから生成された前記コマンドの認証データに対応するコマンド期待値データおよび応答認証データを生成する生成ステップと、前記送信装置から送信されてきた前記コマンドが受信されたとき、前記コマンドに含まれる前記コマンドの認証データと、前記生成ステップの処理で生成された前記コマンド期待値データに基づいて前記送信装置を認証する認証ステップと、前記認証ステップの処理での認証結果に基づいて、前記応答認証データを含む応答を前記送信装置に送信する送信ステップとを備える情報処理方法である。

【0024】

本開示の第4の側面のプログラムは、所定のコマンドに対する応答時間に基づいて送信データの送信可否を判定する送信装置と通信可能な情報処理装置の情報処理用のプログラムであって、前記送信装置との間で共有する共有データから、前記送信装置において前記共有データから生成された前記コマンドの認証データに対応するコマンド期待値データおよび応答認証データを生成する生成ステップと、前記送信装置から送信されてきた前記コマンドが受信されたとき、前記コマンドに含まれる前記コマンドの認証データと、前記生成ステップの処理で生成された前記コマンド期待値データに基づいて前記送信装置を認証する認証ステップと、前記認証ステップの処理での認証結果に基づいて、前記応答認証データを含む応答を前記送信装置に送信する送信ステップとを含む処理をコンピュータに実行させるプログラムである。

【0025】

本開示の第4の側面によれば、前記送信装置との間で共有する共有データから、前記送

10

20

30

40

50

信装置において前記共有データから生成された前記コマンドの認証データに対応するコマンド期待値データおよび応答認証データが生成され、前記送信装置から送信されてきた前記コマンドが受信されたとき、前記コマンドに含まれる前記コマンドの認証データと、生成された前記コマンド期待値データに基づいて前記送信装置が認証され、認証結果に基づいて、前記応答認証データを含む応答が前記送信装置に送信される。

【発明の効果】

【0026】

本開示の第1および第3の側面によれば、受信装置の応答時間を適切に計測することができる。

【0027】

本開示の第2および第4の側面によれば、送信装置における応答時間の適切な計測に必要な情報を提供することができる。

【図面の簡単な説明】

【0028】

【図1】本開示を適用した情報通信システムの利用例を示す図である。

【図2】図1の端末の構成例を示すブロック図である。

【図3】図2の送信可否判定部の構成例を示すブロック図である。

【図4】図2の応答制御部の構成例を示すブロック図である。

【図5】送信可否判定処理および応答処理を説明するフローチャートである。

【図6】期待値および認証データの生成方法を説明する図である。

【図7】期待値および認証データの他の生成方法を説明する図である。

【図8】図1の端末の動作を説明する図である。

【図9】図2の送信可否判定部の他の構成例を示すブロック図である。

【図10】図2の応答制御部の他の構成例を示すブロック図である。

【図11】他の送信可否判定処理を説明するフローチャートである。

【図12】他の応答処理を説明するフローチャートである。

【図13】図1の端末の動作を説明する他の図である。

【図14】図1の端末の動作を説明する他の図である。

【図15】図1の端末の動作を説明する他の図である。

【図16】パーソナルコンピュータ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】

【0029】

図1は、本開示を適用した端末11からなる情報通信システムの構成例を示している。

【0030】

LAN1-1、1-2（以下、個々に区別する必要がない場合、単位、LAN1と称する。他の場合についても同様である）がインターネットに代表されるWAN2を介して相互に接続されている。

【0031】

LAN1-1は、例えば、家屋内に設けられ、特定の個人（あるいは、家族）が使用する程度の規模のものであり、それには、スイッチングハブ（図示せず）を介して、パーソナルコンピュータやAV機器等の端末11-1および端末11-2が接続されている。LAN1-1と端末11-1および11-2との接続は、例えば、Ethernet（登録商標）（100BASE-TX）等の高速インタフェースによる。端末11-1および11-2は、LAN1-1およびWAN2を介して、LAN1-2に接続することができる。

【0032】

LAN1-2は、LAN1-1と同様に構成されており、それには、端末11-3が接続されている。

【0033】

各端末11は、本情報通信システムに登録された正規の機器であり、図2に示すように、送信可否判定部21、応答制御部22、通信部23、および送信データ格納部24を含

10

20

30

40

50

んで構成されている。

【0034】

送信可否判定部21は、他の端末11（受信側の端末11）に所定のデータを送信する際に、通信部23を介して、受信側の端末11（正確には、その応答制御部22）と後述するように通信することで、受信側の端末11が本情報通信システムにおける正規の機器であるか否かを認証するとともに、所定の要求に対する受信側の端末11の応答時間を、受信側の端末11との通信時間として計測する。

【0035】

送信可否判定部21は、受信側の端末11の認証結果および応答時間に基づく通信距離の判別結果に基づいて、受信側の端末11に対するデータの送信可否を判定する。

10

【0036】

例えば、受信側の端末11が、送信側の端末11と異なるLAN1に接続されている場合（WAN2を介して接続され、いわゆる通信距離が長い場合）、応答時間は、同じLAN1に接続されている場合（通信距離が短い場合）に比べて長くなるので、例えば、通信が同一LAN1内に制限されているとき、送信可否判定部21は、計測した応答時間から受信側の端末11が送信側の端末11と同じLAN1に接続されているか否かを判定し、その判定結果と受信側の端末11の認証結果に基づいて、データ送信の可否を判定する。

【0037】

すなわち図1の例では、端末11-1（送信側）が端末11-2（受信側）にデータを送信する場合、端末11-1の送信可否判定部21は、計測した端末11-2の応答時間から、端末11-2がLAN1-1に接続されていることを判定し、データ送信を行う。一方、端末11-1が端末11-3にデータを送信する場合、端末11-1の送信可否判定部21は、計測した端末11-3の応答時間から、端末11-3はLAN1-1と異なるLAN（LAN1-2）に接続されていることを判定し、データ送信を行わない。

20

【0038】

なおこのような通信距離による通信制御は、映画などのコンテンツを一定の地域に対して先行配給し、他の地域には後日配給するなどのコンテンツ配給ビジネスに適用することができる。

【0039】

図2に戻り、応答制御部22は、送信側の端末11から所定のデータの送信を受ける際、通信部23を介して、送信側の端末11（正確には、その送信可否判定部21）と後述するように通信することで、送信側の端末11における認証および応答時間の適切な計測に必要な情報を送信側の端末11に送信する。

30

【0040】

通信部23は、LAN1に接続されており、同一のLAN1内の端末11、又はWAN2を介して異なるLAN1に接続されている端末11との通信を行う。

【0041】

送信データ格納部24は、受信側の端末11に送信される、所定のデータが格納されている。

【0042】

図3は、端末11の送信可否判定部21の構成例を示している。

40

【0043】

ランダムチャレンジ生成部31は、所定ビット数の疑似乱数（以下、ランダムチャレンジと称する）を生成し、ランダムチャレンジ送信制御部32および期待値生成部33に供給する。

【0044】

ランダムチャレンジ送信制御部32は、ランダムチャレンジ生成部31から供給されたランダムチャレンジを、通信部23を介して、受信側の端末11に送信する。ランダムチャレンジ送信制御部32はまた、通信部23を介して、受信側の端末11から送信されてきた、ランダムチャレンジを受信した旨のメッセージ（以下、RC受信メッセージと称す

50

る)を受信し、そのときRC受信メッセージを受信した旨をコマンド送信制御部34に通知する。

【0045】

期待値生成部33は、ランダムチャレンジ生成部31から供給されたランダムチャレンジに対して、例えば、受信側の端末11と共有する秘密鍵を利用したHMAC (Keyed-Hashing for Message Authentication, IETF RFC 2104) アルゴリズムによるハッシュ処理(いわゆる鍵付きハッシュ処理)を施して、受信側の端末11でランダムチャレンジから生成される認証データの期待値を生成し、判定部35に供給する。期待値生成部33はまた、端末11に予め設定された端末11固有の情報(例えば、機器ID)とランダムチャレンジを連結したものに鍵付きハッシュ処理を施して期待値を生成することもできる。

10

【0046】

なお、ハッシュ処理で利用される秘密鍵は、本情報通信システムの正規の機器に所定のタイミングで安全に配信される。

【0047】

コマンド送信制御部34は、ランダムチャレンジ送信制御部32から、RC受信メッセージを受信した旨が通知されたとき、又は判定部35からの指示に従って、応答を要求するコマンド(以下、応答要求コマンドと称する)を、通信部23を介して、受信側の端末11に送信する。

【0048】

コマンド送信制御部34又は、通信部23を介して、送信した応答要求コマンドに対する応答として、受信側の端末11から送信されてきたメッセージ(以下、応答メッセージと称する)を受信し、それを判定部35に供給する。応答メッセージには、ランダムチャレンジ送信制御部32により送信されたランダムチャレンジから生成された認証データが組み込まれている。

20

【0049】

コマンド送信制御部34又は、応答要求コマンドを送信した後、応答時間計測部36を制御して、応答時間の計測を開始させるとともに、その応答要求コマンドに対する応答としての応答メッセージを受信したとき、応答時間の計測を終了させる。

【0050】

判定部35は、コマンド送信制御部34からの応答メッセージに組み込まれている認証データと、期待値生成部33で生成されたその認証データの期待値に基づいて、受信側の端末11が、本情報通信システムにおける正規の機器であるかの認証を行う。判定部35はまた、応答時間計測部36で計測された応答時間が所定の時間TLを越えているか否かを判定して、通信距離の判別(送信側の端末11と同一のLAN1に接続されているかの判定)を行う。

30

【0051】

判定部35は、受信側の端末11の認証結果および通信距離の判別結果に基づいて、データの送信可否の判定を行う。判定部35は、その判定結果に基づいて、通信部23を制御し、送信データ格納部24に格納されているデータを、受信側の端末11に送信させる。

40

【0052】

応答時間計測部36は、コマンド送信制御部34からの指示に従って、内蔵するタイマを動作させ、受信側の端末11の応答時間を計測する。

【0053】

図4は、端末11の応答制御部22の構成例を示している。

【0054】

ランダムチャレンジ受信制御部41は、通信部23を介して、送信側の端末11(正確には、その送信可否判定部21)から送信されてきたランダムチャレンジを受信し、それを認証データ生成部42に供給する。ランダムチャレンジ受信制御部41はまた、通信部23を介して、RC受信メッセージ(ランダムチャレンジを受信した旨を表すメッセージ

50

）を、送信側の端末 1 1 に送信し、そのとき R C 受信メッセージを送信した旨を応答メッセージ送信制御部 4 4 に通知する。

【0055】

認証データ生成部 4 2 は、ランダムチャレンジ受信制御部 4 1 から供給されたランダムチャレンジに対して、送信側の端末 1 1（送信可否判定部 2 1 の期待値生成部 3 3）における場合と同様の鍵付きハッシュ処理を施して、第三者が予測できない認証データを生成し、応答メッセージ生成部 4 3 に供給する。

【0056】

応答メッセージ生成部 4 3 は、応答メッセージ送信制御部 4 4 の制御に従って、認証データ生成部 4 2 から供給された認証データを組み込んだ応答メッセージを生成し、応答メッセージ送信制御部 4 4 に供給する。

10

【0057】

応答メッセージ送信制御部 4 4 は、通信部 2 3 を介して、送信側の端末 1 1 から送信されてきた応答要求コマンドを受信する。

【0058】

応答メッセージ送信制御部 4 4 は、応答要求コマンドを受信する前のタイミングで（送信側の端末 1 1 から応答要求コマンドが送信されてくる前のタイミングで）、応答メッセージ生成部 4 3 を制御して、受信する応答要求コマンドに対応した認証データが組み込まれた応答メッセージを生成させるとともに、応答要求コマンドを受信したとき、通信部 2 3 を介して、その応答メッセージを送信先の端末 1 1 に送信する。

20

【0059】

次に、図 5 のフローチャートを参照して、送信可否判定処理を行う場合の端末 1 1 の送信可否判定部 2 1（図 2，3）の動作を説明する。

【0060】

ステップ S 1 において、端末 1 1（送信側の端末 1 1）の送信可否判定部 2 1 のランダムチャレンジ生成部 3 1 は、ランダムチャレンジを生成し、それをランダムチャレンジ送信制御部 3 2 および期待値生成部 3 3 に供給する。

【0061】

ステップ S 2 において、ランダムチャレンジ送信制御部 3 2 は、供給されたランダムチャレンジを、通信部 2 3 を介して受信側の端末 1 1 に送信し、ステップ S 3 において、期待値生成部 3 3 は、供給されたランダムチャレンジに対して鍵付きハッシュ処理を施して、受信側の端末 1 1 で生成される認証データの期待値を生成する。

30

【0062】

なおこの例の場合、送信側の端末 1 1 は、データ送信の可否を判定するのに、最大 N（＝1，2，・・・）回応答要求コマンドを送信するので、ここでは、送信され得る N 個の応答要求コマンドに応じた認証データの N 個の期待値が生成される。

【0063】

N 個の期待値は、例えば、ランダムチャレンジに対して鍵付きハッシュ処理を施した結果得られたデータを複数個に分割し、その分割して得られたデータから N 個の期待値を生成することができる。図 6 の例の場合、ランダムチャレンジに対して鍵付きハッシュ処理を施した結果得られたデータが、N 個に分割されて、N 個の期待値 1 乃至期待値 N が生成される。

40

【0064】

また、ランダムチャレンジに対する鍵付きハッシュ処理を、複数回繰り返して行い、その処理毎に得られたデータから、N 個の期待値を生成することができる。図 7 の例の場合、ランダムチャレンジに対する鍵付きハッシュ処理が N 回繰り返して行われ、その処理毎に得られた N 個のデータが期待値となる。図 7 中、期待値 1 は、ランダムチャレンジに鍵付きハッシュ処理が 1 回施された結果得られたものであり、期待値 2 は、期待値 1 に、鍵付きハッシュ処理がさらに施された結果得られたものである。

【0065】

50

図 5 に戻り、ステップ S 4 において、ランダムチャレンジ送信制御部 3 2 は、後述するように受信側の端末 1 1 から送信されてきた、ステップ S 2 で送信されたランダムチャレンジを受信した旨を示す RC 受信メッセージを（ステップ S 2 3）、通信部 2 3 を介して受信し、その旨をコマンド送信制御部 3 4 に通知する。ステップ S 5 において、コマンド送信制御部 3 4 は、応答要求コマンドが何番目に送信されるものか（送信の順番）を示すカウンタ i に 1 を初期設定する。

【0066】

次に、ステップ S 6 において、コマンド送信制御部 3 4 は、通信部 2 3 を介して、応答要求コマンドを受信側の端末 1 1 に送信し、ステップ S 7 において、応答時間計測部 3 6 を制御して、応答時間の計測を開始させる。

【0067】

ステップ S 8 において、コマンド送信制御部 3 4 は、後述するように受信側の端末 1 1 から送信されてきた、ステップ S 6 で送信された応答要求コマンドに対する応答しての応答メッセージを、通信部 2 3 を介して受信して、判定部 3 5 に供給し、ステップ S 9 において、応答時間計測部 3 6 を制御して、応答時間の計測を終了させる。すなわちステップ S 7 で開始しステップ S 9 で終了する時間計測で得られた時間が受信側の端末 1 1 の応答時間となる。

【0068】

ステップ S 10 において、判定部 3 5 は、コマンド送信制御部 3 4 から供給された応答メッセージに組み込まれている認証データと、期待値生成部 3 3 により生成された、その認証データの期待値（具体的には、カウンタ i が示す順番に送信された応答要求コマンド（以下、第 i 番目に送信された応答要求コマンドと称する）に対応する期待値）とが一致するか否かを判定し、一致すると判定した場合、受信側の端末 1 1 を、情報通信システムにおける正規の端末であると認証し、ステップ S 11 に進む。

【0069】

ステップ S 11 において、判定部 3 5 は、応答時間計測部 3 6 で計測された、第 i 番目に送信された応答要求コマンドに対する受信側の端末 1 1 の応答時間が所定の時間 TL を越えているか否かを判定する。時間 TL は、例えば、同一 LAN 1 に接続された端末 1 1 間で要する通信時間である。すなわち応答時間が時間 TL を越える場合、受信側の端末 1 1 は、送信側の端末 1 1 と異なる LAN 1 に接続され、また、時間 TL を越えない場合（応答時間＝時間 TL を含む）、同一の LAN 1 に接続されていると判定することができる（通信距離を判別することができる）。

【0070】

ステップ S 11 で、時間 TL を越えると判定された場合、ステップ S 12 に進み、判定部 3 5 は、その結果を、コマンド送信制御部 3 4 に通知し、コマンド送信制御部 3 4 はそのとき、カウンタ i を 1 だけインクリメントする。

【0071】

ステップ S 13 において、コマンド送信制御部 3 4 は、カウンタ $i = N + 1$ であるか否かを判定する。カウンタ $i = N + 1$ ではないと判定された場合には、所定時間経過後、ステップ S 6 に戻る。ステップ S 13 で、カウンタ $i = N + 1$ であると判定されたとき（すなわち、応答要求コマンドの送信が N 回行われたとき）、又はステップ S 10 で、受信側の端末 1 1 が本情報通信システムにおける正規の機器ではないと判定されたとき、ステップ S 14 に進み、その旨を、判定部 3 5 に通知する。判定部 3 5 はそのとき、受信側の端末 1 1 へのデータ送信を不可とし、通信部 2 3 を制御して、送信データ格納部 2 4 に格納されているデータの受信側の端末 1 1 に対する送信を禁止する。

【0072】

ステップ S 11 で、第 i 番目に送信された応答要求コマンドに対する応答時間が、時間 TL を越えないと判定された場合、すなわち、受信側の端末 1 1 が、本情報通信システムにおける正規の機器であり、かつ、例えば送信側の端末 1 1 と同じ LAN 1 に接続されている端末 1 1 であるとき、ステップ S 15 に進み、判定部 3 5 は、通信部 2 3 を制御して、送

10

20

30

40

50

信データ格納部 2 4 に格納されているデータを、受信側の端末 1 1 に送信させる。

【0073】

ステップ S 1 4 又はステップ S 1 5 で、受信側の端末 1 1 に対するデータ送信可否が判定されたとき、判定部 3 5 は、通信部 2 3 を介して、送信可否判定が終了した旨を表すメッセージ（以下、判定終了メッセージと称する）を受信側の端末 1 1 に送信する。その後、送信可否判定処理は、処理を終了する。

【0074】

次に、図 5 のフローチャートを参照して、応答処理を行う場合の端末 1 1 の応答制御部 2 2（図 2，4）の動作を説明する。

【0075】

ステップ S 2 1 において、端末 1 1（受信側の端末 1 1）の応答制御部 2 2 のランダムチャレンジ受信制御部 4 1 は、送信先の端末 1 1 から送信されてきたランダムチャレンジを（ステップ S 2）、通信部 2 3 を介して受信し、認証データ生成部 4 2 に供給する。ステップ S 2 2 において、認証データ生成部 4 2 は、ランダムチャレンジ受信制御部 4 1 から供給されたランダムチャレンジに対して、送信側の端末 1 1 の送信可否判定部 2 1（期待値生成部 3 3）における鍵付きハッシュ処理（ステップ S 3）と同様の鍵付きハッシュ処理を施し、認証データを生成し、応答メッセージ生成部 4 3 に供給する。

【0076】

なおこの例では、最大 N 個の応答要求コマンドを受信し得るので、その応答要求コマンドに対応する期待値と対比される（ステップ S 1 0）N 個の認証データが生成される。N 個の認証データは、期待値の生成方法（図 6，7）と同じ方法で生成される。

【0077】

このように認証データが生成されると、ステップ S 2 3 において、ランダムチャレンジ受信制御部 4 1 は、通信部 2 3 を介して、RC 受信メッセージを送信側の端末 1 1 に送信し、その旨を、応答メッセージ送信制御部 4 4 に通知する。

【0078】

ステップ S 2 4 において、応答メッセージ送信制御部 4 4 は、これから受信する応答要求コマンドが何番目に受信されるものかを示すカウンタ j に 1 を初期設定し、ステップ S 2 5 において、応答メッセージ生成部 4 3 を制御して、カウンタ j が示す順番に受信される応答要求コマンド（以下、第 j 番目に受信される応答要求コマンドと称する）に対応する認証データを組み込んだ応答メッセージを生成させる。

【0079】

次に、ステップ S 2 6 において、応答メッセージ送信制御部 4 4 は、送信先の端末 1 1 から送信されてきた応答要求コマンドを（ステップ S 6）、通信部 2 3 を介して受信すると、ステップ S 2 7 において、ステップ S 2 5 で生成された第 j 番目に受信される応答要求コマンドに応じた認証データが組み込まれた応答メッセージを、通信部 2 3 を介して、送信側の端末 1 1 に送信する。これにより上述したように送信側の端末 1 1 で（ステップ S 1 0 で）、第 j 番目に受信された（第 i 番目に送信された）応答要求コマンドに対応する認証データと、第 i 番目に送信された（第 j 番目に受信された）応答要求コマンドの期待値とが比較される。

【0080】

ステップ S 2 8 において、受信側の端末 1 1 の応答制御部 2 2 の応答メッセージ送信制御部 4 4 は、送信側の端末 1 1 から送信される判定終了メッセージ（ステップ S 1 6）が受信されたか否かを判定し、所定の時間内に受信されていないと判定した場合、ステップ S 2 9 に進む。ステップ S 2 9 において、応答メッセージ送信制御部 4 4 は、カウンタ j を 1 だけインクリメントし、ステップ S 3 0 で、カウンタ j = N + 1 であるか否かを判定する。

【0081】

ステップ S 3 0 で、カウンタ j = N + 1 ではないと判定されたとき（すなわち、応答要求コマンドを N 回受信されていないとき）、ステップ S 2 5 に戻り、次に受信される応答

10

20

30

40

50

要求コマンドに対して、それ以降の処理を実行する。

【0082】

ステップS28で、判定終了メッセージが受信されたとき、又はステップS30で、カウンタ $j = N + 1$ であると判定されたとき（すなわち、応答要求コマンドがN回受信されたとき）、応答制御部22は、応答処理を終了する。

【0083】

以上のように、ランダムチャレンジから生成された認証データ（ステップS22）とその期待値（ステップS3）とに基づいて認証された受信側の端末11についてのみ応答時間に基づく通信距離の判別を行うようにしたので（ステップS10でNOの判定がなされた場合、ステップS11の処理がスキップされるので）、正規の機器のようになりすました機器にデータが送信されることを防止することができる（正規の機器のようになりすました機器が応答要求コマンドを受信し、応答要求メッセージを送信して、その機器にデータが送信されることはない）。

10

【0084】

また送信側の端末11で、応答要求コマンドに、新たに生成したランダムチャレンジを込み込んで受信側の端末11に送信し（ステップS6）、受信側の端末11で、応答要求コマンドを受信したとき（ステップS26）、予め生成された認証データ（ステップS22）と、その応答要求コマンドに組み込まれたランダムチャレンジとを連結して、又は両者の論理演算を行って新たな認証データを生成し、それを組み込んだ応答メッセージを返信することもできる（ステップS27）。なおこのとき送信側の端末11では、ステップS10で新たな認証データと比較される期待値が、ステップS3で生成された期待値と、応答要求コマンドに組み込まれたランダムチャレンジと連結されて、又は両者の論理演算が行われて生成される。

20

【0085】

このように応答要求コマンドに組み込んだランダムチャレンジを利用して認証データおよび期待値が生成されるようにすることで、受信側の端末11は、送信側の端末11からの応答要求コマンドを受信した後でなければ、応答メッセージを送信することができなくなる。したがって、応答時間を短縮するために、応答要求コマンドを受信する前に応答メッセージを送信するなどといった不正行為を防止することができる。

【0086】

また、以上のように、受信側の端末11において、応答要求コマンドを受信する前に、認証データおよびそれが組み込まれた応答メッセージを生成するようにしたので（ステップS22、S25）、応答要求コマンドを受信した後直ちに応答メッセージを送信側の端末11に返信することができる（ステップS27）。

30

【0087】

例えば、応答要求コマンドを受信した後に、認証データおよび応答要求メッセージを生成するようになされている場合、送信側の端末11で計測される応答時間に、その処理にかかる時間が含まれてしまうので、通信時間としての応答時間を正確に計測することができない。しかしながら本開示のように応答要求コマンドを受信した後直ちに応答メッセージを送信することができるようにしておくことにより、通信時間としての応答時間が正確に計測される。

40

【0088】

また、以上においては、送信側の端末11がランダムチャレンジを生成し（ステップS1）、受信側の端末11に提供するようにしたが（ステップS2）、受信側の端末11が生成して送信側の端末11に提供するようにすることもできる。

【0089】

また、以上においては、秘密鍵を送信側の端末11と受信側の端末11で共有している場合を例として説明したが、秘密鍵の共有がない場合には、デフィー・ヘルマン鍵交換（Diffie-Hellman key exchange）のアルゴリズムなどを使って鍵の共有を行うことができる。この場合は、鍵交換した相手は、応答時間を測定する相手であることの証明書など

50

を基に確認される。鍵交換の後、鍵交換で得られた鍵そのものを認証データと期待値とすることもできるし、上記のように乱数に交換した鍵での鍵付きハッシュ処理を施し、認証データや期待値を得るようにすることもできる。

【0090】

また以上においては、送信側の端末11において、受信側の端末11で生成された応答の認証データ（以下、認証データRRと称する）（ステップS22）と送信側の端末11で生成された応答の期待値（以下、期待値QRと称する）（ステップS3）とに基づき受信側の端末11が認証されたが（ステップS10）、受信側の端末11においても、送信側の端末11からの応答要求コマンドの認証データ（以下、認証データRSと称する）とその期待値（以下、期待値QSと称する）とに基づき送信側の端末11の認証を行うようにすることができる。

10

【0091】

図5の例では、受信側の端末11は、応答要求コマンドを受ければ（ステップS26）、直ちに応答メッセージを送り返すので（ステップS27）、例えば、図8に示すように、送信側の端末11（送信機器）と同一のLAN1に第3の機器xを挿入し、はじめに機器xが受信機器に応答要求コマンドを送って（S111）、受信機器から応答メッセージを取得しておき（S112）、そして送信機器から応答要求コマンドが来たときに（S121）、取得した応答メッセージを返すことで（S122）、機器xは、正規の機器になりすますことができる。

【0092】

20

そこで受信側の端末11においても、応答メッセージを返信する際に、送信側の端末11を認証すれば、このような不正を防止することができる（不正な機器に応答メッセージを返信することを防止することができる）。

【0093】

図9は、送信可否判定部21の、図10は、応答制御部22の、このように受信側の端末11でも送信側の端末11の認証がなされる場合の構成例を示している。

【0094】

送信可否判定部21のランダムチャレンジ生成部51は、図3のランダムチャレンジ生成部31と同様に、所定ビット数の疑似乱数列を、ランダムチャレンジRCとして生成し、期待値生成部52および認証データ生成部53に供給する。

30

【0095】

期待値生成部52は、ランダムチャレンジ生成部51から供給されたランダムチャレンジRCに対して、例えば、受信側の端末11と共有する秘密鍵を利用した受信側の端末11（認証データ生成部73）における場合と同様の鍵付きハッシュ処理を施して、受信側の端末11の認証データRRの期待値QR（対応する認証データRRと同値の期待値QR）を生成し、応答認証部57に供給する。

【0096】

認証データ生成部53は、ランダムチャレンジ生成部51から供給されたランダムチャレンジRCに対して、受信側の端末11と共有する秘密鍵を利用した鍵付きハッシュ処理を施して、第三者が予測できないコマンドの認証データRSを生成し、応答要求コマンド送信部55に供給する。

40

【0097】

制御コマンド通信制御部54は、開始コマンド等の制御コマンドCCを受信側の端末11に送信したり、受信側の端末11から送信されてきた、制御コマンドCCに対する応答メッセージCCRを受信する。

【0098】

応答要求コマンド送信部55は、認証データ生成部53により生成された認証データRSを含む、応答要求コマンドMCを、通信部23を介して、受信側の端末11に送信する。

【0099】

応答受信部56は、送信された応答要求コマンドMCに対する応答として、受信側の端末

50

1 1 から送信されてきた応答メッセージMCRを、通信部 2 3 を介して受信し、そこに組み込まれている応答の認証データRRを応答認証部 5 7 に供給する。

【0 1 0 0】

応答認証部 5 7 は、応答受信部 5 6 からの応答の認証データRRと、期待値生成部 5 2 で生成されたその認証データRRの期待値QRに基づいて、受信側の端末 1 1 が、本情報通信システムにおける正規の機器であるかの認証を行い、その認証結果を、制御判定部 5 8 に通知する。

【0 1 0 1】

制御判定部 5 8 は、応答時間計測部 5 9 で計測された、応答要求コマンドMCに対する受信側の端末 1 1 の応答時間RTTが所定の時間TLを越えているか否かを判定して、通信距離の判別（送信側の端末 1 1 と同一のLAN 1 に接続されているかの判定）を行う。

10

【0 1 0 2】

制御判定部 5 8 は、受信側の端末 1 1 の認証結果および通信距離の判別結果に基づいて、受信側の端末 1 1 に対するデータの送信可否の判定を行う。制御判定部 5 8 は、その判定結果に基づいて、通信部 2 3 を制御し、送信データ格納部 2 4 に格納されているデータを、受信側の端末 1 1 に送信させる。

【0 1 0 3】

応答時間計測部 5 9 は、応答要求コマンド送信部 5 5 および応答受信部 5 6 からの通知に応じて、応答要求コマンドMCに対する、受信側の端末 1 1 の応答時間RTTを計測する。

【0 1 0 4】

20

次に、応答制御部 2 2 の構成（図 1 0）を説明する。

【0 1 0 5】

制御応答通信制御部 7 1 は、通信部 2 3 を介して、送信側の端末 1 1 から送信されてきた制御コマンドCCを受信したり、その制御コマンドCCに対する応答メッセージCCRを送信側の端末 1 1 に送信する。

【0 1 0 6】

期待値生成部 7 2 は、制御応答通信制御部 7 1 により受信された制御コマンドCCに含まれるランダムチャレンジRCに対して、送信側の端末 1 1 と共有する秘密鍵を利用した送信側の端末 1 1 （認証データ生成部 5 3）における場合と同様の鍵付きハッシュ処理を施して、送信側の端末 1 1 のコマンド認証データRSの期待値QS（対応する認証データRSと同値の期待値QS）を生成し、コマンド認証部 7 6 に供給する。

30

【0 1 0 7】

認証データ生成部 7 3 は、制御応答通信制御部 7 1 により受信された制御コマンドCCに含まれるランダムチャレンジRCに対して、送信側の端末 1 1 と共有する秘密鍵を利用した鍵付きハッシュ処理を施して、第三者が予測できない応答の認証データRRを生成し、応答送信部 7 4 に供給する。

【0 1 0 8】

応答送信部 7 4 は、コマンド認証部 7 6 による認証結果に基づいて、認証データ生成部 7 3 により生成された応答の認証データRRを含む、送信側の端末 1 1 からの応答要求コマンドMCに対する応答メッセージMCRを、通信部 2 3 を介して送信側の端末 1 1 に送信する。

40

【0 1 0 9】

応答要求コマンド受信部 7 5 は、送信側の端末 1 1 から送信されてきた応答要求コマンドMCを、通信部 2 3 を介して受信し、そこに組み込まれているコマンドの認証データRSをコマンド認証部 7 6 に供給する。

【0 1 1 0】

コマンド認証部 7 6 は、応答要求コマンド受信部 7 5 からのコマンドの認証データRSと、期待値生成部 7 2 で生成されたその認証データRSの期待値QSに基づいて、送信側の端末 1 1 が、本情報通信システムにおける正規の機器であるかの認証を行い、その認証結果を、応答送信部 7 4 に通知する。

50

【0111】

次に、図9の送信可否判定部21の動作を、図11のフローチャートを参照して説明する。

【0112】

ステップS51において、端末11の送信可否判定部21の制御コマンド通信制御部54は、受信側の機器と、TCPコネクションを確立する。TCPコネクションのためのポート番号は予め送信側の端末11と受信側の機器の間に合意されているものとする。送信側の機器と受信側の機器の間に事前にTCPコネクションが確立している場合はこのステップを省略してよい。

【0113】

制御コマンド通信制御部54は、確立したTCPコネクションを介して、応答時間RTTの計測を開始する旨を表す開始コマンド（制御コマンドCC）を受信側の機器に送信する。この開始コマンドCCには、セッション番号SID、ランダムチャレンジRC、送信側の端末11が実行可能な、1セッションでの応答時間RTTの計測のリトライ数（計測回数）ksが含まれている。

【0114】

セッション番号SIDは、これから行われる受信側の機器に対する一連の認証処理（1つのセッション）に割り当てられた番号であり、この番号を送信側と受信側とで共有することにより、セッション毎に認証処理を区別することができる。

【0115】

また応答時間RTTの計測のために必要なデータ（例えば、応答要求コマンドMCやその応答メッセージMCR）の通信は、パケットの再送を行わないUDPでなされるので、通信状態によっては、データが途中で消滅してしまうなど、応答時間RTTの計測が適切に行われない場合も考えられる。またネットワーク内の他の通信の影響を受けて、パケットの伝送に遅延が生じることもある。そこで応答時間RTTの計測を何回かリトライ（再施行）できるようになされている。このリトライの回数は、送信側の機器と受信側の機器の設定によって異なることもあるので、この例ではここで送信側の機器のリトライ数（例えば、最大のリトライ数）ksが受信側の機器に通知される。

【0116】

次に、ステップS52において、制御コマンド通信制御部54は、開始コマンドCCに対する、受信側の機器からの応答メッセージCCRを受信する。

【0117】

この応答メッセージCCRには、開始コマンドCCに含まれていたセッション番号SIDの他、受信側が決定した1セッションでの応答時間RTT計測のリトライ数k、および応答要求コマンドMCを受信するためのUDPポート番号pbが含まれている。すなわち開始コマンドCCとその応答メッセージCCRの授受により、送信側の端末11と受信側の機器は、応答時間RTTの計測のリトライ数（計測回数）kとセッション番号SID、および応答要求コマンドMCとその応答メッセージMCRの授受のために利用するUDPポート番号pbを合意する。

【0118】

なお受信側の機器は、開始コマンドCCを介して通知された送信側の端末11で実行可能な応答時間RTT計測のリトライ数ksと受信側が実行可能な応答時間RTT計測のリトライ数のうちの小さい方を、今回の応答時間RTT計測のリトライ数kに決定し、応答メッセージCCRを介して送信側の機器に通知する。

【0119】

ステップS53において、期待値生成部52は、ランダムチャレンジ生成部51により生成されたランダムチャレンジRCに対して、受信側の端末11の応答制御部22（認証データ生成部73）における鍵付きハッシュ処理と同様の鍵付きハッシュ処理を施し、受信側の機器の認証データRRの期待値QRを生成する。

【0120】

この例の場合、応答時間RTT計測が最大k回行われるので（応答要求コマンドMCの応答

10

20

30

40

50

メッセージMCRが最大k回受信されるので)、受信され得るk個の応答メッセージMCRに含まれる認証データRRそれぞれの期待値QRが生成される。

【0121】

またこのとき認証データ生成部53は、ランダムチャレンジ生成部51により生成されたランダムチャレンジRCに対して鍵付きハッシュ処理を施して、コマンドの認証データRSを生成する。

【0122】

この例の場合、応答時間RTT計測が最大k回行われるので(応答要求コマンドMCが最大k回送信されるので)、送信され得るk個の応答要求コマンドMCそれぞれの認証データRSが生成される。

10

【0123】

ステップS54において、制御判定部58に内蔵されるカウンタiの値が1に初期設定される。このとき期待値生成部52は、カウンタiの値に対応する期待値QR(例えば、第i番目に生成された期待値QRi)を応答認証部57に供給する。また認証データ生成部53は、カウンタiの値に対応する認証データRSiを、応答要求コマンド送信部55に供給する。

【0124】

ステップS55において、応答要求コマンド送信部55は、セッション番号SID、認証データ生成部53から供給された認証データRSi(k個の認証データRSのうちのカウンタiの値に対応する認証データRSi)、およびシーケンス番号Ci(カウンタiの値を表す番号)を含む応答要求コマンドMCを、制御コマンドCCの応答CCRに含まれていたUDPポート番号pbでのUDP通信で、受信側の機器に送信する。

20

【0125】

応答要求コマンド送信部55は、応答要求コマンドMCを送信したとき、その旨の通知STRを応答時間計測部59に行う。これにより応答時間計測部59は、応答時間の計測を開始する。

【0126】

ステップS56において、応答受信部56は、受信側の機器からの応答メッセージMCRを受信したか否かを判定し、受信していないと判定した場合、ステップS57に進み、所定時間以上応答を待っているか否かを判定する(ステップS55で応答時間RTT計測が開始されてから所定の時間経過したか否かを判定する)。

30

【0127】

ステップS57で、まだ所定の時間経過していないと判定された場合、ステップS56に戻り、それ以降の処理が実行される。一方ステップS57で所定の時間経過したと判定された場合、ステップS62に進み、カウンタiの値がリトライ数kより小さいか否かが判定され(応答時間RTTの計測がk回行われたか否かが判定され)、小さいと判定された場合(k回行われていない場合)、ステップS63に進み、カウンタiの値が1だけインクリメントされて、ステップS55に戻る。

【0128】

応答要求コマンドMCを送るUDPでは、パケットが通信相手に届かないことがあるので、送信側の端末11は、応答要求コマンドMCを送った後、所定時間が経っても応答メッセージMCRが受信されない場合は、この回の計測は失敗したものとして、次の応答時間RTTの計測が開始される(ステップS55以降の処理が開始される)。

40

【0129】

ステップS56で、応答メッセージMCRが受信されたと判定された場合、ステップS58に進み、応答受信部56は、受信した応答メッセージMCRに含まれている応答の認証データRRj、およびシーケンス番号Cjを読み出し、応答認証部57に供給する。

【0130】

応答認証部57は、応答受信部56から供給されたシーケンス番号Cjが、カウンタiの値(送信された応答要求コマンドMCのシーケンス番号Ci)と一致するか否かを判定する。

50

【0131】

なお応答メッセージMCRのシーケンス番号Cjと応答要求コマンドMCのシーケンス番号Ciを確認することの効果については後述する。

【0132】

ステップS58で、一致しないと判定された場合、ステップS56に戻り、それ以降の処理が行われ、一致すると判定された場合、ステップS59に進む。

【0133】

ステップS59において、応答受信部56は、応答メッセージMCRを受信した旨の通知ENDを応答時間計測部59に行う。応答時間計測部59は、ステップS55で開始した応答時間RTT計測を終了し、計測結果（応答時間RTT）を、制御判定部58に供給する。

10

【0134】

ステップS60において、応答認証部57は、応答受信部56から供給された応答の認証データRRjと、期待値生成部52により生成された、その認証データRRjの期待値QRiとが一致するか否かを判定し、一致すると判定した場合、受信側の端末11を、本情報通信システムにおける正規の端末であると認証し、ステップS61に進む。

【0135】

ステップS61において、制御判定部58は、応答時間計測部59から供給された応答時間RTTが、所定の規定時間TLより大きいかな否かを判定する。

【0136】

規定時間TLは、応答時間RTTが、送信側の端末11と受信側の機器が同一LAN1に接続されていたならば、それを超えないであろう時間である。すなわち応答時間RTTが規定時間TLより大きければ、受信側の機器は送信側の端末11と同一のLAN1に接続されていないと判定することができる。一方、応答時間RTTが規定時間TLより大きくない（それ以下である場合）、受信側の機器は送信側の端末11と同一LAN1に接続されていると判定することができる。

20

【0137】

ステップS61で、YESの判定がなされたとき（第i回目の応答時間RTT計測で、受信側の機器が送信側の端末11と同一のLAN1に接続されているものではないと判定されたとき）、ステップS62に進み、制御判定部58は、カウンタiの値がkより小さい値かな否か（応答時間RTT計測がk回リトライされたかな否か）を判定し、小さいと判定した場合（応答時間RTT計測がまだk回行われていない場合）、ステップS63に進み、カウンタiの値が1だけインクリメントされる。このとき期待値生成部52は、カウンタiの新たな値に対応する期待値QRiを応答認証部57に供給し、認証データ生成部53は、カウンタiの新たな値に対応する認証データRSiを、応答要求コマンド送信部55に供給する。

30

【0138】

その後ステップS55に戻り、それ以降の処理が行われる。すなわち応答時間RTTが規定時間TL内になる応答メッセージMCRが得られるまで、最大k回、応答時間RTTの計測が行われる。

【0139】

ステップS61で、NOの判定がなされたとき（応答時間RTTが規定時間TL以下となる応答メッセージMCRが得られたとき）、ステップS64に進む。

40

【0140】

ステップS64に進み、制御判定部58は、受信側の機器は、送信データを送信できる機器（正規の機器であって、送信側の端末11と同じLAN1に接続されている機器）である旨を、通信部23（図3）に通知する。これにより通信部23は、所定の送信データを送信データ格納部24から読み出して、受信側の機器（端末11）に送信する。

【0141】

ステップS62で、カウンタiの値が、k以上であると判定された場合（応答時間RTTの計測をk回行っても、応答時間RTTが規定時間TL以下になる応答が得られなかった場合）、ステップS65に進み、制御判定部58は、受信側の機器は、ローカルネットワーク外

50

の機器（送信側の端末 1 1 と同じ LAN 1 に接続されていない機器）である旨を、制御コマンド通信制御部 5 4 に通知する。これにより制御コマンド通信制御部 5 4 は、受信側の機器の認証が失敗した旨を示す終了コマンド CC を、受信側の機器に送信する。

【0142】

ステップ S 6 0 で、応答の認証データ RR_j とその期待値 QR_i 一致しないと判定された場合、ステップ S 6 6 に進み、制御判定部 5 8 は、受信側の機器は、不正な機器である旨を、制御コマンド通信制御部 5 4 に通知する。これにより制御コマンド通信制御部 5 4 は、受信側の機器の認証が失敗した旨を示す終了コマンド CC を、受信側の機器に送信する。

【0143】

以上のようにして送信可否判定処理が行われる。

10

【0144】

なお以上においては、ステップ S 5 3 において k 個の認証データ RS を生成したが、それに代えて、ステップ S 5 5 において、応答要求コマンド MC を送信する毎にそのコマンドに使う認証データ RS を毎回生成するようにしてもよい。

【0145】

次に、図 1 0 の応答制御部 2 2 の動作を、図 1 2 のフローチャートを参照して説明する。

【0146】

ステップ S 8 1 において、受信側の端末 1 1 の応答制御部 2 2 の制御応答通信制御部 7 1 は、送信側の機器と協働して、TCP コネクションを確立し、その TCP コネクションを介して送信側の機器から送信されてきた、開始コマンド CC（ステップ S 5 1）を受信する。制御応答通信制御部 7 1 は、受信した開始コマンド CC に含まれているランダムチャレンジ RC を、期待値生成部 7 2 および認証データ生成部 7 3 に供給する。

20

【0147】

次にステップ S 8 2 において、応答要求コマンド受信部 7 5 は、送信側の機器から送信されてくる応答要求コマンド MC を受信するための UDP ポート番号 pb を決定する。

【0148】

応答要求コマンド受信部 7 5 はまた、制御コマンド CC に含まれている送信側の機器が実行可能な応答時間 RTT 計測のリトライ数 k_s と、受信側の端末 1 1 が対応可能な応答時間 RTT の計測のリトライ数のいずれか小さい方を、今回の応答時間 RTT の計測のリトライ数 k に決定する。

30

【0149】

ステップ S 8 3 において、制御応答通信制御部 7 1 は、ステップ S 8 1 で受信された制御コマンド CC に含まれていたセッション番号 SID、応答時間 RTT の計測のリトライ数 k、および UDP ポート番号 pb を含む応答メッセージ CCR を、ステップ S 8 1 で確立された TCP コネクトを介して送信側の機器に送信する。送信側の機器は、ここで送信された応答メッセージ CCR を受信する（ステップ S 5 2）。

【0150】

ステップ S 8 4 において、認証データ生成部 7 3 は、制御応答通信制御部 7 1 から供給されたランダムチャレンジ RC に対して鍵付きハッシュ処理を施して、応答の認証データ RR を生成する。

40

【0151】

この例の場合、応答時間 RTT 計測が最大 k 回行われるので（応答要求コマンド MC の応答メッセージ MCR が最大 k 回送信されるので）、送信され得る k 個の応答メッセージ MCR それぞれの認証データ RR が生成される。

【0152】

期待値生成部 7 2 は、制御応答通信制御部 7 1 から供給されたランダムチャレンジ RC に対して、送信側の端末 1 1 の送信可否判定部 2 1（認証データ生成部 5 3）における鍵付きハッシュ処理と同様の鍵付きハッシュ処理を施し、送信側の端末 1 1 の認証データ RS の期待値 QS を生成する。

50

【0153】

この例の場合、応答時間RTT計測が最大k回行われるので（応答要求コマンドMCが最大k回受信されるので）、受信され得るk個の応答要求コマンドMCに含まれる認証データRSそれぞれの期待値QSが生成される。

【0154】

ステップS85において、コマンド認証部76に内蔵されているカウンタjの値が1に初期設定される。

【0155】

ステップS86において、コマンドが受信されるまで待機され、コマンドが受信されたと判定された場合、ステップS87に進み、受信されたコマンドが応答要求コマンドMC（ステップS55）であるか否かを判定し、応答要求コマンドMCであると判定された場合、ステップS88に進む。 10

【0156】

ステップS88において、受信されたコマンドに含まれるシーケンス番号Ciとカウンタjが比較され、シーケンス番号Ciがカウンタj以上の値であることが確認される。カウンタj以上の値である場合、ステップS89に進み、カウンタjがシーケンス番号Ciの値に設定される。

【0157】

これは、コマンドが欠落した場合、順番どおりに来なかった場合に、カウンタjをシーケンス番号Ciに合致させるための対策である。 20

【0158】

期待値生成部72はこのとき、カウンタjの値に対応する期待値QS（例えば、第j番目に生成された期待値QSj）をコマンド認証部76に供給する。また認証データ生成部73は、カウンタjの値に対応する認証データRRjを、応答送信部74に供給する。

【0159】

次にステップS90において、コマンド認証部76は、応答要求コマンド受信部75により受信された応答要求コマンドMCに組み込まれている認証データRSiと、期待値生成部72により生成された期待値QSj（カウンタjが示す順番に生成された期待値）とが一致するか否かを判定し、一致すると判定した場合、送信側の端末11を、本情報通信システムにおける正規の端末であると認証し、ステップS91に進む。 30

【0160】

ステップS91において、コマンド認証部76は、送信側の端末11が正規の機器である旨を、応答送信部74に通知する。これにより応答送信部74は、セッション番号SID、カウンタjの値を表すシーケンス番号Cj、認証データ生成部73から供給された認証データRRjを含む応答メッセージMCRを、送信側の機器に送信する。

【0161】

一方ステップS90で、一致しないと判定された場合、ステップS92に進み、コマンド認証部76は、その旨を、応答送信部74に通知する。これにより応答送信部74は、セッション番号SID、カウンタjの値を表すシーケンス番号Cj、および送信側の機器における受信側の機器の認証（ステップS60）が失敗するような認証データRR（=××）を含む応答メッセージMCRを、送信側の機器に送信する。 40

【0162】

ステップS91又はステップS92で、応答メッセージMCRが送信されたとき、ステップS93で、カウンタjの値が1だけインクリメントされ、その後、ステップS86に戻り、それ以降の処理が実行される。

【0163】

また、ステップS88において、カウンタjの値が受信されたコマンドに含まれるシーケンス番号Ciよりも小さい場合も、ステップS86に戻り、それ以降の処理が実行される。

【0164】

ステップ S 8 7 で、受信されたコマンドが応答要求コマンドではないと判定された場合（終了コマンド CC（ステップ S 6 5， S 6 6）であるとき）、処理は終了する。

【 0 1 6 5 】

次に図 1 1 のステップ S 5 8 の処理について説明する。ステップ S 5 8 の処理では、受信側の機器からの応答メッセージ MCR のシーケンス番号 Cj と応答要求コマンド MC のシーケンス番号 Ci（カウンタ i の値）が一致するか否かが判定されるが、このように応答要求コマンド MC と応答メッセージ MCR の対応関係を確認するようにしたので、応答要求コマンド MC に対応しない応答メッセージ MCR（他の応答要求コマンド MC の応答メッセージ MCR）に基づいて応答時間 RTT による距離判定が行われない。

【 0 1 6 6 】

例えば、図 1 3 に示すように、受信側の機器で、第 1 番目の応答要求コマンド MC に対する応答メッセージ MCR の送信に時間がかかり（ステップ S 9 1， S 9 2）、送信側の端末 1 1 で、タイムアウトと判定されて（ステップ S 5 7）、第 2 番目の応答要求コマンド MC が受信側の機器に送信されたものとする。第 1 番目の応答要求コマンド MC に対する応答メッセージ MCR は、第 2 番目の応答要求コマンド MC が送信された後（ステップ S 5 5）、第 2 番目の応答要求コマンド MC との関係でタイムアウトとならない間（ステップ S 5 7）に送信側の端末 1 1 に受信されたものとする（ステップ S 5 6）。

【 0 1 6 7 】

しかしながらこの場合本開示では、受信側の機器からの第 1 番目の応答メッセージ MCR のシーケンス番号（＝ 1）と、第 2 番目の応答要求コマンド MC のシーケンス番号（＝ 2）が一致しないと判定され、送信側の端末 1 1 は、第 2 番目の応答要求コマンド MC に対する応答メッセージ MCR が受信されるまで待機することになり（ステップ S 5 6 に戻る）、対応しない応答メッセージ MCR が受信されても応答時間 RTT による距離判定は行われない。

【 0 1 6 8 】

次に、不正に対する端末 1 1 の動作を具体的に説明する。

【 0 1 6 9 】

例えば図 8 に示した送信機器と同一の LAN 1 に接続された不正な機器 x が、受信機器から応答を得るために応答要求コマンドを送信するものとする。しかしながら、機器 x は、受信機器と共有する秘密鍵を有していないので、受信機器での送信機器の認証に必要な認証データ RS を得ることができない。したがって図 1 4 に示すように、機器 x が、不適当な認証データ RS（＝？）を含む応答要求コマンド MC を受信機器に送信するが、受信機器からは、受信機器の認証が失敗する認証データ RR（＝××）を含む応答メッセージ MCR が送信されてくる（ステップ S 9 2）。したがって機器 x が、その後、送信機器からの応答要求コマンド MC に対して、その応答メッセージ MCR を送信機器に送信して応答しても、送信機器において、機器 x は認証されず、送信データは機器 x に送信されない。

【 0 1 7 0 】

そこで図 1 5 に示すように、不正の機器 x は、送信機器から応答要求コマンド MC を受けてそれを受信機器に送信し、受信機器から、適当な認証データ RR を含む応答メッセージ MCR を取得する。そして機器 x は、取得した応答メッセージ MCR を、送信機器に送信することも考えられる。

【 0 1 7 1 】

しかしながらこの例の場合、応答要求コマンド MC は、送信機器から機器 x、そして機器 x から受信機器に送信され、応答メッセージ MCR が、受信機器から機器 x に、そして機器 x から送信機器へ伝送されるので、応答要求コマンド MC と応答メッセージ MCR の伝送路が、通常の伝送経路（送信機器と受信機器間の伝送路）より長くなる。したがってこの場合、結局応答時間 RTT が規定時間 TL より長くなるので、機器 x は、送信機器と同一 LAN 1 に接続されていないものとして、機器 x には送信データが提供されない。

【 0 1 7 2 】

上述した一連の処理は、ハードウェアにより実現させることもできるが、ソフトウェアにより実現させることもできる。一連の処理をソフトウェアにより実現する場合には、そ

10

20

30

40

50

のソフトウェアを構成するプログラムがコンピュータにインストールされ、そのプログラムがコンピュータで実行されることより、上述した送信可否判定部 2 1 および応答制御部 2 2 が機能的に実現される。

【0173】

図 1 6 は、上述のような送信可否判定部 2 1 および応答制御部 2 2 として機能するコンピュータ 1 0 1 の一実施の形態の構成を示すブロック図である。CPU (Central Processing Unit) 1 1 1 にはバス 1 1 5 を介して入出力インタフェース 1 1 6 が接続されており、CPU 1 1 1 は、入出力インタフェース 1 1 6 を介して、ユーザから、キーボード、マウスなどよりなる入力部 1 1 7 から指令が入力されると、例えば、ROM (Read Only Memory) 1 1 2、ハードディスク 1 1 4、又はドライブ 1 2 0 に装着される磁気ディスク 1 3 1、光ディスク 1 3 2、光磁気ディスク 1 3 3、若しくは半導体メモリ 1 3 4 などの記録媒体に格納されているプログラムを、RAM (Random Access Memory) 1 1 3 にロードして実行する。これにより、上述した各種の処理が行われる。さらに、CPU 1 1 1 は、その処理結果を、例えば、入出力インタフェース 1 1 6 を介して、LCD (Liquid Crystal Display) などよりなる出力部 1 1 8 に必要に応じて出力する。なお、プログラムは、ハードディスク 1 1 4 や ROM 1 1 2 に予め記憶しておき、コンピュータ 1 0 1 と一体的にユーザに提供したり、磁気ディスク 1 3 1、光ディスク 1 3 2、光磁気ディスク 1 3 3、半導体メモリ 1 3 4 等のパッケージメディアとして提供したり、衛星、ネットワーク等から通信部 1 1 9 を介してハードディスク 1 1 4 に提供することができる。

【0174】

なお、本明細書において、記録媒体により提供されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【0175】

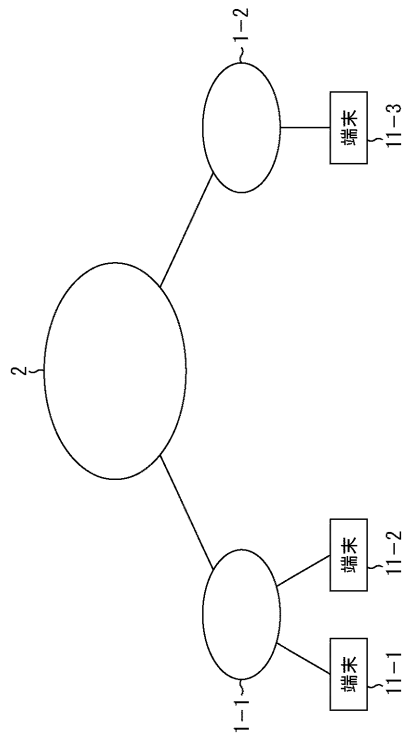
また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【符号の説明】

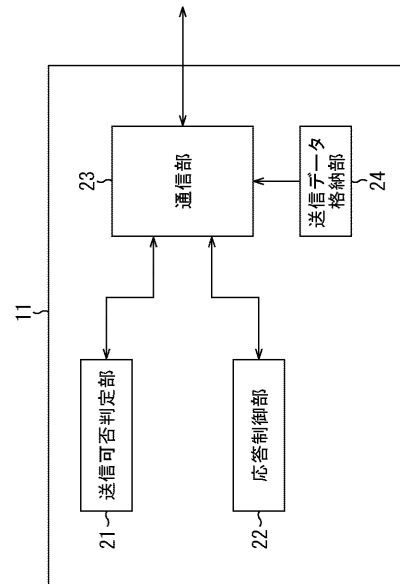
【0176】

1 LAN, 1 1 端末, 2 1 送信可否判定部, 2 2 応答制御部, 2 3 通信部, 2 4 送信データ格納部, 3 1 ランダムチャレンジ生成部, 3 2 ランダムチャレンジ送信制御部, 3 3 期待値生成部, 3 4 コマンド送信制御部, 3 5 判別部, 3 6 応答時間計測部, 4 1 ランダムチャレンジ受信制御部, 4 2 認証データ生成部, 4 3 応答メッセージ生成部, 4 4 応答メッセージ送信制御部, 5 1 ランダムチャレンジ生成部, 5 2 期待値生成部, 5 3 認証データ生成部, 5 4 制御コマンド通信制御部, 5 5 応答要求コマンド送信部, 5 6 応答受信部, 5 7 応答認証部, 5 8 制御判定部, 5 9 応答時間計測部, 7 1 制御応答通信制御部, 7 2 期待値生成部, 7 3 認証データ生成部, 7 4 応答送信部, 7 5 応答要求コマンド受信部, 7 6 コマンド認証部

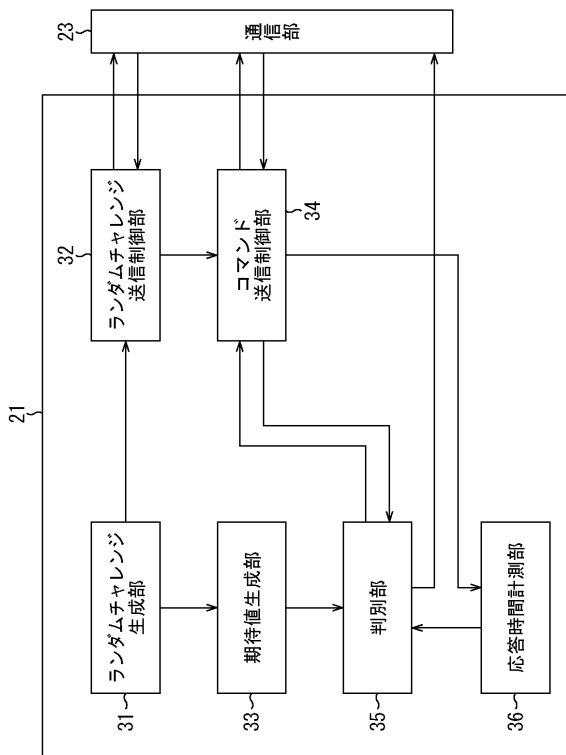
【図1】
図1



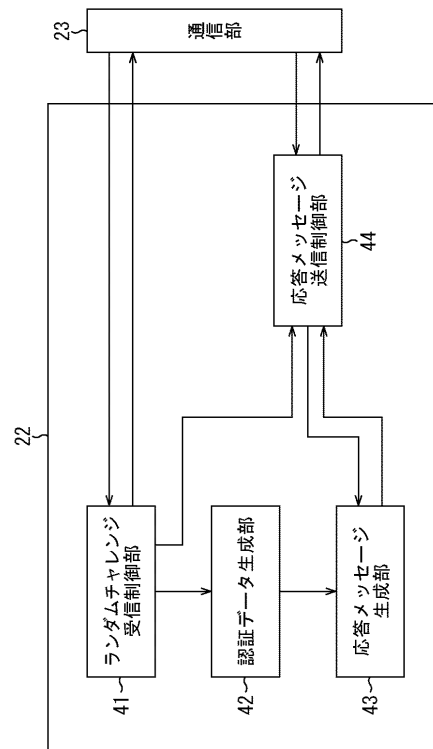
【図2】
図2



【図3】
図3

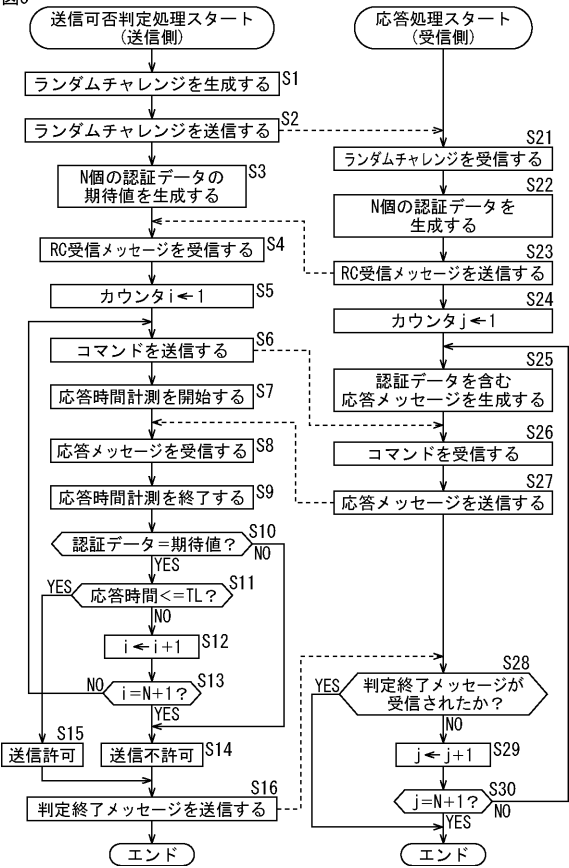


【図4】
図4



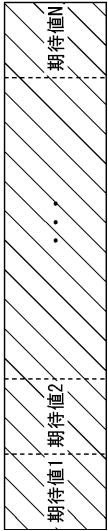
【図 5】

図5



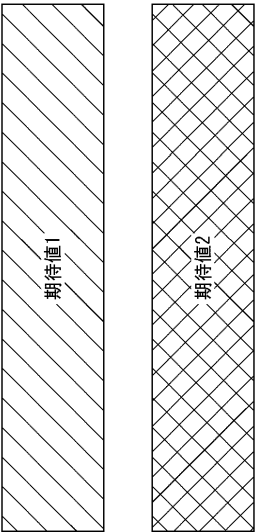
【図 6】

図6



【図 7】

図7

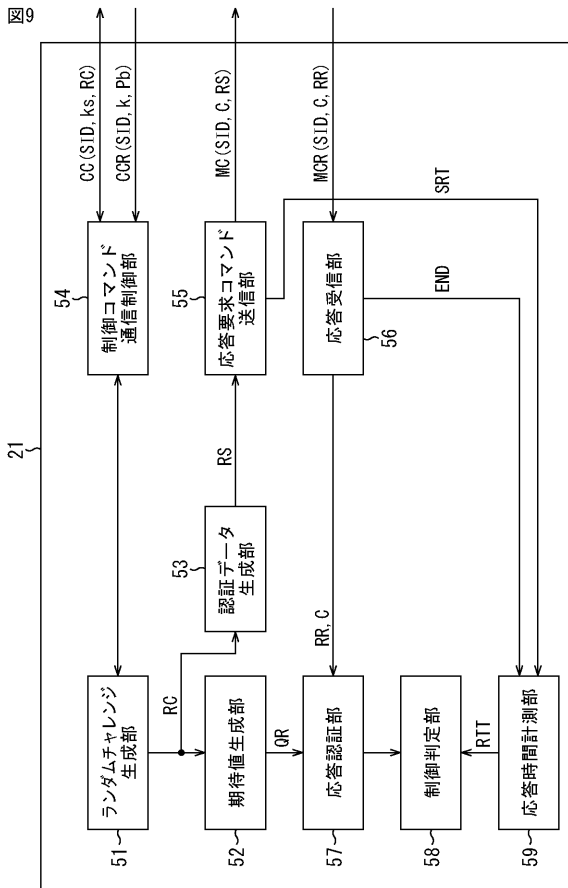


【図 8】

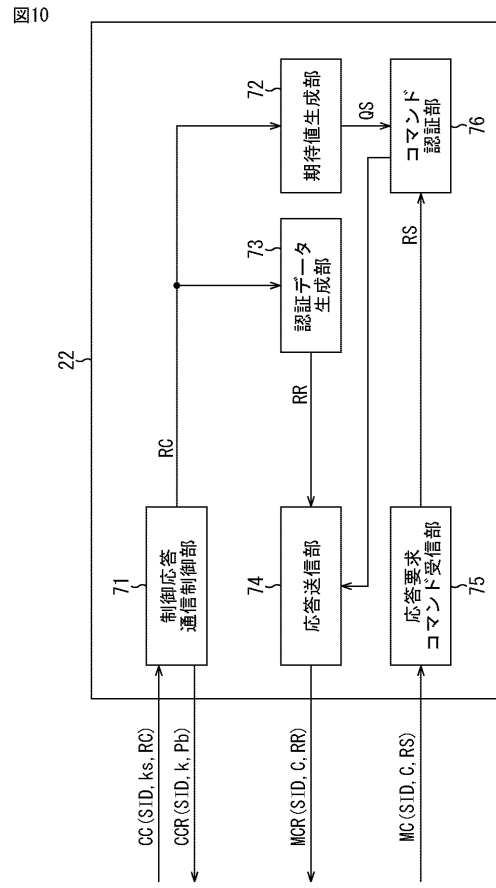
図8



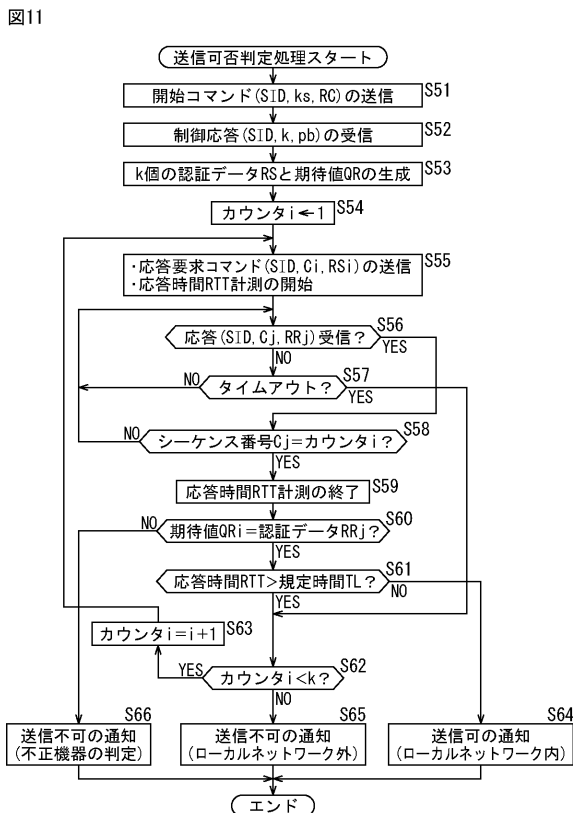
【図 9】



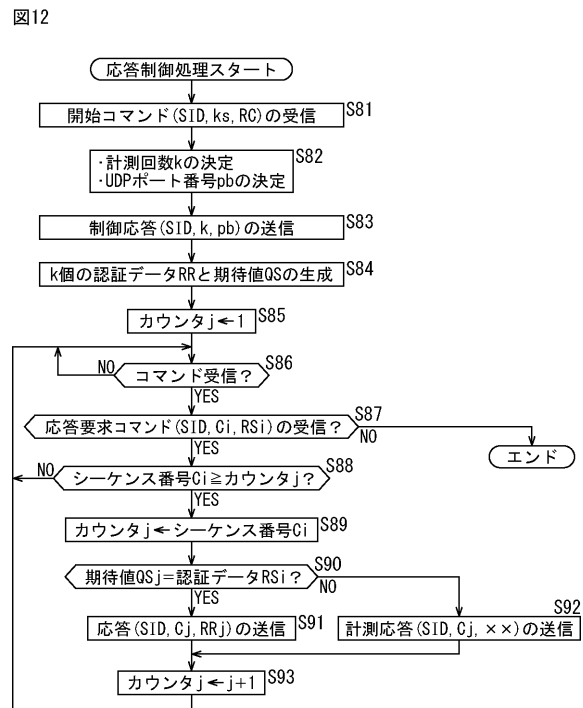
【図 10】



【図 11】

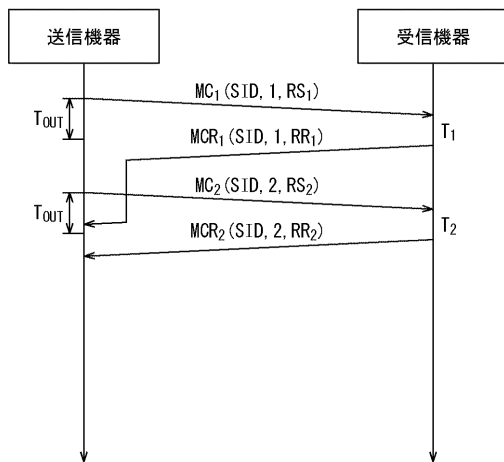


【図 12】



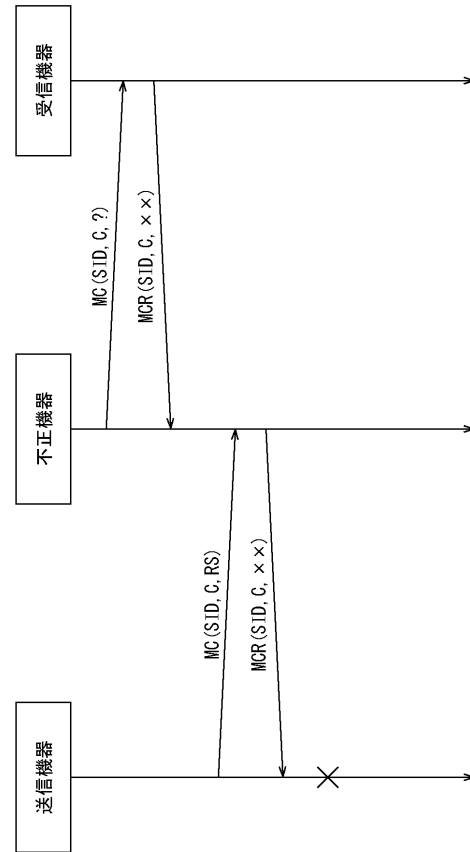
【図 13】

図13



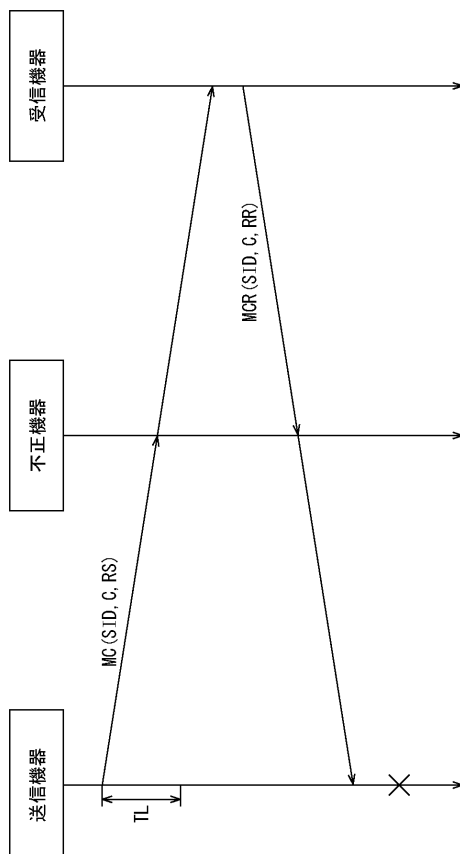
【図 14】

図14



【図 15】

図15



【図 16】

図16

