

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第4223698号
(P4223698)

(45) 発行日 平成21年2月12日(2009.2.12)

(24) 登録日 平成20年11月28日(2008.11.28)

(51) Int.Cl.

F 1

HO4W 84/12	(2009.01)	HO 4 L	12/28	300Z
G06F 1/00	(2006.01)	G06F	1/00	370E
HO4W 12/00	(2009.01)	HO 4 B	7/26	109R

請求項の数 28 (全 33 頁)

(21) 出願番号	特願2001-183315 (P2001-183315)
(22) 出願日	平成13年6月18日 (2001.6.18)
(65) 公開番号	特開2002-374261 (P2002-374261A)
(43) 公開日	平成14年12月26日 (2002.12.26)
審査請求日	平成15年2月20日 (2003.2.20)
審判番号	不服2006-4097 (P2006-4097/J1)
審判請求日	平成18年3月6日 (2006.3.6)

(73) 特許権者	000002185 ソニー株式会社 東京都港区港南1丁目7番1号
(74) 代理人	100082131 弁理士 稲本 義雄
(72) 発明者	松野 克巳 東京都品川区北品川6丁目7番35号 ソ ニー株式会社内

合議体
 審判長 石井 研一
 審判官 萩原 義則
 審判官 柳下 勝幸

最終頁に続く

(54) 【発明の名称】情報処理装置および方法、情報処理システム、記録媒体、並びにプログラム

(57) 【特許請求の範囲】

【請求項 1】

ネットワークを介して他の情報処理装置と接続される情報処理装置において、
 オンオフを入力する入力手段と、
 前記入力手段によりオンまたはオフが入力された入力タイミングを計測する入力タイミング計測手段と、

前記他の情報処理装置より送信されてくる、前記他の情報処理装置の他の入力手段によりオンまたはオフが入力された入力タイミングを受信する入力タイミング受信手段と、

前記入力タイミング計測手段により計測された入力タイミングと、前記入力タイミング受信手段により受信された入力タイミングとを比較する比較手段と、

前記比較手段の比較結果に基づいて、前記他の情報処理装置との認証処理を実行する認証手段と

を備えることを特徴とする情報処理装置。

【請求項 2】

前記ネットワークは、ブルートゥースにより構成される
 ことを特徴とする請求項1に記載の情報処理装置。

【請求項 3】

前記入力タイミング計測手段は、
 前記入力手段によりオンが入力された第1のオンタイミングを計測する第1のオンタイミング計測手段と、

10

20

前記入力手段によりオフが入力された第1のオフタイミングを計測する第1のオフタイミング計測手段とをさらに備え、

前記入力タイミング受信手段は、前記他の情報処理装置より送信されてくる、前記他の情報処理装置の他の入力手段によりオンが入力された第2のオンタイミング、および、オフが入力された第2のオフタイミングを入力タイミングとして受信し、

前記比較手段は、前記第1のオンタイミングと前記第2のオンタイミング、および、前記第1のオフタイミングと前記第2のオフタイミングを、それぞれ比較する

ことを特徴とする請求項1に記載の情報処理装置。

【請求項4】

前記比較手段は、前記第1のオンタイミングと前記第1のオフタイミング、および、前記第2のオンタイミングと第2のオフタイミングとの、それぞれの差を求めて、前記差が所定範囲内であるか否かを比較する

ことを特徴とする請求項3に記載の情報処理装置。

【請求項5】

前記認証手段は、前記それぞれの差が、いずれも前記所定の範囲内であるとき、前記他の情報処理装置を認証する

ことを特徴とする請求項4に記載の情報処理装置。

【請求項6】

前記第1のオンタイミング計測手段、および、前記第1のオフタイミング計測手段は、いずれも複数回数のタイミングを計測し、前記受信手段は、前記他の入力手段により複数回数オンが入力された第2のオンタイミング、および、複数回数オフにされた第2のオフタイミングを受信する

ことを特徴とする請求項3に記載の情報処理装置。

【請求項7】

ネットワークを介して他の情報処理装置と接続される情報処理装置の情報処理方法において、

オンオフを入力する入力ステップと、

前記入力ステップの処理でオンまたはオフが入力された入力タイミングを計測する入力タイミング計測ステップと、

前記他の情報処理装置より送信されてくる、前記他の情報処理装置の他の入力ステップの処理でオンまたはオフが入力された入力タイミングを受信する入力タイミング受信ステップと、

前記入力タイミング計測ステップの処理により計測された入力タイミングと、前記入力タイミング受信ステップの処理により受信された入力タイミングとを比較する比較ステップと、

前記比較ステップの処理での比較結果に基づいて、前記他の情報処理装置との認証処理を実行する認証ステップと

を含むことを特徴とする情報処理方法。

【請求項8】

ネットワークを介して他の情報処理装置と接続される情報処理装置を制御するプログラムであって、

オンオフの入力を制御する入力ステップと、

前記入力制御ステップの処理でオンまたはオフが入力された入力タイミングの計測を制御する入力タイミング計測制御ステップと、

前記他の情報処理装置より送信されてくる、前記他の情報処理装置の他の入力制御ステップの処理でオンまたはオフが入力された入力タイミングの受信を制御する入力タイミング受信制御ステップと、

前記入力タイミング計測制御ステップの処理により計測された入力タイミングと、前記入力タイミング受信制御ステップの処理により受信された入力タイミングとを比較を制御する比較制御ステップと、

10

20

30

40

50

前記比較制御ステップの処理での比較結果に基づいて、前記他の情報処理装置との認証処理の実行を制御する認証制御ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項 9】

ネットワークを介して他の情報処理装置と接続される情報処理装置を制御するコンピュータに、

オンオフの入力を制御する入力ステップと、

前記入力制御ステップの処理でオンまたはオフが入力された入力タイミングの計測を制御する入力タイミング計測制御ステップと、

前記他の情報処理装置より送信されてくる、前記他の情報処理装置の他の入力制御ステップの処理でオンまたはオフが入力された入力タイミングの受信を制御する入力タイミング受信制御ステップと、

前記入力タイミング計測制御ステップの処理により計測された入力タイミングと、前記入力タイミング受信制御ステップの処理により受信された入力タイミングとを比較を制御する比較制御ステップと、

前記比較制御ステップの処理での比較結果に基づいて、前記他の情報処理装置との認証処理の実行を制御する認証制御ステップと

を実行させるプログラム。

【請求項 10】

ネットワークを介して相互に接続される第1の情報処理装置と第2の情報処理装置からなる情報処理システムにおいて、

第1の情報処理装置は、

オンオフを入力する第1の入力手段と、

前記第1の入力手段によりオンまたはオフが入力された第1の入力タイミングを計測する第1の入力タイミング計測手段と、

前記第1のタイミングを前記ネットワークを介して前記第2の情報処理装置に送信する送信手段と

を備え、

第2の情報処理装置は、

オンオフを入力する第2の入力手段と、

前記第2の入力手段によりオンまたはオフが入力された第2の入力タイミングを計測する第2の入力タイミング計測手段と、

前記第1の情報処理装置より送信されてくる、前記第1の入力タイミングを受信する受信手段と、

前記第1の入力タイミングと前記第2の入力タイミングとを比較する比較手段と、

前記比較手段の比較結果に基づいて、前記第1の情報処理装置との認証処理を実行する認証手段と

を備える

ことを特徴とする情報処理システム。

【請求項 11】

前記第1の入力タイミング計測手段は、

前記第1の入力手段によりオンが入力された第1のオンタイミングを計測する第1のオンタイミング計測手段と、

前記第1の入力手段によりオフが入力された第1のオフタイミングを計測する第1のオフタイミング計測手段とをさらに備え、

前記第1の入力タイミングを前記第1のオンタイミングおよび前記第1のオフタイミングとして計測し、

前記第2の入力タイミング計測手段は、

前記第2の入力手段によりオンが入力された第2のオンタイミングを計測する第2の

10

20

30

40

50

オンタイミング計測手段と、

前記第2の入力手段によりオフが入力された第2のオフタイミングを計測する第2のオフタイミング計測手段とをさらに備え、

前記第2の入力タイミングを前記第2のオンタイミングおよび前記第2のオフタイミングとして計測し、

前記送信手段は、前記入力タイミングとして、前記第1のオンタイミング、および、前記第1のオフタイミングを前記ネットワークを介して前記第2の情報処理装置に送信し、

前記受信手段は、前記第1の情報処理装置より送信されてくる、前記第1のオンタイミング、および、前記第1のオフタイミングを前記入力タイミングとして受信し、

前記比較手段は、前記第1のオンタイミングと前記第2のオンタイミング、および、前記第1のオフタイミングと前記第2のオフタイミングとをそれぞれ比較する

ことを特徴とする請求項10に記載の情報処理システム。

【請求項12】

ネットワークを介して相互に接続される第1の情報処理装置と第2の情報処理装置からなる情報処理システムの情報処理方法において、

第1の情報処理装置の情報処理方法は、

オンオフを入力する第1の入力ステップと、

前記第1の入力手段によりオンまたはオフが入力された第1の入力タイミングを計測する第1の入力タイミング計測ステップと、

前記第1の入力タイミングを前記ネットワークを介して前記第2の情報処理装置に送信する送信ステップと

を含み、

第2の情報処理装置の情報処理方法は、

オンオフを入力する第2の入力ステップと、

前記第2の入力ステップの処理でオンまたはオフが入力された第2の入力タイミングを計測する第2の入力タイミング計測ステップと、

前記第1の情報処理装置より送信されてくる、前記第1の入力タイミングを受信する受信ステップと、

前記第1の入力タイミングと前記第2の入力タイミングとを比較する比較ステップと

、

前記比較ステップの処理での比較結果に基づいて、前記第1の情報処理装置との認証処理を実行する認証ステップと

を含む

ことを特徴とする情報処理システムの情報処理方法。

【請求項13】

ネットワークを介して相互に接続される第1の情報処理装置と第2の情報処理装置からなる情報処理システムを制御するプログラムであって、

第1の情報処理装置を制御するプログラムは、

オンオフの入力を制御する第1の入力制御ステップと、

前記第1の入力制御ステップの処理でオンまたはオフが入力された第1の入力タイミングの計測を制御する第1の入力タイミング計測制御ステップと、

前記第1の入力タイミングの前記ネットワークを介した前記第2の情報処理装置への送信を制御する送信制御ステップと

を含み、

第2の情報処理装置を制御するプログラムは、

オンオフの入力を制御する第2の入力制御ステップと、

前記第2の入力制御ステップの処理でオンまたはオフが入力された第2の入力タイミングの計測を制御する第2の入力タイミング計測制御ステップと、

前記第1の情報処理装置より送信されてくる、前記第1の入力タイミングの受信を制御する受信制御ステップと、

10

20

30

40

50

前記第1の入力タイミングと前記第2の入力タイミングとの比較を制御する比較制御ステップと、

前記比較制御ステップの処理での比較結果に基づいた、前記第1の情報処理装置との認証処理の実行を制御する認証制御ステップと

を含む

ことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項14】

ネットワークを介して相互に接続される第1の情報処理装置と第2の情報処理装置からなる情報処理システムを制御するコンピュータのうち、

10

第1の情報処理装置を制御するコンピュータに、

オンオフの入力を制御する第1の入力制御ステップと、

前記第1の入力制御ステップの処理でオンまたはオフが入力された第1の入力タイミングの計測を制御する第1の入力タイミング計測制御ステップと、

前記第1の入力タイミングの前記ネットワークを介した前記第2の情報処理装置への送信を制御する送信制御ステップと

を実行させ、

第2の情報処理装置を制御するコンピュータに、

オンオフの入力を制御する第2の入力制御ステップと、

前記第2の入力制御ステップの処理でオンまたはオフが入力された第2の入力タイミングの計測を制御する第2の入力タイミング計測制御ステップと、

20

前記第1の情報処理装置より送信されてくる、前記第1の入力タイミングの受信を制御する受信制御ステップと、

前記第1の入力タイミングと前記第2の入力タイミングとの比較を制御する比較制御ステップと、

前記比較制御ステップの処理での比較結果に基づいた、前記第1の情報処理装置との認証処理の実行を制御する認証制御ステップと

を実行させるプログラム。

【請求項15】

ネットワークを介して他の情報処理装置と接続される情報処理装置において、

30

オンオフを入力する入力手段と、

前記入力手段によりオンまたはオフが入力された入力タイミングを計測する入力タイミング計測手段と、

前記入力タイミングを前記ネットワークを介して前記他の情報処理装置に送信する送信手段と、

前記他の情報処理装置より送信されてくる、前記送信手段により送信された前記入力タイミングに対応した、前記他の情報処理装置の他の入力手段によりオンまたはオフが入力された入力タイミングを受信する受信手段と、

前記入力タイミング計測手段により計測された入力タイミングと、前記受信手段により受信された前記入力タイミングとを比較する比較手段と、

40

前記比較手段の比較結果に基づいて、前記他の情報処理装置との認証処理を実行する認証手段と

を備えることを特徴とする情報処理装置。

【請求項16】

前記ネットワークは、ブルートゥースにより構成される

ことを特徴とする請求項15に記載の情報処理装置。

【請求項17】

前記入力タイミング計測手段は、

前記入力手段によりオンが入力された第1のオンタイミングを計測する第1のオンタイミング計測手段と、

50

前記入力手段によりオフが入力された第1のオフタイミングを計測する第1のオフタイミング計測手段とをさらに備え、

前記送信手段は、前記入力タイミングを、前記第1のオンタイミング、および、前記第1のオフタイミングとして、前記ネットワークを介して前記他の情報処理装置に送信し、

前記受信手段は、前記他の情報処理装置より送信されてくる、前記送信手段により送信された前記第1のオンタイミング、および、前記第1のオフタイミングに対応した、前記他の情報処理装置の他の入力手段によりオンが入力された第2のオンタイミング、および、オフが入力された第2のオフタイミングを受信し、

前記比較手段は、前記第1のオンタイミングと前記第2のオンタイミング、または、前記第1のオフタイミングと前記第2のオフタイミングとを比較する

ことを特徴とする請求項1-5に記載の情報処理装置。

10

【請求項18】

前記第1のオンタイミング計測手段、および、前記第1のオフタイミング計測手段は、いずれも複数回数のタイミングを計測し、前記受信手段は、前記他の入力手段により複数回数オンが入力された第2のオンタイミング、および、複数回数オフにされた第2のオフタイミングを受信する

ことを特徴とする請求項1-7に記載の情報処理装置。

【請求項19】

前記比較手段は、前記第1のオンタイミングと前記第2のオンタイミング、または、前記第1のオフタイミングと前記第2のオフタイミングとの差を求めて、前記差が所定範囲内になるか否かを比較する

20

ことを特徴とする請求項1-7に記載の情報処理装置。

【請求項20】

前記認証手段は、前記差が、前記所定の範囲内であるとき、前記他の情報処理装置を認証する

ことを特徴とする請求項1-9に記載の情報処理装置。

【請求項21】

ネットワークを介して他の情報処理装置と接続される情報処理装置の情報処理方法において、

オンオフを入力する入力ステップと、

30

前記入力ステップの処理でオンまたはオフが入力された入力タイミングを計測する入力タイミング計測ステップと、

前記入力タイミングを前記ネットワークを介して前記他の情報処理装置に送信する送信ステップと、

前記他の情報処理装置より送信されてくる、前記送信ステップの処理で送信された前記入力タイミングに対応した、前記他の情報処理装置の他の入力ステップの処理でオンまたはオフが入力された入力タイミングを受信する受信ステップと、

前記入力タイミング計測手段により計測された入力タイミングと、前記受信手段により受信された前記入力タイミングとを比較する比較ステップと、

前記比較ステップの処理での比較結果に基づいて、前記他の情報処理装置との認証処理を実行する認証ステップと

40

を含むことを特徴とする情報処理方法。

【請求項22】

ネットワークを介して他の情報処理装置と接続される情報処理装置を制御するプログラムであって、

オンオフの入力を制御する入力制御ステップと、

前記入力制御ステップの処理でオンまたはオフが入力された入力タイミングの計測を制御する入力タイミング計測制御ステップと、

前記入力タイミングの前記ネットワークを介した前記他の情報処理装置への送信を制御する送信制御ステップと、

50

前記他の情報処理装置より送信されてくる、前記送信制御ステップの処理で送信された前記入力タイミングに対応した、前記他の情報処理装置の他の入力制御ステップの処理でオンまたはオフが入力された入力タイミングの受信を制御する受信制御ステップと、

前記入力タイミング計測制御ステップの処理により計測された入力タイミングと、前記受信制御ステップの処理により受信された前記入力タイミングとの比較を制御する比較制御ステップと、

前記比較制御ステップの処理での比較結果に基づいて、前記他の情報処理装置との認証処理の実行を制御する認証制御ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

10

【請求項 2 3】

ネットワークを介して他の情報処理装置と接続される情報処理装置を制御するコンピュータに、

オンオフの入力を制御する入力制御ステップと、

前記入力制御ステップの処理でオンまたはオフが入力された入力タイミングの計測を制御する入力タイミング計測制御ステップと、

前記入力タイミングの前記ネットワークを介した前記他の情報処理装置への送信を制御する送信制御ステップと、

前記他の情報処理装置より送信されてくる、前記送信制御ステップの処理で送信された前記入力タイミングに対応した、前記他の情報処理装置の他の入力制御ステップの処理でオンまたはオフが入力された入力タイミングの受信を制御する受信制御ステップと、

20

前記入力タイミング計測制御ステップの処理により計測された入力タイミングと、前記受信制御ステップの処理により受信された前記入力タイミングとの比較を制御する比較制御ステップと、

前記比較制御ステップの処理での比較結果に基づいて、前記他の情報処理装置との認証処理の実行を制御する認証制御ステップと

を実行させるプログラム。

【請求項 2 4】

ネットワークを介して相互に接続される、オンオフを入力する第1の入力手段と、前記第1の入力手段によりオンまたはオフが入力された第1の入力タイミングを計測する第1の入力タイミング計測手段と、前記第1の入力タイミングを前記ネットワークを介して第2の情報処理装置に送信する第1の送信手段とを備えた第1の情報処理装置と、オンオフを入力する第2の入力手段と、前記第2の入力手段によりオンまたはオフが入力された第2の入力タイミングを計測する第2の入力タイミング計測手段と、前記第2の入力タイミングを前記ネットワークを介して第1の情報処理装置に送信する第2の送信手段とを備えた前記第2の情報処理装置から構成された情報処理システムにおいて、

30

前記第1の情報処理装置は、

前記第2の情報処理装置より送信されてくる、前記第2の入力タイミングを受信する第1の受信手段と、

前記第1の入力タイミングと前記第2の入力タイミングとを比較する第1の比較手段と、

40

前記第1の比較手段の比較結果に基づいて、前記第2の情報処理装置との認証処理を実行する第1の認証手段と

を備え、

前記第2の情報処理装置は、

前記第1の情報処理装置より送信されてくる、前記第1の入力タイミングを受信する第2の受信手段と、

前記第1の入力タイミングと前記第2の入力タイミングとを比較する第2の比較手段と、

前記第2の比較手段の比較結果に基づいて、前記第1の情報処理装置との認証処理を

50

実行する第2の認証手段と
を備える
ことを特徴とする情報処理システム。

【請求項25】

前記第1の入力タイミング計測手段は、

前記第1の入力手段によりオンが入力された第1のオンタイミングを計測する第1の
オンタイミング計測手段と、

前記第1の入力手段によりオフが入力された第1のオフタイミングを計測する第1の
オフタイミング計測手段とをさらに備え、

前記第1のオンタイミング、および、前記第1のオフタイミングを前記第1の入力タ
イミングとして計測し、10

前記第2の入力タイミング計測手段は、

前記第2の入力手段によりオンが入力された第2のオンタイミングを計測する第2の
タイミング計測手段と、

前記第2の入力手段によりオフが入力された第2のオフタイミングを計測する第2の
タイミング計測手段とをさらに備え、

前記第2のオンタイミング、および、前記第2のオフタイミングを前記第2の入力タ
イミングとして計測し、

前記第1の送信手段は、前記第1の入力タイミングのうち、前記第1のオフタイミング
を前記ネットワークを介して第2の情報処理装置に送信し、20

前記第2の送信手段は、前記第2の入力タイミングのうち、前記第2のオンタイミング
を前記ネットワークを介して第1の情報処理装置に送信し、

前記第1の受信手段は、前記第2の情報処理装置より送信されてくる、前記第2の入力
タイミングのうちの前記第2のオンタイミングを受信し、

前記第2の受信手段は、前記第1の情報処理装置より送信されてくる、前記第1の入力
タイミングのうち、前記第1のオフタイミングを受信し、

前記第1の比較手段は、前記第1の入力タイミングのうちの前記第1のオンタイミング
と、前記第2の入力タイミングのうちの前記第2のオンタイミングとを比較し、

前記第2の比較手段は、前記第1の入力タイミングのうちの前記第1のオフタイミング
と、前記第2の入力タイミングのうちの前記第2のオフタイミングとを比較する30

ことを特徴とする請求項24に記載の情報処理システム。

【請求項26】

ネットワークを介して相互に接続される、オンオフを入力する第1の入力手段と、前記
第1の入力手段によりオンまたはオフが入力された第1の入力タイミングを計測する第1
の入力タイミング計測手段と、前記第1の入力タイミングを前記ネットワークを介して第
2の情報処理装置に送信する第1の送信手段とを備えた第1の情報処理装置と、オンオフ
を入力する第2の入力手段と、前記第2の入力手段によりオンまたはオフが入力された第
2の入力タイミングを計測する第2の入力タイミング計測手段と、前記第2の入力タイミ
ングを前記ネットワークを介して第1の情報処理装置に送信する第2の送信手段とを備え
た前記第2の情報処理装置から構成された情報処理システムの情報処理方法において、40

前記第1の情報処理装置の情報処理方法は、

前記第2の情報処理装置より送信されてくる、前記第2の入力タイミングを受信する
第1の受信ステップと、

前記第1の入力タイミングと前記第2の入力タイミングとを比較する第1の比較ステ
ップと、

前記第1の比較ステップの処理の比較結果に基づいて、前記第2の情報処理装置との
認証処理を実行する第1の認証ステップと

を含み、

前記第2の情報処理装置の情報処理方法は、

前記第1の情報処理装置より送信されてくる、前記第1の入力タイミングを受信する50

第 2 の受信ステップと、

前記第 1 の入力タイミングと前記第 2 の入力タイミングとを比較する第 2 の比較ステップと、

前記第 2 の比較ステップの処理の比較結果に基づいて、前記第 1 の情報処理装置との認証処理を実行する第 2 の認証ステップと

を含む

ことを特徴とする情報処理システムの情報処理方法。

【請求項 2 7】

ネットワークを介して相互に接続される、オンオフを入力する第 1 の入力手段と、前記第 1 の入力手段によりオンまたはオフが入力された第 1 の入力タイミングを計測する第 1 の入力タイミング計測手段と、前記第 1 の入力タイミングを前記ネットワークを介して第 2 の情報処理装置に送信する第 1 の送信手段とを備えた第 1 の情報処理装置と、オンオフを入力する第 2 の入力手段と、前記第 2 の入力手段によりオンまたはオフが入力された第 2 の入力タイミングを計測する第 2 の入力タイミング計測手段と、前記第 2 の入力タイミングを前記ネットワークを介して第 1 の情報処理装置に送信する第 2 の送信手段とを備えた前記第 2 の情報処理装置から構成された情報処理システムを制御するプログラムであつて、

前記第 1 の情報処理装置を制御するプログラムは、

前記第 2 の情報処理装置より送信されてくる、前記第 2 の入力タイミングの受信を制御する第 1 の受信制御ステップと、

前記第 1 の入力タイミングと前記第 2 の入力タイミングとの比較を制御する第 1 の比較制御ステップと、

前記第 1 の比較制御ステップの処理の比較結果に基づいて、前記第 2 の情報処理装置との認証処理の実行を制御する第 1 の認証制御ステップと

を含み、

前記第 2 の情報処理装置を制御するプログラムは、

前記第 1 の情報処理装置より送信されてくる、前記第 1 の入力タイミングの受信を制御する第 2 の受信制御ステップと、

前記第 1 の入力タイミングと前記第 2 の入力タイミングとの比較を制御する第 2 の比較制御ステップと、

前記第 2 の比較制御ステップの処理の比較結果に基づいて、前記第 1 の情報処理装置との認証処理の実行を制御する第 2 の認証制御ステップと

を含む

ことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項 2 8】

ネットワークを介して相互に接続される、オンオフを入力する第 1 の入力手段と、前記第 1 の入力手段によりオンまたはオフが入力された第 1 の入力タイミングを計測する第 1 の入力タイミング計測手段と、前記第 1 の入力タイミングを前記ネットワークを介して第 2 の情報処理装置に送信する第 1 の送信手段とを備えた第 1 の情報処理装置と、オンオフを入力する第 2 の入力手段と、前記第 2 の入力手段によりオンまたはオフが入力された第 2 の入力タイミングを計測する第 2 の入力タイミング計測手段と、前記第 2 の入力タイミングを前記ネットワークを介して第 1 の情報処理装置に送信する第 2 の送信手段とを備えた前記第 2 の情報処理装置から構成された情報処理システムを制御するコンピュータのうち、

前記第 1 の情報処理装置を制御するコンピュータに、

前記第 2 の情報処理装置より送信されてくる、前記第 2 の入力タイミングの受信を制御する第 1 の受信制御ステップと、

前記第 1 の入力タイミングと前記第 2 の入力タイミングとの比較を制御する第 1 の比較制御ステップと、

10

20

30

40

50

前記第1の比較制御ステップの処理の比較結果に基づいて、前記第2の情報処理装置との認証処理の実行を制御する第1の認証制御ステップと
を含む処理を実行させ、

前記第2の情報処理装置を制御するコンピュータに、

前記第1の情報処理装置より送信されてくる、前記第1の入力タイミングの受信を制御する第2の受信制御ステップと、

前記第1の入力タイミングと前記第2の入力タイミングとの比較を制御する第2の比較制御ステップと、

前記第2の比較制御ステップの処理の比較結果に基づいて、前記第1の情報処理装置との認証処理の実行を制御する第2の認証制御ステップと

を含む処理を実行させるプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報処理装置および方法、情報処理システム、記録媒体、並びにプログラムに関し、特に、簡易に電子機器間の相互認証処理を実行できるようにした情報処理装置および方法、記録媒体、情報処理システム、並びにプログラムに関する。

【0002】

【従来の技術】

ブルートゥースを利用した至近距離での電子機器間の無線通信技術が一般に普及しつつある。

【0003】

ブルートゥースは、2.45GHzの周波数帯域を利用した無線通信技術で、到達距離は最大約10m程度のものである。類似した通信方法として赤外線通信があるが、ブルートゥースの場合は無線通信であるため障害物を通して通信することが可能であり、その点が、赤外線通信と異なり、メリットとなっている。

【0004】

ブルートゥースにより、例えば、図1に示すように、パーソナルコンピュータ(PC:Personal Computer)1とカムコーダ2(図1(A))、携帯電話機3とハンディカムコーダ4(図1(B))、カムコーダ2と携帯情報端末機5(図1(C))、および、携帯型パーソナルコンピュータ6と携帯情報通信端末機5(図1(D))などの間で、無線通信による情報の授受が可能とされる。

【0005】

このように特に配線を必要としないブルートゥースの無線接続により、例えば、携帯情報端末機5のデータを異なる部屋に存在する携帯型パーソナルコンピュータ6に転送したり、携帯電話機3をユーザの衣服のポケットに入れたままハンディカムコーダ4と接続し、ハンディカムコーダ4に記録されている映像をインターネットを介して他の電子機器に送信するということも可能である。

【0006】

これらの電子機器間での通信を行うためには、通信による誤動作、誤接続、または、データ転送時のデータの漏洩などを防止するため、それぞれの電子機器間で、1回目の通信で相互認証処理を実行させる。このとき、ユーザは必要に応じて、英数字などからなるパスワードの入力を、それぞれの電子機器で行い、認証処理を実行させる。

【0007】

ここで、例えば、図1(A)で示す、パーソナルコンピュータ1とカムコーダ2の間で最初に行われる認証処理について、図2のフローチャートを参照して説明する。

【0008】

ステップS1において、パーソナルコンピュータ1(以下においては、PC1とも称する)は、キーボードなどの入力部より、ブルートゥースの規格上でPIN(Personal Identification Number)と呼ばれるユーザを特定するパスワードが入力されたか否かを判定し、入

10

20

30

40

50

力されるまでその処理を繰り返し、入力されたと判定された場合、その処理は、ステップS2に進む。このとき、カムコーダ2も、ステップS21において、同様の処理を実行する。

【0009】

ステップS2において、PC1は、乱数R0を発生しカムコーダ2に送信し、ステップS3において、乱数R0、PIN、および、BDADDR-Cam(Blue-tooth Device Address for Camcoder:カムコーダ2を識別する固有の番号)から所定の関数E22により共通鍵E22(R0,PIN,BDADDR-Cam)を演算する。ここで、BDADDR-Camは、ユーザがPC1と接続しようとする電子機器(今の場合、カムコーダ2)を指定することで選択される。

【0010】

ステップS22において、カムコーダ2は、ステップS3の処理でPC1が使用したものと同様の関数E22により、乱数R0、PIN、および、BDADDR-Camから共通鍵CK(=E22(R0,PIN,BDADDR-Cam))を演算し、PC1の応答として送信する。

【0011】

ステップS4において、PC1は、認証用の乱数R1を発生し、カムコーダ2に送信すると共に、ステップS5において、乱数R1、共通鍵CK、および、BDADDR-Camより、関数E1を用いてパスワードA(=E1(R1,CK,BDADDR-Cam))を演算する。

【0012】

このとき、ステップS23において、カムコーダ2は、PC1より送信されてきた乱数R1、共通鍵、および、BDADDR-Camより、ステップS4の処理でPC1により使用されたものと同様の関数E1によりパスワードA'(=E1(R1,CK,BDADDR-Cam))を演算し、PC1に送信する。

【0013】

ステップS6において、PC1は、自らが演算したパスワードAと、カムコーダ2より送信されてきたパスワードA'が一致するか否かを判定し、一致したと判定した場合、ステップS7において、パスワードが一致したことをカムコーダ2に通知する。

【0014】

ステップS24において、カムコーダ2は、PC1からの通知を受信し、ステップS25において、パスワードAとパスワードA'が一致したか否かを判定する。今の場合、ステップS7の処理によりパスワードが一致している通知がPC1より送信されてきているので、ステップS26において、認証用の乱数R2を発生し、PC1に送信すると共に、ステップS27において、乱数R2、共通鍵CK、および、BDADDR-PCより、認証用の関数パスワードB(=E1(R2,CK,BDADDR-PC))を生成する。一方、ステップS8において、PC1は、カムコーダ2より送信されてきた乱数R2、共通鍵CK、および、BDADDR-PCより、関数E1を使用してパスワードB'(=E1(R2,CK,BDADDR-PC))を演算し、カムコーダ2に送信する。

【0015】

ステップS28において、カムコーダ2は、パスワードBとパスワードB'が一致したか否かを判定し、一致したと判定した場合、その処理は、ステップS29において、認証が認められたことを認識し、同時に、パスワードBとパスワードB'が一致したことをPC1に送信する。ステップS9において、PC1は、通知を受信し、パスワードが一致し、認証が認められたことを認識する。

【0016】

ステップS6において、パスワードAとパスワードA'が一致しないと判定された場合、ステップS10において、パスワードAとパスワードA'が一致しなかったことをカムコーダ2に通知し、その処理を終了する。

【0017】

この場合、ステップS24では、パスワードAとパスワードA'が一致しなかったことを示す通知が、カムコーダ2に受信されるので、ステップS25において、カムコーダ2は、パスワードAとパスワードA'が一致しなかったと判定し、その処理は、終了する。

【0018】

10

20

30

40

50

ステップS28において、パスワードBとパスワードB'が一致しないと判定された場合、ステップS30において、カムコーダ2は、認証が認められないと認識し、パスワードBとパスワードB'が一致しなかったことを示す通知をPC1に送信する。

【0019】

そして、2回目以降の接続では、通信させようとする電子機器が、1回目の認証処理で記憶されたパスワードや、最初の接続で生成された共通鍵CKなどを利用して自動認証を行うことにより、ユーザによるパスワードの入力処理が省略されるようになっている。

【0020】

【発明が解決しようとする課題】

しかしながら、上記のような構成では、PC1とカムコーダ2や、LAN (Local Area Network) 内の無線アクセスポイントに接続するなど、固定的な通信相手に対して行う場合、あまり問題とならないが、例えば、PC1上で実行させるアプリケーションソフトウェアなどにより他の電子機器と一緒に画像データなどを交換し、次のタイミングでは、通信相手を変えるような場合、新しい接続相手となる他の電子機器と接続する度に、毎回パスワードの入力が必要となるため、その処理が面倒なものであったと言う課題があった。

【0021】

本発明はこのような状況に鑑みてなされたものであり、ブルートゥースによる無線通信を実行する際、最初の相互認証を簡易な処理で実行できるようにするものである。

【0023】

前記ネットワークは、ブルートゥースにより構成されるようにすることができる。

10

【0024】

前記オンタイミング計測手段、および、オフタイミング計測手段には、いずれも複数回数のタイミングを計測させるようにすることができる。

【0028】

【課題を解決するための手段】

本発明の第1の情報処理装置は、オンオフを入力する入力手段と、入力手段によりオンまたはオフが入力された入力タイミングを計測する入力タイミング計測手段と、他の情報処理装置より送信されてくる、他の情報処理装置の他の入力手段によりオンまたはオフが入力された入力タイミングを受信する入力タイミング受信手段と、入力タイミング計測手段により計測された入力タイミングと、入力タイミング受信手段により受信された入力タイミングとを比較する比較手段と、比較手段の比較結果に基づいて、他の情報処理装置との認証処理を実行する認証手段とを備えることを特徴とする。

30

【0029】

前記ネットワークは、ブルートゥースにより構成されるようにすることができる。

【0030】

前記入力タイミング計測手段には、入力手段によりオンが入力された第1のオンタイミングを計測する第1のオンタイミング計測手段と、入力手段によりオフが入力された第1のオフタイミングを計測する第1のオフタイミング計測手段とをさらに設けるようにさせることができ、入力タイミング受信手段には、他の情報処理装置より送信されてくる、他の情報処理装置の他の入力手段によりオンが入力された第2のオンタイミング、および、オフが入力された第2のオフタイミングを入力タイミングとして受信せざるようにすることができ、比較手段には、第1のオンタイミングと第2のオンタイミング、および、第1のオフタイミングと第2のオフタイミングを、それぞれ比較せざるようにすることができる。

40

前記比較手段には、第1のオンタイミングと第1のオフタイミング、および、第2のオンタイミングと第2のオフタイミングとの、それぞれの差を求めて、差が所定範囲内であるか否かを比較せざるようにすることができる。

【0031】

前記認証手段には、それぞれの差が、いずれも所定の範囲内であるとき、他の情報処理装置を認証せざるようにすることができる。

50

【0032】

前記第1のオンタイミング計測手段、および、第1のオフタイミング計測手段には、いずれも複数回数のタイミングを計測させるようにすることができ、受信手段には、他の入力手段により複数回数オンが入力された第2のオンタイミング、および、複数回数オフにされた第2のオフタイミングを受信させるようにすることができる。

【0033】

本発明の第1の情報処理方法は、オンオフを入力する入力ステップと、入力ステップの処理でオンまたはオフが入力されたタイミングを計測する入力タイミング計測ステップと、他の情報処理装置より送信されてくる、他の情報処理装置の他の入力ステップの処理でオンまたはオフが入力された入力タイミングを受信する入力タイミング受信ステップと、入力タイミング計測ステップの処理により計測された入力タイミングと、入力タイミング受信ステップの処理により受信された入力タイミングとを比較する比較ステップと、比較ステップの処理での比較結果に基づいて、他の情報処理装置との認証処理を実行する認証ステップとを含むことを特徴とする。

10

【0034】

本発明の第1の記録媒体のプログラムは、オンオフの入力を制御する入力ステップと、入力制御ステップの処理でオンまたはオフが入力された入力タイミングの計測を制御する入力タイミング計測制御ステップと、他の情報処理装置より送信されてくる、他の情報処理装置の他の入力制御ステップの処理でオンまたはオフが入力された入力タイミングの受信を制御する入力タイミング受信制御ステップと、入力タイミング計測制御ステップの処理により計測された入力タイミングと、入力タイミング受信制御ステップの処理により受信された入力タイミングとを比較を制御する比較制御ステップと、比較制御ステップの処理での比較結果に基づいて、他の情報処理装置との認証処理の実行を制御する認証制御ステップとを含むことを特徴とする。

20

【0035】

本発明の第1のプログラムは、オンオフの入力を制御する入力ステップと、入力制御ステップの処理でオンまたはオフが入力された入力タイミングの計測を制御する入力タイミング計測制御ステップと、他の情報処理装置より送信されてくる、他の情報処理装置の他の入力制御ステップの処理でオンまたはオフが入力された入力タイミングの受信を制御する入力タイミング受信制御ステップと、入力タイミング計測制御ステップの処理により計測された入力タイミングと、入力タイミング受信制御ステップの処理により受信された入力タイミングとを比較を制御する比較制御ステップと、比較制御ステップの処理での比較結果に基づいて、他の情報処理装置との認証処理の実行を制御する認証制御ステップとを実行させる。

30

【0036】

本発明の第1の情報処理システムは、第1の情報処理装置が、オンオフを入力する第1の入力手段と、第1の入力手段によりオンまたはオフが入力された第1の入力タイミングを計測する第1の入力タイミング計測手段と、第1の入力タイミングをネットワークを介して第2の情報処理装置に送信する送信手段とを備え、第2の情報処理装置が、オンオフを入力する第2の入力手段と、第2の入力手段によりオンまたはオフが入力された第2の入力タイミングを計測する第2の入力タイミング計測手段と、第1の情報処理装置より送信されてくる、第1の入力タイミングを受信する受信手段と、第1の入力タイミングと第2の入力タイミングとを比較する比較手段と、比較手段の比較結果に基づいて、第1の情報処理装置との認証処理を実行する認証手段とを備えることを特徴とする。

40

第1の入力タイミング計測手段には、第1の入力手段によりオンが入力された第1のオンタイミングを計測する第1のオンタイミング計測手段と、第1の入力手段によりオフが入力された第1のオフタイミングを計測する第1のオフタイミング計測手段とをさらに設けるようにさせることができ、第1の入力タイミングを第1のオンタイミングおよび第1のオフタイミングとして計測せしめるようにすることができ、第2の入力タイミング計測手段には、第2の入力手段によりオンが入力された第2のオンタイミングを計測する第2の

50

オンラインタイミング計測手段と、第2の入力手段によりオフが入力された第2のオフタイミングを計測する第2のオフタイミング計測手段とをさらに設けるようにさせることができ、第2の入力タイミングを第2のオンラインおよび第2のオフタイミングとして計測させようすることができ、送信手段には、入力タイミングとして、第1のオンライン、および、第1のオフタイミングをネットワークを介して第2の情報処理装置に送信させようすることができ、受信手段には、第1の情報処理装置より送信されてくる、第1のオンライン、および、第1のオフタイミングを入力タイミングとして受信せらるようすることができ、比較手段には、第1のオンラインと第2のオンライン、および、第1のオフタイミングと第2のオフタイミングとをそれぞれ比較せらるようすることができる。

10

【0037】

本発明の第1の情報処理システムの情報処理方法は、第1の情報処理装置の情報処理方法が、オンオフを入力する第1の入力ステップと、第1の入力手段によりオンまたはオフが入力された第1の入力タイミングを計測する第1の入力タイミング計測ステップと、第1の入力タイミングをネットワークを介して第2の情報処理装置に送信する送信ステップとを含み、第2の情報処理装置の情報処理方法は、オンオフを入力する第2の入力ステップと、第2の入力ステップの処理でオンまたはオフが入力された第2の入力タイミングを計測する第2の入力タイミング計測ステップと、第1の情報処理装置より送信されてくる、第1の入力タイミングを受信する受信ステップと、第1の入力タイミングと第2の入力タイミングとを比較する比較ステップと、比較ステップの処理での比較結果に基づいて、第1の情報処理装置との認証処理を実行する認証ステップとを含むことを特徴とする。

20

【0038】

本発明の第2の記録媒体のプログラムは、第1の情報処理装置を制御するプログラムが、オンオフの入力を制御する第1の入力制御ステップと、第1の入力制御ステップの処理でオンまたはオフが入力された第1の入力タイミングの計測を制御する第1の入力タイミング計測制御ステップと、第1の入力タイミングのネットワークを介した第2の情報処理装置への送信を制御する送信制御ステップとを含み、第2の情報処理装置を制御するプログラムが、オンオフの入力を制御する第2の入力制御ステップと、第2の入力制御ステップの処理でオンまたはオフが入力された第2の入力タイミングの計測を制御する第2の入力タイミング計測制御ステップと、第1の情報処理装置より送信されてくる、第1の入力タイミングの受信を制御する受信制御ステップと、第1の入力タイミングと第2の入力タイミングとの比較を制御する比較制御ステップと、比較制御ステップの処理での比較結果に基づいた、第1の情報処理装置との認証処理の実行を制御する認証制御ステップとを含むことを特徴とする。

30

【0039】

本発明の第2のプログラムは、第1の情報処理装置を制御するコンピュータに、オンオフの入力を制御する第1の入力制御ステップと、第1の入力制御ステップの処理でオンまたはオフが入力された第1の入力タイミングの計測を制御する第1の入力タイミング計測制御ステップと、第1の入力タイミングのネットワークを介した第2の情報処理装置への送信を制御する送信制御ステップとを実行させ、第2の情報処理装置を制御するコンピュータに、オンオフの入力を制御する第2の入力制御ステップと、第2の入力制御ステップの処理でオンまたはオフが入力された第2の入力タイミングの計測を制御する第2の入力タイミング計測制御ステップと、第1の情報処理装置より送信されてくる、第1の入力タイミングの受信を制御する受信制御ステップと、第1の入力タイミングと第2の入力タイミングとの比較を制御する比較制御ステップと、比較制御ステップの処理での比較結果に基づいた、第1の情報処理装置との認証処理の実行を制御する認証制御ステップとを実行させる。

40

【0040】

本発明の第2の情報処理装置は、オンオフを入力する入力手段と、入力手段によりオンまたはオフが入力された入力タイミングを計測する入力タイミング計測手段と、入力タイ

50

ミングをネットワークを介して他の情報処理装置に送信する送信手段と、他の情報処理装置より送信されてくる、送信手段により送信された入力タイミングに対応した、他の情報処理装置の他の入力手段によりオンまたはオフが入力された入力タイミングを受信する受信手段と、入力タイミング計測手段により計測された入力タイミングと、受信手段により受信された入力タイミングとを比較する比較手段と、比較手段の比較結果に基づいて、他の情報処理装置との認証処理を実行する認証手段とを備えることを特徴とする。

【0041】

前記ネットワークは、ブルートゥースにより構成されるようにすることができる。

【0042】

前記入力タイミング計測手段には、入力手段によりオンが入力された第1のオンタイミングを計測する第1のオンタイミング計測手段と、入力手段によりオフが入力された第1のオフタイミングを計測する第1のオフタイミング計測手段とをさらに設けるようにさせることができ、送信手段には、入力タイミングを、第1のオンタイミング、および、第1のオフタイミングとして、ネットワークを介して他の情報処理装置に送信させるようにすることができ、受信手段には、他の情報処理装置より送信されてくる、送信手段により送信された第1のオンタイミング、および、第1のオフタイミングに対応した、他の情報処理装置の他の入力手段によりオンが入力された第2のオンタイミング、および、オフが入力された第2のオフタイミングを受信させるようにすることができ、比較手段には、第1のオンタイミングと第2のオンタイミング、または、第1のオフタイミングと第2のオフタイミングとを比較させるようにすることができる。

10

前記第1のオンタイミング計測手段、および、第1のオフタイミング計測手段には、いずれも複数回数のタイミングを計測させるようにすることができ、受信手段には、他の入力手段により複数回数オンが入力された第2のオンタイミング、および、複数回数オフにされた第2のオフタイミングを受信させるようにすることができる。

20

【0043】

前記比較手段には、第1のオンタイミングと第2のオンタイミング、または、第1のオフタイミングと第2のオフタイミングとの差を求めさせて、差が所定範囲内になるか否かを比較せるようにすることができる。

【0044】

前記認証手段には、差が、所定の範囲内であるとき、他の情報処理装置を認証させるようにすることができる。

30

【0045】

本発明の第2の情報処理方法は、オンオフを入力する入力ステップと、入力ステップの処理でオンまたはオフが入力された入力タイミングを計測する入力タイミング計測ステップと、入力タイミングをネットワークを介して他の情報処理装置に送信する送信ステップと、他の情報処理装置より送信されてくる、送信ステップの処理で送信された入力タイミングに対応した、他の情報処理装置の他の入力ステップの処理でオンまたはオフが入力された入力タイミングを受信する受信ステップと、入力タイミング計測手段により計測された入力タイミングと、受信手段により受信された入力タイミングとを比較する比較ステップと、比較ステップの処理での比較結果に基づいて、他の情報処理装置との認証処理を実行する認証ステップとを含むことを特徴とする。

40

【0046】

本発明の第3の記録媒体のプログラムは、オンオフの入力を制御する入力制御ステップと、入力制御ステップの処理でオンまたはオフが入力された入力タイミングの計測を制御する入力タイミング計測制御ステップと、入力タイミングのネットワークを介した他の情報処理装置への送信を制御する送信制御ステップと、他の情報処理装置より送信されてくる、送信制御ステップの処理で送信された入力タイミングに対応した、他の情報処理装置の他の入力制御ステップの処理でオンまたはオフが入力された入力タイミングの受信を制御する受信制御ステップと、入力タイミング計測制御ステップの処理により計測された入力タイミングと、受信制御ステップの処理により受信された入力タイミングとの比較を制

50

御する比較制御ステップと、比較制御ステップの処理での比較結果に基づいて、他の情報処理装置との認証処理の実行を制御する認証制御ステップとを含むことを特徴とする。

【0047】

本発明の第3のプログラムは、オンオフの入力を制御する入力制御ステップと、入力制御ステップの処理でオンまたはオフが入力された入力タイミングの計測を制御する入力タイミング計測制御ステップと、入力タイミングのネットワークを介した他の情報処理装置への送信を制御する送信制御ステップと、他の情報処理装置より送信されてくる、送信制御ステップの処理で送信された入力タイミングに対応した、他の情報処理装置の他の入力制御ステップの処理でオンまたはオフが入力された入力タイミングの受信を制御する受信制御ステップと、入力タイミング計測制御ステップの処理により計測された入力タイミングと、受信制御ステップの処理により受信された入力タイミングとの比較を制御する比較制御ステップと、比較制御ステップの処理での比較結果に基づいて、他の情報処理装置との認証処理の実行を制御する認証制御ステップとを実行させる。

【0048】

本発明の第2の情報処理システムは、第1の情報処理装置が、第2の情報処理装置より送信されてくる、第2の入力タイミングを受信する第1の受信手段と、第1の入力タイミングと第2の入力タイミングとを比較する第1の比較手段と、第1の比較手段の比較結果に基づいて、第2の情報処理装置との認証処理を実行する第1の認証手段とを備え、第2の情報処理装置が、第1の情報処理装置より送信されてくる、第1の入力タイミングを受信する第2の受信手段と、第1の入力タイミングと第2の入力タイミングとを比較する第2の比較手段と、第2の比較手段の比較結果に基づいて、第1の情報処理装置との認証処理を実行する第2の認証手段とを備えることを特徴とする。

前記第1の入力タイミング計測手段には、第1の入力手段によりオンが入力された第1のオンタイミングを計測する第1のオンタイミング計測手段と、第1の入力手段によりオフが入力された第1のオフタイミングを計測する第1のオフタイミング計測手段とをさらに設けるようにさせることができ、第1のオンタイミング、および、第1のオフタイミングを第1の入力タイミングとして計測させるようにすることができ、第2の入力タイミング計測手段には、第2の入力手段によりオンが入力された第2のオンタイミングを計測する第2のタイミング計測手段と、第2の入力手段によりオフが入力された第2のオフタイミングを計測する第2のタイミング計測手段とをさらに設けるようにさせることができ、第2のオンタイミング、および、第2のオフタイミングを第2の入力タイミングとして計測させるようにすることができ、第1の送信手段には、第1の入力タイミングのうち、第1のオフタイミングをネットワークを介して第2の情報処理装置に送信させるようにすることができ、第2の送信手段には、第2の入力タイミングのうち、第2のオンタイミングをネットワークを介して第1の情報処理装置に送信させるようにすることができ、第1の受信手段には、第2の情報処理装置より送信されてくる、第2の入力タイミングのうちの第2のオンタイミングを受信させることができ、第2の受信手段には、第1の情報処理装置より送信されてくる、第1の入力タイミングのうち、第1のオフタイミングを受信させないようにすることができ、第1の比較手段には、第1の入力タイミングのうちの第1のオンタイミングと、第2の入力タイミングのうちの第2のオンタイミングとを比較せないようにすることができ、第2の比較手段には、第1の入力タイミングのうちの第1のオフタイミングと、第2の入力タイミングのうちの第2のオフタイミングとを比較せないようにすることができ、

【0049】

本発明の第2の情報処理システムの情報処理方法は、第1の情報処理装置の情報処理方法が、第2の情報処理装置より送信されてくる、第2の入力タイミングを受信する第1の受信ステップと、第1の入力タイミングと第2の入力タイミングとを比較する第1の比較ステップと、第1の比較ステップの処理の比較結果に基づいて、第2の情報処理装置との認証処理を実行する第1の認証ステップとを含み、第2の情報処理装置の情報処理方法が、第1の情報処理装置より送信されてくる、第1の入力タイミングを受信する第2の受信

10

20

30

40

50

ステップと、第1の入力タイミングと第2の入力タイミングとを比較する第2の比較ステップと、第2の比較ステップの処理の比較結果に基づいて、第1の情報処理装置との認証処理を実行する第2の認証ステップとを含むことを特徴とする。

【0050】

本発明の第4の記録媒体のプログラムは、第1の情報処理装置を制御するプログラムが、第2の情報処理装置より送信されてくる、第2の入力タイミングの受信を制御する第1の受信制御ステップと、第1の入力タイミングと第2の入力タイミングとの比較を制御する第1の比較制御ステップと、第1の比較制御ステップの処理の比較結果に基づいて、第2の情報処理装置との認証処理の実行を制御する第1の認証制御ステップとを含み、第2の情報処理装置を制御するプログラムは、第1の情報処理装置より送信されてくる、第1の入力タイミングの受信を制御する第2の受信制御ステップと、第1の入力タイミングと第2の入力タイミングとの比較を制御する第2の比較制御ステップと、第2の比較制御ステップの処理の比較結果に基づいて、第1の情報処理装置との認証処理の実行を制御する第2の認証制御ステップとを含むことを特徴とする。

【0051】

本発明の第4のプログラムは、第1の情報処理装置を制御するコンピュータに、第2の情報処理装置より送信されてくる、第2の入力タイミングの受信を制御する第1の受信制御ステップと、第1の入力タイミングと第2の入力タイミングとの比較を制御する第1の比較制御ステップと、第1の比較制御ステップの処理の比較結果に基づいて、第2の情報処理装置との認証処理の実行を制御する第1の認証制御ステップとを含む処理を実行させ、第2の情報処理装置を制御するコンピュータに、第1の情報処理装置より送信されてくる、第1の入力タイミングの受信を制御する第2の受信制御ステップと、第1の入力タイミングと第2の入力タイミングとの比較を制御する第2の比較制御ステップと、第2の比較制御ステップの処理の比較結果に基づいて、第1の情報処理装置との認証処理の実行を制御する第2の認証制御ステップとを含む処理を実行させる。

【0053】

本発明の第1の情報処理装置および方法、並びに第1のプログラムにおいては、オンオフが入力され、オンまたはオフが入力された入力タイミングが計測され、他の情報処理装置より送信されてくる、他の情報処理装置にオンまたはオフが入力された入力タイミングが受信され、計測された入力タイミングと、受信された入力タイミングとが比較され、比較結果に基づいて、他の情報処理装置との認証処理が実行される。

【0054】

本発明の第1の情報処理システムおよび方法、並びに第2のプログラムにおいては、第1の情報処理装置により、オンオフが入力され、オンまたはオフが入力された第1の入力タイミングが計測され、第1の入力タイミングがネットワークを介して第2の情報処理装置に送信され、第2の情報処理装置により、オンオフが入力され、オンまたはオフが入力された第2の入力タイミングが計測され、第1の情報処理装置より送信されてくる、第1の入力タイミングが受信され、第1の入力タイミングと第2の入力タイミングとが比較され、比較結果に基づいて、第1の情報処理装置との認証処理が実行される。

【0055】

本発明の第2の情報処理装置および方法、並びに第3のプログラムにおいては、オンオフが入力され、オンまたはオフが入力された入力タイミングが計測され、入力タイミングがネットワークを介して他の情報処理装置に送信され、他の情報処理装置より送信されてくる、送信された入力タイミングに対応した、他の情報処理装置のオンまたはオフが入力された入力タイミングが受信され、計測された入力タイミングと、受信された入力タイミングとが比較され、比較結果に基づいて、他の情報処理装置との認証処理が実行される。

【0056】

本発明の第2の情報処理システムおよび方法、並びに第4のプログラムにおいては、第1の情報処理装置により、第2の情報処理装置より送信されてくる、第2の入力タイミングが受信され、第1の入力タイミングと第2の入力タイミングとが比較され、比較結果に

10

20

30

40

50

基づいて、第2の情報処理装置との認証処理が実行され、第2の情報処理装置により、第1の情報処理装置より送信されてくる、第1の入力タイミングが受信され、第1の入力タイミングと第2の入力タイミングとが比較され、比較結果に基づいて、第1の情報処理装置との認証処理が実行される。

【0057】

【発明の実施の形態】

図3は、本発明に係る無線通信システムの一実施の形態の構成を示す図である。尚、図3以降の図面の説明においては、従来の場合と対応する部分には同一の符号を付してあり、その説明は適宜省略する。パーソナルコンピュータ1とカムコーダ2は、上述のブルートウースを用いることにより相互にデータを無線通信で交換することができる。

10

【0058】

図4は、本発明を適用したパーソナルコンピュータ1とカムコーダ2の構成を示したブロック図である。まず、パーソナルコンピュータ1の構成について説明する。パーソナルコンピュータ1のマイクロコンピュータ21は、CPU(Central Processing Unit)、ROM(Read Only Memory)、および、RAM(Random Access Memory)から構成されており、CPUが、ROMに記憶されたプログラムを適宜RAMに読み込んで、各種の処理を実行する。また、マイクロコンピュータ21は、パーソナルコンピュータ1の全体の動作を制御しており、バス27を介してハードディスク22に記憶されている、認証プログラム22aを始めとした各種のプログラムを内部のRAMに展開させて、各種の処理を実行する。さらに、マイクロコンピュータ21は、バス27を介してドライブ201に装着された磁気ディスク211、光ディスク212、光磁気ディスク213、または、半導体メモリ214に記憶された各種のプログラムを読み込んで実行すると共に、必要に応じて、各種のプログラムやデータを書き込む。

20

【0059】

ハードディスク22は、通信部25により接続されるカムコーダ2などの電子機器間の認証処理を実行する認証プログラム22aを始めとして、各種のプログラムを記憶すると共に、プログラムの実行に必要なデータを記憶する。表示部23は、マイクロコンピュータ21により制御され、CRT(Cathode Ray Tube)やLCD(Liquid Crystal Display)などからなり、各種の処理結果や、後述する操作用のウィンドウを表示する。認証プログラム22aは、認証ボタン26の押下されたタイミング、押下が終了したタイミングのそれぞれの時刻を計測し、これをカムコーダ2より送信されてくる、同様のタイミングの時刻とを、カムコーダ2の基準時刻と自らの基準時刻との時間差を考慮して比較し、比較結果に基づいて認証処理を実行する。PC1の自らの基準時刻は、図示せぬリアルタイムクロックにより発生されている。

30

【0060】

入力部24は、キーボードやマウスなどからなりユーザが、各種のコマンドを入力するとき操作される。通信部25は、いわゆるブルートウースにより構成されており、マイクロコンピュータ21からの指令に基づいて、無線によりカムコーダ2を始めとした電子機器と各種データの授受を実行する。認証ボタン26は、認証しようとするカムコーダ2と、ブルートウースにより規定された最初の認証処理を行うとき、認証しようとするカムコーダ2に設けられた認証ボタン35と同時に操作され、同じタイミングでオンオフされることにより、認証処理を実行させるためのものである。認証ボタン26、35の操作の詳細については後述する。

40

【0061】

次に、カムコーダ2の構成について説明する。カムコーダ2のマイクロコンピュータ31は、カムコーダ2の全体の動作を制御しており、CPU、ROM、および、RAMから構成されている。マイクロコンピュータ31のCPUは、ROMに記憶された各種のプログラムを適宜RAMに読み込んで各種の処理を実行する。また、マイクロコンピュータ31は、バス41に接続されたハードディスク32に記憶された、認証プログラム32aを始めとして、各種のプログラムを読み込んで実行する。認証プログラム32aは、認証ボタン35の押下されたタ

50

イミング、押下が終了したタイミングのそれぞれの時刻を計測し、これらをPC 1より送信されてくる、同様のタイミングを示す時刻と、PC 1の基準時刻と自らの基準時刻との時間差を考慮して比較し、比較結果に基づいて認証処理を実行する。カムコーダ2の自らの基準時刻は、図示せぬリアルタイムクロックより発生されている。

【0062】

表示部33は、撮像部34により撮像された画像や、メカデッキ39に装着された記録媒体に記録された画像を表示させる。撮像部34は、CCD(Charge Coupled Device)カメラなどからなり、図示せぬ被写体を撮像して画像データを生成する。通信部36は、上述と同様のブルートゥースから構成されており、マイクロコンピュータ31により制御され、無線通信によりPC1と各種のデータを授受する。

10

【0063】

入力部37は、タブレットボタンなどから構成されており、ユーザが、各種のコマンドを入力するとき操作される。記録再生制御部38は、マイクロコンピュータ31からの指令に基づいて、撮像部34により撮像された画像・音声データを所定の方式で圧縮して、メカデッキ39に装着された記録媒体に記録すると共に、記録媒体に記録された圧縮された画像・音声データを伸長し、元の画像・音声データとして再生して、表示部33に表示する。

【0064】

次に、PC1の認証ボタン26と、カムコーダ2の認証ボタン35の認証操作について説明する。認証を行う際、ユーザは、認証させようとするPC1とカムコーダ2のそれぞれに設けられた認証ボタン26, 35を、同じタイミングで押下する。双方の認証プログラム22a, 32aは、相互の認証ボタン26, 35が押下された時刻と、押下が終了された時刻をそれぞれ相互に測定し、無線通信により相互に授受し、同じタイミングで押下されたことが認識されると、認証が成立するというものである。すなわち、相互認証しようとする電子機器同士でなければ、認証ボタン26, 35が同じタイミングで押下される可能性は、極めて低く、逆に、相互の認証ボタン26, 35が同じタイミングで操作されれば、相互に認証処理がなされているものであるとみなし、認証を成立させるというものである。

20

【0065】

ただし、ユーザによる操作であるため（人間により操作されるものであるので）、それぞれの認証ボタン26, 35を同時に押下したつもりでも、厳密に同じタイミングで押下することはできないことがある。そこで、タイミングには、余裕が持たせてある。

30

【0066】

すなわち、図5(A)に示すように、PC1の認証ボタン26が押下されたタイミングをタイミングtA1とし、認証ボタン26の押下が終了したタイミングをタイミングtA2であるとし、さらに、カムコーダ2の認証ボタン35の押下されたタイミングをタイミングtB1とし、押下が終了したタイミングをタイミングtB2とする。この場合、例えば、カムコーダ2の認証ボタン35が押下されたタイミングを基準とすると、前後に時間e(=200ms程度)の余裕を持たせて、タイミングtA1が、tB1 - e < tA1 < tB1 + eを満たし、かつ、時刻tA2が、tB2 - e < tA2 < tB2 + eを満たすとき、双方の認証ボタン26, 35は、同時に押下されたものとみなす。これにより、押下されたタイミング（時刻）が、ユーザの（人間の）操作により生じてしまう程度の誤差範囲内で同時に押下されれば、相互の電子機器は認証を成立させることができる。尚、以上の説明においては、カムコーダ2の認証ボタン35が押下されたタイミングを基準として説明してきたが、当然のことながら、PC1の認証ボタン26が押下されたタイミングを基準としても同様である。また、上述の例では、PC1、および、カムコーダ2の相互に認証用の専用ボタンである認証ボタン26, 35をそれぞれに操作した場合について説明してきたが、必ずしも専用のボタンを設ける必要はなく、例えば、PC1については、キーボードの所定のボタンを押下することで代用させるようにしてよいし、カムコーダ2については、停止ボタンなどの認証処理時に動作に寄与しないボタンなどで代用させるようにしても

40

50

良い。認証ボタン 26, 35 は、押下できるもの、或いは、オンオフを切替えられるものであれば、必ずしもボタンでなくとも良く、例えば、ジョグダイヤルに代表される、回転押圧式操作素子などにより認証ボタン 26, 35 を代用させるようにしても良いし、タッチパネルなどにより、ユーザに触れられているか否かによりオンオフが切替えられるものであればよい。

【0067】

次に、図6のフローチャートを参照して、PC1とカムコーダ2が認証処理を実行するときの動作について説明する。

【0068】

ステップS41において、PC1の認証プログラム22aは、認証ボタン26がオンにされたか（押下されたか）否かを判定し、オンにされたと判定されるまで同様の処理を繰り返し、認証ボタン26がオンにされたと判定された場合、ステップS42において、認証プログラム22aは、認証ボタン26がオンにされた、すなわち、押下されたタイミングである時刻tA1を測定し記憶する。

10

【0069】

ステップS43において、PC1の認証プログラム22aは、認証ボタン26がオフにされたか（押下された状態が解除されたか）否かを判定し、オフにされたと判定されるまで同様の処理を繰り返し、認証ボタン26がオフにされたと判定された場合、ステップS44において、認証プログラム22aは、認証ボタン26がオフにされた、すなわち、押下された状態が解除されたタイミングである時刻tA2を測定し記憶する。

20

【0070】

このとき、ステップS61乃至S64において、カムコーダ2の認証プログラム32aもPC1の認証プログラム22aと同様の処理を実行する。すなわち、ステップS61において、カムコーダ2の認証プログラム32aは、認証ボタン35がオンにされたか（押下されたか）否かを判定し、オンにされたと判定されるまで同様の処理を繰り返し、認証ボタン35がオンにされたと判定された場合、ステップS62において、認証プログラム32aは、認証ボタン35がオンにされた、すなわち、押下されたタイミングである時刻tB1を測定し記憶する。

【0071】

ステップS63において、カムコーダ2の認証プログラム32aは、認証ボタン35がオフにされたか（押下された状態が解除されたか）否かを判定し、オフにされたと判定されるまで同様の処理を繰り返し、認証ボタン35がオフにされたと判定された場合、ステップS64において、認証プログラム32aは、認証ボタン35がオフにされた、すなわち、押下された状態が解除されたタイミングである時刻tB2を測定し記憶する。

30

【0072】

ステップS45において、PC1の認証プログラム22aは、通信部25を制御して、基準時刻tA0をカムコーダ2に送信する。

【0073】

ステップS65において、カムコーダ2の認証プログラム32aは、通信部36を制御して、基準タイミングtA0を受信したか否かを判定し、基準時刻tA0が受信されるまで、その処理を繰り返し、受信したと判定された場合、ステップS66において、自らの基準時刻との時間差（tB0 - tA0）を演算し、時刻tB1, tB2を補正する。すなわち、PC1で計測されたタイミングとカムコーダ2で計測されたタイミングを比較することになるので、PC1の基準時刻、すなわち、例えば、基準時刻を送信する際のPC1のリアルタイムクロックで計測された時刻tA0を送信すると、カムコーダ2は、これを受信し、自らの基準時刻tB0との差を求めて、PC1との時間差を求め、これを利用して、以下の式（1）、式（2）に示すように、自らが計測した時刻tB1, tB2から、その時間差を減算して求める。

40

$$tB1(\text{補正後}) = tB1(\text{補正前}) - (tB0 - tA0) \dots (1)$$

$$tB2(\text{補正後}) = tB2(\text{補正前}) - (tB0 - tA0) \dots (2)$$

50

【0074】

ステップS46において、認証プログラム22aは、通信部25を制御して、時刻tA1, tA2をカムコーダ2に送信する。

【0075】

ステップS67において、カムコーダ2の認証プログラム32aは、PC1より時刻tA1, tA2の情報を受信したか否かを判定し、受信するまでその処理を繰り返し、受信したと判定した場合、その処理は、ステップS68に進む。

【0076】

ステップS68において、認証プログラム32aは、tA1がtB1 - e < tA1 < tB1 + eを満たしているか否かを判定し、例えば、図5に示すように、満たしていると判定された場合、その処理は、ステップS69に進む。

10

【0077】

ステップS69において、認証プログラム32aは、tA2がtB2 - e < tA2 < tB2 + eを満たしているか否かを判定し、例えば、図5に示すように、満たしていると判定された場合、ステップS70において、認証が認められたことをPC1に通知する。

【0078】

ステップS47において、PC1の認証プログラム22aは、通知を受信したか否かを判定し、通知が受信されるまで同様の処理を繰り返し、例えば、ステップS70の処理により、認証が認められた通知が受信されると、ステップS48において、PC1の認証プログラム22aは、認証結果を認識し、今の場合、認証が認められたことを認識する。

20

【0079】

ステップS68, S69において、tA1がtB1 - e < tA1 < tB1 + eを満たしていない、または、tA2がtB2 - e < tA2 < tB2 + eを満たしていないと判定された場合、ステップS71において、認証プログラム32aは、認証が認められなかった、すなわち、認証ボタン26, 35が同時に操作されなかったとみなし、通信部36を制御して、認証が認められなかったことをPC1に通知する。

【0080】

以上の例においては、カムコーダ2側でPC1とカムコーダ2の認証ボタン26, 35が同時に操作されたかを認証判定する処理について説明してきたが、当然のことながら、PC1側で認証判定処理（図6のステップS68, 69の処理）を実行するようにしてもよい。

30

【0081】

また、認証判定処理は、PC1とカムコーダ2で、相互に実行するようにしてもよく、その場合の処理について、図7のフローチャートを参照して説明する。

【0082】

ステップS81において、PC1の認証プログラム22aは、認証ボタン26がオンにされたか（押下されたか）否かを判定し、オンにされたと判定されるまで同様の処理を繰り返し、認証ボタン26がオンにされたと判定された場合、ステップS82において、認証プログラム22aは、認証ボタン26がオンにされた、すなわち、押下されたタイミングである時刻tA1を測定し記憶する。

40

【0083】

ステップS83において、PC1の認証プログラム22aは、認証ボタン26がオフにされたか（押下された状態が解除されたか）否かを判定し、オフにされたと判定されるまで同様の処理を繰り返し、認証ボタン26がオフにされたと判定された場合、ステップS84において、認証プログラム22aは、認証ボタン26がオフにされた、すなわち、押下された状態が解除されたタイミングである時刻tA2を測定し記憶する。

【0084】

このとき、ステップS101乃至S104において、カムコーダ2の認証プログラム32aもPC1の認証プログラム22aと同様の処理を実行する。すなわち、ステップS101において、カムコーダ2の認証プログラム32aは、認証ボタン35がオンにされたか（押下されたか）否かを判定し、オンにされたと判定されるまで同様の処理を繰り返し、認

50

証ボタン35がオンにされたと判定された場合、ステップS102において、認証プログラム32aは、認証ボタン35がオンにされた、すなわち、押下されたタイミングである時刻tB1を測定し記憶する。

【0085】

ステップS103において、カムコーダ2の認証プログラム32aは、認証ボタン35がオフにされたか（押下された状態が解除されたか）否かを判定し、オフにされたと判定されるまで同様の処理を繰り返し、認証ボタン35がオフにされたと判定された場合、ステップS104において、認証プログラム32aは、認証ボタン35がオフにされた、すなわち、押下された状態が解除されたタイミングである時刻tB2を測定し記憶する。

【0086】

ステップS85において、PC1の認証プログラム22aは、通信部25を制御して、基準時刻tA0をカムコーダ2に送信する。

【0087】

ステップS105において、カムコーダ2の認証プログラム32aは、通信部36を制御して、基準タイミングtA0を受信したか否かを判定し、基準時刻tA0が受信されるまで、その処理を繰り返し、受信したと判定された場合、ステップS106において、自らの基準時刻との時間差（tB0 - tA0）を演算し、時刻tB1, tB2を補正する。

【0088】

ステップS86において、認証プログラム22aは、通信部25を制御して、時刻tA1をカムコーダ2に送信する。

【0089】

ステップS107において、カムコーダ2の認証プログラム32aは、PC1より時刻tA1の情報を受信したか否かを判定し、受信するまでその処理を繰り返し、受信したと判定した場合、その処理は、ステップS108に進む。

【0090】

ステップS108において、認証プログラム32aは、tA1がtB1 - e < tA1 < tB1 + eを満たしているか否かを判定し、例えば、図8（B）に示すように、満たしていると判定された場合、その処理は、ステップS109に進む。

【0091】

ステップS109において、認証プログラム32aは、通信部36を制御して、認証が認められたことをPC1に通知する。

【0092】

ステップS87において、PC1の認証プログラム22aは、通知を受信したか否かを判定し、通知が受信されるまで同様の処理を繰り返し、例えば、ステップS109の処理により、認証が認められた通知が受信されると、その処理は、ステップS88に進む。

【0093】

ステップS110において、認証プログラム32aは、通信部36を制御して、時刻tB2をPC1に送信する。

【0094】

ステップS88において、PC1の認証プログラム22aは、通信部25を制御して、時刻tB2をカムコーダ2より受信したか否かを判定し、受信されるまで、その処理を繰り返し、受信されたと判定された場合、その処理は、ステップS89に進む。

【0095】

ステップS89において、認証プログラム22aは、tB2がtA2 - e < tB2 < tA2 + eを満たしているか否かを判定し、例えば、図8（A）に示すように、満たしていると判定された場合、ステップS90において、通信部25を制御して、認証が認められたことをカムコーダ2に通知する。

【0096】

ステップS111において、カムコーダ2の認証プログラム32aは、PC1から送信されてくる認証結果を受信し、認識する。例えば、ステップS90の処理により送信されてく

10

20

30

40

50

る認証結果により認証が認められたことを認識する。

【0097】

ステップS108において、 t_{A1} が $t_{B1} - e < t_{A1} < t_{B1} + e$ を満たしていないと判定された場合、ステップS112において、認証プログラム32aは、認証が認められなかった、すなわち、認証ボタン26, 35が同時に操作されなかったとみなし、通信部36を制御して、認証が認められなかったことをPC1に通知する。

【0098】

結果として、ステップS87において、認証プログラム22aは、認証が認められなかつたと判定し、その処理は終了する。

【0099】

また、ステップS89において、 t_{B2} が $t_{A2} - e < t_{B2} < t_{A2} + e$ を満たしていないと判定された場合、ステップS91において、PC1の認証プログラム22aは、通信部25を制御して認証が認められなかったことをカムコーダ2に送信する。

【0100】

以上のように、カムコーダ2では、認証ボタン26, 35が押下されたタイミングの時刻が比較され、PC1では、認証ボタン26, 35の押下が解除されたタイミングの時刻が比較されることにより、相互で認証処理を行うことができる。もちろん、以上の例とは、逆に、PC1が、認証ボタン26, 35が押下されたタイミングの時刻を比較し、カムコーダ2が、認証ボタン26, 35の押下が解除されたタイミングの時刻を比較するようにしてもよい。

【0101】

また、以上の例においては、認証ボタン26, 35が相互に1回だけ押下された場合の処理について説明してきたが、1回の押下では、誤操作などにより偶然に認証が認められてしまう可能性がある。このため、認証ボタン26, 35を押下する回数は、複数回数にするようにして、誤操作の発生を防止させることもできる。

【0102】

そこで、次に、認証ボタン26, 35を相互に複数回数ずつ押下する場合（例えば、n回押下する場合）について、図9のフローチャートを参照して説明する。このとき、認証プログラム22a, 32aは、押下された回数をカウントするためのカウンタ*i*をそれぞれ備える。

【0103】

ステップS121において、PC1の認証プログラム22aは、自らのカウンタ*i*を1に初期化する。ステップS122において、PC1の認証プログラム22aは、認証ボタン26がオンにされたか（押下されたか）否かを判定し、オンにされたと判定されるまで同様の処理を繰り返し、認証ボタン26がオンにされたと判定された場合、ステップS123において、認証プログラム22aは、認証ボタン26がオンにされた、すなわち、押下されたタイミングである時刻 t_{A_i} を測定し記憶する。

【0104】

ステップS124において、PC1の認証プログラム22aは、認証ボタン26がオフにされたか（押下された状態が解除されたか）否かを判定し、オフにされたと判定されるまで同様の処理を繰り返し、認証ボタン26がオフにされたと判定された場合、ステップS125において、認証プログラム22aは、認証ボタン26がオフにされた、すなわち、押下された状態が解除されたタイミングである時刻 $t_{A(i+1)}$ を測定し記憶する。ステップS126において、認証プログラム22aは、カウンタ*i*を2だけインクリメントする。ステップS127において、カウンタ*i* / 2がnより大きいか否かを判定し、カウンタ*i* / 2がnより大きくないと判定された場合、その処理は、ステップS122に戻りそれ以降の処理が繰り返され、認証ボタン26が押下されるべき設定回数であるnよりも*i* / 2が大きくなるまで、ステップS122乃至S126の処理が繰り返される。ステップS127において、カウンタ*i* / 2が認証ボタン26が押下される所定回数nより大きいと判定された場合、その処理は、ステップS128に進む。

10

20

30

40

50

【0105】

このとき、ステップS141乃至S147において、カムコーダ2の認証プログラム32aもPC1の認証プログラム22aと同様の処理を実行する。すなわち、ステップS141において、カムコーダ2の認証プログラム32aは、自らのカウンタ*i*を1に初期化する。ステップS142において、カムコーダ2の認証プログラム32aは、認証ボタン35がオンにされたか（押下されたか）否かを判定し、オンにされたと判定されるまで同様の処理を繰り返し、認証ボタン35がオンにされたと判定された場合、ステップS143において、認証プログラム32aは、認証ボタン35がオンにされた、すなわち、押下されたタイミングである時刻tB*i*を測定し記憶する。

【0106】

10

ステップS144において、カムコーダ2の認証プログラム32aは、認証ボタン35がオフにされたか（押下された状態が解除されたか）否かを判定し、オフにされたと判定されるまで同様の処理を繰り返し、認証ボタン35がオフにされたと判定された場合、ステップS145において、認証プログラム32aは、認証ボタン35がオフにされた、すなわち、押下された状態が解除されたタイミングである時刻tB(*i*+1)を測定し記憶する。

【0107】

20

ステップS146において、カムコーダ2の認証プログラム32aは、カウンタ*i*を2だけインクリメントする。ステップS147において、カウンタ*i*/2がnより大きいか否かを判定し、カウンタ*i*/2がnより大きくないと判定された場合、その処理は、ステップS142に戻りそれ以降の処理が繰り返され、認証ボタン35が押下されるべき設定回数であるnよりも*i*/2が大きくなるまで、ステップS142乃至S146の処理が繰り返される。ステップS147において、カウンタ*i*/2が認証ボタン35が押下される所定回数nより大きいと判定された場合、その処理は、ステップS148に進む。

【0108】

ステップS128において、PC1の認証プログラム22aは、通信部25を制御して、基準時刻tA0をカムコーダ2に送信する。

【0109】

30

ステップS148において、カムコーダ2の認証プログラム32aは、通信部36を制御して、基準タイミングtA0を受信したか否かを判定し、基準時刻tA0が受信されるまで、その処理を繰り返し、受信したと判定された場合、ステップS149において、自らの基準時刻との時間差（tB0 - tA0）を演算し、時刻tB1, tB2, ..., tB(2n)を補正する。

【0110】

ステップS129において、認証プログラム22aは、通信部25を制御して、時刻tA1, tA2, ..., tA(2n)をカムコーダ2に送信する。

【0111】

ステップS150において、カムコーダ2の認証プログラム32aは、PC1より時刻tA1, tA2, ..., tA(2n)の情報を受信したか否かを判定し、受信するまでその処理を繰り返し、受信したと判定した場合、その処理は、ステップS151に進む。

40

【0112】

ステップS151において、認証プログラム32aは、全ての*i*（*i*=1乃至2n）について、tAiがtBi - e < tAi < tBi + eを満たしているか否かを判定し、例えば、図10に示すように、tB1 - e < tA1 < tB1 + e, tB2 - e < tA2 < tB2 + e, tB3 - e < tA3 < tB3 + e, tB4 - e < tA4 < tB4 + e, ..., tB(2n-1) - e < tA(2n-1) < tB(2n-1) + e, tB(2n) - e < tA(2n) < tB(2n) + eを満たしていると判定された場合、その処理は、ステップS152に進む。ステップS152において、認証プログラム32aは、認証が認められたことをPC1に通知する。

【0113】

50

ステップS130において、PC1の認証プログラム22aは、通知を受信したか否かを判定し、通知が受信されるまで同様の処理を繰り返し、例えば、ステップS152の処理により、認証が認められた通知が受信されると、ステップS131において、PC1の認証プログラム22aは、認証結果を認識し、今の場合、認証が認められたことを認識する。

【0114】

ステップS151において、全ての*i* (*i* = 1 乃至 2 *n*) について、*tAi*が*tBi - e* < *tAi* < *tBi + e* を満たしていないと判定された場合、ステップS153において、認証プログラム32aは、認証が認められなかった、すなわち、認証ボタン26, 35が同時に操作されなかったとみなし、通信部36を制御して、認証が認められなかったことをPC1に通知する。

10

【0115】

以上の例においては、カムコーダ2側でPC1とカムコーダ2の認証ボタン26, 35が、複数回数に渡って同時に操作されたかを認証判定する処理について説明してきたが、当然のことながら、PC1側で認証判定処理（図9のステップS151の処理）を実行するようにしてよい。

【0116】

また、認証ボタン26, 35を複数回数押下する場合でも、図7のフローチャートを参照して説明したように、認証判定処理は、PC1とカムコーダ2で、相互に実行するようにしてもよく、その場合の処理について、図11のフローチャートを参照して説明する。

20

【0117】

ステップS171において、PC1の認証プログラム22aは、自らのカウンタ*i*を1に初期化する。ステップS172において、PC1の認証プログラム22aは、認証ボタン26がオンにされたか（押下されたか）否かを判定し、オンにされたと判定されるまで同様の処理を繰り返し、認証ボタン26がオンにされたと判定された場合、ステップS173において、認証プログラム22aは、認証ボタン26がオンにされた、すなわち、押下されたタイミングである時刻*tAi*を測定し記憶する。

【0118】

ステップS174において、PC1の認証プログラム22aは、認証ボタン26がオフにされたか（押下された状態が解除されたか）否かを判定し、オフにされたと判定されるまで同様の処理を繰り返し、認証ボタン26がオフにされたと判定された場合、ステップS175において、認証プログラム22aは、認証ボタン26がオフにされた、すなわち、押下された状態が解除されたタイミングである時刻*tA* (*i* + 1)を測定し記憶する。

30

【0119】

ステップS176において、認証プログラム22aは、カウンタ*i*を2だけインクリメントする。ステップS177において、カウンタ*i* / 2 が*n*より大きいか否かを判定し、カウンタ*i* / 2 が*n*より大きくないと判定された場合、その処理は、ステップS172に戻りそれ以降の処理が繰り返され、認証ボタン26が押下されるべき設定回数である*n*よりも*i* / 2 が大きくなるまで、ステップS172乃至S176の処理が繰り返される。ステップS177において、カウンタ*i* / 2 が認証ボタン26が押下される所定回数*n*より大きいと判定された場合、その処理は、ステップS178に進む。

40

【0120】

このとき、ステップS201乃至S207において、カムコーダ2の認証プログラム32aもPC1の認証プログラム22aと同様の処理を実行する。すなわち、ステップS201において、カムコーダ32aは、カウンタ*i*を1に初期化する。さらに、ステップS202において、カムコーダ2の認証プログラム32aは、認証ボタン35がオンにされたか（押下されたか）否かを判定し、オンにされたと判定されるまで同様の処理を繰り返し、認証ボタン35がオンにされたと判定された場合、ステップS203において、認証プログラム32aは、認証ボタン35がオンにされた、すなわち、押下されたタイミングである時刻*tBi*を測定し記憶する。

【0121】

50

ステップS204において、カムコーダ2の認証プログラム32aは、認証ボタン35がオフにされたか（押下された状態が解除されたか）否かを判定し、オフにされたと判定されるまで同様の処理を繰り返し、認証ボタン35がオフにされたと判定された場合、ステップS205において、認証プログラム32aは、認証ボタン35がオフにされた、すなわち、押下された状態が解除されたタイミングである時刻tB(i+1)を測定し記憶する。

【0122】

ステップS206において、認証プログラム32aは、カウンタiを2だけインクリメントする。ステップS207において、カウンタi/2がnより大きいか否かを判定し、カウンタi/2がnより大きくないと判定された場合、その処理は、ステップS202に戻りそれ以降の処理が繰り返され、認証ボタン35が押下されるべき設定回数であるnよりもi/2が大きくなるまで、ステップS202乃至S206の処理が繰り返される。ステップS207において、カウンタi/2が認証ボタン35が押下される所定回数nより大きいと判定された場合、その処理は、ステップS208に進む。

10

【0123】

ステップS178において、PC1の認証プログラム22aは、通信部25を制御して、基準時刻tA0をカムコーダ2に送信する。

【0124】

ステップS208において、カムコーダ2の認証プログラム32aは、通信部36を制御して、基準タイミングtA0を受信したか否かを判定し、基準時刻tA0が受信されるまで、その処理を繰り返し、受信したと判定された場合、ステップS209において、自らの基準時刻との時間差(tB0 - tA0)を演算し、時刻tB1, tB2, ..., tB(2n)を補正する。

20

【0125】

ステップS179において、認証プログラム22aは、通信部25を制御して、tAiのうちカウンタiが奇数となる時刻tA1, tA3, ..., tA(2n-1)をカムコーダ2に送信する。

【0126】

ステップS210において、カムコーダ2の認証プログラム32aは、PC1よりtAiのうちカウンタiが奇数となる時刻tA1, tA3, ..., tA(2n-1)の情報を受信したか否かを判定し、受信するまでその処理を繰り返し、受信したと判定した場合、その処理は、ステップS211に進む。

30

【0127】

ステップS211において、認証プログラム32aは、全ての奇数のカウンタi(i=1, 3, 5, ..., 2n-1)のtAiについて、tBi - e < tAi < tBi + eを満たしているか否かを判定し、例えば、図12(B)に示すように、tB1 - e < tA1 < tB1 + e, tB3 - e < tA3 < tB3 + e, ..., tB(2n-1) - e < tA(2n-1) < tB(2n-1) + eを満たしていると判定された場合、その処理は、ステップS212において、認証が認められたことをPC1に通知する。

【0128】

40

ステップS180において、PC1の認証プログラム22aは、通知を受信したか否かを判定し、通知が受信されるまで同様の処理を繰り返し、例えば、ステップS212の処理により、認証が認められた通知が受信されると、ステップS181に進む。

【0129】

ステップS213において、認証プログラム32aは、通信部36を制御して、時刻tBiのうち、iが偶数の時刻tB2, tB4, ..., tB(2n)をPC1に送信する。

【0130】

ステップS181において、PC1の認証プログラム22aは、通信部25を制御して、時刻tB2, tB4, ..., tB(2n)をカムコーダ2より受信したか否かを判定し、受信されるまで、その処理を繰り返し、受信されたと判定された場合、その処理は、ステッ

50

プ S 1 8 2 に進む。

【 0 1 3 1 】

ステップ S 1 8 2 において、認証プログラム 2 2 a は、時刻 $t_{B2}, t_{B4} \dots, t_{B(2n)}$ が $t_{A2} - e < t_{B2} < t_{A2} + e, t_{A4} - e < t_{B4} < t_{A4} + e \dots t_{A(2n)} - e < t_{B(2n)} < t_{A(2n)} + e$ を満たしているか否かを判定し、例えば、図 1 2 (A) に示すように、満たしていると判定された場合、ステップ S 1 8 3 において、通信部 2 5 を制御して、認証が認められたことをカムコーダ 2 に通知する。

【 0 1 3 2 】

ステップ S 2 1 4 において、カムコーダ 2 の認証プログラム 3 2 a は、PC 1 から送信されてくる認証結果を受信し、認識する。例えば、ステップ S 1 8 3 の処理により送信されてくる認証結果により認証が認められたことを認識する。

10

【 0 1 3 3 】

ステップ S 2 1 1 において、 t_{Ai} のうち i が奇数のものが $t_{Bi} - e < t_{Ai} < t_{Bi} + e$ を満たしていないと判定された場合、ステップ S 2 1 5 において、認証プログラム 3 2 a は、認証が認められなかった、すなわち、認証ボタン 2 6, 3 5 が複数回数に渡って同時に操作されなかったとみなし、通信部 3 6 を制御して、認証が認められなかったことを PC 1 に通知する。

【 0 1 3 4 】

結果として、ステップ S 1 8 0 において、認証プログラム 2 2 a は、認証が認められなかったと判定し、その処理は終了する。

20

【 0 1 3 5 】

また、ステップ S 1 8 2 において、 t_{Bi} のうち i が偶数のものが $t_{Ai} - e < t_{Bi} < t_{Ai} + e$ を満たしていないと判定された場合、ステップ S 1 8 4 において、PC 1 の認証プログラム 2 2 a は、通信部 2 5 を制御して認証が認められなかったことをカムコーダ 2 に送信する。

【 0 1 3 6 】

以上のように、複数回数に渡り、PC 1 とカムコーダ 2 の相互で認証処理を実行させることもでき、認証処理時の誤動作などにも対応することができる。

【 0 1 3 7 】

以上の例においては、PC 1 とカムコーダ 2 の間での認証処理について説明してきたが、それ以外の電子機器間でも、ブルートゥースを備えた電子機器間であればよく、例えば、図 1 (B) 乃至 (D) に示すように、ブルートゥースを備えた携帯電話機 3 とハンディカムコーダ 4、カムコーダ 2 と携帯情報端末機 5、携帯型パーソナルコンピュータ 6 と携帯情報端末機 5 などに代表される様々な電子機器間でも、同様の処理による認証処理を実現させることができる。

30

【 0 1 3 8 】

また、ブルートゥースの規格においては、PIN=0とすることにより PIN の入力を省略させた状態で接続することができるようになっている。この PIN の省略機能を利用して、最初の認証処理は、ブルートゥースの規格通りの認証処理として、それ以降の認証処理は、上述のように認証ボタンを用いる方法とするようにしてもよい。

40

【 0 1 3 9 】

さらに、認証処理を実行する毎に、認証ボタン 2 6, 3 5 の押下回数 n を変化させるようにもよい。

【 0 1 4 0 】

また、上述の例では、PC 1 とカムコーダ 2 の認証プログラム 2 2 a, 3 2 a で、相互に認証処理を実行する場合、一方の認証プログラムが認証ボタン 2 6, 3 5 が押下された時刻を比較し、他方の認証プログラムが認証ボタン 2 6, 3 5 の押下状態が解除された時刻を比較することにより認証処理を行う例について説明してきたが、相互の認証プログラムが比較する時刻は、互いに重なり合わない時刻同士であれば、2 つの集合に分けて、相互に比較するようにしてもよい。

50

【0141】

さらに、相互の基準時刻 t_{A0} , t_{B0} を使用せずに、例えば、それぞれの最初に認証ボタン 26, 35 が押下されるタイミングである時刻 t_{A1} , t_{B1} を基準として、各時刻との差を求めて、 $t_{Ai} - t_{A1}$ と $t_{Bi} - t_{B1}$ を、 $i = 1$ 乃至 $2n$ の範囲で求めて、それぞれ対応する時刻を比較するようにしてもよい。このとき、時刻 t_{A1} , t_{B1} は、基準時刻と同様に扱われるため、タイミングを比較する時刻の数が 1 個分減ることになるので、1 回の押下 ($n = 1$) だけでは、相互に認証処理を実行することができないので、相互に認証処理を実行するには、複数回数の押下の開始と終了のタイミングの時刻情報が必要となる。

【0142】

10

また、本発明は、通信部 25, 36 としてブルートゥースを用いた例について説明してきたが、ブルートゥース以外の通信部からなる無線通信システム、または、有線通信システム上での認証処理に使用するようにしてもよい。

【0143】

以上によれば、簡単な操作で、認証処理を実現させることができる。

【0144】

20

上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行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行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行させることが可能な、例えば汎用のパーソナルコンピュータなどに記録媒体からインストールされる。

【0145】

この記録媒体は、図 4 に示すようにパーソナルコンピュータ 1 に予め組み込まれた状態でユーザに提供される、プログラムが記録されているハードディスク 22 だけではなく、コンピュータとは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク 211 (フレキシブルディスクを含む)、光ディスク 212 (CD-ROM(Compact Disc-Read Only Memory), DVD (Digital Versatile Disc) を含む)、光磁気ディスク 213 (MD (Mini-Disc) (登録商標) を含む)、もしくは半導体メモリ 214 (Memory Stickを含む) などよりなるパッケージメディアにより構成される。

30

【0146】

尚、本明細書において、記録媒体に記録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含むものである。

【0147】

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。

【0149】

【発明の効果】

40

本発明の第 1 の情報処理装置および方法、並びに第 1 のプログラムによれば、オンオフを入力し、オンまたはオフが入力された入力タイミングを計測し、他の情報処理装置より送信されてくる、他の情報処理装置にオンまたはオフが入力された入力タイミングを受信し、計測された入力タイミングと、受信された入力タイミングとを比較し、比較結果に基づいて、他の情報処理装置との認証処理を実行するようにした。

【0150】

本発明の第 1 の情報処理システムおよび方法、並びに第 2 のプログラムによれば、第 1 の情報処理装置が、オンオフを入力し、オンまたはオフを入力した第 1 の入力タイミングを計測し、第 1 の入力タイミングをネットワークを介して第 2 の情報処理装置に送信し、第 2 の情報処理装置が、オンオフを入力し、オンまたはオフを入力した第 2 の入力タイミングを計測し、第 1 の情報処理装置より送信されてくる、第 1 の入力タイミングを受信し

50

、第1の入力タイミングと第2の入力タイミングとを比較し、比較結果に基づいて、第1の情報処理装置との認証処理を実行するようにした。

【0151】

本発明の第2の情報処理装置および方法、並びに第3のプログラムによれば、オンオフを入力し、オンまたはオフが入力した入力タイミングを計測し、入力タイミングをネットワークを介して他の情報処理装置に送信し、他の情報処理装置より送信されてくる、送信された入力タイミングに対応した、他の情報処理装置のオンまたはオフを入力した入力タイミングを受信し、計測した入力タイミングと、受信した入力タイミングとを比較し、比較結果に基づいて、他の情報処理装置との認証処理を実行するようにした。

【0152】

10

本発明の第2の情報処理システムおよび方法、並びに第4のプログラムによれば、第1の情報処理装置が、第2の情報処理装置より送信されてくる、第2の入力タイミングを受信し、第1の入力タイミングと第2の入力タイミングとを比較し、比較結果に基づいて、第2の情報処理装置との認証処理を実行し、第2の情報処理装置が、第1の情報処理装置より送信されてくる、第1の入力タイミングを受信し、第1の入力タイミングと第2の入力タイミングとを比較し、比較結果に基づいて、第1の情報処理装置との認証処理を実行するようにした。

【0153】

いずれにおいても、結果として、相互認証処理を簡単に実行することが可能となる。

【図面の簡単な説明】

20

【図1】従来の無線接続による電子機器の組合せを示す図である。

【図2】従来の認証処理を説明するフローチャートである。

【図3】本発明を適用した無線通信システムの一実施の形態の構成を示す図である。

【図4】図3のパーソナルコンピュータとカムコーダの構成を示すブロック図である。

【図5】認証ボタンの押下のタイミングを示すタイミングチャートである。

【図6】本発明を適用した認証処理を説明するフローチャートである。

【図7】本発明を適用した認証処理を説明するフローチャートである。

【図8】認証ボタンの押下のタイミングを示すタイミングチャートである。

【図9】本発明を適用した認証処理を説明するフローチャートである。

【図10】認証ボタンの押下のタイミングを示すタイミングチャートである。

30

【図11】本発明を適用した認証処理を説明するフローチャートである。

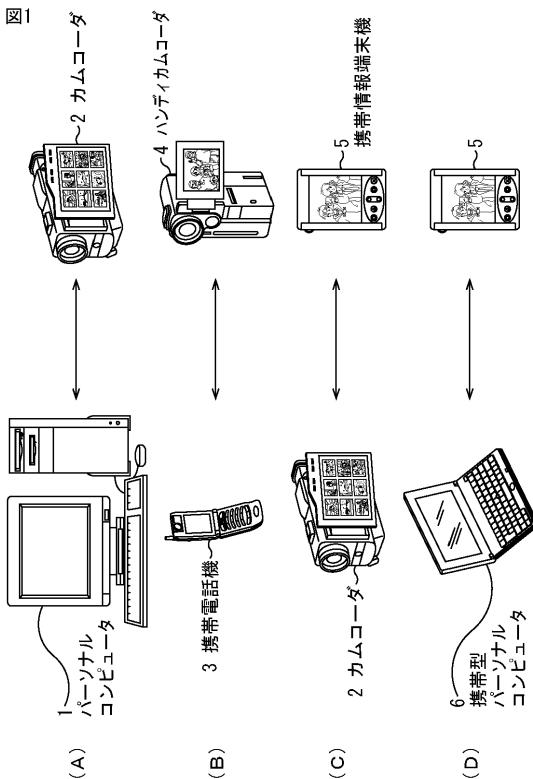
【図12】認証ボタンの押下のタイミングを示すタイミングチャートである。

【符号の説明】

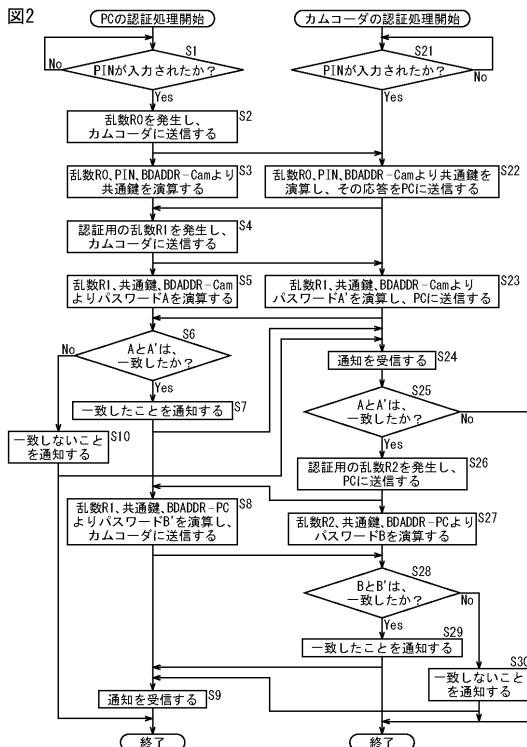
1 パーソナルコンピュータ, 2 カムコーダ, 22a 認証プログラム, 26 認証ボタン, 32a 認証プログラム, 35 認証ボタン

【 図 1 】

义 1

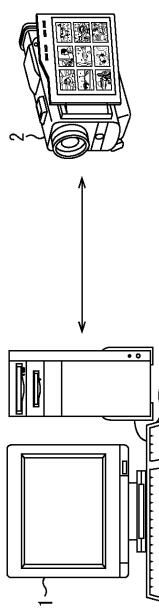


【図2】

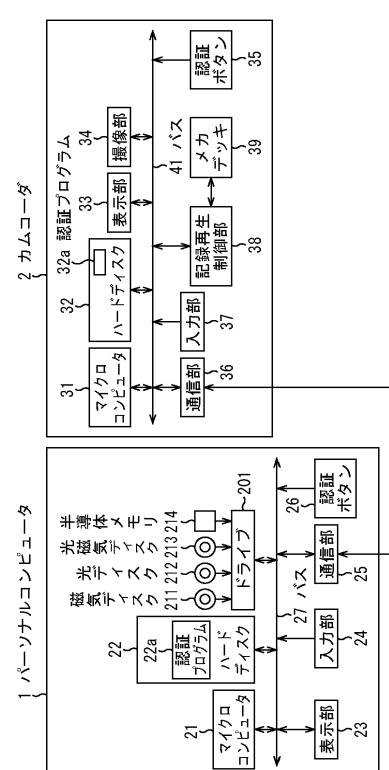


〔 3 〕

义3

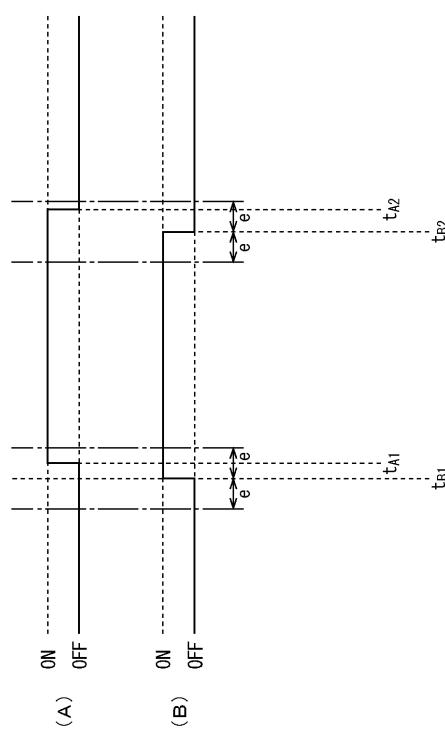


【 4 】

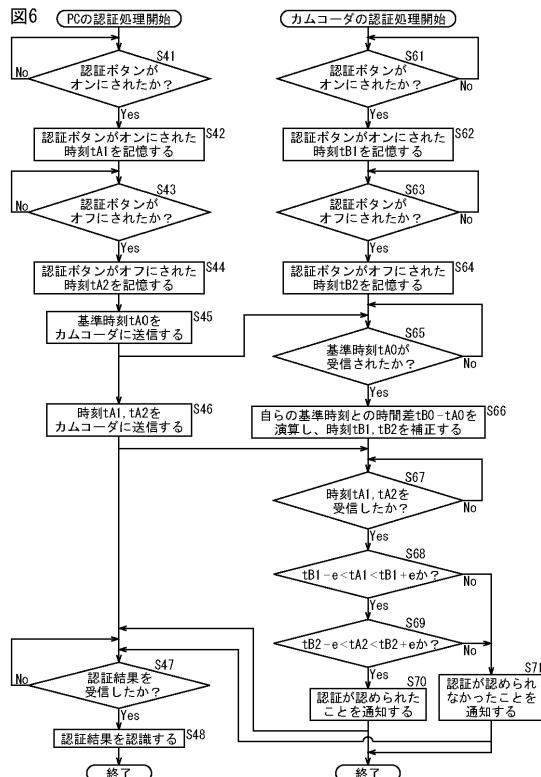


【図5】

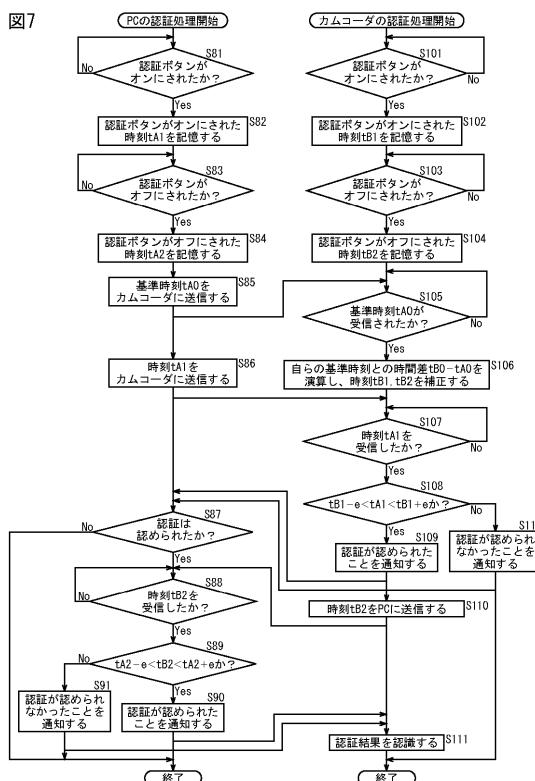
図5



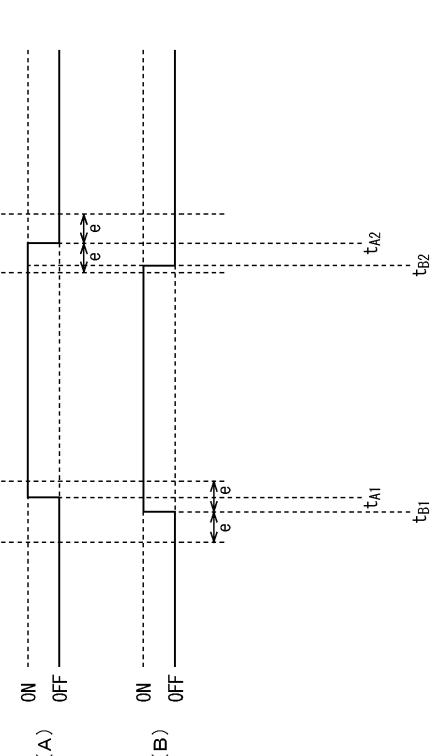
【図6】



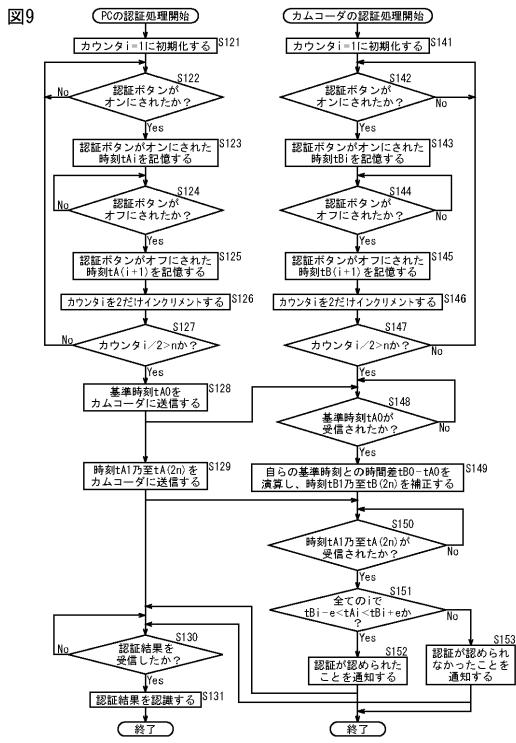
【図7】



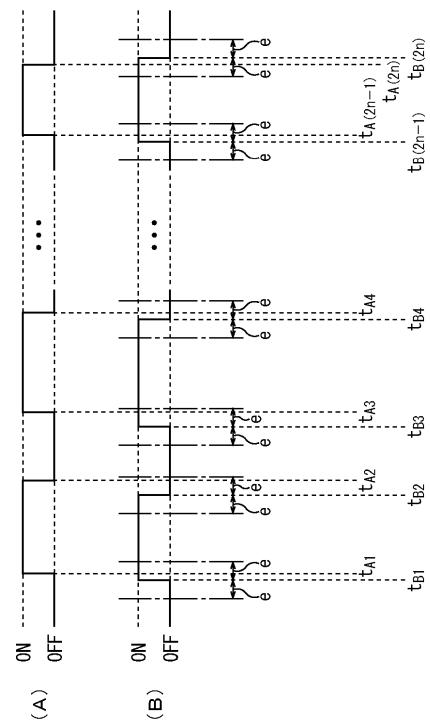
【図8】



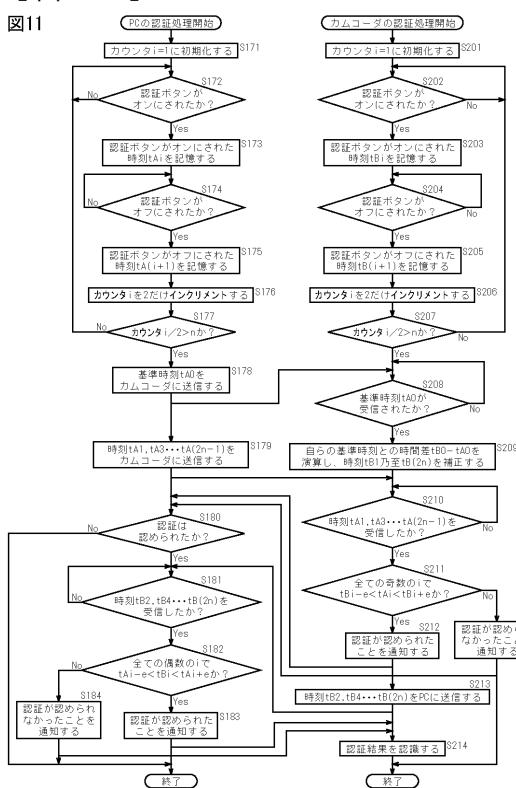
【図9】



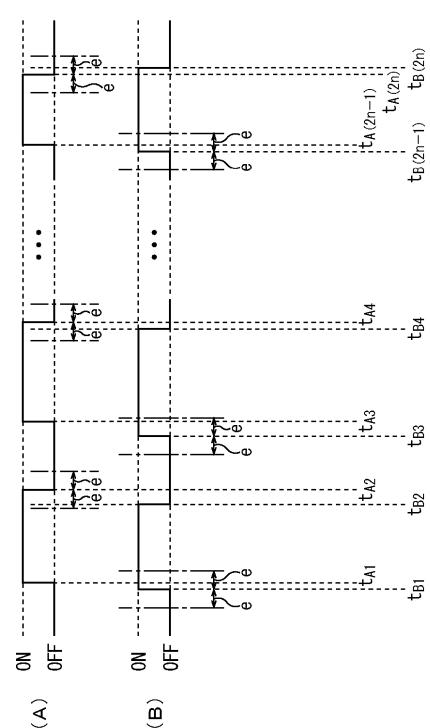
【図10】



【図11】



【図12】



フロントページの続き

(56)参考文献 特開平1-198897(JP, A)
特開平10-84589(JP, A)

(58)調査した分野(Int.Cl., DB名)
H04L12/28-46