

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第6100795号
(P6100795)

(45) 発行日 平成29年3月22日(2017.3.22)

(24) 登録日 平成29年3月3日(2017.3.3)

(51) Int.Cl. F I
G 0 6 F 21/12 (2013.01)
G 0 6 F 21/44 (2013.01)

G O 6 F 21/12
 G O 6 F 21/44

請求項の数 21 (全 71 頁)

(21) 出願番号 特願2014-546864 (P2014-546864)
 (86) (22) 出願日 平成25年11月11日(2013.11.11)
 (86) 国際出願番号 PCT/JP2013/006620
 (87) 国際公開番号 W02014/076927
 (87) 国際公開日 平成26年5月22日(2014.5.22)
 審査請求日 平成28年10月6日(2016.10.6)
 (31) 優先権主張番号 61/725,782
 (32) 優先日 平成24年11月13日(2012.11.13)
 (33) 優先権主張国 米国 (US)

(73) 特許権者 514136668
 パナソニック インテレクチュアル プロ
 パティ コーポレーション オブ アメリ
 カ
 Panasonic Intellect
 ual Property Corpor
 ation of America
 アメリカ合衆国 90503 カリフォル
 ニア州, トーランス, スイート 200,
 マリナー アベニュー 20000
 (74) 代理人 110001900
 特許業務法人 ナカジマ知的財産総合事務
 所

最終頁に続く

(54) 【発明の名称】 機器を遠隔操作するシステムにおいて用いられる方法

(57) 【特許請求の範囲】

【請求項 1】

操作端末に記憶されている制御プログラム内の遠隔操作命令の実行により、機器を遠隔操作する遠隔操作システムにおいて用いられる方法であって、

第1時点において、前記機器に対する遠隔操作元の操作端末に近接する可搬媒体に固有の第1識別子を取得する第1取得ステップと、

取得した前記第1識別子を前記操作端末に記憶されている前記制御プログラムに埋め込む埋込ステップと、

前記第1時点の後の第2時点において、前記機器に対する遠隔操作元の操作端末に近接する可搬媒体に固有の第2識別子を取得する第2取得ステップと、

前記制御プログラムに埋め込まれた前記第1識別子と、前記第2取得ステップにより取得された前記第2識別子とが一致するか否かを判断する判断ステップと、

前記第1識別子と前記第2識別子とが一致しない場合、前記機器に対する遠隔操作を禁止する禁止ステップと

を含むことを特徴とする方法。

【請求項 2】

前記操作端末は、サーバ装置を介して、前記機器を遠隔操作し、

前記サーバ装置は、前記第1識別子が埋め込まれる前の前記制御プログラムを記憶しており、

前記判断ステップは、

10

20

前記操作端末において、前記第1識別子が埋め込まれた前記制御プログラムに一方方向性演算を施して、第1演算値を生成し、生成した前記第1演算値と取得した前記第2識別子とに、演算を施して第2演算値を生成する第1ステップと、

前記サーバ装置において、記憶している前記制御プログラムに第1識別子を埋め込み、第1識別子が埋め込まれた前記制御プログラムに前記一方方向性演算と同一の一方方向性演算を施して、第3演算値を生成し、生成した前記第3演算値と取得した前記第1識別子とに、前記演算と同一の演算を施して第4演算値を生成する第2ステップと、

前記サーバ装置において、前記第2演算値と前記第4演算値とが一致するか否かを判断することにより、前記第1識別子と前記第2識別子とが一致するか否かを判断する第3ステップと

10

を含むことを特徴とする請求項1に記載の方法。

【請求項3】

前記方法において、さらに、前記第1取得ステップ、前記埋込ステップ、前記第2取得ステップ、前記判断ステップ及び前記禁止ステップによる前記第1識別子の取得、前記制御プログラムの埋込み、前記第2識別子の取得、前記判断及び前記禁止を繰り返し、

前記埋込ステップにおいて、前記第1取得ステップにより前記第1識別子が取得される都度、当該第1識別子を埋め込む

ことを特徴とする請求項1に記載の方法。

【請求項4】

前記第1時点は、前記操作端末において、前記機器に対する遠隔操作を受け付けた時であり、

20

前記第1取得ステップにおいて、前記遠隔操作を受け付ける都度、前記第1識別子を取得する

ことを特徴とする請求項3に記載の方法。

【請求項5】

前記埋込ステップにおいて、乱数を生成し、生成した乱数と取得した第1識別子とに可逆の変換を施し、得られた変換値を前記制御プログラムに埋め込み、

前記判断ステップにおいて、前記乱数と前記制御プログラムに埋め込まれた変換値とに、前記変換の逆変換を施して、前記第1識別子を復元する

ことを特徴とする請求項1に記載の方法。

30

【請求項6】

前記方法において、さらに、前記第1取得ステップ、前記埋込ステップ、前記第2取得ステップ、前記判断ステップ及び前記禁止ステップによる前記第1識別子の取得、前記制御プログラムの埋込み、前記第2識別子の取得、前記判断及び前記禁止を繰り返し、

前記埋込ステップにおいて、前記第1取得ステップにより前記第1識別子が取得される都度、異なる乱数を生成し、生成した乱数と取得した前記第1識別子とに前記変換を施し、得られた前記変換値を前記制御プログラムに埋め込む

ことを特徴とする請求項5に記載の方法。

【請求項7】

前記判断ステップにおいて、前記第1識別子が埋め込まれた前記制御プログラムを取得し、取得した前記制御プログラムから前記第1識別子を抽出する

40

ことを特徴とする請求項1に記載の方法。

【請求項8】

前記埋込ステップにおいて、前記第1識別子を分割して複数の識別子片を生成し、生成した複数の識別子片を、前記制御プログラムの全体又はその一部に分散して埋め込み、

前記判断ステップにおいて、前記制御プログラムの全体又はその一部から、前記複数の識別子片を抽出し、抽出して得られた前記複数の識別子片を結合して前記第1識別子を復元する

ことを特徴とする請求項1に記載の方法。

【請求項9】

50

前記制御プログラムは、命令が記録されている命令領域と、データが記録されているデータ領域を含み、

前記埋込ステップにおいて、前記第1識別子を、前記制御プログラム中の前記データ領域に埋め込む

ことを特徴とする請求項1に記載の方法。

【請求項10】

前記制御プログラムは、命令が記録されている命令領域と、データが記録されているデータ領域を含み、前記命令領域は、実行されないダミー命令を含み、

前記埋込ステップにおいて、前記第1識別子を、前記制御プログラム中の前記ダミー命令に埋め込む

10

ことを特徴とする請求項1に記載の方法。

【請求項11】

前記埋込ステップにおいて、前記制御プログラムに対する前記第1識別子の埋込みを制御する埋込プログラムを取得し、前記操作端末において取得した前記埋込プログラムが実行されることにより、前記第1識別子が前記制御プログラムに埋め込まれる

ことを特徴とする請求項1に記載の方法。

【請求項12】

前記埋込プログラムは、前記制御プログラムにおける前記第1識別子の埋込み位置を記憶しており、

前記埋込ステップにおいて、前記操作端末において前記埋込プログラムが実行されることにより、前記第1識別子が前記制御プログラム内の前記埋込み位置に埋め込まれる

20

ことを特徴とする請求項11に記載の方法。

【請求項13】

前記第1時点は、前記制御プログラムが前記操作端末にインストールされる時、前記操作端末における前記制御プログラムの最初の起動時、又は、前記操作端末における前記制御プログラムの起動時であり、

前記第2時点は、前記操作端末において、前記機器に対する遠隔操作を受け付けた時である

ことを特徴とする請求項1に記載の方法。

【請求項14】

30

前記第1時点は、前記操作端末において、前記機器に対する第1遠隔操作を受け付けた時であり、

前記第2時点は、前記操作端末において、前記機器に対する第2遠隔操作を受け付けた時である

ことを特徴とする請求項1に記載の方法。

【請求項15】

前記操作端末は、サーバ装置を介して、前記機器を遠隔操作し、

前記方法は、さらに、

前記操作端末において、前記機器に対する複数の遠隔操作のうち、利用者により選択可能な遠隔操作を表示する表示ステップと、

40

前記操作端末において、利用者から、表示された遠隔操作のうちの遠隔操作を受け付ける受付ステップと、

前記操作端末において、受け付けた遠隔操作を、前記サーバ装置を介して、前記機器に対して送信する送信ステップと

を含むことを特徴とする請求項1に記載の方法。

【請求項16】

前記操作端末は、サーバ装置を介して、前記機器を遠隔操作し、

前記方法は、さらに、

前記操作端末において、前記機器に対する遠隔操作に対応付けて、前記遠隔操作を受け付けるための第1条件と、前記第1条件に代えて前記遠隔操作を受け付けるための変更候

50

補としての第2条件とを表示する表示ステップと、

前記操作端末において、利用者から、前記第2条件の指定を受け付ける受付ステップと

、
指定を受け付けた前記第2条件を、前記操作端末から前記サーバ装置に対して送信する送信ステップと、

前記サーバ装置において、前記機器に対する前記遠隔操作に対応付けて、前記第1条件に代えて、前記第2条件を記憶する記憶ステップと

を含むことを特徴とする請求項1に記載の方法。

【請求項17】

記憶されている制御プログラム内の遠隔操作命令の実行により機器を遠隔操作する操作端末と、前記機器との間において、遠隔操作を中継するサーバ装置であって、

第1時点において、前記機器に対する遠隔操作元の操作端末に近接する可搬媒体に固有の第1識別子を取得する第1取得手段と、

取得した前記第1識別子を前記操作端末に記憶されている前記制御プログラムに埋め込ませるために、前記第1識別子を前記操作端末に送信する送信手段と、

前記第1時点の後の第2時点において、前記機器に対する遠隔操作元の操作端末に近接する可搬媒体に固有の第2識別子を取得する第2取得手段と、

前記制御プログラムに埋め込まれた前記第1識別子と、前記第2取得手段により取得された前記第2識別子とが一致するか否かを判断する判断手段と、

前記第1識別子と前記第2識別子とが一致しない場合、前記機器に対する遠隔操作を禁止する禁止手段と

を備えることを特徴とするサーバ装置。

【請求項18】

記憶されている制御プログラム内の遠隔操作命令の実行により機器を遠隔操作する操作端末と、前記機器との間において、遠隔操作を中継するサーバ装置において用いられるコンピュータプログラムを記録しているコンピュータ読取可能な記録媒体であって、

第1時点において、前記機器に対する遠隔操作元の操作端末に近接する可搬媒体に固有の第1識別子を取得する第1取得ステップと、

取得した前記第1識別子を前記操作端末に記憶されている前記制御プログラムに埋め込ませるために、前記第1識別子を前記操作端末に送信する送信ステップと、

前記第1時点の後の第2時点において、前記機器に対する遠隔操作元の操作端末に近接する可搬媒体に固有の第2識別子を取得する第2取得ステップと、

前記制御プログラムに埋め込まれた前記第1識別子と、前記第2取得ステップにより取得された前記第2識別子とが一致するか否かを判断する判断ステップと、

前記第1識別子と前記第2識別子とが一致しない場合、前記機器に対する遠隔操作を禁止する禁止ステップと

を実行するためのコンピュータプログラムを記録している記録媒体。

【請求項19】

記憶されている制御プログラム内の遠隔操作命令の実行により機器を遠隔操作する操作端末と、前記機器との間において、遠隔操作を中継するサーバ装置において用いられる方法であって、

第1時点において、前記機器に対する遠隔操作元の操作端末に近接する可搬媒体に固有の第1識別子を取得する第1取得ステップと、

取得した前記第1識別子を前記操作端末に記憶されている前記制御プログラムに埋め込ませるために、前記第1識別子を前記操作端末に送信する送信ステップと、

前記第1時点の後の第2時点において、前記機器に対する遠隔操作元の操作端末に近接する可搬媒体に固有の第2識別子を取得する第2取得ステップと、

前記制御プログラムに埋め込まれた前記第1識別子と、前記第2取得ステップにより取得された前記第2識別子とが一致するか否かを判断する判断ステップと、

前記第1識別子と前記第2識別子とが一致しない場合、前記機器に対する遠隔操作を禁

10

20

30

40

50

止する禁止ステップと
を含むことを特徴とする方法。

【請求項 20】

記憶されている制御プログラム内の遠隔操作命令の実行により機器を遠隔操作する操作端末と、前記機器との間において、遠隔操作を中継するサーバ装置を構成する集積回路であって、

第1時点において、前記機器に対する遠隔操作元の操作端末に近接する可搬媒体に固有の第1識別子を取得する第1取得手段と、

取得した前記第1識別子を前記操作端末に記憶されている前記制御プログラムに埋め込ませるために、前記第1識別子を前記操作端末に送信する送信手段と、

前記第1時点の後の第2時点において、前記機器に対する遠隔操作元の操作端末に近接する可搬媒体に固有の第2識別子を取得する第2取得手段と、

前記制御プログラムに埋め込まれた前記第1識別子と、前記第2取得手段により取得された前記第2識別子とが一致するか否かを判断する判断手段と、

前記第1識別子と前記第2識別子とが一致しない場合、前記機器に対する遠隔操作を禁止する禁止手段と

を備えることを特徴とする集積回路。

【請求項 21】

記憶されている制御プログラム内の遠隔操作命令の実行により機器を遠隔操作する操作端末と、前記機器と、前記操作端末と前記機器との間において、遠隔操作を中継するサーバ装置とから構成されるシステムであって、

前記サーバ装置は、

第1時点において、前記機器に対する遠隔操作元の操作端末に近接する可搬媒体に固有の第1識別子を取得する第1取得手段と、

取得した前記第1識別子を前記操作端末に記憶されている前記制御プログラムに埋め込ませるために、前記第1識別子を前記操作端末に送信する送信手段と、

前記第1時点の後の第2時点において、前記機器に対する遠隔操作元の操作端末に近接する可搬媒体に固有の第2識別子を取得する第2取得手段と、

前記制御プログラムに埋め込まれた前記第1識別子と、前記第2取得手段により取得された前記第2識別子とが一致するか否かを判断する判断手段と、

前記第1識別子と前記第2識別子とが一致しない場合、前記機器に対する遠隔操作を禁止する禁止手段とを備え、

前記操作端末は、

当該操作端末に近接する可搬媒体から、当該可搬媒体に固有の識別子を取得する取得手段と、

取得した前記識別子を前記サーバ装置に対して送信する送信手段と、

前記サーバ装置から、前記第1識別子を受信し、受信した第1識別子を前記制御プログラムに埋め込む埋込手段とを備える

ことを特徴とするシステム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、機器を遠隔操作するシステムにおいて用いられる技術に関する。

【背景技術】

【0002】

近年、スマートフォンやタブレットなどのモバイル端末に対して、ネットワークなどを介して、様々なコンピュータプログラムが提供されている。これらのコンピュータプログラムを実行することにより、モバイル端末は、利用者に対して様々な機能やサービスを提供することができる。

【0003】

特許文献 1 には、ディスプレイ装置を遠隔操作するモバイル端末が開示されている。モバイル端末は、ディスプレイ装置に対する制御を受け付けるための制御画面を表示する。利用者は、モバイル端末に表示される制御画面を用いて、命令を入力する。入力された命令は、ディスプレイ装置に伝送され、ディスプレイ装置は、命令に従って、動作する。

【0004】

宅外からモバイル端末等を用いて、宅内に設置された機器を遠隔制御する場合、モバイル端末等は、例えば、利用者の本人確認のため、利用者の識別子やパスワードの入力を要求する。

【先行技術文献】

【特許文献】

10

【0005】

【特許文献 1】特開 2013-45467 号公報

【発明の概要】

【発明が解決しようとする課題】

【0006】

しかし、例えば、利用者の識別子やパスワードが第三者に知られた場合には、第三者が利用者本人に成りすまして、利用者の宅内に設置された機器を遠隔制御することが可能となるという問題がある。

【0007】

このような問題を解決するため、本発明は、不正な第三者により利用者の機器が遠隔操作されることを防ぐことができる方法、サーバ装置及びシステムを提供することを目的とする。

20

【課題を解決するための手段】

【0008】

上記目的を達成するため、本発明の一態様は、操作端末に記憶されている制御プログラム内の遠隔操作命令の実行により、機器を遠隔操作する遠隔操作システムにおいて用いられる方法であって、第 1 時点において、前記機器に対する遠隔操作元の操作端末に近接する可搬媒体に固有の第 1 識別子を取得する第 1 取得ステップと、取得した前記第 1 識別子を前記操作端末に記憶されている前記制御プログラムに埋め込む埋込ステップと、前記第 1 時点の後の第 2 時点において、前記機器に対する遠隔操作元の操作端末に近接する可搬媒体に固有の第 2 識別子を取得する第 2 取得ステップと、前記制御プログラムに埋め込まれた前記第 1 識別子と、前記第 2 取得ステップにより取得された前記第 2 識別子とが一致するか否かを判断する判断ステップと、前記第 1 識別子と前記第 2 識別子とが一致しない場合、前記機器に対する遠隔操作を禁止する禁止ステップとを含むことを特徴とする。

30

【発明の効果】

【0009】

この態様によると、不正な第三者により利用者の機器が遠隔操作されることを防ぐことができる。

【図面の簡単な説明】

【0010】

40

【図 1】本発明の実施の形態 2 としての遠隔操作システム 10 のシステム構成図である。

【図 2】配信サーバ装置 100 の構成を示すブロック図である。

【図 3】確認サーバ装置 200 の構成を示すブロック図である。

【図 4】制御プログラム 231 のデータ構造の一例を示す。

【図 5】付随データ 251 のデータ構造の一例を示す。

【図 6】アカウント管理テーブル 261 のデータ構造の一例を示す。

【図 7】条件テーブル 271 のデータ構造の一例を示す。

【図 8】制御ルール管理テーブル 281 のデータ構造の一例を示す。

【図 9】端末装置 300 の構成を示すブロック図である。

【図 10】インストールされた制御プログラム 331 のデータ構造の一例を示す。

50

- 【図 1 1】 端末装置 3 0 0 において動作する制御プログラム 3 3 1 の機能構成図を示す。
- 【図 1 2】 端末装置 3 0 0 において表示される機器操作画面 3 5 1 を示す。
- 【図 1 3】 端末装置 3 0 0 において表示される制御ルール変更画面 3 6 1 を示す。
- 【図 1 4】 メモリカード 4 0 0 の構成を示すブロック図である。
- 【図 1 5】 確認サーバ装置 2 0 0 の相互認証部 2 0 3 及びメモリカード 4 0 0 の相互認証部 4 0 3 の構成を示すブロック図である。
- 【図 1 6】 機器 5 0 0 の構成を示すブロック図である。
- 【図 1 7】 遠隔操作システム 1 0 における制御プログラムの制作及び配信処理の手順を示すシーケンス図である。
- 【図 1 8】 遠隔操作システム 1 0 における制御プログラムの起動の手順を示すシーケンス図（その 1）である。図 1 9 へ続く。 10
- 【図 1 9】 遠隔操作システム 1 0 における制御プログラムの起動の手順を示すシーケンス図（その 2）である。図 2 0 へ続く。
- 【図 2 0】 遠隔操作システム 1 0 における制御プログラムの起動の手順を示すシーケンス図（その 3）である。
- 【図 2 1】 遠隔操作システム 1 0 における各機器に対する遠隔処理及び関連する処理の手順を示すフローチャートである。
- 【図 2 2】 遠隔操作システム 1 0 における機器情報取得処理の手順を示すシーケンス図である。
- 【図 2 3】 遠隔操作システム 1 0 における遠隔操作関連処理の手順を示すシーケンス図である。 20
- 【図 2 4】 遠隔操作システム 1 0 における機器制御ルール修正処理の手順を示すシーケンス図である。
- 【図 2 5】 遠隔操作システム 1 0 の確認サーバ装置 2 0 0 とメモリカード 4 0 0 との間における相互認証及び鍵共有の手順を示すシーケンス図（その 1）である。図 2 6 へ続く。
- 【図 2 6】 遠隔操作システム 1 0 の確認サーバ装置 2 0 0 とメモリカード 4 0 0 との間における相互認証及び鍵共有の手順を示すシーケンス図（その 2）である。
- 【図 2 7】 本発明の一態様である遠隔操作システム 1 0 a のシステム構成を示す。
- 【図 2 8】 本発明の一態様である遠隔操作システム 1 0 b における動作手順を示すシーケンス図である。 30
- 【図 2 9】 遠隔操作システム 1 0 b において、制御プログラム 6 0 5 に対する複数の識別子片の埋め込み及び複数の識別子片の結合を示す図である。この図においては、複数の識別子片が、制御プログラム 6 0 5 の全体に分散して埋め込まれる。
- 【図 3 0】 遠隔操作システム 1 0 b において、制御プログラム 6 0 5 に対する複数の識別子片の埋め込み及び複数の識別子片の結合を示す図である。この図においては、複数の識別子片が、制御プログラム 6 0 5 の一部分に分散して埋め込まれる。
- 【図 3 1】 遠隔操作システム 1 0 b において、制御プログラム 6 5 1 内のダミー命令 6 5 4 に第 1 識別子の埋め込みを示す図である。
- 【図 3 2】 遠隔操作システム 1 0 b において、埋込プログラム 6 6 6 の実行により、制御プログラム 6 6 2 に対する第 1 識別子の埋め込みを示す図である。 40
- 【図 3 3】 本発明の一態様である遠隔操作システム 1 0 c における動作手順を示すシーケンス図である。
- 【図 3 4】 本発明の一態様である遠隔操作システム 1 0 d における動作手順を示すシーケンス図である。
- 【図 3 5】 本発明の実施の形態 1 としての遠隔操作システム 1 0 e における動作手順を示すフローチャートである。
- 【発明を実施するための形態】
- 【0 0 1 1】

本発明の一態様は、操作端末に記憶されている制御プログラム内の遠隔操作命令の実行により、機器を遠隔操作する遠隔操作システムにおいて用いられる方法であって、第 1 時 50

点において、前記機器に対する遠隔操作元の操作端末に近接する可搬媒体に固有の第1識別子を取得する第1取得ステップと、取得した前記第1識別子を前記操作端末に記憶されている前記制御プログラムに埋め込む埋込ステップと、前記第1時点の後の第2時点において、前記機器に対する遠隔操作元の操作端末に近接する可搬媒体に固有の第2識別子を取得する第2取得ステップと、前記制御プログラムに埋め込まれた前記第1識別子と、前記第2取得ステップにより取得された前記第2識別子とが一致するか否かを判断する判断ステップと、前記第1識別子と前記第2識別子とが一致しない場合、前記機器に対する遠隔操作を禁止する禁止ステップとを含むことを特徴とする。

【0012】

この態様によると、不正な第三者により利用者の機器が遠隔操作されることを防ぐことができる。

10

【0013】

ここで、前記操作端末は、サーバ装置を介して、前記機器を遠隔操作してもよい。前記サーバ装置は、前記第1識別子が埋め込まれる前の前記制御プログラムを記憶している。前記判断ステップは、前記操作端末において、前記第1識別子が埋め込まれた前記制御プログラムに一方方向性演算を施して、第1演算値を生成し、生成した前記第1演算値と取得した前記第2識別子とに、演算を施して第2演算値を生成する第1ステップと、前記サーバ装置において、記憶している前記制御プログラムに第1識別子を埋め込み、第1識別子が埋め込まれた前記制御プログラムに前記一方方向性演算と同一の一方方向性演算を施して、第3演算値を生成し、生成した前記第3演算値と取得した前記第1識別子とに、前記演算と同一の演算を施して第4演算値を生成する第2ステップと、前記サーバ装置において、前記第2演算値と前記第4演算値とが一致するか否かを判断することにより、前記第1識別子と前記第2識別子とが一致するか否かを判断する第3ステップとを含むとしてもよい。

20

【0014】

この構成によると、第1識別子と第2識別子とを直接比較することなく、一致の判断をすることができる。

【0015】

ここで、前記方法において、さらに、前記第1取得ステップ、前記埋込ステップ、前記第2取得ステップ、前記判断ステップ及び前記禁止ステップによる前記第1識別子の取得、前記制御プログラムの埋込み、前記第2識別子の取得、前記判断及び前記禁止を繰り返し、前記埋込ステップにおいて、前記第1取得ステップにより前記第1識別子が取得される都度、当該第1識別子を埋め込むとしてもよい。

30

【0016】

この構成によると、第1識別子の埋め込みを繰り返すので、不正な遠隔操作に対する防御性を高めることができる。

【0017】

ここで、前記第1時点は、前記操作端末において、前記機器に対する遠隔操作を受け付けた時であり、前記第1取得ステップにおいて、前記遠隔操作を受け付ける都度、前記第1識別子を取得してもよい。

40

【0018】

ここで、前記埋込ステップにおいて、乱数を生成し、生成した乱数と取得した第1識別子とに可逆の変換を施し、得られた変換値を前記制御プログラムに埋め込み、前記判断ステップにおいて、前記乱数と前記制御プログラムに埋め込まれた変換値とに、前記変換の逆変換を施して、前記第1識別子を復元してもよい。

【0019】

この構成によると、乱数と第1識別子から生成された変換値を埋め込むので、不正な遠隔操作に対する防御性を高めることができる。

【0020】

ここで、前記方法において、さらに、前記第1取得ステップ、前記埋込ステップ、前記

50

第2取得ステップ、前記判断ステップ及び前記禁止ステップによる前記第1識別子の取得、前記制御プログラムの埋込み、前記第2識別子の取得、前記判断及び前記禁止を繰り返し、前記埋込ステップにおいて、前記第1取得ステップにより前記第1識別子が取得される都度、異なる乱数を生成し、生成した乱数と取得した前記第1識別子とに前記変換を施し、得られた前記変換値を前記制御プログラムに埋め込むとしてもよい。

【0021】

ここで、前記判断ステップにおいて、前記第1識別子が埋め込まれた前記制御プログラムを取得し、取得した前記制御プログラムから前記第1識別子を抽出してもよい。

【0022】

この構成によると、前記制御プログラムが別の制御プログラムに改ざんされた場合に、第1識別子を抽出できる可能性が低くなり、不正な遠隔操作に対する防御性を高めることができる。

10

【0023】

ここで、前記埋込ステップにおいて、前記第1識別子を分割して複数の識別子片を生成し、生成した複数の識別子片を、前記制御プログラムの全体又はその一部に分散して埋め込み、前記判断ステップにおいて、前記制御プログラムの全体又はその一部から、前記複数の識別子片を抽出し、抽出して得られた前記複数の識別子片を結合して前記第1識別子を復元してもよい。

【0024】

この構成によると、前記制御プログラムが別の制御プログラムに改ざんされた場合に、第1識別子を抽出できる可能性が低くなり、制御プログラムの不正な改ざんに対する防御性を高めることができる。

20

【0025】

ここで、前記制御プログラムは、命令が記録されている命令領域と、データが記録されているデータ領域を含み、前記埋込ステップにおいて、前記第1識別子を、前記制御プログラム中の前記データ領域に埋め込むとしてもよい。

【0026】

この構成によると、第1識別子をデータ領域に埋め込むので、制御プログラム中の命令に影響を与えない。

【0027】

30

ここで、前記制御プログラムは、命令が記録されている命令領域と、データが記録されているデータ領域を含み、前記命令領域は、実行されないダミー命令を含み、前記埋込ステップにおいて、前記第1識別子を、前記制御プログラム中の前記ダミー命令に埋め込むとしてもよい。

【0028】

この構成によると、第1識別子をダミー命令に埋め込むので、制御プログラム中の命令に影響を与えない。

【0029】

ここで、前記埋込ステップにおいて、前記制御プログラムに対する前記第1識別子の埋込みを制御する埋込プログラムを取得し、前記操作端末において取得した前記埋込プログラムが実行されることにより、前記第1識別子が前記制御プログラムに埋め込まれるとしてもよい。

40

【0030】

この構成によると、埋込プログラムにより、第1識別子の埋込みを制御することができる。

【0031】

ここで、前記埋込プログラムは、前記制御プログラムにおける前記第1識別子の埋込み位置を記憶しており、前記埋込ステップにおいて、前記操作端末において前記埋込プログラムが実行されることにより、前記第1識別子が前記制御プログラム内の前記埋込み位置に埋め込まれるとしてもよい。

50

【0032】

この構成によると、埋込プログラムにより、第1識別子を埋め込む位置を制御することができる。

【0033】

ここで、前記第1時点は、前記制御プログラムが前記操作端末にインストールされる時、前記操作端末における前記制御プログラムの最初の起動時、又は、前記操作端末における前記制御プログラムの起動時であり、前記第2時点は、前記操作端末において、前記機器に対する遠隔操作を受け付けた時であるとしてもよい。

【0034】

ここで、前記第1時点は、前記操作端末において、前記機器に対する第1遠隔操作を受け付けた時であり、前記第2時点は、前記操作端末において、前記機器に対する第2遠隔操作を受け付けた時であるとしてもよい。

10

【0035】

ここで、前記操作端末は、サーバ装置を介して、前記機器を遠隔操作してもよい。前記方法は、さらに、前記操作端末において、前記機器に対する複数の遠隔操作のうち、利用者により選択可能な遠隔操作を表示する表示ステップと、前記操作端末において、利用者から、表示された遠隔操作のうちの遠隔操作を受け付ける受付ステップと、前記操作端末において、受け付けた遠隔操作を、前記サーバ装置を介して、前記機器に対して送信する送信ステップとを含むとしてもよい。

【0036】

20

ここで、前記操作端末は、サーバ装置を介して、前記機器を遠隔操作してもよい。前記方法は、さらに、前記操作端末において、前記機器に対する遠隔操作に対応付けて、前記遠隔操作を受け付けるための第1条件と、前記第1条件に代えて前記遠隔操作を受け付けるための変更候補としての第2条件とを表示する表示ステップと、前記操作端末において、利用者から、前記第2条件の指定を受け付ける受付ステップと、指定を受け付けた前記第2条件を、前記操作端末から前記サーバ装置に対して送信する送信ステップと、前記サーバ装置において、前記機器に対する前記遠隔操作に対応付けて、前記第1条件に代えて、前記第2条件を記憶する記憶ステップとを含むとしてもよい。

【0037】

本発明の別の一態様は、記憶されている制御プログラム内の遠隔操作命令の実行により機器を遠隔操作する操作端末と、前記機器との間において、遠隔操作を中継するサーバ装置であって、第1時点において、前記機器に対する遠隔操作元の操作端末に近接する可搬媒体に固有の第1識別子を取得する第1取得手段と、取得した前記第1識別子を前記操作端末に記憶されている前記制御プログラムに埋め込ませるために、前記第1識別子を前記操作端末に送信する送信手段と、前記第1時点の後の第2時点において、前記機器に対する遠隔操作元の操作端末に近接する可搬媒体に固有の第2識別子を取得する第2取得手段と、前記制御プログラムに埋め込まれた前記第1識別子と、前記第2取得手段により取得された前記第2識別子とが一致するか否かを判断する判断手段と、前記第1識別子と前記第2識別子とが一致しない場合、前記機器に対する遠隔操作を禁止する禁止手段とを備えることを特徴とする。

30

40

【0038】

この態様によると、不正な第三者により利用者の機器が遠隔操作されることを防ぐことができる。

【0039】

本発明の別の一態様は、記憶されている制御プログラム内の遠隔操作命令の実行により機器を遠隔操作する操作端末と、前記機器との間において、遠隔操作を中継するサーバ装置において用いられるコンピュータプログラムを記録しているコンピュータ読取可能な記録媒体であって、第1時点において、前記機器に対する遠隔操作元の操作端末に近接する可搬媒体に固有の第1識別子を取得する第1取得ステップと、取得した前記第1識別子を前記操作端末に記憶されている前記制御プログラムに埋め込ませるために、前記第1識別

50

子を前記操作端末に送信する送信ステップと、前記第1時点の後の第2時点において、前記機器に対する遠隔操作元の操作端末に近接する可搬媒体に固有の第2識別子を取得する第2取得ステップと、前記制御プログラムに埋め込まれた前記第1識別子と、前記第2取得ステップにより取得された前記第2識別子とが一致するか否かを判断する判断ステップと、前記第1識別子と前記第2識別子とが一致しない場合、前記機器に対する遠隔操作を禁止する禁止ステップとを実行するためのコンピュータプログラムを記録していることを特徴とする。

【0040】

この態様によると、不正な第三者により利用者の機器が遠隔操作されることを防ぐことができる。

10

【0041】

本発明の別の一態様は、記憶されている制御プログラム内の遠隔操作命令の実行により機器を遠隔操作する操作端末と、前記機器との間において、遠隔操作を中継するサーバ装置において用いられる方法であって、第1時点において、前記機器に対する遠隔操作元の操作端末に近接する可搬媒体に固有の第1識別子を取得する第1取得ステップと、取得した前記第1識別子を前記操作端末に記憶されている前記制御プログラムに埋め込ませるために、前記第1識別子を前記操作端末に送信する送信ステップと、前記第1時点の後の第2時点において、前記機器に対する遠隔操作元の操作端末に近接する可搬媒体に固有の第2識別子を取得する第2取得ステップと、前記制御プログラムに埋め込まれた前記第1識別子と、前記第2取得ステップにより取得された前記第2識別子とが一致するか否かを判断する判断ステップと、前記第1識別子と前記第2識別子とが一致しない場合、前記機器に対する遠隔操作を禁止する禁止ステップとを含むことを特徴とする。

20

【0042】

この態様によると、不正な第三者により利用者の機器が遠隔操作されることを防ぐことができる。

【0043】

本発明の別の一態様は、記憶されている制御プログラム内の遠隔操作命令の実行により機器を遠隔操作する操作端末と、前記機器との間において、遠隔操作を中継するサーバ装置を構成する集積回路であって、第1時点において、前記機器に対する遠隔操作元の操作端末に近接する可搬媒体に固有の第1識別子を取得する第1取得手段と、取得した前記第1識別子を前記操作端末に記憶されている前記制御プログラムに埋め込ませるために、前記第1識別子を前記操作端末に送信する送信手段と、前記第1時点の後の第2時点において、前記機器に対する遠隔操作元の操作端末に近接する可搬媒体に固有の第2識別子を取得する第2取得手段と、前記制御プログラムに埋め込まれた前記第1識別子と、前記第2取得手段により取得された前記第2識別子とが一致するか否かを判断する判断手段と、前記第1識別子と前記第2識別子とが一致しない場合、前記機器に対する遠隔操作を禁止する禁止手段とを備えることを特徴とする。

30

【0044】

この態様によると、不正な第三者により利用者の機器が遠隔操作されることを防ぐことができる。

40

【0045】

本発明の別の一態様は、記憶されている制御プログラム内の遠隔操作命令の実行により機器を遠隔操作する操作端末と、前記機器と、前記操作端末と前記機器との間において、遠隔操作を中継するサーバ装置とから構成されるシステムであって、前記サーバ装置は、第1時点において、前記機器に対する遠隔操作元の操作端末に近接する可搬媒体に固有の第1識別子を取得する第1取得手段と、取得した前記第1識別子を前記操作端末に記憶されている前記制御プログラムに埋め込ませるために、前記第1識別子を前記操作端末に送信する送信手段と、前記第1時点の後の第2時点において、前記機器に対する遠隔操作元の操作端末に近接する可搬媒体に固有の第2識別子を取得する第2取得手段と、前記制御プログラムに埋め込まれた前記第1識別子と、前記第2取得手段により取得された前記第

50

2 識別子とが一致するか否かを判断する判断手段と、前記第 1 識別子と前記第 2 識別子とが一致しない場合、前記機器に対する遠隔操作を禁止する禁止手段とを備え、前記操作端末は、当該操作端末に近接する可搬媒体から、当該可搬媒体に固有の識別子を取得する取得手段と、取得した前記識別子を前記サーバ装置に対して送信する送信手段と、前記サーバ装置から、前記第 1 識別子を受信し、受信した第 1 識別子を前記制御プログラムに埋め込む埋込手段とを備えることを特徴とする。

【0046】

この態様によると、不正な第三者により利用者の機器が遠隔操作されることを防ぐことができる。

【0047】

1. 実施の形態 1

本発明に係る実施の形態 1 としての遠隔操作システム 10 e について説明する。

【0048】

(1) 操作端末に記憶されている制御プログラム内の遠隔操作命令の実行により、機器を遠隔操作する遠隔操作システム 10 e において用いられる方法について、図 35 に示すフローチャートを用いて説明する。

【0049】

遠隔操作システム 10 e において用いられる方法は、第 1 時点において、前記機器に対する遠隔操作元の操作端末に近接する可搬媒体に固有の第 1 識別子を取得する第 1 取得ステップ（ステップ S801）と、取得した前記第 1 識別子を前記操作端末に記憶されている前記制御プログラムに埋め込む埋込ステップ（ステップ S802）と、前記第 1 時点の後の第 2 時点において、前記機器に対する遠隔操作元の操作端末に近接する可搬媒体に固有の第 2 識別子を取得する第 2 取得ステップ（ステップ S803）と、前記制御プログラムに埋め込まれた前記第 1 識別子と、第 2 取得ステップにより取得された前記第 2 識別子とが一致するか否かを判断する判断ステップ（ステップ S804）と、前記第 1 識別子と前記第 2 識別子とが一致しない場合、前記機器に対する遠隔操作を禁止する禁止ステップ（ステップ S805）とを含む。

【0050】

(2) 前記操作端末は、サーバ装置を介して、前記機器を遠隔操作してもよい。前記サーバ装置は、前記第 1 識別子が埋め込まれる前の前記制御プログラムを記憶している。

【0051】

前記判断ステップは、前記操作端末において、前記第 1 識別子が埋め込まれた前記制御プログラムに方向性演算を施して、第 1 演算値を生成し、生成した前記第 1 演算値と取得した前記第 2 識別子とに、演算を施して第 2 演算値を生成する第 1 ステップと、前記サーバ装置において、記憶している前記制御プログラムに第 1 識別子を埋め込み、第 1 識別子が埋め込まれた前記制御プログラムに前記方向性演算と同一の方向性演算を施して、第 3 演算値を生成し、生成した前記第 3 演算値と取得した前記第 1 識別子とに、前記演算と同一の演算を施して第 4 演算値を生成する第 2 ステップと、前記サーバ装置において、前記第 2 演算値と前記第 4 演算値とが一致するか否かを判断することにより、前記第 1 識別子と前記第 2 識別子とが一致するか否かを判断する第 3 ステップとを含むとしてもよい。

【0052】

(3) 前記方法において、さらに、前記第 1 取得ステップ、前記埋込ステップ、前記第 2 取得ステップ、前記判断ステップ及び前記禁止ステップによる前記第 1 識別子の取得、前記制御プログラムの埋込み、前記第 2 識別子の取得、前記判断及び前記禁止を繰り返す。前記埋込ステップにおいて、前記第 1 取得ステップにより前記第 1 識別子が取得される都度、当該第 1 識別子を埋め込むとしてもよい。

【0053】

(4) 前記第 1 時点は、前記操作端末において、前記機器に対する遠隔操作を受け付けた時であるとしてもよい。

10

20

30

40

50

【0054】

ここで、前記第1取得ステップにおいて、前記遠隔操作を受け付ける都度、前記第1識別子を取得する。

【0055】

(5) 前記埋込ステップにおいて、乱数を生成し、生成した乱数と取得した第1識別子とに可逆の変換を施し、得られた変換値を前記制御プログラムに埋め込み、前記判断ステップにおいて、前記乱数と前記制御プログラムに埋め込まれた変換値とに、前記変換の逆変換を施して、前記第1識別子を復元してもよい。

【0056】

(6) 前記方法において、さらに、前記第1取得ステップ、前記埋込ステップ、前記第2取得ステップ、前記判断ステップ及び前記禁止ステップによる前記第1識別子の取得、前記制御プログラムの埋込み、前記第2識別子の取得、前記判断及び前記禁止を繰り返してもよい。

10

【0057】

前記埋込ステップにおいて、前記第1取得ステップにより前記第1識別子が取得される都度、異なる乱数を生成し、生成した乱数と取得した前記第1識別子とに前記変換を施し、得られた前記変換値を前記制御プログラムに埋め込む。

【0058】

(7) 前記判断ステップにおいて、前記第1識別子が埋め込まれた前記制御プログラムを取得し、取得した前記制御プログラムから前記第1識別子を抽出してもよい。

20

【0059】

(8) 前記埋込ステップにおいて、前記第1識別子を分割して複数の識別子片を生成し、生成した複数の識別子片を、前記制御プログラムの全体又はその一部に分散して埋め込むとしてもよい。

【0060】

前記判断ステップにおいて、前記制御プログラムの全体又はその一部から、前記複数の識別子片を抽出し、抽出して得られた前記複数の識別子片を結合して前記第1識別子を復元する。

【0061】

(9) 前記制御プログラムは、命令が記録されている命令領域と、データが記録されているデータ領域を含むとしてもよい。

30

【0062】

前記埋込ステップにおいて、前記第1識別子を、前記制御プログラム中の前記データ領域に埋め込む。

【0063】

(10) 前記制御プログラムは、命令が記録されている命令領域と、データが記録されているデータ領域を含み、前記命令領域は、実行されないダミー命令を含むとしてもよい。前記埋込ステップにおいて、前記第1識別子を、前記制御プログラム中の前記ダミー命令に埋め込む。

【0064】

40

(11) 前記埋込ステップにおいて、前記制御プログラムに対する前記第1識別子の埋込みを制御する埋込プログラムを取得し、前記操作端末において取得した前記埋込プログラムが実行されることにより、前記第1識別子が前記制御プログラムに埋め込まれるとしてもよい。

【0065】

(12) 前記埋込プログラムは、前記制御プログラムにおける前記第1識別子の埋込み位置を記憶しているとしてもよい。前記埋込ステップにおいて、前記操作端末において前記埋込プログラムが実行されることにより、前記第1識別子が前記制御プログラム内の前記埋込み位置に埋め込まれる。

【0066】

50

(13) 前記第1時点は、前記制御プログラムが前記操作端末にインストールされる時、前記操作端末における前記制御プログラムの最初の起動時、又は、前記操作端末における前記制御プログラムの起動時であるとしてもよい。

【0067】

前記第2時点は、前記操作端末において、前記機器に対する遠隔操作を受け付けた時である。

【0068】

(14) 前記第1時点は、前記操作端末において、前記機器に対する第1遠隔操作を受け付けた時であるとしてもよい。

【0069】

前記第2時点は、前記操作端末において、前記機器に対する第2遠隔操作を受け付けた時である。

【0070】

(15) 前記操作端末は、サーバ装置を介して、前記機器を遠隔操作してもよい。

【0071】

前記方法は、さらに、前記操作端末において、前記機器に対する複数の遠隔操作のうち、利用者により選択可能な遠隔操作を表示する表示ステップと、前記操作端末において、利用者から、表示された遠隔操作のうちの遠隔操作を受け付ける受付ステップと、前記操作端末において、受け付けた遠隔操作を、前記サーバ装置を介して、前記機器に対して送信する送信ステップとを含むとしてもよい。

【0072】

(16) 前記操作端末は、サーバ装置を介して、前記機器を遠隔操作してもよい。

【0073】

前記方法は、さらに、前記操作端末において、前記機器に対する遠隔操作に対応付けて、前記遠隔操作を受け付けるための第1条件と、前記第1条件に代えて前記遠隔操作を受け付けるための変更候補としての第2条件とを表示する表示ステップと、前記操作端末において、利用者から、前記第2条件の指定を受け付ける受付ステップと、指定を受け付けた前記第2条件を、前記操作端末から前記サーバ装置に対して送信する送信ステップと、前記サーバ装置において、前記機器に対する前記遠隔操作に対応付けて、前記第1条件に代えて、前記第2条件を記憶する記憶ステップとを含むとしてもよい。

【0074】

2. 実施の形態2

本発明に係る実施の形態2としての遠隔操作システム10について説明する。

【0075】

2.1 遠隔操作システム10

遠隔操作システム10は、図1に示すように、配信サーバ装置100、確認サーバ装置200、端末装置300、メモリカード400、機器500a、500b、500c、500d及び500eから構成されている。

【0076】

配信サーバ装置100、確認サーバ装置200及び端末装置300は、ネットワーク20を介して、接続されている。また、機器500a、500b、500c、500d及び500eは、利用者の家屋40に設置されている。機器500a、500b、500c、500d及び500eは、ルータ30を介して、ネットワーク20に接続されている。

【0077】

機器500a、500b、500c、500d及び500eは、それぞれ、一例として、テレビ受像機、エアコン、照明器具、ドアの施錠機構及び監視カメラである。

【0078】

端末装置300には、可搬型のメモリカード400が装着される。

【0079】

なお、以下において、機器500a、500b、500c、500d及び500eを代

10

20

30

40

50

表して、機器 500 として言及する場合がある。

【0080】

端末装置 300 は、確認サーバ装置 200 を介して、機器 500 に対して、例えば、次のような遠隔操作命令を送信する。

【0081】

テレビ受像機である機器 500 a に対して、電源の ON、OFF、チャンネルの選択、録画の予約、予約の解除、受信再生中のチャンネル情報の取得、受信再生中の番組情報の取得。エアコンである機器 500 b に対して、電源の ON、OFF、設定温度の変更、現在の温度の取得、現在の湿度の取得、冷房、暖房、送風の切換え。照明器具である機器 500 c に対して、電源の ON、OFF、明るさの切換え。ドアの施錠機構である機器 500 d に対して、施錠、開錠、施錠されているか、開錠されているかを示す施錠状況の取得。監視カメラである機器 500 e に対して、録画の開始、録画の停止、録画された映像のテレビ受像機への転送、録画された映像の削除。

10

【0082】

確認サーバ装置 200 は、機器を遠隔操作するための制御プログラムを配信サーバ装置 100 に対して送信する。端末装置 300 は、配信サーバ装置 100 から制御プログラムを受信し、受信した制御プログラムをインストールする。

【0083】

端末装置 300 は、利用者の指示により、制御プログラムを起動する。次に、端末装置 300 は、端末装置 300 に装着されたメモリカード 400 から固有識別子を取得し、取得した固有識別子を確認サーバ装置 200 に対して送信する。端末装置 300 は、付随データを記憶していれば、制御プログラムに付随データを埋め込む。

20

【0084】

確認サーバ装置 200 は、端末装置 300 から固有識別子を取得する。端末装置 300 の利用者からのログインが正常になされれば、確認サーバ装置 200 は、取得した固有識別子を含む付随データを生成し、生成した付随データを端末装置 300 に対して送信する。端末装置 300 は、付随データを受信し、受信した付随データを記憶する。

【0085】

確認サーバ装置 200 は、付随データを制御プログラムに埋め込み、制御プログラムからハッシュ値を算出し、乱数、ハッシュ値及び固有識別子を用いて、評価値 S を算出する。

30

【0086】

端末装置 300 は、メモリカード 400 から固有識別子を取得し、制御プログラムからハッシュ値を算出し、乱数、ハッシュ値及び固有識別子を用いて、評価値 S' を算出する。

【0087】

確認サーバ装置 200 は、端末装置 300 から評価値 S' を受信し、評価値 S と評価値 S' とを比較する。評価値 S と評価値 S' とが一致すれば、機器に対する遠隔操作を許可する。評価値 S と評価値 S' とが一致しなければ、機器に対する遠隔操作を禁止する。

【0088】

2. 2 配信サーバ装置 100

配信サーバ装置 100 は、図 2 に示すように、制御部 101、通信部 102、相互認証部 103、鍵格納部 104、記憶部 105、アカウント格納部 106 及びアカウント確認部 107 から構成されている。

40

【0089】

配信サーバ装置 100 は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクデバイスなどから構成されるコンピュータシステムである。前記 RAM 又は前記ハードディスクデバイスには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、配信サーバ装置 100 は、その機能を達成する。

50

【0090】

(1) 鍵格納部104及び記憶部105

鍵格納部104は、一例として、ハードディスクデバイスから構成されている。鍵格納部104は、配信サーバ装置100に割り当てられた私有鍵を記憶している。また、予め、システム鍵Kscを記憶している。システム鍵Kscは、遠隔操作システムに共通の鍵である。なお、確認サーバ装置200、端末装置300及びメモリカード400が有するどの鍵格納部も、鍵格納部104が有するシステム鍵Kscと同一のシステム鍵Kscを予め記憶している。

【0091】

記憶部105は、一例として、ハードディスクデバイスから構成されている。記憶部105は、制御プログラムを記憶するための領域を備えている。

【0092】

(2) 通信部102

通信部102は、ネットワーク20を介して、確認サーバ装置200及び端末装置300との間で、情報の送受信を行う。

【0093】

具体的には、通信部102は、確認サーバ装置200から、ネットワーク20を介して、安全な手段により、制御プログラムを受信する。制御プログラムを受信すると、通信部102は、受信した制御プログラムを記憶部105に書き込む。また、通信部102は、端末装置300から、ネットワーク20を介して、制御プログラムの要求を受信する。制御プログラムの要求を受信すると、通信部102は、受信した要求を制御部101に対して出力する。また、通信部102は、端末装置300から、ネットワーク20を介して、安全な手段により、利用者識別子及びパスワードを受信する。利用者識別子及びパスワードを受信すると、通信部102は、受信した利用者識別子及びパスワードをアカウント確認部107に対して出力する。

【0094】

また、通信部102は、制御部101の制御により、利用者識別子及びパスワードの要求を、端末装置300に対して送信する。また、通信部102は、制御部101の制御により、記憶部105に記憶されている制御プログラムを読み出す。次に、通信部102は、読み出した制御プログラムを、安全な手段により、端末装置300に対して送信する。また、通信部102は、制御部101の制御により、メッセージを端末装置300に対して送信する。なお、安全な手段については、後述する。

【0095】

(3) アカウント格納部106及びアカウント確認部107

アカウント格納部106は、利用者に割り当てられた利用者識別子及び利用者のパスワードを対応付けて記憶している。利用者識別子及びパスワードは、配信サーバ装置100の操作者により、入力されたものである。

【0096】

アカウント確認部107は、端末装置300から、ネットワーク20及び通信部102を介して、安全な手段により、端末装置300の利用者の利用者識別子及びパスワードを受信する。利用者識別子及びパスワードを受信すると、次に、アカウント確認部107は、受信した利用者識別子及びパスワードが、アカウント格納部106において、記憶されているか否かを確認する。

【0097】

受信した利用者識別子及びパスワードが、アカウント格納部106に記憶されていない場合、アカウント確認部107は、ログインに失敗した（ログイン異常）とみなす。受信した利用者識別子及びパスワードが、アカウント格納部106に記憶されている場合、アカウント確認部107は、ログインに成功した（ログイン正常）とみなす。

【0098】

受信した利用者識別子及びパスワードが、アカウント格納部106において、記憶され

10

20

30

40

50

ていない場合、つまり、ログイン異常の場合、アカウント確認部107は、ログイン異常を示すメッセージを生成する。次に、アカウント確認部107は、生成したメッセージを、通信部102及びネットワーク20を介して、端末装置300に対して送信する。次に、アカウント確認部107は、受信した利用者識別子及びパスワードによるログインを禁止する。

【0099】

受信した利用者識別子及びパスワードが、アカウント格納部106において、記憶されている場合、アカウント確認部107は、受信した利用者識別子及びパスワードによるログインを許可する。

【0100】

アカウント確認部107は、ログインの許可又は禁止を示す許否情報を制御部101に対して出力する。

【0101】

(4) 制御部101

制御部101は、通信部102、相互認証部103、鍵格納部104、記憶部105、アカウント格納部106及びアカウント確認部107を制御する。

【0102】

制御部101は、端末装置300から、ネットワーク20及び通信部102を介して、制御プログラムの要求を受信する。制御プログラムの要求を受信すると、制御部101は、通信部102及びネットワーク20を介して、端末装置300に対して、利用者識別子及びパスワードの要求を送信する。

【0103】

制御部101は、アカウント確認部107から、ログインの許可又は禁止を示す許否情報を受け取る。

【0104】

制御プログラムの要求を受信し、許否情報がログインの許可を示す場合、制御部101は、通信部102に対して、記憶部105から制御プログラムを読み出すように制御する。次に、通信部102に対して、読み出した制御プログラムを、安全な手段により、通信部102及びネットワーク20を介して、端末装置300に対して送信するように、制御する。

【0105】

(5) 相互認証部103

相互認証部103は、確認サーバ装置200の相互認証部203と、同様の構成を有している。

【0106】

相互認証部103は、制御プログラムを受信する場合に、確認サーバ装置200の相互認証部203との間で、相互認証及び鍵共有を行う。また、相互認証部103は、制御プログラムを送信する場合に、端末装置300の相互認証部303との間で、相互認証及び鍵共有を行う。なお、相互認証及び鍵共有については、後述する。

【0107】

また、相互認証部103は、確認サーバ装置200又は端末装置300との間の安全な手段による通信を支援する。なお、安全な手段による通信については、後述する。

【0108】

2.3 確認サーバ装置200

確認サーバ装置200は、図3に示すように、制御部201、通信部202、相互認証部203、鍵格納部204、プログラム制作部206、プログラム格納部207、付随データ生成部208、アカウント格納部209、信頼性評価部210、機器情報格納部212、機器制御部213、署名生成部214、アカウント確認部215及び固有識別子取得部216から構成されている。

【0109】

確認サーバ装置 200 は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクデバイス、ディスプレイデバイス、キーボードなどから構成されるコンピュータシステムである。前記 RAM 又は前記ハードディスクデバイスには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、確認サーバ装置 200 は、その機能を達成する。

【0110】

(1) プログラム格納部 207、鍵格納部 204 及び機器情報格納部 212

(プログラム格納部 207)

プログラム格納部 207 は、一例として、ハードディスクデバイスから構成されている。プログラム格納部 207 は、制御プログラム 231 及び制御プログラム 331 を格納するための領域を備えている。

10

【0111】

制御プログラム 231 は、配信サーバ装置 100 を介して、端末装置 300 に対して配信すべきコンピュータプログラムである。一方、制御プログラム 331 は、端末装置 300 においてインストールされたコンピュータプログラムと同一のコンピュータプログラムである。確認サーバ装置 200 が端末装置 300 においてインストールされた制御プログラムの状態を再現するために、プログラム格納部 207 は、制御プログラム 331 を記憶するための領域を備えている。

【0112】

(a) 図 4 に制御プログラム 231 のデータ構造を示す。この図に示すように、制御プログラム 231 は、実行部領域 232、第 1 データ領域 233 及び署名領域 234 から構成されている。

20

【0113】

実行部領域 232 には、複数の命令群 232a、232b、・・・が記録されている。各命令群は、端末装置 300 において実行されるオペレーションコマンドを含む。第 1 データ領域 233 は、複数の命令群 232a、232b、・・・が実行される際に、参照のみされるデータ 233a、233b、・・・を含む。署名領域 234 は、署名データ 234a を含む。

【0114】

署名データ 234a は、署名生成部 214 により生成される。署名データ 234a は、確認サーバ装置 200 に割り当てられた私有鍵 241 を用いて、制御プログラム 231 の実行部領域 232 及び第 1 データ領域 233 に、デジタル署名 Sign を施して得られた署名データである。

30

【0115】

署名データ 234a = Sign (私有鍵 241、(実行部領域 232 及び第 1 データ領域 233))

ここで、Sign (A、B) は、私有鍵 A を用いて、データ B に対して、デジタル署名 Sign を施すことにより、生成された署名データを示す。ここで、デジタル署名 Sign は、一例として、ECDSA (Elliptic Curve Digital Signature Standard) によるデジタル署名アルゴリズムである。

40

【0116】

署名データ 234a を用いて、デジタル署名 Sign に対応するデジタル署名検証 Vrfy を行うことにより、実行部領域 232 及び第 1 データ領域 233 が改ざんされていないことを確認することができる。ここで、デジタル署名検証 Vrfy は、一例として、ECDSA (Elliptic Curve Digital Signature Standard) によるデジタル署名検証アルゴリズムである。

【0117】

(b) 図 10 に制御プログラム 331 のデータ構造を示す。この図に示すように、制御プログラム 331 は、実行部領域 332、第 1 データ領域 333、署名領域 334、第 2 データ領域 335 及び第 3 データ領域 336 から構成されている。

50

【0118】

実行部領域332には、複数の命令群332a、332b、・・・が記録されている。各命令群は、端末装置300において実行されるオペレーションコマンドを含む。第1データ領域333は、複数の命令群332a、332b、・・・が実行される際に、参照のみされるデータ333a、333b、・・・を含む。署名領域334は、署名データ334aを含む。

【0119】

実行部領域332、第1データ領域333及び署名領域334は、それぞれ、図4に示す実行部領域232、第1データ領域233及び署名領域234と同一である。実行部領域332に含まれている複数の命令群332a、332b、・・・は、図4に示す複数の命令群232a、232b、・・・と同一である。第1データ領域333に含まれているデータ333a、333b、・・・は、図4に示すデータ233a、233b、・・・と同一である。また、署名領域334に含まれている署名データ334aは、図4に示す署名データ234aと同一である。

10

【0120】

第2データ領域335には、付随データ335aが含まれる。付随データ335aについては、後述する。

【0121】

第3データ領域336には、データ336aが含まれる。データ336aは、命令群332a、332b、・・・により、追加の書き込み、更新、上書き、参照がされるデータである。

20

【0122】

(鍵格納部204)

鍵格納部204は、一例として、ハードディスクデバイスから構成されている。鍵格納部204は、確認サーバ装置200に割り当てられた私有鍵241を記憶している。また、予め、システム鍵Kscを記憶している。

【0123】

(機器情報格納部212)

機器情報格納部212は、予め、条件テーブル271及び制御ルール管理テーブル281を保持している。

30

【0124】

条件テーブル271は、図7に一例として示すように、複数の条件情報を記憶するための領域を備えている。

【0125】

各条件情報は、機器情報及び条件を対応付けて含む。機器情報は、機器に関する情報の種類を示す。条件は、機器情報により示される機器状態情報を取得するための条件を示す。機器状態情報は、機器情報によりその種類が示され、機器における現実の状態を示す情報である。

【0126】

ここで、機器がエアコンである場合、機器情報の一例は、「エアコンの室内温度、湿度」である。また、機器情報により示される機器状態情報の一例は、当該エアコンにより現実的に測定された室内温度「25度」及び湿度「50パーセント」である。

40

【0127】

また、機器がテレビ受像機である場合、機器情報の一例は、「再生中のチャンネル」である。また、機器情報により示される機器状態情報の一例は、当該テレビ受像機により現実的に再生されているチャンネル「16」である。

【0128】

また、機器がDVD再生装置である場合、機器情報の一例は、「再生中のDVDのタイトル」である。また、機器情報により示される機器状態情報の一例は、当該DVD再生装置により現実的に再生されているDVDのタイトル「銀河戦争」である。

50

【0129】

条件の具体例は、端末装置300から、確認サーバ装置200に対して、ログインしている必要があるか否か、及び、端末装置300に装着されたメモリカード400の固有識別子が必要であるか否かである。

【0130】

条件テーブル271は、一例として、条件情報272を含んでいる。条件情報272は、機器情報273「エアコンの室内温度、湿度」及び条件274「ログイン不要、固有識別子要」を対応付けて含む。この条件情報272は、機器であるエアコンにより測定された室内温度及び湿度を、ネットワーク20を介して、端末装置300が取得するためには、端末装置300から、確認サーバ装置200に対して、ログインは不要であるが、固有識別子が必要であることを示している。

10

【0131】

制御ルール管理テーブル281は、図8に示すように、利用者識別子と、複数の制御ルール情報とを対応付けて記憶するための領域を備えている。

【0132】

利用者識別子は、遠隔操作システム10の利用者を識別するための識別情報である。各制御ルール情報は、操作内容、条件及び項目を含む。操作内容は、利用者に許可することができる操作の内容を示す。条件は、当該操作内容を利用者に許可する場合の条件を示す。項目は、操作内容により操作の対象となる項目を示す。

【0133】

20

制御ルール管理テーブル281は、図8に示すように、一例として、制御ルール情報283を含む。制御ルール情報283は、操作内容284「ドア開閉」、条件285「固有識別子要」及び項目286「施錠」を含む。

【0134】

このように、制御ルール情報283は、ドアを開閉するという操作内容に対し、固有識別子が必要であり、この操作内容においては、施錠が操作の対象となる、ことを示している。

【0135】

(2) プログラム制作部206

プログラム制作部206は、確認サーバ装置200の利用者の操作により、制御プログラムを制作する。プログラム制作部206は、制作された制御プログラムをプログラム格納部207に書き込む。

30

【0136】

制御プログラムは、遠隔操作の対象である機器500に関する情報の取得、機器500の遠隔操作に関連する操作、機器制御ルールの修正及びその他の指示をするためのコンピュータプログラムを含んでいる。

【0137】

ここで、制作される制御プログラムは、一例として、図4に示す制御プログラム231のうち、実行部領域232及び第1データ領域233からなる。

【0138】

40

また、プログラム制作部206は、確認サーバ装置200の利用者の操作により、プログラム格納部207から、図4に示す制御プログラム231を読み出す。次に、読み出した制御プログラム231を、プログラム格納部207にインストールする。この結果、図10に示す制御プログラム331がプログラム格納部207に格納される。制御プログラム331においては、上述したように、制御プログラム231に対して、第2データ領域335及び第3データ領域336が付加されている。この時点において、第2データ領域335及び第3データ領域336は、何も記録されていない初期状態である。

【0139】

(3) アカун ト格納部209及びアカウン ト確認部215

(アカウン ト格納部209)

50

アカウント格納部 209 は、アカウント管理テーブル 261 を保持している。

【0140】

アカウント管理テーブル 261 は、図 6 に一例として示すように、複数のアカウント情報を記憶するための領域を備えている。各アカウント情報は、利用者に対応している。各アカウント情報は、利用者識別子、パスワード、時変パラメータ及び固有識別子を含む。利用者識別子は、当該利用者を一意に識別するための識別情報である。パスワードは、当該利用者であることを認証するための認証情報である。時変パラメータは、その都度生成される乱数である。固有識別子は、当該利用者が有するメモリカードに固有の識別情報である。

【0141】

アカウント管理テーブル 261 は、図 6 に一例として示すように、アカウント情報 262 を含んでいる。アカウント情報 262 は、利用者識別子 263 「S A T O」、パスワード 264 「1 2 3 4」、時変パラメータ 265 「A D 7 C」及び固有識別子 266 「8 D A 4」を含む。

【0142】

(アカウント確認部 215)

アカウント確認部 215 は、端末装置 300 から、ネットワーク 20 及び通信部 202 を介して、ログインの要否を受信する。次に、アカウント確認部 215 は、受信したログインの要否が、ログインを要求することを示すか、要求しないことを示すかを判断する。

【0143】

受信したログインの要否が、ログインを要求しないことを示す場合、アカウント確認部 215 は、ログインの処理を行わない。

【0144】

受信したログインの要否が、ログインを要求することを示す場合、アカウント確認部 215 は、端末装置 300 から、ネットワーク 20 及び通信部 202 を介して、安全な手段により、利用者の利用者識別子及びパスワードを受信する。安全な手段については、後述する。次に、アカウント確認部 215 は、受信した利用者識別子及びパスワードの組が、アカウント格納部 209 のアカウント管理テーブル 261 に記憶されているか否かを確認する。

【0145】

アカウント確認部 215 は、端末装置 300 からログインの要否を受信した後、一例として、5 分以上、経過しても、端末装置 300 から利用者識別子及びパスワードを受信しない場合には、ログインに失敗した（ログイン異常）とみなす。また、受信した利用者識別子及びパスワードが、アカウント管理テーブル 261 に記憶されていない場合、アカウント確認部 215 は、ログインに失敗した（ログイン異常）とみなす。

【0146】

受信した利用者識別子及びパスワードが、アカウント管理テーブル 261 に記憶されている場合、アカウント確認部 215 は、ログインに成功した（ログイン正常）とみなす。

【0147】

アカウント確認部 215 は、ログイン正常か又はログイン異常かを示すログイン結果を制御部 201 に通知する。

【0148】

ログイン異常の場合、アカウント確認部 215 は、ログイン異常を示すメッセージを生成する。次に、アカウント確認部 215 は、当該メッセージを、通信部 202 及びネットワーク 20 を介して、端末装置 300 に対して送信する。

【0149】

(4) 固有識別子取得部 216

固有識別子取得部 216 は、制御部 201 から、接続要求を受け取る。接続要求を受け取ると、相互認証及び鍵共有がなされた後、固有識別子取得部 216 は、通信部 202、ネットワーク 20 及び端末装置 300 を介して、メモリカード 400 に対して、固有識別

10

20

30

40

50

子の要求を送信する。

【0150】

次に、固有識別子取得部216は、メモリカード400から、端末装置300、ネットワーク20及び通信部202を介して、安全な手段により、固有識別子Y又はメモリカード400に固有識別子が記録されていないことを示すメッセージ「固有識別子無し」を受信する。安全な手段については、後述する。また、固有識別子取得部216は、メモリカード400に対して、固有識別子の要求を送信した後、所定時間を経過しても、固有識別子Y又は固有識別子が記録されていないことを示すメッセージを受信しないときは、メッセージ「固有識別子無し」を生成する。ここで、所定時間は、一例として、200m秒である。

10

【0151】

次に、固有識別子取得部216は、取得した固有識別子Y又はメッセージ「固有識別子無し」を付随データ生成部208及び信頼性評価部210に対して出力する。

【0152】

(5) 制御部201

制御部201は、通信部202、相互認証部203、鍵格納部204、プログラム制作部206、プログラム格納部207、付随データ生成部208、アカウント格納部209、信頼性評価部210、機器情報格納部212、機器制御部213、署名生成部214、アカウント確認部215及び固有識別子取得部216を制御する。

【0153】

また、制御部201は、端末装置300から、ネットワーク20及び通信部202を介して、機器操作のための接続要求を受け取る。接続要求を受け取ると、制御部201は、相互認証部203及び固有識別子取得部216に対して、機器操作のための接続要求を出力する。

20

【0154】

制御部201は、アカウント確認部215から、ログイン正常か又はログイン異常かを示すログイン結果を受け取る。ログイン正常を示すログイン結果を受け取った場合、制御部201は、受信した利用者識別子及びパスワードを記憶する。

【0155】

(6) 通信部202

通信部202は、制御部201の制御により、ネットワーク20を介して、配信サーバ装置100、端末装置300、メモリカード400、機器500a、500b、500c、500d及び500eとの間で、情報の送受信を行う。

30

【0156】

具体的には、通信部202は、制御部201の制御により、ネットワーク20を介して、制御プログラムを配信サーバ装置100に対して送信する。

【0157】

また、通信部202は、制御部201の制御により、ネットワーク20及び端末装置300を介して、固有識別子の要求をメモリカード400に対して送信する。また、通信部202は、ネットワーク20を介して、メッセージ、付随データ、乱数Rを端末装置300に対して送信する。

40

【0158】

また、通信部202は、端末装置300から、ネットワーク20を介して、機器操作のための接続要求、ログインの要否、利用者識別子及びパスワード、機器に対する操作指示並びに評価値S'を受信する。通信部202は、メモリカード400から、端末装置300及びネットワーク20を介して、固有識別子Y又はメッセージ「固有識別子無し」を受信する。

【0159】

(7) 相互認証部203

相互認証部203は、制御部201から、制御プログラムの送信のための接続要求及び

50

機器操作のための接続要求を受け取る。

【0160】

制御プログラムの送信のための接続要求を受け取ると、相互認証部203は、配信サーバ装置100の相互認証部103との間で、相互認証を行い、配信サーバ装置100と同一の共有鍵を共有する。

【0161】

また、機器操作のための接続要求を受け取ると、相互認証部203は、端末装置300の相互認証部303との間で、相互認証を行い、端末装置300と同一の共有鍵を共有する。また、相互認証部203は、メモリカード400の相互認証部403との間で、相互認証を行い、メモリカード400と同一の共有鍵を共有する。

10

【0162】

相互認証部203は、図15に示すように、乱数生成部A11、乱数比較部A12、復号部A13、暗号化部A14、鍵共有部A15及び暗復号化部A16から構成されている。

【0163】

乱数生成部A10は、ランダムに乱数R1を生成する。次に、生成した乱数R1を乱数比較部A12に出力する。また、生成した乱数R1を相互認証の相手の装置の相互認証部に送信する。

【0164】

復号部A13は、相互認証の相手の装置の相互認証部から、暗号化乱数E3(Ksc、R1)を受け取る。次に、復号アルゴリズムD3により、システム鍵Kscを用いて、受け取った暗号化乱数E3(Ksc、R1)を復号して復号文R1' = D3(Ksc、E3(Ksc、R1))を生成する。次に、生成した復号文R1'を乱数比較部A12へ出力する。

20

【0165】

ここで、復号アルゴリズムD3は、秘密鍵暗号方式による復号アルゴリズムである。復号アルゴリズムD3は、一例として、AES(Advanced Encryption Standard)によるものである。E3(K、A)は、鍵Kを用いて、平文Aに対して暗号化アルゴリズムE3を施して生成した暗号文を示す。また、D3(K、B)は、鍵Kを用いて、暗号文Bに対して復号アルゴリズムD3を施して生成した復号文を示す。

30

【0166】

乱数比較部A12は、乱数生成部A11から乱数R1を受け取り、復号部A13から復号文R1'を受け取る。次に、乱数R1と復号文R1'とを比較する。乱数R1と復号文R1'とが一致する場合に、相互認証部203は、相手の装置が正当であると判断する。乱数R1と復号文R1'とが一致しない場合に、相互認証部203は、相手の装置が不正であると判断する。

【0167】

暗号化部A14は、相手の装置の相互認証部から乱数R2を受け取る。乱数R2を受け取ると、システム鍵Kscを用いて、暗号化アルゴリズムE4により、乱数R2を暗号化して、暗号化乱数E4(Ksc、R2)を生成し、生成した暗号化乱数E4(Ksc、R2)を相手の装置へ送信する。

40

【0168】

ここで、暗号化アルゴリズムE4は、秘密鍵暗号方式による暗号化アルゴリズムである。暗号化アルゴリズムE4は、一例として、AESによるものである。また、E4(K、A)は、鍵Kを用いて、平文Aに対して暗号化アルゴリズムE4を施して生成した暗号文を示す。

【0169】

相互の認証に成功すると、鍵共有部A15は、鍵共有の処理を実行して、共有鍵kを算出する。相互の認証に失敗すると、共有鍵kの算出は、行われない。

【0170】

50

相互の認証に成功すると、暗復号化部A 1 6は、算出された共有鍵kを用いて、データを暗号化して、暗号化データを生成する。暗号化データは、相手の装置に送信される。また、暗復号化部A 1 6は、相手の装置から暗号化データを受信する。次に、算出された共有鍵kを用いて、暗号化データを復号して、元のデータを生成する。この動作手順により、上述した安全な手段が実現される。

【0171】

(8) 付随データ生成部208

付随データ生成部208は、固有識別子取得部216から、取得した固有識別子Y又はメッセージ「固有識別子無し」を受信する。

【0172】

次に、付随データ生成部208は、固有識別子Yを受信しているか否かを確認する。固有識別子Yを受信している場合、付随データ生成部208は、ランダムに乱数Rを生成する。付随データ生成部208は、受信した利用者識別子及びパスワードに対応付けて、生成した乱数Rと受信した固有識別子Yとを、時変パラメータ及び固有識別子として、アカウント管理テーブル261に書き込む。

【0173】

次に、付随データ生成部208は、次の式により、固有識別子Y及び乱数Rを用いて、変数Kを算出する。

【0174】

変数K = 固有識別子Y XOR 乱数R

ここで、XORは、排他的論理和を示す演算子である。

【0175】

次に、付随データ生成部208は、図5に示すように、変数領域252及び署名領域253からなる付随データ251を生成する。この時点において、変数領域252及び署名領域253は、何も記録されていない初期状態である。

【0176】

次に、付随データ生成部208は、算出して得られた変数K(254)を変数領域252に書き込む。

【0177】

次に、付随データ生成部208は、署名生成部214に対して、変数K(254)を出力し、変数K(254)の署名データを生成するよう指示する。次に、付随データ生成部208は、署名生成部214から、変数K(254)の署名データ255を受け取る。ここで、署名データ255は、確認サーバ装置200に割り当てられた私有鍵241を用いて、変数K(254)に対して、デジタル署名Signを施して得られたデータである。署名生成部214から、署名データ255を受け取ると、付随データ生成部208は、付随データ251の署名領域253に署名データ255を書き込む。

【0178】

図5に示すように、付随データ251は、変数領域252及び署名領域253から構成されている。変数領域252は、変数K(254)を含み、署名領域253は、署名データ255を含む。

【0179】

次に、付随データ生成部208は、付随データ251及び乱数Rを、通信部202及びネットワーク20を介して、端末装置300に対して、安全な手段により、送信する。

【0180】

固有識別子Yを受信していない場合、付随データ生成部208は、乱数Rの生成、変数Kの算出、付随データの生成、署名データの生成指示及び付随データ及び乱数Rの送信を行わない。

【0181】

固有識別子Yを受信しており、機器に対する操作指示を受け取っている場合、付随データ生成部208は、プログラム格納部207に記憶され、インストールされている状態の

10

20

30

40

50

制御プログラム 3 3 1 の第 2 データ領域 3 3 5 に、変数 K (2 5 4) と署名データ 2 5 5 を含む付随データ 2 5 1 を上書きする。

【 0 1 8 2 】

付随データ 2 5 1 の上書きが完了すると、付随データ生成部 2 0 8 は、付随データ 2 5 1 の上書きが完了したことを示す完了通知を、信頼性評価部 2 1 0 に対して出力する。

【 0 1 8 3 】

固有識別子を受信していない場合、付随データ生成部 2 0 8 は、制御プログラム 3 3 1 の第 2 データ領域 3 3 5 に対する付随データの上書きを行わない。

【 0 1 8 4 】

(9) 署名生成部 2 1 4

署名生成部 2 1 4 は、プログラム制作部 2 0 6 及び付随データ生成部 2 0 8 から、署名データの生成の指示を受け取る。

【 0 1 8 5 】

プログラム制作部 2 0 6 から署名データの生成の指示を受け取ると、署名生成部 2 1 4 は、鍵格納部 2 0 4 から、確認サーバ装置 2 0 0 に割り当てられた私有鍵 2 4 1 を読み出す。次に、プログラム格納部 2 0 7 から制御プログラムを読み出す。ここで、読み出した制御プログラムは、図 4 に示すように、実行部領域 2 3 2 と第 1 データ領域 2 3 3 とを含む。しかし、読み出した制御プログラムは、この段階では、図 4 に示す署名領域 2 3 4 を含まない。

【 0 1 8 6 】

署名生成部 2 1 4 は、次に、読み出した私有鍵 2 4 1 を用いて、読み出した制御プログラムにデジタル署名 S i g n を施して、署名データ 2 3 4 a を生成する。

【 0 1 8 7 】

署名データ 2 3 4 a = S i g n (私有鍵 2 4 1 、制御プログラム)

次に、署名生成部 2 1 4 は、生成した署名データ 2 3 4 a を制御プログラムに付加し、署名データが付加された制御プログラム 2 3 1 を、プログラム格納部 2 0 7 に記憶されている制御プログラムに上書きする。

【 0 1 8 8 】

また、付随データ生成部 2 0 8 から署名データの生成の指示を受け取ると、署名生成部 2 1 4 は、さらに、付随データ生成部 2 0 8 から変数 K (2 5 4) を受け取る。次に、署名生成部 2 1 4 は、鍵格納部 2 0 4 から確認サーバ装置 2 0 0 に割り当てられた私有鍵 2 4 1 を読み出す。次に、署名生成部 2 1 4 は、私有鍵 2 4 1 を用いて、変数 K (2 5 4) に対してデジタル署名 S i g n を施して、署名データ 2 5 5 を生成する。

【 0 1 8 9 】

署名データ 2 5 5 = S i g n (私有鍵 2 4 1 、変数 K (2 5 4))

次に、署名生成部 2 1 4 は、署名データ 2 5 5 を付随データ生成部 2 0 8 に対して出力する。

【 0 1 9 0 】

(1 0) 信頼性評価部 2 1 0

信頼性評価部 2 1 0 は、固有識別子取得部 2 1 6 から、取得した固有識別子 Y 又はメッセージ「固有識別子無し」を受け取る。また、信頼性評価部 2 1 0 は、付随データ生成部 2 0 8 から乱数 R を受け取る。また、信頼性評価部 2 1 0 は、付随データ生成部 2 0 8 から、制御プログラムに対する付随データ 2 5 1 の上書きが完了したことを示す完了通知を受け取る。

【 0 1 9 1 】

完了通知を受け取り、固有識別子 Y を受け取ると、信頼性評価部 2 1 0 は、プログラム格納部 2 0 7 から、付随データが上書きされた制御プログラム 3 3 1 を読み出す。次に、読み出した制御プログラム 3 3 1 のうち、実行部領域 3 3 2 、第 1 データ領域 3 3 3 、署名領域 3 3 4 及び第 2 データ領域 3 3 5 に含まれる命令及びデータにハッシュ演算 H a s h を施して、ハッシュ値 H を算出する。

【0192】

ハッシュ値 $H = \text{Hash}$ (制御プログラム 331 のうち、実行部領域 332、第 1 データ領域 333、署名領域 334 及び第 2 データ領域 335 に含まれる命令及びデータ)

ここで、第 3 データ領域 336 をハッシュ演算 Hash の対象から除外しているのは、第 3 データ領域 336 は、制御プログラム 331 の実行状態により変化するデータを含んでいるからである。

【0193】

また、ハッシュ演算 Hash は、一例として、 $\text{SHA}-1$ (Secure Hash Algorithm 1) である。また、ハッシュ演算 Hash は、 $\text{SHA}-2$ (Secure Hash Algorithm 2)、 $\text{SHA}-256$ (Secure Hash Algorithm 256-bit) 等であるとしてもよい。

10

【0194】

なお、ここで用いられるハッシュ演算 Hash と、固有識別子取得処理部 902 において用いられるハッシュ演算 Hash とは、同一の演算でなければならない。

【0195】

次に、信頼性評価部 210 は、固有識別子 Y 、ハッシュ値 H 及び乱数 R を用いて、評価値 S を算出する。

【0196】

評価値 $S = \text{固有識別子 } Y \text{ XOR Oneway (ハッシュ値 } H \text{、乱数 } R)$

ここで、一方向性演算 $\text{Oneway} (A, B)$ は、データ A とデータ B に対して、一方向性演算を施して得られた値を示す。例えば、一方向性演算 $\text{Oneway} (A, B)$ は、データ B を鍵として用いて、データ A に鍵付きハッシュ演算を施して得られたハッシュ値である。また、一方向性演算 $\text{Oneway} (A, B)$ は、データ A とデータ B をこの順序で結合して結合体を得、得られた結合体に対して、ハッシュ演算を施して得られたハッシュ値であるとしてもよい。また、一方向性演算 $\text{Oneway} (A, B)$ は、データ B を鍵として用いて、秘密鍵暗号方式としての AES による暗号化アルゴリズムを施して、暗号文を生成し、生成した暗号文にハッシュ演算 $\text{SHA}-1$ を施して得られたハッシュ値であるとしてもよい。

20

【0197】

なお、ここで用いられる一方向性演算 Oneway と、固有識別子取得処理部 902 において用いられる一方向性演算 Oneway とは、同一の演算でなければならない。

30

【0198】

また、信頼性評価部 210 は、端末装置 300 から、ネットワーク 20 及び通信部 202 を介して、評価値 S' を受信する。

【0199】

次に、信頼性評価部 210 は、算出された評価値 S と受信された評価値 S' とが一致するか否かを判断する。評価値 S と評価値 S' とが一致する場合、機器に対する遠隔操作及び関連操作が許可される。評価値 S と評価値 S' とが一致しない場合、機器に対する遠隔操作及び関連操作が禁止される。

【0200】

評価値 S と評価値 S' とが一致しない場合、信頼性評価部 210 は、機器に対する遠隔操作及び関連操作が禁止される旨を示すメッセージを生成する。次に、生成したメッセージを、通信部 202 及びネットワーク 20 を介して、端末装置 300 に対して送信する。

40

【0201】

評価値 S と評価値 S' とが一致する場合、機器制御部 213 に対して、機器に対する遠隔操作及び関連操作を許可する許可情報を出力する。この場合に限り、機器の遠隔処理及び関連操作が行われる。評価値 S と評価値 S' とが一致しない場合、機器制御部 213 に対して、機器に対する遠隔操作及び関連操作を禁止する禁止情報を出力する。この場合に、機器の遠隔処理及び関連操作は、行われない。

【0202】

固有識別子 Y を受け取っていない場合、信頼性評価部 210 は、ハッシュ値 H の算出、

50

評価値 S の算出及び評価値 S と評価値 S ' の比較を行わない。

【0203】

(11) 機器情報管理部 217

機器情報管理部 217 は、端末装置 300 から、ネットワーク 20 及び通信部 202 を介して、制御ルールの変更操作を受信する。次に、機器情報管理部 217 は、受信した変更操作を用いて、機器情報格納部 212 に保持されている制御ルール管理テーブル 281 を変更する。

【0204】

(12) 機器制御部 213

機器制御部 213 は、端末装置 300 から、ネットワーク 20 及び通信部 202 を介して、操作指示を受信する。操作指示には、機器 500 に関する情報の取得の要求、機器 500 の遠隔操作に関連する指示、機器制御ルールの修正の指示及びその他の指示が含まれる。

10

【0205】

機器制御部 213 は、受信した操作指示が、機器 500 に関する情報の取得の要求、機器 500 の遠隔操作に関連する指示、機器制御ルールの修正の指示及びその他の指示のいずれであるかを判断する。

【0206】

操作指示が、機器 500 に関する情報の取得の要求である場合、機器制御部 213 は、機器 500 に関する情報の取得の処理を行う。操作指示が、機器 500 の遠隔操作に関連する指示である場合、機器制御部 213 は、機器 500 の遠隔操作に関連する処理を行う。操作指示が、機器制御ルールの修正の指示である場合、機器制御部 213 は、機器制御ルールの修正の処理を行う。操作指示が、その他の指示である場合、機器制御部 213 は、その他の処理を行う。

20

【0207】

(機器 500 に関する情報の取得)

機器制御部 213 は、端末装置 300 から受け取った機器 500 に関する情報の取得の要求から、機器情報を抽出する。次に、抽出した機器情報に対応する条件を、条件テーブル 271 から読み出す。

【0208】

次に、機器制御部 213 は、確認サーバ装置 200 の現在の状態が、条件テーブル 271 から読み出された条件を満たすか否かを判断する。

30

【0209】

ここで、確認サーバ装置 200 の現在の状態とは、具体的には、端末装置 300 の利用者によるログイン状態にあるか否か、及び、端末装置 300 に装着されたメモリカード 400 から固有識別子を取得しているか否かである。

【0210】

例えば、確認サーバ装置 200 が利用者によるログイン状態になく、固有識別子を取得していない場合、読み出した条件が「ログイン不要、固有識別子要」又は「ログイン要、固有識別子要」であれば、確認サーバ装置 200 の現在の状態は、読み出した条件を満たしていない。

40

【0211】

また、例えば、確認サーバ装置 200 が利用者によるログイン状態にあり、固有識別子を取得していない場合、読み出した条件が「ログイン要、固有識別子要」であれば、確認サーバ装置 200 の現在の状態は、読み出した条件を満たしていない。読み出した条件が「ログイン要、固有識別子不要」であれば、確認サーバ装置 200 の現在の状態は、読み出した条件を満たしている。

【0212】

また、例えば、確認サーバ装置 200 が利用者によるログイン状態にあり、固有識別子を取得している場合、読み出した条件が「ログイン不要、固有識別子要」又は「ログイン

50

要、固有識別子要」であれば、確認サーバ装置 200 の現在の状態は、読み出した条件を満たしている。

【0213】

確認サーバ装置 200 の現在の状態が、読み出した条件を満たしていない場合、機器制御部 213 は、機器状態情報の取得ができない旨を示すメッセージを生成する。次に、生成したメッセージを、通信部 202 及びネットワーク 20 を介して、端末装置 300 に対して送信する。

【0214】

確認サーバ装置 200 の現在の状態が、読み出した条件を満たしている場合、機器制御部 213 は、機器状態情報の取得の要求を、通信部 202 及びネットワーク 20 を介して、機器 500 に対して出力する。

10

【0215】

確認サーバ装置 200 の機器制御部 213 は、機器 500 から、ネットワーク 20 及び通信部 202 を介して、機器状態情報を受信する。次に、受信した機器状態情報を含むメッセージを生成する。次に、機器制御部 213 は、生成したメッセージを、通信部 202 及びネットワーク 20 を介して、端末装置 300 に対して送信する。

【0216】

(機器 500 に対する遠隔操作に関連する処理)

機器制御部 213 は、制御ルール管理テーブル 281 に含まれている全ての制御ルール情報について、次の手順 (a) ~ (d) を繰り返す。

20

【0217】

(a) 機器制御部 213 は、制御ルール管理テーブル 281 から一つの制御ルール情報を読み出す。

【0218】

(b) 次に、機器制御部 213 は、確認サーバ装置 200 の現在の状態が、読み出した制御ルール情報に含まれる条件を満たすか否かを判断する。

【0219】

ここで、上記の機器 500 に関する情報の取得の説明において述べたように、確認サーバ装置 200 の現在の状態とは、具体的には、端末装置 300 の利用者によるログイン状態にあるか否か、及び、端末装置 300 に装着されたメモリカード 400 から固有識別子を取得しているか否かである。

30

【0220】

また、判断方法についても、上述した通りである。

【0221】

例えば、確認サーバ装置 200 が利用者によるログイン状態になく、固有識別子を取得していない場合、読み出した条件が「ログイン不要、固有識別子要」又は「ログイン要、固有識別子要」であれば、確認サーバ装置 200 の現在の状態は、読み出した条件を満たしていない。

【0222】

また、例えば、確認サーバ装置 200 が利用者によるログイン状態にあり、固有識別子を取得している場合、読み出した条件が「ログイン要、固有識別子要」であれば、確認サーバ装置 200 の現在の状態は、読み出した条件を満たしている。

40

【0223】

(c) 確認サーバ装置 200 の現在の状態が、読み出した条件を満たしていない場合、機器制御部 213 は、読み出した制御ルール情報から、操作内容を抽出する。次に、抽出した操作内容の取得ができない旨を示すメッセージを生成する。次に、生成したメッセージを、通信部 202 及びネットワーク 20 を介して、端末装置 300 に対して送信する。

【0224】

(d) 確認サーバ装置 200 の現在の状態が、読み出した条件を満たしている場合、機器制御部 213 は、読み出した制御ルール情報から、操作内容及び項目を抽出する。次に

50

、抽出した操作内容及び項目を含む示すメッセージを生成する。次に、生成したメッセージを、通信部 202 及びネットワーク 20 を介して、機器 500 に対して出力する。

【0225】

機器制御部 213 は、端末装置 300 から受信した操作指示を、通信部 202、ネットワーク 20 を介して、機器 500 に対して送信する。

【0226】

(機器制御ルールの修正処理)

機器制御部 213 は、端末装置 300 の利用者により、ログインが正常にされているか否かを判断する。また、機器制御部 213 は、固有識別子が取得されているか否かを判断する。

10

【0227】

ログインが正常にされていない場合、機器制御部 213 は、ログインが正常にされていないことを示すメッセージを生成する。次に、生成したメッセージを、通信部 202 及びネットワーク 20 を介して、端末装置 300 に対して送信する。

【0228】

固有識別子が取得されていない場合、機器制御部 213 は、固有識別子が取得されていないことを示すメッセージを生成する。次に、生成したメッセージを、通信部 202 及びネットワーク 20 を介して、端末装置 300 に対して送信する。

【0229】

ログインが正常にされ、固有識別子が取得されている場合、機器制御部 213 は、機器情報格納部 212 から、制御ルール管理テーブル 281 を読み出す。次に、読み出した制御ルール管理テーブル 281 を、通信部 202、ネットワーク 20 を介して、端末装置 300 に対して送信する。

20

【0230】

2.4 端末装置 300

端末装置 300 は、図 9 に示すように、制御部 301、通信部 302、相互認証部 303、鍵格納部 304、プログラム格納部 305、プログラム実行部 306、付随データ格納部 307、入出力部 308、表示部 309、入力部 310 及び検証部 311 から構成されている。

【0231】

30

端末装置 300 は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクデバイス、ディスプレイデバイス、入力デバイスなどから構成されるコンピュータシステムである。前記 RAM 又は前記ハードディスクデバイスには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、端末装置 300 は、その機能を達成する。

【0232】

(1) 鍵格納部 304、プログラム格納部 305 及び付随データ格納部 307

(鍵格納部 304)

鍵格納部 304 は、一例として、ハードディスクデバイスから構成されている。鍵格納部 304 は、一例として、確認サーバ装置 200 の公開鍵を記憶している。また、予め、システム鍵 K_{sc} を記憶している。

40

【0233】

(プログラム格納部 305)

プログラム格納部 305 は、一例として、ハードディスクデバイスから構成されている。プログラム格納部 305 は、配信サーバ装置 100 から送信された制御プログラム 231 及び当該端末装置 300 にインストールされた制御プログラム 331 を記憶するための領域を備えている。

【0234】

制御プログラム 231 は、図 4 に示すデータ構造を有している。また、制御プログラム 331 は、図 10 に示すデータ構造を有している。

50

【0235】

(付随データ格納部307)

付随データ格納部307は、一例として、ハードディスクデバイスから構成されている。付随データ格納部307は、図5に示す付随データ251及び乱数Rを記憶するための領域を備えている。

【0236】

(2) 通信部302

通信部302は、ネットワーク20を介して、配信サーバ装置100及び確認サーバ装置200との間で、情報の送受信を行う。

【0237】

通信部302は、具体的には、制御部301の制御により、制御プログラムの要求、機器操作のための接続要求、ログイン要否、操作指示及び評価値S'を、ネットワーク20を介して、配信サーバ装置100に対して送信する

また、通信部302は、制御部301の制御により、利用者識別子及びパスワードを、安全な手段により、ネットワーク20を介して、配信サーバ装置100に対して送信する。

【0238】

また、通信部302は、確認サーバ装置200から、ネットワーク20を介して、様々なメッセージを受信する。次に、受信したメッセージを表示部309に対して出力する。

【0239】

また、通信部302は、配信サーバ装置100から、安全な手段により、ネットワーク20を介して、制御プログラム、付随データ及び乱数Rを受信する。次に、通信部302は、受信した制御プログラムをプログラム格納部305に書き込む。また、通信部302は、受信した付随データ及び乱数Rを付随データ格納部307に書き込む。

【0240】

また、通信部302は、確認サーバ装置200から、ネットワーク20を介して、情報を受信し、受信した情報を入出力部308を介して、メモ리카ード400に対して出力する。また、通信部302は、メモ리카ード400から、入出力部308を介して、情報を受信し、受信した情報をネットワーク20を介して、確認サーバ装置200に対して送信する。

【0241】

(3) 相互認証部303

相互認証部303は、確認サーバ装置200の相互認証部203と、同様の構成を有している。

【0242】

制御プログラムの取得指示を受け付けた場合に、相互認証部303は、配信サーバ装置100の相互認証部103との間で、相互認証及び鍵共有を行う。

【0243】

また、機器操作のための接続要求を送信する場合に、相互認証部303は、確認サーバ装置200の相互認証部203との間で、相互認証及び鍵共有を行う。

【0244】

さらに、固有識別子を取得する場合に、相互認証部303は、メモ리카ード400の相互認証部403との間で、相互認証及び鍵共有を行う。

【0245】

(4) 検証部311

検証部311は、制御プログラム331の起動を受け付けた場合に、鍵格納部304から、確認サーバ装置200に割り当てられた公開鍵を読み出す。次に、検証部311は、読み出した公開鍵を用いて、プログラム格納部305にインストールされた制御プログラム331の署名領域334に記憶されている署名データ334a、実行部領域332及び第1データ領域333に対して、デジタル署名検証Verifyを施す。

【0246】

デジタル署名検証 V r f y による検証結果が失敗である場合、検証部 3 1 1 は、検証に失敗した旨を示すメッセージを生成し、生成したメッセージを表示部 3 0 9 に対して出力する。これにより、端末装置 3 0 0 は、処理を終了する。

【0247】

デジタル署名検証 V r f y による検証結果が成功である場合、端末装置 3 0 0 の処理は、継続される。

【0248】

検証部 3 1 1 は、検証の成功又は失敗を示す検証結果をプログラム実行部 3 0 6 に対して出力する。

10

【0249】

(5) プログラム実行部 3 0 6

プログラム実行部 3 0 6 は、制御プログラム 2 3 1 をプログラム格納部 3 0 5 にインストールする。これにより、プログラム格納部 3 0 5 に、図 1 0 に示すように、制御プログラム 3 3 1 が格納される。なお、この時点において、第 2 データ領域 3 3 5 及び第 3 データ領域 3 3 6 には、それぞれ付随データ及びデータは、格納されていない。

【0250】

プログラム実行部 3 0 6 は、検証部 3 1 1 から、検証の成功又は失敗を示す検証結果を受け取る。受け取った検証結果が検証の失敗を示す場合には、以降の端末装置 3 0 0 の処理を中止する。

20

【0251】

受け取った検証結果が検証の成功を示す場合には、プログラム実行部 3 0 6 は、制御プログラム 3 3 1 を実行状態にする。

【0252】

プログラム実行部 3 0 6 が制御プログラム 3 3 1 を実行することにより、図 1 1 に示すように、付随データ処理部 9 0 1、固有識別子取得処理部 9 0 2、アカウント提示部 9 0 5、機器制御ルール提示部 9 0 6、機器操作提示部 9 0 7、アカウント取得部 9 0 8、機器制御ルール取得部 9 0 9 及び操作指示取得部 9 1 0 が実現される。

【0253】

(付随データ処理部 9 0 1)

30

付随データ処理部 9 0 1 は、付随データ格納部 3 0 7 に付随データが格納されているか否かを判断する。付随データ格納部 3 0 7 に付随データが格納されている場合、付随データ処理部 9 0 1 は、付随データ格納部 3 0 7 に格納されている付随データを制御プログラム 3 3 1 の第 2 データ領域 3 3 5 に上書きする。付随データ格納部 3 0 7 に付随データが格納されていない場合、付随データ処理部 9 0 1 は、付随データの上書きを行わない。

【0254】

付随データ処理部 9 0 1 は、確認サーバ装置 2 0 0 から、ネットワーク 2 0 及び通信部 3 0 2 を介して、付随データ及び乱数 R を、安全な手段により、受信する。

【0255】

次に、付随データ処理部 9 0 1 は、付随データ及び乱数 R を受信したか否かを確認する。

40

【0256】

付随データ及び乱数 R を受信した場合、付随データ処理部 9 0 1 は、受信した付随データを、付随データ格納部 3 0 7 に書き込む。次に、付随データ処理部 9 0 1 は、受信した乱数 R を、付随データ格納部 3 0 7 に書き込む。

【0257】

付随データ及び乱数 R を受信しなかった場合、付随データ処理部 9 0 1 は、付随データ及び乱数 R の書き込みを行わない。

【0258】

(固有識別子取得処理部 9 0 2)

50

固有識別子取得処理部 902 は、利用者から操作指示を受け取った場合、固有識別子の要求を、入出力部 308 を介して、メモリカード 400 に対して出力する。固有識別子取得処理部 902 は、固有識別子の要求を出力した直後において、変数としての固有識別子 Y' を仮に「0」に設定する。

【0259】

固有識別子取得処理部 902 は、メモリカード 400 から固有識別子を受け取ったか否かを判断する。ここで、受け取るべき固有識別子を固有識別子 Y' と表現する。固有識別子 Y' を受け取った場合、固有識別子取得処理部 902 は、プログラム格納部 305 に格納されている制御プログラム 331 のうち、実行部領域 332、第 1 データ領域 333、署名領域 334 及び第 2 データ領域 335 に格納されているメモリ及びデータに対して、ハッシュ演算 $Hash$ を施すことにより、ハッシュ値 H' を算出する。

10

【0260】

ハッシュ値 $H' = Hash$ (プログラム格納部 305 に格納されている制御プログラム 331 のうちの実行部領域 332、第 1 データ領域 333、署名領域 334 及び第 2 データ領域 335 に格納されているメモリ及びデータ)

ここで、第 3 データ領域 336 をハッシュ演算 $Hash$ の対象から除外しているのは、第 3 データ領域 336 は、制御プログラム 331 の実行状態により変化するデータを含んでいるからである。

【0261】

ここで、ハッシュ演算 $Hash$ は、一例として、 $SHA-1$ である。また、ハッシュ演算 $Hash$ は、 $SHA-2$ 、 $SHA-256$ 等であるとしてもよい。

20

【0262】

なお、ここで用いられるハッシュ演算 $Hash$ と、信頼性評価部 210 において用いられるハッシュ演算 $Hash$ とは、同一の演算でなければならない。

【0263】

次に、固有識別子取得処理部 902 は、固有識別子 Y' 、ハッシュ値 H' 及び乱数 R を用いて、評価値 S' を算出する。

【0264】

評価値 $S' = \text{固有識別子 } Y' \text{ XOR Oneway (ハッシュ値 } H' \text{、乱数 } R)$

ここで、一方向性演算 $Oneway (A, B)$ は、データ A とデータ B に対して、一方向性演算を施して得られた値を示す。例えば、一方向性演算 $Oneway (A, B)$ は、データ B を鍵として用いて、データ A に鍵付きハッシュ演算を施して得られたハッシュ値である。また、一方向性演算 $Oneway (A, B)$ は、データ A とデータ B をこの順序で結合して結合体を得、得られた結合体に対して、ハッシュ演算を施して得られたハッシュ値であるとしてもよい。また、一方向性演算 $Oneway (A, B)$ は、データ B を鍵として用いて、秘密鍵暗号方式としての AES による暗号化アルゴリズムを施して、暗号文を生成し、生成した暗号文にハッシュ演算 $SHA-1$ を施して得られたハッシュ値であるとしてもよい。

30

【0265】

なお、ここで用いられる一方向性演算 $Oneway$ と、信頼性評価部 210 において用いられる一方向性演算 $Oneway$ とは、同一の演算でなければならない。

40

【0266】

次に、固有識別子取得処理部 902 は、評価値 S' を、通信部 302 及びネットワーク 20 を介して、確認サーバ装置 200 に対して送信する。

【0267】

(アカウント提示部 905)

アカウント提示部 905 は、利用者から入力された利用者識別子及びパスワードを表示部 309 に出力して、表示させる。

【0268】

(機器制御ルール提示部 906)

50

＜機器制御ルールの修正＞

機器制御ルール提示部 906 は、確認サーバ装置 200 から、ネットワーク 20 及び通信部 302 を介して、制御ルール管理テーブルを受信する。次に、機器制御ルール提示部 906 は、受信した制御ルール管理テーブルを用いて、制御ルール変更画面 361 を生成する。

【0269】

制御ルール変更画面 361 の一例を図 13 に示す。制御ルール変更画面 361 は、この図に示すように、複数のフィールドを含む。各フィールドは、制御ルール管理テーブルの制御ルール情報に対応する。各フィールドは、表示フィールドとボタンフィールドとの組を含む。表示フィールドは、操作内容及び条件を表示する。ボタンフィールドは、条件の

10

【0270】

機器制御ルール提示部 906 は、制御ルール管理テーブルの制御ルール情報毎に、制御ルール変更画面 361 のフィールドを生成する。具体的には、機器制御ルール提示部 906 は、制御ルール情報に含まれる操作内容及び条件から表示フィールドを生成する。つまり、操作内容及び条件を、表示フィールドの表示内容とする。また、機器制御ルール提示部 906 は、制御ルール情報に含まれる条件からボタンフィールドを生成する。つまり、制御ルール情報に含まれる条件に含まれていない変更候補の条件を生成し、生成した変更候補の条件を、ボタンフィールドの表示内容とする。

【0271】

制御ルール変更画面 361 は、一例として、フィールド 371 及び 372 を含む。

20

【0272】

フィールド 371 に含まれる表示フィールドは、操作内容 362 「ルール変更」及び条件 363 「固有識別子要」を表示し、フィールド 371 に含まれるボタンフィールドは、条件の変更の内容 364 「固有識別子不要に変更」を表示する。

【0273】

フィールド 372 に含まれる表示フィールドは、操作内容 365 「エアコン電源制御」及び条件 366 「固有識別子要」を表示し、フィールド 372 に含まれるボタンフィールドは、条件の変更の内容 367 「固有識別子不要に変更」を表示する。

【0274】

このように、各フィールドは、項目ごとに制限を表示している。制限とは、ログインが必要であるか否か、及び、固有識別子が必要であるか否かである。ボタンフィールドには、現在の制限を変更できる候補を表示している。利用者がボタンフィールドを押すことにより、現在の制限を変更することができる。

30

【0275】

（機器操作提示部 907）

＜機器情報取得の処理＞

機器操作提示部 907 は、確認サーバ装置 200 から、ネットワーク 20 及び通信部 302 を介して、機器の状態を示す機器状態情報の取得ができない旨を示すメッセージを受信する。次に、機器操作提示部 907 は、受信したメッセージを表示部 309 に対して出力する。

40

【0276】

機器操作提示部 907 は、確認サーバ装置 200 から、ネットワーク 20 及び通信部 302 を介して、機器状態情報を含むメッセージを受信する。次に、機器操作提示部 907 は、受信したメッセージを表示部 309 に対して出力する。

【0277】

＜機器 500 に対する遠隔操作に関連する処理＞

機器操作提示部 907 は、確認サーバ装置 200 から、ネットワーク 20 及び通信部 302 を介して、操作内容の取得ができない旨を示すメッセージ及び取得した操作内容及び項目を含むメッセージを受信する。次に、機器操作提示部 907 は、受信したメッセージ

50

のうち、操作内容及び項目を含むメッセージを用いて、機器操作メニューを生成する。

【0278】

生成した機器操作メニューの一例として、図12に機器操作画面351を示す。

【0279】

機器操作画面351は、複数のフィールドを含む。各フィールドは、各機器に対する操作に対応し、また一つのメッセージに対応している。各フィールドは、操作内容及び操作ボタンを含む。

【0280】

機器操作提示部907は、受信した一つのメッセージに対応して、一つのフィールドを生成する。メッセージに含まれる操作内容を、フィールドの操作内容とし、メッセージに含まれる項目を操作ボタンとする。

10

【0281】

図12に示す機器操作画面351では、各機器に対応する操作に応じて、操作内容及び操作ボタンを表示している。また、各操作ボタンは、現在の制限を変更できる候補を表示している。操作ボタンを押すことにより、現在の制限を変更できる。

【0282】

機器操作画面351は、一例として、フィールド358及び359を含む。フィールド358は、操作内容352「ドア開閉」と、これに対応して、操作ボタン353「開錠」及び操作ボタン354「施錠」を含む。操作ボタン353の色をグレー（中間階調）にして表示することにより、操作ボタン353が不活性化されている状態を示している。操作ボタン353に対しては、利用者は、操作ができない。操作ボタン354「施錠」については、現在操作できる操作ボタンであることを表現するため、操作ボタンの表示のコントラストを上げて、活性化されている状態を示している。利用者は、操作ボタン354に対する操作が可能である。なお、操作ボタンの色だけでなく、サイズや形などのデザインにより、活性化又は不活性化されていることを表現してもよい。

20

【0283】

フィールド359は、操作内容355「リビングライト操作」と、これに対応して、操作ボタン356「ON」及び操作ボタン357「OFF」を含む。ここで、操作ボタン356及び操作ボタン357に対して、利用者は、操作が可能である。

【0284】

30

図12に示す機器操作画面351では、各機器に対応する操作に応じて、操作内容及び操作ボタンを表示しているが、各機器の機能毎の操作に応じて、操作内容及び操作ボタンを表示してもよい。例えば、テレビ受像機である機器について、チャンネルの切替え、番組の予約などの機能毎に、操作内容及び操作ボタンを表示してもよい。

【0285】

ここでは、端末装置300において、機器操作画面351を生成している。しかし、これには、限定されない。確認サーバ装置200が機器操作画面351を生成し、生成した機器操作画面351を端末装置300に対して送信してもよい。端末装置300は、機器操作画面351を受信し、受信した機器操作画面351を表示する。

【0286】

40

（アカウント取得部908）

アカウント取得部908は、配信サーバ装置100から、ネットワーク20及び通信部302を介して、利用者識別子及びパスワードの要求を受信する。利用者識別子及びパスワードの要求を受信すると、アカウント取得部908は、入力部310に対して、利用者識別子及びパスワードの入力を受け付けるように制御する。

【0287】

制御プログラムの起動が受け付けられ、確認サーバ装置200に対する接続要求が送信される場合に、アカウント取得部908は、入力部310に対して、ログインの要否の入力を受け付けるように制御する。次に、アカウント取得部908は、入力部310からログインの要否を受け取る。次に、アカウント取得部908は、通信部302及びネットワ

50

ーク 20 を介して、ログインの要否を確認サーバ装置 200 に対して送信する。

【0288】

また、アカウント取得部 908 は、受け取ったログインの要否が、ログインを要求することを示すか要求しないことを示すかを判断する。受け取ったログインの要否が、ログインを要求することを示す場合、アカウント取得部 908 は、入力部 310 に対して、利用者識別子及びパスワードの入力を受け付けるように制御する。受け取ったログインの要否が、ログインを要求しないことを示す場合、アカウント取得部 908 は、入力部 310 に対して、利用者識別子及びパスワードの入力を受け付けるように要求しない。

【0289】

アカウント取得部 908 は、入力部 310 から、利用者識別子及びパスワードを受け取る。次に、アカウント取得部 908 は、入力を受け付けた利用者識別子及びパスワードを、安全な手段により、通信部 302 及びネットワーク 20 を介して、配信サーバ装置 100 に対して送信する。

【0290】

(機器制御ルール取得部 909)

機器制御ルール取得部 909 は、入力部 310 から、制御ルールの変更操作を受け取る。次に、機器制御ルール取得部 909 は、制御ルールの変更操作を、通信部 302 及びネットワーク 20 を介して、確認サーバ装置 200 に対して送信する。

【0291】

(操作指示取得部 910)

受け付けた操作指示が処理の終了ではない場合、操作指示取得部 910 は、受け取った操作指示を、通信部 302 及びネットワーク 20 を介して、確認サーバ装置 200 に対して送信する。

【0292】

入力部 310 から操作の終了を示す操作指示を受け取った場合、操作指示取得部 910 は、端末装置 300 の処理を終了するように制御する。

【0293】

(6) 制御部 301

制御部 301 は、通信部 302、相互認証部 303、鍵格納部 304、プログラム格納部 305、プログラム実行部 306、付随データ格納部 307、入出力部 308、表示部 309、入力部 310 及び検証部 311 を制御する。

【0294】

制御部 301 は、配信サーバ装置 100 から、ネットワーク 20 及び通信部 302 を介して、様々なメッセージを受信する。次に、受信したメッセージを表示部 309 に対して出力する。

【0295】

制御部 301 は、ログインが正常にされていないことを示すメッセージを表示部 309 に対して出力する。また、制御部 301 は、固有識別子が取得されていないことを示すメッセージを表示部 309 に対して出力する。

【0296】

(7) 入力部 310、表示部 309 及び入出力部 308

入力部 310 は、端末装置 300 の利用者から、操作指示及びデータを受け付ける。

【0297】

具体的には、入力部 310 は、制御プログラムを取得する指示、利用者識別子及びパスワード、ログインの要否、制御プログラムの起動の操作、機器情報の取得の要求、機器に対する遠隔操作に関連する指示、制御ルールの変更操作を受け付ける。次に、入力部 310 は、受け付けた操作指示及びデータを制御部 301 に対して、出力する。機器に対する遠隔操作に関連する指示には、機器に対する遠隔操作命令が含まれる。遠隔操作命令は、具体的には、テレビ受像機である機器 500a に対する電源 ON の指示、電源 OFF の指示、エアコンである機器 500b に対する電源 ON の指示、電源 OFF の指示、リビング

10

20

30

40

50

ライトである機器 5 0 0 c に対する電源 O N の指示、電源 O F F の指示等を含む。

【0298】

表示部 3 0 9 は、制御部 3 0 1 又は通信部 3 0 2 から様々なメッセージを受け取る。次に、受け取ったメッセージを表示する。前記メッセージには、ログインが正常にされていないことを示すメッセージ、固有識別子が取得されていないことを示すメッセージ等が含まれる。

【0299】

表示部 3 0 9 は、機器操作メニューとして、図 1 2 に示す機器操作画面 3 5 1 を表示する。また、表示部 3 0 9 は、制御ルールの変更にために用いられ、図 1 3 に示す制御ルール変更画面 3 6 1 を表示する。

10

【0300】

入出力部 3 0 8 は、メモ리카ード 4 0 0 とプログラム実行部 3 0 6 との間で、メモ리카ード 4 0 0 と通信部 3 0 2 との間で、又は、メモ리카ード 4 0 0 と制御部 3 0 1 との間で、情報の送受信を中継する。

【0301】

2. 5 メモ리카ード 4 0 0

メモ리카ード 4 0 0 は、図 1 4 に示すように、制御部 4 0 1、相互認証部 4 0 3、鍵格納部 4 0 4、固有識別子格納部 4 0 7 及び入出力部 4 0 8 から構成される。

【0302】

メモ리카ード 4 0 0 は、具体的には、マイクロプロセッサ、ROM、RAM、入出力デバイスなどから構成されるコンピュータシステムである。前記 RAM には、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、メモ리카ード 4 0 0 は、その機能を達成する。

20

【0303】

(1) 固有識別子格納部 4 0 7 及び鍵格納部 4 0 4

固有識別子格納部 4 0 7 は、不揮発性の半導体メモリから構成されている。固有識別子格納部 4 0 7 は、メモ리카ード 4 0 0 に固有の固有識別子を記憶している。固有識別子は、一例として、32ビット長である。

【0304】

鍵格納部 4 0 4 は、予め、システム鍵 K s c を記憶している。

30

【0305】

(2) 制御部 4 0 1

制御部 4 0 1 は、相互認証部 4 0 3、鍵格納部 4 0 4、固有識別子格納部 4 0 7 及び入出力部 4 0 8 を制御する。

【0306】

また、制御部 4 0 1 は、確認サーバ装置 2 0 0 から、ネットワーク 2 0、端末装置 3 0 0 及び入出力部 4 0 8 を介して、固有識別子の要求を受信する。固有識別子の要求を受信すると、制御部 4 0 1 は、固有識別子格納部 4 0 7 から固有識別子の読み出しを試みる。固有識別子の読み出しに成功した場合、制御部 4 0 1 は、読み出した固有識別子を、安全な手段により、入出力部 4 0 8、端末装置 3 0 0 及びネットワーク 2 0 を介して、確認サーバ装置 2 0 0 に対して、送信する。また、固有識別子の読み出しに失敗したときは、制御部 4 0 1 は、固有識別子が無いことを示すメッセージを、安全な手段により、入出力部 4 0 8、端末装置 3 0 0 及びネットワーク 2 0 を介して、確認サーバ装置 2 0 0 に対して送信する。

40

【0307】

また、制御部 4 0 1 は、端末装置 3 0 0 から、入出力部 4 0 8 を介して、固有識別子の要求を受け取る。固有識別子の要求を受け取ると、制御部 4 0 1 は、固有識別子格納部 4 0 7 から固有識別子の読み出しを試みる。固有識別子の読み出しに成功した場合、制御部 4 0 1 は、読み出した固有識別子を、安全な手段により、端末装置 3 0 0 に対して出力する。固有識別子の読み出しに失敗した場合、制御部 4 0 1 は、固有識別子が無いことを示

50

すメッセージを、安全な手段により、端末装置 300 に対して出力する。

【0308】

(3) 相互認証部 403

端末装置 300 から確認サーバ装置 200 に対して、接続要求が送信されたとき、確認サーバ装置 200 からの要求により、相互認証部 403 は、確認サーバ装置 200 の相互認証部 203 との間で、相互認証を行い、確認サーバ装置 200 と共有鍵を共有する。

【0309】

また、端末装置 300 から確認サーバ装置 200 に対して、機器 500 に対する操作指示が送信されたとき、端末装置 300 からの要求により、相互認証部 403 は、端末装置 300 の相互認証部 303 との間で、相互認証を行い、端末装置 300 と共有鍵を共有する。

10

【0310】

相互認証部 403 は、図 15 に示すように、暗号化部 B11、乱数生成部 B12、復号部 B13、乱数比較部 B14、鍵共有部 B15 及び暗復号化部 B16 から構成されている。

【0311】

暗号化部 B11 は、相互認証の相手の装置から乱数 R1 を受け取る。乱数 R1 を受け取ると、システム鍵 Ksc を用いて、暗号化アルゴリズム E3 により、乱数 R1 を暗号化して、暗号化乱数 E3 (Ksc、R1) を生成し、生成した暗号化乱数 E3 (Ksc、R1) を相手の装置へ送信する。

20

【0312】

ここで、暗号化アルゴリズム E3 は、秘密鍵暗号方式による暗号化アルゴリズムである。暗号化アルゴリズム E3 は、一例として、AES によるものである。E3 (K、A) は、鍵 K を用いて、平文 A に対して暗号化アルゴリズム E3 を施して生成した暗号文を示す。

【0313】

乱数生成部 B12 は、乱数 R2 を生成する。次に、生成した乱数 R2 を乱数比較部 B14 に出力する。また、生成した乱数 R2 を相互認証の相手の装置に送信する。

【0314】

復号部 B13 は、相互認証の相手の装置から、暗号化乱数 E4 (Ksc、R2) を受け取る。次に、システム鍵 Ksc を用いて、復号アルゴリズム D4 により、受け取った暗号化乱数 E4 (Ksc、R2) を復号して復号文 R2' = D4 (Ksc、E4 (Ksc、R2)) を生成する。次に、生成した復号文 R2' を乱数比較部 B14 へ出力する。

30

【0315】

ここで、復号アルゴリズム D4 は、秘密鍵暗号方式による暗号化アルゴリズムである。復号アルゴリズム D4 は、一例として、AES によるものである。E4 (K、A) は、鍵 K を用いて、平文 A に対して暗号化アルゴリズム E4 を施して生成した暗号文を示す。また、D4 (K、B) は、鍵 K を用いて、暗号文 B に対して復号アルゴリズム D4 を施して生成した復号文を示す。

【0316】

40

乱数比較部 B14 は、乱数 R2 を受け取り、復号文 R2' を受け取る。次に、乱数 R2 と復号文 R2' とを比較する。乱数 R2 と復号文 R2' とが一致する場合に、相互認証部 403 は、相手の装置が正当であると判断する。乱数 R2 と復号文 R2' とが一致しない場合に、相互認証部 403 は、相手の装置が不正であると判断する。

【0317】

相互の認証に成功すると、鍵共有部 B15 は、鍵共有の処理を実行して、共有鍵 k' を算出する。相互の認証に失敗すると、共有鍵 k' の算出は、行われない。

【0318】

相互の認証に成功すると、暗復号化部 B16 は、算出された共有鍵 k' を用いて、データを暗号化して、暗号化データを生成する。暗号化データは、相手の装置に送信される。

50

また、暗復号化部 B 1 6 は、相手の装置から暗号化データを受信する。次に、算出された共有鍵 k' を用いて、暗号化データを復号して、元のデータを生成する。

【0319】

(4) 入出力部 408

入出力部 408 は、端末装置 300 から情報を受け取り、受け取った情報を制御部 401 又は相互認証部 403 に対して出力する。

【0320】

また、入出力部 408 は、制御部 401 又は相互認証部 403 から情報を受け取り、受け取った情報を端末装置 300 に対して出力する。

【0321】

2. 6 機器 500

ここでは、機器 500 a、500 b、500 c、500 d 及び 500 e を代表して、機器 500 として説明する。

【0322】

機器 500 は、図 16 に示すように、機構制御部 501、通信部 502、命令受信部 506、情報通知部 507 及び機構 508 から構成されている。

【0323】

機構 508 は、機器 500 の機能を達成するための主たる機構である。機器 500 が照明器具である場合、機構 508 は、照明機構である。機器 500 がテレビ受像機である場合、機構 508 は、放送波を受信し、受信した放送波から利用者の所望のチャンネルの番組を抽出し、抽出した番組を再生して表示する。機器 500 が扉である場合、機構 508 は、扉の施錠及び開錠を制御するロック機構である。

【0324】

機構 508 は、機構制御部 501 から、遠隔操作命令を含む操作指示を受け取り、受け取った操作指示に含まれる遠隔操作命令に従って、動作する。

【0325】

通信部 510 は、ネットワーク 20 を介して、確認サーバ装置 200 との間で情報の送受信を行う。

【0326】

情報通知部 507 は、機構制御部 501 から、機器が有する機構 508 の状態を示す機器状態情報を受け取り、受け取った機器状態情報を、通信部 502 及びネットワーク 20 を介して、確認サーバ装置 200 に対して送信する。

【0327】

命令受信部 506 は、確認サーバ装置 200 から、ネットワーク 20 及び通信部 502 を介して、機器 500 の機構 508 を制御する遠隔操作命令を受信し、受信した遠隔操作命令を機構制御部 501 に対して出力する。

【0328】

機構制御部 501 は、命令受信部 506 から、遠隔操作命令を受け取り、受け取った遠隔操作命令により、機構 508 を制御する。また、機構 508 から、機構 508 の状態を示す機器状態情報を取得し、取得した機器状態情報を情報通知部 507 に対して出力する。

【0329】

機構制御部 501 は、確認サーバ装置 200 から、ネットワーク 20、通信部 502 及び命令受信部 506 を介して、機器状態情報の取得の要求を受信する。次に、機構制御部 501 は、機器状態情報の取得の要求から、取得の対象である機器に関する機器情報を抽出し、抽出した機器情報に対応する機器状態情報を機構 508 から取得する。次に、機構制御部 501 は、取得した機器状態情報を、情報通知部 507、通信部 502 及びネットワーク 20 を介して、確認サーバ装置 200 に対して送信する。

【0330】

2. 7 遠隔操作システム 10 における動作

(1) 制御プログラムの制作及び制御プログラムの配信の手順

制御プログラムの制作及び制御プログラムの配信の手順について、図17に示すシーケンス図を用いて説明する。

【0331】

確認サーバ装置200のプログラム制作部206は、確認サーバ装置200の利用者の操作により、制御プログラムを制作する。次に、プログラム制作部206は、制作された制御プログラムをプログラム格納部207に書き込む（ステップS101）。

【0332】

署名生成部214は、鍵格納部204から、確認サーバ装置200に割り当てられた私有鍵を読み出し、プログラム格納部207から制御プログラムを読み出す。次に、読み出した私有鍵を用いて、読み出した制御プログラムにデジタル署名Signを施して、署名データを生成する。次に、署名生成部214は、生成した署名データを制御プログラムに付加し、署名データが付加された制御プログラムを、プログラム格納部207に記憶されている制御プログラムに上書きする（ステップS102）。

【0333】

次に、確認サーバ装置200の相互認証部203と配信サーバ装置100の相互認証部103とは、相互認証及び鍵共有を行う（ステップS103）。なお、相互認証及び鍵共有の詳細手順については、後述する。

【0334】

次に、通信部202は、プログラム格納部207から制御プログラムを読み出す（ステップS104）。

【0335】

次に、確認サーバ装置200の通信部202は、読み出した制御プログラムを、安全な手段により、ネットワーク20を介して、配信サーバ装置100に送信する（ステップS105）。次に、配信サーバ装置100の通信部102は、確認サーバ装置200から、ネットワーク20を介して、安全な手段により、前記制御プログラムを受信する（ステップS105）。

【0336】

ここで、安全な手段による通信は、次の方法により実現される。

【0337】

相互認証部203は、ステップS103に示す相互認証及び鍵共有の手順において、生成された共有鍵を用い、制御プログラムを暗号化して暗号化制御プログラムを生成する。ステップS105において、通信部202は、暗号化制御プログラムを、ネットワーク20を介して、配信サーバ装置100に送信する。次に、通信部102は、確認サーバ装置200から、ネットワーク20を介して、暗号化制御プログラムを受信する。相互認証部103は、ステップS103に示す相互認証及び鍵共有の手順において、生成された共有鍵を用い、暗号化制御プログラムを復号して、制御プログラムを生成する。

【0338】

次に、通信部102は、受信した制御プログラムを記憶部105に書き込む（ステップS106）。

【0339】

以上の手順により、制御プログラムが確認サーバ装置200から配信サーバ装置100に送信される。

【0340】

次に、端末装置300の入力部310は、端末装置300の利用者から、制御プログラムを取得する指示を受け付ける（ステップS111）。

【0341】

次に、配信サーバ装置100の相互認証部103と端末装置300の相互認証部303とは、相互認証及び鍵共有を行う（ステップS112）。

【0342】

次に、通信部 302 は、制御部 301 の制御により、制御プログラムの要求を、ネットワーク 20 を介して、配信サーバ装置 100 に対して送信する（ステップ S113）。配信サーバ装置 100 の制御部 101 は、端末装置 300 から、ネットワーク 20 及び通信部 102 を介して、制御プログラムの要求を受信する（ステップ S113）。

【0343】

次に、制御部 101 は、通信部 102 及びネットワーク 20 を介して、端末装置 300 に対して、利用者識別子及びパスワードの要求を送信する（ステップ S114）。アカウント取得部 908 は、配信サーバ装置 100 から、ネットワーク 20 及び通信部 302 を介して、利用者識別子及びパスワードの要求を受信する（ステップ S114）。

【0344】

次に、入力部 310 は、端末装置 300 の利用者から、利用者識別子及びパスワードの入力を受け付ける（ステップ S115）。アカウント取得部 908 は、入力を受け付けた利用者識別子及びパスワードを、安全な手段により、通信部 302 及びネットワーク 20 を介して、配信サーバ装置 100 に対して送信する（ステップ S116）。アカウント確認部 107 は、端末装置 300 から、ネットワーク 20 及び通信部 102 を介して、安全な手段により、利用者識別子及びパスワードを受信する（ステップ S116）。ここで、安全な手段とは、上述した暗号化及び復号の方法によるものである。

【0345】

次に、アカウント確認部 107 は、受信した利用者識別子及びパスワードが、アカウント格納部 106 に記憶されているか否かを確認する（ステップ S117）。受信した利用者識別子及びパスワードが、アカウント格納部 106 に記憶されていない場合、ログインに失敗した（ログイン異常）とみなす。受信した利用者識別子及びパスワードが、アカウント格納部 106 に記憶されている場合、ログインに成功した（ログイン正常）とみなす。

【0346】

ログイン異常の場合（ステップ S118 で「異常」）、アカウント確認部 107 は、ログイン異常を示すメッセージを生成する（ステップ S119）。次に、当該メッセージを、通信部 102 及びネットワーク 20 を介して、端末装置 300 に対して送信する（ステップ S120）。これにより、配信サーバ装置 100 における処理は、終了する。

【0347】

端末装置 300 の制御部 301 は、配信サーバ装置 100 から、ネットワーク 20 及び通信部 302 を介して、前記メッセージを受信する（ステップ S120）。次に、表示部 309 は、受信した前記メッセージを表示する（ステップ S121）。これにより、端末装置 300 の処理は、終了する。

【0348】

ログイン正常の場合（ステップ S118 で「正常」）、制御部 101 は、記憶部 105 から制御プログラムを読み出す（ステップ S122）。次に、制御部 101 は、読み出した制御プログラムを、安全な手段により、通信部 102 及びネットワーク 20 を介して、端末装置 300 に対して送信する（ステップ S123）。通信部 302 は、配信サーバ装置 100 から、ネットワーク 20 を介して、安全な手段により、制御プログラムを受信する（ステップ S123）。ここで、安全な手段については、上述した通りである。次に、通信部 302 は、受信した制御プログラムをプログラム格納部 305 に書き込む（ステップ S124）。次に、プログラム実行部 306 は、制御プログラムをプログラム格納部 305 にインストールする（ステップ S125）。

【0349】

以上の手順により、制御プログラムが配信サーバ装置 100 から端末装置 300 に送信される。

【0350】

（２）制御プログラムの起動の手順

制御プログラムの起動の手順について、図 18～図 20 に示すシーケンス図を用いて説

10

20

30

40

50

明する。

【0351】

端末装置300の入力部310は、端末装置300の利用者から、制御プログラムの起動の操作を受け付ける（ステップS130）。この時点を実第1時点と呼ぶ。

【0352】

検証部311は、鍵格納部304から、確認サーバ装置200に割り当てられた公開鍵を読み出す。次に、検証部311は、読み出した公開鍵を用いて、プログラム格納部305にインストールされた制御プログラム331の署名領域334に記憶されている署名データ334a、実行部領域332及び第1データ領域333に対して、デジタル署名検証Vrfyを施す（ステップS131）。デジタル署名検証Vrfyによる検証結果が失敗である場合（ステップS132で「失敗」）、検証部311は、デジタル署名検証Vrfyに失敗した旨を示すメッセージを生成し、表示部309は、当該メッセージを表示する（ステップS133）。これにより、端末装置300は、処理を終了する。

10

【0353】

デジタル署名検証Vrfyによる検証結果が成功である場合（ステップS132で「成功」）、プログラム実行部306は、制御プログラムを実行状態にする（ステップS134）。付随データ処理部901は、付随データ格納部307に付随データが格納されているか否かを判断する（ステップS135）。

【0354】

付随データ格納部307に付随データが格納されている場合（ステップS135で「有り」）、検証部311は、鍵格納部304から、確認サーバ装置200に割り当てられた公開鍵を読み出す。次に、検証部311は、読み出した公開鍵を用いて、付随データ格納部307に記録されている付随データの署名領域に記憶されている署名データ、変数領域に記録されている変数Kに対して、デジタル署名検証Vrfyを施す（ステップS136）。デジタル署名検証Vrfyによる検証結果が失敗である場合（ステップS137で「失敗」）、検証部311は、デジタル署名検証Vrfyに失敗した旨を示すメッセージを生成し、表示部309は、当該メッセージを表示する（ステップS138）。これにより、端末装置300は、処理を終了する。

20

【0355】

デジタル署名検証Vrfyによる検証結果が成功である場合（ステップS137で「成功」）、付随データ処理部901は、付随データ格納部307に格納されている付随データを制御プログラム331の第2データ領域335に上書きする（ステップS139）。

30

【0356】

付随データ格納部307に付随データが格納されていない場合（ステップS135で「無し」）、検証部311による検証及び付随データ処理部901による付随データの上書きを行わない。

【0357】

制御部301は、機器500に対する遠隔操作のための接続要求を、通信部302及びネットワーク20を介して、確認サーバ装置200に対して送信する（ステップS140）。制御部201は、端末装置300から、ネットワーク20及び通信部202を介して、接続要求を受信する（ステップS140）。

40

【0358】

次に、確認サーバ装置200の相互認証部203と端末装置300の相互認証部303とは、相互認証及び鍵共有を行う（ステップS141）。

【0359】

次に、確認サーバ装置200の相互認証部203とメモ리카ード400の相互認証部403とは、相互認証及び鍵共有を行う（ステップS142）。

【0360】

確認サーバ装置200の制御部201は、通信部202、ネットワーク20及び端末装置300を介して、メモ리카ード400に対して、固有識別子の要求を送信する（ステッ

50

プS143)。メモリカード400の制御部401は、確認サーバ装置200から、ネットワーク20、端末装置300及び入出力部408を介して、固有識別子の要求を受信する(ステップS143)。次に、制御部401は、固有識別子格納部407から固有識別子Yの読み出しを試みる(ステップS144)。制御部401は、読み出した固有識別子Yを、安全な手段により、入出力部408、端末装置300及びネットワーク20を介して、確認サーバ装置200に対して、送信する(ステップS145)。また、制御部401は、固有識別子Yの読み出しに失敗したときは、固有識別子が無いことを示すメッセージを、安全な手段により、入出力部408、端末装置300及びネットワーク20を介して、確認サーバ装置200に対して送信する(ステップS145)。

【0361】

10

制御部201は、メモリカード400から、端末装置300、ネットワーク20及び通信部202を介して、安全な手段により、固有識別子Y又は固有識別子が無いことを示すメッセージを受信する。また、制御部201は、メモリカード400に対して、固有識別子の要求を送信した後、所定時間を経過しても、固有識別子Y又は固有識別子が無いことを示すメッセージを受信しないときは、固有識別子が無いことを示すメッセージを生成する(ステップS145)。

【0362】

次に、端末装置300の入力部310は、端末装置300の利用者からログインの可否を受け付ける(ステップS146)。次に、アカウント取得部908は、通信部302及びネットワーク20を介して、ログインの可否を確認サーバ装置200に対して送信する(ステップS147)。

20

【0363】

次に、アカウント取得部908は、受け付けたログインの可否が、ログインを要求することを示すか要求しないことを示すかを判断する(ステップS148)。

【0364】

ログインを要求することを示す場合(ステップS148で「要」)、入力部310は、端末装置300の利用者から、利用者識別子及びパスワードの入力を受け付ける(ステップS149)。次に、アカウント取得部908は、受け付けた利用者識別子及びパスワードを、通信部302及びネットワーク20を介して、確認サーバ装置200に対して、安全な手段により、送信する(ステップS150)。

30

【0365】

アカウント確認部215は、端末装置300から、ネットワーク20及び通信部202を介して、ログインの可否を受け取る(ステップS150)。

【0366】

アカウント確認部215は、受け取ったログインの可否が、ログインを要求することを示すか要求しないことを示すかを判断する(ステップS156)。

【0367】

ログインの可否が、ログインを要求しないことを示す場合(ステップS156で「否」)、制御をステップS162へ移す。

【0368】

40

ログインの可否が、ログインを要求することを示す場合(ステップS156で「要」)、アカウント確認部215は、端末装置300から、ネットワーク20及び通信部202を介して、安全な手段により、利用者識別子及びパスワードを受信する(ステップS150)。次に、アカウント確認部215は、受信した利用者識別子及びパスワードの組が、アカウント管理テーブル261に記憶されているか否かを確認する(ステップS151)。アカウント確認部215は、受信した利用者識別子及びパスワードが、アカウント管理テーブル261に記憶されていない場合、ログインに失敗した(ログイン異常)とみなす。アカウント確認部215は、受信した利用者識別子及びパスワードが、アカウント管理テーブル261に記憶されている場合、ログインに成功した(ログイン正常)とみなす。

【0369】

50

ログイン異常の場合（ステップS152で「異常」）、アカウント確認部215は、ログイン異常を示すメッセージを生成する（ステップS153）。次に、当該メッセージを、通信部202及びネットワーク20を介して、端末装置300に対して送信する（ステップS154）。これにより、確認サーバ装置200における処理は、終了する。

【0370】

端末装置300の通信部302は、確認サーバ装置200から、ネットワーク20を介して、前記メッセージを受信する（ステップS154）。次に、表示部309は、前記メッセージを表示する（ステップS155）。これにより、端末装置300の処理は、終了する。

【0371】

ログイン正常の場合（ステップS152で「正常」）、制御部101は、利用者識別子及びパスワードを記憶する（ステップS161）。

【0372】

次に、付随データ生成部208は、メモリカード400から固有識別子を受信しているか否かを確認する（ステップS162）。固有識別子を受信している場合（ステップS162で「有り」）、付随データ生成部208は、乱数Rを生成し（ステップS163）、変数 $K = \text{固有識別子} Y \oplus \text{乱数} R$ を算出する（ステップS164）。次に、付随データ生成部208は、算出して得られた変数Kを含む付随データを生成する（ステップS165）。次に、署名生成部214は、付随データに対してデジタル署名Signを施して、署名データを生成し、生成した署名データを付随データに付加する（ステップS166）。次に、付随データ生成部208は、付随データ及び乱数Rを、通信部202及びネットワーク20を介して、端末装置300に対して、安全な手段により、送信する（ステップS167）。

【0373】

固有識別子を受信していない場合（ステップS162で「無し」）、乱数Rの生成、変数Kの算出、付随データの生成、署名データの生成及び付随データ及び乱数Rの送信は、行われない。

【0374】

付随データ処理部901は、確認サーバ装置200から、ネットワーク20及び通信部302を介して、付随データ及び乱数Rを、安全な手段により、受信する場合がある（ステップS167）。

【0375】

次に、付随データ処理部901は、付随データ及び乱数Rを受信したか否かを確認する（ステップS168）。

【0376】

付随データ及び乱数Rを受信した場合（ステップS168で「YES」）、付随データ処理部901は、受信した付随データを、付随データ格納部307に書き込む（ステップS169）。次に、付随データ処理部901は、受信した乱数Rを、付随データ格納部307に書き込む（ステップS170）。

付随データ及び乱数Rを受信しなかった場合（ステップS168で「NO」）、付随データ及び乱数Rの書き込みは、行われない。

【0377】

端末装置300の入力部310は、端末装置300の利用者から、操作指示を受け付ける（ステップS181）。この時点を第2時点と呼ぶ。受け付けた操作指示が処理の終了を示す場合（ステップS182で「YES」）、端末装置300は、処理を終了する。

【0378】

受け付けた操作指示が処理の終了ではない場合（ステップS182で「NO」）、操作指示取得部910は、受け取った操作指示を、通信部302及びネットワーク20を介して、確認サーバ装置200に対して送信する（ステップS183）。

【0379】

10

20

30

40

50

確認サーバ装置 200 の機器制御部 213 は、端末装置 300 から、ネットワーク 20 及び通信部 202 を介して、操作指示を受け取る（ステップ S183）。次に、信頼性評価部 210 は、固有識別子を受け取ったか否かを判断する（ステップ S200）。

【0380】

固有識別子を受け取った場合（ステップ S200 で「有り」）、付随データ生成部 208 は、付随データをプログラム格納部 207 に記憶されている制御プログラムに上書きする（ステップ S201）。次に、信頼性評価部 210 は、制御プログラムにハッシュ演算 Hash を施して、ハッシュ値 H を算出する（ステップ S202）。次に、信頼性評価部 210 は、評価値 $S = \text{固有識別子 } Y \oplus \text{Oneway}$ （ハッシュ値 H、乱数 R）を算出する（ステップ S203）。 10

【0381】

ステップ S183 で操作指示を送信した後、端末装置 300 の相互認証部 303 と、メモリカード 400 の相互認証部 403 とは、相互認証及び鍵共有を行う（ステップ S184）。

【0382】

次に、端末装置 300 の固有識別子取得処理部 902 は、固有識別子の要求を、入出力部 308 を介して、メモリカード 400 に対して出力する（ステップ S185）。次に、メモリカード 400 の制御部 401 は、端末装置 300 から、入出力部 408 を介して、固有識別子の要求を受け取る（ステップ S185）。 20

【0383】

固有識別子取得処理部 902 は、ステップ S185 において、固有識別子の要求を出力した後で、固有識別子 Y' を「0」に設定する（ステップ S186）。 20

【0384】

メモリカード 400 の制御部 401 は、固有識別子格納部 407 から固有識別子の読み出しを試みる。ここでは、固有識別子 Y' が読み出されるとする。読み出した固有識別子 Y' を、安全な手段により、端末装置 300 に対して出力する。固有識別子の読み出しができない場合、制御部 401 は、固有識別子が無いことを示すメッセージを、安全な手段により、端末装置 300 に対して出力する（ステップ S188）。 20

【0385】

次に、固有識別子取得処理部 902 は、メモリカード 400 から固有識別子 Y' を受け取ったか否かを判断する（ステップ S189）。固有識別子 Y' を受け取った場合（ステップ S189 で「有り」）、固有識別子取得処理部 902 は、ハッシュ値 $H' = \text{Hash}$ （プログラム格納部 305 に格納されている制御プログラム）を算出する（ステップ S190）。次に、固有識別子取得処理部 902 は、評価値 $S' = \text{固有識別子 } Y' \oplus \text{Oneway}$ （ハッシュ値 H'、乱数 R）を算出する（ステップ S191）。次に、固有識別子取得処理部 902 は、評価値 S' を、通信部 302 及びネットワーク 20 を介して、確認サーバ装置 200 に対して送信する（ステップ S192）。 30

【0386】

信頼性評価部 210 は、端末装置 300 から、ネットワーク 20 及び通信部 202 を介して、評価値 S' を受信する（ステップ S192）。 40

【0387】

次に、信頼性評価部 210 は、算出された評価値 S と受信された評価値 S' とが一致するか否かを判断する（ステップ S204）。評価値 S と評価値 S' とが一致しない場合（ステップ S204 で「不一致」）、信頼性評価部 210 は、機器制御部 213 に対して、機器に対する操作を禁止する禁止情報を出力し、評価値 S と評価値 S' とが一致しない旨を示すメッセージを生成する（ステップ S205）。次に、生成したメッセージを、通信部 202 及びネットワーク 20 を介して、端末装置 300 に対して送信する（ステップ S206）。 40

【0388】

端末装置 300 の制御部 301 は、確認サーバ装置 200 から、ネットワーク 20 及び 50

通信部 302 を介して、評価値 S と評価値 S' とが一致しない旨を示す前記メッセージを受け取る（ステップ S206）。次に、表示部 309 は、受け取ったメッセージを表示する（ステップ S207）。これにより、端末装置 300 による処理を終了する。

【0389】

評価値 S と評価値 S' とが一致する場合（ステップ S204 で「一致」）、機器制御部 213 に対して、機器に対する操作を許可する許可情報を出力し、機器に対する遠隔処理等が行われる（ステップ S208）。これにより、処理が終了する。

【0390】

固有識別子を受け取っていない場合（ステップ S200 で「無し」）、付随データの上書き、ハッシュ値 H の算出、評価値 S の算出及び評価値 S と評価値 S' の比較は、行われない。

10

【0391】

なお、ステップ S208 において、機器に対する遠隔処理等が終了した後で、利用者は、制御プログラムを終了させるとしてもよい。又は、ステップ S208 において、機器に対する遠隔処理等が終了した後で、ステップ S130 に戻って、処理を繰り返すとしてもよい。

【0392】

また、ステップ S208 において、機器に対する遠隔処理等が終了した後で、ステップ S181 に戻って、処理を繰り返すとしてもよい。

【0393】

20

（３）機器の遠隔処理及び関連する処理の手順

機器の遠隔処理及び関連する処理の手順について、図 21 に示すフローチャートを用いて説明する。なお、ここで説明する機器の遠隔処理及び関連する処理は、図 20 のステップ S208 の詳細である。

【0394】

機器制御部 213 は、端末装置 300 から、ネットワーク 20 及び通信部 202 を介して受信した操作指示が、機器 500 に関する情報の取得の要求、機器 500 の遠隔操作に関連する指示、機器制御ルール of 修正の指示及びその他の指示のいずれであるかを判断する（ステップ S251）。

【0395】

30

操作指示が、機器 500 に関する情報の取得の要求である場合（ステップ S251 で「機器情報取得要求」）、機器制御部 213 は、機器 500 に関する情報の取得の処理を行う（ステップ S252）。

【0396】

操作指示が、機器 500 の遠隔操作に関連する指示である場合（ステップ S251 で「遠隔操作関連指示」）、機器制御部 213 は、機器 500 の遠隔操作に関連する処理を行う（ステップ S253）。

【0397】

操作指示が、機器制御ルールの修正の指示である場合（ステップ S251 で「機器制御ルール修正指示」）、機器制御部 213 は、機器制御ルールの修正の処理を行う（ステップ S254）。

40

【0398】

操作指示が、その他の指示である場合（ステップ S251 で「他の指示」）、機器制御部 213 は、その他の処理を行う（ステップ S255）。

【0399】

これにより、機器の遠隔処理及び関連する処理を終了する。

【0400】

（４）機器 500 に関する情報の取得の手順

機器 500 に関する情報の取得の手順について、図 22 に示すフローチャートを用いて説明する。なお、ここで説明する機器 500 に関する情報の取得の手順は、図 21 のステ

50

ップ S 2 5 2 の詳細である。

【0401】

機器制御部 2 1 3 は、機器 5 0 0 に関する情報の取得の要求から、機器情報を抽出し、抽出した機器情報に対応する条件を、条件テーブル 2 7 1 から読み出す（ステップ S 3 0 1）。

【0402】

次に、確認サーバ装置 2 0 0 の現在の状態が、条件テーブル 2 7 1 から読み出された条件を満たすか否かを判断する（ステップ S 3 0 2）。

【0403】

確認サーバ装置 2 0 0 の現在の状態が、読み出した条件を満たしていない場合（ステップ S 3 0 2 で「満たさない」）、機器制御部 2 1 3 は、機器の状態を示す機器状態情報の取得ができない旨を示すメッセージを生成する（ステップ S 3 0 3）。次に、生成したメッセージを、通信部 2 0 2 及びネットワーク 2 0 を介して、端末装置 3 0 0 に対して送信する（ステップ S 3 0 4）。

10

【0404】

端末装置 3 0 0 の機器操作提示部 9 0 7 は、確認サーバ装置 2 0 0 から、ネットワーク 2 0 及び通信部 3 0 2 を介して、機器状態情報の取得ができない旨を示すメッセージを受信する（ステップ S 3 0 4）。次に、機器操作提示部 9 0 7 は、受信したメッセージを表示部 3 0 9 に対して出力する。表示部 3 0 9 は、メッセージを受け取り、受け取ったメッセージを表示する（ステップ S 3 1 0）。これにより、機器状態情報の取得の処理を終了する。

20

【0405】

確認サーバ装置 2 0 0 の現在の状態が、読み出した条件を満たしている場合（ステップ S 3 0 2 で「満たす」）、機器制御部 2 1 3 は、機器状態情報の取得の要求を、通信部 2 0 2 及びネットワーク 2 0 を介して、機器 5 0 0 に対して出力する（ステップ S 3 0 5）。

【0406】

機器 5 0 0 の機構制御部 5 0 1 は、確認サーバ装置 2 0 0 から、ネットワーク 2 0、通信部 5 0 2 及び命令受信部 5 0 6 を介して、機器状態情報の取得の要求を受信する（ステップ S 3 0 5）。次に、機構制御部 5 0 1 は、機器状態情報の取得の要求から、取得の対象である機器に関する機器情報を抽出し、抽出した機器情報に対応する機器状態情報を機構 5 0 8 から取得する（ステップ S 3 0 6）。次に、機構制御部 5 0 1 は、取得した機器状態情報を、情報通知部 5 0 7、通信部 5 0 2 及びネットワーク 2 0 を介して、確認サーバ装置 2 0 0 に対して送信する（ステップ S 3 0 7）。

30

【0407】

確認サーバ装置 2 0 0 の機器制御部 2 1 3 は、機器 5 0 0 から、ネットワーク 2 0 及び通信部 2 0 2 を介して、機器状態情報を受信する（ステップ S 3 0 7）。次に、受信した機器状態情報を含むメッセージを生成する（ステップ S 3 0 8）。次に、機器制御部 2 1 3 は、生成したメッセージを、通信部 2 0 2 及びネットワーク 2 0 を介して、端末装置 3 0 0 に対して送信する（ステップ S 3 0 9）。

40

【0408】

端末装置 3 0 0 の機器操作提示部 9 0 7 は、確認サーバ装置 2 0 0 から、ネットワーク 2 0 及び通信部 3 0 2 を介して、機器状態情報を含むメッセージを受信する（ステップ S 3 0 9）。次に、機器操作提示部 9 0 7 は、受信したメッセージを表示部 3 0 9 に対して出力する。表示部 3 0 9 は、メッセージを受け取り、受け取ったメッセージを表示する（ステップ S 3 1 0）。これにより、機器状態情報の取得の処理を終了する。

【0409】

（５）機器 5 0 0 に対する遠隔操作に関連する処理の手順

機器 5 0 0 に対する遠隔操作に関連する処理の手順について、図 2 3 に示すフローチャートを用いて説明する。なお、ここで説明する機器 5 0 0 に対する遠隔操作に関連する処

50

理の手順は、図 2 1 のステップ S 2 5 3 の詳細である。

【0 4 1 0】

機器制御部 2 1 3 は、制御ルール管理テーブル 2 8 1 に含まれている全ての制御ルール情報について、ステップ S 3 3 2 ～ S 3 3 8 を繰り返す（ステップ S 3 3 1 ～ S 3 3 9）。

【0 4 1 1】

機器制御部 2 1 3 は、制御ルール管理テーブル 2 8 1 から一つの制御ルール情報を読み出す（ステップ S 3 3 2）。

【0 4 1 2】

次に、機器制御部 2 1 3 は、確認サーバ装置 2 0 0 の現在の状態が、読み出した制御ルール情報に含まれる条件を満たすか否かを判断する（ステップ S 3 3 3）。 10

【0 4 1 3】

確認サーバ装置 2 0 0 の現在の状態が、読み出した条件を満たしていない場合（ステップ S 3 3 3 で「満たさない」）、機器制御部 2 1 3 は、読み出した制御ルール情報から、操作内容を抽出し、抽出した操作内容の取得ができない旨を示すメッセージを生成する（ステップ S 3 3 4）。次に、生成したメッセージを、通信部 2 0 2 及びネットワーク 2 0 を介して、端末装置 3 0 0 に対して送信する（ステップ S 3 3 5）。

【0 4 1 4】

確認サーバ装置 2 0 0 の現在の状態が、読み出した条件を満たしている場合（ステップ S 3 3 3 で「満たす」）、機器制御部 2 1 3 は、読み出した制御ルール情報から、操作内容及び項目を抽出し（ステップ S 3 3 6）、抽出した操作内容及び項目を含むメッセージを生成する（ステップ S 3 3 7）。次に、生成したメッセージを、通信部 2 0 2 及びネットワーク 2 0 を介して、機器 5 0 0 に対して出力する（ステップ S 3 3 8）。 20

【0 4 1 5】

端末装置 3 0 0 の機器操作提示部 9 0 7 は、確認サーバ装置 2 0 0 から、ネットワーク 2 0 及び通信部 3 0 2 を介して、前記メッセージを受信する（ステップ S 3 3 5、S 3 3 8）。

【0 4 1 6】

次に、機器操作提示部 9 0 7 は、受信したメッセージを用いて、機器操作メニューを生成し、表示部 3 0 9 は、機器操作メニューを表示する（ステップ S 3 4 0）。 30

【0 4 1 7】

入力部 3 1 0 は、端末装置 3 0 0 の利用者から、機器 5 0 0 に対する操作指示を受け付ける（ステップ S 3 4 1）。制御部 3 0 1 は、操作指示を、通信部 3 0 2 及びネットワーク 2 0 を介して、確認サーバ装置 2 0 0 に対して送信する。確認サーバ装置 2 0 0 の機器制御部 2 1 3 は、操作指示を、通信部 2 0 2 及びネットワーク 2 0 を介して、機器 5 0 0 に対して送信する（ステップ S 3 4 2）。

【0 4 1 8】

機器 5 0 0 の機構制御部 5 0 1 は、確認サーバ装置 2 0 0 から、ネットワーク 2 0、通信部 5 0 2 及び命令受信部 5 0 6 を介して、操作指示に含まれる遠隔操作命令を受け取る（ステップ S 3 4 2）。次に、機構制御部 5 0 1 は、受け取った操作指示に含まれる遠隔操作命令に従って、機構 5 0 8 を制御する。機構 5 0 8 は、操作指示に含まれる遠隔操作命令に従って動作する（ステップ S 3 4 3）。 40

【0 4 1 9】

以上により、機器 5 0 0 に対する遠隔操作に関連する動作を終了する。

【0 4 2 0】

（6）機器制御ルールの修正処理の手順

機器制御ルールの修正処理の手順について、図 2 4 に示すフローチャートを用いて説明する。なお、ここで説明する機器制御ルールの修正処理の手順は、図 2 1 のステップ S 2 5 4 の詳細である。

【0 4 2 1】

機器制御部 213 は、端末装置 300 の利用者により、ログインが正常にされているか否かを判断する（ステップ S361）。

【0422】

ログインが正常にされていない場合（ステップ S361 で「異常」）、機器制御部 213 は、ログインが正常にされていないことを示すメッセージを生成する（ステップ S363）。次に、生成したメッセージを、通信部 202 及びネットワーク 20 を介して、端末装置 300 に対して送信する（ステップ S364）。制御部 301 は、ログインが正常にされていないことを示すメッセージを表示部 309 に対して出力する。表示部 309 は、当該メッセージを表示する（ステップ S365）。これにより、機器制御ルールの修正処理を終了する。

10

【0423】

ログインが正常にされている場合（ステップ S361 で「正常」）、機器制御部 213 は、機器制御部 213 は、固有識別子が取得されているか否かを判断する（ステップ S362）。固有識別子が取得されていない場合（ステップ S362 で「無し」）、機器制御部 213 は、固有識別子が取得されていないことを示すメッセージを生成する（ステップ S363）。次に、生成したメッセージを、通信部 202 及びネットワーク 20 を介して、端末装置 300 に対して送信する（ステップ S364）。制御部 301 は、固有識別子が取得されていないことを示すメッセージを表示部 309 に対して出力する。表示部 309 は、当該メッセージを表示する（ステップ S365）。これにより、機器制御ルールの修正処理を終了する。

20

【0424】

固有識別子が取得されている場合（ステップ S362 で「有り」）、機器制御部 213 は、機器情報格納部 212 から、制御ルール管理テーブル 281 を読み出す（ステップ S371）。次に、読み出した制御ルール管理テーブルを、通信部 202、ネットワーク 20 を介して、端末装置 300 に対して送信する（ステップ S372）。

【0425】

端末装置 300 の機器制御ルール提示部 906 は、確認サーバ装置 200 から、ネットワーク 20 及び通信部 302 を介して、制御ルール管理テーブルを受信する（ステップ S372）。

【0426】

次に、機器制御ルール提示部 906 は、受信した制御ルール管理テーブルを用いて、制御ルール変更画面 361 を生成する（ステップ S373）。表示部 309 は、制御ルール変更画面 361 を表示する（ステップ S374）。

30

【0427】

次に、入力部 310 は、制御ルールの変更操作を受け付ける。機器制御ルール取得部 909 は、制御ルールの変更操作を受け取る（ステップ S375）。次に、機器制御ルール取得部 909 は、制御ルールの変更操作を、通信部 302 及びネットワーク 20 を介して、確認サーバ装置 200 に対して送信する（ステップ S376）。

【0428】

機器情報管理部 217 は、端末装置 300 から、ネットワーク 20 及び通信部 202 を介して、制御ルールの変更操作を受信する（ステップ S376）。次に、機器情報管理部 217 は、受信した変更操作を用いて、機器情報格納部 212 に保持されている制御ルール管理テーブル 281 を変更する（ステップ S377）。

40

【0429】

以上により、機器制御ルールの修正処理を終了する。

【0430】

（7）相互認証及び鍵共有の手順

確認サーバ装置 200 とメモリカード 400 との間の相互認証及び鍵共有の手順について、図 25～図 26 に示すシーケンス図を用いて説明する。

【0431】

50

乱数生成部A10は、乱数R1を生成する（ステップS401）。次に、生成した乱数R1を、ネットワーク20及び端末装置300を介して、メモリカード400に送信する（ステップS402）。

【0432】

暗号化部B11は、確認サーバ装置200から乱数R1を受信する（ステップS402）。次に、システム鍵Kscを用いて、暗号化アルゴリズムE3により、乱数R1を暗号化して、暗号化乱数E3（Ksc、R1）を生成する（ステップS403）。次に、生成した暗号化乱数E3（Ksc、R1）を、端末装置300及びネットワーク20を介して、確認サーバ装置200に対して送信する（ステップS404）。

【0433】

復号部A13は、メモリカード400から、暗号化乱数E3（Ksc、R1）を受け取る（ステップS404）。次に、システム鍵Kscを用いて、復号アルゴリズムD3により、受け取った暗号化乱数E3（Ksc、R1）を復号して復号文 $R1' = D3(Ksc, E3(Ksc, R1))$ を生成する（ステップS405）。

【0434】

乱数比較部A12は、乱数R1と復号文 $R1'$ とを比較する（ステップS406）。乱数R1と復号文 $R1'$ とが一致しない場合に（ステップS406で「不一致」）、相互認証部203は、メモリカード400が不正であると判断する。相互認証部203は、その旨を示すメッセージを生成し（ステップS407）、生成したメッセージを端末装置300に対して送信する（ステップS408）。端末装置300は、メッセージを受信し（ステップS408）、表示部309は、メッセージを表示する（ステップS409）。これにより、相互認証の処理を終了する。

【0435】

次に、乱数生成部B10は、乱数R2を生成する（ステップS410）。次に、生成した乱数R2を確認サーバ装置200に送信する（ステップS411）。

【0436】

一方、乱数R1と復号文 $R1'$ とが一致する場合に（ステップS406で「一致」）、相互認証部203は、相手の装置が正当であると判断する。暗号化部A14は、相手の装置から乱数R2を受け取る（ステップS411）。システム鍵Kscを用いて、暗号化アルゴリズムE4により、乱数R2を暗号化して、暗号化乱数E4（Ksc、R2）を生成し（ステップS412）、生成した暗号化乱数E4（Ksc、R2）をメモリカード400へ送信する（ステップS413）。

【0437】

復号部B13は、確認サーバ装置200から、暗号化乱数E4（Ksc、R2）を受け取る（ステップS413）。次に、システム鍵Kscを用いて、復号アルゴリズムD4により、受け取った暗号化乱数E4（Ksc、R2）を復号して復号文 $R2' = D4(Ksc, E4(Ksc, R2))$ を生成する（ステップS414）。

【0438】

乱数比較部B14は、乱数R2と復号文 $R2'$ とを比較する（ステップS415）。乱数R2と復号文 $R2'$ とが一致しない場合に（ステップS415で「不一致」）、相互認証部403は、その旨を示すメッセージを生成する（ステップS416）。次に、生成したメッセージを端末装置300に対して送信する（ステップS417）。端末装置300は、メッセージを受信し（ステップS417）、表示部309は、メッセージを表示する（ステップS418）。これにより、相互認証の処理を終了する。

【0439】

一方、乱数R2と復号文 $R2'$ とが一致する場合に（ステップS415で「一致」）、相互認証部403は、相手の装置が正当であると判断する。

【0440】

認証に成功した場合に（ステップS406で、「一致」）、鍵共有部A15は、スカラー値である x_A を設定する（ステップS431）。次に、楕円曲線上の点 $Y_A = x_A * G$

10

20

30

40

50

を算出する（ステップS432）。ここで、Gは、楕円曲線上の点である。また、 $a * B$ は、楕円曲線上の乗算を示す。次に、鍵共有部A15は、楕円曲線上の点YAをメモリカード400に対して送信する（ステップS433）。

【0441】

認証に成功した場合には（ステップS415で、「一致」）、鍵共有部B15は、スカラー値である $x B$ を設定する（ステップS434）。次に、楕円曲線上の点 $Y B = x B * G$ を算出する（ステップS435）。次に、鍵共有部B15は、楕円曲線上の点YBを確認サーバ装置200に対して送信する（ステップS436）。

【0442】

鍵共有部A15は、スカラー値である共有鍵 $k = x A * Y B$ を算出する（ステップS437）。 10

【0443】

また、鍵共有部B15は、スカラー値である共有鍵 $k' = x B * Y A$ を算出する（ステップS438）。これにより、相互認証及び鍵共有の処理を終了する。

【0444】

ここで、共有鍵 $k = x A * Y B$
 $= x A \times (x B * G)$
 $= x B \times (x A * G)$
 $= x B * Y A$
 $= \text{共有鍵 } k' \text{ である。}$ 20

【0445】

なお、確認サーバ装置200と配信サーバ装置100との間の相互認証及び鍵共有、確認サーバ装置200と端末装置300との間の相互認証及び鍵共有、並びに、配信サーバ装置100と端末装置300との間の相互認証及び鍵共有についても、上記と同様であるので、説明を省略する。

【0446】

3. その他の変形例

なお、本発明を上記の実施の形態に基づいて説明しているが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

【0447】

（1）本発明の別の一態様は、遠隔操作システム10aであるとしてもよい。 30

【0448】

遠隔操作システム10aは、図27に示すように、操作端末300a、可搬媒体400a、サーバ装置100a及び機器500fから構成されている。

【0449】

操作端末300aは、記憶されている制御プログラム内の遠隔操作命令の実行により機器を遠隔操作する。サーバ装置100aは、操作端末300aと機器500fとの間において、遠隔操作を中継する。

【0450】

サーバ装置100aは、図27に示すように、第1取得部101a、送信部102a、第2取得部103a、判断部104a及び禁止部105aから構成されている。 40

【0451】

第1取得部101aは、第1時点において、機器500fに対する遠隔操作元の操作端末に近接する可搬媒体に固有の第1識別子を取得する。

【0452】

送信部102aは、取得した前記第1識別子を前記操作端末に記憶されている前記制御プログラムに埋め込ませるために、前記第1識別子を前記操作端末に送信する。

【0453】

第2取得部103aは、前記第1時点の後の第2時点において、機器500fに対する遠隔操作元の操作端末に近接する可搬媒体に固有の第2識別子を取得する。 50

【0454】

判断部104aは、前記制御プログラムに埋め込まれた前記第1識別子と、第2取得部103aにより取得された前記第2識別子とが一致するか否かを判断する。

【0455】

禁止部105aは、前記第1識別子と前記第2識別子とが一致しない場合、機器500fに対する遠隔操作を禁止する。

【0456】

操作端末300aは、取得部301a、送信部302a及び埋込部303aから構成されている。

【0457】

取得部301aは、操作端末300aは近接する可搬媒体400aから、可搬媒体400aに固有の識別子を取得する。

【0458】

送信部302aは、取得した前記識別子をサーバ装置100aに対して送信する。

【0459】

埋込部303aは、サーバ装置100aから、前記第1識別子を受信し、受信した第1識別子を前記制御プログラムに埋め込む。

【0460】

ここで、サーバ装置100aは、第2取得部103aを有しないとしてもよい。この場合、第1取得部101aは、さらに、前記第1時点の後の第2時点において、機器500fに対する遠隔操作元の操作端末に近接する可搬媒体に固有の第2識別子を取得する。

【0461】

(2) 本発明の別の一態様は、遠隔操作システム10bであるとしてもよい。遠隔操作システム10bは、サーバ装置と操作端末と機器とから構成される。操作端末は、記憶されている制御プログラム内の遠隔操作命令の実行により機器を遠隔操作する。サーバ装置は、操作端末と機器との間において、遠隔操作を中継する。操作端末には、可搬媒体が装着される。可搬媒体は、当該可搬媒体に固有の識別子を保持している。図28に示すシーケンス図を用いて、遠隔操作システム10bについて説明する。

【0462】

操作端末の取得部は、可搬媒体から、固有の第1識別子を取得する(ステップS501)。

【0463】

操作端末の埋込部は、操作端末が記憶している制御プログラムに、取得した第1識別子を埋め込む(ステップS502)。

【0464】

操作端末の送信部は、第1識別子が埋め込まれた制御プログラムをサーバ装置に対して送信する(ステップS503)。

【0465】

サーバ装置の抽出部は、制御プログラムから第1識別子を抽出する(ステップS504)。

【0466】

操作端末の取得部は、さらに、可搬媒体から、固有の第2識別子を取得する(ステップS505)。

【0467】

操作端末の送信部は、さらに、取得した第2識別子をサーバ装置に対して送信する(ステップS506)。

【0468】

サーバ装置の判断部は、抽出された第1識別子と、送信された第2識別子とを比較する(ステップS507)。第1識別子と第2識別子とが一致しない場合(ステップS507で「不一致」)、サーバ装置の制御部は、機器に対する遠隔操作を禁止する(ステップS

10

20

30

40

50

508)。

【0469】

第1識別子と第2識別子とが一致する場合（ステップS507で「一致」）、サーバ装置の制御部は、機器に対して、操作端末から受け取った操作指示を送信する（ステップS509）。

【0470】

機器は、サーバ装置から操作指示を受信し（ステップS509）、受信した操作指示に従って動作する（ステップS510）。

【0471】

（3）遠隔操作システム10bにおいて、次に示すようにしてもよい。

10

【0472】

図28に示すステップS502において、端末装置の埋込部は、図29に示すように、一例として64ビット長の第1識別子を分割して、8個の第1識別子片602、第2識別子片603、・・・、第8識別子片604を生成する（ステップS601）。第1識別子片602、第2識別子片603、・・・、第8識別子片604は、一例として、それぞれ、8ビット長である。

【0473】

制御プログラム605は、8個の第1領域610、第2領域611、・・・、第8領域612に分割されている。埋込部は、第1識別子片602を第1領域610の領域607に埋め込む。また、埋込部は、第2識別子片603を第2領域611の領域608に埋め込む。同様に、埋込部は、第8識別子片604を第8領域612の領域609に埋め込む。このように、埋込部は、各識別子片を、制御プログラム605の各領域に分散して埋め込む（ステップS602）。

20

【0474】

図28に示すステップS504において、図29に示すように、サーバ装置の抽出部は、制御プログラム605の第1領域610の領域607から第1識別子片613を抽出する。また、制御プログラム605の第2領域611の領域608から第2識別子片614を抽出する。同様に、制御プログラム605の第8領域612の領域609から第8識別子片615を抽出する。このように、サーバ装置の抽出部は、制御プログラム605の各領域から各識別子片を抽出する。各識別子片は、8ビット長である。次に、抽出した8個の第1識別子片613、第2識別子片614、・・・、第8識別子片615をこの順序で結合して第1識別子616を生成する（ステップS603）。第1識別子616は、64ビット長である。

30

【0475】

上記の埋込方法を、上記の実施の形態1及び2において、適用してもよい。

【0476】

（4）遠隔操作システム10bにおいて、次に示すようにしてもよい。

【0477】

図28に示すステップS502において、端末装置の埋込部は、図30に示すように、一例として64ビット長の第1識別子を分割して、8個の第1識別子片602、第2識別子片603、・・・、第8識別子片604を生成する（ステップS601）。第1識別子片602、第2識別子片603、・・・、第8識別子片604は、一例として、それぞれ、8ビット長である。

40

【0478】

制御プログラム605は、8個の第1領域610、第2領域611、・・・、第8領域612に分割されている。埋込部は、第1識別子片602を第2領域611の領域607aに埋め込む。また、埋込部は、第2識別子片603を第2領域611の領域608aに埋め込む。同様に、埋込部は、第8識別子片604を第2領域611の領域609aに埋め込む。このように、埋込部は、各識別子片を、制御プログラム605の第2領域に埋め込む（ステップS602a）。

50

【0479】

図28に示すステップS504において、図30に示すように、サーバ装置の抽出部は、制御プログラム605の第2領域611の領域607aから第1識別子片613aを抽出する。また、制御プログラム605の第2領域611の領域608aから第2識別子片614aを抽出する。同様に、制御プログラム605の第2領域611の領域609aから第8識別子片615aを抽出する。このように、サーバ装置の抽出部は、制御プログラム605の第2領域611から各識別子片を抽出する。各識別子片は、8ビット長である。次に、抽出した8個の第1識別子片613a、第2識別子片614a、・・・、第8識別子片615aをこの順序で結合して第1識別子616aを生成する（ステップS603a）。第1識別子616は、64ビット長である。

10

【0480】

上記の埋込方法を、上記の実施の形態1及び2において、適用してもよい。

【0481】

(5) 遠隔操作システム10bにおいて、次に示すようにしてもよい。

【0482】

図31に示すように、操作端末が記憶している制御プログラム651は、命令領域652とデータ領域653とから構成されている。命令領域652には、複数の命令が含まれる。複数の命令の一部は、ダミー命令654である。ダミー命令654は、実行されないように配置されている。データ領域653は、データを含む。

20

【0483】

図28に示すステップS502において、端末装置の埋込部は、図31に示すように、第1識別子を、命令領域652内のダミー命令654に埋め込む（ステップS611）。

【0484】

上記の埋込方法を、上記の実施の形態1及び2において、適用してもよい。

【0485】

図28に示すステップS504において、サーバ装置の抽出部は、制御プログラム651の命令領域652のダミー命令654に埋め込まれた第1識別子を抽出してもよい。

【0486】

(6) 遠隔操作システム10bにおいて、次に示すようにしてもよい。

【0487】

30

図32に示すように、サーバ装置の送信部は、操作端末に対して、埋込プログラム666を送信する（ステップS631）。

【0488】

埋込プログラム666は、図32に示すように、埋込命令667、対象データアドレス668及び埋込先アドレス669からなる命令を含む。埋込命令667は、対象データアドレス668により示される位置に格納されているデータを、埋込先アドレス669により示される位置に、埋め込むことを指示する。

【0489】

操作端末の受信部は、サーバ装置から、埋込プログラム666を受信する（ステップS631）。

40

【0490】

端末装置は、制御プログラム662を記憶している。制御プログラム662は、命令領域663及びデータ領域664から構成されている。

【0491】

端末装置のプログラム実行部は、受信した埋込プログラム666を実行する（ステップS632）。これにより、対象データアドレス668により示される位置に格納されているデータ、言い換えると、第1識別子661が、制御プログラム662のデータ領域664において、埋込先アドレス669により示される位置にある領域665に、埋め込まれる。

【0492】

50

上記の埋込方法を、上記の実施の形態 1 及び 2 において、適用してもよい。

【0493】

(7) 本発明の別の一態様は、遠隔操作システム 10c であるとしてもよい。遠隔操作システム 10c は、サーバ装置と操作端末と機器とから構成される。操作端末は、記憶されている制御プログラム内の遠隔操作命令の実行により機器を遠隔操作する。サーバ装置は、操作端末と機器との間において、遠隔操作を中継する。操作端末には、可搬媒体が装着される。可搬媒体は、当該可搬媒体に固有の識別子を保持している。図 33 に示すシーケンス図を用いて、遠隔操作システム 10c について説明する。

【0494】

操作端末の取得部は、可搬媒体から、固有の第 1 識別子を取得する (ステップ S531)。
10

【0495】

操作端末の送信部は、第 1 識別子をサーバ装置に対して送信する (ステップ S532)。
。

【0496】

操作端末の埋込部は、操作端末が記憶している制御プログラムに、取得した第 1 識別子を埋め込む (ステップ S533)。

【0497】

操作端末の取得部は、さらに、可搬媒体から、固有の第 2 識別子を取得する (ステップ S534)。
20

【0498】

サーバ装置の埋込部は、受信した第 1 識別子を、サーバ装置が記憶している制御プログラムに埋め込む (ステップ S535)。

【0499】

サーバ装置の第 3 演算部は、サーバ装置が記憶し、第 1 識別子が埋め込まれた制御プログラムに対して、ハッシュ演算 Hash を施して、第 3 演算値を算出する (ステップ S536)。

【0500】

サーバ装置の第 4 演算部は、第 3 演算値と、受信した第 1 識別子とに、排他的論理和 XOR を施して、第 4 演算値を算出する (ステップ S537)。
30

【0501】

端末装置の第 1 演算部は、端末装置が記憶し、第 1 識別子が埋め込まれた制御プログラムに対して、ハッシュ演算 Hash を施して、第 1 演算値を算出する (ステップ S538)。
。

【0502】

端末装置の第 2 演算部は、第 1 演算値と、取得した第 2 識別子とに、排他的論理和 XOR を施して、第 2 演算値を算出する (ステップ S539)。

【0503】

端末装置の送信部は、第 2 演算値をサーバ装置に対して送信する (ステップ S540)。
40

【0504】

サーバ装置の判断部は、算出された第 4 演算値と、送信された第 2 演算値とを比較する (ステップ S541)。第 4 演算値と第 2 演算値とが一致しない場合 (ステップ S541 で「不一致」)、サーバ装置の制御部は、機器に対する遠隔操作を禁止する (ステップ S542)。

【0505】

第 4 演算値と第 2 演算値とが一致する場合 (ステップ S541 で「一致」)、サーバ装置の制御部は、機器に対して、操作端末から受け取った操作指示を送信する (ステップ S543)。

【0506】

機器は、サーバ装置から操作指示を受信し（ステップS543）、受信した操作指示に従って動作する（ステップS544）。

【0507】

（8）本発明の別の一態様は、遠隔操作システム10dであるとしてもよい。遠隔操作システム10dは、サーバ装置と操作端末と機器とから構成される。操作端末は、記憶されている制御プログラム内の遠隔操作命令の実行により機器を遠隔操作する。サーバ装置は、操作端末と機器との間において、遠隔操作を中継する。操作端末には、可搬媒体が装着される。可搬媒体は、当該可搬媒体に固有の識別子を保持している。図34に示すシーケンス図を用いて、遠隔操作システム10dについて説明する。

【0508】

操作端末の取得部は、可搬媒体から、固有の第1識別子を取得する（ステップS561）。

【0509】

操作端末の送信部は、第1識別子をサーバ装置に対して送信する（ステップS562）。

【0510】

サーバ装置の乱数生成部は、ランダムに乱数を生成する（ステップS563）。

【0511】

サーバ装置の変換値生成部は、生成された乱数と、受信した第1識別子とに、排他的論理和XORを施して、変換値を生成する（ステップS564）。

【0512】

サーバ装置の送信部は、生成された変換値を操作端末に対して送信する（ステップS565）。

【0513】

操作端末の埋込部は、操作端末が記憶している制御プログラムに、受信した変換値を埋め込む（ステップS566）。

【0514】

端末装置の送信部は、変換値が埋め込まれた制御プログラムをサーバ装置に対して送信する（ステップS567）。

【0515】

サーバ装置の演算部は、受信した制御プログラムから、変換値を抽出し、前記乱数と、抽出した変換値とに、排他的論理和XORを施して、第1識別子を復元する（ステップS568）。

【0516】

操作端末の取得部は、可搬媒体から、固有の第2識別子を取得する（ステップS569）。

【0517】

操作端末の送信部は、第2識別子をサーバ装置に対して送信する（ステップS570）。

【0518】

サーバ装置の判断部は、復元された第1識別子と、送信された第2識別子とを比較する（ステップS571）。第1識別子と第2識別子とが一致しない場合（ステップS571で「不一致」）、サーバ装置の制御部は、機器に対する遠隔操作を禁止する（ステップS572）。

【0519】

第1識別子と第2識別子とが一致する場合（ステップS571で「一致」）、サーバ装置の制御部は、機器に対して、操作端末から受け取った操作指示を送信する（ステップS573）。

【0520】

機器は、サーバ装置から操作指示を受信し（ステップS573）、受信した操作指示に

10

20

30

40

50

従って動作する（ステップ S 5 7 4）。

【0 5 2 1】

（９）上記の各実施の形態、各変形例、各態様において、メモリカード及び可搬媒体は、一例として、SDカードである。しかし、SDカードには、限定されない。固有識別子を記憶することができれば、ハードディスクデバイス、内蔵メモリデバイスなどあるとしてもよい。

【0 5 2 2】

また、メモリカード及び可搬媒体は、端末装置との間で、短距離無線通信などの非接触型の通信を行うとしてもよい。

【0 5 2 3】

また、メモリカード及び可搬媒体に代えて、固有識別子を記憶している携帯端末装置であるとしてもよい。

【0 5 2 4】

（１０）上記の実施の形態 2 において、次のようにしてもよい。

【0 5 2 5】

信頼性評価部 2 1 0 は、固有識別子取得部 2 1 6 により受信した固有識別子と、アカウント確認部 2 1 5 により取得した利用者識別子及びパスワードを用いて、端末装置 3 0 0 にインストールされた制御プログラムの信頼性を評価してもよい。具体的には、以下の確認及びこれらの組合せにより評価を行う。

【0 5 2 6】

（a）取得した固有識別子とアカウント管理テーブル 2 6 1 に記録されている固有識別子の一致を確認する。

【0 5 2 7】

（b）取得した利用者識別子及びパスワードと、アカウント管理テーブル 2 6 1 に記載されている利用者識別子及びパスワードの一致を確認する。

【0 5 2 8】

（c）確認サーバ装置 2 0 0 において生成された生成された付随データと、端末装置 3 0 0 において、制御プログラムに埋め込まれた付随データとが一致するか否か確認する。

【0 5 2 9】

機器制御部 2 1 3 は、これらの確認による確認結果の組合せに応じて、機器 5 0 0 に対する遠隔操作を許可し又は禁止する。例えば、（a）～（c）のうち、いずれか一つでも確認できない場合、機器制御部 2 1 3 は、機器 5 0 0 に対する遠隔操作を禁止する。（a）～（c）のうち、全てにおいて確認できる場合、機器制御部 2 1 3 は、機器 5 0 0 に対する遠隔操作を許可する。

【0 5 3 0】

（１１）上記の実施の形態 2 において、次のようにしてもよい。

【0 5 3 1】

信頼性評価部 2 1 0 は、次の評価を行う。

【0 5 3 2】

（a）取得した固有識別子とアカウント管理テーブル 2 6 1 に記録されている固有識別子の一致を確認する。

【0 5 3 3】

（b）生成された付随データと、制御プログラムに埋め込まれた付随データとが一致するか否か確認する。

【0 5 3 4】

（a）において固有識別子の一致が確認できない場合、又は（b）において付随データの一致が確認できない場合、信頼性評価部 2 1 0 は、端末装置 3 0 0 に対して、利用者による利用者識別子とパスワードの入力を要求する。

【0 5 3 5】

端末装置 3 0 0 のアカウント取得部 9 0 8 は、利用者に対して、利用者識別子とパスワ

10

20

30

40

50

ードの入力を求め、利用者から利用者識別子とパスワードの入力を受け付ける。次に、アカウント取得部 908 は、利用者識別子とパスワードを確認サーバ装置 200 に対して送信する。

【0536】

確認サーバ装置 200 のアカウント確認部 215 は、利用者識別子とパスワードを受信し、受信した利用者識別子及びパスワードが、アカウント管理テーブル 261 に記憶されているか否かを確認する。

【0537】

利用者識別子及びパスワードがアカウント管理テーブル 261 に記憶されている場合、機器制御部 213 は、機器 500 に対する遠隔操作を許可する。利用者識別子及びパスワードがアカウント管理テーブル 261 に記憶されていない場合、機器制御部 213 は、機器 500 に対する遠隔操作を禁止する。

10

【0538】

(12) 上記の実施の形態 2 では、制御プログラムの起動を受け付ける時点を第 1 時点と呼び、第 1 時点において、固有識別子 Y を取得している。また、操作指示を受け付ける時点を第 2 時点と呼び、第 2 時点において、固有識別子 Y' を取得している。

【0539】

しかし、これには限定されない。第 1 時点は、制御プログラムを最初に起動する時であるとしてもよいし、制御プログラムを起動する時であるとしてもよい。

【0540】

20

また、図 17 のステップ S125 において、制御プログラムがインストールされた時点を第 1 時点としてもよい。また、この第 1 時点において、固有識別子 Y を取得してもよい。

【0541】

また、図 20 のステップ S181 において、操作指示を受け付ける時点を第 1 時点としてもよい。この第 1 時点において、固有識別子 Y を取得するとしてもよい。利用者から、再度、操作指示を受け付け、この時点を第 2 時点としてもよい。この第 2 時点において、固有識別子 Y' を取得してもよい。

【0542】

(13) 上記の各装置は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクデバイスなどから構成されるコンピュータシステムであるとしてもよい。前記 RAM 又はハードディスクデバイスには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、各装置は、その機能を達成する。ここでコンピュータプログラムは、所定の機能を達成するために、コンピュータに対する指令を示す命令コードが複数個組み合わせられて構成されたものである。

30

【0543】

(14) 上記の各装置を構成する構成要素の一部又は全部は、1 個のシステム LSI (Large Scale Integration: 大規模集積回路) から構成されているとしてもよい。システム LSI は、複数の構成部を 1 個のチップ上に集積して製造された超多機能 LSI である。システム LSI は、具体的には、マイクロプロセッサ、ROM、RAM などを含んで構成されるコンピュータシステムである。前記 RAM には、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、システム LSI は、その機能を達成する。

40

【0544】

また、上記の各装置を構成する構成要素の各部は、個別に 1 チップ化されていてもよいし、一部又は全てを含むように 1 チップ化されてもよい。

【0545】

また、上記の各装置を構成する構成要素の一部又は全部は、システム LSI であるとしているが、システム LSI とは集積度の異なる IC、LSI、スーパー LSI、ウルトラ

50

L S I 等により実現されるとしてもよい。

【0546】

また、集積回路化の手法はL S Iに限るものではなく、専用回路又は汎用プロセッサにより実現してもよい。L S I製造後に、プログラムすることが可能なF P G A (Field Programmable Gate Array) や、L S I内部の回路セルの接続や設定を再構成可能なリコンフィギュラブル・プロセッサを利用してもよい。

【0547】

さらには、半導体技術の進歩又は派生する別技術によりL S Iに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行ってもよい。

【0548】

(15) 上記の各装置を構成する構成要素の一部又は全部は、各装置に脱着可能なI Cカード又は単体のモジュールから構成されているとしてもよい。前記I Cカード又は前記モジュールは、マイクロプロセッサ、ROM、RAMなどから構成されるコンピュータシステムである。前記I Cカード又は前記モジュールは、上記の超多機能L S Iを含むとしてもよい。マイクロプロセッサが、コンピュータプログラムに従って動作することにより、前記I Cカード又は前記モジュールは、その機能を達成する。前記I Cカード又は前記モジュールは、耐タンパ性を有するとしてもよい。

【0549】

(16) また、前記コンピュータプログラムは、コンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、C D - R O M、M O、D V D、D V D - R O M、D V D - R A M、B D (B l u - r a y D i s c (登録商標))、半導体メモリなどに記録されているとしてもよい。

【0550】

また、前記コンピュータプログラムは、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送されるとしてもよい。

【0551】

また、前記コンピュータプログラムを前記記録媒体に記録して移送することにより、又は、前記コンピュータプログラムを前記ネットワーク等を経由して移送することにより、前記コンピュータプログラムを独立した他のコンピュータシステムにより実行するとしてもよい。

【0552】

(17) 以下に示すようにしてもよい。

【0553】

本発明の一態様は、ユーザ所有機器の情報提供、もしくは、ユーザ所有機器の遠隔操作を実現するための、信頼性確認サーバ、プログラムを実行するモバイル機器から構成される信頼性確認システムであって、前記プログラムは、前記信頼性確認サーバから前記プログラムの一部を受け取り、前記プログラムの一部を実行し、実行結果を前記信頼性確認サーバに通知し、前記信頼性確認サーバは、前記プログラムから受け取る前記実行結果から前記プログラムの信頼性を確認し、信頼性が低い場合、前記プログラムからの情報提示要求、ないし、機器操作要求の実行を制限することを特徴とする。

【0554】

ここで、前記信頼性確認サーバは、前記プログラムが起動されると、新たな前記プログラムの一部を前記プログラムに送信し、前記プログラムの一部は、前記信頼性確認サーバが管理する秘密番号に紐づいていて、前記プログラムの一部を実行した結果を確認することで、前記プログラムの信頼性を評価してもよい。

【0555】

ここで、前記信頼性確認システムは、さらに、固有I Dを格納する固有I D格納機器から構成され、前記固有I D格納機器は、前記モバイル機器に接続され、前記固有I D格納機器は、格納している前記固有I Dを、前記プログラム経由で、前記信頼性確認サーバに通知し、前記信頼性確認サーバは、受け取った前記固有I Dを確認することで、前記固有

10

20

30

40

50

I Dの受取り時に経由した前記プログラムの信頼性を評価してもよい。

【0556】

ここで、本発明の別の一態様は、ユーザ所有機器の情報提供、もしくは、ユーザ所有機器の遠隔操作を実現するための、信頼性確認サーバ、プログラムを実行するモバイル機器から構成される信頼性確認システムの前記信頼性確認サーバであって、前記プログラムは、前記信頼性確認サーバから前記プログラムの一部を受け取り、前記プログラムの一部を実行し、実行結果を前記信頼性確認サーバに通知し、前記信頼性確認サーバは、前記プログラムから受け取る前記実行結果から前記プログラムの信頼性を評価し、信頼性が低い場合、前記プログラムからの情報提示要求、ないし、機器操作要求の実行を制限することを特徴とする。

10

【0557】

ここで、前記信頼性確認サーバは、前記プログラムが起動されると、新たな前記プログラムの一部を送信し、前記プログラムの一部は、前記信頼性確認サーバが管理する秘密番号に紐づいていて、前記プログラムの一部を実行した結果を確認することで、前記プログラムの信頼性を評価してもよい。

【0558】

ここで、前記信頼性確認システムは、さらに、固有I Dを格納する固有I D格納機器から構成され、前記固有I D格納機器は、前記モバイル機器に接続され、前記固有I D格納機器は、格納している前記固有I Dを、前記プログラム経由で、前記信頼性確認サーバに通知し、前記信頼性確認サーバは、受け取った前記固有I Dを確認することで、前記固有I Dの受取り時に経由した前記プログラムの信頼性を評価してもよい。

20

【0559】

本発明の別の一態様は、ユーザ所有機器の遠隔操作を実現するための、信頼性確認サーバ、プログラムを実行するモバイル機器、固有I Dを格納する固有I D格納装置から構成される信頼性確認システムの前記プログラムであって、前記プログラムは、前記信頼性確認サーバから前記プログラムの一部を受け取り、前記プログラムの一部を実行し、実行結果を前記信頼性確認サーバに通知し、前記固有I D格納機器は、前記モバイル機器に接続され、前記固有I D格納機器は、格納している前記固有I Dを、前記プログラム経由で、前記信頼性確認サーバに通知し、前記信頼性確認サーバは、前記プログラムから受け取る前記実行結果、ないし、受け取った前記固有I D、ないし、その両方を確認することで、前記固有I Dの受取り時に経由した前記プログラムの信頼性を評価し、前記プログラムの信頼性が低い場合、前記信頼性確認サーバは、前記プログラムからの情報提示要求、ないし、機器操作要求の実行を制限し、前記プログラムは、前記信頼性確認サーバから受け取った機器、ないし、機能、ないし、機能グループごとの操作可否情報を元に、機器の操作可否を表現するユーザ提示用画面を生成することを特徴とする。

30

【0560】

本発明の別の一態様は、ユーザ所有機器の遠隔操作を実現するための、前記信頼性確認サーバ、プログラムを実行する前記モバイル機器から構成される前記信頼性確認システムにおけるプログラムのユーザーインターフェースであって、前記プログラムは、前記信頼性確認サーバから受け取る操作可能機器情報に従って、操作可能機器を提示するUIを生成し、操作できない前記ユーザ所有機器の描写が、操作可能な前記ユーザ所有機器の描写に比べて、不活性化されていることを特徴とする。

40

【0561】

本発明の別の一態様は、ユーザ所有機器の遠隔操作を実現する前記信頼性確認サーバ、前記プログラムを実行する前記モバイル機器から構成される前記信頼性確認システムにおけるプログラムのユーザーインターフェースであって、前記プログラムは、前記信頼性確認サーバから受け取る操作可能機能情報に従って、操作可能機能を提示するUIを生成し、操作できない前記機能の描写が、操作可能な前記機能の描写に比べて、不活性化されていることを特徴とする。

【0562】

50

ここで、前記信頼性確認システムは、さらに前記固有 I D 格納装置を備え、前記プログラムは、前記固有 I D 格納装置の固有 I D を通知するメッセージを受け取り、前記信頼性確認サーバに通知してもよい。

【0563】

(18) 本発明の一態様によると、モバイル機器におけるアプリケーションプログラムや OS (オペレーティングシステム) の不正な改ざんの有無を確認し、モバイル機器において不正な実行環境となっているか否かを確認する。これにより、成りすましのリスクが高い場合、個人情報出力を止めたり、宅内機器の操作を抑制したりする。こうして、成りすましによるリスクを低減し、安全性を高める。

【0564】

プログラム実行環境と独立して、グローバルユニークに定義された固有識別子を安全に管理する仕組みがある。信頼性を確認するサーバが、評価対象のプログラムを経由して、固有識別子を取得できれば、固有識別子を持つ装置とプログラムを実行しているモバイル機器が、高い確率で物理的に近傍にいて、その結果、ユーザ本人がプログラムを実行し操作している可能性が高いと言える。固有識別子を持つ装置は、一例として、SDカード、内蔵 HDD や内蔵フラッシュメモリを有するデバイス、USB メモリなどである。

【0565】

さらに、信頼性を確認するサーバがプログラムの一部を作り直して、モバイル機器に格納されているプログラムの一部を更新させ、次回起動時に新たなプログラムの一部を用いて初期化、及び、プログラムの改ざん検出を行う。つまり、時変要素を織り交ぜたデータを、起動の都度チェックすることで、プログラム改ざんを高い確率で検出し、不正を防止することができる。

【0566】

(19) 上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【産業上の利用可能性】

【0567】

本発明の機器を遠隔操作するシステムにおいて用いられる方法は、不正な第三者により利用者の機器が遠隔操作されることを防ぐことができ、機器を遠隔操作する技術として有用である。

【符号の説明】

【0568】

10、10a、10b、10c、10d、10e	遠隔操作システム
20	ネットワーク
100	配信サーバ装置
101	制御部
102	通信部
103	相互認証部
104	鍵格納部
105	記憶部
106	アカウント格納部
107	アカウント確認部
200	確認サーバ装置
201	制御部
202	通信部
203	相互認証部
204	鍵格納部
206	プログラム制作部
207	プログラム格納部
208	付随データ生成部
209	アカウント格納部

10

20

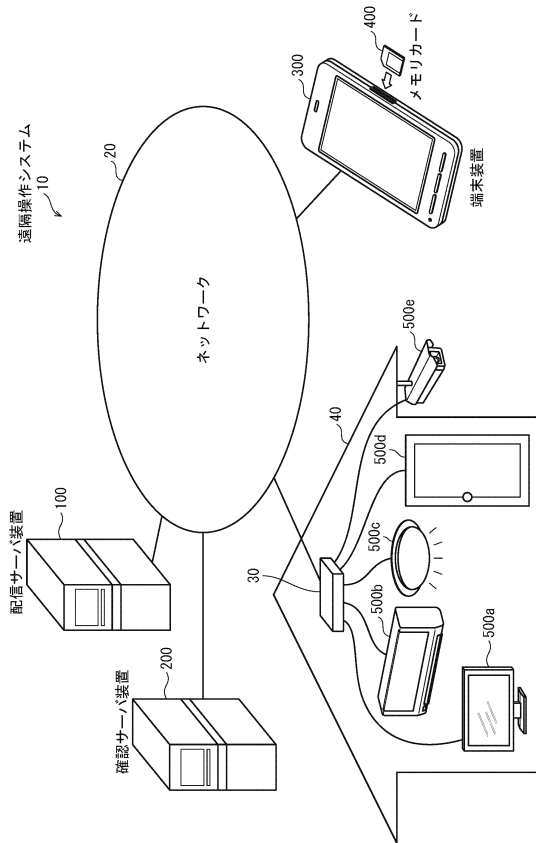
30

40

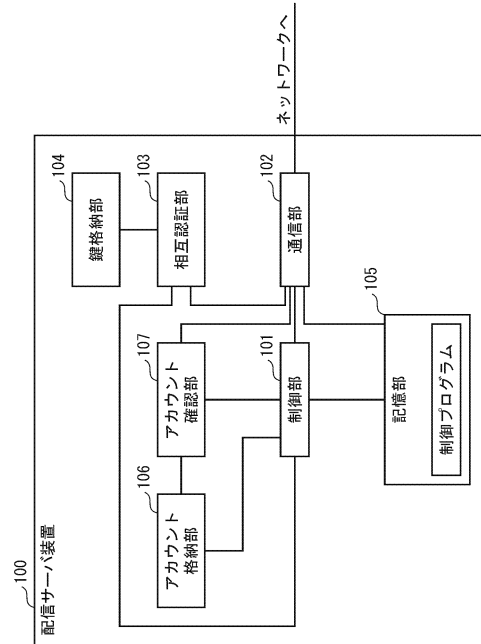
50

2 1 0	信頼性評価部	
2 1 2	機器情報格納部	
2 1 3	機器制御部	
2 1 4	署名生成部	
2 1 5	アカウント確認部	
2 1 6	固有識別子取得部	
2 1 7	機器情報管理部	
3 0 0	端末装置	
3 0 1	制御部	
3 0 2	通信部	10
3 0 3	相互認証部	
3 0 4	鍵格納部	
3 0 5	プログラム格納部	
3 0 6	プログラム実行部	
3 0 7	付随データ格納部	
3 0 8	入出力部	
3 0 9	表示部	
3 1 0	入力部	
3 1 1	検証部	
4 0 0	メモリカード	20
4 0 1	制御部	
4 0 3	相互認証部	
4 0 4	鍵格納部	
4 0 7	固有識別子格納部	
4 0 8	入出力部	
5 0 0	機器	
5 0 1	機構制御部	
5 0 2	通信部	
5 0 6	命令受信部	
5 0 7	情報通知部	30
5 0 8	機構	
5 1 0	通信部	

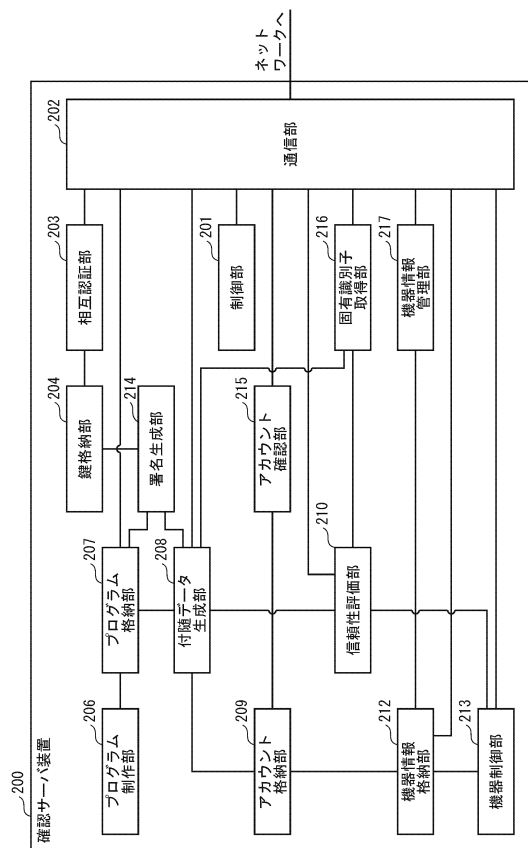
【図 1】



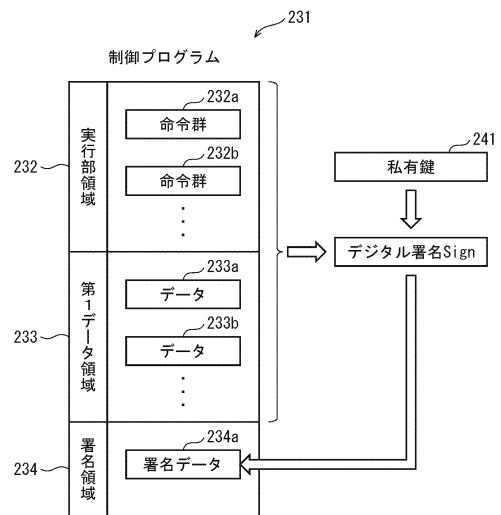
【図 2】



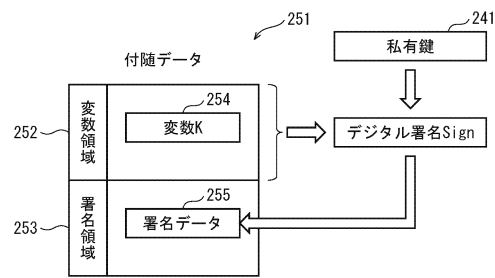
【図 3】



【図 4】



【図 5】



【図 7】

条件テーブル	
条件情報	
機器情報	条件
エアコンの室内温度、湿度	ログイン不要 固有識別子要
ドアのロック状態	ログイン要 固有識別子要
テレビの再生中チャンネル	ログイン不要 固有識別子要
再生中のDVDのタイトル	ログイン不要 固有識別子要
⋮	⋮

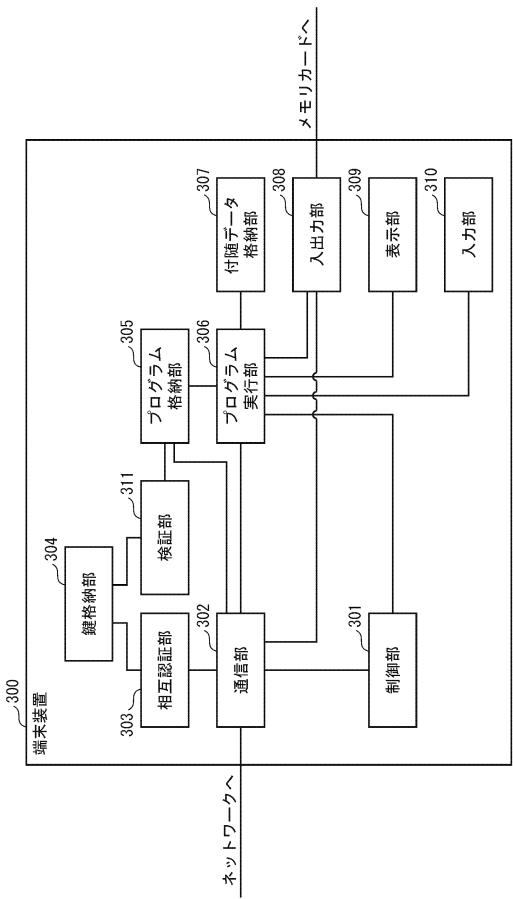
【図 6】

アカウント管理テーブル			
アカウント情報			
利用者識別子	パスワード	時変 パラメータ	固有識別子
SATO	1234	AD7C	8DA4
ITO	Abcd	7D2B	9C5E
JOHN	A2C4	4A69	7A3E
PETER	9876	F93C	85A1
⋮	⋮	⋮	⋮

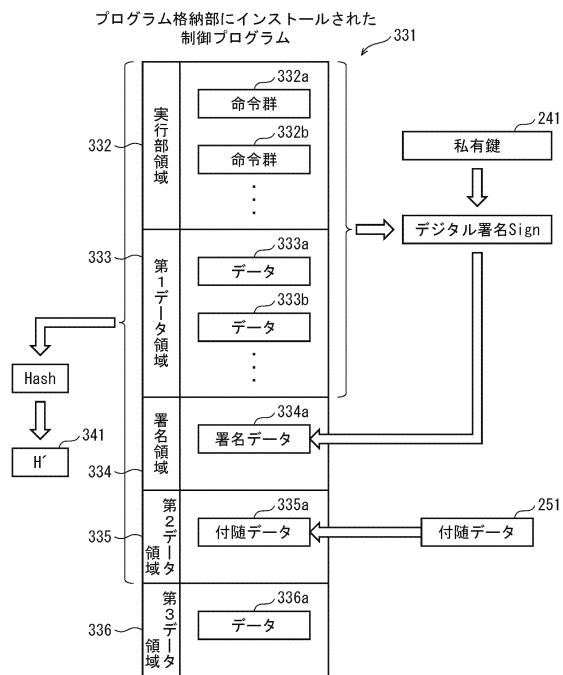
【図 8】

制御ルール管理テーブル		
利用者識別子	SATO	
制御ルール情報		
操作内容	条件	項目
ルール変更	固有識別子要	—
ドア開閉	固有識別子要	施錠
エアコン電源制御	固有識別子要	OFF
テレビ番組予約	固有識別子不要 ログイン要	予約開始
リビングライト 操作	固有識別子要	ON, OFF
ダイニングライト 操作	固有識別子要	ON, OFF
防犯カメラ 操作	固有識別子要 ログイン要	データ削除
⋮	⋮	⋮

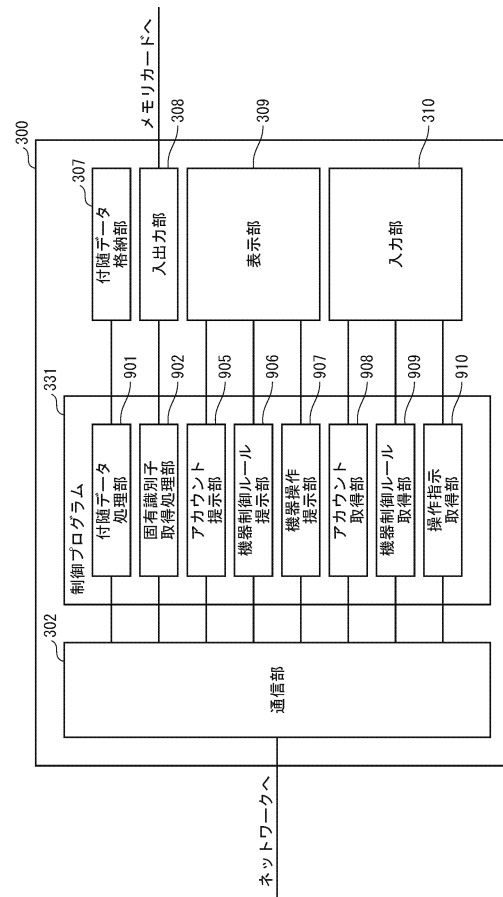
【図 9】



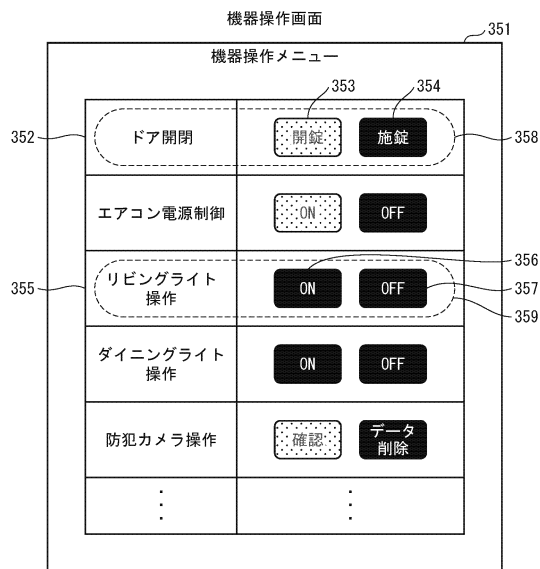
【図 10】



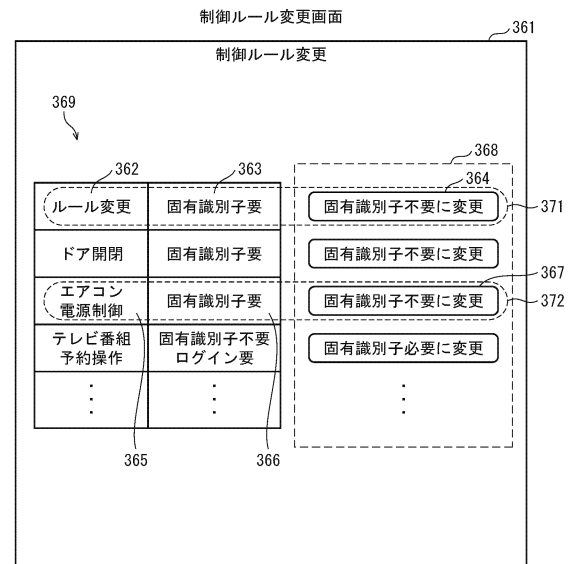
【図 11】



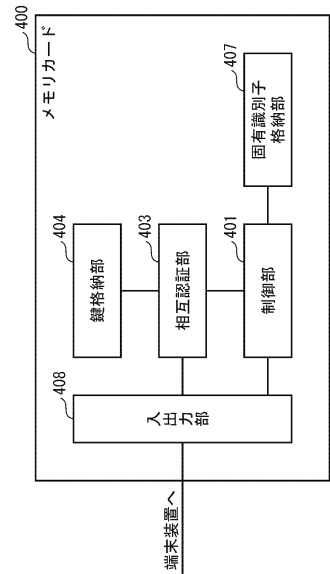
【図 12】



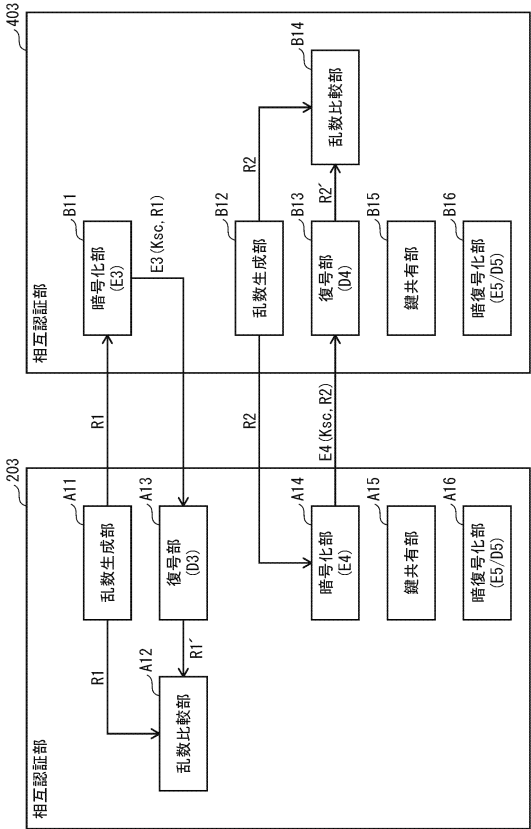
【図 13】



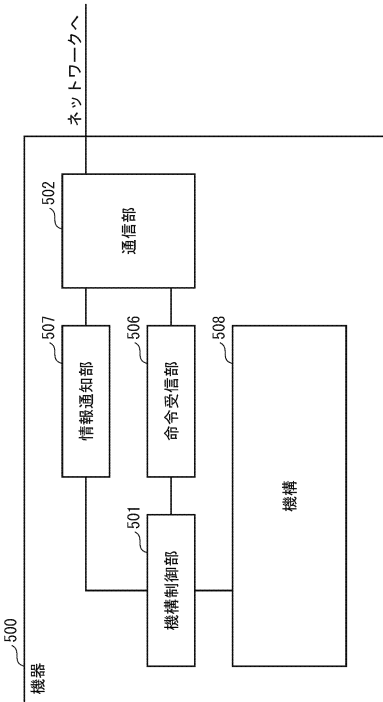
【図 1 4】



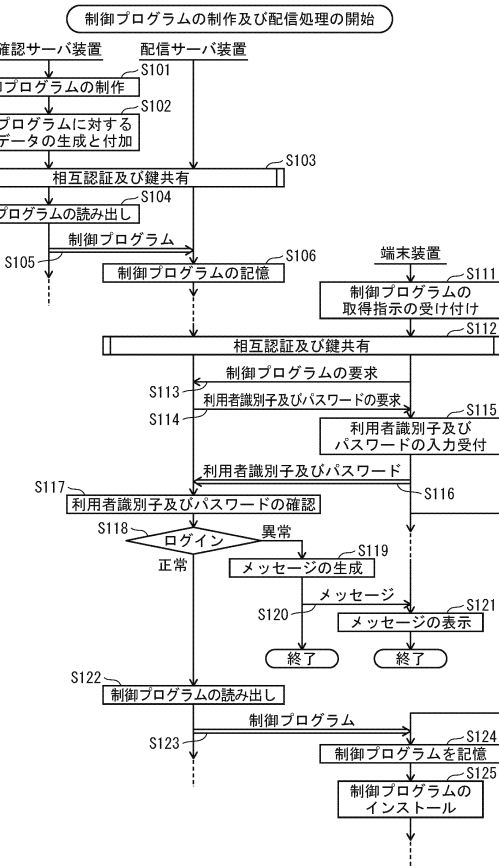
【図 1 5】



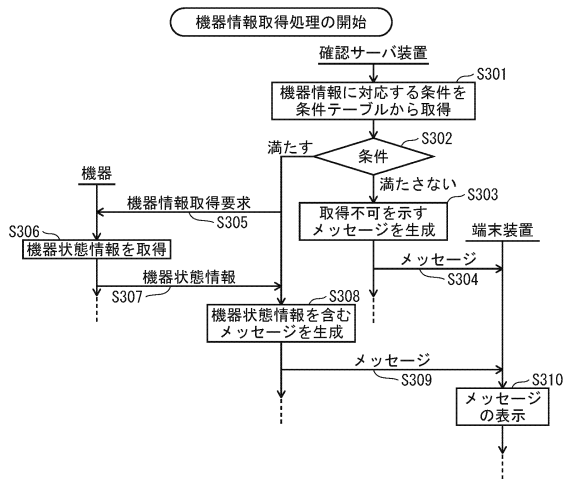
【図 1 6】



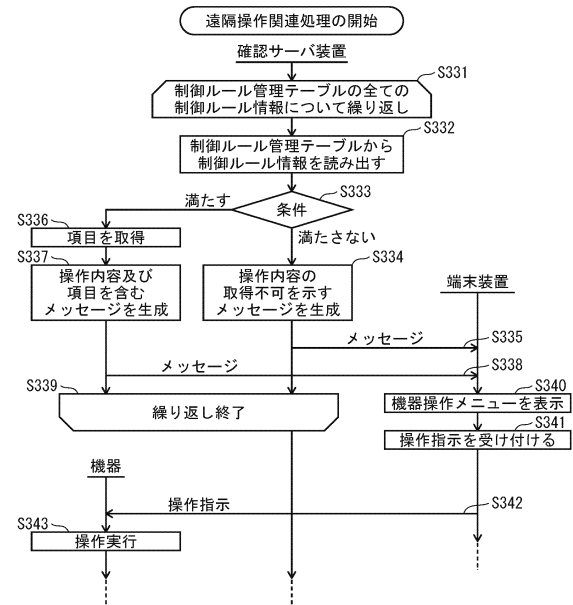
【図 1 7】



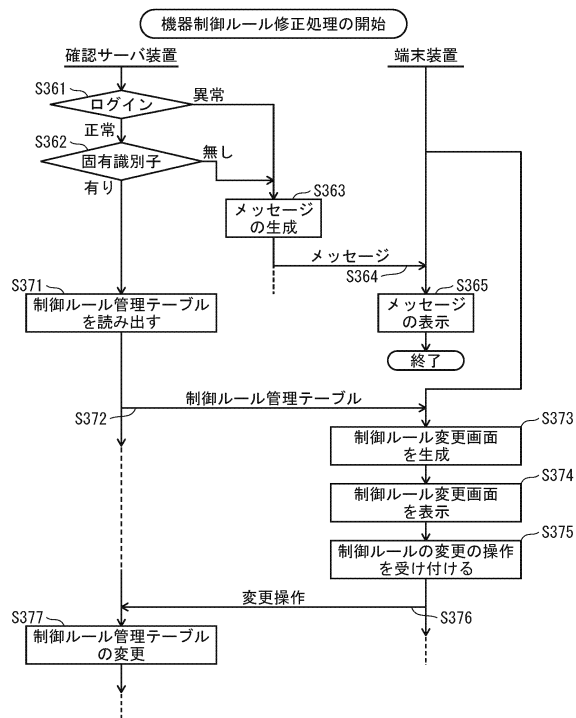
【図 2 2】



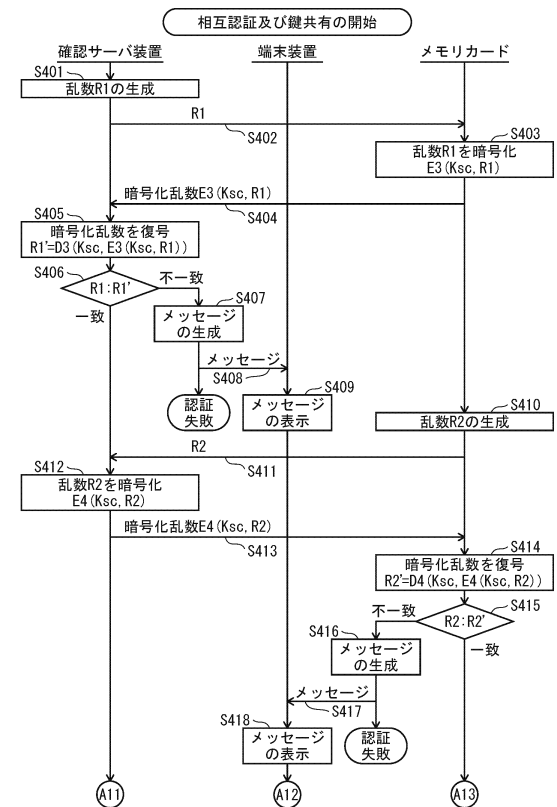
【図 2 3】



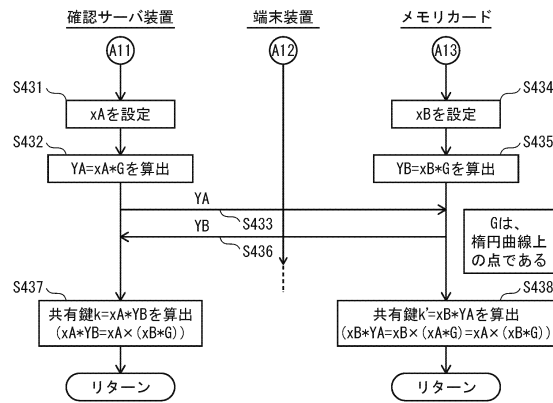
【図 2 4】



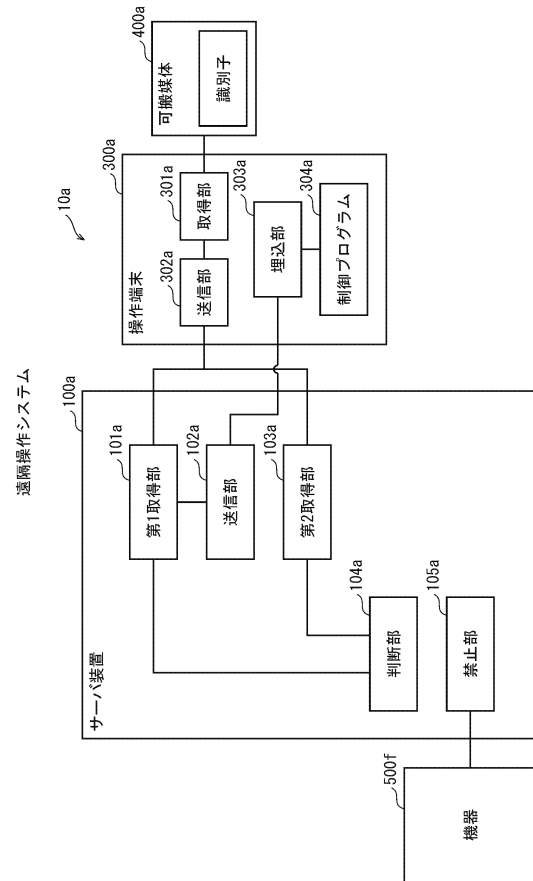
【図 2 5】



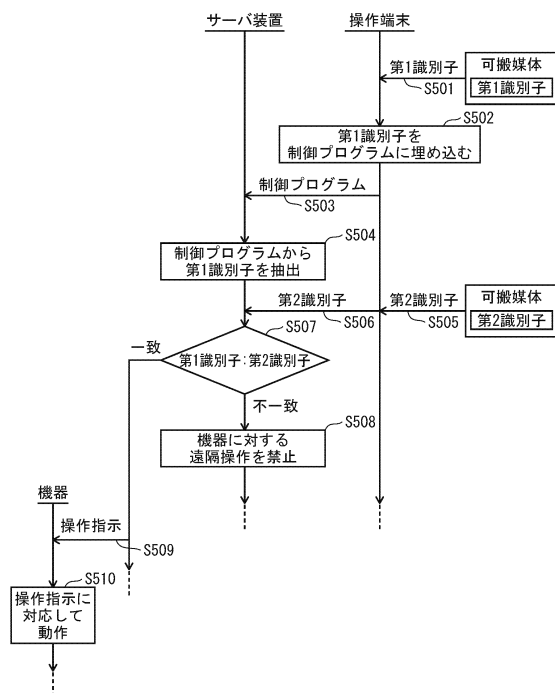
【図 26】



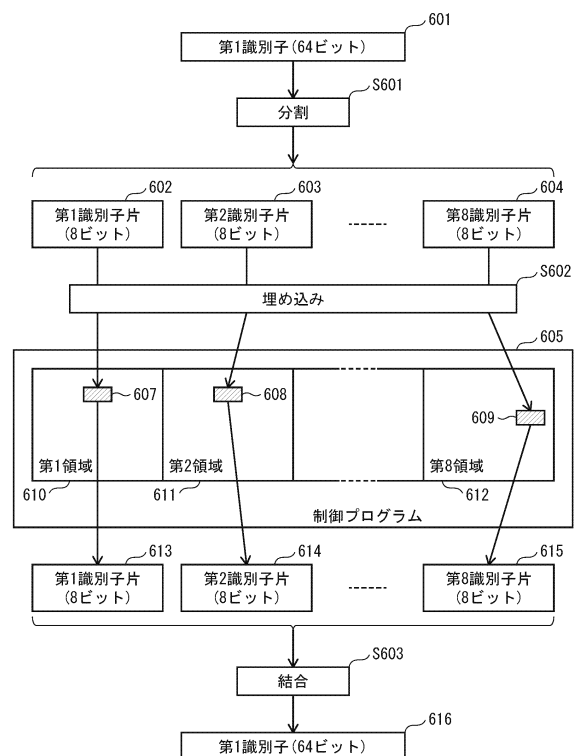
【図 27】



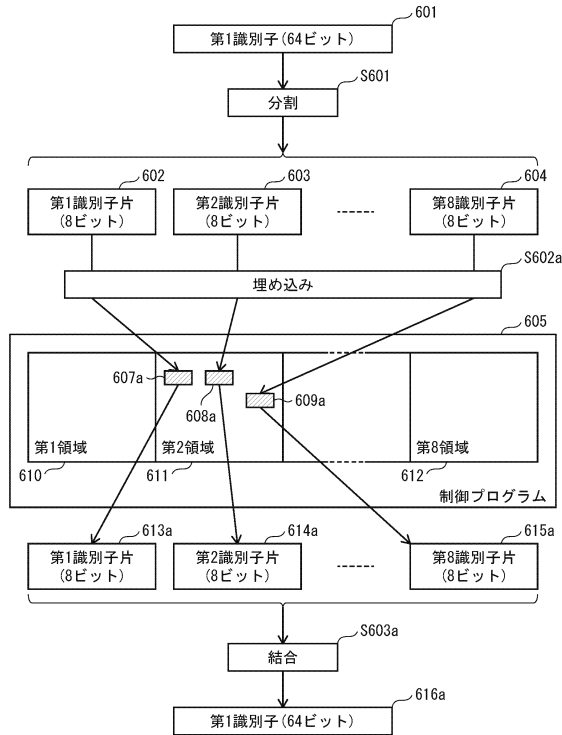
【図 28】



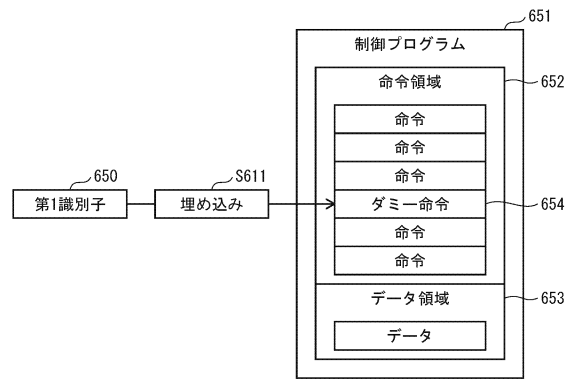
【図 29】



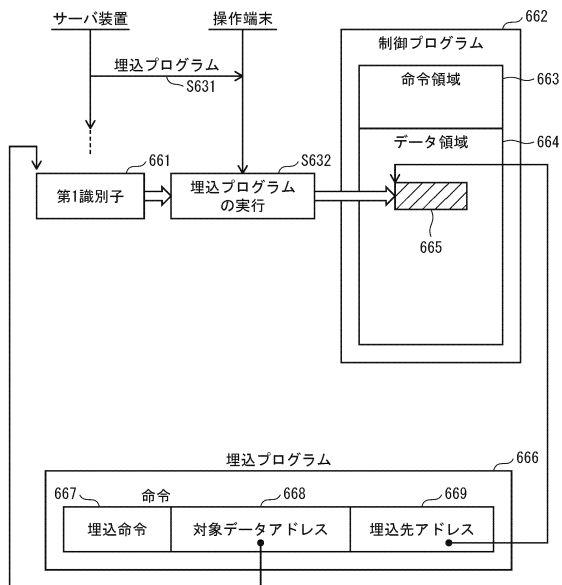
【図 30】



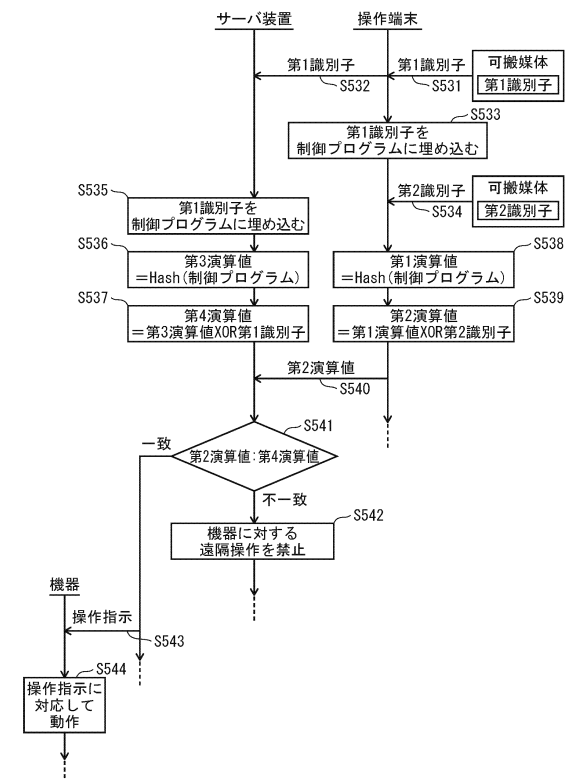
【図 31】



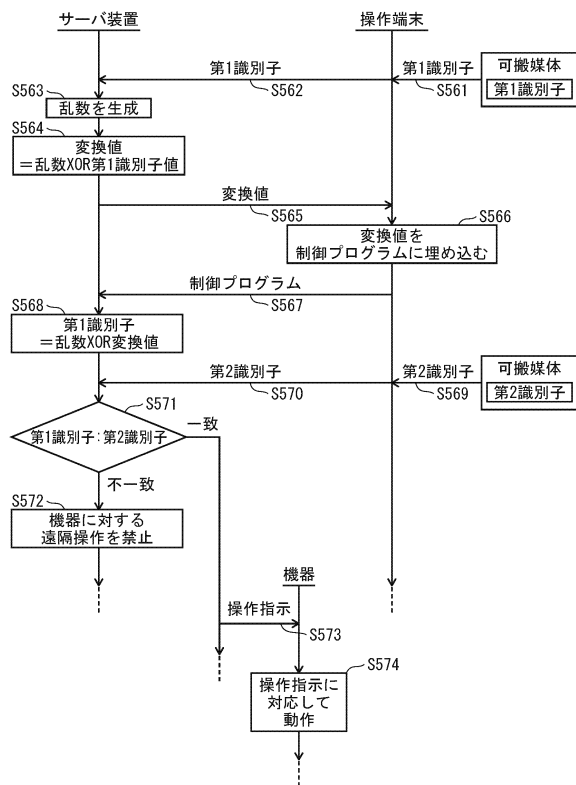
【図 32】



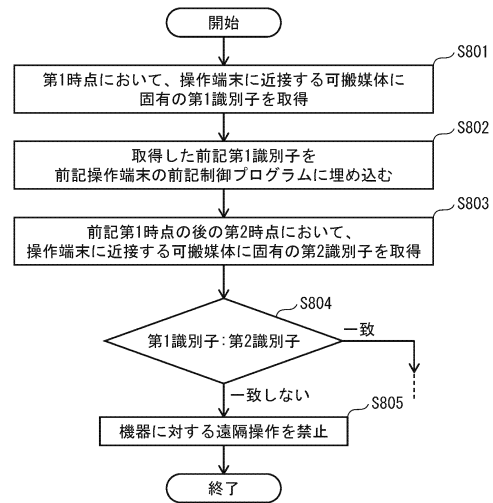
【図 33】



【図 3 4】



【図 3 5】



フロントページの続き

- (72)発明者 山口 高弘
大阪府門真市大字門真1006番地 パナソニック株式会社内
- (72)発明者 布田 裕一
大阪府門真市大字門真1006番地 パナソニック株式会社内
- (72)発明者 松崎 なつめ
大阪府門真市大字門真1006番地 パナソニック株式会社内

審査官 宮司 卓佳

- (56)参考文献 国際公開第2008/129773 (WO, A1)
特開2003-78971 (JP, A)
特開2006-129184 (JP, A)

- (58)調査した分野(Int.Cl., DB名)
G06F21/00-21/88