

明 細 書

発明の名称：

情報処理システム、情報処理方法、及び情報処理プログラム

技術分野

[0001] 本発明の実施形態は、情報処理システム、情報処理方法、及び情報処理プログラムに関する。

背景技術

[0002] モノのインターネット化（ＩｏＴ化）が進み、家庭内の汎用機器や自動車などの移動体などがインターネットと繋がり、各機器にどこからでもアクセスして制御でき、機器から取得される各種のデータを活用して電力などの供給を効率化するなど、データを活用したより利便性の高い社会が実現されつつある。

[0003] また、近年、人工知能（ＡＩ）の開発が急速に進んでおり、機器から取得されるデータなどの膨大情報を機械に学習させて最適な制御モデルを生成することで、ユーザにとってより快適なシステムの構築が可能となっている。

先行技術文献

特許文献

[0004] 特許文献１：特表２０１０－５３９５７４号公報

発明の概要

発明が解決しようとする課題

[0005] ＩｏＴ化が進み、インターネットを介して様々な機器が、どこにいても制御可能となる一方で、機器の脆弱性を未然に予防することは困難であり、悪意の第三者が機器を意図的に動作させるように機器に侵入するなど、機器がインターネットを介してサイバー攻撃を受けるおそれは常に存在する。

[0006] また、人工知能は、大量のデータ情報により学習しなければ、正しい制御モデルを形成できない場合があり、不十分なデータにより生成された制御モデルでは、誤認識が発生してしまう。このため、人工知能に機器の制御を任

せた場合、ユーザの予期しない制御動作が発生するおそれがある。

[0007] 本発明はこのような事情を考慮してなされたもので、ネットワークを介して制御可能な機器において、機器の制御動作の安全性を保持できる情報処理システム、情報処理方法、及び情報処理プログラムを提供することを目的とする。

課題を解決するための手段

[0008] 本発明の実施形態に係る情報処理システムは、ネットワークを介して機器の制御が可能なシステムであって、前記機器のそれぞれにおける、適切な制御条件を予め登録するホワイト制御条件登録部と、前記機器に対して前記制御を実行するために設定された前記設定情報を、当該機器への設定に対応する前記適切な制御条件と照合して前記機器の制御を実行する制御部と、を備えることを特徴とする。

発明の効果

[0009] 本発明の実施形態により、ネットワークを介して制御可能な機器において、機器の制御動作の安全性を保持できる情報処理システム、情報処理方法、及び情報処理プログラムが提供される。

図面の簡単な説明

[0010] [図1]本実施形態に係る情報処理システムの構成の一例を示す構成図。
[図2]機器のそれぞれに対応して設定されるホワイト制御条件の一例を示す図。
。
[図3]機器制御部において管理者端末の認証に用いる認証情報の一例を示す図。
。
[図4]本実施形態に係る情報処理方法の一例を示すフローチャート。
[図5]本実施形態に係る情報処理方法において、管理者端末の認証の流れを示すフローチャート。

発明を実施するための形態

[0011] 以下、本発明の実施形態を添付図面に基づいて説明する。

図 1 は、本実施形態に係る情報処理システム 100 の構成の一例を示す図である。

[0012] 実施形態に係る情報処理システム 100 は、インターネットなどのネットワークを介して制御が可能である機器 14 のそれぞれにおける、適切な制御条件（以下適宜、「ホワイト制御条件」と称する）を予め登録しておき、機器 14 に対して制御を実行するためにユーザにより設定された設定情報を、当該機器 14 への設定に対応する適切な制御条件と照合して機器 14 の制御を実行することで、機器 14 の制御動作の安全性を保持するシステムである。

[0013] ここで、機器 14 とは、インターネットなどのネットワークを介して動作の制御が可能な装置の全てを意味しており、家庭用機器（例えば、冷蔵庫 14 a や冷暖房機 14 b）、移動体（例えば、自動車 14 c やドローン 14 d）、製造プラント内に配置される製造装置（図示省略）が例示される。

[0014] 具体的な構成について説明する。

情報処理システム 100 は、機器制御部 10 と、ユーザ端末 11 と、管理者端末 12 と、管理携帯端末 13 と、機器 14 と、から構成されている。

[0015] 機器制御部 10 は、ネットワークを介して機器 14 と通信可能に接続されている。なお、図 1 に示す機器 14（14 a, 14 b）等のように機器制御部 10 と機器 14 とが直接通信可能に接続されてもよい。

[0016] 機器制御部 10 は、機器 14 を制御するためにユーザにより設定される設定情報を受け付ける。ユーザにより設定される機器 14 への設定情報は、機器 14 に対して設定情報の信号がユーザから直接入力される場合（例えばリモコンやタッチパネルによる入力、移動体においては速度などを制御するためのユーザの制御動作）、あるいはユーザ端末 11 からネットワーク介して設定情報の信号が機器 14 に送信される場合があり、機器制御部 10 は、ユーザにより設定される設定情報を常時受け付けている。

[0017] ユーザ端末 11 は、機器 14 に対して動作を制御するための設定情報を送信可能な端末である。ユーザ端末 11 は、設定情報を送信するときには、口

グイン認証などの認証を機器 14 とのそれぞれの間で実行して、ユーザによる設定情報を機器 14 に送信する。このとき、ユーザによる設定情報は、機器制御部 10 に対しても送信される。なお、ユーザ端末 11 と機器 14 との認証は、ログイン認証に加えて、ユーザ端末 11 によるユーザの生体認証など多段階に認証を実行してもよい。

[0018] 機器制御部 10 は、制御部 17 と、ホワイト制御条件登録部 18 と、認証情報要求部 19 と、認証部 20 と、を備えている。なお、機器制御部 10 は、一人のユーザが保有する機器 14 のそれぞれを制御するためにネットワーク上に配置されてもよいし、複数のユーザを 1 つのグループとして、各ユーザが保有する機器 14 を制御するためにネットワーク上に配置されてもよい。

[0019] なお、機器制御部 10 を構成する各ユニットの機能は、所定のプログラムコードを、プロセッサを用いて実行することによって実現しても良く、このようなソフトウェア処理に限らず、例えば、ASIC 等を用いたハードウェア処理で実現してもよいし、ソフトウェア処理とハードウェア処理とを組み合わせ実現してもよい。

[0020] ホワイト制御条件登録部 18 は、機器 14 のそれぞれにおける、適切な制御条件を予め登録している。機器 14 のそれぞれに登録される適切な制御条件は、制御を実行するためにユーザにより設定される項目のそれぞれに対応付けて適切な条件が設定される。ホワイト制御条件登録部 18 に登録される適切な制御条件は、後述する管理者端末 12 の管理者により設定される。また、適切な制御条件は、認証を受けた管理者が機器制御部 10 に対して直接設定してもよい。

[0021] ホワイト制御条件は、より具体的には、機器 14 のそれぞれを識別するための識別情報に対応付けて制御項目が設定されており、制御項目のそれぞれについて、機器 14 が動作する上で適切となる制御値や制御範囲が設定される。適切な制御条件として設定される制御値や制御範囲以外は機器 14 の動作上想定されない制御の条件となる。

- [0022] 制御項目としては、機器 14 の設定温度や設定風量、動作が開始されるべき開始時間（または終了時間）、動作継続時間など、移動体や製造プラント内に配置される製造装置の場合には速度や回転数等が例示される。加えて、制御項目として、機器 14 の制御動作が開始された後に、機器 14 に配置されたセンサなど用いて取得される各種データについて、機器 14 が動作する上で適切となる制御値や制御範囲をホワイト制御条件として設定してもよい。例えば、センサを介して取得できる機器 14 の内部の音量、機器 14 の振動数、温度、圧力、燃料残量や、電力、電圧および電流や位置情報などが設定される。機器 14 の位置情報について、適切となる位置範囲が設定されてもよい。適切となる位置範囲は、座標による指定でもよいし、一定の位置範囲（指定された位置座標を中心にして、一定の領域（例えば半径 10メートル以内））によって指定してもよい。
- [0023] さらに、制御項目として、機器 14 の制御動作が開始された後において、機器 14 が動作する上で適切となる動作順序（動作フロー）が設定されてもよい。
- [0024] また、機器 14 の制御動作の実行情報を逐次記録してログとして保存する設定をユーザがする場合において、当該ログの保存先を制御項目に設定してもよい。例えば、機器 14 の制御動作の実行情報が記録されたログの適切な保存先として、機器 14 自体に設定する。機器 14 に保存されたログは、機器 14 のディスプレイ等の表示装置でのみ閲覧可能な構成としてもよい。
- [0025] また、ログの適切な保存先として、機器制御部 10 内に設けられた記憶媒体を設定してもよい。この場合、機器制御部 10 に保存されたログは、機器制御部 10 の認証部 20 による認証が整合した管理者端末 12 からのみアクセス（閲覧）可能な構成としてもよい。なお、機器制御部 10 と管理者端末 12 との認証方法については後述する。これにより、機器制御部 10 に保存されたログは、認証された端末からのみアクセス可能となるため、ログデータを安全に保存できる。
- [0026] また、ホワイト制御条件は、1 つの制御項目に対して 1 つの適切な制御値

や制御範囲を設定する場合に限られず、1つの制御項目について1つの適切となる制御値などを設定した上で、さらに付随的な制御項目を設定し、適切となる制御値などを設定してもよい。これにより、1つの制御項目について、適切となる制御の条件をより細かく設定することができる。

[0027] 図2は、機器14のそれぞれに対応して設定されるホワイト制御条件の一例を示す図である。機器14のそれぞれの識別IDに対応付けて制御項目が設定されており、各項目には機器14が動作する上で適切となる制御値や制御範囲（ホワイト制御条件）が設定されている。例えば、機器14の識別IDが00xxに対して、「温度」及び「機器14動作シーケンス」の2つの制御項目が設定されており、それぞれについて適切となる温度範囲と動作シーケンスが決められている。さらに、制御項目「温度」については、「稼働時間帯」という付随的な条件が設定されており、適切となる稼働時間帯が追加条件として加えられている。同様に、機器14の識別IDが00x1、00x2に対しても制御項目が設定されて、それぞれにホワイト制御条件が設定されている。また、識別IDが00x3では、機器14のログの適切な保存先として、機器14本体が設定されている。

[0028] 図1に戻って説明を続ける。

制御部17は、機器14に対して制御を実行するために設定された設定情報を、当該機器14への設定に対応する適切な制御条件と照合して機器14の制御を実行する。

[0029] ユーザにより設定された設定情報（例えば機器14の温度）が、この設定情報に対応する制御項目のホワイト制御条件と一致あるいは範囲内である場合には正常であると判断する。

[0030] 一方で、制御部17は、ユーザにより設定された設定情報が、この設定情報に対応する制御項目のホワイト制御条件と一致せず、あるいは範囲外である場合には異常な設定と判断する。異常な設定と判断した場合には、当該機器14の制御動作を停止させる、あるいは適切な制御値に自動で設定を変更する。また、ユーザ端末11、管理者端末12あるいは管理携帯端末13に

異常な設定値が設定された旨を通知してもよい。これにより、機器 14 は、制御動作の安全性が常時保持される。

[0031] また、ユーザ端末 11 と機器 14 とのログイン認証等の認証時に、機器制御部 10 は、ログイン時におけるユーザ端末 11 の位置情報をユーザの設定情報として取得してもよい。この場合、ホワイト制御条件として、ユーザ端末 11 の位置情報に基づいて設定されてもよい。具体的には、ホワイト制御条件として、ユーザ端末 11 の適切となる位置範囲が設定される。適切となる位置範囲は、座標による指定でもよいし、一定の位置範囲（指定された位置座標を中心にして、一定の領域（例えば半径 10メートル以内））によって指定してもよい。また、ホワイト制御条件として、機器 14 とユーザ端末 11 との距離（例えば、30メートル以内）を設定しておき、機器 14 とユーザ端末 11 との距離が設定距離を超えている場合には、制御部 17 はユーザ端末 11 による異常な設定と判断してもよい。また、ホワイト制御条件として設定される距離は、機器 14 とユーザ端末 11 との距離に限定されるものではなく、位置の取得が可能な装置・機器（例えば、ネットワークの中継器）とユーザ端末 11 との距離に基づいて設定されてもよい。ユーザ端末 11 の位置情報は、ログイン認証時のみならず、ユーザ端末 11 が機器 14 にアクセスしている状態において継続的に取得してもよい。

[0032] また、プラントなどに配置された機器 14 が、タブレットなどのポータブル端末から制御される場合、タブレット端末の位置情報をユーザの設定情報として取得してもよい。ホワイト制御条件として、タブレット端末の位置情報に基づいて設定されてもよい。具体的には、タブレット端末の適切となる位置範囲が設定される。また、ホワイト制御条件として、機器 14 とこのポータブル端末との距離（例えば、10メートル以内）を設定しておき、設定距離の範囲を超えている場合には、制御部 17 はポータブル端末による異常な設定と判断してもよい。また、ホワイト制御条件として設定される距離は、機器 14 とポータブル端末機器との距離に限定されるものではなく、位置の取得が可能な装置・機器（例えば、ネットワークの中継器）とポータブル

端末との距離に基づいて設定されてもよい。

- [0033] さらに、ユーザ端末 1 1、機器 1 4、及び、後述するホワイト制御条件を管理する管理者端末 1 2 の位置情報を取得して、3つの位置情報に基づいてホワイト制御条件を設定してもよい。具体的には、ユーザ端末 1 1、機器 1 4、及び管理者端末 1 2 が、同時に位置すべき位置範囲を適切な制御条件と設定する。例えば、ユーザ端末 1 1、機器 1 4、及び管理者端末 1 2 が、特定の地域（例えば東京）に同時に位置することを適切な制御条件と設定し、いずれか 1 つの機器が設定された地域に無い場合には、制御部 1 7 は異常な設定と判断してもよい。さらに、ユーザ端末 1 1、機器 1 4、及び管理者端末 1 2 のそれぞれについて、位置すべき位置範囲を個別に設定してもよいし、ユーザ端末 1 1 と機器 1 4 とは同時に位置すべき位置範囲（例えば東京）を設定する一方、管理者端末 1 2 は別の位置範囲（例えば大阪）を設定するなどのように適切な位置範囲を組み合わせで設定してもよい。
- [0034] 例えば、悪意の第三者端末 5 0 が、機器 1 4 に不正にアクセスして、機器 1 4 に異常動作させるように、偽の設定情報を送信した場合であっても、偽の設定情報がホワイト制御条件の範囲外となる場合には機器 1 4 に設定されることはなく、制御動作の安全性が保持される。
- [0035] また、機器 1 4 の制御が、過去に入力された設定情報や機器 1 4 に配置されたセンサなどの取得データから機械学習を行い、機器 1 4 の動作において最適となる制御モデル、すなわち AI（人工知能）を形成して、このモデルに基づく制御である場合がある。この場合は、制御部 1 7 は、機械学習において形成された制御モデルにより機器 1 4 に対して設定される設定情報を、当該機器 1 4 への設定に対応する適切な制御条件と照合して機器 1 4 の制御を実行してもよい。
- [0036] 機械学習による制御モデルを形成する場合、学習用のデータが少ない状態での制御モデルでは、機器 1 4 の状態を十分に AI が認識できず誤動作が発生するおそれがある。本実施形態では、制御モデルにより機器 1 4 に対して設定される設定情報を、当該機器 1 4 への設定に対応する適切な制御条件（

ホワイト制御条件)と照合して機器14の制御を実行する。具体的には、制御部17は、人工知能による設定情報を、適切な制御条件(ホワイト制御条件)と照合する。人工知能による設定情報が、この設定情報に対応する制御項目のホワイト制御条件と一致せず、あるいは範囲外である場合には異常な設定と判断する。異常であると判断した場合には、当該機器14の制御動作を停止させる、あるいは適切な制御値に自動で設定を変更する。このようにすることで、人工知能による誤認識による異常動作を防止でき、機器14の制御動作の安全性が保持できる。

[0037] 続いて、ホワイト制御条件登録部18に登録された機器14のホワイト制御条件を変更する(更新する)場合について検討する。

[0038] 管理者端末12は、ホワイト制御条件登録部18に登録された、機器14のそれぞれに対応する適切な制御条件を管理するための端末である。管理者端末12は、ホワイト制御条件変更部21と、認証情報送信部22と、を備えている。

[0039] ここで、機器制御部10の認証部20は、管理者端末12からアクセスがあった際に、管理者端末12を識別して認証するための認証情報を予め登録している。認証情報として、例えば管理者端末12の位置情報を登録する。なお、認証情報として、管理者端末12を識別するための固有の識別情報(端末のMACアドレスなど)、管理者端末12の管理者の指紋情報、「顔」情報などの生体情報を登録してもよい。

[0040] 管理者端末12のホワイト制御条件変更部21は、ホワイト制御条件を更新する際に、更新された制御条件を機器制御部10に送信して制御条件の変更を要求する。ホワイト制御条件の更新を受け付けた機器制御部10の認証情報要求部19は、管理者端末12の認証情報を管理者端末12に要求する。

[0041] そして、管理者端末12の認証情報送信部22は、管理者端末12の認証情報を機器制御部10に送信する。

[0042] 機器制御部10の認証部20は、管理者端末12から受け付けた認証情報

を、予め登録されている登録認証情報と照合することで、正しい管理者端末 12 からのホワイト制御条件の更新要求か否かを判断する。受け付けた認証情報が登録されている登録認証情報と一致する場合には、正しい管理者端末 12 からのアクセスを認めて、ホワイト制御条件登録部 18 のホワイト制御条件を上書き更新する。

[0043] 一方で、受け付けた認証情報が登録されている登録認証情報と一致しない場合には、ホワイト制御条件登録部 18 のホワイト制御条件は更新されない。このように、ホワイト制御条件登録部 18 のホワイト制御条件は、管理者端末 12 からのみ更新することができる。

[0044] また、管理者端末 12 に関連付けて登録した管理携帯端末 13 を用いて管理者端末 12 の認証を行ってもよい。このとき、管理者端末 12 に対して、管理携帯端末 13 を識別するための識別情報（携帯端末の識別番号、電話番号、位置情報など）が関連付けられる。

[0045] 図 3 は、管理者端末 12 の認証に用いる認証情報の一例を示す図である。

機器制御部 10 の認証部 20 では、管理者端末 12 の識別番号に対応して管理者端末 12 の位置情報が登録されている。加えて、管理者端末 12 に対応して管理携帯端末 13 の識別番号、電話番号、及び位置情報が関連付けて登録されている。なお、位置情報は、座標による指定でもよいし、一定の位置範囲（指定された位置座標を中心にして、一定の領域（例えば半径 10 メートル以内））によって指定してもよい。

[0046] 管理携帯端末 13 を用いた管理者端末 12 の認証方法として、具体的には、ホワイト制御条件の更新を受け付けた機器制御部 10 の認証情報要求部 19 は、管理携帯端末 13 に認証用のキー（識別コード）を送信して、認証用のキーの送信を管理者端末 12 に対して要求する。認証用のキーは、例えばランダムに発生されたワンタイムパスワードである。

[0047] 機器制御部 10 の認証部 20 は、管理者端末 12 から、先に管理携帯端末 13 に送信した認証用のキーと同じキーを受け付けた場合に、正しい管理者端末 12 からのアクセスと認めて、ホワイト制御条件登録部 18 のホワイト

制御条件を上書き更新する。

[0048] また、機器制御部 10 の認証部 20 は、管理携帯端末 13 の位置情報を管理者端末 12 の認証に用いてもよい。なお、機器制御部 10 の認証部 20 は、複数の認証サーバから構成されて、認証用のキーを管理携帯端末 13 に送信するサーバと、管理者端末 12 から認証用のキーを受け付けて認証するサーバを別々に構成してもよい。

[0049] このように、機器制御部 10 の認証部 20 は、管理者端末 12 の位置情報などを用いて正しい管理者端末 12 からのアクセスか否かを認証することで、ホワイト制御条件登録部 18 のホワイト制御条件を強固に保護することができる。仮に悪意の第三者端末 50 が、ホワイト制御条件を変更しようとした場合であっても、機器制御部 10 の認証を認めることはできないため、ホワイト制御条件を変更することはできない。

[0050] 続いて、本実施形態に係る情報処理システム 100 の動作について説明する。

図 4 は、本実施形態に係る情報処理方法の一例を示すフローチャートである（適宜、図 1 参照）。

[0051] 機器制御部 10 の制御部 17 は、ユーザにより設定される設定情報を受け付ける（S10）。そして、制御部 17 は、ユーザにより設定された設定情報に対応するホワイト制御条件を確認する（S11）。

[0052] 制御部 17 は、ユーザにより設定された設定情報が、この設定情報に対応する制御項目のホワイト制御条件と一致あるいは範囲内である場合には、正常であると判断して、設定情報に基づく機器 14 の制御を継続させる（S12：YES、S13）。

[0053] 一方で、制御部 17 は、ユーザにより設定された設定情報が、この設定情報に対応する制御項目のホワイト制御条件と一致せず、あるいは範囲外である場合には異常な設定と判断して、例えば当該機器 14 の制御動作を停止させる（S12：NO）。なお、制御部 17 は、ユーザ端末 11 と機器 14 とのログイン認証等の認証時などに、ユーザ端末 11 の位置情報を取得して、

機器 1 4 とユーザ端末 1 1 との距離に基づいて異常な設定か否かを判断してもよい。

[0054] 続いて、図 5 は、本実施形態に係る情報処理方法において、管理者端末 1 2 の認証の流れを示すフローチャートである（適宜、図 1 参照）。ここでは、管理者端末 1 2 のホワイト制御条件変更部 2 1 が、ホワイト制御条件を更新する際に、更新された制御条件をホワイト制御条件登録部 1 8 に送信した場合について検討する。

[0055] 機器制御部 1 0 の認証情報要求部 1 9 は、管理者端末 1 2 に対して認証情報を要求する（S 2 0）。

[0056] 続いて、管理者端末 1 2 の認証情報送信部 2 2 は、管理者端末 1 2 の位置情報を機器制御部 1 0 に送信する（S 2 1）。

[0057] 機器制御部 1 0 の認証部 2 0 は、送信された位置情報を、登録されている位置情報と照合する。送信された位置情報が、登録された位置情報の範囲内でない場合には、正しいアクセスでないとして終了する（S 2 2 : NO、終了）。

[0058] 一方で、認証部 2 0 は、送信された位置情報が登録された位置情報の範囲にある場合に、管理携帯端末 1 3 に認証キーを送信する（S 2 2 : YES、S 2 3）。

[0059] そして、管理者端末 1 2 の管理者は、管理携帯端末 1 3 で認証キーを確認して、管理者端末 1 2 から機器制御部 1 0 に当該認証キーを送信する。

[0060] 機器制御部 1 0 の認証部 2 0 は、管理者端末 1 2 から送信された認証キーが正しいものである場合には、ホワイト制御条件を更新する（S 2 4 : YES、S 2 5）。一方で、送信された認証キーが正しいものでない場合には、正しいアクセスでないとして終了する（S 2 4 : NO、終了）。

[0061] 以上述べた実施形態の情報処理システムによれば、機器のそれぞれにおける、適切な制御条件を予め登録しておき、機器に対して制御を実行するために設定された設定情報を、当該機器への設定に対応する適切な制御条件と照合して機器の制御を実行することで、器の制御動作の安全性を保持できる。

加えて、正しい管理者端末からのアクセスか否かを認証することで、ホワイト制御条件を強固に保護することができる。

[0062] なお、情報処理システムを構成する装置で実行されるプログラムは、ROM等の記憶回路に予め組み込んで提供される。もしくは、このプログラムは、インストール可能な形式または実行可能な形式のファイルでCD-ROM、CD-R、メモリカード、DVD、フレキシブルディスク等のコンピュータで読み取り可能な記憶媒体に記憶されて提供するようにしてもよい。また、情報処理システムで実行されるプログラムは、インターネット等のネットワークに接続されたコンピュータ上に格納し、ネットワーク経由でダウンロードさせて提供するようにしてもよい。

[0063] 本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

符号の説明

[0064] 10…機器制御部、11…ユーザ端末、12…管理者端末、13…管理携帯端末、14a, 14b…家庭用機器、14c…移動体（自動車）、14d…移動体（ドローン）、17…制御部、18…ホワイト制御条件登録部、19…認証情報要求部、20…認証部、21…ホワイト制御条件変更部、22…認証情報送信部、50…第三者端末、100…情報処理システム。

請求の範囲

- [請求項1] ネットワークを介して機器の制御が可能なシステムであって、
前記機器のそれぞれにおける、適切な制御条件を予め登録するホワイト制御条件登録部と、
前記機器に対して前記制御を実行するために設定された設定情報を、当該機器への設定に対応する前記適切な制御条件と照合して前記機器の制御を実行する制御部と、
を備えることを特徴とする情報処理システム。
- [請求項2] 前記機器のそれぞれに登録される前記適切な制御条件は、前記制御を実行するためにユーザにより設定される項目のそれぞれに対応付けて適切な条件が設定される、
ことを特徴とする請求項1に記載の情報処理システム。
- [請求項3] 機器の制御が、機械学習を用いた制御である場合に、
前記制御部は、機械学習において生成された制御モデルにより設定される設定情報を、当該機器への設定に対応する前記適切な制御条件と照合して前記機器の制御を実行する、
ことを特徴とする請求項1に記載の情報処理システム。
- [請求項4] 前記機器のそれぞれに対応する前記適切な制御条件を管理して、更新した前記制御条件を前記ホワイト制御条件登録部に送信する管理者端末を備えて、
更新された前記制御条件が送信された際に、前記管理者端末の認証情報を前記管理者端末に要求して、予め登録した登録認証情報と合致する場合に、更新された前記制御条件の前記ホワイト制御条件登録部への更新を認める認証部と、をさらに有する、
ことを特徴とする請求項1に記載の情報処理システム。
- [請求項5] 前記認証情報は、前記管理者端末の位置情報である、
ことを特徴とする請求項4に記載の情報処理システム。
- [請求項6] 前記管理者端末に対応して登録された管理携帯端末を備えて、

前記認証部は、更新された前記制御条件が送信された際に、前記管理携帯端末に認証用の識別コードを送り、当該識別コードを前記管理者端末から受け付けた際に、更新された前記制御条件の前記ホワイト制御条件登録部への更新を認める、
ことを特徴とする請求項4に記載の情報処理システム。

[請求項7] 前記設定情報には、前記機器を制御するユーザ機器の位置情報が含まれて、

前記ホワイト制御条件登録部は、前記ユーザ機器の位置情報に基づいて適切な制御条件が予め登録される、
ことを特徴とする請求項1に記載の情報処理システム。

[請求項8] 前記設定情報には、前記機器、前記機器を制御するユーザ機器、前記管理者端末の位置情報が含まれて、

前記ホワイト制御条件登録部は、前記機器、前記機器を制御するユーザ機器、前記管理者端末のいずれか1つの位置情報に基づいて適切な制御条件が予め登録される、
ことを特徴とする請求項4に記載の情報処理システム。

[請求項9] ネットワークを介して機器の制御が可能な情報処理方法であって、
前記機器のそれぞれにおける、適切な制御条件をホワイト制御条件登録部に予め登録するステップと、

前記機器に対して前記制御を実行するために設定された設定情報を、当該機器への設定に対応する前記適切な制御条件と照合して前記機器の制御を実行するステップと、
を含むことを特徴とする情報処理方法。

[請求項10] コンピュータを、
ネットワークを介して制御が可能な機器のそれぞれにおける、適切な制御条件をホワイト制御条件登録部に予め登録する機能、

前記機器に対して前記制御を実行するために設定された設定情報を、当該機器への設定に対応する前記適切な制御条件と照合して前記機

器の制御を実行する機能、
として機能させることを特徴とする情報処理プログラム。