(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6640802号
(P6640802)

(45)発行日　令和2年2月5日(2020.2.5)　(24)登録日　令和2年1月7日(2020.1.7)

(51)Int.Cl.		F I	
G06F 21/62	(2013.01)	G06F	21/62
G06F 21/31	(2013.01)	G06F	21/31
G06Q 50/04	(2012.01)	G06Q	50/04

請求項の数 9　(全 21 頁)

(21)出願番号　特願2017-171061(P2017-171061)
(22)出願日　平成29年9月6日(2017.9.6)
(65)公開番号　特開2019-46349(P2019-46349A)
(43)公開日　平成31年3月22日(2019.3.22)
審査請求日　平成30年11月19日(2018.11.19)

早期審査対象出願

(73)特許権者　390008235
ファナック株式会社
山梨県南都留郡忍野村忍草字古馬場３５８０番地
(74)代理人　100106002
弁理士　正林　真之
(74)代理人　100165157
弁理士　芝　哲央
(74)代理人　100160794
弁理士　星野　寛明
(72)発明者　西　浩次
山梨県南都留郡忍野村忍草字古馬場３５８０番地　ファナック株式会社内

審査官　岸野　徹

最終頁に続く

(54)【発明の名称】エッジサーバ及びアプリケーションセキュリティ管理システム

(57)【特許請求の範囲】
【請求項１】
１台以上のエッジ機器と通信可能に接続されたエッジサーバであって、
前記エッジサーバで稼働する、前記エッジ機器の機能の使用及び／又は前記エッジ機器の処理データに対するアクセスを行うアプリケーションの実行を管理するアプリケーション実行管理手段と、
前記アプリケーションを記憶するアプリケーション記憶部と、
予め設定された前記エッジ機器の機能の使用の有無及び／又は前記エッジ機器の処理データに対するアクセスの有無に係るスキル情報別アクセスコントロールリストを記憶するアクセスコントロール記憶部と、
前記エッジサーバを含むシステムへのログインが承認されたユーザのスキル情報を取得するスキル情報取得手段と、
前記ユーザが前記アプリケーションを介して前記エッジ機器の機能の使用及び／又は前記エッジ機器の処理データに対するアクセスを要求する際に、前記ユーザのスキル情報と、前記アクセスコントロール記憶部に記憶された前記スキル情報別アクセスコントロールリストとに基づいて、前記ユーザの前記エッジ機器の機能の使用及び／又は前記エッジ機器の処理データに対するアクセスに係る権限の有無を判断するアクセス権限判断手段と、
前記アクセス権限判断手段によって前記ユーザの権限が有ると判断された場合に限り、前記ユーザの前記アプリケーションを介した前記エッジ機器に係る機能の使用及び／又は前記エッジ機器の処理データへのアクセスを許可するアクセス制御手段と、

を備える、
エッジサーバ。
【請求項２】
請求項１に記載のエッジサーバにおいて、
前記スキル情報別アクセスコントロールリストは、前記スキル情報ごとに前記エッジ機器の種類及び／又は設置グループに対するアクセス可否情報を含む、
エッジサーバ。
【請求項３】
請求項１又は請求項２に記載のエッジサーバにおいて、
前記スキル情報取得手段は、前記エッジサーバに対して通信可能に接続され、前記エッジサーバを含むシステムのユーザを管理する管理サーバから、前記ユーザのスキル情報を取得する、
エッジサーバ。
【請求項４】
請求項３に記載のエッジサーバにおいて、
前記エッジサーバを含むシステムのユーザを管理する前記管理サーバのエージェントである管理エージェントを備え、
前記スキル情報取得手段は、前記管理エージェントから、前記ユーザのスキル情報を取得する、
エッジサーバ。
【請求項５】
請求項１から請求項４までのいずれかに記載のエッジサーバにおいて、
前記スキル情報別アクセスコントロールリストは、前記スキル情報ごとに、
前記エッジ機器の動作状態に係る各機能の使用可否情報及び／又は各処理データに対するアクセス可否情報、
前記エッジ機器の生産状況に係る各機能の使用可否情報及び／又は各処理データに対するアクセス可否情報、
前記エッジ機器の品質保守に係る各機能の使用可否情報及び／又は各処理データに対するアクセス可否情報、
前記エッジ機器のイベント（履歴）に係る各機能の使用可否情報及び／又は各処理データに対するアクセス可否情報、及び
前記エッジ機器のアーカイブに係る各機能の使用可否情報及び／又は各処理データに対するアクセス可否情報を含む、
エッジサーバ。
【請求項６】
請求項１から請求項５までのいずれかに記載のエッジサーバにおいて、
前記スキル情報は、さらに、
各ユーザの資格に関する情報、所属するグループに関する情報、作業可能なエッジ機器に関する情報、作業可能な作業内容に関する情報及びそれらの研修受講有無に関する情報の少なくともいずれかを含む、
エッジサーバ。
【請求項７】
請求項１から請求項６までのいずれかに記載のエッジサーバにおいて、
前記アプリケーションは、
前記エッジサーバを前記アクセス権限判断手段及び／又は前記アクセス制御手段として機能させる、
エッジサーバ。
【請求項８】
請求項１から請求項７までのいずれかに記載のエッジサーバにおいて、
前記アプリケーション記憶部は、前記アプリケーションと、前記アプリケーションの前

記エッジ機器の機能の使用の有無及び／又は前記エッジ機器の処理データに対するアクセスの有無に係るセキュリティリスクリストとを記憶し、
前記アクセス制御手段は、前記セキュリティリスクリストの内容に基づいて、前記アプリケーションのエッジ機器の機能の使用及び／又は前記エッジ機器の処理データへのアクセスに係る要求を監視し、前記セキュリティリスクリストに開示された前記エッジ機器に係る機能の使用及び／又は前記エッジ機器の処理データへのアクセスに係る要求のみを許可する、
エッジサーバ。
【請求項９】
請求項１から請求項８に記載のエッジサーバと、
前記エッジサーバに対して通信可能に接続された管理サーバと、
を備えたアプリケーションセキュリティ管理システムであって、
前記エッジサーバは、前記エッジサーバを含むシステムへのログインが承認されていない場合に、ユーザのログイン情報を前記管理サーバに送信し、
前記管理サーバは、
各ユーザの前記スキル情報を記憶するスキル情報記憶部と、
前記ユーザのログイン情報を、前記エッジサーバから受け付けるログイン受付手段と、
前記ログイン受付手段により受け付けた前記ログイン情報を使用して認証を行う認証手段と、
前記認証手段により認証がされた場合に、前記スキル情報記憶部から前記ユーザに対応する前記スキル情報を抽出して、前記エッジサーバに対して送信するスキル情報送信手段と、
を備え、
前記エッジサーバの前記スキル情報取得手段は、前記管理サーバから受信した前記スキル情報を、前記ログインが承認されたユーザのスキル情報として取得する、
アプリケーションセキュリティ管理システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、エッジサーバ及びアプリケーションセキュリティ管理システムに関する。
【背景技術】
【０００２】
製造装置の分野において、昨今、製造現場向けに様々な機能や目的を持ったサーバアプリケーションソフトウェア（以降、単に「アプリケーション」、「アプリ」ともいう。）が、様々な会社で開発されている。アプリケーションは、使用者のユースケースを想定して開発されることが多い。開発されるアプリケーションとしては、例えば、製造現場の管理者向けの製造ライン管理用途のアプリケーションや、製造装置の保守サービス員向けの保守作業支援アプリケーション、ネットワークインテグレータ向けのネットワーク設定支援アプリケーション等である。
そして、コンピュータを利用する際に、ユーザ名とパスワード等を入力してサインオンすることで、事前登録された者かどうかの確認が行われ、悪意ある者に不正使用されないような対応が、一般的に行われる。サインオンは、コンピュータを使用開始する前に一度行われる場合や、コンピュータでアプリケーションを使用開始する前に一度行われる場合がある。一般的なサインオンは、例えば、工場責任者等の責任者がコンピュータやアプリケーションの使用者のユーザ情報とパスワードとを、例えば、クラウド上の管理サーバに予め登録することで行われる。そして、コンピュータやアプリケーションが複数ある場合でも、コンピュータやアプリケーションへのサインオンの際に、管理サーバにユーザ情報とパスワードとを送信して、使用者が登録されているかを問い合わせが行われることで、各コンピュータやアプリケーションソフトウェアごとに使用者を登録する必要がない。
【０００３】

一般的なサインオンは、使用者がコンピュータやアプリケーションの使用を一度許可されると、使用者は、コンピュータやアプリケーションの全ての機能を利用することができる。しかし、アプリケーションが持つ機能リスクに基づき、サインオンできる使用者の一部のみに、リスクの高い機能を利用可能にし、他の使用者は利用不可にしたい場合がある。

このような問題に対処すべく、例えば、特許文献１には、使用者の役割に応じて、使用できるアプリケーションの機能を制限する技術が開示されている。具体的には、特許文献１に記載の情報処理装置は、管理者に割り当てるロールと、一般的なユーザに割り当てるロールとがあり、ロールにしたがってログインしたユーザの機能制限を行うものである。

【先行技術文献】

【特許文献】

【０００４】

【特許文献１】特開２０１７－９１１０７号公報

【発明の概要】

【発明が解決しようとする課題】

【０００５】

例えば、製造ライン内の製造装置の各種パラメータを設定する作業は、機能リスクの高い作業となる。そのため、製造現場作業者向けの製造ライン作業用途のアプリケーションにおいては、十分な教育を受けてスキルを持った作業者だけがリスクの高い作業を行うことができるようにし、それ以外の作業者は、リスクの低い製造装置の動作状況をモニタリングするような作業のみを許すようにしたい場合がある。また、製造装置の保守サービス員向けの保守作業支援アプリケーションの場合、製造装置が設置されているラインやステーションごとに保守作業者を規定している場合もあり、担当範囲のラインやステーションに設置されている製造装置に対してのみアプリケーションを使って保守作業を行えるようにしたい。また、製造装置のメーカごとに保守作業ができる作業者が規定されている場合もあり、その場合には、製造装置の操作に関する安全教育や保守教育を受けている作業者のみが、そのメーカの製造装置の遠隔操作用アプリケーションを使用可能にする必要がある。

【０００６】

しかし、既存の技術では、上述したような作業者のスキルに基づいたきめの細かいスキルごとの制限を行うのは、難しかった。

本発明は、作業者又は使用者のスキルに合わせてアプリケーションで実行する機能をきめ細かく制限できるようにしたエッジサーバ及び管理サーバ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】

【０００７】

（１）本発明のエッジサーバ（例えば、後述の「エッジサーバ１００」）は、１台以上のエッジ機器（例えば、後述の「エッジ機器４００」）と通信可能に接続されており、前記エッジサーバで稼働する、前記エッジ機器の機能の使用及び／又は前記エッジ機器の処理データに対してアクセスするアプリケーションの実行を管理するアプリケーション実行管理手段（例えば、後述の「アプリ実行管理部１１１」）と、前記アプリケーションを記憶するアプリケーション記憶部（例えば、後述の「アプリ記憶部１２１」）と、予め設定された前記エッジ機器の機能の使用及び／又は前記エッジ機器の処理データに対するスキル情報別アクセスコントロールリスト（例えば、後述の「スキル別アクセスリスト」）を記憶するアクセスコントロール記憶部（例えば、後述の「アクセスコントロール記憶部１２３」）と、前記エッジサーバを含むシステムへのログインが承認されたユーザのスキル情報を取得するスキル情報取得手段（例えば、後述の「スキル情報取得部１１２」）と、前記ユーザが前記アプリケーションを介して前記エッジ機器の機能の使用及び／又は前記エッジ機器の処理データに対してアクセス要求する際に、前記ユーザのスキル情報と、前記アクセスコントロール記憶部に記憶された前記スキル情報別アクセスコントロールリス

トとに基づいて、前記ユーザの前記エッジ機器の機能の使用及び／又は前記エッジ機器の処理データに対するアクセス権限の有無を判断するアクセス権限判断手段（例えば、後述の「アクセス制御部１１３」）と、前記アクセス権限判断手段によって前記ユーザのアクセス権限が有ると判断された場合に限り、前記ユーザの前記アプリケーションを介した前記エッジ機器に係る機能の使用及び／又は前記エッジ機器の処理データへのアクセスを許可するアクセス制御手段（例えば、後述の「アクセス制御部１１３」）と、を備える。

【０００８】

（２）　（１）に記載のエッジサーバ（例えば、後述の「エッジサーバ１００」）において、前記スキル情報別アクセスコントロールリスト（例えば、後述の「スキル別アクセスリスト」）は、前記スキル情報ごとに前記エッジ機器（例えば、後述の「エッジ機器４００」）の種類及び／又は設置グループに対するアクセス可否情報を含むものであってもよい。

【０００９】

（３）　（１）又は（２）に記載のエッジサーバ（例えば、後述の「エッジサーバ１００」）において、前記スキル情報取得手段（例えば、後述の「スキル情報取得部１１２」）は、前記エッジサーバに対して通信可能に接続され、前記エッジサーバを含むシステムのユーザを管理する管理サーバ（例えば、後述の「管理サーバ３００」）から、前記ユーザのスキル情報を取得するものであってもよい。

【００１０】

（４）　（３）に記載のエッジサーバ（例えば、後述の「エッジサーバ１００」）において、前記エッジサーバを含むシステムのユーザを管理する前記管理サーバ（例えば、後述の「管理サーバ３００」）のエージェントである管理エージェント（例えば、後述の「管理エージェント１５０」）を備え、前記スキル情報取得手段（例えば、後述の「スキル情報取得部１１２」）は、前記管理エージェントから、前記ユーザのスキル情報を取得するものであってもよい。

【００１１】

（５）　（１）から（４）までのいずれかに記載のエッジサーバ（例えば、後述の「エッジサーバ１００」）において、前記スキル情報別アクセスコントロールリスト（例えば、後述の「スキル別アクセスリスト」）は、前記スキル情報ごとに、前記エッジ機器（例えば、後述の「エッジ機器４００」）の動作状態に係る各機能の使用可否情報及び／又は各処理データに対するアクセス可否情報、前記エッジ機器の生産状況に係る各機能の使用可否情報及び／又は各処理データに対するアクセス可否情報、前記エッジ機器の品質保守に係る各機能の使用可否情報及び／又は各処理データに対するアクセス可否情報、前記エッジ機器のイベント（履歴）に係る各機能の使用可否情報及び／又は各処理データに対するアクセス可否情報、及び前記エッジ機器のアーカイブに係る各機能の使用可否情報及び／又は各処理データに対するアクセス可否情報を含むものであってもよい。

【００１２】

（６）　（１）から（５）までのいずれかに記載のエッジサーバ（例えば、後述の「エッジサーバ１００」）において、前記スキル情報は、さらに、各ユーザの資格に関する情報、所属するグループに関する情報、作業可能なエッジ機器に関する情報、作業可能な作業内容に関する情報及びそれらの研修受講有無に関する情報の少なくともいずれかを含むものであってもよい。

【００１３】

（７）　（１）から（６）までのいずれかに記載のエッジサーバ（例えば、後述の「エッジサーバ１００」）において、前記アプリケーションは、前記エッジサーバを前記アクセス権限判断手段（例えば、後述の「アクセス制御部１１３」）及び／又は前記アクセス制御手段（例えば、後述の「アクセス制御部１１３」）として機能させるものであってもよい。

【００１４】

（８）　（１）から（７）までのいずれかに記載のエッジサーバ（例えば、後述の「エ

ッジサーバ１００」）において、前記アプリケーション記憶部（例えば、後述の「アプリ記憶部１２１」）は、前記アプリケーションと、前記アプリケーションの前記エッジ機器（例えば、後述の「エッジ機器４００」）の機能の使用及び／又は前記エッジ機器の処理データに対するアクセスの有無に係るセキュリティリスクリスト（例えば、後述の「アクセス申告リスト」）とを記憶し、前記アクセス制御手段（例えば、後述の「アクセス制御部１１３」）は、前記セキュリティリスクリストの内容に基づいて、前記アプリケーションのエッジ機器の機能の使用及び／又は前記エッジ機器の処理データへのアクセス要求を監視し、前記セキュリティリスクリストに開示された前記エッジ機器に係る機能の使用及び／又は前記エッジ機器の処理データへのアクセス要求のみを許可するものであってもよい。

【００１５】

（９）　（１）から（８）までのいずれかに記載のエッジサーバ（例えば、後述の「エッジサーバ１００」）に対して通信可能に接続された管理サーバ（例えば、後述の「管理サーバ３００」）は、各ユーザの前記スキル情報を記憶するスキル情報記憶部（例えば、後述の「スキル情報記憶部３２２」）と、ユーザのログイン情報を、前記エッジサーバを経由して受け付けるログイン受付手段（例えば、後述の「ログイン受付部３１１」）と、前記ログイン受付手段により受け付けた前記ログイン情報を使用して認証を行う認証手段（例えば、後述の「認証部３１２」）と、前記認証手段により認証がされた場合に、前記エッジサーバに対して前記ユーザに対応する前記スキル情報を、前記スキル情報記憶部から抽出して送信するスキル情報送信手段（例えば、後述の「スキル情報送信部３１３」）と、を備える。

【発明の効果】

【００１６】

本発明によれば、作業者又は使用者のスキルに合わせてアプリケーションで実行する機能をきめ細かく制限できるようにしたエッジサーバ及び管理サーバを提供することができる。

【図面の簡単な説明】

【００１７】

【図１】本実施形態におけるアプリセキュリティ管理システムの基本的構成を示す概略図である。

【図２】本実施形態におけるアプリセキュリティ管理システムの機能ブロック図である。

【図３】本実施形態におけるリストの項目例を示す図である。

【図４】本実施形態における処理データのデータモデルの例を示す図である。

【図５】本実施形態におけるアプリセキュリティ管理システムでのユーザ管理及びにスキル情報を取得する処理を説明するための図である。

【図６】本実施形態におけるエッジサーバでのアクセス制御処理を示すフローチャートである。

【図７】本実施形態におけるエッジサーバでのアクセス制御処理の一例を示す図である。

【図８Ａ】本実施形態におけるエッジサーバ１００での作業者別のアクセスに関する具体例を説明するための図である。

【図８Ｂ】本実施形態におけるエッジサーバ１００での作業者別のアクセスに関する具体例を説明するための図である。

【図９】本実施形態の変形例におけるエッジサーバでのアクセス制御処理の一例を示す図である。

【発明を実施するための形態】

【００１８】

（実施形態）

本実施形態に係るアプリケーションセキュリティ管理システム１０００（以下、簡単のため「アプリセキュリティ管理システム１０００」ともいう。）の構成について、図１を参照しながら概略を説明する。

図１は、本実施形態におけるアプリセキュリティ管理システム１０００の基本的構成を示す概略図である。

図１に示すように、アプリセキュリティ管理システム１０００は、エッジサーバ１００と、ユーザ端末２００（以下、簡単のため「端末２００」ともいう。）と、管理サーバ３００と、エッジ機器４００とを備えている。

【００１９】

エッジサーバ１００と、端末２００と、管理サーバ３００とは、ネットワークＮ１を介して接続されている。ネットワークＮ１は、例えば、インターネットや、ＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）、公衆電話網等である。ネットワークＮ１における具体的な通信方式や、有線接続及び無線接続のいずれであるか等については、特に限定されない。

エッジサーバ１００と、１台以上のエッジ機器４００とは、例えば、ユーザの工場施設等に設置され、ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）等のネットワークＮ２を介して通信可能に接続されている。ネットワークＮ２は、ネットワークスイッチ等を含んでもよい。

【００２０】

エッジ機器４００は、特に断らない限り、工場等の製造現場に設置された、ＣＮＣ工作機械、産業機器、産業用ロボット等を含む製造装置、及び画像センサ、ＰＬＣ（ｐｒｏｇｒａｍｍａｂｌｅ　ｌｏｇｉｃ　ｃｏｎｔｒｏｌｌｅｒ）等の製造装置に付帯する機器を指す。１台以上のエッジ機器４００は、例えば、工場のラインやセルを構成する。

【００２１】

エッジサーバ１００は、後述するアプリ記憶部１２１に記憶されたアプリケーションを実行させることにより、１台以上のエッジ機器４００から、エッジ機器４００に係る機能を実行し、及び／又は、エッジ機器４００の処理データにアクセスし、当該アプリケーションに係る所定の情報処理をするサーバである。ここで、エッジ機器４００の処理データとは、例えば当該エッジ機器４００に係る動作状態を示すデータ、生産状況を示すデータ、生産物の品質状況を示すデータ、稼働状況を示すデータ等を指す。

【００２２】

なお、エッジサーバ１００は、アプリケーションの実行中に、当該アプリケーションのエッジ機器４００に係る機能の使用及び／又はエッジ機器４００の処理データへのアクセス状況をセキュリティリスクリスト（以下、「アクセス申告リスト」ともいう。）に基づいて制御する。

具体的には、エッジサーバ１００は、予めアプリケーションをエッジサーバ１００上で実行する際に使用する、エッジ機器４００の機能の使用の有無及び／又はエッジ機器４００の処理データに対するアクセスの有無に係るアクセス申告リストが登録されており、アプリケーションは、アクセス申告リストでエッジ機器４００の機能の使用の有及び／又はエッジ機器４００の処理データに対するアクセス有と申告された範囲内で、所定の情報処理を行うように制御される。

【００２３】

さらに、エッジサーバ１００は、使用者（ユーザ）がアプリケーションを介して、エッジ機器４００に係る機能を実行し、及び／又は、エッジ機器４００の処理データにアクセスする場合に、使用者（ユーザ）に紐づけられたスキルに応じて、エッジ機器４００の機能の使用及び／又はエッジ機器４００の処理データに対するアクセスを制限するように制御する。

具体的には、使用者（ユーザ）のスキル別に、エッジ機器４００の機能の使用の有無及び／又はエッジ機器４００の処理データのアクセスの有無に係るスキル情報別アクセスコントロールリスト（以下、「スキル別アクセスリスト」ともいう。）が予め登録されており、エッジサーバ１００は、スキル別アクセスリストに基づいて、使用者（ユーザ）に関連付けられたスキルに許容される範囲内で、所定の情報処理を行うように制御される。

【００２４】

したがって、使用者（ユーザ）がエッジサーバ１００上のアプリケーションを介して、エッジ機器４００の機能を実行し、及び／又は、エッジ機器４００の処理データにアクセスする場合、エッジサーバ１００は、当該アプリケーションのアクセス申告リストの範囲内で、かつ使用者（ユーザ）のスキルに応じて、スキル別アクセスリストで許容される範囲内で、所定の情報処理を行うように制御される。

【００２５】

端末２００は、例えば、パーソナルコンピュータ（ＰＣ）である。端末２００は、エッジサーバ１００に通信可能に接続され、使用者（ユーザ）が使用する端末である。使用者（ユーザ）は、例えば、エッジサーバ１００及びエッジ機器４００を含む工場施設内で作業をする作業者や、作業者を管理する管理者、工場責任者等である。以降、使用者（ユーザ）を、単に「ユーザ」ともいう。ここで、ユーザが使用する端末２００は、工場施設内に有していても、工場施設外に有していてもよい。そして、ユーザは、端末２００を介して、エッジサーバ１００にアクセスし、アプリケーションの実行時には、アプリケーションが、ユーザのスキル情報に基づき、スキル別アクセスリストで許可されたエッジ機器４００に係る機能の使用及び／又はエッジ機器４００の処理データへのアクセスを行うことができる。

【００２６】

管理サーバ３００は、アプリセキュリティ管理システム１０００を使用するユーザを管理するためのサーバである。アプリセキュリティ管理システム１０００では、予め必要な条件（資格等）を満たし、アプリセキュリティ管理システム１０００に対してアクセスをするためのユーザＩＤ（ＩＤｅｎｔｉｆｉｃａｔｉｏｎ）の付与されたユーザのみが使用可能である。管理サーバ３００は、各ユーザのログイン情報（例えば、ユーザＩＤ及びパスワード等）と、ユーザごとのスキル情報とを記憶する。

【００２７】

こうすることで、管理サーバ３００は、このアプリセキュリティ管理システム１０００に属するエッジサーバ１００へのアプリケーションの使用者によるサインオン（以下、「ログイン」ともいう。）や、エッジサーバ１００で実行するアプリケーションへの使用者によるログインを管理し、シングルサインオンを実現する。

【００２８】

次に、アプリセキュリティ管理システム１０００の各装置の機能について説明する。

図２は、本実施形態におけるアプリセキュリティ管理システム１０００の機能ブロック図である。

＜エッジサーバ１００＞

エッジサーバ１００は、制御部１１０と、記憶部１２０と、通信部１３０とを備える。

制御部１１０は、例えば、ＣＰＵであり、記憶部１２０に記憶された各種プログラムを実行することにより、エッジサーバ１００を統括制御する。

例えば、ＣＰＵは、ユーザの端末２００から、アプリケーションの実行を受け付けアプリケーションの実行を管理する処理（以下、「アプリ実行管理処理」という。）のためのプログラムを実行する。また、ＣＰＵは、ユーザのスキル情報を取得する処理（以下、「スキル情報取得処理」という。）のためのプログラムを実行する。また、ＣＰＵは、実行中のアプリケーションのアクセス有無を判断し、アクセスを制御する処理（以下、「アクセス制御処理」という。）のためのプログラムを実行する。

このように、アプリ実行管理処理、スキル情報取得処理、及びアクセス制御処理のためのプログラムを実行することにより、ＣＰＵには、機能的構成として、アプリ実行管理部１１１と、スキル情報取得部１１２と、アクセス制御部１１３と、が形成される。

【００２９】

制御部１１０の各機能部の説明の前に、まず、記憶部１２０について説明する。

記憶部１２０は、制御部１１０により実行されるプログラムの他、アプリ記憶部１２１と、スキル情報記憶部１２２と、アクセスコントロール記憶部１２３とを備える。

アプリ記憶部１２１は、エッジサーバ１００上で実行されるアプリケーションを記憶す

る記憶領域である。アプリケーションは、例えば、アプリ開発者が開発したアプリケーションであって、図示しない販売管理サイト等から購入して、エッジサーバ１００にダウンロードされたものである。

スキル情報記憶部１２２は、エッジサーバ１００上で実行されるアプリケーションを使用するユーザのスキル情報を記憶する一時記憶領域である。当該ユーザのスキル情報は、例えば、当該ユーザがエッジサーバ１００にログインした際や、ログインした後にアプリケーションを実行する際に、管理サーバ３００等から取得して当該ユーザがログアウトするまで（一時的に）記憶される。

【００３０】

スキル情報としては、例えば、ユーザの資格に関する情報、ユーザの所属するグループに関する情報、ユーザの作業可能なエッジ機器４００に関する情報、ユーザの作業可能な作業内容に関する情報及びユーザのエッジ機器４００に係る技術等の研修受講有無に関する情報等がある。

ユーザの資格に関する情報は、例えば、エッジ機器４００の種類に応じて、エッジ機器４００を扱うために必要な資格の情報や、製造システムの管理者、一般作業者、システムインテグレータ、保守作業者、特権管理者といった作業者の役割（ロール）や作業権利を表す情報である。

ユーザの所属するグループに関する情報は、例えば、第一加工課、溶接品質課といった作業者が所属する部署の情報や、ラインＬ１保全、ラインＬ２保全、ラインＬ３保全といった、エッジ機器４００が設置されている工場のラインやステーションといった場所に関する情報である。

ユーザの作業可能なエッジ機器４００に関する情報は、例えば、ユーザの扱えるエッジ機器４００を限定する情報である。これは、ユーザが扱えるエッジ機器４００の種類であってもよいし、ユーザが扱えるエッジ機器のメーカであってもよい。また、ユーザが扱えるエッジ機器４００のハードウェアのバージョンであってもよい。

ユーザの作業可能な作業内容に関する情報は、例えば、エッジ機器４００の各種設定作業、立上げ、廃棄といった詳細な各作業に対するユーザの作業可能か否かを示す情報である。

ユーザのエッジ機器４００に係る技術等の研修受講有無に関する情報は、例えば、ユーザのエッジ機器４００の取扱に関する教育の受講有無の情報であり、例えば、ＣＮＣ工作機械の保全に関する教育の受講有無や、産業用ロボットのティーチングに関する教育に受講有無等である。

ユーザのスキル情報は、上述した情報を、コンピュータが解釈可能なようにコード化したものである。

【００３１】

アクセスコントロール記憶部１２３は、アクセス申告リスト及びスキル別アクセスリストを記憶する記憶領域である。

上述したとおり、アプリケーションごとに登録されるアクセス申告リストは、当該アプリケーションがエッジサーバ１００上で実行される際に当該アプリケーションの使用する、エッジ機器４００の機能の使用の有無及び／又はエッジ機器４００の処理データに対するアクセスの有無を登録したリストである。

これに対して、スキル別アクセスリストは、スキルごとに、エッジサーバ１００と接続可能とされたエッジ機器４００の機能の使用の有無及び／又はエッジ機器４００の処理データのアクセスの有無を登録したリストである。

【００３２】

図３にアクセス申告リスト、及びスキル別アクセスリストの一例を示す。図３に示す「製造装置」とは、エッジ機器４００に該当するものであり、実際には、ＣＮＣ工作機械、産業機器、産業用ロボット等が指定されている。また、リスト項目のうち、アクセス可のものには、例えば、チェックボックスにチェック（レ点）が入っている。

なお、アクセス申告リストは、アプリケーションごとに登録されるのに対して、スキル

別アクセスリストは、分類されるスキルごとに登録されるものとなる。
図３に示すリスト項目６２０は、アクセス申告リストと、スキル別アクセスリストとの両方に共通の項目の一例を示すものである。スキル別アクセスリストは、スキル情報ごとにリスト項目６２０に示す内容のリストを有する。また、アクセス申告リストは、アプリケーションごとにリスト項目６２０に示す内容のリストを有する。なお、スキル別アクセスリストと、アクセス申告リストとは、共に、図３に示す内容が、コンピュータが解釈可能なようにコード化されている。

【００３３】
より具体的には、エッジ機器４００の処理データとして、例えば、エッジ機器４００に係る動作状態を示すデータ、生産状況を示すデータ、生産物の品質状況を示すデータ、稼働状況等のイベント（履歴）を示すデータ等がある。これらの処理データは、予めデータモデル化（すなわち、標準化）されており、このように標準化されたデータモデルに基づいてアクセスの有無が設定される。このような仕組みによって、エッジ機器４００に係る処理データへのアクセスをするための標準化されたインタフェースを提供することができる。

【００３４】
図４に、ＣＮＣ工作機械の場合における処理データのデータモデル６３０の例を示す。データモデル６３０に示すように、処理データは、動作状態の情報、生産状況の情報、品質保守の情報、各種イベント（履歴）の情報、アーカイブの各カテゴリに分けられる。そして、各カテゴリにおいて、コモンデータと、各部位データとがある。コモンデータは、ＣＮＣ工作機械に共通のデータであり、各部位データは、ＣＮＣ工作機械のうち、軸や、モータといったＣＮＣ工作機械を構成する各部品に関するデータである。
なお、図示しないが、エッジ機器４００の機能に関しても、処理データと同様に、動作状態に関する機能、生産状況に関する機能、品質保守に関する機能、各種イベント（履歴）に関する機能、アーカイブに関する機能があり、データモデルと同様にエッジ機器４００の提供する機能のモデル化を行うことができる。そうすることで、エッジ機器４００の提供する機能を使用するための標準化されたインタフェースを提供することができる。

【００３５】
次に、制御部１１０の備える各機能部について説明する。
アプリ実行管理部１１１は、アプリケーションの起動要求に基づいて、アプリ記憶部１２１に記憶されたアプリケーションを実行する。また、アプリ実行管理部１１１は、アプリケーションの実行を管理する。
スキル情報取得部１１２は、ユーザがエッジサーバ１００にログインした際や、ログインした後にアプリケーションを実行する際に、当該ユーザのスキル情報を管理サーバ３００等から取得して、当該ユーザがログアウトするまで（一時的に）スキル情報記憶部１２２に記憶する。

【００３６】
アクセス制御部１１３は、ユーザがエッジサーバ１００上で実行されるアプリケーションを介してエッジ機器４００の機能の使用及び／又はエッジ機器４００の処理データに対するアクセスを要求する際に、当該ユーザのスキル情報と、アクセスコントロール記憶部１２３に記憶されたスキル別アクセスリストとに基づいて、ユーザのエッジ機器４００の機能の使用及び／又はエッジ機器４００の処理データに対するアクセス権限の有無を判断する。
そして、アクセス制御部１１３は、当該ユーザがアクセス権限を有すると判断されたエッジ機器４００の機能の使用及び／又はエッジ機器４００の処理データに対するアプリケーションによるアクセスを許可する。

【００３７】
なお、アクセス制御部１１３は、上述したとおり、当該アプリケーションをエッジサーバ１００上で実行する際に使用する、エッジ機器４００の機能の使用の有無及び／又はエッジ機器４００の処理データに対するアクセスの有無に係るアクセス申告リストに示され

たエッジ機器４００に係る機能の使用及び／又はエッジ機器４００の処理データへのアクセスのみを許可する。したがって、当該ユーザのスキル情報に対応して、スキル別アクセスリストにおいて許可されるエッジ機器４００に係る機能の使用及び／又はエッジ機器４００の処理データへのアクセスであっても、当該アプリケーションのアクセス申告リストで許可されていない場合、アクセス制御部１１３は、当該エッジ機器４００に係る機能の使用及び／又は当該エッジ機器４００の処理データへのアクセスを許可しない。

【００３８】

このように、アクセス制御部１１３は、アプリ実行管理部１１１が実行したアプリケーションに対応付けられたアクセス申告リストの内容、及びユーザのスキルに対応するスキル別アクセスリストに基づいて、アプリケーションのエッジ機器４００の機能の使用及び／又はエッジ機器４００の処理データへのアクセスを制御する。具体的には、アクセス制御部１１３は、当該ユーザに対して、アクセス申告リストに示されたエッジ機器４００に係る機能の使用及び／又はエッジ機器４００の処理データへのアクセスであって、当該ユーザのスキル情報に対応するスキル別アクセスリストに示されたエッジ機器４００に係る機能の使用及び／又はエッジ機器４００の処理データへのアクセスのみを許可するように制御する。

【００３９】

なお、アクセス制御部１１３は、当該ユーザがアクセス権限を有さないと判断したエッジ機器４００の機能の使用及び／又はエッジ機器４００の処理データに対するアプリケーションによるアクセス要求を検出した場合には、警告メッセージを表示して、当該ユーザのアプリケーションの使用を停止させてもよい。

【００４０】

なお、図２には記載していないが、エッジサーバ１００は、管理サーバ３００のエージェントである管理エージェントを備えることが好ましい。管理エージェントは、エッジサーバ１００にインストールされ、管理サーバ３００とのインタフェースを、例えば、端末２００やエッジサーバ１００内の機能部に提供する。なお、エージェントの機能については、当業者にとって公知であり、詳細な説明は省略する。

【００４１】

通信部１３０は、ネットワークＮ１を介して外部機器（例えば、管理サーバ３００等）とデータの送受信を行い、ネットワークＮ２を介して外部機器（例えば、エッジ機器４００）とデータの送受信を行う通信制御デバイスである。

【００４２】

＜管理サーバ３００＞

管理サーバ３００は、制御部３１０と、記憶部３２０と、通信部３３０とを備える。

制御部３１０は、例えば、ＣＰＵであり、記憶部３２０に記憶された各種プログラムを実行することにより、管理サーバ３００を統括制御する。

例えば、ＣＰＵは、ユーザの端末２００から、ログイン情報を受け付ける処理（以下、「ログイン受付処理」という。）のためのプログラムを実行する。また、ＣＰＵは、ログイン情報に基づきユーザを認証する処理（以下、「認証処理」という。）のためのプログラムを実行する。また、ＣＰＵは、認証がされた場合に、ユーザのスキル情報を送信する処理（以下、「スキル情報送信処理」という。）のためのプログラムを実行する。

このように、ログイン受付処理、認証処理、及びスキル情報送信処理のためのプログラムを実行することにより、ＣＰＵには、機能的構成として、ログイン受付部３１１と、認証部３１２と、スキル情報送信部３１３と、が形成される。

【００４３】

制御部３１０の各機能部の説明の前に、まず、記憶部３２０について説明する。

記憶部３２０は、制御部３１０により実行されるプログラムの他、ユーザ情報記憶部３２１と、スキル情報記憶部３２２とを備える。

ユーザ情報記憶部３２１は、アプリセキュリティ管理システム１０００を使用可能なユーザのログイン情報や、所属情報等を記憶する記憶領域である。ユーザのログイン情報は

、例えば、ユーザ名、ログインＩＤ、パスワード等である。ユーザの所属情報は、例えば、ユーザの配属されている部署名や、所在地等である。ユーザ情報記憶部３２１に記憶されるユーザのデータは、アプリセキュリティ管理システム１０００のユーザの使用開始前に、例えば、工場責任者等によって登録される。

スキル情報記憶部３２２は、ユーザごとにスキル情報を記憶する記憶領域である。

【００４４】

次に、制御部３１０の備える各機能部について説明する。

ログイン受付部３１１は、ユーザから端末２００を介してエッジサーバ１００に対するアクセスがあり、当該ユーザが認証済ではない場合に、例えば、エッジサーバ１００にインストールされている管理エージェント１５０を介して当該ユーザからのログイン情報を受け付ける。

認証部３１２は、ログイン受付部３１１が受け付けたユーザのログイン情報に基づいて、ユーザ情報記憶部３２１を参照し、当該ユーザの認証を行う。

スキル情報送信部３１３は、認証部３１２により当該ユーザの認証がされた場合に、当該ユーザのスキル情報をスキル情報記憶部３２２から抽出して、エッジサーバ１００に対して送信する。

なお、ログインしたユーザを管理する管理エージェント１５０が、エッジサーバ１００にインストールされている場合には、スキル情報送信部３１３は、エッジサーバ１００の管理エージェント１５０からスキル情報の送信要求を受け付けたときにも、ユーザのスキル情報を、エッジサーバ１００に対して送信する。

通信部３３０は、ネットワークＮ１を介して外部機器（例えば、端末２００、エッジサーバ１００等）とデータの送受信を行う通信制御デバイスである。

【００４５】

ここで、ユーザ管理及びスキル情報を取得する処理について、図５を参照しながら説明する。なお、エッジサーバ１００には、管理サーバ３００のエージェントである管理エージェント１５０がインストールされているものとする。

図５は、本実施形態におけるアプリセキュリティ管理システム１０００でのユーザ管理及びにスキル情報を取得する処理を説明するための図である。

前提として、工場責任者等の責任者は、管理サーバ３００にアクセスし、データを更新する権限を予め有する。

【００４６】

まず、ステップＳ（以降、単に「Ｓ」という。）１０において、工場責任者等は、端末２００から管理サーバ３００に対して、アプリセキュリティ管理システム１０００の使用を許可するユーザを登録する。工場責任者は、例えば、工場責任者が属する工場の作業者のユーザ名や所属等のグループ情報、及びユーザのスキル情報等を、決められたフォームにしたがって登録する。

Ｓ１１において、管理サーバ３００の制御部３１０は、受け付けた情報に基づいて、当該ユーザのユーザ名や所属等のグループ情報を、ユーザ情報記憶部３２１に記憶させる。

なお、管理サーバ３００は、例えば、工場責任者等から入力された、及び／又は、他のスキル管理サーバ（図示せず）から取得された当該ユーザのスキル情報を、スキル情報記憶部３２２に記憶させる。

以上により、当該ユーザは、アプリセキュリティ管理システム１０００にログインすることが可能となる。

【００４７】

次に、管理サーバ３００のユーザ情報記憶部３２１にログイン情報等が登録されている作業者Ａは、Ｓ２０において、端末２００を使用してエッジサーバ１００にログインする。その際、最初の一度は、ログイン情報とパスワードとを入力してログインするが、その後に、アプリセキュリティ管理システム１０００の他のエッジサーバ１００等にアクセスする際は、管理エージェント１５０にログイン情報が引き継がれるため、ログイン不要である。

【００４８】
ログイン情報を受け付けた管理サーバ３００は、Ｓ２１において、作業者Ａを認証し、承認した場合には、作業者Ａのスキル情報を、エッジサーバ１００に送信する。エッジサーバ１００は、作業者Ａのスキル情報を、管理エージェント１５０が管理することで、作業者Ａが、アプリセキュリティ管理システム１０００の他のエッジサーバ１００にアクセスする際には、管理エージェント１５０が、他のエッジサーバ１００に、スキル情報を送信するようにしてもよい。また、作業者Ａのスキル情報を、管理エージェント１５０が管理しない場合には、作業者Ａが、アプリセキュリティ管理システム１０００の他のエッジサーバ１００にアクセスする際には、管理サーバ３００が、他のエッジサーバ１００に、スキル情報を送信するようにしてもよい。
【００４９】
このようなユーザ管理の仕組みによって、アプリセキュリティ管理システム１０００を使用する際には、最初にログインをすれば、何度も再度ログインをする必要はなく、ログイン情報が他のエッジサーバ１００や、アプリケーションに引き継がれるので、煩わしい操作をユーザにさせずに済み、ユーザの負担を減らすことができる。
また、管理サーバ３００に記憶されているユーザのスキル情報を、必要とするエッジサーバ１００に送信することができる。
【００５０】
そして、ユーザがアプリケーションを実行する際に、ユーザのスキル情報に基づいて、スキル別アクセスリストで当該スキルに対して許可されているエッジ機器４００の機能の使用及び／又はエッジ機器４００の処理データに対するアクセスをすることが可能になる。
このように、ユーザによるエッジ機器４００に係る機能の使用及び／又はエッジ機器４００の処理データへのアクセスの制限を行うことができる。
【００５１】
以上、エッジサーバ１００及び管理サーバ３００に含まれる機能ブロックについて説明した。
なお、上記のアプリセキュリティ管理システム１０００に含まれる各装置のそれぞれは、ハードウェア、ソフトウェア又はこれらの組み合わせにより実現することができる。ここで、ソフトウェアによって実現されるとは、コンピュータがプログラム（アプリケーション）を読み込んで実行することにより実現されることを意味する。
具体例として、エッジサーバ１００及び管理サーバ３００は、一般的なサーバに、本実施形態を実現するためのプログラム（アプリケーション）を組み込むことにより実現できる。
【００５２】
次に、エッジサーバ１００でのスキル別アクセスリストを用いたアプリケーションの制御に係る処理フローについて、図６及び図７を参照しながら説明する。
図６は、本実施形態におけるエッジサーバ１００でのアクセス制御処理を示すフローチャートである。なお、図６の処理フローにおいて、アクセス要求が、アクセス申告リストに示されたエッジ機器４００に係る機能の使用及び／又はエッジ機器４００の処理データへのアクセスか否かを判断するステップについては省略している。
【００５３】
図６のＳ４０において、例えば、ユーザによるアプリケーションの起動要求を受け付けたことに応じて、エッジサーバ１００のアプリ実行管理部１１１は、アプリ記憶部１２１に記憶されたアプリケーションを起動させる。
Ｓ４１において、スキル情報取得部１１２は、アプリケーションを起動したユーザのスキル情報を、管理サーバ３００等から取得して、当該ユーザがログアウトするまで（一時的に）スキル情報記憶部１２２に記憶する。
Ｓ４２において、アクセス制御部１１３は、読み込んだ当該ユーザのスキル情報に対応したスキル別アクセスリストを、アクセスコントロール記憶部１２３から読み込む。

【００５４】
Ｓ４３において、アクセス制御部１１３は、アプリケーションからエッジ機器４００の機能の使用及び／又はエッジ機器４００処理データへのアクセス要求を受け付けたか否かを判断する。要求を受け付けた場合（Ｓ４３：ＹＥＳ）には、アクセス制御部１１３は、処理をＳ４４に移す。要求を受け付けていない場合（Ｓ４３：ＮＯ）には、アクセス制御部１１３は、処理をＳ４６に移す。
【００５５】
Ｓ４４において、アクセス制御部１１３は、要求に対応するエッジ機器４００の機能の使用及び／又はエッジ機器４００処理データへのアクセスが許可されているか否かを、スキル別アクセスリストに基づいて判断する。アクセスが許可されている場合（Ｓ４４：ＹＥＳ）には、アクセス制御部１１３は、処理をＳ４５に移す。他方、アクセスが許可されていない場合（Ｓ４４：ＮＯ）には、アクセス制御部１１３は、処理をＳ４６に移す。つまり、当該スキルに対してアクセスが許可されていない場合には、アクセス制御部１１３は、例えば、端末２００に警告メッセージを出力し、当該ユーザから要求されたエッジ機器４００の機能の実行及び／又はエッジ機器４００処理データに対するしてアクセスを行わない。
Ｓ４５において、アクセス制御部１１３は、当該ユーザから要求されたエッジ機器４００の機能を実行し、及び／又はエッジ機器４００処理データに対してアクセスする処理を行う。
【００５６】
Ｓ４６において、制御部１１０は、アプリケーションの終了を受け付けたか否かを判断する。制御部１１０は、例えば、ユーザによるアプリケーションの終了操作を受け付けた場合の他、エッジサーバ１００の電源切断操作を受け付けた場合や、アプリケーションの強制終了操作を受け付けた場合等に、アプリケーションの終了を受け付けたと判断する。アプリケーションの終了を受け付けた場合（Ｓ４６：ＹＥＳ）には、制御部１１０は、処理をＳ４７に移し、アプリケーションを終了させる。他方、アプリケーションの終了を受け付けていない場合（Ｓ４６：ＮＯ）には、アクセス制御部１１３は、処理をＳ４３に移す。
【００５７】
図７は、本実施形態におけるエッジサーバ１００でのアクセス制御処理の一例を示す図である。
図７に示す例では、アプリケーション５１０を制御するコントローラ５５０に、当該ユーザのスキル情報５２０と、スキル情報５２０に対応したスキル別アクセスリスト５３０とが読み込まれる。
図７に示すように、エッジサーバ１００は、アクセス対象５６０として、データａ，ｂと、機能Ｑ，Ｒとを有する。ここで、機能Ｑ及びデータａについてはアクセスが許可され、機能Ｒ及びデータｂについてはアクセスが不許可とする。
そうすると、図７に示すように、アプリケーション５１０から受け付けた要求がデータａに対するアクセス要求であれば、アクセス制御部１１３は、ユーザのスキル情報５２０に対応したスキル別アクセスリスト５３０を参照し、アクセスが許可されていることから、アクセス制御部１１３は、アプリケーション５１０によりデータａにアクセスする処理を行う。
また、アプリケーション５１０から受け付けた要求が、機能Ｒに対するアクセス要求であれば、アクセス制御部１１３は、ユーザのスキル情報５２０に対応したスキル別アクセスリスト５３０を参照し、アクセスが許可されていないことから、アプリケーション５１０により機能Ｒを実行しない。
このように、作業者のスキル情報に応じて、任意のアプリケーションに係るアクセス制御が行われる。
【００５８】
次に、作業者のスキル情報に応じたアプリケーションのアクセスに関する具体例を説明

する。
図８Ａ及び図８Ｂは、本実施形態におけるエッジサーバ１００での作業者別のアクセスに関する具体例を説明するための図である。
図８Ａは、ラインＬ１の一般作業者である作業者Ａがアプリケーションを実行する場合の例を示す。
前提として、エッジサーバ１００は、アプリケーションＸと、アプリケーションＹとを記憶しており、実行可能である。アプリケーションＸは、ラインＬ１のデータａ及びデータｂを使用する機能Ｑ及び機能Ｒを実行する。また、アプリケーションＹは、ラインＬ２のデータｃ～データｅを使用する機能Ｓ及び機能Ｔを実行する。
作業者Ａは、ラインＬ１の担当であるので、作業者Ａのスキル情報は、少なくともラインＬ１に対する情報を有する。また、作業者Ａのスキル情報に基づけば、スキル別アクセスリストによって、例えば、一般作業者が行うことができる機能Ｑの実行のみを許可する。よって、作業者Ａがアプリケーション Ｘを実行した場合、機能Ｑのみを行うことができる。また、作業者Ａがアプリケーション Ｙを実行しても、全ての機能について許可されていないため、何の処理も行われない。
【００５９】
他方、図８Ｂは、ラインＬ１及びラインＬ２の保守作業者である作業者Ｂがアプリケーションを実行する場合の例を示す。
作業者Ｂは、ラインＬ１及びラインＬ２の担当であるので、作業者Ａのスキル情報は、少なくともラインＬ１及びラインＬ２に対する情報を有する。また、作業者Ｂのスキル情報に基づけば、スキル別アクセスリストによって、例えば、保守作業で使用可能な機能Ｒ及び機能Ｓの実行を許可する。しかし、保守作業では使用しない機能Ｑ及び機能Ｔの実行は、許可しない。また、保守作業で使用可能な機能Ｓのうち、作業者Ｂのスキル情報に基づけば、スキル別アクセスリストによって、例えば、作業者Ｂが保守作業を行うことができるエッジ機器ｃの処理データに対するアクセスは許可するが、作業者Ｂが保守作業を行うことができないエッジ機器ｄの処理データに対するアクセスは許可しない。
【００６０】
［変形例］
上述した例では、アプリケーションに対するユーザからのアクセス要求が、アクセス申告リストに示されたエッジ機器４００に係る機能の使用及び／又はエッジ機器４００の処理データへのアクセスか否かを判断することを省略し、スキル情報と、スキル別アクセスリストとを使用したアプリケーションのアクセス制御に関するものであった。
ここでは、アプリケーションに対するユーザからのアクセス要求が、アクセス申告リストに示されたエッジ機器４００に係る機能の使用及び／又はエッジ機器４００の処理データへのアクセスか否かを判断する場合について簡単に説明する。
【００６１】
この場合、図６に示した処理フローにおいて、Ｓ４３とＳ４４の間に、ユーザからのアクセス要求が、アクセス申告リストに示されたエッジ機器４００に係る機能の使用及び／又はエッジ機器４００の処理データへのアクセスか否かを判断するステップを挿入すればよい。そうすることで、アクセス制御部１１３は、当該ユーザからのアプリケーションを介する、エッジ機器４００に係る機能の使用及び／又はエッジ機器４００の処理データへのアクセス要求に対して、当該アプリケーションのアクセス申告リストに示されたエッジ機器４００に係る機能の使用及び／又はエッジ機器４００の処理データへのアクセス要求であって、かつ当該ユーザのスキル情報に対応するスキル別アクセスリストに示されたエッジ機器４００に係る機能の使用及び／又はエッジ機器４００の処理データへのアクセス要求のみを許可するように制御することができる。
【００６２】
図９は、エッジサーバ１００でのアクセス制御処理の一例を示す図である。
これは、図７で説明したものに、さらに、アプリケーションに対応するアクセス申告リスト５４０で登録されたアクセス有無が追加されたものである。

図９を参照すると、アクセス申告リスト５４０が、機能Ｒの使用を許可しないものである場合、図７と比較して、機能Ｒのアクセスを許可しないものになっている。

【００６３】

以上により、アプリセキュリティ管理システム１０００は、ユーザのスキル情報と、スキル別アクセスリストとに基づいて、実行するアプリケーションのエッジ機器４００の機能及び／又はエッジ機器４００の処理データに対するアクセスを監視するので、ユーザのスキルにあったアクセスのみを許容する仕組みにでき、セキュリティ性をより向上できる。

また、スキル情報は、様々なスキルに関する情報を有するので、アプリケーションの実行に際し、ユーザのスキルにあったきめ細かい機能の制限を行うことができる。

【００６４】

本発明で使用するアプリケーションを初めとするプログラムは、様々なタイプの非一時的なコンピュータ可読媒体（ｎｏｎ－ｔｒａｎｓｉｔｏｒｙ　ｃｏｍｐｕｔｅｒ　ｒｅａｄａｂｌｅ　ｍｅｄｉｕｍ）を用いて格納され、コンピュータに供給することができる。非一時的なコンピュータ可読媒体は、様々なタイプの実体のある記録媒体（ｔａｎｇｉｂｌｅ　ｓｔｏｒａｇｅ　ｍｅｄｉｕｍ）を含む。非一時的なコンピュータ可読媒体の例は、磁気記録媒体（例えば、フレキシブルディスク、磁気テープ、ハードディスクドライブ）、光磁気記録媒体（例えば、光磁気ディスク）、ＣＤ－ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）、ＣＤ－Ｒ、ＣＤ－Ｒ／Ｗ、半導体メモリ（例えば、マスクＲＯＭ、ＰＲＯＭ（Ｐｒｏｇｒａｍｍａｂｌｅ　ＲＯＭ）、ＥＰＲＯＭ（Ｅｒａｓａｂｌｅ　ＰＲＯＭ）、フラッシュＲＯＭ、ＲＡＭ（ｒａｎｄｏｍ　ａｃｃｅｓｓ　ｍｅｍｏｒｙ））を含む。また、プログラムは、様々なタイプの一時的なコンピュータ可読媒体（ｔｒａｎｓｉｔｏｒｙ　ｃｏｍｐｕｔｅｒ　ｒｅａｄａｂｌｅ　ｍｅｄｉｕｍ）によってコンピュータに供給されてもよい。一時的なコンピュータ可読媒体の例は、電気信号、光信号、及び電磁波を含む。一時的なコンピュータ可読媒体は、電線及び光ファイバ等の有線通信路、又は無線通信路を介して、プログラムをコンピュータに供給できる。

【００６５】

また、上述した実施形態は、本発明の好適な実施形態ではあるが、上記実施形態のみに本発明の範囲を限定するものではなく、本発明の要旨を逸脱しない範囲において種々の変更を施した形態での実施が可能である。

【００６６】

（変形例１）

上述した実施形態では、スキル別アクセスリスト及びアクセス申告リストのリスト項目の例として、図３に一例を示したが、これに限定されない。また、データモデルの例として、図４に一例を示したが、これに限定されない。ＣＮＣ工作機械を除く各種の製造装置に関しても、図４と同様のデータモデルを適用してもよい。

【００６７】

（変形例２）

上述した実施形態でのスキル情報と、スキル別アクセスリストとに基づく、ユーザごとのエッジ機器４００の機能の使用及び／又はエッジ機器４００の処理データに対するアクセス制御について、例を示して説明したが、これに限定されない。エッジ機器４００の機能の使用やエッジ機器４００の処理データは、上述したリスト項目やデータモデルで示したように、さらに細分化しているものが好ましい。また、スキル情報に、時刻情報をさらに組み合わせてアクセス制御をしてもよい。例えば、保守作業者であっても、アクセスする日時が保守作業日以外であれば、エッジ機器４００の機能の使用及び／又はエッジ機器４００の処理データに対してアクセスができないようにする。この処理は、管理サーバ３００から取得するスキル情報を、ログインした日時によって、異なるものにすることで、行うことができる。

【００６８】

（変形例３）

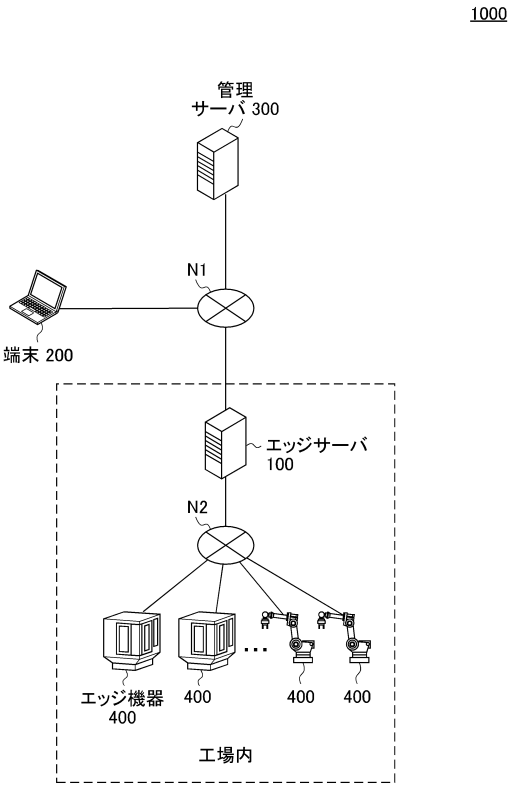
上述した実施形態では、エッジサーバ１００でのアクセス制御を、コントローラ５５０が行うものを例に説明したが、これに限定されない。スキル別アクセスリストやアクセス申告リストを、アプリケーションのプログラム構成として、スキル別アクセスリストやアクセス申告リストに基づいて、エッジ機器４００の機能の使用要求及び／又はエッジ機器４００の処理データに対するアクセス要求を行うように、プログラム化されるようにしてもよい。ただし、その場合においても、アクセス制御部１１３によるダブルチェックを行うことが好ましい。

【符号の説明】

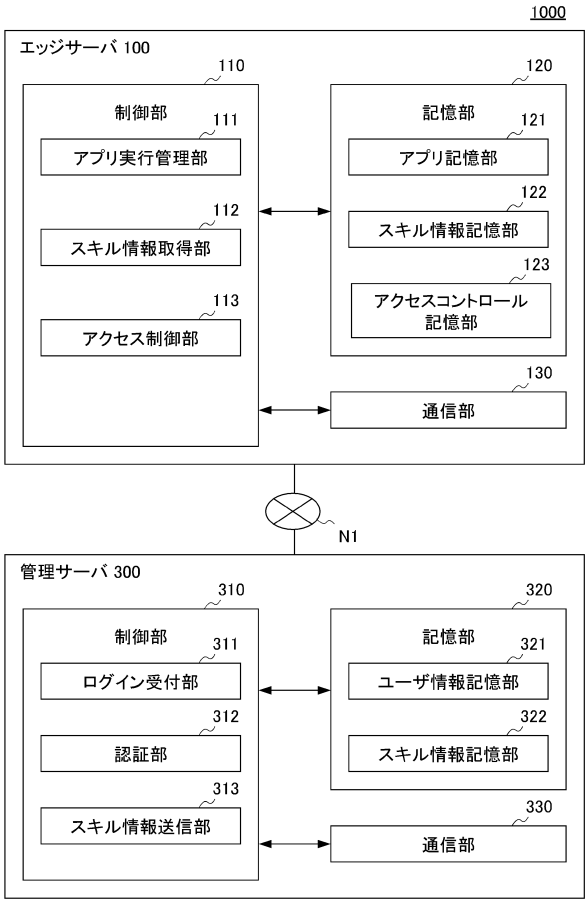
【００６９】

１００　エッジサーバ
１１０，３１０　制御部
１１１　アプリ実行管理部
１１２　スキル情報取得部
１１３　アクセス制御部
１２０，３２０　記憶部
１２１　アプリ記憶部
１２２　スキル情報記憶部
１２３　アクセスコントロール記憶部
２００　端末
３００　管理サーバ
３１１　ログイン受付部
３１２　認証部
３１３　スキル情報送信部
３２１　ユーザ情報記憶部
３２２　スキル情報記憶部
４００　エッジ機器
１０００　アプリセキュリティ管理システム

【図１】



【図２】



【図３】

620

リスト項目	
□現在の製造装置の状態が表示できる	処理データ
□現在の製造装置の状態を保存できる	
□製造履歴が表示できる	
□製造履歴が保存できる	
□製造品質情報が表示できる	
□製造品質情報が保存できる	
・・・	
□製造稼働・停止が指示できる	機能
□製造プログラムを表示できる	
□製造プログラムを変更できる	
□製造プログラムを保存できる	
□製造装置の設定を表示できる	
□製造装置の設定を変更できる	
□製造装置の設定を保存できる	
□製造装置をリモートで操作できる	
□製造装置をリモートで保守できる	
□インターネットにデータをアップロードできる	
□インターネットからデータをダウンロードできる	
□通信データを記録できる	
□通信データを中継できる	
・・・	

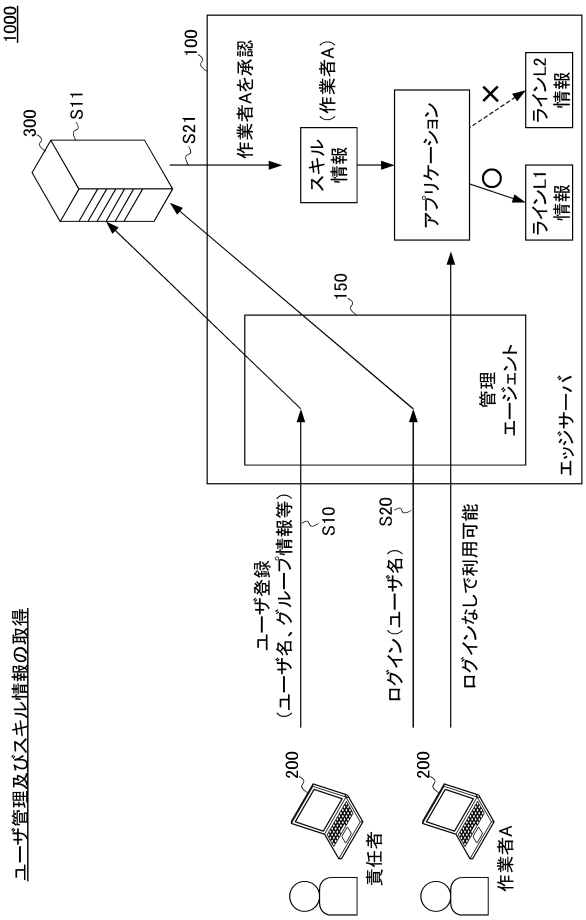
【図４】

630

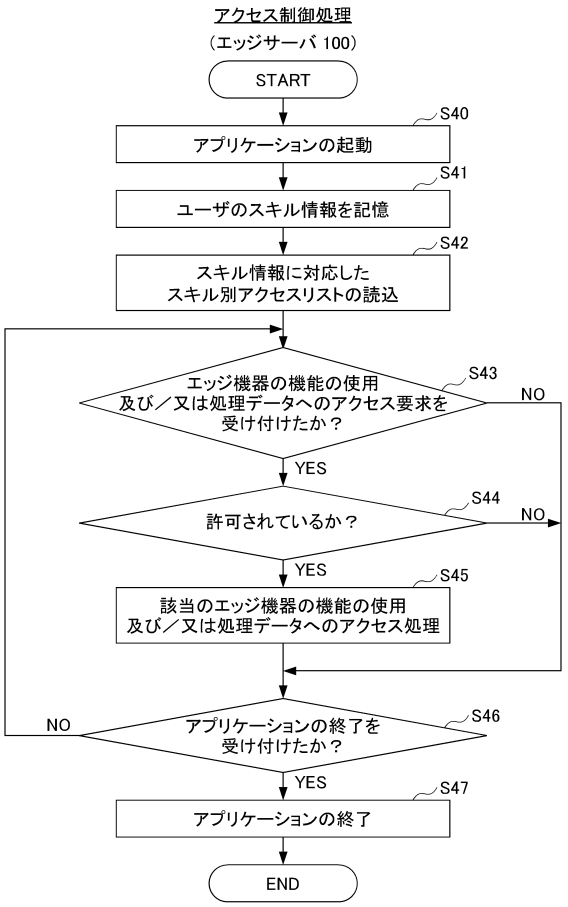
CNCデータモデル

カテゴリ	コモンデータ	各部位データ
動作状態の情報	動作状態 動作状態CNC	動作状態CNC系統 動作状態CNC軸 動作状態CNCモータ 動作状態センサ ・・・
生産状況の情報	生産状況	—
品質保守の情報	品質保守情報 品質保守情報CNC	品質保守情報CNC系統 品質保守情報CNC軸 品質保守情報CNCモータ 品質保守＿検査結果 ・・・
各種イベントの情報	操作履歴 プログラム変更履歴 アラーム履歴 保守通知イベント 故障予知イベント ・・・	—
アーカイブ	メンテナンス仕様アーカイブ ・・・	個別アーカイブ ・・・

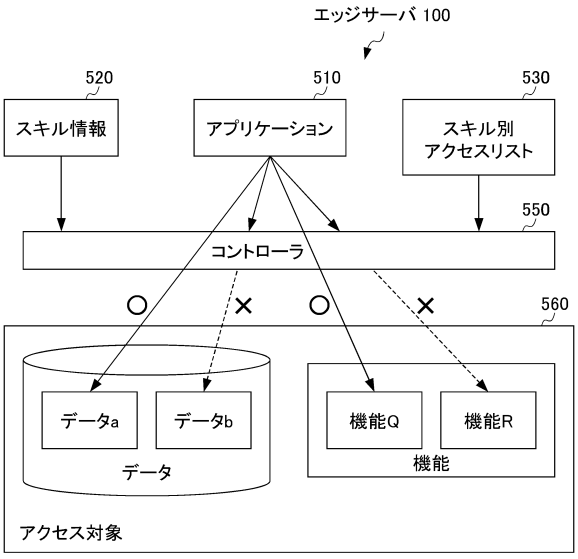
【図５】


1000
100
300
S11
S21
作業者Aを承認
スキル情報
（作業者A）
アプリケーション
ラインL2情報
ラインL1情報
150
管理エージェント
エッジサーバ
ユーザ管理及びスキル情報の取得
ユーザ登録（ユーザ名、グループ情報等）
S10
ログイン（ユーザ名）
S20
ログインなしで利用可能
200
200
責任者
作業者A

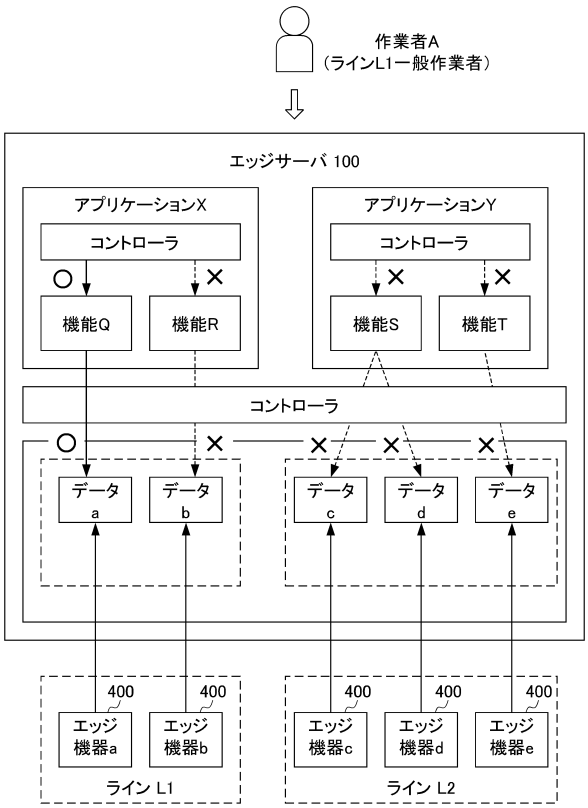
【図６】


アクセス制御処理
（エッジサーバ 100）
START
S40
アプリケーションの起動
S41
ユーザのスキル情報を記憶
S42
スキル情報に対応した
スキル別アクセスリストの読込
S43
エッジ機器の機能の使用
及び／又は処理データへのアクセス要求を
受け付けたか？
NO
YES
S44
許可されているか？
NO
YES
S45
該当のエッジ機器の機能の使用
及び／又は処理データへのアクセス処理
S46
NO
アプリケーションの終了を
受け付けたか？
YES
S47
アプリケーションの終了
END

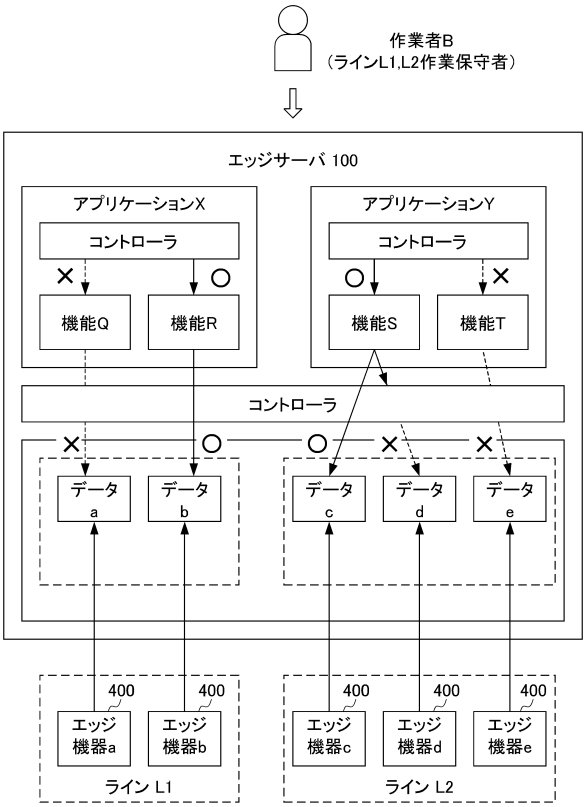
【図７】


エッジサーバ 100
520
スキル情報
510
アプリケーション
530
スキル別
アクセスリスト
550
コントローラ
560
データa
データb
データ
機能Q
機能R
機能
アクセス対象

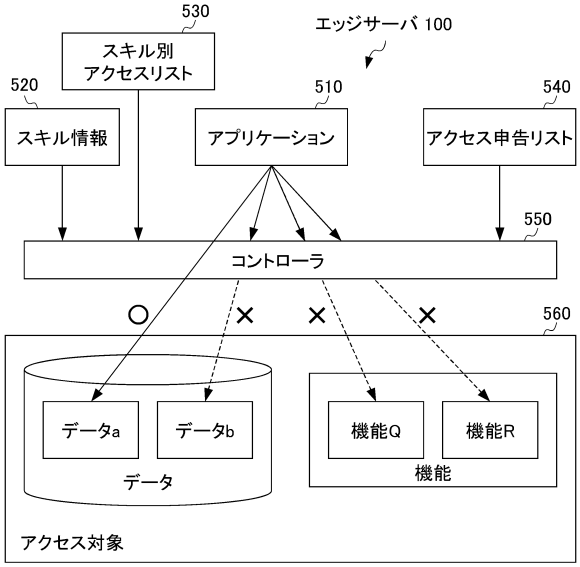
【図８Ａ】


作業者A
（ラインL1一般作業者）
エッジサーバ 100
アプリケーションX
コントローラ
機能Q
機能R
アプリケーションY
コントローラ
機能S
機能T
コントローラ
データ a
データ b
データ c
データ d
データ e
400
400
400
400
400
エッジ機器a
エッジ機器b
エッジ機器c
エッジ機器d
エッジ機器e
ライン L1
ライン L2

【図８Ｂ】


作業者B
（ラインL1,L2作業保守者）
エッジサーバ 100
アプリケーションX
コントローラ
機能Q
機能R
アプリケーションY
コントローラ
機能S
機能T
コントローラ
データ a
データ b
データ c
データ d
データ e
400
エッジ 機器a
エッジ 機器b
ライン L1
エッジ 機器c
エッジ 機器d
エッジ 機器e
ライン L2

【図９】


530
スキル別 アクセスリスト
エッジサーバ 100
520
スキル情報
510
アプリケーション
540
アクセス申告リスト
550
コントローラ
560
データa
データb
データ
機能Q
機能R
機能
アクセス対象

フロントページの続き

(56)参考文献 特開２００２－２７９０５７（ＪＰ，Ａ）
特開２０１５－１２５７４５（ＪＰ，Ａ）
特開２００４－０６２６１０（ＪＰ，Ａ）
特開２０００－１１２８９１（ＪＰ，Ａ）
特開平１０－１１１８３３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／６２
Ｇ０６Ｆ　２１／３１
Ｇ０６Ｑ　５０／０４