(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6605959号
(P6605959)
(45)発行日　令和1年11月13日(2019.11.13)　(24)登録日　令和1年10月25日(2019.10.25)

(51)Int.Cl.　F I
*G05B 23/02 (2006.01)*　G05B 23/02 V

請求項の数 12 (全 17 頁)

(21)出願番号　特願2015-555175 (P2015-555175)
(86)(22)出願日　平成26年1月7日 (2014.1.7)
(65)公表番号　特表2016-506002 (P2016-506002A)
(43)公表日　平成28年2月25日 (2016.2.25)
(86)国際出願番号　PCT/US2014/010454
(87)国際公開番号　WO2014/116411
(87)国際公開日　平成26年7月31日 (2014.7.31)
審査請求日　平成28年12月27日 (2016.12.27)
審判番号　不服2018-6855 (P2018-6855/J1)
審判請求日　平成30年5月21日 (2018.5.21)
(31)優先権主張番号　13/749,670
(32)優先日　平成25年1月24日 (2013.1.24)
(33)優先権主張国・地域又は機関
米国 (US)

(73)特許権者　390041542
ゼネラル・エレクトリック・カンパニイ
アメリカ合衆国、ニューヨーク州　１２３４５、スケネクタデイ、リバーロード、１番
(74)代理人　100105588
弁理士　小倉　博
(74)代理人　100113974
弁理士　田中　拓人
(72)発明者　ブラウン，スーザン・ジーン
アメリカ合衆国、ヴァージニア州・２４１５３、セイラム、ロアノーク・ブールヴァード、１５０１番

最終頁に続く

(54)【発明の名称】高度制御システムセキュリティのためのシステムおよび方法

(57)【特許請求の範囲】
【請求項１】
工業システムを制御するコントローラと、
ユーザＩＤとアプリケーション証明書を特定する情報とを有する第１のマッピングデータ構造および前記ユーザＩＤ及び他のユーザＩＤをユーザ特権に関連付ける第２のマッピングデータ構造を記憶するように構成されたデータリポジトリと、
前記コントローラと前記データリポジトリとに通信可能に結合した、プロセス制御（ＯＰＣ）統一アーキテクチャ（ＵＡ）サーバと、
を備え、
前記ＯＰＣ　ＵＡサーバは、
クライアントからのアプリケーション証明書を受信して、セキュリティ通信プロトコルを使用したＯＰＣ　ＵＡクライアントとの通信接続を開始し、
前記第１のマッピングデータ構造を使用して前記ＯＰＣ　ＵＡクライアントのユーザＩＤを特定し、
前記セキュリティ通信プロトコルを使用した通信接続が開始した後、自動的に、前記第２のマッピングデータ構造と前記アプリケーション証明書を使用して、前記ＯＰＣ　ＵＡクライアントのユーザ特権を特定し、
特定されたユーザ特権に基づいて前記コントローラへのアクセス権を前記ＯＰＣ　ＵＡクライアントに提供して、前記ＯＰＣ　ＵＡクライアントが前記コントローラに指示して前記工業システムの制御動作を実行させることを可能にするように構成される、システム。

【請求項２】
前記ＯＰＣ　ＵＡサーバが、前記ＯＰＣ　ＵＡクライアントのユーザＩＤを特定するために前記第１のマッピングデータ構造に前記アプリケーション証明書を入力し、前記ＯＰＣ　ＵＡクライアントのユーザ特権を特定するために前記第２のマッピングデータ構造に前記ユーザＩＤを入力するように構成された、請求項１に記載のシステム。
【請求項３】
前記アプリケーション証明書が、証明書の通し番号、アルゴリズム、発行者の識別、有効期間、および、署名セクションとを含む証明書オブジェクトである、請求項１または２に記載のシステム。
【請求項４】
前記データリポジトリが、前記第１のマッピングデータ構造および前記第２のマッピングデータ構造を保持するデータストアを備え、
前記ＯＰＣ　ＵＡサーバが、サーバ証明書を前記ＯＰＣ　ＵＡクライアントに送信するように構成され、前記ＯＰＣ　ＵＡクライアントが、前記サーバ証明書を使用することによって前記ＯＰＣ　ＵＡサーバを認証し、前記ＯＰＣ　ＵＡクライアントのユーザのユーザ特権を判定するために、前記アプリケーション証明書を前記データストアに送信するように構成され、
前記データストアが、前記ユーザＩＤと前記ユーザ特権とを前記ＯＰＣ　ＵＡサーバに送信するように構成された、請求項１乃至３のいずれかに記載のシステム。
【請求項５】
前記ＯＰＣ　ＵＡサーバが、前記アプリケーション証明書および信頼されたストアを使用することによって前記ＯＰＣ　ＵＡクライアントを認証するように構成される、請求項１乃至４のいずれかに記載のシステム。
【請求項６】
前記第１のマッピングデータ構造および前記第２のマッピングデータ構造を作成するように構成されたアプリケーション証明書マッピング（ＡＣＭ）システムを備え、
前記ＡＣＭシステムが、前記ユーザＩＤを前記アプリケーション証明書に視覚的に関連付けることによって前記第１のマッピングデータ構造を作成するように構成されたユーザ対アプリケーション証明書マッピング画面を備え、
前記ＡＣＭシステムが、前記ユーザＩＤを前記ユーザ特権に視覚的に関連付けることによって前記第２のマッピングデータ構造を作成するように構成されたユーザ対ユーザ特権マッピング画面を備える、請求項１乃至５のいずれかに記載のシステム。
【請求項７】
前記コントローラが、タービンシステム、ガス化システム、工業プラント、発電システム、またはそれらの組合せの動作を制御するように構成された三重モジュール式冗長（ＴＭＲ）コントローラであり、
前記工業システムが、ガスタービンシステム、ガス化システム、蒸気タービンシステム、風力タービンシステム、水力タービンシステム、発電システム、またはそれらの任意の組合せを備える工業オートメーションシステムである、請求項１乃至６のいずれかに記載のシステム。
【請求項８】
アプリケーション証明書管理システムを使用して、ユーザＩＤとアプリケーション証明書を特定する情報とを有する第１のマッピングデータ構造を作成するステップと、
前記アプリケーション証明書管理システムを使用して、前記ユーザＩＤ及び他のユーザＩＤをユーザ特権に関連付ける第２のマッピングデータ構造を作成するステップと、
プロセス制御のためのオブジェクトのリンクと埋め込み（ＯＬＥ）（ＯＰＣ）統一アーキテクチャ（ＵＡ）クライアントから前記アプリケーション証明書をプロセス制御（ＯＰＣ）統一アーキテクチャ（ＵＡ）サーバが受信するステップと、
前記ＯＰＣ　ＵＡサーバを使用して、前記アプリケーション証明書が信頼されたストアに記録されているかを判定するステップと、

前記アプリケーション証明書が前記信頼されたストアに記録されている場合、前記アプリケーション証明書に基づいて、セキュリティ通信プロトコルを使用した前記ＯＰＣ　ＵＡクライアントとの通信接続を開始し、前記第１のマッピングデータ構造を使用して、前記ＯＰＣ　ＵＡクライアントのユーザＩＤを前記ＯＰＣ　ＵＡサーバを使用して特定するステップと、

前記セキュリティ通信プロトコルを使用した通信接続が開始した後、自動的に、前記第２のマッピングデータ構造と前記アプリケーション証明書を使用して、前記ＯＰＣ　ＵＡクライアントのユーザ特権を前記ＯＰＣ　ＵＡサーバを使用して特定するステップと、

前記ＯＰＣ　ＵＡサーバを使用して、特定されたユーザ特権に基づいて、前記ＯＰＣ　ＵＡクライアントにコントローラへのアクセス権を付与し、前記ＯＰＣ　ＵＡクライアントが前記コントローラに指示して工業システムの制御動作を実行させることを可能にするステップと、

を含む、方法。

【請求項９】

前記第１のマッピングデータ構造および前記第２のマッピングデータ構造の使用が、前記第１のマッピングデータ構造を使用することによって前記ユーザＩＤを前記アプリケーション証明書に突き合わせるステップと、前記第２のマッピングデータ構造を使用することによって前記ユーザ特権を前記ユーザＩＤに突き合わせるステップとを含む、請求項８記載の方法。

【請求項１０】

前記ユーザ特権が、発電システムまたは自動製造システムに行われるメソッド呼出しに対応する、請求項８または９に記載の方法。

【請求項１１】

グラフィカルユーザインターフェース（ＧＵＩ）に前記第１のマッピングデータ構造および前記第２のマッピングデータ構造を表示するステップを含み、

前記第１のマッピングデータ構造が、複数のユーザＩＤを１つのアプリケーション証明書に関連付け、

前記アプリケーション証明書が、証明書オブジェクトである、請求項８乃至１０のいずれかに記載の方法。

【請求項１２】

工業システムのプロセッサによって実行可能な複数の命令を記憶する、有形の、非一時的な、コンピュータ可読媒体であって、前記命令が、

ユーザＩＤとアプリケーション証明書を特定する情報とを有する第１のマッピングデータ構造を作成し、

前記ユーザＩＤ及び他のユーザＩＤをユーザ特権に関連付けるように構成された第２のマッピングデータ構造を作成し、

前記工業システムへのアクセス権限を要求するプロセス制御のためのオブジェクトのリンクと埋め込み（ＯＬＥ）（ＯＰＣ）統一アーキテクチャ（ＵＡ）クライアントから前記アプリケーション証明書を受信して、前記アプリケーション証明書に基づいて、セキュリティ通信プロトコルを使用した前記ＯＰＣ　ＵＡクライアントとの通信接続を開始し、

データリポジトリに記録された前記第１のマッピングデータ構造を使用して、前記ＯＰＣ　ＵＡクライアントのユーザＩＤを特定し、

前記セキュリティ通信プロトコルを使用した通信接続が開始した後、自動的に、前記データリポジトリに記録された前記第２のマッピングデータ構造と前記アプリケーション証明書を使用して、前記ＯＰＣ　ＵＡクライアントのユーザ特権を特定し、

特定されたユーザ特権に基づいて、前記ＯＰＣ　ＵＡクライアントにコントローラへのアクセス権を付与し、前記ＯＰＣ　ＵＡクライアントが前記コントローラに指示して前記工業システムの制御動作を実行させるための命令を備える、媒体。

【発明の詳細な説明】

【技術分野】

【０００１】
本明細書で開示される主題は、高度セキュリティ制御システムのためのシステムおよび方法に関する。
【背景技術】
【０００２】
工業オートメーションシステムなどのある種のシステムは、システムの制御および監視を可能にする機能を含むことがある。たとえば、工業オートメーションシステムは、コントローラ、フィールドデバイス、および、その後の分析のためにデータを監視するセンサを含み得る。さらに、そのような工業制御システムは、コントローラに結合することができ、「プロセス制御のためのオブジェクトのリンクと埋め込み（ＯＬＥ）（ＯＰＣ）」統一アーキテクチャ（ＵＡ）プロトコルに従って他のシステムと通信することができる、１つまたは複数のデバイスを含み得る。ＯＰＣ　ＵＡは、ＯＰＣ　Ｆｏｕｎｄａｔｉｏｎによって指定された工業オートメーションシステム（たとえば、自動発電システムおよび自動製造システム）で使用される製造業者に依存しない通信のためのプロトコルである。たとえば、工業オートメーションシステムは、工業オートメーションシステムの動作パラメータに関する情報を全体として記憶することができるＯＰＣ　ＵＡサーバを含み得る。加えて、ＯＰＣ　ＵＡサーバはまた、別の場所で動作する１つまたは複数のＯＰＣクライアントに、ネットワーク接続を介して、この情報を入手可能にすることができる。それは、制御システムセキュリティを改善するために有益になろう。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】米国特許出願公開第２０１１／０３５７９２Ａ１号明細書
【発明の概要】
【課題を解決するための手段】
【０００４】
出願時に特許請求されている発明と範囲において同等のある種の実施形態が、以下に要約される。これらの実施形態は、特許請求されている本発明の範囲を限定するものではなく、むしろ、これらの実施形態は、本発明の可能な形態の簡潔な要約を提供することのみを意図されている。実際、本発明は、以下に記載の実施形態と同様であり得るまたはそれらとは異なり得る様々な形態を包含し得る。
【０００５】
第１の実施形態では、システムは、ユーザをアプリケーション証明書に関連付ける第１のマッピングと、ユーザをユーザ特権に関連付ける第２のマッピングとを記憶するように構成されたデータリポジトリを有するコントローラを含む。本システムはさらに、ＯＰＣ　ＵＡクライアントからのアプリケーション証明書の受信とユーザ特権の実施に基づいてサーバアクセスを提供するように構成され、ユーザ特権が第１のマッピングおよび第２のマッピングに基づいて検索可能である、ＯＰＣ統一アーキテクチャ（ＵＡ）サーバを含む。
【０００６】
第２の実施形態では、方法は、ユーザをアプリケーション証明書に関連付ける第１のマップと、そのユーザをユーザ特権に関連付ける第２のマップとを作成するステップを含む。本方法はまた、ＯＰＣ統一アーキテクチャ（ＵＡ）クライアントからアプリケーション証明書を受信するステップを含む。本方法はさらに、ユーザ特権の検索に基づいてコントローラへのアクセスを限定するステップを含み、そのユーザ特権の検索は、第１のマッピングおよび第２のマッピングの使用を含む。
【０００７】
第３の実施形態では、有形の、非一時的、コンピュータ可読媒体が、電子デバイスのプロセッサによって実行可能な複数の命令を記憶し、その命令は、ユーザをアプリケーション証明書に関連付ける第１のマップとそのユーザをユーザ特権に関連付ける第２のマップ

とを作成するための命令を含む。その命令はまた、ＯＰＣ統一アーキテクチャ（ＵＡ）クライアントからアプリケーション証明書を受信するための命令を含む。その命令はさらに、ユーザ特権に基づいてコントローラへのアクセスを限定するための命令を含み、ユーザ特権は、第１のマッピングおよび第２のマッピングを使用することによって判定される。

【０００８】

同様の文字が図面をとおして同様の部分を表す添付の図面を参照し、以下の詳細な説明が読まれるときに、本発明のこれらのおよび他の特徴、態様、および利点は、よりよく理解されよう。

【図面の簡単な説明】

【０００９】

【図１】コントローラ、ＯＰＣ　ＵＡサーバ、およびＯＰＣ　ＵＡクライアントを含む工業制御システムの一実施形態のブロック図である。

【図２】図１に示す、アクセスがＯＰＣ　ＵＡサーバに限定されるプロセスの一実施形態を示す流れ図である。

【図３】図１に示すＯＰＣ　ＵＡクライアントとＯＰＣ　ＵＡサーバの間の通信の一実施形態を示す情報流れ図である。

【図４】複数のユーザおよび関連する証明書を示す画面ビューの一実施形態を示す図である。

【図５】証明書のクラスおよびユーザ名の選択を示す画面ビューの一実施形態を示す図である。

【図６】複数のユーザおよび関連する特権を示す画面ビューの一実施形態を示す図である。

【発明を実施するための形態】

【００１０】

本発明の１つまたは複数の特定の実施形態が、以下に説明されることになる。これらの実施形態の簡潔な説明を提供することを目的として、実際の実装形態のすべての特徴は、本明細書には記載されないことがある。任意のそのような実際の実装形態の開発では、どの技術または設計プロジェクトでもそうであるように、実装形態によって変わり得る、システム関連およびビジネス関連の制約の順守など、開発者の特定の目的を達成するために、多数の実装形態特有の決定が行われる必要があることを理解されたい。さらに、そのような開発活動は、複雑で時間を要することがあるが、それでもなお、本開示の利益を有する当業者のための設計、製作、および製造を請け負うルーチンであろうことを理解されたい。

【００１１】

本発明の様々な実施形態の要素を紹介するとき、「ａ」、「ａｎ」「ｔｈｅ」、および「ｓａｉｄ」という冠詞は、それらの要素が１つまたは複数存在することを意味するものである。「備える」、「含む」、および、「有する」という用語は、包括的なものであり、記載された要素以外の追加の要素が存在し得ることを意味する。

【００１２】

本明細書に記載のある種の実施形態では、ＯＰＣ　ＵＡプロトコルは、ＯＰＣ　ＵＡサーバおよびユーザ（人間のユーザおよび／または自動化されたエンティティ）がＯＰＣ　ＵＡクライアントを使用してネットワークを介して互いに通信することを可能にするために、自動発電システム（たとえば、ガス、蒸気、風力、または水力タービン、熱回収蒸気発生器（ＨＲＳＧ）、ガス化システム、燃焼システム、発電機、または同様の自動発電システム）および自動製造システム（たとえば、化学プラント、石油精製所、または同様の製造システム）などの工業オートメーションまたは制御システムで使用され得る。所望のセキュリティレベルを実現するために、および、ＯＰＣ　ＵＡサーバとユーザの間の通信の制御を改良するために、ユーザおよび関連ユーザ情報をより効率的に識別することはＯＰＣ　ＵＡサーバの利益になり得る。たとえば、より効率的にユーザを識別することによって、ＯＰＣ　ＵＡサーバは、より速くユーザをユーザ特権に関連付け、その関連付けに

基づいてより高速の制御動作を行うことができる。

【００１３】

したがって、ここで開示される実施形態は、ＯＰＣ　ＵＡクライアントのユーザ、アプリケーション証明書、ユーザ役割、およびユーザ特権の間の複数のマッピングを作成および使用することができる。たとえば、１つのマッピングは、ユーザをアプリケーション証明書に関連付けることができ、もう１つのマッピングは、ユーザをユーザ特権に関連付けることができる。サーバにアプリケーション証明書を提示することによって、クライアントは、そのアプリケーション証明書にリンクされたユーザに関連付けられたすべての役割および特権を与えられ得る。さらに、ここで開示される実施形態は、基礎となるクライアントまたはサーバセキュリティＯＰＣアーキテクチャを変えなくてもまたは損なわなくてもよい。言い換えれば、ＯＰＣ　Ｆｏｕｎｄａｔｉｏｎによって定められた仕様に合うＯＰＣ　ＵＡクライアントが、再コード化なしに使用され得る。そのような例示的クライアントの一例は、オハイオ州オーバーン郡区のＯＰＣ　Ｆｏｕｎｄａｔｉｏｎから入手可能である。実際、かなりの数のＯＰＣクライアントは、開示される技法を修正なしに使用することができる。

【００１４】

前述を考慮し、本明細書で開示される技法を組み込むオートメーションシステムを説明することは有益であり得る。したがって、図１は、本明細書で開示される改良された制御セキュリティ技法を組み込む工業オートメーションシステムの例示的実施形態としてガスタービンシステム１０を示す。図示するように、タービンシステム１０は、燃焼するための燃料／空気混合物を受け取ることができる燃焼器１２を含み得る。この燃焼は、高温の加圧された排気ガスを作り出し、燃焼器１２は、タービン１４（たとえば、ロータの部分）を介して排気口１６にその排気ガスを向ける。その排気ガスがタービン１４を通過するとき、結果として生じる力によりタービンブレードがタービンシステム１０の軸に沿ってドライブシャフト１８を回転させる。図示するように、ドライブシャフト１８は、圧縮機２０を含むタービンシステム１０の様々な部品に接続される。

【００１５】

ドライブシャフト１８は、たとえば、同心円状に位置合わせされ得る、１つまたは複数のシャフトを含み得る。ドライブシャフト１８は、タービン１４を圧縮機２０に接続してロータを形成するシャフトを含み得る。圧縮機２０は、ドライブシャフト１８に結合されたブレードを含み得る。それにより、タービン１４内のタービンブレードの回転は、圧縮機２０にタービン１４を接続するシャフトに圧縮機２０内のブレードを回転させることができる。圧縮機２０内のブレードの回転は、空気取り入れ口２２を介して受け取られた空気を圧縮する。圧縮された空気は、燃焼器１２に送り込まれ、燃料と混合されて、より高い効率の燃焼を可能にする。シャフト１８はまた、負荷２４に接続されてもよく、負荷２４は、乗り物であっても、発電所の発電機または航空機のプロペラなど固定負荷でもあってもよい。負荷２４が発電機であるとき、その発電機は、たとえば住宅および商用のユーザに、電力を分配するための電力網２６に結合され得る。

【００１６】

タービンシステム１０はまた、タービンシステム１０の動作および性能に関する複数のエンジンパラメータを監視するように構成された複数のセンサおよびフィールドデバイスを含み得る。たとえば、それらのセンサおよびフィールドデバイスは、それぞれ、たとえば、タービン１４、および圧縮機２０の入口および出口部分、に隣接して位置付けられた入口センサおよびフィールドデバイス３０と、出口センサおよびフィールドデバイス３２とを含み得る。入口センサおよびフィールドデバイス３０と出口センサおよびフィールドデバイス３２とは、たとえば、周囲温度および周囲気圧などの環境条件、ならびに、排気ガス温度、ロータ速度、エンジン温度、エンジン圧力、ガス温度、エンジン燃料流量、排気流量、振動、回転する部品と固定部品の間の間隔、圧縮機排出圧力、汚染（たとえば、窒素酸化物、硫黄酸化物、酸化炭素および／または微粒子総数）、およびタービン排気圧力などのタービンシステム１０の動作および性能に関する複数のエンジンパラメータを測

定することができる。さらに、センサおよびフィールドデバイス３０および３２はまた、バルブの位置、および可変ジオメトリ部品（たとえば、空気入口にある入口ガイドベーン）の幾何学的位置などのアクチュエータ情報を測定することができる。それらの複数のセンサおよびフィールドデバイス３０および３２はまた、タービンシステム１０の様々な動作段階に関するエンジンパラメータを監視するように構成され得る。複数のセンサおよびフィールドデバイス３０および３２によって得られた測定結果（すなわち、工業オートメーションシステム１０の動作パラメータ）は、コントローラ３８に通信で結合され得るモジュールライン３４および３６を介して、送信され得る。コントローラ３８は、三重モジュール式冗長（ＴＭＲ）コントローラなどの冗長コントローラでもよい。冗長コントローラ３８は、処理コアなどの複数の（たとえば2つ、３つ、４つ、５つ、またはそれ以上の）システムを含む。たとえば、ＴＭＲコントローラ３８は、３つのシステムの多数決によって判定された出力で単一のタスクを実行する３つのシステム（たとえば、処理コア）を有する。たとえば、モジュールライン３４は、圧縮機２０から測定結果を送信するために使用することができ、一方、モジュールライン３６は、タービン１４から測定結果を送信するために使用することができる。コントローラ３８は、それらの測定結果を使用してタービンシステム１０をアクティブに制御することができる。

【００１７】

燃焼器１２センサ、排気装置１６センサ、取り入れ口２２センサ、間隔センサ、および負荷２４センサを含む他のセンサが使用され得ることを理解されたい。同様に、Ｆｉｅｌｄｂｕｓ　Ｆｏｕｎｄａｔｉｏｎ、Ｐｒｏｆｉｂｕｓ、および／またはＨａｒｔフィールドデバイスなどの「スマート」フィールドデバイスを含む任意のタイプのフィールドデバイスが、使用され得る。ガスタービンシステム１０は、工業オートメーションシステムの単に例示的実施形態であり、他の工業オートメーションシステムは、たとえば、ガスタービン、蒸気タービン、風力タービン、もしくは水力タービン、熱回収蒸気発生器（ＨＲＳＧ）、発電機、燃料スキッド、ガス処理システム、または任意の他の自動発電システムもしくは部分的に自動の発電システムなどの自動発電システムを含み得ることもまた理解されたい。他の工業オートメーションシステムは、化学プラント、製薬工場、石油精製所、自動生産ラインまたは同様の自動のもしくは部分的に自動の製造システムなどの自動製造システムを含み得る。

【００１８】

前述のように、ＯＰＣ　ＵＡサーバ４０は、それが、システム１０の動作パラメータに関するコントローラ３８からのデータを要求および／または受信することができるように、コントローラ３８に通信で結合され得る。ある種の実施形態では、ＯＰＣ　ＵＡサーバ４０は、コントローラ３８の部分でもよく、または、ネットワーク接続（たとえば、内部ネットワーク接続４１）を介してコントローラ３８に結合され得る。システム１０の動作パラメータは、たとえば、ガスタービンシステム１０などの工業オートメーションシステムのコントローラ３８によって一般に追跡することができる、状況（たとえば、機能、動作、機能不良、セキュリティ、または同様の状況）、性能（たとえば、パワー出力、１分当たりの回転、負荷、または同様の性能パラメータ）、環境条件（たとえば、温度、圧力、電圧、電流、特定の分析物の存在もしくはレベル、または同様の環境条件）などに関する情報を含み得る。

【００１９】

開示されるＯＰＣ　ＵＡサーバ実施形態は、ＯＰＣ　ＵＡサーバ４０とＯＰＣ　ＵＡクライアント４６などのＯＰＣ　ＵＡクライアントを使用するユーザ４４との間の通信のより多くの制御を可能にするが、ＯＰＣ　ＵＡクライアント４６は、一般に、標準プロトコルに従って、開示されるＯＰＣ　ＵＡサーバ４０と通信することができる（たとえば、外部ネットワーク接続４８を使用して）。たとえば、ＯＰＣ　ＵＡサーバ４０は、サーバ４０を識別するサーバ証明書４９を送信することになり、ＯＰＣ　ＵＡクライアント４６は、ユーザ４４を識別するアプリケーション証明書５０をＯＰＣ　ＵＡサーバ４０に送信することになる。前述のように、ＯＰＣ　ＵＡクライアント４６は、任意の標準ＯＰＣ　Ｕ

Ａクライアントでもよく、そのようなものとして、実質的に最も多くのＯＰＣ認定クライアントが、本明細書に記載の技法を使用することができる。たとえば、一実施形態では、ＯＰＣ　ＵＡ４６クライアントは、ニューヨーク州スケネクタディのＧｅｎｅｒａｌ　Ｅｌｅｃｔｒｉｃ　Ｃｏｍｐａｎｙから入手可能なＣｏｎｔｒｏｌＳＴＴＭを含み得る。ＣｏｎｔｒｏｌＳＴＴＭは、マシン可読媒体に記憶され、たとえばコントローラ３８の、コミッショニング、プログラミング、設定１／０、傾向分析、および分析診断のために使用される、非一時的実行可能ソフトウェアまたはコンピュータ命令を含み得る。そのソフトウェアは、コントローラ３８での改良された品質の時間コヒーレントなデータのソースと、機器資産をより効果的に制御および／または管理するためのプラントレベルとを提供することができる。

【００２０】

一般に、データストア５４は、任意のタイプのデータリポジトリでもよい。たとえば、データストア５４は、データベースまたは他のタイプのデータサーバでもよい。加えて、ある種の実施形態では、データストア５４は、コントローラ３８の部分でもよい。データストア５４は、現場に存在し、ＯＰＣ　ＵＡサーバ４０に通信で結合することができ（たとえば、内部バスまたは内部ネットワーク接続でもよい接続５５を介して）、あるいは、現場外にあり、外部ネットワーク接続を介してＯＰＣ　ＵＡサーバ４０に結合され得る。他の実施形態では、データストア５４は、ＯＰＣ　ＵＡサーバ４０と同じ電気デバイス（たとえば、コンピュータ、サーバ、または同様の処理もしくは計算デバイス）上にあってもよく、その通信は、ローカル接続（たとえば、ローカルループバック、共用ファイルまたは記憶空間など）を代わりに含んでもよい。

【００２１】

図示されたデータストア５４は、ユーザ、アプリケーション証明書、ユーザ役割、およびユーザ特権の間の前述のマッピングと、ユーザに関連する任意の他のデータとを記憶することができる。そのユーザは、人間のユーザ、自動化されたエンティティ（たとえば、ソフトウェアおよび／またはハードウェアエンティティ）、あるいはそれらの組合せを含み得る。一実施形態では、第１のマッピング５６は、ユーザをアプリケーション証明書に関連付ける。第２のマッピング５８は、ユーザをユーザ特権に関連付ける。他の実施形態では、第３のマッピング６０がユーザを少なくとも１つのユーザ役割（たとえば、システム管理者役割、コミッショニング技術者役割、基本的ユーザ役割）に関連付けることを理解されたい。前述のマッピングは、アプリケーション証明書管理（ＡＣＭ）システム６１内で作成され、データストア５４に通信で結合され得る。いくつかの実施形態では、ＡＣＭ６１は、システム管理者が手動か自動かのいずれかで関連付けを作成することを可能にするアプリケーションでもよい。以下にさらに示すように、そのアプリケーションは、マッピング５６、５８、６０を視覚化ならびに編集するためのグラフィカルユーザインターフェース（ＧＵＩ）を含むと有用であることがある。マッピングは、所定でも、そのアプリケーションを実行することができる任意のコンピューティングマシンで作成されてもよい。マッピング５６、５８、６０は、ネットワーク接続を介して、または携帯記憶装置（たとえば、サムドライブ、ＤＶＤ）を使用することによって、データストア５４に転送することができる。したがって、ＡＣＭは現場にあっても現場外にあってもよいことを理解されたい。一代替実施形態では、ＡＣＭ６１は、データストア５４と同じ計算デバイス（たとえば、ワークステーション、ラップトップ、タブレット、携帯電話）上にあって、ローカル接続を伴い得る。

【００２２】

信頼されたストア６２は、ＯＰＣ　ＵＡサーバ４０にアクセスするために使用されるアプリケーション証明書の信頼されたリスト６４を記憶することができる。一実施形態では、信頼されたストア６２は、ＯＰＣ　ＵＡ機能を提供するＯＰＣ　ＵＡオーバレイまたは層を有する標準Ｍｉｃｒｏｓｏｆｔ　Ｗｉｎｄｏｗｓ（登録商標）証明書ストアである。その証明書ストアの使用は、次いで、たとえばシステム管理者による、信頼されたリスト６４の容易な編集を可能にすることができる。さらに、これらの技法は、ＯＰＣ　ＵＡサ

ーバ４０およびＯＰＣ　ＵＡクライアント４６と連動した共通の規格、たとえば、Ｍｉｃｒｏｓｏｆｔ　Ｗｉｎｄｏｗｓ（登録商標）証明書ストア、の使用を実現する。任意の他の共通の証明書ストア規格が、開示される実施形態で使用され得る。信頼されたストア６２は、ＯＰＣ　ＵＡサーバ４０に通信で結合される。ある種の実施形態では、信頼されたストア６２は、現場にあって、たとえば内部ネットワーク接続を介して、ＯＰＣ　ＵＡサーバ４０と通信することができ、あるいは、現場外にあって、外部ネットワーク接続を介してＯＰＣ　ＵＡサーバ４０に結合されてもよい。これらの実施形態では、信頼されたストア６２は、任意のＭｉｃｒｏｓｏｆｔ　Ｗｉｎｄｏｗｓ（登録商標）証明書ストアにアクセスすることができるコンピューティングマシンで使用され得ることを理解されたい。他の実施形態では、信頼されたストア６２は、ＯＰＣ　ＵＡサーバ４０と同じ計算デバイス（たとえば、コンピュータ、サーバ、ラップトップ、タブレット、携帯電話、携帯デバイス、または同様の処理もしくは計算デバイス）上にあってもよく、その通信は、代わって、ローカル接続（たとえば、ローカルエリアネットワーク（ＬＡＮ））を伴い得る。その通信は、図２に関して以下にさらに詳しく説明されるように、証明書４９、５０を交換し、たとえばユーザ４４特権および役割を、導出するために使用することができる。

【００２３】

図２は、それによってＯＰＣ　ＵＡサーバ４０が、ここで開示される実施形態に従ってアクセスを限定することができる、プロセス１２０の一実施形態を示す流れ図である。プロセス１２０は、コントローラ３８、サーバ４０、クライアント４６、データストア５４、またはそれらの組合せのメモリなどのマシン可読媒体内に記憶された実行可能な非一時的コンピュータ命令またはコード内に含まれ得る。プロセス１２０は、第１のマッピング５６をＡＣＭ６１が作成すること（ブロック１２１）で開始し得る。前述のように、第１のマッピング５６は、１人または複数のユーザ４４を１つまたは複数のアプリケーション証明書５０に関連付ける、またはリンクする。次に、ＡＣＭ６１が、第２のマッピング５８を作成する（ブロック１２２）。前述のように、第２のマップ５８は、１人または複数のユーザ４４を１つまたは複数のユーザ特権と関連付ける。そのユーザ特権は、読み取る、書き込む、更新する、他のメソッド呼出しを行う、または、より一般的には、ＯＰＣ　ＵＡサーバ４０にアクセスするための能力を含む。ユーザ特権は、発電システムまたは自動製造システムなどのシステム１０に行われ得るメソッド呼出しに相当し得ることを理解されたい。マップ５６、５８が作成された後は、ＯＰＣ　ＵＡサーバ４０は、ＯＰＣ　ＵＡクライアント４６などのＯＰＣ　ＵＡクライアントからアプリケーション証明書５０を受信する（ブロック１２３）。アプリケーション証明書５０および第１のマッピング５６を使用し、ＯＰＣ　ＵＡサーバ４０は、ＯＰＣ　ＵＡクライアント４６でユーザ４４を導出する（ブロック１２４）。すなわち、第１のマッピング５６は、サーバ４０が、受信されたアプリケーション証明書５０を使用すること、および、関連ユーザの識別を導出することを可能にする。したがって、追加のユーザ身分証明、（たとえば、ユーザ名、パスワード）を入力するのに費やされたであろう時間は、最小限に抑えるまたは削減することができる。ユーザ４４が導出された後、ＯＰＣ　ＵＡサーバ４０は、導出されたユーザ４４および第２のマッピング５８を使用し、ユーザ特権を導出する（ブロック１２５）。第２のマッピング５８は、サーバ４０が、導出されたユーザ４４を使用すること、および、ユーザ４４に関連するユーザ特権を導出することを可能にする。それにより、ＯＰＣ　ＵＡサーバ４０は、導出されたユーザ特権に基づいてクライアント４６へのアクセスを限定することができる（ブロック１２６）。たとえば、クライアント４６がサーバ４０に書込みをしようと試みる場合、サーバ４０は、次いで、導出されたユーザ特権を確認して、クライアント４６が書込み特権を提供されているかどうかを判定することができる。サーバ４０は、コントローラ３８に通信で結合され得るまたはコントローラ３８に含まれ得るので、導出された特権は、コントローラ３８へのアクセスを限定するために使用され得る。したがって、コントローラ３８によって行われる制御動作は、送信された証明書５０と、導出されたユーザ特権および／または役割とに基づいて、限定され得る。この方式で、マッピング５６、５８は、より効率的なコントローラ３８セキュリティシステムを可能にする

ことができる。

【００２４】

図３は、図２に示されたプロセス１２０によるＯＰＣ　ＵＡクライアント４６とＯＰＣ　ＵＡサーバ４０の間の通信の一実施形態を示す情報流れ図である。ＯＰＣ　ＵＡクライアント４６とＯＰＣ　ＵＡサーバ４０の間の通信は、トランスポート層セキュリティ（ＴＬＳ）またはセキュリティソケット層（ＳＳＬ）などの任意の標準セキュリティプロトコルを使用してもよい。たとえば、一実施形態では、ＯＰＣ　ＵＡサーバ４０とＯＰＣ　ＵＡクライアント４６の間の最初の接続１３０の後、ＯＰＣ　ＵＡサーバ４０は、ＯＰＣ　ＵＡクライアント４６がそれが所望のサーバ４０と通信していることを確認することができるように、ＯＰＣ　ＵＡクライアント４６にサーバ証明書４９を送信することになる。ＯＰＣ　ＵＡクライアント４６がそれが所望のサーバ４０と通信していることを確認した後は、ＯＰＣ　ＵＡクライアント４６は、アプリケーション証明書５０をＯＰＣ　ＵＡサーバ４０に送信して、ＯＰＣ　ＵＡクライアント４６を使用するまたはそれに関連付けられたユーザ４４を識別することになる。使用することができる１つのタイプのアプリケーション証明書５０は、Ｘ．５０９証明書である。Ｘ．５０９証明書規格は、証明書所有者をそれの公開鍵に暗号法で結び付ける。Ｘ．５０９証明書は、データセクション（すなわち、バージョン番号、その証明書の通し番号、アルゴリズム、発行者の識別、有効期間、および、主題の識別）と、署名セクションとを含む。他の証明書タイプは、ＥＶ（Ｅｘｔｅｎｄｅｄ　Ｖａｌｉｄａｔｉｏｎ、拡張された検証）ＳＳＬ証明書、ＯＶ（Ｏｒｇａｎｉｚａｔｉｏｎ　Ｖａｌｉｄａｔｉｏｎ、組織検証）ＳＳＬ証明書、および、ＤＶ（Ｄｏｍａｉｎ　Ｖａｌｉｄａｔｉｏｎ、ドメイン検証）ＳＳＬ証明書を含み得る。

【００２５】

アプリケーション証明書５０を受信した後、ＯＰＣ　ＵＡサーバ４０は、ＯＰＣ　ＵＡクライアント４６がＯＰＣ　ＵＡサーバ４０と通信することを許可されることを確保するために、アプリケーション証明書５０が信頼されたストア６２内で見つかることを確認する（通信矢印１３１）。次に、アプリケーション証明書５０が、ＯＰＣ　ＵＡクライアント４６のユーザのユーザ特権を判定するために（導出１３２）、データストア５４に送信される。前述のように、データストア５４は、アプリケーション証明書５０をユーザ４４に関連付ける第１のマッピング５６と、ユーザ４４をユーザ特権および／または役割に関連付ける第２のマッピングとを使用することができる。データストア５４は、ユーザ役割をユーザ特権に関連付ける第３のマッピングを使用することができることを理解されたい。ユーザとユーザ役割、ユーザとコントローラ動作、ユーザとハードウェア、ユーザとアプリケーションなどの間のマッピングを含む、他のマッピングが、マッピング５６、５８、６０に加えてまたはそれらの代わりに使用され得る。したがって、ユーザアクセスは、そのユーザが使用することを許可され得るコントローラ動作、ハードウェア、および／またはソフトウェアアプリケーションを導出することによって、見つけることができる。ユーザ特権および／または役割が導出された（導出１３２）後は、特権フィルタ１３４が、ＯＰＣ　ＵＡサーバ４０内で作成される。それにより、ＯＰＣ　ＵＡクライアント４６のユーザ４４がメソッド呼出し１３３を行おうとまたは他の方法でＯＰＣ　ＵＡサーバ４０にアクセスしようと試みる度に、ＯＰＣ　ＵＡサーバ４０は、クライアント４６が適切なユーザ特権および／または役割を有するかどうかを確認することになる。ＯＰＣ　ＵＡサーバ４０がクライアント４６が適切なユーザ特権および／または役割を有さないと判定した場合、ＯＰＣ　ＵＡサーバ４０は、不良アクセス結果１３５で応答することができる。他方で、クライアント４６が適切な特権および／または役割を有する場合、ＯＰＣ　ＵＡサーバ４０は、要求された動作１３６を行うことができる。

【００２６】

本明細書に記載の技法より前には、ＯＰＣ　ＵＡサーバ４０およびＯＰＣ　ＵＡクライアント４６は、複雑なおよび多数のステップを介して通信することができた。比較して、本明細書に記載の技法は、特権フィルタ１３４の作成および使用によって、ＯＰＣ　ＵＡサーバ４０とＯＰＣ　ＵＡクライアント４６の間の通信を単純化することができる。した

がって、ＯＰＣ　ＵＡサーバ４０とＯＰＣ　ＵＡクライアント４６の間の通信のセキュリティは、通信の制御の強化で改良され得る。たとえば、ＯＰＣ　ＵＡサーバ４０は、ユーザ５２をユーザ証明書５０に関連付けることができ得る。本明細書に記載の技法を実装するために使用され得るアプリケーションの一実施形態のグラフィカルユーザインターフェース（ＧＵＩ）の画面ビューが、図４～６に示される。

【００２７】

図４は、ユーザセル１４２を証明書識別子セル１４０と関連付けることによって、ＡＣＭ６１によって作成された第１のマッピング５６を実装するアプリケーションの画面ビュー１３８、ＧＵＩ、の一実施形態である。画面ビュー１３８は、コンピュータ、サーバ、ラップトップ、タブレット、携帯電話、携帯デバイス、または同様の処理もしくは計算デバイスのメモリなどの非一時的コンピュータ可読媒体内で記憶されたコンピュータ命令を使用することによって、実装され得る。図示された実施形態では、画面ビュー１３８は、ＯＰＣ　ＵＡサーバタブ１４４を第１に選択することによって、表示され得る。画面ビュー１３８内に見ることができるように、選択することができる他のタブは、Ｇｅｎｅｒａｌ（一般）、ＯＰＣＤＡサーバ、Ｖａｒｉａｂｌｅｓ（変数）、およびＥＧＤを含む。ＯＰＣ　ＵＡ　Ｓｅｒｖｅｒ（サーバ）タブ１４４が選択された後は、ＯＰＣ　ＵＡツリー制御１４６が、セキュリティ証明書ノード１４８、画面ビュー１３８、および、ＯＰＣ　ＵＡクライアントのリストを表示するＯＰＣ　ＵＡクライアントノード１５０の間を移動するために使用され得る。セキュリティ証明書ノード１４８が選択されるとき、証明書識別子リストまたは欄１５２、および、特権ユーザ名リストまたは欄１５４が、コンピュータなどのアプリケーションを実行するデバイスに表示され得る。第１のマッピング５６を実装するために、「ユーザ３」１４２で示されるものなど、特権ユーザ名リスト１５４からの各ユーザは、証明書識別子リスト１５２の「Ｄ６２７Ａ８Ｄ４ＤＢＡ９６Ｂ８ＥＡ３３８６７１４ＢＣ２Ｆ４Ａ０７５９９７３Ｅ５９」１４０などの証明書識別子と関連付けられ得る。特権ユーザ名リスト１５４内のユーザは証明書識別子リスト１５２中の証明書識別子と視覚的に関連付けられ得ることを理解されたい。前述のように、ＡＣＭ６１は、特権ユーザリスト１５４内のエントリと証明書識別子リスト１５２内のエントリの間の関連付け（たとえば、マッピング５６）を追加、変更または除去する能力を有し得る。これを実装するために使用され得るアプリケーションは、図５中に見ることができる。

【００２８】

図５は、証明書識別子１５８および関連ユーザ名１５９の選択を示すダイアログボックスの画面ビュー１５６、ＧＵＩ、の一実施形態である。説明のために、エントリの編集は、「ユーザ３」１４２というラベルを付けられたユーザ４４と「Ｄ６２７Ａ８Ｄ４ＤＢＡ９６Ｂ８ＥＡ３３８６７１４ＢＣ２Ｆ４Ａ０７５９９７３Ｅ５９　１４０」というラベルを付けられた関連証明書識別子１４０との関連で論じられることになる。画面ビュー１５６は、コンピュータ、サーバ、ラップトップ、タブレット、携帯電話、携帯デバイス、または同様の処理もしくは計算デバイスのメモリなどの非一時的コンピュータ可読媒体に記憶されたコンピュータ命令を使用することによって、実装され得る。どのエントリが編集されているかを判定するために、クライアント４６セキュリティ証明書が、ドロップダウンメニュー１７０から選択され得る。画面ビュー１５６で、選択されたクライアント４６は、「会社ＡＢＣ　ＯＰＣ　ＵＡクライアント」のラベルを付けられる。クライアント４６セキュリティ証明書が選択された後は、証明書識別子１５８に関連付けられ得るある種のアイテムが存在し得る。第１のアイテムは、クライアントの名１６０を含み得る。クライアントの名１６０の一例は、「会社ＡＢＣ　ＯＰＣ　ＵＡクライアント」１６２のラベルを付けられる。別のアイテムは、識別名（ＤＮ）１６４を含み得る。ＤＮ１６４は、Ｘ．５０９証明書規格で知られた一意の識別子である。図示された例で、ＤＮ１６４は、「ＣＮ＝会社ＡＢＣ　ＯＰＣ　ＵＡクライアント、ＯＵ＝アルファベット、Ｏ＝会社ＡＢＣ、Ｌ＝Ｌｅｔｔｅｒｖｉｌｌｅ、Ｓ＝ＮＹ、Ｃ＝ＵＳ１６６」のラベルを付けられる。第３のアイテムは、文字のランダムな列で構成される一意のサムプリント１６８を含み得る。図示された例で、一意のサムプリント１６８は、「Ｄ６２７Ａ８Ｄ４ＤＢＡ９６Ｂ８Ｅ

Ａ３３８６７１４ＢＣ２Ｆ４Ａ０７５９９７３Ｅ５９　１４０」のラベルを付けられる。各アイテムは、異なるレベルのセキュリティを提供することができることが、理解されよう。たとえば、一意のサムプリント１６８は、名１６０よりも安全であり得る。画面ビュー１５６で、一意のサムプリント１６８オプションが選ばれる。それにより、証明書識別子１５８は、Ｄ６２７Ａ８Ｄ４ＤＢＡ９６Ｂ８ＥＡ３３８６７１４ＢＣ２Ｆ４Ａ０７５９９７３Ｅ５９　１４０を使用するようにセットされる。バイオメトリックアイテム、セキュリティトークン、チャレンジレスポンス鍵などを含む他のアイテムが、使用され得る。

【００２９】

証明書識別子１５８が選択された後、対応するユーザ名１５９がドロップダウンメニュー１７２から選択され得る。画面ビュー１５６で、選ばれたユーザ名１５９は、「ユーザ３」１４２のラベルを付けられる。図４に関して、証明書識別子１５８とユーザ名１５９の間の画面ビュー１５６内で選ばれた関連付けが、画面ビュー１３８内に表示される。受信された証明書識別子１５８に基づいてユーザ名１５９を識別することが可能であるので、次のステップは、図６に示すように、ユーザ名１５９をユーザ特権および／または役割に関連付けることでもよい。

【００３０】

図６は、ユーザ１４２をユーザ特権および／または役割に関連付けることによって、第２のマッピング５８を実装することができるアプリケーションの画面ビュー１７４、ＧＵＩ、の一実施形態である。やはり説明のために、ユーザ特権および／または役割の関連付けは、「ユーザ３」１４２のラベルを付けられたユーザ４４との関連で論じられることになる。画面ビュー１７４は、コンピュータ、サーバ、ラップトップ、タブレット、携帯電話、携帯デバイス、または同様の処理もしくは計算デバイスのメモリなどの非一時的コンピュータ可読媒体に記憶されたコンピュータ命令を使用することによって、実装され得る。図示された実施形態では、画面ビュー１７４は、ツリービューリスト１７７からユーザおよび役割ノード１７６を選択することによって、表示することができる。他のノードオプションは、警報システム、診断翻訳、書式仕様セット、ＨＭＩリソース、ＨＭＩ画面、およびプラントエリアを含み得る。

【００３１】

画面ビュー１７４は、ユーザ１４２をユーザ特権および／または役割に関連付けるために、２つの別個のテーブル１７８および１８６を使用することができる。第１のテーブル１７８は、ユーザ名１８０のリストまたは欄を役割のリストまたは欄１８２に関連付けることができる。たとえば、ユーザ１４２は、オペレータ１８４の役割と関連付けられる。ユーザと関連付けられ得る他の役割は、管理者、保守、およびビューを含む。第２のテーブル１８６は、次いで、役割のリスト１８８をユーザ特権１９０、１９２、１９４、１９６、１９８、２００、２０２、２０４と関連付けることができる。ユーザ特権１９０、１９２、１９４、１９６、１９８、２００、２０２、２０４は、制御システム内で行われ得るある種のメソッド呼出しおよび他のアクションへのアクセスを可能にするために使用することができる。画面ビュー１７４にあるように、各ユーザ特権は、別個の欄でもよい。たとえば、１つのユーザ特権は、タグアウト特権１９０である。タグアウト特権１９０欄で、「タグアウト」することができる各ユーザ役割は真（Ｔｒｕｅ）を有することができ、「タグアウト」することができない各ユーザは偽（Ｆａｌｓｅ）を有することができる。画面ビュー１７４に図示された実施形態では、オペレータユーザ役割１８８は、「タグアウト」することができる。したがって、ユーザ３　１４２はオペレータの役割１８８に関連するので、ユーザ３　１４２は「タグアウト」することができることになる。他のユーザ特権は、ライブデータ修正特権１９２、ライブデータ強制特権１９４、警報特権１９６、ＨＭＩグラフィックから定義に進む特権１９８、警報サービス特権２００、ダウンロード特権２０２、および警報シェルブ特権２０４を含み得る。ユーザ名１８０のリスト内のユーザはユーザ特権１９０、１９２、１９４、１９６、１９８、２００、２０２、２０４と視覚的に関連付けられ得ることを理解されたい。加えて、ユーザ１４２とユーザ特権の間の単一テーブルマッピングがＯＰＣ　ＵＡサーバ４０によって使用され得ることも理

解されたい。さらに、ユーザ１４２は、複数の役割、ハードウェアアクセス、ソフトウェアアクセス、制御動作アクセスなどを割り当てられ得ることが分かる。

【００３２】

加えて、第１のテーブル１７８は、人－マシンインターフェース（ＨＭＩ）リソース２０６のリストにユーザ名のリスト１８０を関連付けることができる。画面ビュー１７４に表された実施形態では、ユーザ１４２は、「Ｃｏｏｌｉｎｇ、ＬｕｂｅＡおよびＰｕｍｐｌ」のラベルを付けられたＨＭＩリソースと関連付けられる。リストに記載されたＨＭＩリソースは、ユーザ１４２が制御システム１０へのアクセスを有するアイテムを含み得る。たとえば、ユーザ３　１４２は、Ｐｕｍｐｌで制御システムにアクセスすることができ得る。

【００３３】

開示される実施形態の技術的効果は、ＯＰＣ　ＵＡサーバ４０がＯＰＣ　ＵＡサーバ４０とＯＰＣ　ＵＡクライアント４６の間の通信のセキュリティを改善することを可能にすることを含む。具体的には、ＯＰＣ　ＵＡサーバ４０は、ＯＰＣ　ＵＡクライアント４６でユーザ５２をより効率的に識別し、ユーザ５２がメソッド呼出しを行うことを可能にするユーザ特権にユーザ５２を関連付けることができ得る。言い換えれば、ＯＰＣ　ＵＡサーバ４０は、誰がＯＰＣ　ＵＡクライアント４６上にあるかと、彼らが制御システム１０内で何を行うことができるかを判定することができる。

【００３４】

本明細書は、最良の形態を含めて本発明を開示するために、また、任意のデバイスまたはシステムの作成および使用と任意の組み込まれた方法の実行とを含めて、当業者が本発明を実施することを可能にするために、例を使用する。本発明の特許性のある範囲は、特許請求の範囲によって定義され、当業者が思い付く他の例を含み得る。そのような他の例は、それらが本特許請求の範囲の文字通りの文言と異ならない構造的要素を有する場合、またはそれらが本特許請求の範囲の文字通りの文言とごくわずかな差を有する同等の構造的要素を含む場合、本特許請求の範囲内にあるものとする。

【符号の説明】

【００３５】

１０　システム
１２　燃焼器
１４　タービン
１６　排気口
１８　ドライブシャフト
２０　圧縮機
２２　空気取り入れ口
２４　負荷
２６　電力網
３０　入口センサおよびフィールドデバイス
３２　出口センサおよびフィールドデバイス
３４　モジュールライン
３６　モジュールライン
３８　コントローラ
４０　ＯＰＣ　ＵＡサーバ
４１　内部ネットワーク接続
４４　ユーザ
４６　ＯＰＣ　ＵＡクライアント
４８　外部ネットワーク接続
４９　サーバ証明書
５０　アプリケーション証明書
５２　ユーザ

５４　データストア
５５　接続
５６　第１のマッピング
５８　第２のマッピング
６０　第３のマッピング
６１　アプリケーション証明書管理（ＡＣＭ）システム
６２　信頼されたストア
６４　信頼されたリスト
１３８　画面ビュー
１４０　証明書識別子セル
１４２　ユーザセル
１４４　ＯＰＣ　ＵＡサーバタブ
１４６　ＯＰＣ　ＵＡツリー制御
１４８　セキュリティ証明書ノード
１５０　ＯＰＣ　ＵＡクライアントノード
１５２　証明書識別子リストまたは欄
１５４　特権ユーザ名リストまたは欄
１５６　画面ビュー
１５８　証明書識別子
１５９　関連ユーザ名
１６０　クライアントの名
１６２　ラベル「会社ＡＢＣ　ＯＰＣ　ＵＡクライアント」
１６４　識別名（ＤＮ）
１６６　ラベル「ＣＮ＝会社ＡＢＣ　ＯＰＣ　ＵＡクライアント、ＯＵ＝アルファベット、Ｏ＝会社ＡＢＣ、Ｌ＝Ｌｅｔｔｅｒｖｉｌｌｅ、Ｓ＝ＮＹ、Ｃ＝ＵＳ」
１６８　サムプリント
１７０　ドロップダウンメニュー
１７２　ドロップダウンメニュー
１７４　画面ビュー
１７６　ユーザおよび役割ノード
１７７　ツリービューリスト
１７８　テーブル
１８０　ユーザ名
１８２　役割のリストまたは欄
１８４　オペレータ
１８６　第２のテーブル
１８８　ユーザ役割
１９０　ユーザ特権
１９２　ユーザ特権
１９４　ユーザ特権
１９６　ユーザ特権
１９８　ユーザ特権
２００　ユーザ特権
２０２　ユーザ特権
２０４　ユーザ特権

【図１】

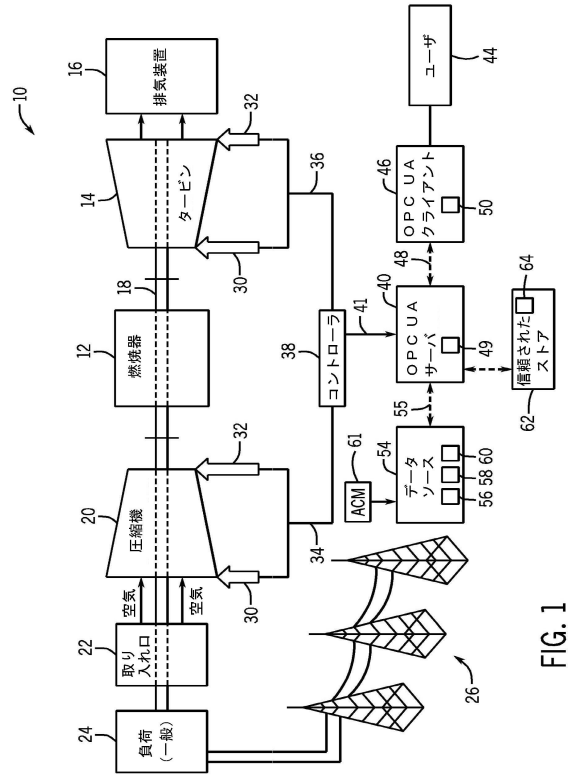


FIG. 1

【図２】

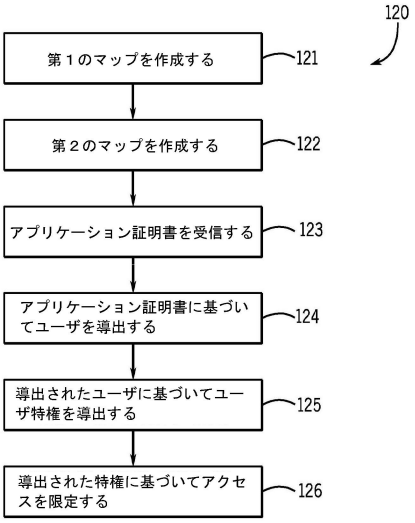


FIG. 2

【図３】

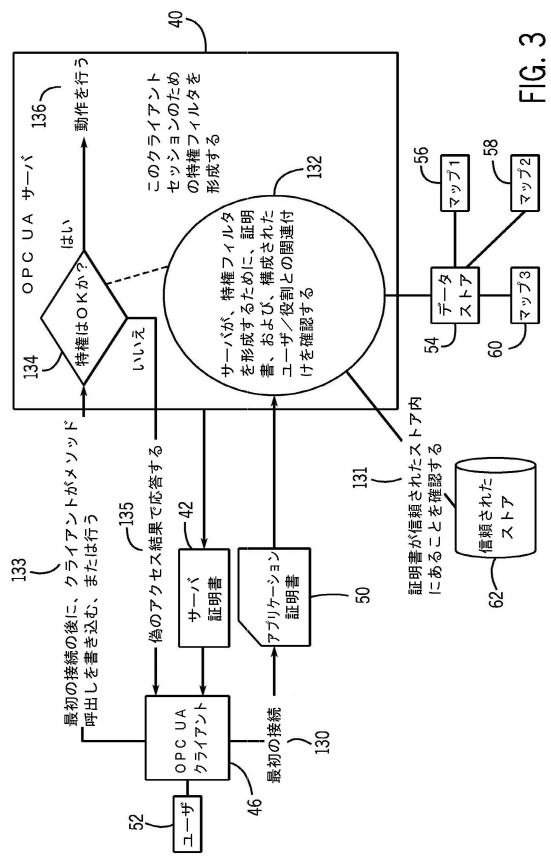


FIG. 3

【図４】

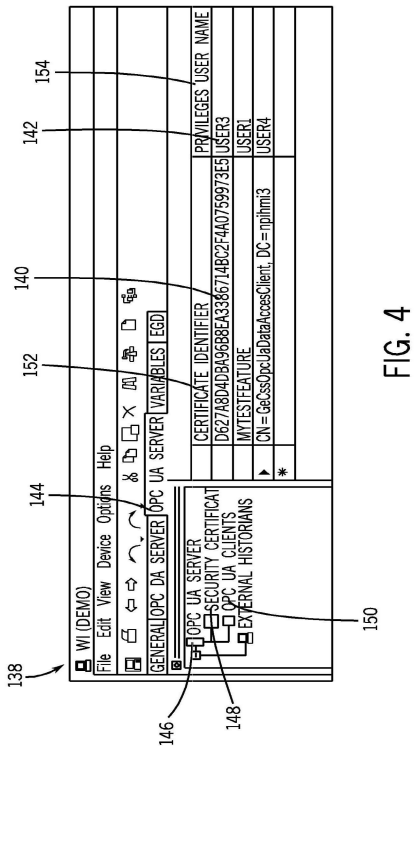


FIG. 4

【図５】

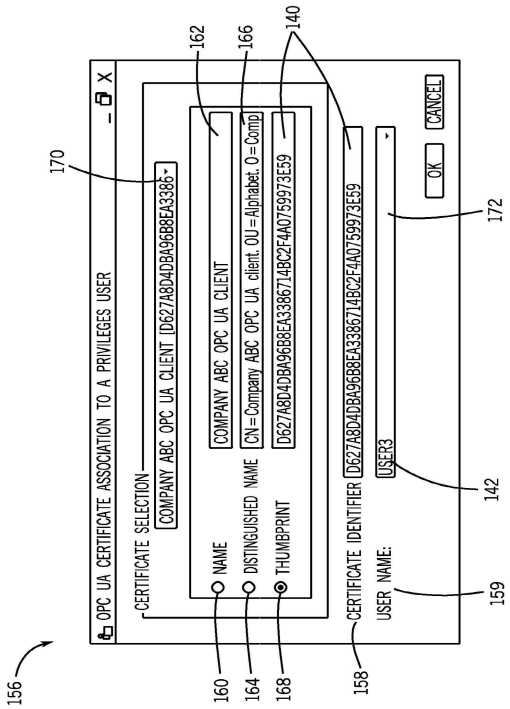


FIG. 5

【図６】

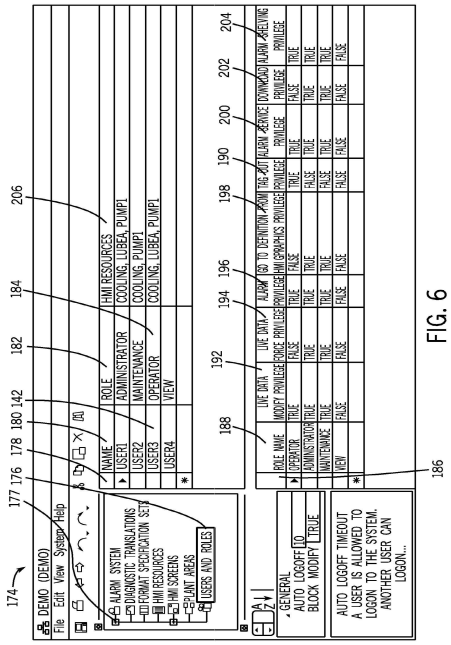


FIG. 6

フロントページの続き

(72)発明者　ショー，リチャード・ウィリアム
アメリカ合衆国、ヴァージニア州・２４１５３、セイラム、ロアノーク・ブールヴァード、１５０１番
(72)発明者　エマリー，ジェフリー・マーティン
アメリカ合衆国、ヴァージニア州・２４１５３、セイラム、ロアノーク・ブールヴァード、１５０１番

合議体
審判長　栗田　雅弘
審判官　小川　悟史
審判官　見目　省二

(56)参考文献　特開２０１１－２０４２３８（ＪＰ，Ａ）
特開２００２－１３５８６７（ＪＰ，Ａ）
特開２００５－１５７８４５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G05B 23/02