

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第4953609号
(P4953609)

(45) 発行日 平成24年6月13日 (2012. 6. 13)

(24) 登録日 平成24年3月23日 (2012. 3. 23)

(51) Int. Cl.

F I

G05B 19/418 (2006.01)
G06Q 50/04 (2012.01)
G06Q 10/00 (2012.01)

G05B 19/418 Z
G06F 17/60 106
G06F 17/60 512

請求項の数 13 外国語出願 (全 24 頁)

(21) 出願番号 特願2005-283949 (P2005-283949)
(22) 出願日 平成17年9月29日 (2005. 9. 29)
(65) 公開番号 特開2006-185416 (P2006-185416A)
(43) 公開日 平成18年7月13日 (2006. 7. 13)
審査請求日 平成20年7月31日 (2008. 7. 31)
(31) 優先権主張番号 10/955, 495
(32) 優先日 平成16年9月30日 (2004. 9. 30)
(33) 優先権主張国 米国 (US)

(73) 特許権者 503300421
ロックウェル オートメーション テクノ
ロジーズ, インコーポレーテッド
ROCKWELL AUTOMATION
TECHNOLOGIES, INC.
アメリカ合衆国 44124 オハイオ、
メイフィールド ハイツ、アレン-ブラッ
ドリー ドライブ 1
(74) 代理人 100066692
弁理士 浅村 皓
(74) 代理人 100072040
弁理士 浅村 肇
(74) 代理人 100091339
弁理士 清水 邦明

最終頁に続く

(54) 【発明の名称】 産業用オートメーションのためのスケーラブルで柔軟な情報セキュリティ

(57) 【特許請求の範囲】

【請求項 1】

産業用オートメーションのセキュリティに関連するセキュリティ・システムであって、
工場のフロア (102, 202, 302) の区域 (108, 208, 306, 410)
に関連するセキュリティ・ポリシーを修正するセキュリティ修正要求を受信する構成要素で
あって、前記区域 (108, 208, 306, 410) が前記工場のフロア (102, 2
02, 302) 全体より小さい前記構成要素と、

前記セキュリティ修正要求を解析して、前記要求に関係する区域 (107, 208, 3
06, 410) を動的に決定する動的区域生成装置 (304, 408) と、

前記要求に基づいて、前記区域 (108, 208, 306, 410) に特有のセキュリ
ティ・ポリシーを実施するためのセキュリティ手順を生成する区域セキュリティ構成要素 (106, 212, 308, 414) を備えた集中セキュリティ・システム (104, 204) と、

前記区域セキュリティ構成要素から前記セキュリティ手順を受信する産業用コントロー
ラ (404) であって、前記区域内に配置された産業用コントローラ (404) と、

少なくとも一部が所定のデータ・モデルで規定したポリシーに基づく制御・管理に関す
る要求を受信した場合に、前記集中セキュリティ・システム (104, 204) によって、
各区域毎に各セキュリティ手順が設定された分散型セキュリティ・モデルを制御・管理
することを容易にする自動要求生成装置 (406) とを備え、

前記自動要求生成装置 (406) が、前記産業用コントローラ (404) から、前記工

10

20

場のフロア（１０２，２０２，３０２）に設置されたデバイスに関連するアラームを受信すると、当該アラームに関連するセキュリティ修正要求を生成し（８０２，８０４）、

前記動的区域生成装置（３０４，４０８）が、前記区域（１０８，２０８，３０６，４１０）内に存在する前記デバイスを認識して、前記デバイスを含むように前記セキュリティ修正要求に関連する区域を動的に決定し（８０８）、

前記区域セキュリティ構成要素（１０６，２１２）が、前記セキュリティ修正要求に基づいて、決定した区域に修正セキュリティ手順を生成して実施する（８１０）ことにより、前記分散型セキュリティ・モデルの制御・管理を容易にすることを特徴とするセキュリティ・システム。

【請求項２】

前記生成したセキュリティ手順が、少なくとも一部は、前記既存のセキュリティ手順をベースとする、請求項１に記載のセキュリティ・システム。

【請求項３】

前記生成したセキュリティ手順が、少なくとも一部は、前記デバイスに関する前記区域セキュリティ構成要素（１０６，２１２）の認識をベースとする、請求項１に記載のセキュリティ・システム。

【請求項４】

前記セキュリティ手順が種々のレベルのデバイス認証（２１０）であって、工場フロア（１０２，２０２，３０２）上のデバイスや動作のひとつ以上を認証する前記デバイス認証（２１０）を含む、請求項１に記載のセキュリティ・システム。

【請求項５】

前記種々のレベルのデバイス認証（２１０）が、１つまたは複数のデジタル署名および証明書に基づいてなされる、請求項４に記載のセキュリティ・システム。

【請求項６】

前記セキュリティ手順が、ユーザに関連するコンテキスト情報に基づいて生成される、請求項１に記載のセキュリティ・システム。

【請求項７】

前記コンテキスト情報が、ユーザの識別、ユーザの位置、ユーザの役割、時刻およびユーザの行動のうちの少なくとも１つを含む、請求項６に記載のセキュリティ・システム。

【請求項８】

請求項１に記載の前記区域セキュリティ・システム（１０４，２０４）を備える集中セキュリティ・システム。

【請求項９】

工場のフロアの一部のためのセキュリティ手順を生成するための方法（５００）であって、

受信手段が、工場のフロア（５０２）に関連するセキュリティ・ポリシーを修正するためにセキュリティ修正要求を受信するステップ（５０４，６０４）と、

動的区域生成手段が、前記要求を解析して、少なくとも一部は前記セキュリティ修正要求に基づいて、前記工場のフロアの区域を動的に決定するステップ（５０６）と、

集中セキュリティ・システム（１０４，２０４）内の区域セキュリティ構成要素（１０６，２１２，３０８，４１４）が、少なくとも一部は前記要求に基づいて、前記区域に対するセキュリティ手順を生成するステップ（５０８）であって、前記要求に基づいて前記区域に特定の前記セキュリティ・ポリシーを実施するために前記セキュリティ手順を生成するステップ（５０８）と、

前記産業用コントローラ（４０４）が、前記区域セキュリティ構成要素からの前記セキュリティ手順を受信するステップと、

自動要求生成装置（４０６）が、少なくとも一部が所定のデータ・モデルで規定したポリシーに基づく制御・管理に関する要求を受信した場合に、前記集中セキュリティ・システム（１０４，２０４）によって、各区域毎に各セキュリティ手順が設定された分散型セキュリティ・モデルを制御・管理することを容易にするステップと、

10

20

30

40

50

前記自動要求生成装置（４０６）が、前記産業用コントローラ（４０４）から、前記工場のフロア（１０２，２０２，３０２）に設置されたデバイスに関連するアラームを受信すると、当該アラームに関連するセキュリティ修正要求を生成（８０２，８０４）するステップと、

前記動的な区域生成手段（３０４，４０８）が、前記区域（１０８，２０８，３０６，４１０）内に存在する前記デバイスを認識して、前記デバイスを含むように前記セキュリティ修正要求に関連する区域を動的に決定（８０８）するステップと、

前記区域セキュリティ構成要素（１０６，２１２）が、前記セキュリティ修正要求に基づいて、決定した区域に修正セキュリティ手順を生成して実施する（８１０）ことにより、前記分散型セキュリティ・モデルの制御・管理を容易にするステップと、

10

を含む方法。

【請求項１０】

前記セキュリティ手順を産業用コントローラに中継するステップをさらに含む、請求項９に記載の方法。

【請求項１１】

前記要求を入力および送信するオペレータを認証するステップ（７０４）をさらに含む、請求項９に記載の方法。

【請求項１２】

前記区域が、画定した区域のオペレータの選択に基づいて決定される（７０６）、請求項９に記載の方法。

20

【請求項１３】

前記工場のフロア上のデバイスをプロキシ・サーバと関連づけるステップ（６０２）と、
前記プロキシ・サーバを介して、前記デバイスに関する前記生成したセキュリティ手順を実施するステップ（６０８）とをさらに含む、請求項９に記載の方法（６００）。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、概して、産業用システム・オートメーションに関し、特に産業用システム内の工場のフロアのデバイスに関連するセキュリティに関する。

30

【背景技術】

【０００２】

技術の進歩により、多くの状況で多くの工場環境を部分的または完全に自動化できるようになり、そのため品質および効率の両方で出力が改善している。例えば、かつては自分達自身が重機および他の種々の危険な状況の近くにいないければいけなかった作業を今ではこのような危険から安全な距離のところで完全に行うことができる。さらに、人間の動作に関連する欠陥が、高度に精密な機械を使用することにより最小限度にまで軽減されている。これらの工場のデバイスの多くは、製造に関連するデータを工場のフロアにいるシステム／プロセス／プロジェクト・マネージャがアクセスすることができるデータベースに供給する。例えば、センサは、特定の機械が所与の設定した時間内にある動作を完了したことを何回でも検出することができる。さらに、センサは、データをシステムのアラームに関連する処理ユニットに配信することができる。それ故、工場用オートメーション・システムは、収集したデータをチェックし、デバイスの保守、デバイスの交換および生産工程の自動化に関連する他の種々の手順を自動的および／または準自動的に計画することができる。

40

【０００３】

産業用コントローラから収集したデータは、その後で工場に関連するハイレベルのシステムにより使用することができる。例えば、統合基幹業務（ERP；Enterprise Resource Planning）システムは、全製品スケジュールで、サブラ

50

イ・チェーン協調等を助長するために、産業用コントローラから入手したデータを使用することができる。E R Pシステムは、ビジネス／会社の作業または生産面に関連する多くのビジネス業務を統合し、自動化する情報管理システムである。通常、E R Pシステムは、相互機能的なもので企業全体を通して使用されるので、作業または生産に関連する機能的部署を1つのシステムに統合することができる。

【0004】

E R Pシステムは、実質的なセキュリティ機構に関連する。何故なら、E R Pシステムを実施するには、通常、かなりの量の資金および工数を必要とするからであり、会社はこの投資を保護したいと考える。例えば、E R Pシステムは、外部のソースからの攻撃からシステムを保護し、内部のユーザがE R Pシステム環境の外で内部の機械を操作するのを防止するためにファイアウォールを使用する。より詳細に説明すると、内部のユーザは、このようなシステムの外部でワークステーションを使用するためにシステムを操作することはできない。このような厳格なセキュリティ・ポリシーは、工場のフロア上のデバイスにとって最適なものとはいえない。工場のフロアのセキュリティ・システムは、主として不測の内部的セキュリティ違反から保護するために使用される。例えば、ユーザが偶発的に医薬品のレシピを変更した場合には、大きな災害をもたらす恐れがある。従来の工場のフロアのセキュリティ・システムは、セキュリティ違反を防止するためにグローバルなセキュリティ手段を使用する。より詳細に説明すると、保守の問題が発生した場合、またはレシピを変更した場合には、従来のセキュリティ・システムの場合には、工場の全フロアの作業を中止するか、セキュリティ・システムの保護は受けられない状態で作業を継続しなければならない。それ故、これらの工場のフロアのセキュリティ・システムを使用している場合には、生産が非効率的になるか、および／または動作環境が不安定になる。

【0005】

少なくとも上記の観点から、この業界においては、工場のフロアのデバイスと一緒に改良形のセキュリティ・システムを使用する必要がある。

【0006】

本発明のいくつかの態様を基本的理解してもらうために、以下に本発明の簡単な概要について説明する。この概要は本発明を広範な見地から見たものではない。この概要は、本発明の重要なまたは重大な要素を特定するためのものでもなければ、本発明の範囲を限定するためのものでもない。その目的は、単に、後のより詳細な説明の前置きとして簡単な形で本発明のいくつかのコンセプトを説明することである。

【発明の開示】

【発明が解決しようとする課題】

【0007】

本発明は、工場のフロア上で、ある区域のセキュリティの実施を容易にするシステムおよび／または方法を提供する。例えば、工場のフロア上においては、多くの場合、1つのデバイス、プロセス・セル、ユニット等に関するセキュリティ規定を修正することが望ましい場合がある。すでに説明したように、従来の工場のフロアのセキュリティ・システムは、柔軟なものではなく、工場の全フロアまたはその大部分のセキュリティを修正しなければならない。それ故、例えば、1つのサブプロセスのみをオフラインにし、デバッグしたい場合でも、このようなデバッグを容易にするために、工場の全フロアをオフラインにしなければならない。そのため、他のデバイス／プロセスの性能、処理能力およびセキュリティが悪影響を受ける。本発明を使用すれば、ある区域を指定／決定することができ、その場合は、工場の全フロアのセキュリティを修正しなくても、その区域のセキュリティを状況に応じて実施し、修正することができる。それ故、本発明は、工場のフロア上のアプリケーションをより効率的にし、より安全にする。

【課題を解決するための手段】

【0008】

本発明の1つの態様によれば、セキュリティ・システムは、工場のフロア（例えば、特定のデバイス、ユニット、プロセス・セル等）の一部に関する現在のセキュリティを修正

するようにとの要求を受信することができる。その後で、工場のフロアの一部を含むある区域を決定することができる。例えば、工場のフロアの表示内の区域を予め規定することができ、そのため工場のフロアの表示内の工場のフロアの対応する一部を選択する場合に、ある区域が自動的に決定される。さらに、工場のフロア上で行われた動作および／またはデバイスの発見に基づいて、区域を動的に決定することができる。例えば、あるデバイス用のアラームを解除すると、別のデバイスのアラームを必ずトリガすることになり、それ故、両方のアラームを解除することが望ましい。それ故、ある構成要素が、工場のフロアおよびその構成を意識しているので、ある区域を、好適に修正したデバイス、プロセス・セル、エリア、ユニット、サイト、動作、段階等に基づいて動的に決定することができる。

10

【0009】

本発明の区域セキュリティ・システムは、区域セキュリティ手順の生成および実施に関連して構造化データ・モデルを使用することができる。より詳細に説明すると、従来の産業用コントローラは、単にセンサおよびアクチュエータの状態を監視するだけで、データをハイレベルのシステム（例えば、ERPシステムおよび／またはMESシステム）により分析することができる構造化モデルに変換するにはミドルウェアが必要である。しかし、本発明は、工場のフロアの産業用コントローラおよびハイレベルのシステムの両方が、認識し、生成することができる構造化データ・モデルの使用を考えている。さらに、このデータ・モデルは、工場のフロアの表示の生成に関連して使用することができる。それ故、ミドルウェアを使用しなくても、産業用コントローラおよびハイレベルのシステムの両方へ／から直接データを送ることができる。さらに、区域セキュリティ手順は、これらの構造化データ・モデルを通して実施することができる。例えば、SP95およびS88は、本発明により構造化データ・モデルとして使用することができる2つの規格である。しかし、本発明に関連して任意の適当な構造化データ・モデルを使用することができ、これらのデータ・モデルも添付の特許請求の範囲内に含まれる。

20

【0010】

本発明の他の態様によれば、工場のフロアのデバイスをセキュリティ違反から保護するために、種々の認証技術を使用することができる。例えば、従来のユーザ名およびパスワードを、オペレータを識別し、このオペレータが要求したセキュリティの修正を確実に実施する許可を受けるために使用することができる。さらに、セキュリティの修正が受け入れられるものかどうかを判断するために、コンテキスト・データを分析することができる。例えば、特定のオペレータは、特定の時間および／またはプラントの位置でだけ、セキュリティを修正する許可を受けることができる。さらに、セキュリティを修正することができるかどうかを決定するために、現在の工場のフロアの動作を分析することができる。もう1つの例の場合には、それに関連する修正したセキュリティ手順を実施する前に、デバイスを認証することができる。より詳細に説明すると、セキュリティ修正が間違ったデバイスに送られると、大きな災害になる恐れがある。それ故、デジタル署名、簡単な鍵から複雑な鍵まで使用できる証明書のような種々のレベルのデバイスの認証を本発明に関連して使用することができる。

30

【0011】

上記および関連する目的を達成するために、本発明は、以下に詳細に説明し、特許請求の範囲内で詳細に指摘する機能を含む。下記の説明および添付の図面は、本発明のいくつかの例示としての態様を詳細に説明し、図示する。しかし、これらの態様は本発明の原理を使用することができる種々の方法の数例に過ぎず、本発明はこのようなすべての態様およびその等価物を含むものである。添付の図面を参照しながら、本発明の下記の詳細な説明を読めば、本発明の他の目的、利点および新規な機能を理解することができるだろう。

40

【実施例】

【0012】

図面を参照しながら以下に本発明について説明する。図面全体を通して、同様の参照番号は同様の要素を表すために使用してある。下記の説明においては、本発明を完全に理解

50

してもらうために、説明の目的で多くの特定の詳細を記述する。しかし、本発明は、これらの特定の詳細を使用しなくても実行することができることは明らかである。他の例の場合には、本発明の記述を分かり易くするために周知の構造体およびデバイスをブロック図の形で示してある。

【0013】

本明細書で使用する場合、「構成要素」、「ハンドラ」、「モデル」、「システム」等の用語は、ハードウェア、ハードウェアとソフトウェアとの組み合わせ、ソフトウェア、または実行中のソフトウェアのような、コンピュータ関連のエンティティを示すためのものである。例えば、構成要素は、プロセッサ上で稼働しているプロセス、プロセッサ、オブジェクト、実行可能なもの、一連の実行、プログラム、および／またはコンピュータであってもよいが、これらに限定されない。例を挙げて説明すると、サーバ上で稼働しているアプリケーションおよびサーバの両方は1つの構成要素であってもよい。1つまたは複数の構成要素は、プロセスおよび／または一連の実行内に常駐することができ、構成要素は1つのコンピュータ上で使用することもできるし、および／または2つ以上のコンピュータ間で分散することもできる。また、これらの構成要素は、その上に記憶している種々のデータ構造体を有する種々のコンピュータが読むことができる媒体から実行することができる。構成要素は、1つまたは複数のデータ・パケット（例えば、信号により、ローカル・システム、分散システム内および／または他のシステムを含むインターネットのようなネットワークに渡って他の構成要素と相互に作用する1つの構成要素からのデータ）を含む信号によるように、ローカルおよび／または遠隔プロセスを介して通信することができる。

【0014】

ここで図面を参照すると、図1は、本発明のある態様に関連するハイレベルのシステムの全体図である。本発明は、工場のフロアのデバイスに関するスケーラブルで柔軟なセキュリティ・システムの実施を容易にする新規なシステム100に関する。システム100は、1つまたは複数の動作、段階等を完了するために使用するデバイスを備える工場のフロア102を含む。工場のフロア102は、セキュリティ要求を受信するセキュリティ・システム104と関連する。例えば、セキュリティ要求は、ユーザから、センサとユーザとの組み合わせから、センサだけから、ソフトウェアから、またはセキュリティ要求を生成することができる任意の他の適当な方法から行うことができる。システム100は、産業用システムと一緒に使用する従来のセキュリティ・システムでは得られないセキュリティの利益を提供する。より詳細に説明すると、多くの場合、保守、試験、デバッグ、再作動等は、工場のフロアのデバイス、部材、システム、プロセス等のところで行うことが望ましい。従来のセキュリティ・システムは、産業用システムの一部だけが好適にセキュリティ・システムから切り離された場合でも、または好適にセキュリティ・システムの修正内に位置している場合でも、セキュリティ・システム全体が動作不能になったり、または修正しなければならないという点で柔軟性に欠けていた。

【0015】

システム100は、ある区域108に対してセキュリティ手順を実施するために、工場のフロア102からその区域108を分離することができる区域セキュリティ構成要素106を使用することにより上記欠点を緩和する。区域108は、特定のデバイスまたはデバイスの組、プロセス、部材または一連の部材、ユニット、動作、エリア、または工場のフロアの任意の他の適当な区域であってもよい。より詳細に説明すると、区域108は、医薬品用の生産プロセスの完了に関連して使用する混合動作を表すことができる。セキュリティ・システム104は、通常、製造中の医薬品に悪影響を与える恐れがあるプロセスへの偶発的な変更を避けるために、混合動作（例えば、区域108）にユーザ／オペレータがアクセスおよび／または修正できないようにする。従来は、オペレータがデバッグのために混合動作にアクセスすることができるようにするために、セキュリティ・システム104を、工場の全フロア102に対して動作不能にした。このようなグローバルな動作停止を行うと、工場のフロア102が、悪意のあるオペレータまたは単純なミスによる内

部的セキュリティ違反の影響を受けることになる。本発明を使用すれば、区域セキュリティ構成要素106は、区域108を工場のフロア102から分離することができ、工場のフロア102の残りの部分に関するセキュリティを変更しないで、区域108に関連するセキュリティ手順を提供することができる。それ故、工場のフロア102上の他のデバイス、プロセス・セル、エリア、サイト等のセキュリティに悪影響を与えないで、区域108に対して保守動作等を行うことができる。セキュリティ手順を、任意の適当なデータ送信システム／方法により、セキュリティ・システム104から区域108に送信することができる。例えば、セキュリティ手順を無線でおよび／または有線接続を通して送信することができる。

【0016】

本発明の1つの態様によれば、工場のフロア102上に常駐する産業用コントローラ（図示せず）は、区域108のセキュリティに関連する適当な行動を行うために、セキュリティ・システム104および区域セキュリティ構成要素106と通信することができる。例えば、好適に試験および／またはデバッグの対象になるあるセル／ユニットまたは手順を制御するために、産業用コントローラを使用することができる。より詳細に説明すると、産業用コントローラは、上記手順および／またはセル／ユニットを実行するために使用する制御論理の少なくとも一部を含む。このような手順のデバッグに対する要求は、セキュリティ・システム104に送ることができ、区域セキュリティ構成要素106は、セル／エリア／手順およびそれらに関連するデバイスを制御するために使用する（ひとつまたは複数の）産業用コントローラの位置を決定することができる。次に、区域セキュリティ構成要素106は、（ひとつまたは複数の）産業用コントローラと（ひとつまたは複数の）関連するデバイスとだけに関連するセキュリティおよび発行セキュリティ手順に関して工場のフロア102から（ひとつまたは複数の）産業用コントローラおよび（ひとつまたは複数の）関連するデバイスを効果的に分離することができる。例えば、これらの手順は、オペレータに制御論理へのアクセスを提供する前にアラームを一時解除し、保守、デバッグ、試験等に関連する動作が完了した場合に安全回路をリセットするステップを含むことができる。

【0017】

区域108の少なくとも一部である産業用コントローラは、プログラマブル論理コントローラ（PLC）であってもよい。PLCは、現実の世界のプロセス（例えば、産業環境での機械の制御）を自動化するために使用する小型コンピュータである。通常、PLCは、モジュラ型または一体型入出力回路を含むマイクロプロセッサをベースとするデバイスである。このような回路は、フィールド接続センサ入力の状態を監視するために使用され、さらに論理プログラムにより出力アクチュエータを制御するために使用される。PLCはシステム100で産業用コントローラとして使用されるが、任意の適当な産業用制御デバイスも、本発明と一緒に使用することができることを理解されたい。例えば、任意の適当なマイクロプロセッサおよび／またはマイクロコントローラを、システム100で産業用コントローラとして使用することができる。

【0018】

本発明のさらに他の態様によれば、セキュリティ・システム104は、工場のフロア102上のインテリジェント・デバイスと直接通信することができる。従来の産業用オートメーション・システムは、ハイレベルの産業用オートメーション・システムと工場のフロア102との間の通信を容易にするためにミドルウェアを使用する。このようなハイレベルの産業用オートメーション・システムは、統合基幹業務（ERP；Enterprise Resource Planning）システムおよび生産実行システム（MES；Manufacturing Execution System）を含むが、これらに限定されない。従来の工場のフロアのデバイスは、センサおよびアクチュエータの状態を監視し、それ故「1」と「0」のストリングの形でデータを入手し記憶するだけであったが、ハイレベルのオートメーション・システムは、構造化データ・モデルを使用する。しかし、本発明は、ハイレベルのオートメーション・システム（例えば、セキュリティ・シ

10

20

30

40

50

システム104を実施するために使用するシステム)で使用するような工場のフロア102(例えば、産業用コントローラ)上のインテリジェント・デバイス内でのほぼ類似のデータ・モデルの使用を考えている。それ故、セキュリティ・システム104(および区域セキュリティ構成要素106)は、十分な処理および記憶機能と関連している工場のフロア102上のデバイスと直接通信することができる。工場のフロアのデバイスおよびハイレベルのシステムに共通のデータ・モデルと一緒に使用することができる2つの例示としての規格は、S88およびSP95である。S88は、バッチ処理アプリケーション用に主として使用する規格であり、SP95は、プラントの階層的表示を生成するための機構を提供する規格である。これら2つの規格の間には、プラントおよびプラント内で行う動作を十分に表すデータ・モデルを生成することができる。S88およびSP95は、本発明と一緒に使用することができる2つの規格であるが、本発明者が、任意の構造化データ・モデルを考慮の対象にしたこと、すべての適当なデータ・モデルは、添付の特許請求の範囲に含まれることを理解されたい。直接通信を行うことにより、区域セキュリティ手順のある区域の効率的な決定および効率的な実施が容易になる。

10

【0019】

さらに、工場のフロア上のインテリジェント・デバイスおよびハイレベルのシステムの両方が使用する共通なデータ・モデルにより、分散型セキュリティ・モデルを自動的に統合することができる。例えば、相手先商標による製造会社(OEM)の機械で使用する局在化セキュリティ・モデルを、エンド・ユーザのサイトの集中セキュリティと統合することができる。より詳細に説明すると、共通のデータ・モデルで定義したポリシーは、この

20

【0020】

ここで図2を参照すると、この図は、区域セキュリティ手順の生成およびその実施を容易にするシステム200を示す。システム200は、セキュリティ・システム204により動作する工場のフロア202を含む。例えば、セキュリティ・システム204は、確実に安全スイッチが正しく設定されて、アラームおよび他の通常のセキュリティ手段が動作できるようにするために使用することができる。システム200は、さらに、工場のフロア202に関連して存在するデバイス、プロセス・セル、エリア等を表す産業用システム表示206を含む。例えば、システム表示206は、プラントおよび/または工場のフロア202の階層的表示を含むことができる。さらに、システム表示206は、工場のフロア202で行われる手順/プロセスの表示を含むことができる。例えば、食品を製造するために使用する手順およびサブ手順をシステム表示206内に表示することができる。

30

【0021】

システム表示206は、1つまたは複数のデバイス、プロセス・セル、エリア、サイト等に関連するセキュリティ要求を受信する。例えば、ヒューマン・マシン・インタフェース(HMI)または他の適当なグラフィカル・ユーザ・インタフェースを通して、オペレータは、工場のフロア202内の特定の区域208に関連するセキュリティ要求を生成することができる。より詳細に説明すると、オペレータは、区域208に関連する特定のセキュリティ手順/デバイスの動作停止/修正を要求することができる。それ故、オペレータは、システム表示206内の工場のフロア202上で実施する手順のグラフィカルな表示を見ることができ、手順に関するセキュリティ関連の要求をシステム表示206に送ることができる。その後で、セキュリティ要求をセキュリティ・システム204に送ることができ、セキュリティ・システム204は、セキュリティ要求を行っているオペレータが、要求に関連するセキュリティ手順の実行を許可されているかどうかを判断することができる。このことは、ユーザ名、パスワード、ユーザの役割、プラントの位置、時刻、曜日、要求により実行したデバイス、要求により行った手順、または任意の他の適当なセキュリティ関連の要因のような表示に基づいて、許可の決定を行うことができる認証構成要素210により行うことができる。さらに、セキュリティ・システム204は、認証アルゴリズムおよび関連するデータを記憶し、実行するために、セキュリティ・サーバ(図示せず)等を使用することができる。本発明の1つの態様によれば、指紋、網膜走査、音声認

40

50

識技術等のような生物測定属性を、オペレータの認証と一緒に使用することができる。それ故、認証構成要素 210 は、許可に関連するものだけを、工場のフロア 202 と関連している場合に、セキュリティ・システム 204 のポリシー／手順を修正することができるようにすることにより、追加のセキュリティ層を提供する。

【0022】

オペレータ／ユーザが、デバイス、デバイスの組、プロセス・セル、エリア、サイト等に関する現在のセキュリティ手順を修正する許可を受けている場合には、要求は区域セキュリティ構成要素 212 に送られる。次に、区域セキュリティ構成要素 212 は、区域 208 に対するセキュリティ手順を生成することができる。この場合、区域 208 は最初の要求に関連する。より詳細に説明すると、要求が、装置の特定の部分のアラームの解除に 10
関連している場合には、区域 208 はこのようなプロセスからなるデバイスを含むことができる。それ故、従来のセキュリティ・システムで要求されるように全工場のフロア 202 に関連しているのではなく、特定のデバイス、プロセス・セル、エリア等に関連するセキュリティ手順を実行するために、区域セキュリティ構成要素 212 を使用することができる。

【0023】

本発明の他の態様によれば、区域セキュリティ構成要素 212 が生成したセキュリティ手順が、区域 208 内の（ひとつまたは複数の）適当なデバイスに確実に送られるように 20
認証構成要素 210 を使用することができる。例えば、区域セキュリティ構成要素 212 は、好適には、医薬品のための混合動作と一緒に使用するデバイスに関連するアラームを解除することができる。その後で、アラームを解除するために実際にコマンドを供給しているデバイスが、好適には、コマンドを供給しているデバイスであることを確認するために、認証構成要素 210 を使用することができる。異なるデバイスがアラーム解除コマンドまたは他のセキュリティ関連命令を受信した場合には、非常に重大な結果が起こる（例えば、アラームが作動しないために、間違った医薬品ができる）。それ故、認証構成要素 210 は、種々のレベルのデバイス認証をサポートする。例えば、認証は、デジタル署名および証明書を使用することができるが、これらに限定されない。この場合、鍵および暗号化は 1 つの産業用オートメーション企業内で簡単なものから複雑なものにわたる場合がある。今まで、工場のフロア 202 上のオペレータおよびデバイスの両方の認証に関連して 30
認証構成要素 210 を説明してきたが、このような認証のために別の構成要素を使用することができることを理解されたい。

【0024】

ここで図 3 を参照すると、この図は、工場のフロア 302 の一部へのセキュリティ手順の提供を容易にするシステム 300 を示す。工場のフロア 302 は、製造プロセスのために使用する複数のデバイスを含む。動的区域生成装置 304 は、工場のフロア 302 の一部に関連するセキュリティを修正するための要求を受信する。例えば、セキュリティ修正要求は、特定のデバイス、プロセス・セル、エリア、サイト等の試験、デバッグ、保守等と関連を持つことができる。要求に基づいて、動的区域生成装置 304 は、このような工場のフロア 302 の現在の構成を決定するために、工場のフロア 302 またはその表示に 40
問い合わせを行うことができる。決定した構成に基づいて、動的区域生成装置 304 は、セキュリティ修正を行う区域 306 を生成することができる。動的区域生成装置 304 の動作をはっきり理解するには特定の例が役に立つ。オペレータは、そのようなデバイス上で保守を行うために、特定のデバイスに対するアラームを解除することを要求する。動的区域生成装置 304 は、この要求を受信し、そのデバイスに関連する工場のフロア 302 の構成を決定する。より詳細に説明すると、動的区域生成装置 304 は、デバイス、相互接続しているデバイス、関連デバイス等を含む動作に関連する情報を入手する。例えば、デバイスの停止動作およびアラームの解除は、異なるデバイスに関連する異なるアラームをトリガしてもよい。それ故、他の関連するアラームも解除しなければならない。動的区域生成装置 304 は、特にデバイスの現在の構成および全体的な工場のフロア 302 に基づいて、どのアラームを解除するのかを決定することができる。 50

【0025】

区域306を動的に生成した場合、セキュリティ要求および関連区域情報を、工場のフロア302に関するセキュリティを提供するために使用するセキュリティ・システム310内の区域セキュリティ構成要素308により受信することができる。その後、区域セキュリティ構成要素308は、区域306に対するセキュリティ手順を供給することができる。例えば、セキュリティ手順は、保守のためにアラームを解除することと、その後、保守が完了した場合に安全スイッチをリセットすることを含むことができる。手順実行構成要素312は、区域306内でのデバイス／動作の再初期化の前に、すべての適当なセキュリティ手順がコンパイルされたことを確認する。例えば、区域セキュリティ構成要素308が生成したセキュリティ手順がコンパイルされない場合には、手順実行構成要素312は、区域306が通常の動作に復帰するのを禁止する。手順実行構成要素312は、必要な手順および他の適当な実行機構をオペレータにリマインドさせるために、アラーム、グラフィカル・ユーザ・インタフェースと関連づけることができる。

10

【0026】

ここで図4を参照すると、この図は、工場のフロア402の一部のためにセキュリティ手順の実施を容易にするシステム400を示す。工場のフロア402は、センサおよびアクチュエータの状態を監視することができ、工場のフロア402内で行われる製造プロセスの制御に関連して使用することができる産業用コントローラ404を含む。データのこの収集に基づいて、コントローラ404は、自動要求生成装置406によりセキュリティ要求に変換することができるアラームまたは同様の表示を生成することができる。例えば、コントローラ404がアラームを供給した場合には、自動要求生成装置406は、コントローラ404に関連するアラームを解除するための要求を生成することができる。

20

【0027】

次に、セキュリティ手順を適用する工場のフロア402内のある区域410を決定することができる動的区域生成装置408に、セキュリティ要求を送ることができる。例えば、動的区域生成装置408は、工場のフロア402に問い合わせを行い、コントローラ404（例えば、コントローラ404により制御されるデバイスおよび／または動作）の構成を決定することができる。このような決定に基づいて、動的区域生成装置408は、区域410が他のコントローラ、デバイス等を含むことができるこのようなコントローラ404を含む区域410を生成することができる。本発明の他の態様によれば、工場のフロア402は予め複数の区域に分割されている。それ故、動的区域生成装置408は、コントローラ404を含む正しく画定された区域410の位置を決定するだけでよい。区域410を決定および／または生成した場合には、工場のフロア402をセキュリティ状態にするために動作するセキュリティ・システム412は、要求および対応する区域410を受信し、区域セキュリティ構成要素414は、区域410に関連するセキュリティ手順を生成する。例えば、区域410は、製造動作に関連して使用するコントローラ404により制御される複数のデバイスを含むことができる。区域セキュリティ構成要素414が生成したセキュリティ手順は、アラームの解除、セキュリティ・スイッチの設定、セキュリティ・スイッチのリセット、および他の適当なセキュリティ関連手順と関連づけることができる。

30

40

【0028】

図5を参照すると、この図は、工場のフロアの一部内だけでセキュリティ手順を実施するための方法500を示す。説明を簡単にするために、方法500を一連の行動として図示し、説明するが、本発明は動作の順序により制限されないことを理解し、了解されたい。何故なら、本発明によれば、いくつかの動作は、異なる順序で行うこともできるし、および／または本明細書内に図示し、説明するのは異なる他の行動と同時に行うことができるからである。例えば、当業者であれば、別の方法としては、この方法を状態図に示すような一連の相互に関連する状態またはイベントで表すことができることを理解し、了解することができるだろう。さらに、本発明による方法を実施するのに、図のすべての動作を必要としない場合がある。

50

【0029】

ステップ502において、工場のフロア表示が提供される。例えば、ユーザがこのような表示を見ることができるよう、工場のフロア表示をグラフィカル・ユーザ・インタフェースまたはHMI上に表示することができる。さらに、SP95規格および／またはS88規格を工場のフロアの表示と一緒に使用することができる。それ故、工場のフロアの階層的表示を再現することができる。階層はプラントのフロアのアプリケーションにより論理的に生成される。さらに、バッチ処理アプリケーション（例えば、レシピの記述）を表示するために、データ・モデルを使用することができる。組合わせて使用する場合には、工場のフロアの完全な表示を生成することができる。例えば、デバイスを工場のフロア表示内の異なるデバイスと関連づけることができ、このようなデバイスを製造アプリケーションを完成する目的で、連結して作動するために表示することができる。これら上記の規格は、システム表示の生成に関連して使用することができるが、任意の適当なデータ・モデルは、工場のフロア表示の提供と一緒に使用することもできることを理解されたい。

10

【0030】

ステップ504において、セキュリティ修正の要求を受信する。要求はデバイス装置のオペレータにより生成することもできるし、および／または1つまたは複数のインテリジェント工場のフロアのデバイス（例えば、産業用コントローラ）により自動的に生成することもできる。例えば、デバイスの保守作業をいつ行うのかを決めるためにタイマを使用することができる。デバイスを保守する時期がきていることを感知した場合には、産業用コントローラまたは他のインテリジェント工場のフロアのデバイスは、保守を行うデバイスに関連するアラームを解除する要求を生成することができる。オペレータは、産業用コントローラでロジックを試験またはデバッグしている時に、特定のデバイスまたはデバイスの組に対するアラームを解除するように要求することができる。例えば、オペレータは、親プロセス用のレシピのセキュリティに悪影響を与えないで、サブプロセス用の制御プログラムの試験を希望することができる。それ故、オペレータは、このような修正に対する要求を生成することができる。

20

【0031】

ステップ506において、修正要求に関連する区域が決定される。例えば、オペレータは、どの（ひとつまたは複数の）デバイス、（ひとつまたは複数の）動作、アプリケーション等が要求に関連する区域を形成するのかを正確に指定することができる。本発明の他の態様によれば、工場のフロアの修正は、画定した区域を含むことができる。画定した区域のうちの1つまたは複数を要求に関連する（ひとつまたは複数の）区域として選択することができる。このような区域の選択は、オペレータにより自動的に完了することもできるし、指定することもできる。さらに、工場のフロアの構成および要求に基づいて、区域を動的に決定することができる。例えば、オペレータは、産業用コントローラに関連する特定のセキュリティ修正を要求することができる。この場合、産業用コントローラに関するこのような要求を実施すると、他の関連するデバイスを異常に操作することになり得る。それ故、これらのデバイスに関するセキュリティ手順も修正しなければならない。それ故、要求および工場のフロアの構成に基づいて、適当な区域を自動的に決定することができる。

30

40

【0032】

ステップ508において、決定した区域のセキュリティが修正される。例えば、このような区域を決定した場合に、決定した区域特有のセキュリティ手順を生成および実施することができる。これにより、全工場のフロアのセキュリティに悪影響を与えないで、特定のデバイス、デバイスの組、手順、アプリケーション等を試験、デバッグ、保守、診断、再起動等することができる。このような区域セキュリティにより、他のデバイスまたは動作のセキュリティに影響を与えないで、特定の動作またはデバイスをセキュリティ・システムから抽出することができる。

【0033】

ここで図6を参照すると、この図は、実質的なインテリジェンスを備えていないプラン

50

トのフロアのデバイスに区域セキュリティ手順を提供するための方法600を示す。ステップ602において、1つまたは複数の工場のフロアのデバイスがプロキシ・サーバと関連づけられる。工場のフロアの複数のデバイスは、好ましくは、あるプロキシ・サーバと関連づけることができる。何故なら、このようなデバイスのうちのいくつかは、実質的なインテリジェンスおよび／または処理能力を備えていないからである。それどころか、このようなデバイスは、通常、1つの動作に最適化されていて、通常、実質的なインテリジェンスおよび／または処理能力を必要としない。それ故、工場のフロアのデバイスに関する処理機能および／または記憶機能は、セキュリティの基本的な事項を記憶し、操作するのに十分なものではない。しかし、本発明の態様によれば、このようなデバイスにはプロキシ・サーバを通してアクセスし、通信することができる。それ故、オペレータおよび／または構成要素が、このようなデバイスにアクセスし、またはそれを使用するためには、プロキシ・サーバを使用しなければならない（例えば、プロキシ・サーバを通るすべての通信チャネル）。それ故、プロキシ・サーバを使用することにより複数のデバイスを統合することができ、その後で、プロキシ・サーバは、このような工場のフロアのデバイスにセキュリティを提供することができる。

10

【0034】

ステップ604において、十分なインテリジェンスを備えていない工場のフロアのデバイスに関するセキュリティ修正のための要求を受信する。例えば、特定の産業用コントローラを十分な量の処理機能および／またはメモリと関連づけることはできないかもしれない。それ故、その中にセキュリティの基本的事項を記憶し、実施するのが実際上無理になるか、不可能になる。しかし、例えば、産業用コントローラにより制御されているデバイスの保守を行うために、このような産業用コントローラに関連するアラームを解除することが望ましい場合もある。それ故、ステップ606において、要求されたセキュリティ修正は、上記プロキシ・サーバを介して1つまたは複数の工場のフロアのデバイスに送られる。プロキシ・サーバは、セキュリティ特権を記憶し、実施し、その後で1つまたは複数のデバイスに区域セキュリティ手順を送り／実施するのに十分なメモリおよび／または処理機能と関連している。ステップ608において、区域セキュリティ手順が、要求に従って実施される。例えば、区域セキュリティ手順を、プロキシ・サーバを通して通信するすべてのデバイスに適用することができる。本発明の他の態様によれば、プロキシ・サーバを介して通信する1つまたは複数のデバイス上でセキュリティ手順を選択的に実施するために、プロキシ・サーバを使用することができる。

20

30

【0035】

ここで図7を参照すると、この図は、区域セキュリティ手順を生成し、実施するための方法700を示す。ステップ702において、特定のデバイス、アプリケーション、手順、デバイスのグループ等に関連するセキュリティ修正に対する要求が図示される。例えば、好ましくは、操作に関連する制御論理を試験することができる。それ故、このような制御論理を使用する産業用コントローラに関連するセキュリティを、オペレータがこのような制御論理を効果的に試験できるように緩和しなければならない。本発明の1つの態様によれば、要求はオペレータにより始動または許可される。ステップ704において、要求に関連するオペレータが認証される。例えば、ユーザ名およびパスワードのような従来の認証技術を使用することができる。さらに、ユーザの認証に関連して人工知能技術を使用することができる。

40

【0036】

本明細書で使用する場合、「推論する」または「推論」という用語は、通常、イベントおよび／またはデータにより入手する一組の観察から、システム、環境および／またはユーザの状態を推理または推論するプロセスを意味する。推論は、特定のコンテキストまたは行動を識別するのに使用することができ、または例えば、状態についての確率分布を生成することができる。推論は見込みに基づくものであってもよい。すなわち、データおよびイベントの考慮に基づく問題の状態についての確率分布の計算であってもよい。推論は、一組のイベントおよび／またはデータから、もっと高いレベルのイベントを構成するた

50

めに使用する技術を参照することもできる。このような推論により、イベントが時間的に近接して相互に関連していてもいなくても、イベントおよびデータが1つまたはいくつかのイベントおよびデータ・ソースからのものであってもなくても、一組の観察したイベントおよび／または記憶しているイベント・データから新しいイベントまたは行動を構成することができる。例えば、あるオペレータに関連するコンテキスト・データに基づいて、上記オペレータが特定の区域に関連するセキュリティにアクセスおよび／または修正する許可を受けているかどうかを決定することができる。それ故、特定のオペレータは、特定の時間、デバイス手順、オペレータの位置等を与えられた特定のデバイスの修正の許可だけを受けることができる。それ故、工場のフロア、区域および／またはオペレータに関連するコンテキスト・データを使用することにより、種々の許可の推論を行うことができる。

10

【0037】

ステップ706において、ステップ702において受信した要求に関連する区域が決定される。この区域は、インテリジェント構成要素により動的に決定することができ、または既知のエリア、手順、デバイス、サイト、プロセス・セル等により予め規定することができる。ステップ708において、すでに説明したように、決定した区域に対するセキュリティ手順が生成され、実施される。本発明の1つの態様によれば、工場のフロアのデバイス（例えば、産業用コントローラ）およびハイレベルのシステム（例えば、ERPシステムおよびMESシステム）両方が生成し、理解することができる共通のデータ・モデルを、区域セキュリティ手順の生成および実施を容易にするために使用することができる。

20

【0038】

ここで図8を参照すると、この図は、このような要求に基づいて、自動的にセキュリティ修正要求を生成し、区域セキュリティ手順を実施するための方法800を示す。ステップ802において、工場のデバイスに関連するアラームを受信する。例えば、プレス、ポンプ、鋸等のようなデバイスは故障する恐れがあり、その場合、産業用コントローラはアラームを発生する。さらに、1つまたは複数のセンサが、製品が間違った組成を有していることを感知した場合にはアラームを発生する。上記はアラームの発生の簡単な特定の例であり、方法800に関連して任意の適当なアラームを受信することができることを理解されたい。ステップ804において、アラームを受信すると、セキュリティ要求が自動的に生成される。例えば、アラームが特定のデバイスに関連している場合には、そのデバイス

30

【0039】

ステップ806において、セキュリティ要求に関連するオペレータの承認を受信する。このようなオペレータの承認は、誤警報の発生を低減する。例えば、故障したセンサがアラームを発生する恐れがある。それ故、故障したセンサに基づいて動作に関連するセキュリティを動作不能にするのは効率的でない。セキュリティを修正する前にオペレータがセキュリティ要求を承認することができるようにすることにより、セキュリティを修正する前にセンサの故障を判断することができる。ステップ808において、オペレータの承認を受けると、セキュリティ要求に関連する区域が決定される。それ故、アラームがあるデバイスからのものである場合には、そのデバイスを含む区域を決定することができる。さらに、そのデバイスを使用する動作を区域であると見なすことができる。ステップ810において、決定した区域に対するセキュリティ手順をその区域内で生成し、実施することができる。

40

【0040】

ここで図9を参照すると、この図は、本発明と一緒に使用することができる例示としての工場のフロアの表示900を示す。この表示900は、特定の工場のフロアの階層的表示である。階層の一番高いレベルには、フォルダ902またはプロセス・セルの図形表示が位置する。プロセス・セルは、1つまたは複数のバッチ動作と一緒に使用する装置を含む装置の論理的グループである。プロセス・セルを階層の上部に示してあるが、プロセス・セルは、企業、サイト、エリア等内の表示に含ませることができることを理解されたい

50

。例示としての表示900によれば、プロセス・セル・フォルダ902を、このようなプラント・プロセス内の特定のユニットを表示するために拡張することができる。より詳細に説明すると、プラントは、第1のユニットを示すフォルダ904、第2のユニットを示すフォルダ906、およびM番目のユニットを示すフォルダ908を含む。Mは整数である。ユニットは、制御モジュールおよび／または機器モジュールおよび1つまたは複数の処理活動を行うことができる他の装置の集合体として規定されてもよい。

【0041】

図のフォルダ906は拡張されていて、第1の機器モジュールを示すフォルダ910、第2の機器モジュールを示すフォルダ912、およびN番目の機器モジュールを示すフォルダ914を含む。Nは整数である。機器モジュールは、有限の数の特定の動作を実行することができる装置の機能グループであってもよい。フォルダ912は拡張されていて、図では、それぞれ制御モジュール1および制御モジュール2の表示916および918を含む。図では、プロセス・セル、ユニット1～M、および機器モジュール1～Nはフォルダになっているが、本発明と一緒に任意の適当な階層的表示を使用することができることを理解されたい。さらに、詳細には示していないが、表示900は、特定の動作ステップ、レシピおよび他のバッチ製造情報の表示を含むことができ、SP95規格およびS88規格により生成されてもよい。

【0042】

本発明によれば、フォルダ902～914のうちの任意のフォルダを、区域セキュリティ修正を実施するための区域として選択することができる。例えば、オペレータが全プロセス・セルに関連するセキュリティを修正したい場合には、このようなオペレータは、プロセス・セルに関するこのような修正の生成および実施に関連してフォルダ902を選択することができる。同様に、オペレータが特定のユニット、機器モジュールまたは制御モジュールに関して、区域修正を生成したい場合には、オペレータは、このような区域手順修正を行うために、工場のフロア表示900内の対応する表示を選択することができる。

【0043】

ここで図10を参照すると、この図は、オートメーション環境内のアプリケーション／動作の他の例示としての階層的表示1000を示す。表示1000は、それぞれ第1のレシピ手順および第2のレシピ手順を表すフォルダ1002および1004を含む。レシピ手順は、バッチ製品のレシピの全体である。それ故、工場のフロア上で複数のレシピ手順を使用することができる。フォルダ1004は、第1のユニット手順、第2のユニット手順、およびM番目のユニット手順を表すフォルダ1006～1010を示すために拡張されている。なお、Mは整数である。ユニット手順は、特定のユニットに関して実行される一組の手順であると規定することができる。それ故、1つのレシピ手順を複数のユニット手順と関連づけることができる。第1の動作およびN番目の操作を表すフォルダ1012および1014を示すために、フォルダ1008は拡張されている。なお、Nは整数である。操作は、各段階の始動、編成および制御のために使用する（ひとつまたは複数の）アルゴリズムからなる独立の処理活動であると規定することができる。フォルダ1012は、拡張されており、第1の段階1016および第2の段階1018の表示を含む。各段階は、階層的表示1000内の機器モジュール（図9）を実行する際に使用する最低レベルの手順要素である。図9の階層的表示900のように、任意の適当なフォルダおよび／または表示を、本発明に関連するセキュリティ区域として選択することができる。例えば、第2のユニット手順（動作1～Mおよびすべての関連する段階を含む）をセキュリティ区域として選択することができる。同様に、段階1をセキュリティ区域として選択することができる。

【0044】

ここで図11を参照すると、この図は、小さなインテリジェンスを含むデバイスへの区域セキュリティ・ポリシーの提供を容易にするシステム1100を示す。システム1100は、第1のプラントフロアデバイス1102、第2のプラントフロアデバイス1104からN番目のプラントフロアデバイス1106までを含む。なお、Nは整数である。プラ

10

20

30

40

50

ントフロアデバイス1102～1106は、相互に通信し、プロキシ・サーバ1108を介して、異なるセキュリティ構成要素／システムからセキュリティ・コマンドを受信する。オートメーション・コントローラ（例えば、プログラマブル論理コントローラ）からのものであり、アクチュエータおよび他の工場のフロアのデバイスに配信される制御コマンドは、プロキシ・サーバ1108を通過する必要はない。何故なら、このような要件は、オートメーション・システムの性能に影響を与えるからである。例えば、好ましくは、第1のプラントフロアデバイス1102が、第2のプラントフロアデバイス1104に通信を配信する場合には、第1のプラントフロアデバイスはこのような通信を直接配信しない。第1の工場のフロアのデバイス1102は、この通信をプロキシ・サーバ1108に配信し、プロキシ・サーバはその後でこの通信を第2の工場のフロアのデバイス1104に送る。同様に、ハイレベルのシステムが、プラントフロアデバイス1102～1106のうちの1つと通信したい場合には、同様にこのシステムはプロキシ・サーバ1108を通して通信する。システム1100は、さらに、工場のフロアに関する区域セキュリティ手順を実施することができるセキュリティ・システム1110を含む。しかし、プラントフロアデバイス1102～1106は、セキュリティ特権を記憶し、実施するのに十分なインテリジェンスを含んでいない。それ故、セキュリティ・システム1110は、プラントフロアデバイス1102～1106に関連するセキュリティ手順を、プロキシ・サーバ1108を介して配信する。本発明の1つの態様によれば、プラントフロアデバイス1102～1106はある区域内に集まっている。それ故、第1のプラントフロアデバイス1102に関連して実施したセキュリティ手順は、また、第2のプラントフロアデバイス1104に関しても実施される。工場のフロアのデバイス1102～1106が非常に小さなインテリジェンスを含んでいる場合も同じである。別の方法としては、プロキシ・サーバ1108は、別々に、プラントフロアデバイス1102～1106に区域セキュリティ手順を配信することもできる。

10

20

【0045】

ここで図12を参照すると、この図は、ハイレベルのシステム1202と産業用コントローラ1204との間の例示としての通信1200を示す。例えば、ハイレベルのシステムは、ERPシステムおよび／またはMESシステムであってもよいし、産業用コントローラ1204は、プログラマブル論理コントローラ（PLC）であってもよい。しかし、工場のフロア上の任意の適当なシステムを、ハイレベルのシステム1202として使用することもできるし、任意の適当な産業用コントローラを産業用コントローラ1204として使用することができることを理解されたい。

30

【0046】

産業用コントローラは、ハイレベルのシステム1202に対する通信の送受信に関連してデータ・モデル1206を使用する。従来の産業用コントローラは、センサおよびアクチュエータの状態を監視するだけであり、構造化されていないビットのストリングで通信するだけであった。しかし、データ・モデル1206を使用することにより、産業用コントローラ1204は、ハイレベルのシステム1202と直接通信することができる。何故なら、ハイレベルのシステム1202は、産業用コントローラ1204が使用するデータ・モデル1206とほぼ同様のデータ・モデル1208を使用するからである。このような直接通信により、区域セキュリティ手順の実施が容易になる。何故なら、ハイレベルのシステム1202が、産業用コントローラ1204にセキュリティ手順を直接送ることができるからである。さらに、共通のデータ・モデルを使用することにより、区域セキュリティ手順の発生および実施に関連して使用することができる工場のフロアを表示を生成することができる。例えば、SP95規格およびS88規格は、データ・モデル1206および1208として使用することができる2つの例示としての規格である。しかし、本発明により任意の適当な構造化データ・モデルを使用することができることを理解されたい。

40

【0047】

図13の場合には、本発明の種々の態様を実施するための例示としての環境1310は

50

、コンピュータ1312を含む。コンピュータ1312は、処理ユニット1314、システム・メモリ1316、およびシステム・バス1318を含む。システム・バス1318は、システム・メモリ1316を含む（但し、これに限定されない）システム構成要素を、処理ユニット1314に結合する。処理ユニット1314は、入手できる種々のプロセッサのうちの任意のものであってもよい。デュアル・マイクロプロセッサおよび他のマルチプロセッサ・アーキテクチャも、処理ユニット1314として使用することができる。

【0048】

システム・バス1318は、メモリ・バスまたはメモリ・コントローラ、周辺バスまたは外部バスであってもよく、更に、8ビット・バス、Industrial Standard Architecture (ISA)、マイクロチャネル・アーキテクチャ (MCA)、拡張ISA (EISA)、インテリジェント・ドライブ・エレクトロニクス (IDE)、VESAローカル・バス (VLB)、Peripheral Component Interconnect (PCI)、ユニバーサル・シリアル・バス (USB)、Advanced Graphics Port (AGP)、Personal Computer Memory Card International Association bus (PCMCIA)、およびスモール・コンピュータ・システム・インタフェース (SCSI) を含むが、これらに限定されず、種々の有用なバス・アーキテクチャのうちの任意のものを使用するローカル・バスを含むいくつかのタイプのバス構造体のうちの任意のものであってもよい。

【0049】

システム・メモリ1316は、揮発性メモリ1320および不揮発性メモリ1322を含む。スタートの際等に、コンピュータ1312内の要素間で情報を移送するための基本ルーチンを含む基本入出力システム (BIOS) は、不揮発性メモリ1322内に記憶される。不揮発性メモリ1322は、説明のためのものであって本発明を制限するものではないが、読み出し専用メモリ (ROM)、プログラマブルROM (PROM)、電氣的にプログラム可能なROM (EPROM)、電氣的に消去可能なROM (EEPROM) またはフラッシュ・メモリを含むことができる。揮発性メモリ1320は、外部キャッシュ・メモリとして機能するランダム・アクセス・メモリ (RAM) を含む。RAMは、説明のためのものであって本発明を制限するものではないが、同期型RAM (SRAM)、ダイナミックRAM (DRAM)、同期型DRAM (SDRAM)、ダブル・データ・レート SDRAM (DDR SDRAM)、エンハンスドSDRAM (ESDRAM)、Synchronous DRAM (SLDRAM)、およびダイレクト Rambus RAM (DRRAM) のような多くの形式で使用するすることができる。

【0050】

コンピュータ1312は、また、取り外すことができる／取り外すことができない揮発性／不揮発性コンピュータ記憶媒体を含む。図13は、例えば、ディスク記憶領域1324を示す。ディスク記憶領域1324は、磁気ディスク・ドライブ、フレキシブル・ディスク・ドライブ、テープ・ドライブ、Jazドライブ、Zipドライブ、LS-100ドライブ、フラッシュ・メモリ・カードまたはメモリ・スティックのようなデバイスを含むが、これらに限定されない。さらに、ディスク記憶領域1324は、別々に、またはコンパクト・ディスクROMデバイス (CD-ROM)、CD追記型ドライブ (CD-Rドライブ)、CD書込可能ドライブ (CD-RWドライブ) またはデジタル汎用ディスクROMドライブ (DVD-ROM) のような光ディスク・ドライブを含む（但し、これらに限定されない）記憶媒体と一緒に若しくは別々に含むことができる。システム・バス1318とディスク記憶領域1324との接続を容易にするために、インタフェース1326のような取り外すことができる、または取り外すことができないインタフェースが通常使用される。

【0051】

図13は、ユーザと適当な動作環境1310内で記述した基本コンピュータ・リソースとの間の仲介者として動作するソフトウェアを示していることを理解されたい。このよう

10

20

30

40

50

なソフトウェアは、オペレーティング・システム 1 3 2 8 を含む。ディスク記憶領域 1 3 2 4 上に記憶することができるオペレーティング・システム 1 3 2 8 は、コンピュータ・システム 1 3 1 2 のリソースを制御し、割り当てる働きをする。システム・アプリケーション 1 3 3 0 は、システム・メモリ 1 3 1 6 内またはディスク記憶領域 1 3 2 4 上に記憶されているプログラム・モジュール 1 3 3 2 およびプログラム・データ 1 3 3 4 を通して、オペレーティング・システム 1 3 2 8 によるリソースの管理を利用する。本発明は種々のオペレーティング・システムまたはオペレーティング・システムの組合わせと一緒に実施することができることを理解されたい。

【0052】

ユーザは、入力装置 1 3 3 6 を通して、コンピュータ 1 3 1 2 内にコマンドまたは情報を 10
入力する。入力装置 1 3 3 6 は、マウス、トラックボール、スタイラス、タッチパッド、キーボード、マイクロホン、ジョイスティック、ゲーム・パッド、衛星用ディッシュ、スキャナ、TV チューナ・カード、デジタル・カメラ、デジタル・ビデオ・カメラ、ウェブ・カメラ等のようなポインティング・デバイスを含むが、これらに限定されない。これらおよび他の入力装置は、（ひとつまたは複数の）インタフェース・ポート 1 3 3 8 を通して、システム・バス 1 3 1 8 により、処理ユニット 1 3 1 4 に接続される。インタフェース・ポート 1 3 3 8 は、例えば、シリアル・ポート、パラレル・ポート、ゲーム・ポート 20
およびユニバーサル・シリアル・バス（USB）を含む。（ひとつまたは複数の）出力装置 1 3 4 0 は、（ひとつまたは複数の）入力装置 1 3 3 6 と同じタイプのポートのうちのいくつかを使用する。それ故、例えば、USB ポートは、コンピュータ 1 3 1 2 に入力 20
するため、またコンピュータ 1 3 1 2 から出力装置 1 3 4 0 に情報を出力するために使用することができる。出力アダプタ 1 3 4 2 は、特種なアダプタを必要とする他の出力装置 1 3 4 0 のうちのモニタ、スピーカ、およびプリンタのようないくつかの出力装置 1 3 4 0 があることを説明するために示されたものである。出力アダプタ 1 3 4 2 は、説明のためのものであって本発明を制限するためのものではないが、出力装置 1 3 4 0 とシステム・バス 1 3 1 8 との間の接続手段となるビデオ・カードおよび音声カードを含む。他のデバイスおよび／またはデバイスのシステムは、（ひとつまたは複数の）リモート・コンピュータ 1 3 4 4 のような入力機能および出力機能の両方を供給することに留意されたい。

【0053】

コンピュータ 1 3 1 2 は、リモート・コンピュータ 1 3 4 4 のように、1 つまたは複数の 30
リモート・コンピュータへの論理接続によりネットワークで接続している環境内で動作することができる。リモート・コンピュータ 1 3 4 4 は、パーソナル・コンピュータであっても、サーバであっても、ルータであっても、ネットワーク PC であっても、ワークステーションであっても、マイクロプロセッサをベースとするツールであっても、ピア・デバイスまたは他の共通のネットワーク・ノード等であってもよく、通常、コンピュータ 1 3 1 2 に関連して説明した多くのまたはすべての要素を含む。説明を簡単にするために、リモート・コンピュータ 1 3 4 4 と一緒にメモリ記憶領域 1 3 4 6 だけを図示してある。リモート・コンピュータ 1 3 4 4 は、ネットワーク・インタフェース 1 3 4 8 を通して、論理的にコンピュータ 1 3 1 2 に接続していて、次に通信接続 1 3 5 0 を通して物理的に 40
接続している。ネットワーク・インタフェース 1 3 4 8 は、ローカル・エリア・ネットワーク（LAN）、ワイド・エリア・ネットワーク（WAN）のような通信ネットワークを含む。LAN 技術は、ファイバ分散データ・インタフェース（FDDI）、銅線分散データ・インタフェース（CDDI）、イーサネット（登録商標）／IEEE 1102.3、トークンリング／IEEE 1102.5 等を含む。WAN 技術は、二点間リンク、デジタル総合サービス網（ISDN）のような回線交換網およびそれを修正したもの、パケット交換網およびデジタル加入者ライン（DSL）を含むが、これらに限定されない。

【0054】

通信接続 1 3 5 0 は、ネットワーク・インタフェース 1 3 4 8 を、バス 1 3 1 8 に接続 50
するために使用するハードウェア／ソフトウェアである。図では、通信接続 1 3 5 0 は、説明を分かりやすくするためにコンピュータ 1 3 1 2 内に位置しているが、コンピュータ

1312の外部に設置することもできる。ネットワーク・インタフェース1348へ接続するために必要なハードウェア／ソフトウェアは、通常の電話級のモデム、ケーブル・モデムおよびDSLモデム、ISDNアダプタおよびイーサネット（登録商標）・カードを含むモデムのような内部および外部技術を含むが、これらは単に例示としてのものに過ぎない。

【0055】

図14は、本発明が相互作用を行うことができるサンプル・コンピューティング環境の簡単なブロック図である。システム1400は、1つまたは複数のクライアント1410を含む。クライアント1410は、ハードウェアおよび／またはソフトウェア（例えば、スレッド、プロセス、計算デバイス）であってもよい。システム1400は、また1つまたは複数のサーバ1430を含む。サーバ1430は、またハードウェアおよび／またはソフトウェア（例えば、スレッド、プロセス、計算デバイス）であってもよい。サーバ1430は、例えば、本発明を使用しての変換を行うためにスレッドを内蔵することができる。クライアント1410とサーバ1430との間の唯一の可能な通信は、2つ以上のコンピュータ・プロセス間で送信することができるデータ・パケットの形をとることができる。システム1400は、クライアント1410とサーバ1430間の通信を容易にするために使用することができる通信フレームワーク1450を含む。クライアント1410は、クライアント1410にとってローカルな情報を記憶するために使用することができる1つまたは複数のクライアント・データ記憶領域1460に動作できるように接続されている。同様に、サーバ1430は、サーバ1430にとってローカルな情報を記憶するために使用することができる1つまたは複数のサーバ・データ記憶領域1440に動作できるように接続されている。

【0056】

上記説明は本発明のいくつかの例を含む。もちろん、本発明を記述するために構成要素または方法の考えられるすべての組み合わせを記述することはできないが、通常の当業者であれば、本発明の多くの他の組み合わせおよび順列が可能であることを理解することができるだろう。それ故、本発明は、添付の特許請求の範囲の精神および範囲に含まれるすべてのこのような変更、修正および変形版を含むものである。さらに、詳細な説明または特許請求の範囲内で「含む」という用語を使用した場合には、この用語は「備える」という用語に類似の方法で包括的なものである。何故なら、「備える」は、使用した場合、特許請求の範囲内の遷移的な語と解釈されるからである。

【図面の簡単な説明】

【0057】

【図1】本発明のある態様による、工場のフロア内で区域セキュリティ手順の生成および実施を容易にするシステムのハイレベルのブロック図である。

【図2】本発明のある態様による、工場のフロア内で区域セキュリティ手順の生成および実施を容易にするシステムのブロック図である。

【図3】本発明のある態様による、工場のフロア内で区域セキュリティ手順の生成および実施を容易にするシステムのブロック図である。

【図4】本発明のある態様による、工場のフロア内で区域セキュリティ手順の生成および実施を容易にするシステムのブロック図である。

【図5】本発明のある態様による、工場のフロア内である区域に関連するセキュリティを修正するための方法を示す代表的な流れ図である。

【図6】本発明のある態様による、プロキシ・サーバを介して1つまたは複数の工場のフロアのデバイスに関連するセキュリティを修正するための方法を示す代表的な流れ図である。

【図7】本発明のある態様による、区域セキュリティ手順を実施する前に、オペレータを認証するための方法を示す代表的な流れ図である。

【図8】本発明のある態様による、工場のフロア上のアラームに基づく区域セキュリティ手順を自動的に生成するための方法を示す代表的な流れ図である。

【図 9】本発明に関連して使用することができる例示としてのシステム表示である。

【図 10】本発明に関連して使用することができるオートメーション環境内のアプリケーション／動作の例示としての階層的表示である。

【図 11】本発明のある態様による、プロキシ・サーバを介して工場のフロアのデバイスへのセキュリティ手順の適用を容易にするシステムのブロック図である。

【図 12】本発明のある態様による、産業用コントローラとハイレベルのシステムとの間の直接通信を容易にするシステムのブロック図である。

【図 13】本発明に関連して使用することができる例示としての動作環境である。

【図 14】本発明に関連して使用することができる例示としての動作環境である。

【符号の説明】

10

【0058】

1, 2 制御モジュール

100, 200, 300, 400 システム

102, 202, 302, 402 工場のフロア

104, 204 セキュリティ・システム

106, 212, 306, 308, 414 区域セキュリティ構成要素

108, 208, 306, 410 区域

206 システム表示

210 認証構成要素

304, 408 動的区域生成装置

312 手順実行構成要素

404 産業用コントローラ

412 セキュリティ・システム

900, 916, 918 表示

902, 904, 906, 908, 910, 912 フォルダ

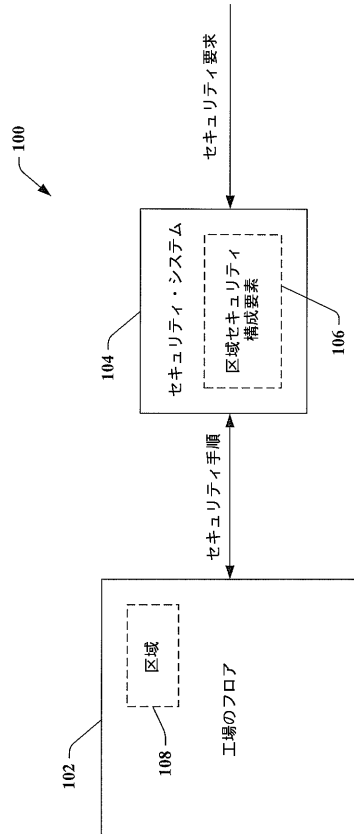
1000 階層的表示

1002, 1004, 1006~1014 フォルダ

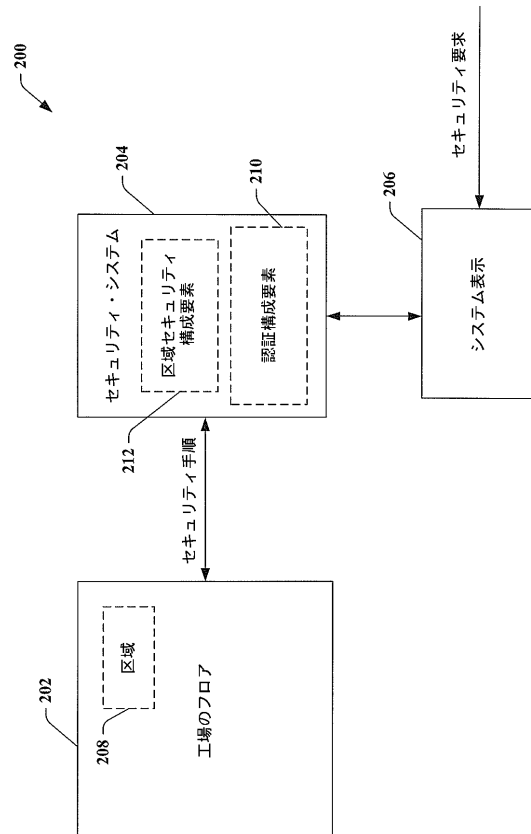
1016, 1018 段階

20

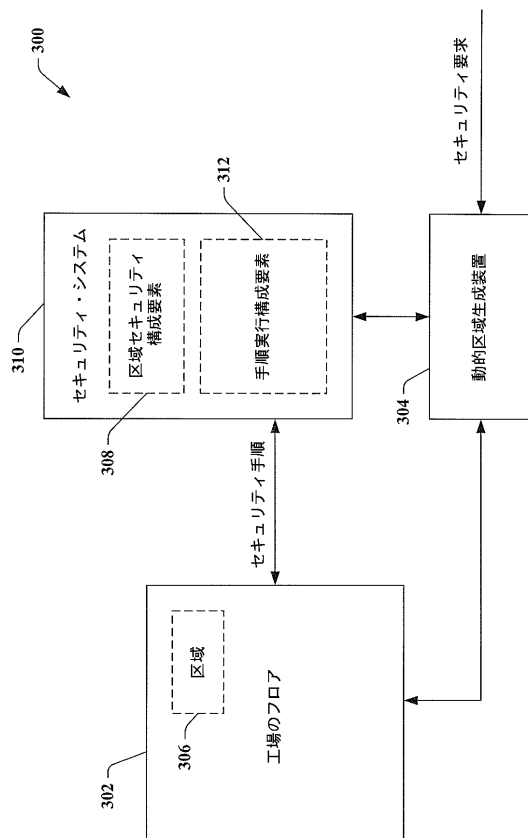
【図 1】



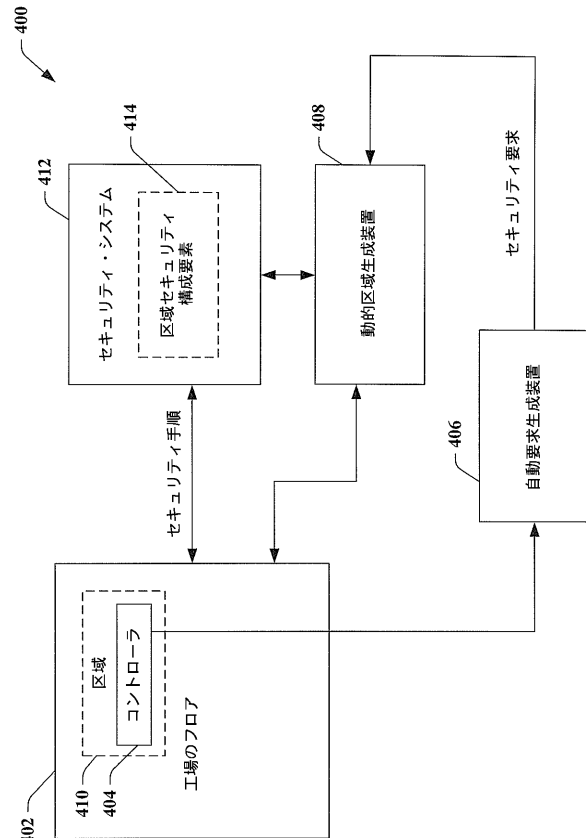
【図 2】



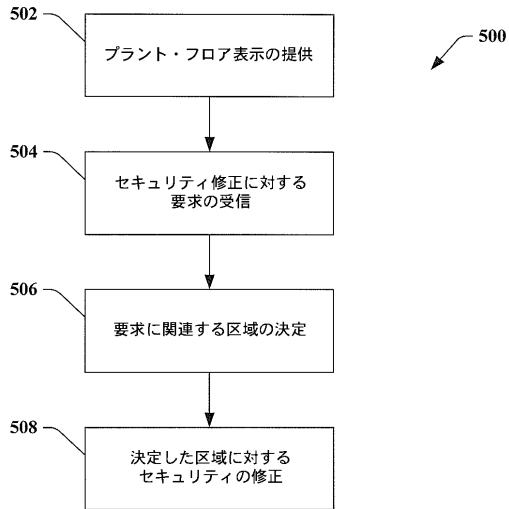
【図 3】



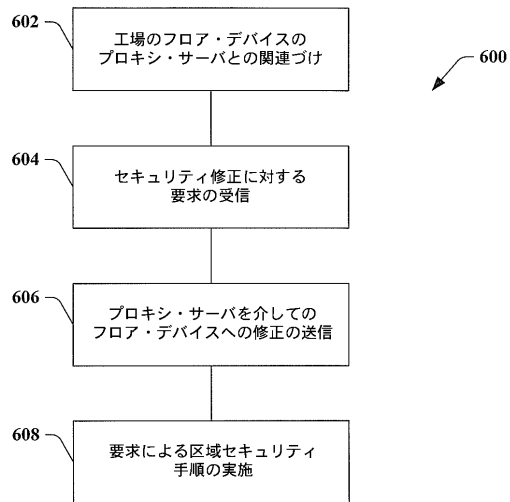
【図 4】



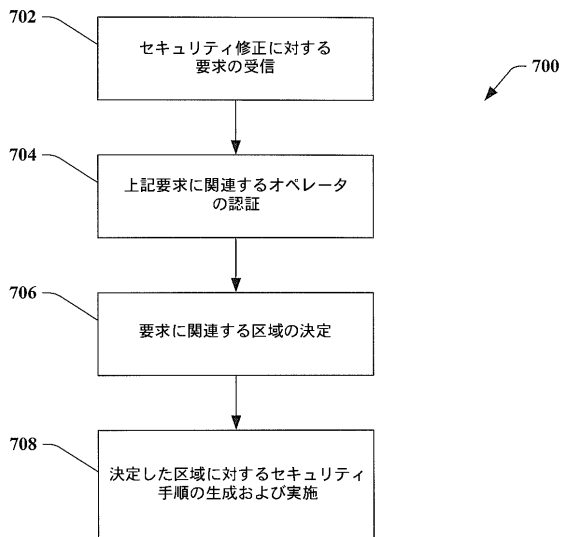
【図 5】



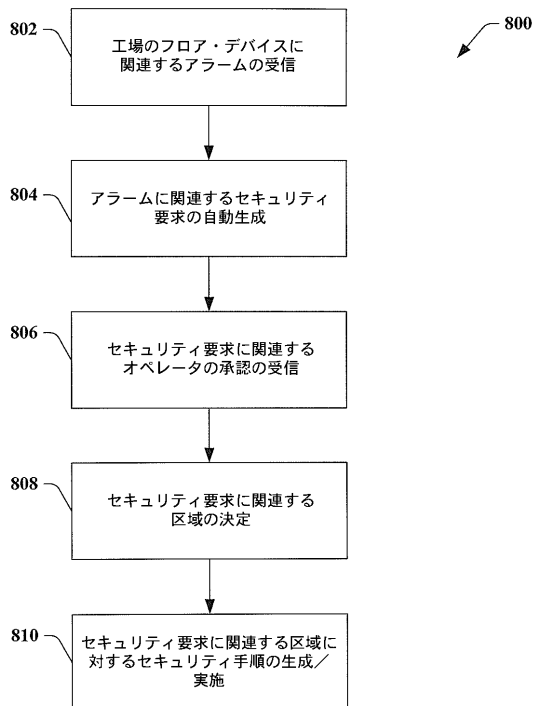
【図 6】



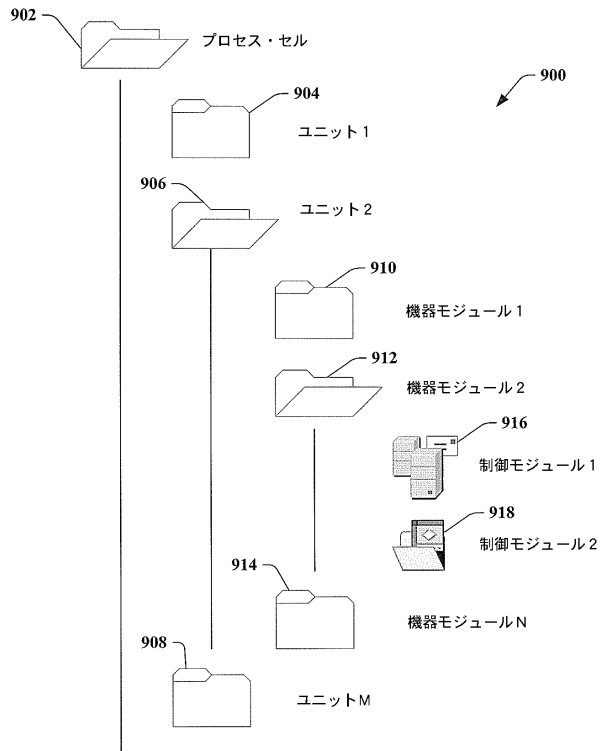
【図 7】



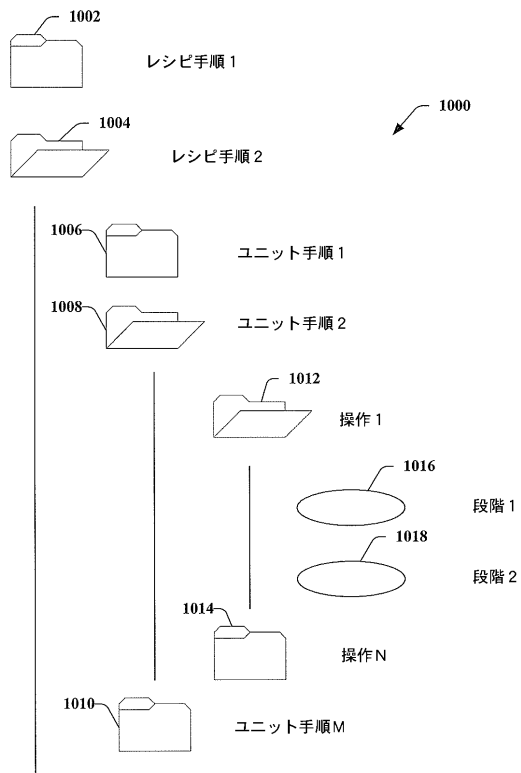
【図 8】



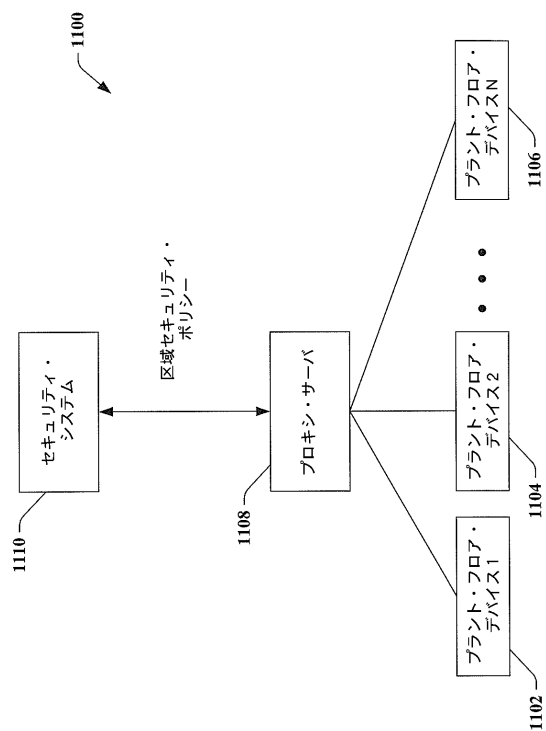
【図 9】



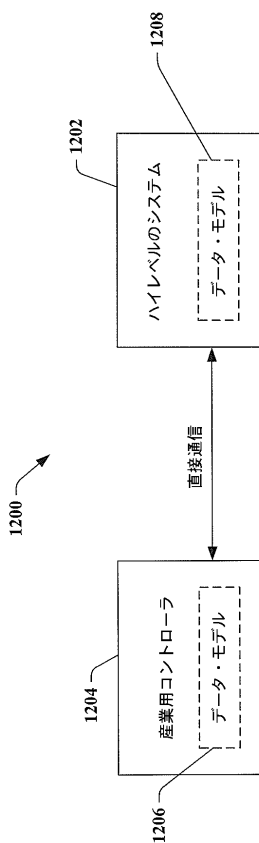
【図 10】



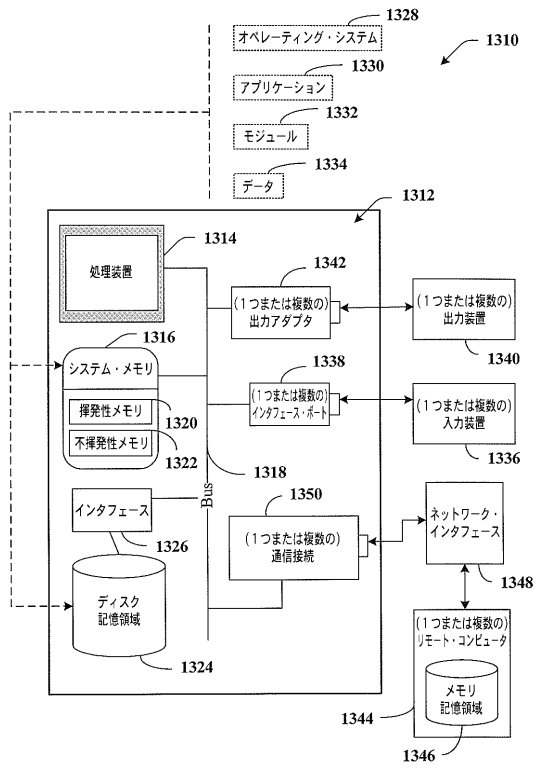
【図 11】



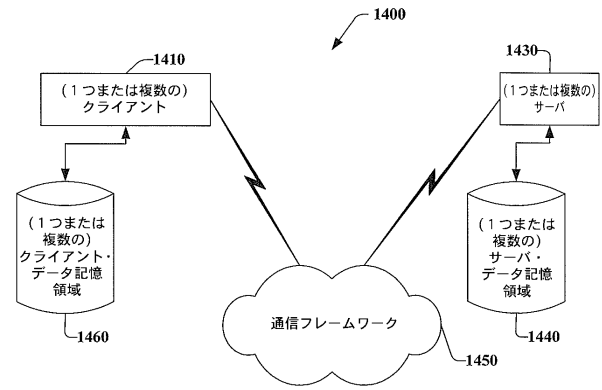
【図 12】



【図 13】



【図 14】



フロントページの続き

- (74)代理人 100094673
弁理士 林 鉦三
- (72)発明者 スジー チャンド
アメリカ合衆国、ウィスコンシン、ブルックフィールド、 レジェンド コート 19460
- (72)発明者 デビッド ダブリュ. ファーチミン
アメリカ合衆国、ウィスコンシン、グラフトン、 エッジウォーター ドライブ 2166
- (72)発明者 ジョン ジェイ. バイアー
アメリカ合衆国、オハイオ、メントール、 レン コート 9072
- (72)発明者 マイケル ディー. カラン
アメリカ合衆国、オハイオ、ハイランド ハイツ、 ノース アップルクロス ロード 6260
- (72)発明者 ロンダール エー. マルカルド
アメリカ合衆国、ウィスコンシン、ウォーキショー、 コペンヒル ドライブ 1340
- (72)発明者 リチャード エー. モース
アメリカ合衆国、オハイオ、ハドソン、 ロンドネイリー ブールバード 5622
- (72)発明者 スティーブン シー. プライアント
アメリカ合衆国、ペンシルヴァニア、ムーン タウンシップ、 スプリング ラン ロード エク
ステンション 1550

審査官 佐藤 彰洋

- (56)参考文献 特開2001-273388 (JP, A)
特開2003-150748 (JP, A)
国際公開第03/096168 (WO, A1)
特表2004-527805 (JP, A)
特開2003-196476 (JP, A)
特開平06-231381 (JP, A)
特開平09-106491 (JP, A)
特開平02-171896 (JP, A)
特開2002-163450 (JP, A)
特開2000-182169 (JP, A)
特開2001-358717 (JP, A)
特開2003-099602 (JP, A)

(58)調査した分野(Int.Cl., DB名)

G05B 19/418
G06Q 10/00
G06Q 50/04
G05B 9/02-9/03
G05B 23/02
F16P 1/00-7/02
G08B 19/00-31/00