(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2020-13591
(P2020-13591A)
(43)公開日　令和2年1月23日(2020.1.23)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/33	***(2013.01)***	G06F	21/33		2E250
E05B 49/00	*(2006.01)*	E05B	49/00	Z	
		E05B	49/00	J	

審査請求 有　請求項の数 24　ＯＬ　外国語出願　（全 28 頁）

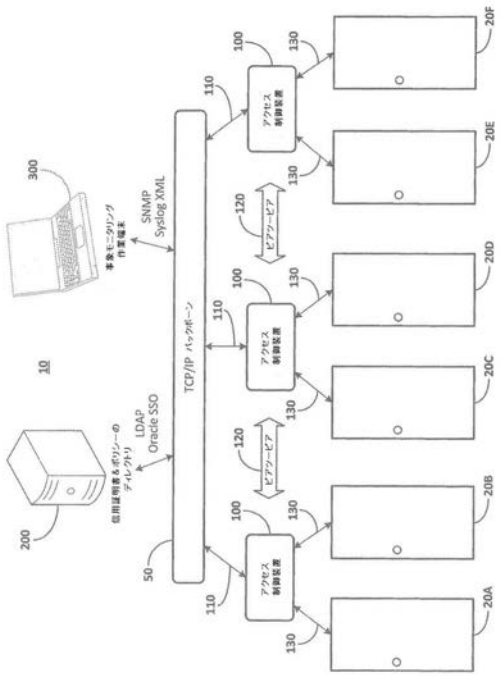
(21)出願番号　特願2019-150636 (P2019-150636)
(22)出願日　令和1年8月20日 (2019.8.20)
(62)分割の表示　特願2016-506316 (P2016-506316)の分割
原出願日　平成26年3月13日 (2014.3.13)
(31)優先権主張番号　13/855,543
(32)優先日　平成25年4月2日 (2013.4.2)
(33)優先権主張国・地域又は機関
米国 (US)

(71)出願人　515274653
アヴィジロン　アナリティックス　コーポレーション
カナダ　ブイ６シー　０エー３　ブリティッシュコロンビア州　バンクーバー　バラード・ストリート　２９００－５５０
(74)代理人　100082072
弁理士　清原　義博
(72)発明者　ニーリー，イー．，テリー
アメリカ合衆国　２０１９０　バージニア州　レストン　スイート２０００　プラザ・アメリカ・ドライブ　１１７１０

Ｆターム(参考)　2E250 AA03 BB05 BB09 DD06 DD08 FF05 FF23 FF27 FF36

(54)【発明の名称】自己プロビジョニングアクセス制御

(57)【要約】　（修正有）
【課題】アクセス制御装置によるディレクトリの周期的な自動化したクエリを介してアクセス制御装置の自己プロビジョニングを可能にする。
【解決手段】アクセス制御装置において、アクセスコントーローラの方法は、信用証明書及びポリシーのディレクトリ情報を受信する工程、アクセスを必要とする１以上の個人に関する信用証明書及びポリシー情報を、ディレクトリから獲得する工程、獲得した信用証明書及びポリシー情報をローカルキャッシュに保存する工程、個人のアクセスを許可するためにアクセス要求を受信する工程、アクセス要求を、キャッシュにおける信用証明書及びポリシー情報と比較する工程及び比較が一致を示す場合に個人のアクセスを認める工程を含む。
【選択図】図１Ａ



【特許請求の範囲】
【請求項１】
プロセッサにより実行されるアクセス制御方法であって：
プロセッサにおいて、アクセス制御装置によるディレクトリの周期的な自動化したクエリを介してアクセス制御装置の自己プロビジョニングを可能にするようにアクセス制御装置を構成するために、信用証明書及びポリシーのディレクトリ情報を受信する工程；
アクセスを必要とし得る１以上の個人に関する信用証明書及びポリシー情報を、プロセッサを用いてディレクトリから獲得する工程；
獲得した信用証明書及びポリシー情報を、プロセッサによりアクセス可能なローカルキャッシュに保存する工程；
個人のアクセスを許可するためにアクセス要求をプロセッサにおいて受信する工程；
プロセッサにより、アクセス要求を、キャッシュにおける信用証明書及びポリシー情報と比較する工程；及び
比較が一致を示す場合に個人のアクセスを認める工程
を含む方法。
【請求項２】
アクセス要求は包囲されたエリアへのアクセスのためのものである、ことを特徴とする請求項１に記載の方法。
【請求項３】
包囲されたエリアは複数のアクセス制御装置を備え、且つ、アクセス制御装置を構成する工程は：
ユーザーインターフェースを介して第１のアクセス制御装置を構成する工程；及び
他のアクセス制御装置の各々における構成を自動的に複製する工程
を含む、ことを特徴とする請求項２に記載の方法。
【請求項４】
ディレクトリ情報はディレクトリのＵＲＬを含む、ことを特徴とする請求項２に記載の方法。
【請求項５】
アクセス要求は包囲されたエリアの信用証明書リーダにおいて受信され、該信用証明書リーダは個人の信用証明書を読み取るものであり、ここで、アクセス要求は、ローカルキャッシュにおける信用証明書及びポリシー情報と比較するための、信用証明書、及び信用証明書からのポリシー情報を含む、ことを特徴とする請求項２に記載の方法。
【請求項６】
比較は、アクセス要求における情報と、ローカルキャッシュにおける対応する信用証明書及びポリシー情報との完全な一致を要求する、ことを特徴とする請求項２に記載の方法。
【請求項７】
アクセスを認めるために包囲されたエリアへのアクセスドアを解錠する工程を更に含む、請求項２に記載の方法。
【請求項８】
事象モニターのアドレスをプロセッサにより受信する工程；
事象画定情報を受信する工程；及び
受信した事象画定情報に応じて事象をモニタリングし且つ収集するようにアクセス制御装置を構成する工程
を更に含む、ことを特徴とする請求項２に記載の方法。
【請求項９】
収集した事象をバッファ処理し、それを事象モニターに報告するようにアクセス制御装置を構成する工程を更に含む、請求項８に記載の方法。
【請求項１０】
プロセッサは、複数の事象モニターの各々のアドレスを受信し、ここで、方法は複数の

事象モニターの複数のアドレスに事象を同時に送信する工程を含む、ことを特徴とする請求項９に記載の方法。
【請求項１１】
事象は、ドアの開放、ドアの閉鎖、ドアの開固着、ドアの施錠、及びドアの解錠を含む、ことを特徴とする請求項１０に記載の方法。
【請求項１２】
アクセス要求は、資源にアクセスするための要求である、ことを特徴とする請求項１に記載の方法。
【請求項１３】
資源は論理資源である、ことを特徴とする請求項１２に記載の方法。
【請求項１４】
アクセス制御装置は、資源に対する個人の位置に基づいて資源へのアクセスを自己プロビジョニングする、ことを特徴とする請求項１２に記載の方法。
【請求項１５】
比較が一致を示さない場合、方法は、一致を判定するために信用証明書及びポリシーのディレクトリにアクセス要求を送信する工程を含む、ことを特徴とする請求項１に記載の方法。
【請求項１６】
周期的に、ローカルキャッシュにおける信用証明書及びポリシー情報を自動更新する工程を更に含む、請求項１に記載の方法。
【請求項１７】
更新はリアルタイムで継続的に行われる、ことを特徴とする請求項１に記載の方法。
【請求項１８】
個人によるエリアへのアクセスを制御するためのシステムであって；
プロセッサ；及び
コンピュータ可読記憶媒体に埋め込まれるアクセス制御装置
を含み、
前記アクセス制御装置は機械命令を含み、該機械命令は、プロセッサにより実行された場合：
アクセス制御装置によるディレクトリの周期的な自動化したクエリを介してアクセス制御装置の自己プロビジョニングを可能にするために、リモートディレクトリからの信用証明書及びポリシーのディレクトリ情報、及び
エリアへのアクセスを要求する１以上の個人に関する、ディレクトリからの信用証明書及びポリシー情報を受信するようにアクセス制御装置を構成すること；
ディレクトリの受信獲得した信用証明書及びポリシー情報、並びに、１以上の個人の信用証明書及びポリシー情報を、プロセッサによりアクセス可能なローカルキャッシュに保存すること；
包囲されたエリアへの個人のアクセスを許可するためにアクセス要求を受信すること；
アクセス要求を、キャッシュにおける信用証明書及びポリシー情報と比較すること；及び
比較が一致を示す場合に、エリアへの個人のアクセスを認めること
を、プロセッサに行わせる
ことを特徴とするシステム。
【請求項１９】
エリアは複数のアクセス制御装置を備え、且つ、アクセス制御装置を構成する場合、プロセッサは：
ユーザーインターフェースを介して第１のアクセス制御装置を構成し；及び
他のアクセス制御装置の各々における構成を自動的に複製する
ことを特徴とする請求項１８に記載のシステム。

【請求項２０】
ディレクトリ情報は、ディレクトリのＵＲＬを備え、ここで、ディレクトリとプロセッサはＴＣＰ／ＩＰプロトコルを使用して通信する、ことを特徴とする請求項１８に記載のシステム。
【請求項２１】
アクセス要求はエリアの信用証明書リーダにおいて受信され、該信用証明書リーダは個人の信用証明書を読み取るものであり、ここで、アクセス要求は、ローカルキャッシュにおける信用証明書及びポリシー情報と比較するための、信用証明書、及び信用証明書からのポリシー情報を含む、ことを特徴とする請求項１８に記載のシステム。
【請求項２２】
プロセッサは、予め画定された事象確定情報に従い、事象をモニタリングし且つそれを収集するようにアクセス制御装置を構成する、ことを特徴とする請求項１８に記載のシステム。
【請求項２３】
収集した事象を保存するためのバッファを更に備える、請求項１８に記載のシステム。
【請求項２４】
プロセッサは、複数の事象モニターの各々のアドレスを受信し、ここで、プロセッサは複数の事象モニターの複数のアドレスに事象を同時に送信する、ことを特徴とする請求項２３に記載のシステム。
【請求項２５】
個人による資産へのアクセスを制御するようにアクセス制御装置を構成するための、プロセッサにより実行される方法であって：
資産へのアクセスを要求する個人に関する信用証明書及びポリシー情報をプロセッサが獲得する、信用証明書及びポリシーのディレクトリアドレスを、プロセッサにより受信する工程；
信用証明書及びポリシー情報に関する宛先アドレスを受信する工程；
信用証明書及びポリシー情報を獲得するための周期性を確立する工程；
資産へのアクセスを必要とする個人に関する信用証明書及びポリシー情報を獲得する工程；及び
確立された周期性で資産へのアクセスを必要とする個人に関する信用証明書及びポリシー情報を自動的に更新する工程
を含む方法。
【請求項２６】
資産は物理的エリアである、ことを特徴とする請求項２５に記載の方法。
【請求項２７】
資産は論理資産であり、プロセッサは、第１の画定した物理的エリアにおいて論理資産への第１のアクセスレベルを設け、且つ、第２の画定した物理的エリアにおいて第１のアクセスレベルよりも高い第２のアクセスレベルを設ける、ことを特徴とする請求項２５に記載の方法。
【請求項２８】
個人は、個人の信用証明書の第１の読み取りに基づいて第１の画定したエリアに位置するものとして識別され、且つ、信用証明書の第２の読み取りに基づいて第２の画定したエリアに位置するものとして識別され、ここで、個人は、個人が第２の画定したエリアに位置するものとして識別された場合、第２のアクセスレベルで論理資産へのアクセスを認められる、ことを特徴とする請求項２７に記載の方法。
【請求項２９】
自己プロビジョニング／自己レポーティングアクセス制御装置であって：
資産へのアクセスを制御するための機械命令を保存するための手段；及び
機械命令を実行するための手段であって：
機械命令を実行するための手段を自己プロビジョニングするための手段、

資産へのアクセスを認める／拒否するための手段、及び
資産へのアクセスの容認及び拒否に関連する事象を報告するための手段
を含む手段
を含む自己プロビジョニング／自己レポーティングアクセス制御装置。
【請求項３０】
自己プロビジョニングするための手段は：
信用証明書及びポリシーのディレクトリとの安全な通信のための手段；
ディレクトリから得た信用証明書及びポリシー情報を、実行するための前記手段によりローカルに保存するための手段；及び
ローカルに保存した信用証明書及びポリシー情報を更新するための手段
を含む、ことを特徴とする請求項２９に記載の自己プロビジョニング／自己レポーティングアクセス制御装置。
【請求項３１】
資産へのアクセスの容認及び拒否に関連する事象を報告するための手段は：
実行するための手段により事象をローカルにバッファ処理するための手段；及び
複数の監視システムに事象を報告するための手段
を含む、ことを特徴とする請求項２９に記載の自己プロビジョニング／自己レポーティングアクセス制御装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、自己プロビジョニングアクセス制御に関する。
【背景技術】
【０００２】
アクセス制御システムは、建物、建物内の部屋、又は入る許可を持つ人々のみに対する囲まれた領域などの、包囲されたエリアへの侵入を制限する場合がある。最新のアクセス制御システムは、建物の侵入ポイント（即ち、ドア）にアクセス・カード・リーダを備える。建物に入る許可を持つ個人は、アクセス・カード・リーダによって読み取られ得るアクセス制御カードを提供される。アクセス・カード・リーダは、アクセス・カードから情報を得て、制御パネルに情報を通信する。制御パネルは、ドアが解錠されるべきかどうか判定する。ドアが解錠されなければならない場合（即ち、アクセス・カードは、侵入する許可を持つ個人に関係している）、制御パネルはドアロック機構に信号を送信して、機構に解錠を行わせる。
【発明の概要】
【０００３】
包囲されたエリアへのアクセスを制御するための、プロセッサにより実行されるアクセス制御方法は、アクセスコントローラによるディレクトリの周期的な自動化したクエリを介してアクセスコントローラの自己プロビジョニングを可能にするようにアクセスコントローラを構成するために、信用証明書及びポリシーのディレクトリ情報を受信する工程；包囲されたエリアへのアクセスを必要とし得る１以上の個人に関する信用証明書及びポリシー情報を、ディレクトリから獲得する工程；獲得した信用証明書及びポリシー情報をローカルキャッシュに保存する工程；包囲されたエリアへの個人のアクセスを許可するためにアクセス要求を受信する工程；アクセス要求を、キャッシュにおける信用証明書及びポリシー情報と比較する工程；及び、比較が一致を示す場合に、包囲されたエリアへの個人のアクセスを認める工程を含む。
【０００４】
個人によるエリアへのアクセスを制御するためのシステムは、コンピュータ可読記憶媒体に具現化されるプロセッサ及びアクセスコントローラを備え、アクセスコントローラは機械命令を含み、該機械命令は、プロセッサにより実行された場合、アクセスコントローラによるディレクトリの周期的な自動化したクエリを介してアクセスコントローラの自己

プロビジョニングを可能にするために、リモートディレクトリからの信用証明書及びポリシーのディレクトリ情報、並びに、エリアへのアクセスを必要とし得る１以上の個人に関する、ディレクトリからの信用証明書及びポリシー情報を受信するようにアクセスコントローラを構成すること、ディレクトリの受信獲得した信用証明書及びポリシー情報、並びに、１以上の個人の信用証明書及びポリシー情報を、ローカルキャッシュに保存すること、包囲されたエリアへの個人のアクセスを許可するためにアクセス要求を受信すること、アクセス要求を、キャッシュにおける信用証明書及びポリシー情報と比較すること、及び、比較が一致を示す場合に、包囲されたエリアへの個人のアクセスを認めることを、プロセッサに行わせる。

【０００５】

個人による資産へのアクセスを制御するためのアクセスコントローラを構成するための、プロセッサにより実行される方法は、資産へのアクセスを要求する個人に関する信用証明書及びポリシー情報をプロセッサが得る、信用証明書及びポリシーのディレクトリアドレスを受信する工程；信用証明書及びポリシー情報に関する宛先アドレスを受信する工程；信用証明書及びポリシー情報を獲得するための周期性を確立する工程；資産へのアクセスを必要とする個人に関する信用証明書及びポリシー情報を獲得する工程；及び、確立された周期性で資産へのアクセスを必要とする個人に関する信用証明書及びポリシー情報を自動的に更新する工程を含む。

【０００６】

自己プロビジョニング／自己レポーティングアクセスコントローラは、資産へのアクセスを制御するための機械命令を保存するための手段、及び、機械命令を実行するための手段を含む。実行するための手段は、自己プロビジョニングを行うための手段、機械命令を実行するための手段、資産へのアクセスを認める／拒否するための手段、及び、資産へのアクセスを認める及び拒否することに関連した事象を報告するための手段を含む。

【図面の簡単な説明】

【０００７】

詳細な記載は、同様の数字が同様のものを指す以下の図面について言及する：

【図１Ａ】アクセス制御システム、及びその選択されたコンポーネントを示す。

【図１Ｂ】アクセス制御システム、及びその選択されたコンポーネントを示す。

【図１Ｃ】アクセス制御システム、及びその選択されたコンポーネントを示す。

【図２】図１Ａ－１Ｃのシステムと共に使用されるアクセスコントローラの一例の要素及びコンポーネントを示す。

【図３】図２のアクセスコントローラを介して可能とされるインターフェースの一例を示す。

【図４】図２のアクセスコントローラのアクセス制御エンジンの一例を示す。

【図５Ａ】図１Ａ－１Ｃのシステム及び図２のアクセスコントローラの方法の例を示すフローチャートである。

【図５Ｂ】図１Ａ－１Ｃのシステム及び図２のアクセスコントローラの方法の例を示すフローチャートである。

【図５Ｃ】図１Ａ－１Ｃのシステム及び図２のアクセスコントローラの方法の例を示すフローチャートである。

【発明を実施するための形態】

【０００８】

認可された個人のみが、保護され又は確保されたエリアにアクセスすることを確実にすることは、極めて重要な場合がある（例えば、空港、軍事施設、オフィスビル等において）。保護され又は確保されたエリアは、物理的なドア（例えば、人間が入るドア）及び壁によって画定され得るか、又は、別の方法で実質的に画定され得る。例えば、保護された領域は、無許可の侵入が検出器に信号妨害を生じさせ、且つ、許可が与えられていない場合に恐らく信号を送信するか又は警報を鳴らすものとして、画定され得る。

【０００９】

アクセス制御システムは、侵入の許可を持つ個人のみに対して、建物、建物内の部屋、又は囲まれた領域、或いは、その中にある資産及び資源の、保護され又は確保されたエリアへの侵入を制限する場合がある。

【００１０】

故に、アクセス制御システムは基本的に、確保されたエリアに侵入するか又は資産にアクセスしようと試みる個人を識別して、その個人が現在侵入又はアクセスを許可されているかを確認しなければならない。本明細書に開示されたアクセス制御システム、デバイス、及び方法は、次のものを含む任意のアクセス技術を包含することもある。

【００１１】

（１）アクセス・ポイント（例えばドア）に関連付けられたキーパッドで入力することができるＰＩＮ及びパスワードの使用；

【００１２】

（２）ドアに関連付けられた特殊なリーダを介して個人が入力することができる生体認証の使用；

【００１３】

（３）ドアに関連付けられた特殊なパッドを介して個人により提供される従来の署名の使用；

【００１４】

（４）スマートカード又は非接触カードの使用（例えば、特殊なリーダ／受信器を介してドアにＰＩＮを送信する）；

【００１５】

（５）デジタル証明書の使用；例えば、カードリーダ又は他の受信器を介して「ドアに通信する」ことができる、スマートカード、非接触カード、又は無線装置に保存されるもの；及び

【００１６】

（６）ドアロックに挿入される物理的なキーの使用；そのようなキー／ロックの構造は、ロックの中で読み取られるキーに対する特殊な符号化を含み得る。

【００１７】

アクセス技術の上記のリストは、完全であることを意味してはいない。更に、設備の中には、これら技術の組み合わせを使用するものもある。この技術は、政府設備、民間企業、公共設備、及び個人の家を含む、任意の環境において使用されることがある。

【００１８】

上記のアクセス技術の幾つかの更なる説明として、幾つかの最新のアクセス制御システムは、個人がＰＩＮ又はパスワードを入力する、キーパッドなどの入力デバイスを備えたドアを使用する。キーパッドは、有効なＰＩＮ／パスワードのリストが保存される付属のメモリ又は基本プロセッサを備えており、それにより、ＰＩＮ／パスワードは、それがまだ有効であるかどうか判定するためにチェックされ得る。ＰＩＮ／パスワードが有効な場合、ドアが開き、有効でなければ、ドアは施錠されたままである。そのような基本のアクセス制御機構は、最小限のセキュリティを提供する。例えば、末端の従業員は、これ以上ドアを通り抜けることを認められない場合がある。しかし、自身のＰＩＮを覚えている末端の従業員は、未だにドアを開けることができる場合がある。それ故、末端の従業員のＰＩＮを「デプログラミングする（ｄｅｐｒｏｇｒａｍ）」ことが必要となる。しかし、このような手順は非常に扱いにくく、且つ高価な場合がある：設備は何百ものドアを備えており、従業員が退職する又は解雇される際に常にそのようなドアを全てデプログラミングすることは、非実用的な場合がある。

【００１９】

幾つかの最新のカードに基づくアクセス制御システムは、無線周波数識別（ＲＦＩＤ）技術を使用する。アクセス・カード・リーダは、ＲＦＩＤトランシーバを備え、アクセス・カードは、ＲＦＩＤタグ又はトランスポンダを備える。カードがＲＦＩＤトランシーバを通過すると、ＲＦＩＤトランシーバはカードに無線周波数（ＲＦ）クエリを送信する。

ＲＦトランスポンダは、カードがＲＦクエリを受信してそれに応答することを可能にする、シリコンチップ及びアンテナを備える。応答は典型的に、予めプログラムされた識別（ＩＤ）番号を含むＲＦ信号である。カードリーダは、信号を受信し、有線又は無線接続を使用して、制御パネルにＩＤ番号を送信する。最新のカードリーダは、制御パネルにデータを送信する前に、識別データの幾つかの基礎的なフォーマットを行なうが、一般的により高度なレベルの機能を行なうことは出来ない。

【００２０】

最新のアクセスコントローラは、信用証明書をプロビジョニング／デプロビジョニング（ｄｅ－ｐｒｏｖｉｓｉｏｎ）し、構成情報を提供し、取引を報告するために、専用のプロトコル（ｐｒｏｐｒｉｅｔａｒｙ　ｐｒｏｔｏｃｏｌ）及びソフトウェアに依存する。これら最新のアクセスコントローラの財産的価値は、変更を実施すること、新しい特徴を加えること、及び、特異的なメーカーの製品が選択され且つ設置された場合に他の技術解決策に一般的に移ることに関して、需要者の選択肢を制限する。アクセスコントローラが、ＲＳ２３２／４８５通信から離れて、ＴＣＰ／ＩＰネットワーク通信媒体上に移動すると、専用のプロトコルは需要者によって十分に許容されるものではない。

【００２１】

更に、物理的セキュリティシステムが、機関の情報技術（ＩＴ）インフラの信頼を高めると、ＩＴ部門は、展開のためのコストと時間を削減するための選択肢を探す場合がある。これは、システムが設置及び通信の両方における基準に従うことを要求する。更なる利益は、基準と民生用の製品とを使用する、論理的セキュリティシステムと物理的セキュリティシステムの間に相互運用性を提供する。

【００２２】

最新のアクセス制御システムに特有のこれら及び他の問題を克服するために、本明細書には、自己プロビジョニングを行うアクセスコントローラ、及び関連するアクセス制御システム、並びにそれらの使用の方法が開示される。本明細書に開示されたアクセスコントローラ、システム、及び方法は、建物、構造物、及びエリアへの物理的なアクセスの制御のために使用され得る。本明細書に開示されたアクセスコントローラ、システム、及び方法は、コンピュータネットワーク上に、分散したアクセス制御のポリシー、手順、及び信用証明書を提供し、その一方で既存の情報技術（ＩＴ）インフラを使用する。

【００２３】

物理的エリアなどの資産へのアクセスをプロビジョニング／デプロビジョニングすることに加えて、本明細書に開示されたアクセスコントローラ、システム、及び方法はまた、ファイル、コンピューティングリソース、又は他のコンピューティングシステムなどの論理的資産又は資源へのアクセスを提供するために、ユーザー／信用証明書の証明書ストア（ｉｄｅｎｔｉｔｙ　ｓｔｏｒｅ）に論理的な特権をプロビジョニングし得る。更に、論理的資産又は資源へのアクセスは、そのようなアクセスを要求する個人の物理的位置に依存して変わることもある。

【００２４】

アクセスコントローラ、制御システム、及び制御方法は、次の用語に関して以下に記載される：

【００２５】

アクセスコントローラ－　証明書ストアにより供給される、キャッシュされた（ｃａｃｈｅｄ）データベースに基づいてアクセス決定を行うために、プログラム化されたデバイス、又はプログラムそのもの。アクセス要求は感知デバイス（カードリーダ、プッシュボタン等）を介して行われる。許可は、ローカルで、又は、処理のために遠隔の証明書ストアに照会することにより、チェックされる。アクセス要求が承認される場合、出力及び入力デバイス／システム（例えば、入室ドア）は、アクセスを可能にするように操作される。

【００２６】

ドアコントローラ－　アクセスコントローラと通信し、且つ、信用証明書リーダ及び関

連付けた入出力ハードウェアに物理的に（例えば、有線式又は無線式で）取り付けられるデバイス。ドアコントローラは、状態変化及び信用証明書の読み取りをアクセスコントローラに送信し、アクセスコントローラからの許可応答を待ち、そして、許可応答に応じて、取り付けられた入力、出力、及び信用証明書のリーダに命令を行う。

【００２７】

ブラウザー　インターネットウェブページにアクセスし且つそれを表示するために使用されるソフトウェアプログラム又はファームウェア。最新のブラウザは、Ｉｎｔｅｒｎｅｔ　Ｅｘｐｌｏｒｅｒ、Ｇｏｏｇｌｅ　Ｃｈｒｏｍｅ、Ｍｏｚｉｌｌａ　Ｆｉｒｅｆｏｘ、及びＡｐｐｌｅ　Ｓａｆａｒｉを含む。

【００２８】

証明書ストア（又はディレクトリ）－　個人、信用証明書、資源、及びグループメンバーシップに対する許可及び許可データを含む、リレーショナルな、階層的な、ネットワーク化された、或いは他の構造を含むデータベース。証明書ストアは、保護されたエリアを所有する及び／又は操作する実体とは異なる実体によって所有され且つ操作される設備に存在することもある。

【００２９】

事象集合－　アクセスコントローラを操作する過程で生じるか又は生成される事象を複数のシステムに保存及び転送する、アクセスコントローラの能力。

【００３０】

一実施形態において、アクセスコントローラは、例えばＬｉｎｕｘ（登録商標）の運用システムを実行する民生用のコンピュータ上で実行することが可能なソフトウェアアプリケーションである。コンピュータは、アクセスコントローラなどの、デスクトップの、ラック実装可能な、クラウドベースの、又は埋め込み式のプラットホーム用に設計されてもよい。コンピュータは、ソフトウェアアプリケーションに必要なプロセッサ、ストレージ、及び接続性を提供する。必要なソフトウェアは全て、任意の他のコンピュータシステム上にソフトウェアをインストールすることを必要とすることなく、コンピュータに搭載される。

【００３１】

アクセスコントローラは、信用証明書及び関連付けられたアクセス権を維持するための、及び、専用の通信プロトコルへのアクセス又はさもなくばその使用を必要とすることなく既存の情報技術（ＩＴ）インフラ及びデータベースを用いてリアルタイムで事象を送信するための、改善された方法を提供する。

【００３２】

アクセスコントローラは、自己プロビジョニングを行うアクセスデバイスとして、信用証明書及び関連付けられたアクセス権のキャッシュされたリストを得て、それを維持し得る。これらのデータは、任意の他のアクセス制御システムへの通信を行うことなく、アクセスコントローラが現場のリアルタイムのアクセス決定を行うことを可能にする。信用証明書及び関連付けられたアクセス権のキャッシュは、スケジュール通りやリアルタイムのように定期的に１以上のホストシステムから、又は完全なスナップショットとして獲得され得る。例えば、アクセスコントローラは、事実上、アクセス信用証明書及び関連付けられたアクセス権のホストシステムのディレクトリに連続的にアクセスし、且つ、信用証明書及び権利の全ての幾つかをダウンロードし得る。一態様において、アクセスコントローラは、選択された数の個人に関するデータをダウンロードする。データがダウンロードされる個人は、独自で身元を明らかにされ、グループ関連付けにより身元を明らかにされ、或いは、割り当てられた役割により身元を明らかにされ得る。

【００３３】

アクセスコントローラは、ロギング及びモニタリングデバイス又はシステムにリアルタイムの事象を送信するために、リアルタイムで、オンデマンドで、又はスケジュール通りに使用され得る。一態様において、事象は、アクセスドアの解錠又は施錠、アクセスドアの開放又は閉鎖信号（例えば、リミットスイッチ又はポジションセンサから、或いは論理

的ルーチンに基づく）、アクセスドアの誤った又は異常な操作（変更可能な閾値を越える時間にわたり開く）等であり得る。事象は、ＸＭＬを含む任意の数のフォーマットで、任意の数のリモートデバイス又はシステムの機能をロギングするリレーショナルデータベース又はシステムに直接送信され得る。接続性が失われる場合、アクセスコントローラは事象をバッファ処理し、且つ、接続性が回復される場合には事象伝達を継続する場合がある。

【００３４】

アクセスコントローラは、ブラウザアクセス可能なユーザーインターフェースを包含し得るか、又はそれを提供し得る。このインターフェースは、アクセス権を伝えるために、任意の数のアクセス・ポイント（例えばドア）を構成し且つそれらを動作させるための性能、及び、個人及び／又はグループに対する関連付けられたマッピング（個人の基準、グループの基準、及び／又は画定された役割の基準に基づく）を、アクセス制御システムのオペレータに提供する。同じインターフェースでは、オペレータは、リレーショナルデータベース、ディレクトリ、又は階層データストア、或いは、カンマ・セパレイテッド・バリュー（ＣＳＶ）ファイルなどのフラットファイル、或いは任意の共通ＡＳＣＩＩファイルに実装されるか、又はそれを使用する信用証明書ソースを含む、信用証明書ソースと通信するためのアクセスコントローラを構成し得る。

【００３５】

インターフェースでは、オペレータは、時間間隔のもの（ｔｉｍｅｄ　ｉｎｔｅｒｖａｌ）、スケジュール通りのもの、オンデマンドのもの、及びリアルタイムのものを含む、一種のデータ同期を選択し、且つ構成する。同期方法は、サブスクリプション（ホストアクセスの信用証明書及びポリシーシステムがアクセスコントローラに情報変化を「配信する（ｐｕｓｈｅｓ）」もの）、監査証跡（アクセスコントローラが情報更新を要求するもの）、又は、データ修正トリガー（ｄａｔａ　ｍｏｄｉｆｉｃａｔｉｏｎ　ｔｒｉｇｇｅｒ）（ホストシステムに書き込まれたコードが、情報変化を検出し、アクセスコントローラに変更された情報を送信するもの）を含む場合がある。サブスクリプション方法は、ホストシステムとアクセスコントローラとの間に持続的な常時接続を必要とし、その一方で他の例となる２つの方法は一時的な接続を用いることもある。

【００３６】

アクセスコントローラは、ソースへの接続を開始して、コントローラのローカルキャッシュを構築するために信用証明書とポリシー情報を検索する。各個人は、複数のソースから１つのレコードへと個人の情報を照合するための固有識別子を有し得る。一旦ローカルキャッシュに転送されると、信用証明書がアクセス制御ポイントで示されるように、情報はアクセス決定において使用されてもよい。

【００３７】

アクセスコントローラは事象を記録し（ｌｏｇ）、この記録は、事象受信部として任意の数のデバイス、サービス、及びシステムを確立するためにユーザーインターフェースにより構成され得る。アクセスコントローラは、例えば、ＳＮＭＰ、直接のソケット接続を介するＸＭＬ（ＧＳＭ（登録商標）、ＬＡＮ、ＷＡＮ、ＷｉＦｉ）、Ｓｙｓｌｏｇを含む任意の数のフォーマットで、及び、シリアルポートを通じて、遠隔のモニタリングサービスに事象を送信し得る。

【００３８】

アクセスコントローラは事象に優先順位を割り当てるために使用され得る。事象の優先順位は、どの事象がどのような順で、遠隔のモニタリングサービスに送信されるのかを判定する。

【００３９】

図１Ａ－Ｃは、アクセス制御システム、及びその選択されたコンポーネントを示す。図１Ａにおいて、アクセス制御システム（１０）は、ドアシステム（２０）、アクセスコントローラ（１００）、信用証明書及びポリシーのディレクトリ（２００）、及び事象モニタリング作業端末（３００）を含み、それら全ては、エリア又は容量へのアクセスを制限

又は制御するように意図される。コントローラ（１００）は、例えば、ＴＣＰ／ＩＰバックボーン（５０）を使用して、ディレクトリ（２００）及び作業端末（３００）と通信する（１００）。ＴＣＰ／ＩＰバックボーン（５０）は有線式又は無線式、或いは、有線と無線の組み合わせでもよい。バックボーン（５０）は、インターネットを含むローカルエリアネットワーク（ＬＡＮ）及び広域ネットワーク（ＷＡＮ）の要素を含んでいてもよい。アクセスコントローラ（１００）とディレクトリ（２００）の間、及びコントローラ（１００）と作業端末（３００）の間の通信（１１０）は、安全な通信（例えばＨＴＴＰＳ通信）でもよい。

【００４０】

図１Ｂは、包囲されたエリア（１２）への個人によるアクセスを制限又は制御するための、アクセスシステム（１０）の選択されたコンポーネントを示す。示されるように、包囲されたエリア（１２）は、入口ドアシステム（２０）及び出口ドアシステム（２０）を備えた６面の構造物である。ドアシステム（２０）は図１Ａ及び１Ｃを参照の上、記載される。ドアシステム（２０）は通常の人間のアクセスのために意図される。他のアクセスポイント（例えば、窓）が存在してもよく、それらの操作は監視され、警報を発せられ、且つ制御されるものであってもよいが、そのようなアクセス・ポイントは本明細書ではこれ以上記載されない。

【００４１】

包囲されたエリア（１２）は、モニタを制御し、ドアシステム（２０）の操作を報告するアクセス制御特徴を実装する、コンピューティングプラットフォーム（１０１）を含む。コンピューティングプラットフォーム（１０１）は固定式又は移動式であってもよい。コンピューティングプラットフォーム（１０１）は包囲されたエリア（１２）の内部に示されるが、その内部にある必要はない。その制御、モニタリング、及びレポーティングの機能を実行する際に、そのアクセス制御特徴を備えたコンピューティングプラットフォーム（１０１）は、包囲されたエリア（１２）の外部で、ネットワーク（５０）を経由して（遠隔）ディレクトリ（２００）及び（遠隔）事象モニタリング作業端末（３００）と通信し得る。ネットワーク（５０）は有線式又は無線式であってもよく、且つ、非安全な通信及び信号伝達に加えて、安全な通信及び信号伝達を提供してもよい。

【００４２】

包囲されたエリア（１２）は、建物の中の部屋、建物自体、又は任意の他の構造物でもよい。包囲されたエリア（１２）は、６面の構成に限定されない。包囲されたエリア（１２）は、オープン構造（例えば競技場）、囲まれたエリア（例えば走路を取り囲むエリア）、又は「目に見えない」フェンス又は「仮想壁」があるエリアでもよい。包囲されたエリア（１２）は、地理的に固定される（例えば、建物、建物の中の部屋）、又は移動可能（例えば、トレーラー、飛行機、船、又はコンテナ）であってもよい。

【００４３】

包囲されたエリア（１２）は、中に含まれる政府又は企業機密の（ｃｌａｓｓｉｆｉｅｄ）文書又はデバイスへのアクセス、中に含まれるコンピュータシステムへのアクセス、個人へのアクセス、珍しい絵画や宝石などの高価な品へのアクセス、及び、危険物又はシステムへのアクセスを制御するために使用されてもよい。包囲されたエリア（１２）は、銀行の金庫又は貴重品保管室、原子炉用の制御室、機密の新技術の飛行機用の格納庫、又は空港の乗客口であってもよい。

【００４４】

移動式の構成において、包囲されたエリア（１２）は、例えば、世界のあらゆる場所に安全な設備を迅速に確立するための現場作業において使用されてもよい。そのような移動式の包囲されたエリア（１２）のセキュリティは、後述の議論から明白となる。更に、移動式の包囲されたエリアは、後述のように、ユーザーインターフェースを介して実施された単純な構成変化により、その用途に依存して、移動式の包囲されたエリア（１２）にアクセスすることが可能な異なる個人による、非常に異なる操作に使用されてもよい。故に、システム（１０）は、高度なセキュリティ、アクセス制御、事象モニタリング及びレポ

ーティングだけでなく、（アクセス制御が所望される）世界中のあらゆる場所での作業又は任務に移動式の包囲されたエリア（１２）を素早く適応させる柔軟性をも、提供する。

【００４５】

図１Ａに戻り、アクセスコントローラ（１００）はまた、ピアツーピア通信（１２０）を使用して、それらの間及び中で通信することができる。例えば、そのようなピアツーピア通信（１２０）は安全なＬＡＮの使用によって可能となり得る。代替的に、ピアツーピア通信（１２０）は無線式の安全な通信でもよい。ピアツーピア通信（１２０）はまた、ＴＣＰ／ＩＰプロトコルに従うものでもよい。

【００４６】

ピアツーピア通信（１２０）は、アクセスコントローラ（１００）が、包囲されたエリア（１２）において使用される他のアクセスコントローラ間でアクセス状況の情報及び事象を送受信することを可能にする。故に、ドアシステム（２０）が動作しない場合、その関連付けられたアクセスコントローラ（１００）は他のアクセスコントローラ（１００）にこの情報を提供してもよい。ピアツーピア通信（１２０）は、１つのアクセスコントローラ（１００）が親の（マスター）アクセスコントローラとして作用し、及び、残りのアクセスコントローラ（１００）が子の（補助的な）アクセスコントローラとして作用することを可能にする。この態様において、情報と構成は、親のアクセスコントローラに保存されるか又はそこで実装され、その後、子のアクセスコントローラ（１００）上で複製され得る。

【００４７】

最終的に、アクセスコントローラ（１００）は、有線又は無線式の安全な通信（１３０）を使用して、ドアシステム（２０）と通信することができる。

【００４８】

図１Ｂを参照してより詳細に記載されるドアシステム（２０）は、包囲されたエリア（１２）への通常の人間のアクセスを制御する。図１Ａの例において、６つのドアシステム（２０）が示される。一態様において、６つのドアシステム（２０）は、３つの包囲されたエリアのアクセス・ポイントを提供し、ドアシステム（２０）は対となって動作し、対となる１つのドアシステム（２０）は、包囲されたエリア（１２）への侵入を可能にし、他の対となるドアシステム（２０）は、包囲されたエリア（１２）からの退出を可能にする。別の態様において、１つのドアシステム（２０）は、包囲されたエリア（１２）への侵入とそこからの退出の両方に使用されてもよい。

【００４９】

図１Ａは、別個のアクセスコントローラ（１００）との通信している各ドアシステムの対を示す。しかし、コントローラ（１００）とドアシステム（２０）の他の組み合わせが、システム（１０）に実装されてもよい。例えば、１つのコントローラ（１００）は、包囲されたエリア（１２）のためにドアシステム（２０）を全て制御してもよい。

【００５０】

図１Ａに示される信用証明書及びポリシーのディレクトリ（２００）は、１以上の実ディレクトリを表わし得る。ディレクトリは、包囲されたエリア（１２）から遠方に位置してもよい。ディレクトリは、包囲されたエリア（１２）のオペレータ以外の実体によって操作されてもよい。例えば、包囲されたエリア（１２）は、政府請負業者のための感知式の区画化された情報施設（ＳＣＩＦ）でもよく、ディレクトリ（２００）は、政府請負業者のためのディレクトリ及び政府系機関のためのディレクトリを表わしてもよい。

【００５１】

ディレクトリ（２００）は、包囲されたエリア（１２）、個人の識別信用証明書（ＰＩＮ／パスワード、ＲＦＩＤタグ、証明書）、及び他の情報へのアクセスを許可される個人に関する識別情報（名前、年齢、身体的特徴、写真）を含み得る。

【００５２】

事象モニタリング作業端末（３００）は、包囲されたエリア（１２）のものと同じ実体によって実施されてもよい。代替的に、事象モニタリング作業端末（３００）は、別個の

実体により、及びその実体において、並びに包囲されたエリア（１２）の実体から離れて実施されてもよい。

【００５３】

事象モニタリング作業端末（３００）は、アクセスコントローラ（１００）から事象データを受信し得る。

【００５４】

図１Ｃは、図１Ａのシステムに実装され得るドアシステムの例を示す。図１Ｃにおいて、ドアシステム（２０）は通信路（１１０）を介してアクセスコントローラ（１００）と通信した状態で示される。ドアシステム（２０）は、アクセスドア（２２）、ドアロック機構（２４）、ドアコントローラ（２６）、及び信用証明書リーダ（２８）を備える。ドア（２２）は、個人が包囲されたエリアに侵入するか又はそこから離れることを可能にする任意のドアであってもよい。ドア（２２）は、ドア（２２）が完全に閉じていない時を示す位置検出器（例えば、リミットスイッチー示されず）を含んでもよい。位置検出器は、信号経路（２１）を介してドアコントローラ（２６）に完全に閉じていない信号を送信し得る。完全に閉じていない信号は、連続的又は定期的に送信されてもよく、且つ、予め定めた時間が過ぎた後まで送信されないこともある。

【００５５】

ロック機構は、ドアコントローラ（２６）から信号経路（２１）を介して送信される電気信号に応答して位置付けられる（施錠される又は解錠される）デッドボルトなどの、遠隔に動作された電気機械的なロック要素（図示せず）を含む。

【００５６】

ドアコントローラ（２６）は、信用証明書リーダ（２８）から信号経路（２９）を介して信用証明書情報を受信し、その情報を信号経路（１３０）を介してアクセスコントローラ（１００）に渡す。ドアコントローラ（２６）は、信号経路（１３０）を介してアクセスコントローラから施錠／解錠の信号を受信する。ドアコントローラ（２６）は、信号経路（２１）を介してロック機構の施錠／解錠の信号をロック機構（２４）に送信する。

【００５７】

信用証明書リーダ（２８）は、個人（４２）に関する信用証明書情報（４０）を受信する。信用証明書情報（４０）は、例えば、ＲＦＩＤチップ、スマートカード上の信用証明書、キーパッドを使用するＰＩＮ／パスワード入力、指紋及び網膜スキャンのデータなどのバイオメトリックデータにおいて、コード化されてもよい。

【００５８】

ドアシステム（２０）は、アクセスコントローラ（１００）に送信されるアクセス要求信号、及び、応答時にアクセスコントローラ（１００）から受信されるアクセス許可信号に基づいて、作動する。ドアシステム（２０）は、オートロック機能を組み込んでもよく、それは、ドア（２２）が開いて閉じた後、解錠信号がロック機構（２４）に送信されたがドア（２２）が特定の時間内に開かない後、又は、他の状態下での特定の時間内で、ドア（２２）を起動する（施錠する）。オートロックのロジックは、ドアコントローラ（２６）又はロック機構（２４）に実装されてもよい。

【００５９】

ドアシステム（２０）は、アクセスコントローラ（１００）経由で事象モニタリングシステム（３００）に事象信号を送信し得る。そのような信号は、ドアの開放、ドアの閉鎖、ロック機構の施錠、及びロック機構の解錠を含む。上記で注意されるように、信号は、ドアシステム（２０）においてリミットスイッチから生じてもよい。

【００６０】

一態様において、ドアシステム（２０）は侵入にのみ使用されてもよく、別個のドアシステム（２０）は退出にのみ使用されてもよい。

【００６１】

どのように構成されようと、ドアシステム（２０）は、侵入と退出それぞれの時点で個人（４２）の信用証明書情報を読み取ることによって得た情報に基づき、個人（４２）が

包囲されたエリア（１２）にいる時、及び、個人（４２）が包囲されたエリア（１２）から退出した時を示し得る。これらの信号は例えば、介在する退出無しに再侵入を防ぐために使用されてもよい。信号（又はそれらが無い（ａｂｓｅｎｓｅ））はまた、エリア及び包囲されたエリア内のシステムへのアクセスを防ぐために使用されてもよい。例えば、個人（４２）は、包囲されたエリア（１２）のドアシステム（２０）の１つから生じる侵入信号が無い状態で、包囲されたエリア（１２）において自身のコンピュータにログオンすることを認められないかもしれない。故に、アクセスコントローラ及びその実装されたセキュリティ機能は、個人が曝され得る階層式の一連のアクセス操作の第一歩かもしれない。

【００６２】

ドアシステム（２０）は、支えられて開いたドア（２２）、固く解錠されたロック機構（２４）、及び、破損又は不良の他の指標などに、様々な警報を組み込んでもよい。

【００６３】

図１Ａ－１Ｃは、建物又は建物の中の部屋等のエリアへの物理的アクセスに主に適用される、アクセス制御システム（１０）を記載する。しかし、上記に開示されるように、アクセス制御システム（１０）、及びその選択されたコンポーネントは、論理資源を含む機関の資産及び資源へのアクセスを制御するために使用され得る。例えば、自己プロビジョニングを行うアクセスコントローラ（１００）は、機関のコンピュータシステム、及び、コンピュータシステムに包含されるファイル（即ち、論理資源）へのアクセスを制御するために使用されてもよい。更に、アクセスコントローラ（１００）は、論理資源への段階的なアクセスを個人に提供するために自己プロビジョニングを行ってもよい。例えば、個人は、第１の包囲されたエリア中のファイル１－１０へのアクセス、及び、第２のより安全な包囲されたエリア中のファイル１－２０へのアクセスを許可される場合がある。この例において、第１の包囲されたエリアは建物であり、第２の包囲されたエリアは建物内のＳＣＩＦでもよい。故に、自己プロビジョニングを行うアクセスコントローラ（１００）は、物理的且つ論理的なアクセスを含む、個人のためのアクセス権に対して非常に洗練された制御を確立し、且つ、個人の信用証明書の読み取りによって示されるような個人の物理的位置に基づいて論理的アクセスを調整し得る。

【００６４】

図２は、図１Ａ－１Ｃのシステム（１０）と共に使用されるアクセスコントローラ（１００）の一例の要素及びコンポーネントを示す。図２において、アクセスコントローラ（１００）はコンピューティングプラットフォーム（１０１）上に実装された状態で示される。例えば、コンピューティングプラットフォーム（１０１）は、メインフレームコンピュータ、デスクトップコンピュータ、ラップトップコンピュータ又はタブレット、及びスマートフォンを含む、任意のコンピューティング装置でもよい。アクセスコントローラ（１００）は、ソフトウェア、ハードウェア、又はファームウェア、或いは、３つの任意の組み合わせとして実装されてもよい。ソフトウェアの中に実装される場合、アクセスコントローラ（１００）は、非一時的なコンピュータ可読記憶媒体に保存されてもよい。

【００６５】

コンピューティングプラットフォーム（１０１）はＬｉｎｕｘ（登録商標）の運用システムを使用してもよい。代替的に、他の運用システムを使用してもよい。コンピューティングプラットフォーム（１０１）はデータストア（１０２）を備え、それは順に、ローカルキャッシュ（１０３）（個人（４２）などの個人に関する信用証明書及びアクセスポリシー情報をローカルに保存するために使用され得るもの）、非一時的なコンピュータ可読記憶媒体（１０４）（アクセスコントローラ（１００）に保存され得るもの）、及び、事象バッファ（１０７）（事象モニタリング作業端末（３００）への伝達間、事象を一時的に保存し得るもの）を備える。コンピューティングプラットフォームは、ブラウザ（１０５）、プロセッサ（１０６）、及びメモリ（１０８）を更に含む。プロセッサ（１０６）は、アクセスコントローラ（１００）を含む実施用のプログラムを、データストア（１０２）からメモリ（１０８）の中へとロードしてもよい。

【００６６】
アクセスコントローラ（１００）は、ローカルキャッシュ（１０３）と通信し、及び、ブラウザ（１０５）を使用して、ディレクトリ（２００）などのディレクトリ、及び事象モニタリング作業端末（３００）などの他のコンピューティング装置と通信する。しかし、ディレクトリ（２００）及び作業端末（３００）との通信は、専用のローカルエリアネットワークなどを含む他の手段によるものでもよい。
【００６７】
アクセスコントローラ（１００）は、インターフェースエンジン（１５０）とアクセス制御エンジン（１９０）を備える。インターフェースエンジン（１５０）は、ユーザーインターフェース（１６０）（図３を参照）を提供し、これは、図３に関して詳述されるように、アクセスコントローラ（１００）による事象報告のための自己プロビジョニング特徴を確立するために、アクセス制御システム（１０）のオペレータ（人間）によって利用され得るものである。
【００６８】
アクセス制御エンジン（１９０）は、キャッシュ（１０３）を自己プロビジョニングするディレクトリ（２００）と通信して、自己プロビジョニングを行ったキャッシュ（１０３）に含まれる情報に基づいてドアシステム（２０）を操作する、ロジックを備える。アクセス制御エンジン（１９０）は、事象を記録し、且つ事象モニタリング作業端末（３００）に事象を報告するためのロジックを備える。ロジックは、アクセスコントローラ（１００）が事象を保存し、且つその事象を複数の宛先に報告する、事象集合を可能にし得る。アクセス制御エンジン（１９０）は、図４に関して詳述される。
【００６９】
図３は、図２のアクセスコントローラ（１００）を介して可能とされるユーザーインターフェース（１６０）の一例を示す。ユーザーインターフェース（１６０）は、包囲されたエリア（１２）のための任意の数のドアシステム（２０）を構成し且つその操作を制御する性能を、オペレータに提供する。ユーザーインターフェース（１６０）は、オペレータが、個人の身元、グループメンバーシップ、及び機関内の割り当てられた役割に基づき、許可された個人のマッピングを作成し、且つアクセス権を伝えることを可能にする。同じインターフェース（１６０）では、オペレータは、任意のリレーショナルデータベース、ディレクトリ又は階層データストアを含む、ディレクトリ（２００）などの信用証明書ソースと通信、或いは、ＣＳＶなどのフラットファイル又は任意の共通ＡＳＣＩＩファイルと通信するように、アクセスコントローラ（１００）を構成し得る。
【００７０】
図３に示されるように、一例のユーザーインターフェース（１６０）は、個人に関係する情報のためのアクセス・ウインドウ（１７０）、及び、事象に関係する情報のための事象・ウインドウ（１８０）を備える。個人のアクセス・ウインドウ（１７０）は、ディレクトリアドレス・ウインドウ（１７１）（オペレータがディレクトリ（２００）のアドレス（例えばＵＲＬ）を入力するもの）；個人名・ウインドウ（１７２）（個人の名前がプルダウンメニューに入力又は列挙され得るもの）；所属・ウインドウ（１７３）（個人の機関が入力され得るもの）；グループ・ウインドウ（１７４）（個人が属するグループが入力され得るもの）；役割・ウインドウ（１７５）（個人に割り当てられた役割又は作業が入力され得るもの）；識別番号・ウインドウ（１７６）（割り当てられた独自の識別が現われるもの）；アクセスレベル・ウインドウ（１７７）（個人のアクセスの最高レベルを列挙するもの）；及び、同期・ウインドウ（１７８）（信用証明書及びポリシーのディレクトリ（２００）への言及により個人のアクセスデータを更新するための周期性が指定され得るもの）を備える。ウインドウ（１７１）－（１７８）の幾つかは、プルダウンメニューの形式であってもよい。同期・ウインドウ（１７８）などの幾つかのウインドウは、一度表示され、その選択された値が全ての個人に適用される。ウインドウ（１７１）－（１７８）は、一度にオペレータのディスプレイに現われてもよい。一旦データが入力されると、オペレータは、選択を確認するための確認ページを提示され得る。全てのウイン

ドウが満たされる必要はない。１つの態様において、オペレータは、ディレクトリアドレス及び個人の名前を提供してもよく、残存データは、アクセスコントローラによってディレクトリ（２００）から検索される。更に、アクセスコントローラ（１００）は、リアルタイム又は連続的な照会に近い、周期的な基礎に基づいてディレクトリ（２００）に照会することにより、データを検索するか、又はリフレッシュさせ得る。代替的に、データは、例えば、長い間隔で、スケジュール通りに、又はオンデマンドで検索されてもよい。故に、アクセスコントローラ（１００）は、包囲されたエリア（１２）へのアクセスを要求する個人に関するアクセス制御情報により、それ自体を自己プロビジョニングすることができる。上述のように、検索されたデータはローカルキャッシュ（１０３）に保存され、アクセスコントローラ（１００）は、アクセス決定を下す場合にローカルキャッシュ（１０３）に照会する。

【００７１】

事象・ウインドウ（１８０）は、多くのデータ入力・ウインドウを提供し、これは更に、プルダウンメニューを備えてもよく、且つ、システムオペレータが、事象モニタリング作業端末（３００）に事象を報告するためのアクセスコントローラ（１００）の初期設定を確立するために使用し得るものである。事象・ウインドウ（１８０）は、事象名又はタイトル、概要、測定パラメータ、及び他の情報が入力され得る事象記載・ウインドウ（１８１）を備える。例えば、事象・ウインドウ（１８０）は、ドア開放事象、ドア開放測定を提供するデバイスの識別、ドア開放事象が意味するもの、及び、ドア開放事象が提供される形態を指定するために使用されてもよい。

【００７２】

事象・ウインドウ（１８０）は、システムオペレータが事象に優先順位を割り当てることができる、事象優先順位・ウインドウ（１８２）を更に備える。優先順位は、事象がアクセスコントローラ（１００）から事象モニタリング作業端末（３００）に送信される順序を判定し得る。故に、例えば、警報又は故障を示す事象は、ドア開放事象よりも上の優先順位を有し得る。

【００７３】

また更に、事象・ウインドウ（１８０）は、システムオペレータが事象モニタリング作業端末（３００）に事象を報告するために時間フレームを設定する、報告周期性・ウインドウ（１８３）を備える。

【００７４】

最終的に、事象・ウインドウ（１８０）は、システムオペレータが事象モニタリング作業端末（３００）のアドレスを入力する、報告宛先・ウインドウ（１８４）を備える。ウインドウ（１８４）を使用して、システムオペレータは、事象報告を受信するために多くの異なる実体を指定することができる。異なる実体は、異なる報告を受信し得る。例えば、第１の事象モニタリング作業端末は、ドア開放及びドア閉鎖の事象のみを受信し、一方で第２の事象モニタリング作業端末は全ての事象を受信し得る。指定先は同じ実体に属する必要はない。

【００７５】

図４は、アクセスコントローラ（１００）におけるアクセスエンジン（１９０）の例を示す。アクセスエンジン（１９０）は、自己プロビジョニングモジュール（１９１）、コンパレータ（１９５）、決定モジュール（１９６）、事象検出器／ロガー（１９７）、及び事象レポータ（１９８）を備える。

【００７６】

システム（１０）が多くのアクセスコントローラ（１００）を備える実施形態において、１つのアクセスコントローラ（１００）は、親のアクセスコントローラとして指定され、他のアクセスコントローラは、子のアクセスコントローラとして指定され得る。マスターアクセスコントローラは、ディレクトリ（２００）からデータを得て、その後、ピアツーピア通信（１２０）を使用して、子のアクセスコントローラに対し獲得データをコピーしてもよい。代替的に、各アクセスコントローラはディレクトリ（２００）と別々に通信

してもよい。
【００７７】
上記で注意されるように、本明細書に開示されたアクセス制御システム、デバイス、及び方法の１つの態様は、信用証明書とポリシーのディレクトリ（２００）から獲得したアクセス制御情報により自己プロビジョニングを行うアクセスコントローラ（１００）の性能であり、これは、アクセスコントローラ（１００）から遠方に位置してもよく、且つ、アクセスコントローラ（１００）を所有し且つ操作するもの以外の実体によって所有され、且つ操作されてもよい。自己プロビジョニングモジュール（１９１）は、自己プロビジョニング機能の幾つかを提供する。自己プロビジョニングモジュール（１９１）は、通信サブモジュール（１９２）、キャッシュフィラー（１９３）、及びキャッシュ通信装置（１９４）を備える。通信サブモジュール（１９２）は、恐らく複数のディレクトリ（２００）、アクセスコントローラ（１００）のどちらが信用証明書とポリシー情報を獲得し且つ更新するために対処されなければならないかを判定する。その後、サブモジュール（１９２）は、選択されたディレクトリ（２００）との安全な（暗号化された；例えばＨＴＴＰＳ）通信を確立し、情報を獲得する。代替的に、幾つかの情報は、非安全な（暗号を解読された）通信を使用して獲得されてもよい。
【００７８】
通信サブモジュール（１９２）はまた、リアルタイムで、リアルタイム付近で（例えば、事象の数秒以内で）、スケジュール通りに、事象モニタリング作業端末（３００）からオンデマンドで、又は幾つかの他の基礎に基づいて事象情報を送信するために、事象モニタリング作業端末（３００）との安全な（又は非安全な）通信を確立することもある。
【００７９】
通信サブモジュール（１９２）とディレクトリ（２００）と事象モニタリング作業端末（３００）の間の通信は、ブラウザ（１０５）経由で行われてもよい。通信サブモジュール（１９２）は、データの暗号化（発信要求／報告のため）、及び解読（ディレクトリ（２００）から受信されたデータパケット、又は事象モニタリング作業端末（３００）から受信された要求のため）を行なってもよい。
【００８０】
キャッシュフィラー（１９３）は、通信サブモジュール（１９２）から獲得情報を受信し、適宜ローカルキャッシュ（１０３）に投入する。キャッシュフィラー（１９２）は、キャッシュ（１０３）に情報を保存する前に受信情報に対してエラーチェックを実行してもよい。
【００８１】
キャッシュ通信装置（１９４）は、例えば、キャッシュ（１０３）に列挙される特定の個人へのアクセスを認めるためにドア（２２）を解錠すべきかどうかを判定するなどのために、アクセス制御エンジン（１９０）の他のコンポーネントに使用するためのキャッシュ（１０３）からデータを検索し得る。キャッシュ通信装置（１０４）は、システムオペレータがキャッシュを探索し、幾つか又は全てのキャッシュコンテンツの報告（表示）を受信することを可能にする、探索／表示機能を備えてもよい。その報告はインターフェース（１６０）に提供され、且つ印刷されてもよい。
【００８２】
コンパレータ（１９５）は、ドアシステム（２０）で獲得した信用証明書情報を受信し、キャッシュ（１０３）から適切な情報を検索するためにキャッシュ通信装置（１９４）と通信する。獲得した信用証明書情報及び検索された情報は、決定モジュール（１９６）に提供され、それは、包囲されたエリア（１２）への個人のアクセスを許容するように情報が（十分に）一致するかどうかを判定するものである。
【００８３】
事象検出器／ロガー（１９７）は、ドアシステム（２０）から信号を受信し、予め定めた事象に従い信号を分類し、報告可能な事象としてデータをフォーマット化して、事象バッファ（１０７）において事象を記録する。その後、事象レポータ（１９８）は、通信サ

ブモジュール（１９２）及びブラウザ（１０５）経由で事象モニタリング作業端末（３００）に、記録された事象を報告する。

【００８４】

図５Ａ－５Ｃは、図１Ａ－１Ｃのシステム及び図２－４のコンポーネントの方法の例を示すフローチャートである。

【００８５】

図５Ａと５Ｂは、アクセスコントローラ（１００）が信用証明書とポリシーのディレクトリ（２００）と事象モニタリング作業端末（３００）の情報（例えば、これらのデバイス／システムのＵＲＬ）を受信し、その情報がアクセスコントローラ（１００）を構成するために使用される場合に、ブロック（５０５）において開始する、方法（５００）を示す。複数のアクセスコントローラ（１００）を備えるアクセス制御システムにおいて、第１（親）のアクセスコントローラの構成は、残り（子）のアクセスコントローラにコピーされてもよい。

【００８６】

ブロック（５１０）において、ディレクトリ情報は、包囲されたエリア（１２）へのアクセスを要求する１以上の個人に関する信用証明書とポリシー情報を獲得するために使用される。

【００８７】

ブロック（５１５）において、このように獲得した信用証明書及びポリシー情報は、各アクセスコントローラ（１００）のローカルキャッシュにロードされる。

【００８８】

ブロック（５２０）において、アクセスコントローラ（１００）は、個人（４２）が（特定のドア（２２）を通って）包囲されたエリア（１２）に侵入する（又は退出する）ことを可能にするためのアクセス要求を受信する。アクセス要求は、信用証明書（４０）からのデータ読み取りに基づいてもよい。

【００８９】

ブロック（５２５）において、受信した要求からの情報は、個人（４２）に関するキャッシュ（１０３）における信用証明書及びポリシー情報を検索するためにアクセスコントローラ（１００）において使用され、その後、検索された情報はアクセス要求に含まれるものと比較される。

【００９０】

ブロック（５３０）において、アクセスコントローラ（１００）は、個人（４２）が包囲されたエリア（１２）にアクセスすることを可能にするように比較が十分な一致を示すかどうかを判定する。例えば、キャッシュ（１０３）から検索された情報の各項目は、証明書（４０）から読み取られるものに正確に一致することを要求され得る。ブロック（５３０）において、一致すると判定された場合、方法（５００）はブロック（５３５）に移る。一致していないと判定された場合、方法（５００）はブロック（５４５）に移る。

【００９１】

ブロック（５３５）において、アクセスコントローラ（１００）は、ドアシステム（２０）に解錠信号を送信する。ブロック（５４０）において、アクセスコントローラ（１００）は、その後、（個人（４２）を許可するために）ドア（２２）が開いており、次に閉じてロックされているかどうかを判定するためにドアシステム（２０）の操作をモニタリングする。

【００９２】

ブロック（５４５）において、システム（１０）に実装される場合、アクセスコントローラ（１００）は、ディレクトリ（２００）にアクセス要求を送信し、それは、信用証明書（４０）から受信した情報が個人（４２）に関するディレクトリ（２００）におけるものに一致するかどうかを判定するために自身の内部処理を使用するものである。

【００９３】

ブロック（５５０）において、アクセスコントローラ（１００）は、一致している又は

一致していないことを示す、ディレクトリ（２００）から信号を受信する。一致していると示された場合、方法（５００）はブロック（５４０）に移る。一致していないと示された場合、方法（５００）はブロック（５５５）に移り、アクセスコントローラ（１００）は個人（４２）へのアクセスを拒否する。

【００９４】

ブロック（５６０）において、ブロック（５４０）の操作に続き、アクセスコントローラ（１００）は、ドアシステム（２０）から事象情報を受信し、事象情報を事象へとフォーマット化し、事象モニタリング作業端末（３００）に事象を送信する。

【００９５】

ブロック（５５５）又は（５６０）の後、方法（５００）はブロック（５６５）に移り、終了する。

【００９６】

図５Ｃは、具体的にはアクセスコントローラ（１００）を構成するための、図５Ａのブロック（５０５）のプロセスの態様の一例を示すフローチャートである。図５Ｃにおいて、方法（５００）は、包囲されたエリア（１２）へのアクセスを要求する個人（４２）に関する信用証明書とポリシー情報をアクセスコントローラ（１００）が獲得する、ディレクトリ（元の）アドレスを設定するために、システムオペレータがインターフェース（１６０）を使用する場合に、ブロック（５７１）において始まる。ブロック（５７３）において、宛先アドレス（即ち、キャッシュ（１０３）のアドレス）が設定される。ブロック（５７５）において、同期時間が設定される。ブロック（５７７）において、アクセスコントローラは、自身の信用証明書と関連情報がキャッシュ（１０３）に入力されることになっている、特定の個人（４２）の指標を受信する。

【００９７】

ブロック（５７９）において、アクセスコントローラは、アクセスコントローラ（１００）によってモニタリングされる事象の画定を受信する。この事象は予め画定されてもよく、又は、例えばインターフェース（１６０）を使用して、システムオペレータによって確立され且つ画定されてもよい。ブロック（５８１）において、アクセスコントローラ（１００）は、事象情報を受信する事象モニタの宛先アドレスを受信する。ブロック（５８３）において、アクセスコントローラ（１００）は、要求される報告の間隔又は周期性を受信する。最終的に、ブロック（５８５）において、アクセスコントローラ（１００）は、どんな情報が各事象と共に提供又は記録されることになっているかを定めるパラメータを受信する。その後、方法（５０５）は終了する。

【００９８】

図面に示されるデバイスの幾つかは、コンピューティングシステムを備える。コンピューティングシステムは、プロセッサ（ＣＰＵ）、及び読み取り専用メモリ（ＲＯＭ）及びランダムアクセスメモリ（ＲＡＭ）などのシステムメモリを含む様々なシステムコンポーネントをプロセッサに結合するシステムバスを備える。他のシステムメモリも同様に、使用のために利用可能であってもよい。コンピューティングシステムは、より大きな処理能力を提供するために、１より多くのプロセッサ、又は、共にネットワーク化されたコンピューティングシステムのグループ又はクラスタを備えてもよい。システムバスは、様々なバス方式の何れかを用いるメモリバス又はメモリコントローラ、周辺バス、及びローカルバスを含む、様々なタイプのバス構造の何れかであってもよい。ＲＯＭなどに保存される基礎的な入力／出力（ＢＩＯＳ）は、スタートアップなどの間に、コンピューティングシステム内の要素間で情報を転送するのを支援する、基礎的なルーチンを提供し得る。コンピューティングシステムは更に、既知のデータベース管理システムに従いデータベースを維持する、データストアを備える。データストアは、ハードディスクドライブ、磁気ディスクドライブ、光ディスクドライブ、テープドライブ、又は、プロセッサによりアクセス可能なデータを保存することができる別のタイプのコンピュータ可読媒体（磁気カセット、フラッシュメモリカード、デジタル多用途ディスク、カートリッジ、ランダムアクセスメモリ（ＲＡＭ）、及び読み取り専用メモリ（ＲＯＭ）など）などの、多くの形態で具現

化されてもよい。データストアは、ドライブインターフェースによってシステムバスに接続されてもよい。データストアは、コンピュータ読み取り可能な指示、データ構造、プログラムモジュール、及び他のデータの不揮発性記憶装置を、コンピューティングシステムに提供する。

【００９９】

人間（及び、幾つかの例では機械）のユーザーとの対話処理を可能にするために、コンピューティングシステムは、音声及びオーディオ用のマイクロホン、ジェスチャ又は図形入力用のタッチ感知式スクリーン、キーボード、マウス、動作入力などの入力デバイスを備えてもよい。出力デバイスは、多くの出力機構の１以上を備え得る。幾つかの例において、多モードシステムにより、ユーザーは、コンピューティングシステムと通信するために複数のタイプの入力を提供することが可能となる。通信用インターフェースにより、通常、コンピューティングデバイスシステムは、様々な通信及びネットワークのプロトコルを使用して、１以上の他のコンピューティングデバイスと通信することが可能となる。

【０１００】

前述の開示は、図５Ａ－５Ｃに表わされた実施形態を示すためのフローチャート及び付随の説明について言及する。開示されたデバイス、コンポーネント、及びシステムは、示された工程を実行するための任意の適切な技術を使用又は実施することを考慮する。故に、図５Ａ－５Ｃは例示のみを目的とするものであり、記載の又は同様の工程は、同時に、個別に、又は組み合わせを含む、任意の適切な時間で実行されてもよい。加えて、フローチャートの工程は、同時に、及び／又は、示され且つ記載されるものとは異なる順で生じる場合もある。更に、開示されたシステムは、追加の、少数の、及び／又は異なる工程を伴うプロセス及び方法を使用してもよい。

【０１０１】

本明細書に開示された実施形態は、本明細書に開示された構造及びその同等物を含む、デジタル電子回路、コンピュータソフトウェア、ファームウェア、又はハードウェアに実装することができる。幾つかの実施形態は、１以上のプロセッサによる実施のためにコンピュータ記憶装置媒体上にコード化される、１以上のコンピュータプログラム（即ち、コンピュータプログラム命令の１以上のモジュール）として実装することができる。コンピュータ記憶装置媒体は、コンピュータ可読記憶デバイス、コンピュータ可読記憶基板、又は、ランダム或いはシリアルアクセスメモリであるか、又はそれらに含まれ得る。コンピュータ記憶装置媒体はまた、複数のＣＤ、ディスク、又は他の記憶デバイスなどの１以上の別個の物理的コンポーネント又は媒体であるか、又はその中に含まれ得る。コンピュータ可読記憶媒体は一時的な信号を含まない。

【０１０２】

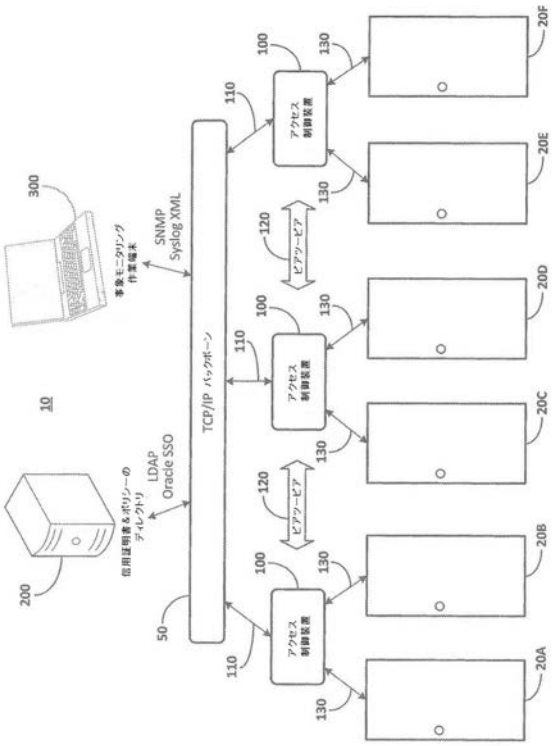
本明細書に開示された方法は、１以上のコンピュータ可読記憶デバイスに保存される、又は他のソースから受信されるデータ上でプロセッサにより行なわれた操作として実施することができる。

【０１０３】

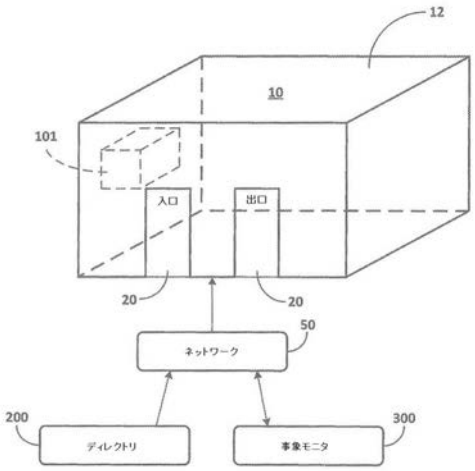
コンピュータプログラム（プログラム、モジュール、エンジン、ソフトウェア、ソフトウェアアプリケーション、スクリプト、又はコードとしても知られる）は、コンパイルされた又は通訳された言語、宣言型又は手続型言語を含む任意の形態のプログラミング言語で書くことができ、且つ、独立プログラム又はモジュールとして、コンポーネント、サブルーチン、オブジェクト、又はコンピュータ環境での使用に適した他のユニットを含む任意の形態で配置することができる。コンピュータプログラムはファイルシステム中のファイルに対応するが、層である必要はない。プログラムは、他のプログラム又はデータ（例えば、マークアップ言語文書に保存される１以上のスクリプト）を保持するファイルの一部に、問題のプログラム専用の１つのファイルに、又は、複数の統合ファイル（例えば、１以上のモジュール、サブプログラム、又はコードの一部を保存するファイル）に、保存することができる。コンピュータプログラムは、１つの場所に位置するか、又は、複数の場所に分布され且つ通信ネットワークにより相互接続される、１つのコンピュータ又は複

数のコンピュータ上で実行されるように、配置することができる。

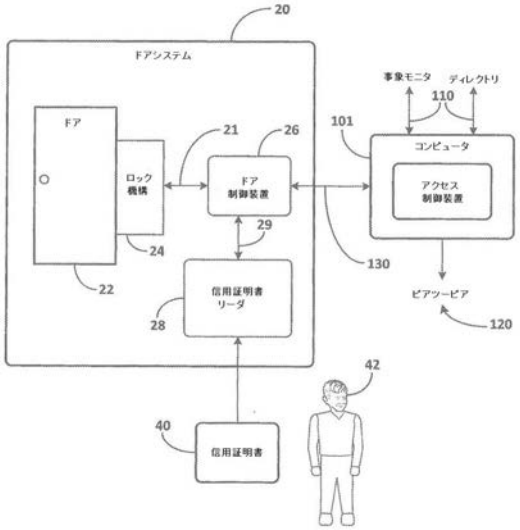
【図１Ａ】



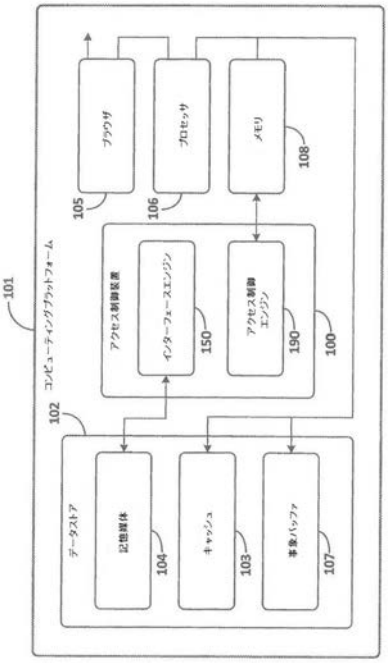
【図１Ｂ】



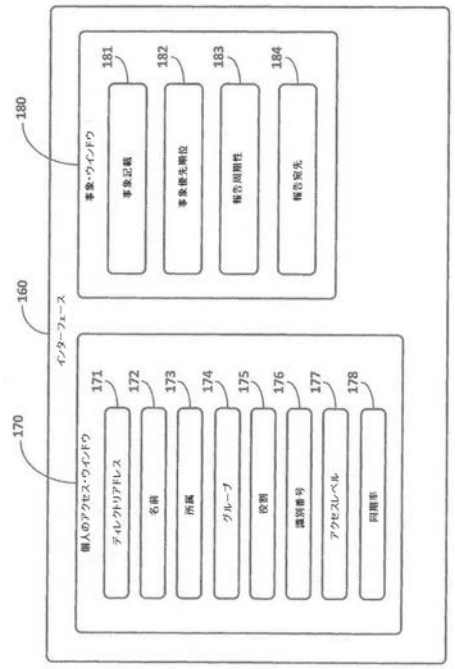
【図１Ｃ】


20
Fアシステム
事象モニタ
ディレクトリ
110
Fア
ロック機構
21
26
Fア制御装置
101
コンピュータ
アクセス制御装置
29
24
130
22
信用証明書リーダ
ピアツーピア
120
28
42
40
信用証明書

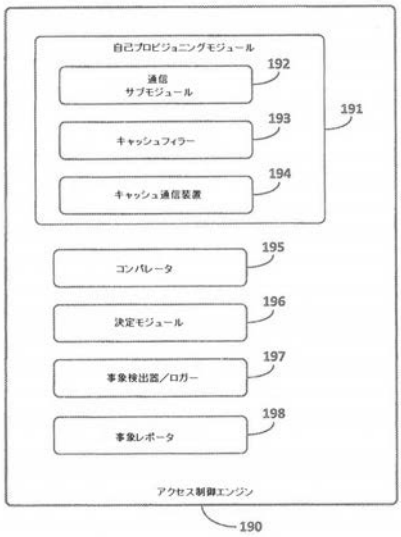
【図２】


101
コンピューティングプラットフォーム
ブラウザ
プロセッサ
メモリ
105
106
108
アクセス制御装置
インターフェースエンジン
アクセス制御エンジン
150
190
100
102
データストア
記憶媒体
キャッシュ
事象バッファ
104
103
107

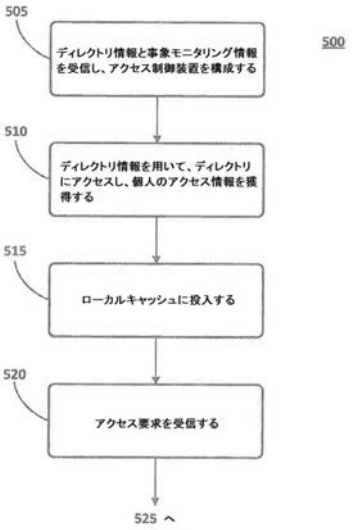
【図３】


180
事象・ウインドウ
181
事象記載
182
事象優先順位
183
報告周期性
184
報告宛先
160
インターフェース
170
個人のアクセス・ウインドウ
171
ディレクトリアドレス
172
名前
173
所属
174
グループ
175
役割
176
識別番号
177
アクセスレベル
178
同期率

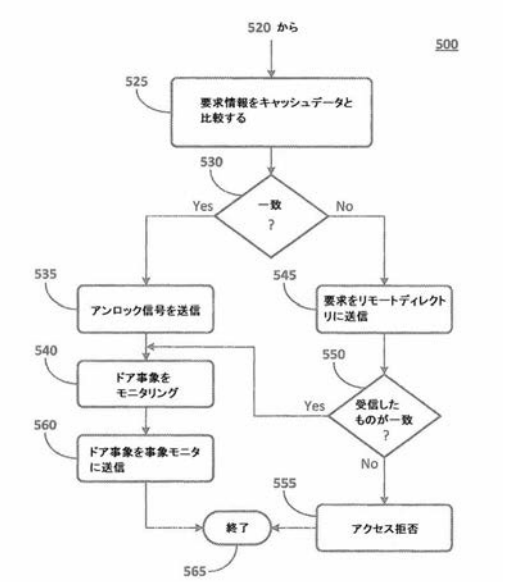
【図４】


自己プロビジョニングモジュール
通信サブモジュール
192
キャッシュフィラー
193
キャッシュ通信装置
194
191
コンパレータ
195
決定モジュール
196
事象検出器／ロガー
197
事象レポータ
198
アクセス制御エンジン
190

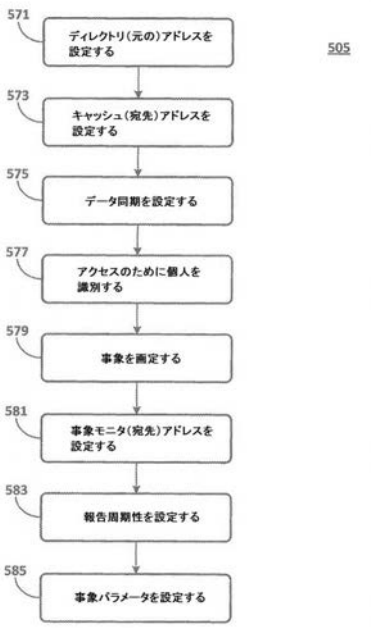
【図５Ａ】


500
505
ディレクトリ情報と事象モニタリング情報を受信し、アクセス制御装置を構成する
510
ディレクトリ情報を用いて、ディレクトリにアクセスし、個人のアクセス情報を獲得する
515
ローカルキャッシュに投入する
520
アクセス要求を受信する
525 へ

【図５Ｂ】


520 から
500
525
要求情報をキャッシュデータと比較する
530
一致？
Yes
No
535
アンロック信号を送信
545
要求をリモートディレクトリに送信
540
ドア事象をモニタリング
550
受信したものが一致？
Yes
No
560
ドア事象を事象モニタに送信
555
アクセス拒否
終了
565

【図５Ｃ】


505
571
ディレクトリ(元の)アドレスを設定する
573
キャッシュ(宛先)アドレスを設定する
575
データ同期を設定する
577
アクセスのために個人を識別する
579
事象を画定する
581
事象モニタ(宛先)アドレスを設定する
583
報告周期性を設定する
585
事象パラメータを設定する

【手続補正書】
【提出日】令和1年9月11日(2019.9.11)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
プロセッサにより実行されるアクセス制御方法であって：
アクセス制御エリアに物理的に位置付けられたプロセッサにおいて、アクセスコントローラによる信用証明書及びポリシーのディレクトリの周期的な自動化したクエリを介してアクセスコントローラの自己プロビジョニングを可能にするように、信用証明書及びポリシーのディレクトリ情報をリアルタイムでホストシステムのリモートディレクトリから直接受信する工程；
アクセス制御エリアへのアクセスを必要とし得る１以上の個人に関する信用証明書及びポリシー情報を、プロセッサを用いて信用証明書及びポリシーのディレクトリから獲得する工程；
獲得した信用証明書及びポリシー情報を、プロセッサによりアクセス可能なローカルキャッシュに保存する工程；
信用証明書及びポリシーのディレクトリからの、信用証明書及びポリシー情報の更新を、プロセッサにより周期的に要求する工程；
周期的な要求に応答して、信用証明書及びポリシー情報の更新を、プロセッサにおいて受信する工程；
信用証明書及びポリシー情報の更新に基づきローカルキャッシュを更新する工程；
アクセス制御エリアへの個人のアクセスを許可するためにアクセス要求をプロセッサにおいて受信する工程；
プロセッサにより、アクセス要求を、ローカルキャッシュにおける信用証明書及びポリシー情報と比較する工程；及び
比較が一致を示す場合にアクセス制御エリアへの個人のアクセスを認める工程
を含む方法。
【請求項２】
アクセス制御エリアは包囲されたエリアである、ことを特徴とする請求項１に記載の方法。
【請求項３】
包囲されたエリアは複数のアクセスコントローラを備え、且つ、アクセスコントローラを構成する工程は：
ユーザーインターフェースを介して第１のアクセスコントローラを構成する工程；及び
他のアクセスコントローラの各々における構成を自動的に複製する工程
を含む、ことを特徴とする請求項２に記載の方法。
【請求項４】
ディレクトリ情報はディレクトリのＵＲＬを含む、ことを特徴とする請求項２に記載の方法。
【請求項５】
比較は、アクセス要求における情報と、ローカルキャッシュにおける対応する信用証明書及びポリシー情報との完全な一致を要求する、ことを特徴とする請求項２に記載の方法。
【請求項６】
アクセスを認めるために包囲されたエリアへのアクセスドアを解錠する工程を更に含む、ことを特徴とする請求項２に記載の方法。

【請求項７】
事象モニターのアドレスをプロセッサにより受信する工程；
事象画定情報を受信する工程；及び
受信した事象画定情報に応じて事象をモニタリングし且つ収集するようにアクセスコントローラを構成する工程
を更に含む、ことを特徴とする請求項２に記載の方法。
【請求項８】
収集した事象をバッファ処理し、それを事象モニターに報告するようにアクセスコントローラを構成する工程を更に含む、ことを特徴とする請求項７に記載の方法。
【請求項９】
プロセッサは、複数の事象モニターの各々のアドレスを受信し、ここで、方法は複数の事象モニターの複数のアドレスに事象を同時に送信する工程を含む、ことを特徴とする請求項８に記載の方法。
【請求項１０】
事象は、ドアの開放、ドアの閉鎖、ドアの開固着、ドアの施錠、及びドアの解錠を含む、ことを特徴とする請求項９に記載の方法。
【請求項１１】
アクセス要求は、アクセス制御エリアにおいて資源にアクセスするための要求である、ことを特徴とする請求項１に記載の方法。
【請求項１２】
資源は論理資源である、ことを特徴とする請求項１１に記載の方法。
【請求項１３】
アクセスコントローラは、資源に対する個人の位置に基づいて資源へのアクセスを自己プロビジョニングする、ことを特徴とする請求項１１に記載の方法。
【請求項１４】
比較が一致を示さない場合、方法は、一致を判定するために信用証明書及びポリシーのディレクトリにアクセス要求を送信する工程を含む、ことを特徴とする請求項１に記載の方法。
【請求項１５】
更新はリアルタイムで継続的に行われる、ことを特徴とする請求項１に記載の方法。
【請求項１６】
個人によるエリアへのアクセスを制御するためのシステムであって；
前記エリアに物理的に位置付けられるプロセッサ；及び
コンピュータ可読記憶媒体に具現化されるソフトウェアアプリケーションであるアクセスコントローラ
を含み、
前記アクセスコントローラは機械命令を含み、該機械命令は、プロセッサにより実行された場合、少なくとも：
アクセスコントローラによる信用証明書及びポリシーのディレクトリの周期的な自動化したクエリを介してアクセスコントローラの自己プロビジョニングを可能にするように、リアルタイムでホストシステムのリモートディレクトリからの信用証明書及びポリシーのディレクトリ情報を直接受信し、及び
エリアへのアクセスを必要とし得る１以上の個人に関する、信用証明書及びポリシーのディレクトリからの信用証明書及びポリシー情報を受信するように、システムを構成すること；
信用証明書及びポリシーのディレクトリの受信された信用証明書及びポリシーのディレクトリの情報、並びに、１以上の個人の信用証明書及びポリシー情報を、プロセッサによりアクセス可能なローカルキャッシュに保存すること；
信用証明書及びポリシーのディレクトリからの、信用証明書及びポリシー情報の更新を周期的に要求すること；

周期的な要求に応答して、信用証明書及びポリシー情報の更新を、プロセッサにおいて受信すること；
信用証明書及びポリシー情報の更新に基づきローカルキャッシュを更新すること；
包囲されたエリアへの１以上の個人の中の１個人のアクセスを許可するためにアクセス要求を受信すること；
アクセス要求を、ローカルキャッシュにおける信用証明書及びポリシー情報と比較すること；及び
比較が一致を示す場合に、エリアへの個人のアクセスを認めること
を、プロセッサに行わせる
ことを特徴とするシステム。
【請求項１７】
エリアは複数のアクセスコントローラを備え、且つ、アクセスコントローラを構成する場合、プロセッサは：
ユーザーインターフェースを介して第１のアクセスコントローラを構成し；及び
他のアクセスコントローラの各々における構成を自動的に複製する
ことを特徴とする請求項１６に記載のシステム。
【請求項１８】
ディレクトリ情報は、ディレクトリのＵＲＬを備え、ここで、ディレクトリとプロセッサはＴＣＰ／ＩＰプロトコルを使用して通信する、ことを特徴とする請求項１６に記載のシステム。
【請求項１９】
プロセッサは、予め確定された事象確定情報に従い、事象をモニタリングし且つそれを収集するようにアクセスコントローラを構成する、ことを特徴とする請求項１６に記載のシステム。
【請求項２０】
収集した事象を保存するためのバッファを更に備える、ことを特徴とする請求項１９に記載のシステム。
【請求項２１】
プロセッサは、複数の事象モニターの各々のアドレスを受信し、ここで、プロセッサは複数の事象モニターの複数のアドレスに事象を同時に送信する、ことを特徴とする請求項２０に記載のシステム。
【請求項２２】
アクセスコントローラの自己プロビジョニング／自己レポーティングのための方法であって：
アクセス制御エリアにおける資産へのアクセスを制御するための機械命令を保存する工程であって、該機械命令は、アクセス制御エリアに物理的に位置付けられたメモリに保存される、工程；及び
機械命令をアクセスコントローラにより実行する工程であって：該工程は、
アクセス制御情報を自己プロビジョニングする工程であって、
ホストシステムのリモートディレクトリからアクセス制御情報のディレクトリアドレスをリアルタイムで要求し、そこからアクセスコントローラが資産へのアクセスを必要とする個人に関するアクセス制御情報を取得する工程、
アクセス制御情報の宛先アドレスを受信する工程、
アクセス制御情報のディレクトリアドレスおよび宛先アドレスに基づいて、資産へのアクセスを必要とする個人に関するアクセス制御情報を周期的に自己プロビジョニングする工程、および
確立された周期で、資産へのアクセスを必要とする個人に関するアクセス制御情報を備えるメモリのローカルキャッシュを自動的に更新する工程、により、アクセス制御情報を自己プロビジョニングする工程、
アクセス制御情報に基づき資産へのアクセスを認める又は拒否する工程、及び

資産へのアクセスの容認及び拒否に関連する事象を報告する工程
を更に含む工程
を含む、方法。
【請求項２３】
自己プロビジョニングする工程は：
信用証明書及びポリシーのディレクトリとの通信を確保する工程；
信用証明書及びポリシーのディレクトリから得た信用証明書及びポリシー情報を、メモリに保存する工程；及び
保存した信用証明書及びポリシー情報を更新する工程
を含む、ことを特徴とする請求項２２に記載の方法。
【請求項２４】
資産へのアクセスの容認及び拒否に関連する事象を報告する工程は：
メモリにおける事象をバッファ処理する工程；及び
複数のモニタリングシステムに事象を報告する工程
を含む、ことを特徴とする請求項２２に記載の方法。

【外国語明細書】
2020013591000001.pdf