(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5270655号
(P5270655)
(45)発行日　平成25年8月21日(2013.8.21)　(24)登録日　平成25年5月17日(2013.5.17)

(51)Int.Cl.　F I
G06Q 10/06 (2012.01)　G06Q 10/06　130

請求項の数 8　(全 47 頁)

(21)出願番号	特願2010-293199(P2010-293199)
(22)出願日	平成22年12月28日(2010.12.28)
(62)分割の表示	特願2008-513614(P2008-513614)の分割
原出願日	平成18年5月22日(2006.5.22)
(65)公開番号	特開2011-76629(P2011-76629A)
(43)公開日	平成23年4月14日(2011.4.14)
審査請求日	平成22年12月28日(2010.12.28)
(31)優先権主張番号	60/683,928
(32)優先日	平成17年5月23日(2005.5.23)
(33)優先権主張国	米国(US)

(73)特許権者　507383220
エスエーピー・ガバナンス・リスク・アンド・コンプライアンス・インコーポレーテッド
アメリカ合衆国・カリフォルニア・９４５３８・フレモント・フレモント・ブールバード・４７２５７
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100064908
弁理士　志賀　正武
(74)代理人　100089037
弁理士　渡邊　隆
(74)代理人　100110364
弁理士　実広　信哉

最終頁に続く

(54)【発明の名称】リアルタイムのリスク分析およびリスク処理のための組み込みモジュール

(57)【特許請求の範囲】
【請求項１】
セキュリティシステムであって、
役割と任命のレコードであって、各役割は許可されたタスクの集まりを含み、前記任命は役割を人々に関連付ける、役割と任命のレコードと、
ユーザを認証する段階と認証されたユーザに、前記ユーザに任命されている役割により許可される場合にのみ物理的設備へのアクセス権を選択的に与える段階とを含むタスクを実行するようにプログラムされている1つまたは複数のサブシステムと、
前記サブシステムに結合されたマネージャであって、
役割と任命の前記レコードへのユーザ提案された変更の通知を受け取る段階と、
前記通知に応答して、前記提案された変更を分析して、1人の人が、特定の物理的設備への同時アクセスが可能であるため所定の役割分担ガイドラインに違反する可能性を識別する段階と、
前記分析オペレーションで前記所定の役割分担ガイドラインに違反する可能性を識別しない場合のみ前記提案された変更を許可する段階と、を備えるオペレーションを実行するようにプログラムされているマネージャと、を備えるセキュリティシステム。
【請求項２】
前記物理的設備は、(1)ドアロック、警報システム、アクセスゾーン、コントローラ、ブームゲート、エレベーター、カード読み取り装置、バイオメトリック読み取り装置、無線ICタグ(RFID)読み取り装置、登録者識別読み取り装置を含む群の遠隔操作設備セキュリ

ティコンポーネント、(2)コピー機、POSシステム、輸送アクセスポイント、冷暖房空調(HVAC)システムおよびコンポーネントを含む群の機器のうちの少なくとも1つを含む請求項１に記載のシステム。

【請求項３】

前記マネージャは、さらに、

所定の基準を物理的設備への人々のアクセス能力に適用し、前記基準が満たされた場合に必ずアラートを発行する段階を含む追加のオペレーションを実行するようにプログラムされている請求項１に記載のシステム。

【請求項４】

前記マネージャは、さらに、

少なくとも所定の最小期間の間、1人の人が1つの場所に留まっていることが判明した場合に必ずアラートを発行する段階を含む追加のオペレーションを実行するようにプログラムされている請求項１に記載のシステム。

【請求項５】

前記マネージャは、さらに、

1人の人が所定の作業場所から離れている時間が所定の最小期間を満たさない場合に必ずアラートを発行する段階を含む追加のオペレーションを実行するようにプログラムされている請求項１に記載のシステム。

【請求項６】

前記マネージャは、さらに、

指定された物質を保管するために割り当てられている物理的空間内に1人の人が居るため、その人がそのような物質への指定暴露限度に達していることが判明した場合に、必ずアラートを発行する段階を含む追加のオペレーションを実行するようにプログラムされている請求項１に記載のシステム。

【請求項７】

規定されているガイドラインを順守しているか構成クライアントサブシステムを監視するためのコンピュータ駆動システムであって、前記クライアントサブシステムは、(1)定義済み役割および任命により許可されたユーザ要求ビジネス活動を選択的に実行する1つまたは複数のコンピュータベースビジネスアプリケーション(CBBA)サブシステム、および(2)定義済み役割および任命により許可された物理的設備へのアクセスを選択的に行えるようにする1つまたは複数のセキュリティサブシステムと、を備え、各サブシステムは、役割と任命のレコードを含み、各役割は許可されたタスクの集まりを含み、各任命は1つまたは複数の役割を1人または複数の人々に関連付け、前記システムは、

マシン可読リスクフレームワークと、

前記リスクフレームワークおよび前記サブシステムに結合されたマネージャであって、

役割と任命の前記レコードへのユーザの提案された変更の通知を受け取る段階と、

前記通知に応答して、前記提案された変更を前記リスクフレームワークと突き合わせて分析し、人々が、

(1)複数の指定された物理的設備にアクセスする同時実行能力、

(2)複数の指定されたコンピュータ実行ビジネスプロセスを実行する同時実行能力、

(3)1つまたは複数の指定された物理的設備にアクセスし、1つまたは複数の指定されたコンピュータ実行ビジネスプロセスを実行する同時実行能力のうちのどれかを有することにより規定されたガイドラインに違反する可能性を識別する段階と、

前記提案された変更で前記規定されたガイドラインに違反する可能性を示さない場合のみ前記提案された変更を許可する段階と、を含むオペレーションを実行するようにプログラムされているマネージャとを備えるコンピュータ駆動システム。

【請求項８】

前記リスクフレームワークは、1人の人が、前記役割および任命でその人に、在庫保管領域に物理的にアクセスし、在庫減価償却を実行するコンピュータベースビジネスプロセスを実行する同時実行能力が与えられた場合に、前記規定されたガイドラインに違反する

可能性を有すると規定する請求項7に記載のシステム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、コンピュータベースビジネスアプリケーション(CBBA)の機能を実行するコンピュータシステムに関する。より具体的には、本発明は、クロスアプリケーション機能および/またはリアルタイムのローカル監視、報告、および予防を可能にするために複数のリアルタイムエージェント(RTA)がローカルCBBAソフトウェアに組み込まれているCBBA管理システムに関する。

【背景技術】

【０００２】

企業資源計画(Enterprise resource planning、ERP)システムは、企業の多くの商行為を統合し、自動化し、追跡し、規制する経営情報システムである。ERPシステムでは、会計、販売、請求書作成、製造、物流業、流通、在庫管理、生産、出荷、品質管理、情報技術、および人事管理などの企業の業務の多くの側面を取り扱うことができる。ERPシステムは、産業スパイなどの外部犯罪から守り、横領などの内部犯罪から守るためのコンピュータセキュリティを備えることができる。ERPシステムは、詐欺、エラー、または不正使用がさまざまな形で発生する場合にそのことを検出し、予防し、報告するようにセットアップすることができる。ERPシステムは、会社と顧客との間の双方向のやり取り(「フロントエンド」活動)、会社の品質管理および他の社内業務(「バックエンド」活動)、仕入れ先および運送業者(「サプライチェーン」)との双方向のやり取り、またはビジネスの他の側面に方向付けることができる。

【０００３】

企業が、「Sarbanes-Oxley」または「Public Company Accounting Reform and Investor Protection Act of 2002」または「SOX」とも呼ばれる、「The Sarbanes-Oxley Act of 2002」(Pub. L. No. 107-204、116 Stat. 745、2002年7月30日) などの近年の法律に照らして順守管理アプリケーションをERPシステムに補うことが次第に有益なことになりつつある。Sarbanes-Oxley法は、企業情報開示の正確さと信頼性を向上させることにより投資家を保護しようとするものである。この法律は、公開会社会計監視委員会、監査人の独立性、企業責任、および強化された財務開示を確立するなどの問題を対象とする。とりわけ、Sarbanes-Oxley法は、CEOおよびCFOが財務報告を証明することを義務付ける。さらに、Sarbanes-Oxley法では、正確な財務開示を確実に行うように計画された一連の社内手続きを義務付けている。

【０００４】

現代的なERPシステムは企業をきちんと組織化し、Sarbanes-Oxley法などの規制基準を満たすという難題にさえ取り組むのに役立つが、ERPシステムの運用、管理、または修正は、ことのほか複雑な作業となる可能性がある。実際、企業内における適用範囲が広いため、ERPソフトウェアシステムは、これまでに作成された最大のソフトウェア群の一部に依存する。いくつかの特定の問題を以下で取りあげる。

【０００５】

まず、従来のERP監視ソリューションでは、ダウンロードされたデータに対し働く検出ソリューションを使用することでリスクを「事後」に評価する。大企業の場合、ダウンロードには数時間かかることがある。ダウンロードと分析が完了するまでに、新しいユーザ、新しい役割の任命、および新しいトランザクションがすでにシステムを変えてしまっている。どのような訂正作業も、このコンフリクトを排除することはできないことがありうる、というのも、すでに変更されてしまっているシステム上で実行するからである。また、訂正作業が成功したかどうかは、他のダウンロードおよび分析が完了できるまで知られることはない。マイナスの効果を次から次へと並べる可能性が高い。

【０００６】

さらに、ひっきりなしに行われるダウンロードは、情報技術(IT)およびシステム資源を

枯渇させるため、毎日または毎週よりも頻繁に制御分析を実行する事後監視の賛同者はほとんどいない。ダウンロードおよび分析の頻度に応じて、違反は、発見されるまでにかなり長い間持続する可能性もある。リスクがこのようにして評価されるまでに、損害がすでに生じしているおそれもある。この点に関して、いくつかの従来のソリューションは、リスクを評価するためにかなりの計算資源を使い果たすが、それでもまだ、十分には速くない。

【０００７】

第2に、市場は、さまざまなベンダーからのERP製品で溢れている。いくつかの例として、SAPのSAP R/3（登録商標）(またはmySAP ERP（登録商標）)、Oracle CorporationのPeopleSoft（登録商標）(またはOracle Financials（登録商標）)、SSA Global TechnologiesのBPCS（登録商標）、Made2Manage SystemsのEnterprise Business System（登録商標）、NetSuite Inc.のNetERP（登録商標）、Microsoft Business DivisionのMicrosoft Dynamics（登録商標）、Ramco SystemsのRamco e.Applications（登録商標）、SYSPROのSYSPRO ERP（登録商標）ソフトウェアなどがある。一部またはすべての場合において、これらの製品は、互いに互換性はない。それでも、単一の企業であれば、たぶん、さまざまなベンダーのERP製品を同時に使用することも可能であろう。しかし、そうすると、企業は、アプリケーション間のリスク、つまり、異なるERPシステム同士の間に生じるリスクに曝されることになる。個々のERPシステムはどれも、これらのアプリケーション間リスクを検出することはできない。

【０００８】

第3に、企業がERPシステムを利用して自社のビジネスプロセス管理を、進行している状態で監視し、強制することができるとしても、そのようなERPアプリケーションが詐欺およびエラーを効果的に、確実に防ぐように、また非効率を最小限に抑えるように適切に構成されることは保証されない。ERPシステムが複雑なシステムであるため、システムにはリスク管理の穴がまだあり、これらの穴は容易には埋められない、という場合がある。これらの管理がうまくいかないと、詐欺率が高くなり、監査コストが著しく増大し、財務諸表作成し直しの可能性が高くなり、投資家の信頼が低下するという形で非常に高いコストがかかることがわかる。

【０００９】

したがって、知られているERPシステムは、いくつかの未解決の問題があるため、すべてのアプリケーションおよびユーザにとって常に適しているとは言えない。

【発明の概要】

【発明が解決しようとする課題】

【００１０】

CBBA管理システムは、クロスアプリケーション機能またはローカル監視、報告、または予防などのリアルタイム機能を使用可能にするためにローカルCBBAソフトウェアに組み込まれている複数のRTAを備える。

【課題を解決するための手段】

【００１１】

本開示の教示は、システム、方法、装置、論理回路、信号搬送媒体、またはこれらの組み合わせなどの多くの異なる方法で実装することができる。本開示は、他にも多数の利点およびメリットをもたらすが、以下の説明から明らかになるであろう。

【図面の簡単な説明】

【００１２】

【図１】RTAがローカルCBBAサブシステムに組み込まれているCBBAシステムのハードウェア/ソフトウェアのコンポーネントおよび相互接続のブロック図である。

【図２】RTAのハードウェア/ソフトウェアのコンポーネントおよび相互接続のブロック図である。

【図３】デジタルデータ処理マシンのブロック図である。

【図４】例示的な信号搬送媒体を示す図である。

【図５】例示的な論理回路の斜視図である。
【図６】RTAを動作させるためのシーケンスを例示する流れ図である。
【図７】共有CBBAマネージャを動作させるためのシーケンスを例示する流れ図である。
【図８】企業ガイドラインに違反する可能性のある役割の作成または修正を検出し、予防し、および/または報告するシーケンスを例示する流れ図である。
【図９】1つまたは複数のCBBAサブシステムにおける活動を監視するためのルールを作成するシーケンスを例示する流れ図である。
【図１０】ビジネス活動、CBBAサブシステム特有のタスク、およびリスクの間の関係を例示するブロック図である。
【発明を実施するための形態】
【００１３】
本発明の性質、目的、および利点は、付属の図面と併せて以下の詳細な説明を考察した後、当業者にさらに明らかになるであろう。
【００１４】
（ハードウェアコンポーネントおよび相互接続）
［全体的構造］
{序論}
本開示の一態様は、さまざまなハードウェア/ソフトウェアのコンポーネントおよび相互接続により具現化できるCBBAシステムに関するものであり、一実施例が図１のシステム100により説明されている。CBBAマネージャ102、ローカルCBBAサブシステム104～106、RTA 104a～106aなどの、図１のさまざまなデータ処理コンポーネントがある。これらのコンポーネントは、1つまたは複数のハードウェアデバイス、ソフトウェアデバイス、1つまたは複数のハードウェアまたはソフトウェアデバイスの一部、または前記の組み合わせにより実装することができる。これらサブコンポーネントの構成は、図３～5を参照しつつ、以下で詳しく説明される。
【００１５】
システム100のコンポーネントは、企業、共同出資者、合弁企業、事業部、政府ユニット、家族、非営利、個人、トラスト、または他の組織もしくは事業体などのクライアントに代わって運用される。つまり、CBBAサブシステム104～106により管理されるデータは、クライアントのビジネスまたは他の利害関係に関係する。クライアントが、システム100自体を運用するか、または他の事業体が、クライアントに代わってシステム100を運用することができる。
【００１６】
システム100は、124～128および129などのユーザインターフェイスを介して受け取った、ユーザの指令に従って、さまざまなビジネス活動を実行する。システム100の他の機能は、さまざまな企業ガイドライン160の違反を回避するためユーザ活動をガイドし、規制し、管理することである。ガイドライン160は、会社方針、政府規制、刑法、会計ルール、公正な商慣行、課せられる条件(例えば、設立許可書、会社定款、補助金、非営利状況の要件などにより)、前記の一部または全部の組み合わせ、あるいはシステム100のビジネス活動が代理に実行される事業体の活動を規制する他の所望のガイドラインのうちの1つまたは複数により具現化されうる。「会社、企業(company)」は、この説明全体を通して使用されるが、これは、典型的な実装の文脈において与えられ、ガイドラインを法人または他の特定の組織の文脈に限定するものと理解すべきではない。これらの教示は、同様に、考えられる事業体にも適用可能であり、このいくつかの例が上で取りあげられている。
【００１７】
説明を簡単にするため、ガイドライン160は、システム100の一部として例示されている。この点に関して、ガイドライン160は、システム100により格納されるか、または参照され、より具体的には、記憶装置111に格納されうる。しかしながら、ガイドライン160は、システム100の一部をなす必要はまったくなく、この場合、説明と理解を容易にするため

にガイドラインが示され、説明される。

【００１８】

システム100は、さまざまなローカルCBBAシステム104、106、108に結合されている共有CBBAマネージャ102を備える。マネージャ102は、個々のCBBAサブシステム内に、さらには複数のCBBAサブシステムにまたがって発生するリスクを分析し、検出することを含む動作を実行するようにプログラムされた中央モジュールである。特定の実施例では、マネージャ102は、Java（登録商標）で書かれたソフトウェアモジュールにより実装される。都合のよいことに、ローカルサブシステム104～108が互いに非互換である場合でも、マネージャ102を使用して、非互換のCBBAシステムが企業ガイドラインに適合しているかどうかを監視することができる。以下でさらに詳しく説明するように、マネージャ102は、RTA 104a～108aからデータを収集し、リスク検出、シミュレーション、軽減、改善、報告などのさまざまな高水準のタスクを実行することができる。

【００１９】

［CBBAサブシステム］

例示されている実施例では、CBBAサブシステム104～108は、異なるCBBA製品を具現化している。都合のよいことに、本開示では、これらのCBBAサブシステムが互いに互換性のない状況を考察し、解決に向けて取り組んでいる。CBBAサブシステム104～108は、ネットワークに接続しているユーザから要求があったときにさまざまな定義済みタスクを実行する排他的メカニズムに使用されるソフトウェアを備え、各サブシステムは、さらに、そのサブシステムのタスクを実行することをどのユーザに許可するかを定義する。例えば、CBBAサブシステムは、ERP、Webサーバーベースのロジスティック、レガシーアプリケーション、物理的プロビジョニング、規制または他の政府規制の順守、または他のコンピュータベースのビジネスアプリケーションなどの機能を実行することができる。

【００２０】

ERPサブシステムのいくつかの例として、SAPのSAP R/3（登録商標）、Oracle CorporationのPeopleSoft（登録商標）、Oracle CorporationのOracle Financials（登録商標）、SSA Global TechnologiesのBPCS（登録商標）、Made2Manage SystemsのEnterprise Business System（登録商標）、NetSuite Inc.のNetERP（登録商標）、Microsoft Business DivisionのMicrosoft Dynamics（登録商標）、Ramco Systemsの（登録商標）、SYSPROのSYSPRO ERP（登録商標）ソフトウェアなどがある。レガシーアプリケーションのいくつかの例としては、ファイルディレクトリ、メインフレームコンピュータ、ファイルサーバー、および他のデータリポジトリがある。

【００２１】

CBBAマネージャ102をサブシステム104～108に結合するには、各RTA 104a～108aを介する。各RTA 104a～108aは、各ローカルCBBAホスト104～108のソフトウェアに組み込まれたプログラムモジュールである。一実施例では、「組み込まれた」RTAとは、RTAが同じソフトウェア、ファームウェア、論理回路、ハードウェア、またはホスト104～108の他の処理機能内に組み込まれることを意味する。例えば、SAPソフトウェアパッケージを使用するCBBAサブシステムの場合、組み込まれたRTAは、Advanced Business Application Programming (ABAP)などのSAP専用ネイティブ言語で書くことができる。さらに、SAPサブシステム内のRTAの機能は、Su01、SU10、プロファイルジェネレータ(PFCG)、ユーザ認可トランザクションなどのSAPトランザクションに直接接続することができる。RTAの構造および動作については、以下で詳述する。

【００２２】

サブシステム104～108は、各ユーザインターフェイス124～128に結合される。ユーザインターフェイス124～128は、ユーザがローカルユニットに入力を行い、そのユニットから出力を受け取るためのデバイスまたはツールを備える。マネージャ102は、さらに、129などの1つまたは複数のユーザインターフェイスに結合される。例示的なユーザインターフェイスでは、マウス、キーボード、ビデオディスプレイ、タッチスクリーン、または他のデバイス、ツール、もしくはソフトウェアモジュールのうちの一部または全部を使用し

て、本開示により要求される機能を実行することができる。

【００２３】

CBBAサブシステム104～108のそれぞれは、ローカルビジネスタスク(104c～108c)のステートメントを含む。タスクは、ホストCBBAサブシステム104～106に専用の言語、構文、または他の形式で記述される。タスク104c～108cは、CBBAサブシステム104～106のビジネス活動を実行するために使用される。ERPシステムにより実装されるCBBAサブシステムの場合、タスク104c～108cにより実行されるビジネス活動のいくつかの実施例は、請求書を作成すること、請求書に対する支払いをすること、請求書を作成すること、ベンダー情報を更新することを含む。ほとんどの場合、これらのビジネス活動は、始めから終わりまでビジネスプロセスの自動化に関係している。いくつかの実施例は、調達から支払いまで、発注から現金支払いまで、生産工程処理、ならびに人事給付金支払いおよび処理を含む。レガシーファイルサーバーにより実装されるCBBAサブシステムの場合、ビジネス活動は、データの読み込み、データの削除、データの書き込み、および他のディスクまたは記憶装置管理操作などのファイル操作に関する。

【００２４】

各CBBAサブシステム104～108は、104b～106bなどの役割および任命のステートメントも含む。概して、役割および任命では、タスク104c～108cのうちのどのタスクをどの人たちが実行できるかを指定する。役割とは、人または役職が実行することを許されているタスクの集まりである。さらに、複数の単一役割からなるグループである、複合役割もありうる。そのため、これらの役割は、各サブシステム104～108におけるタスクの異なる集まりの概要を示し、任命は、どの人たちをどの役割に任命するかを示す。任命は、人々を役割に直接結び付けるか、または役職を役割に結び付け、それと無関係に、人々を役職に結び付けることができる。したがって、役割/任命104b～108bの一機能は、対応するCBBAサブシステムが要求されたタスク104c～108cを実行するために要求側ユーザが持っていなければならない必要な許可を示すことである。

【００２５】

サブシステム104～108のERP実装の場合、役割および任命104b～108cは(例えば)、指定された人が請求書の作成を実行することができることを規定することができる。サブシステム104～108のレガシー実装の場合、役割および任命(例えば)は、ネットワークユーザにより共有されるデータリポジトリの場合のように、システム資源への人々のITアクセス権を規定することができる。

【００２６】

［記憶装置］

マネージャ102は、1つまたは複数のサーバー、ハードドライブ、パーソナルコンピュータ、メインフレームコンピュータ、光ディスク、または本開示の要求に応えるのに適している他のデジタルデータ記憶装置デバイスなどのデジタルデータ記憶装置111を備えるか、またはそれらへのアクセス権を有する。この実施例では、記憶装置は、サブコンポーネント114、122を備える。これらのサブコンポーネントは、同じまたは異なる物理デバイス、論理デバイス、記憶セクタまたは他の領域、レジスタ、ページ、リンクリスト、リレーショナルデータベース、または限定することなく他の記憶装置ユニットにより実装されうる。記憶装置111のサブコンポーネントの動作および使用については、以下でさらに詳しく説明する。以下で、簡単に説明する。

【００２７】

構成レコード122は、CBBAマネージャ102の機能を設定または変更するために使用される、さまざまなデフォルト設定、ユーザ選択可能なオプションなどを保持する。つまり、構成122は、CBBAマネージャ102がどのように動作するかに関するさまざまなオプションのレコードを備える。構成122は、(1)CBBAサブシステム104～108のローカルユーザ、(2)システムレベルユーザ(例えば、ユーザインターフェイス129を介して)、(3)デフォルトで、(4)これらの組み合わせ、(5)他のメカニズムの要求があったときに設定されるいくつかの設定を含むことができる。したがって、構成122は、CBBAマネージャ102の動作の実質的に

いかなる側面についてもデフォルトおよび/またはオプションで用意されている設定のレコードを備え、そのような動作は本開示の全体を通して説明されている。

【００２８】

概して、リスクフレームワーク114では活動および条件を定義し、1つまたは複数のCBBAサブシステム104～108がこれらの活動および条件を許容するように構成されていれば、誰かに企業ガイドライン160の違反を犯す機会を与える道を開くことになる。フレームワーク114の1つのコンポーネントは、システム100を使用して犯すことができる該当する企業ガイドライン(上述)の考えられるすべての違反の概要を示すモジュール114aである。関連して、モジュール114bは、誰か1人に任せた場合に、その人に違反114aのうちの1つを犯させることになりそうなビジネス活動の組み合わせの概要を示す。

【００２９】

一実施例では、違反114aの使用をもたらす可能性を含むビジネス活動の組み合わせ114bの定義は、エラーまたは不正のリスクを予防または低減することを意図されている一次内部統制として職務の分離を含む。これは、どの単一の個人も、商取引のすべての段階を管理することがないようにすることにより達成される。一実施例では、職務の一般的カテゴリとして、認可、保管、記録管理、および差異調整の4つがある。理想的なシステムでは、異なる従業員は、これら4つの主要機能のそれぞれを遂行する。つまり、どの従業員も、これらの責務のうちの2つ以上を管理しないということである。資産の換金性が高ければ高いほど、職務の分離を適切に行う必要が高く、特に、現金、譲渡性小切手、および在庫を取り扱うときにはそうである。

【００３０】

職務の分離がきわめて重要なビジネス領域がある。現金の取り扱いは一例であるが、それは、現金は流動性の高い資産だからである。これは、金銭を、出て行った痕跡を残さずに受け取り使うことが容易であることを意味する。資金を受け取る部門は、会計記録にアクセスすることができるか、または職務の分離に関する任意の種類の資産を管理する。両立しない職務のいくつかの例を以下に挙げる。

・ トランザクションを認可する、そのトランザクションの結果として得られる資産を受け取り、保管維持する。

・ 小切手(内金払い)を受け取り、減価償却を承認する。

・ 現金を預金し、銀行勘定照合表の差異を調整する。

・ タイムカードを承認し、給与小切手を管理下に置く。

【００３１】

一般ビジネス活動の各リスクのある組み合わせ114bにおいて、フレームワーク114は、そのリスクのローカルマニフェステーション114cを規定している。特に、リスクのあるビジネス活動114bの所定の組み合わせについて、モジュール114cは、これらの組み合わせを実行するために使用することが可能である異なるすべてのCBBAサブシステム特有のタスク104c～108cを識別する。この点に関して、モジュール114cは、特定のコード、エントリ、構成、組み合わせ、またはそのサブシステムのローカルCBBA言語と互換性のある他の詳細によりサブシステムのタスク104c～108cを識別することができる。ローカルマニフェステーション114cは、異なるサブシステム104～108に個別に適用可能な異なるサブパート(別に示されていない)を含むことができる。例えば、1つのサブパートは、SAPシステムに特有のローカルマニフェステーションを含むことができ、他のサブパートはOracleシステムなどに特有のローカルマニフェステーションを含む。

【００３２】

一実施例では、リスクフレームワーク114は、違反114aおよび組み合わせ114bを省いて、ローカルマニフェステーション114cにより完全に実装することができる。この場合、モジュール114a～114bは、単にリスクフレームワーク114の背後にある概念の例示および説明を目的として、記憶装置111内に示されている。

【００３３】

サブシステム104～108のうちの1つがSAP ERPシステムにより実装される実施例において

、ローカルマニフェステーション114cは、Virsa Systems, Inc.のCompliance Calibrator バージョン5.0ソフトウェアから分離した実質的ライブラリを使用して実装することができる。この線にそって、表1(以下参照)は、違反114aおよびローカルマニフェステーション114cの例示的リスティングを示すことによりさらに詳細を示している(読みやすいように、ローカルの構文ではなく関数型言語を使用している)。

【００３４】

【表１】

表1

P2Pプロセス	ローカルマニフェステーションの機能説明(114C)	潜在的違反(114A)
ベンダー支払い	標準的なSAP二重払いチェックにより発見されない払い過ぎ	受け取っていない商品またはサービスに対する支払い
ベンダー支払い	組織境界を見渡して標準的なSAP二重払いチェックにより発見されない払い過ぎ	受け取っていない商品またはサービスに対する支払い
ベンダー支払い	請求書の二重払い	支出の過大申告
請求書確認	システムプロセスの外部で完了した無効な手動入力	在庫明細書の不実表示
請求書確認	組織への無効な入力	会社レベルの在庫明細書の不実表示
在庫評価	標準コスト許容範囲またはパーセンテージと見合っていないように見える資材評価変更	在庫品評価の不実表示
在庫評価	移動平均価格許容範囲またはパーセンテージと見合っていないように見える資材評価変更	在庫品評価の不実表示
外部リンク調達	取得承認手続きおよび方針をバイパスするために使用できる購入または取得文書	方針および注文価値限界をバイパスし、未許可取得を行う
外部リンク調達	承認されたリリース承認手続きの外部で処理されている購入トランザクション	方針および注文価値限界をバイパスし、未許可取得を行う
外部リンク調達	承認されたリリース承認手続きの外部で処理された購入文書	商品およびサービスの未許可調達のため調達プロセスの弱点につけ込む
外部リンク調達	承認されたリリース承認手続きの外部で処理された購入文書	商品およびサービスの未許可調達
商品を受け取る	商品受け取り要件をバイパスする処理中の請求書	受け取っていない商品またはサービスに対する支払い
ベンダー支払い	SAP二重払いチェックから除外されるベンダー	意図的/偶発的ベンダー二重払いが生じる潜在的ベンダーレベルシステムバイパス
ベンダー支払い	SAPでの二重払いチェックをバイパスする処理中の請求書	受け取っていない商品またはサービスの支払い、および支出の事業体または組織への不正確な転記
商品を受け取る	SAP調達管理をバイパスするために商品を受け取った後に作成される発注書	商品およびサービスの未許可調達および支払い
在庫を管理する	確定された限界を外れて行われる在庫調整	未許可在庫調整転記、在庫明細書の不実表示、在庫品の横領

【００３５】

［RTAのレイアウト］

図１のCBBAアーキテクチャ全体に加えて、本開示の異なる態様は、個別のRTA 104a～10

8aの構成に関する。各RTAは、さまざまなハードウェア/ソフトウェアのコンポーネントおよび相互接続により具現化することができ、一実施例は図2のRTA 200により説明されている。本発明の実施例では、各RTA 200は、各「ホスト」CBBAサブシステム104～106に組み込まれたソフトウェアモジュールを備える。

【００３６】

例示的なRTA 200は、条件動作プログラミング202、さまざまな他のモジュール210～213、および情報マップ220を含む。以下でさらに詳しく説明するように、プログラミング202では、CBBAマネージャ102と連携して、CBBAサブシステムレベルの機能を実行し、マネージャ102がCBBAサブシステム104～108において、またそれらの間で、ガイドライン160に違反する可能性を識別し、予防し、報告するのを助ける。説明を簡単にするため、RTA 200は、サブシステム104をホストとする文脈において説明される。

【００３７】

プログラミング202は、モジュール210～213とともに、RTA 200の操作命令の集合を提供する。大まかに言うと、プログラミング202は、条件を識別し、それに応じて、モジュール210～213のうちの1つまたは複数を起動する。RTA 200およびそのサブコンポーネントのオペレーションについて、以下でさらに詳しく説明する。

【００３８】

sense、gather、do、およびreportモジュール210～213により、情報マップ220にアクセス可能である。マップ220は、ホストCBBAサブシステム内に格納されているさまざまなクライアントデータ、構成設定、および他の情報の場所の一覧である。データは、物理または論理アドレス、デバイス、ポインタ、セクタ、または他の有用な識別子によりリストすることができる。実施例104では、マップ220は、役割104b、タスク104c、サブシステム104の構成データ、ならびに他のクライアント情報、メタデータ、および構成設定のある場所を示す。

【００３９】

［例示的なデジタルデータ処理装置］

上述のように、CBBAマネージャ102、サブシステム104～108、RTA 104a～108bなどのデータ処理要素を実装するためにさまざまな形態を使用することができる。

【００４０】

いくつかの実施は、汎用プロセッサ、デジタルシグナルプロセッサ(DSP)、特定用途向け集積回路(ASIC)、フィールドプログラマブルゲートアレイ(FPGA)、または他のプログラム可能論理デバイス、ディスクリートゲートまたはトランジスタロジック、ディスクリートハードウェアコンポーネント、または本明細書で説明されている機能を実行するように設計されているこれらの任意の組み合わせを含む。汎用プロセッサは、マイクロプロセッサであってよいが、代替えとして、プロセッサは、任意の従来のプロセッサ、コントローラ、マイクロコントローラ、または状態機械であってよい。プロセッサは、コンピューティングデバイスの組み合わせ、例えば、DSPとマイクロプロセッサの組み合わせ、複数のマイクロプロセッサ、DSPコアと連携する1つまたは複数のマイクロプロセッサ、または他のそのような構成として実装することもできる。

【００４１】

より具体的な実施例として、図３には、デジタルデータ処理装置300が示されている。装置300は、デジタルデータ記憶装置304に結合された、マイクロプロセッサなどのプロセッサ302、パーソナルコンピュータ、ワークステーション、コントローラ、マイクロコントローラ、状態機械、または他の処理機械を含む。本発明の実施例では、記憶装置304は、高速アクセス記憶装置306とともに不揮発性記憶装置308を含む。高速アクセス記憶装置306は、例えば、プロセッサ302により実行されるプログラミング命令を格納するために使用することができる。記憶装置306および308は、図４～5に関してさらに詳しく説明されているようなさまざまなデバイスにより実装されうる。多くの代替え形態も可能である。例えば、コンポーネント306、308のうちの1つを取り除くことができ、さらに、記憶装置304、306、および/または308をプロセッサ302にオンボードで搭載するか、さらには装置30

0の外付けとすることができる。

【００４２】

装置300は、さらに、コネクタ、配線、バス、ケーブル、バッファ、電磁リンク、ネットワーク、モデム、またはプロセッサ302が装置300の外部の他のハードウェアとデータを交換するための他の手段などの入力/出力310も備える。

【００４３】

［信号搬送媒体］

上述のように、デジタルデータ記憶装置のさまざまなインスタンスを、例えば、記憶装置111およびシステム100(図１)により使用される他の記憶装置を実現するため、記憶装置304および308(図３)を具現化するためなどに使用することができる。その用途に応じて、デジタルデータ記憶装置は、データ、機械可読命令、メタデータ、構成設定などを格納するなどのさまざまな機能に使用することができる。記憶媒体などに格納される、機械可読命令は、それ自体、さまざまな処理機能を実行するのを補助することができるか、またはコンピュータ上にソフトウェアプログラムをインストールするために使用することができ、そこでそのようなソフトウェアプログラムは、本開示に関係する他の機能を実行するために実行可能である。

【００４４】

いずれの場合も、デジタルデータ記憶装置は、機械可読信号をデジタル形式で格納する方法をどのようなメカニズムでも、実装することができる。一実施例として、CD-ROM、WORM、DVD、デジタル光テープ、または他の光記憶装置などの光記憶装置400(図４)が挙げられる。他の実施例としては、従来の「ハードドライブ」、安価なディスクで構成される冗長ディスクアレイ(「RAID」)、または他の直接アクセス記憶装置デバイス(「DASD」)などの直接アクセス記憶装置がある。他の実施例は、磁気テープまたは光テープなどの順次アクセス記憶装置である。デジタルデータ記憶装置のさらに他の実施例は、ROM、EPROM、フラッシュPROM、EEPROM、メモリレジスタ、バッテリバックアップRAMなどを含む。

【００４５】

例示的な記憶媒体をプロセッサに結合して、プロセッサがその記憶媒体から情報を読み込み、その記憶媒体に情報を書き込むようにすることができる。代替え形態では、記憶媒体は、プロセッサに一体化することができる。他の実施例では、プロセッサおよび記憶媒体は、ASICまたは他の集積回路内に置くことができる。

【００４６】

［論理回路］

機械実行可能命令(上述のような)を格納する信号搬送媒体とは対照的に、異なる実施形態では、論理回路を使用して、図１～2の処理コンポーネントを実装する。

【００４７】

速度、費用、工具費などの面のアプリケーションの特定の要件に応じて、このロジックは、数千もの小さな集積化トランジスタを備える特定用途向け集積回路(ASIC)を構成することにより実装することができる。このようなASICは、CMOS、TTL、VLSI、または他の好適な構成により実装することが可能である。他の代替え形態は、デジタル信号処理チップ(DSP)、ディスクリート回路(抵抗器、コンデンサ、ダイオード、インダクタ、およびトランジスタなど)、フィールドプログラマブルゲートアレイ(FPGA)、プログラマブルロジックアレイ(PLA)、プログラマブルロジックデバイス(PLD)などを含む。

【００４８】

図5は、集積回路500の形態の論理回路の一実施例を示している。

【００４９】

（オペレーション）

本開示の構造的特徴が説明されたので、次に、本開示のオペレーション面について説明する。本明細書で開示されている実施形態に関して説明されている方法、プロセス、またはアルゴリズムのステップは、ハードウェアで直接、ハードウェアにより実行されるソフトウェアモジュールにより、またはこれら2つの組み合わせにより具現化することができ

る。

【００５０】

［CBBAサブシステムの機能］

CBBAサブシステム104～108はそれぞれ、サブシステムの特定のソフトウェアパッケージおよび管理されているクライアント側の要素に応じて、さまざまなコンピュータベースのビジネスアプリケーションのオペレーションを実行する。ソフトウェアパッケージに関して、これは、SAPのSAP R/3（登録商標）(またはmySAP（登録商標）)、Oracle CorporationのPeopleSoft（登録商標）またはOracle Financials（登録商標）、SSA Global TechnologiesのBPCS（登録商標）、Made2Manage SystemsのEnterprise Business System（登録商標）、NetSuite Inc.のNetERP（登録商標）、Microsoft Business DivisionのMicrosoft Dynamics（登録商標）、Ramco SystemsのRamco e.Applications（登録商標）、SYSPROのSYSPRO ERP（登録商標）ソフトウェア、または他の製品などの製品のよく知られているタスクを伴いうる。クライアント側の要素に関しては、これは、会計システム、買掛金勘定、在庫システム、政府入札または契約順守、規制順守、人事、品質管理、または他の要素を備えることができる。

【００５１】

特定の実施例では、CBBAサブシステム104～108において、ユーザは、請求書を作成すること、請求書の支払いをすること、会計報告書を作成することなどのさまざまなタスク104c～108cを実行することができる。しかし、サブシステム104～108は、タスク104c～108cが役割および任命104b～108bに従って実行される際の条件を制限する。そのため、サブシステム104のユーザがタスク104cのうちの1つまたは複数を実行することを要求し、サブシステム104がユーザの役割104bの外部にあると判定した場合に、サブシステム104は、このタスクの実行を防ぎ、終了し、または報告する。

【００５２】

［RTAのオペレーション］

図６は、一実施例による、RTA 104a～108aのうちの個々の1つを動作させるシーケンス600を示している。シーケンス600は、より広い背景状況において実装することが可能であるが、説明を簡単にするため、以下では、図１～2の特定の環境において説明する。特に、シーケンス600は、レイアウト200により実装されるようなRTA 104aの背景状況において説明される。

【００５３】

ステップ601で、RTA 104aのオペレーションが開始する。ステップ601は、例えば、ホストCBBAサブシステム104がインストールされるとき、製造されるとき、構成されるとき、最初に起動されるとき、再起動されるときに実行されうる。異なる実施例として、RTAは、ホストCBBAサブシステムとは別にオペレーションを開始することができる。

【００５４】

ステップ602では、条件動作プログラミング202により、さまざまなあらかじめ定められている条件が存在しているかどうかが判定される。概して、これらの条件は、ホストCBBAサブシステムのステータス、またはsenseもしくはgatherモジュール210/211によりすでに決定されているような内部で生じるイベント、CBBAマネージャ102から受信された通信、モジュール210～213の実行のステータスなどを含む。いくつかの条件例を以下で説明する。

・ RTA 104aがCBBAマネージャ102から命令を受信したことを感知(610)したという条件。

・ タスク610～613(後述)の1つまたは複数が完了したという条件。

・ タスク610～613の1つまたは複数が、特定の結果を残して完了したという条件。例えば、感知タスク610が、104bの役割を変更する要求をユーザがサブミットしたことを知ること。

・ RTA 104aが、サブシステム104またはそのサブコンポーネントのどれかの特定のデータ、動作可能構成、または他の状態もしくはコンテキストの存在を感知(610)したことを

示す条件。
・ サブシステム104、および/またはサブシステムとユーザもしくはCBBAマネージャ102との通信に関係する他の条件。
【００５５】
条件の発生を見逃すのを避けるため、条件のチェック(ステップ602)が、612に示されているように繰り返し実行される。ステップ602は、定期的に、非定期的スケジュールで、タイマーまたはクロックに応じて、または頻繁に発生するイベントに応じて、または他のトリガで実行されうる。
【００５６】
条件動作プログラミング202が、ステップ602で定義済み条件が発生したことを検出した場合、プログラミング202は、プログラミング202の所定の論理に従ってオペレーション610～613のうちの1つまたは複数を呼び出す。タスク610～613は、各モジュール210～213により実行され、上述のモジュール210～213の機能に従って動作する。
【００５７】
ステップ610で、senseモジュール210は、ホストサブシステム104内のメッセージ、信号、イベント、および他の発生要素を傍観する。例えば、モジュール210は、ユーザが役割または任命104bを変更する要求を出したときにそのことを感知する。他の実施例として、モジュール210は、特定のベンダーについてオフにされている「sense duplicate invoices」オプションなどの機密扱いの構成パラメータの存在を感知することができる。モジュール210は、さらに、再発する入力が所定の閾値を超えた場合などのクリティカルデータ値をも感知できる。他の実施例として、モジュール210は、コマンドがCBBAマネージャ102から受信されたときにそのことを感知することができる。
【００５８】
ステップ610を十分な頻度で実行するために、関連する条件(602)は、再発するアラーム、スケジュールなどの到来であってよい。条件動作プログラミング202に応じて、ステップ610作成の異なる結果から、異なる条件が形成され、これが(ステップ602が再び実行されたときに)、他のタスク610～613の実行をトリガする。例えば、ステップ610は、役割を作成するユーザ要求を感知することができ、これは、CBBAマネージャ102へのこの状況の報告(613)を結果としてもたらす条件(602)を構成する。
【００５９】
ステップ611で、適切な条件(602)に応じて、gatherモジュール211はホストCBBAサブシステム内の活動に関する情報を積極的に取得する。例えば、gatherモジュール211は、ホストサブシステム104の役割および任命(104b)、タスク104c、サブシステム104の他のデータ、サブシステム104のデフォルトまたはユーザ構成などから情報を取り出すことができる。gatherモジュール211のオペレーション611の他の実施例として、これらは、上述の表1からのコントロールのどれかをサポートする情報を収集しようとする場合がある。タスク611を実行する際に、gatherモジュール211は、マップ220を利用する。例えば、情報の一般的要求に応じて(ステップ602)、ステップ611のモジュール211は、マップ220を参照して、このようなデータが置かれているホストCBBAサブシステム104内の特定の記憶場所を識別することができる。
【００６０】
ステップ611により、先行する条件(602)のいくつかの実施例は、CBBAマネージャ102からの直接コマンド、またはタスク610～613のどれかの完了、タスク611～613の特定の結果などを含む。条件動作プログラミング202に応じて、ステップ611作成の異なる結果から、異なる条件が形成され、ステップ602が再び実行されたときに、他のタスク611～613の実行をトリガする。例えば、タスク611の完了により、CBBAマネージャ102への結果の報告613、またはフォローアップアクション(612)の実行をトリガ(ステップ602)することができる。
【００６１】
ステップ612で、doモジュール212は、RTA 200の肯定的活動を実行する。一実施例と

して、doモジュール212は、役割および任命(104b)の変更を防止する、ユーザへの役割の任命を防止するなどを行うことができる。他の実施例として、モジュール212は、「ケース」を作成し、ケース番号を割り当て、ケースに、senseおよびgatherモジュール210、211から得たさまざまな情報を書き込むことができる。ステップ612の場合、条件(602)により、doモジュール212がCBBAマネージャ102により開始された要求、トリガ、または他の活動に応じて、またはタスク610～613のうちの他のタスクの完了または結果に応じて、動作するように指定することができる。

【００６２】

ステップ613で、reportモジュール213は、メッセージ、ファイル、データ編集、アラート、または他の報告をCBBAマネージャ102に送信するオペレーションを規定する。ステップ613は、CBBAマネージャ102からのコマンドなどの条件(602)に応じて、タスク610～613のうちの前のタスクの完了または結果に応じて、動作する。

【００６３】

モジュール210～213側の裁量により、プログラミング202は、さまざまな組み合わせのタスク610～613を先行するさまざまな条件(602)と組み合わせることにより複雑なオペレーションを統合することができる。いくつかの実施例は、senseとdo、senseとreport、gatherとdoとreportなどの複合オペレーションを含む。例えば、senseモジュール210が、役割変更をユーザが要求したことを検出(610)した場合にそれに応答して、プログラミング202は、ユーザに関する情報を収集(611)するようにモジュール211に指令し、次いで、収集された情報の報告をCBBAマネージャ102に送信(613)するようにモジュール213に指令することができる。

【００６４】

［クロスアプリケーション分析を含むシステム機能］

{序論}

図７は、本開示の方法態様の一実施例により、複数の非互換のCBBAサブシステムにまたがって発生するオペレーションを含むさまざまなシステム機能を実行するシーケンス700を示している。シーケンス700は、より広い背景状況において実装することが可能であるが、説明を簡単にするため、以下では、図１～2の特定の環境において説明する。より具体的には、シーケンス700は、CBBAマネージャ102に関して説明される。

【００６５】

概して、ステップ701で、CBBAマネージャ102は、システム100を管理する作業を開始する。ステップ701は、CBBAマネージャ102のインストール、構成、再構成、起動、他のRTAの追加、マネージャ102などのシステム100コンポーネントのアップグレードの後開始することができる。

【００６６】

CBBAマネージャ102が起動(701)した後、マネージャ102は、さまざまなトリガのうちの1つが発生したかどうかを問い合わせる(702)。各トリガ702は、さまざまな定義済みタスク、イベント、条件、または他の発生要素のうちの1つである。トリガのいくつかの実施例は、RTA 104a～108aのうちの1つからの所定のメッセージの到来、所定の時刻の到来、カウンターの終了、CBBAサブシステム上でガイドライン160の違反の発生する可能性の条件の検出などを含む。異なるトリガの場合については、以下で詳述する。

【００６７】

トリガ(702)が発生すると、CBBAマネージャ102は、タスク704、712、714、716のうちの1つを実行する。いずれの場合も、トリガ(702)に対するチェックが反復して実行され(703)、これにより、プロセス704、712、714、716のうちの1つが、前のトリガによりすでに進行中であるかどうかに関係なく、発生する新しいトリガを見逃すのを回避する。

【００６８】

［役割を管理する:序論］

ステップ704で、CBBAマネージャ104は、役割104b～108bを作成、修正、再定義、および修正するCBBAサブシステムユーザを補助する。オペレーション704に対するトリガ702は、

ユーザが新規の役割を追加するか、または既存の役割を修正することを要求したという報告(図6のステップ613)をローカルのRTAがCBBAマネージャ102に送信したときに発生する。本開示では、このような要求は、「役割変更」要求と呼ばれる。役割変更要求(702)を検出したことに応答して、ステップ704で、CBBAマネージャ102は、ユーザの役割変更要求を受け取り、分析し、処理する。

【００６９】

一実施例では、ステップ704において、Virsa Systems, Inc.のROLE EXPERTバージョン4.0ソフトウェア製品を使用することができる。ステップ704では、CBBAマネージャ102は、適用可能なRTAを使用して、ユーザおよびホストCBBAサブシステムとの実質的にリアルタイムのインターフェイスを形成する。役割管理タスク(704)のいくつかの例示的なオペレーションは、以下のものを含む。

・ サブシステム境界に関係なく、複数の役割およびその役割と仕事または地位との一般的な関係を示すこと。
・ 役割を定義し、役割定義を維持すること。
・ タスクを定義し、維持すること。
・ 役割および役割定義を比較すること。
・ ユーザ情報を表示すること。
・ 役割に割り当てられたオブジェクトをレビューすること。
・ 複合役割を定義すること。

【００７０】

これらに加えて、ステップ704では、多数の報告およびユーティリティを利用することができ、いくつかの実施例として以下のものを使用できる。

・ 役割報告書を生成すること。
・ メニューおよび許可においてTCodesをチェックすること。
・ ユーザの役割を比較すること。
・ ユーザに任命された役割の一覧を作成すること。
・ 役割およびトランザクションの一覧を作成すること。
・ 役割ステータスをチェックすること。
・ 導き出された役割を作成または修正すること。
・ 役割またはユーザに対する許可をカウントすること。
・ 所有者、役割、およびユーザを分析すること。
・ ユーザまたは役割により実行されるトランザクションを識別すること。

【００７１】

適宜、役割作成に関係するさまざまな強化された機能を備える役割管理704を適用することができる。役割が作成される場合、仕事に関係する一般的な地位または活動を対象とするようにそれらの役割を作成することができる。組織内の多くの人々が、同じ活動を遂行することができるが、1つの実体または地位に関連する活動のみに限定される。これは、これらの機能が、同じままであるが、地位または実体は変わりうることを意味する。したがって、買掛金勘定担当職員が何百もの企業プラント内に常駐しており、その場合、役割の唯一の変更は、どのようなプラントかということだけである。プラントの他の価値が指定された後、RTAは、組織内の制限を役割に挿入することによりすべての変更形態を生成する。数千の役割も、RTAを使用して、変更される必要がある共通要素を持つすべての役割を見つけることにより維持されうる。例えば、再編成または合併により、特定の役割内容が変化しうる。RTAは、影響のある役割を表示し、ユーザが、ネイティブシステムツールが備える一方法により従来のものを使用するのとは反対に一意的な価値を有するすべての役割を変更することができる。

【００７２】

前記の機能に加えて、ステップ704では、さまざまなリスク報告が簡単に行えるようになっており、後述のように、ステップ705のリスク分析を使用することができる。サブシステム104～106のユーザによって要求される、リスク報告書は、リスクまたはコンフリク

ト、ユーザまたは役割またはプロファイルまたはHRプロジェクトなどによるクリティカルなトランザクションの発生を提示する報告書を含むことができる。

【００７３】

プロセス700は、ステップ704に関係する多数の周辺タスクを含む。つまり、CBBAマネージャ102が役割管理プロセス704に着手した後、CBBAマネージャ102は、他の関係するプロセスをユーザに提供する。ユーザをタスク705～708に仕向けることに加えて、タスク704は、異なるタスク705～708の使用を調整し、さまざまなユーザオペレーションを実行することに対する知的でかつ体系的なアプローチを取るようにすることができる。例えば、要求された役割変更要求が、リスクフレームワーク114に違反していることがわかった後(タスク705で学習されるように、後述)、タスク704は、承認者が役割の選択を1つずつ解除し、次いで、その修正されたプロファイルの効果をシミュレート(タスク707、後述)することを許可することができる。これにより、承認者は、提案された(複数の)役割が役割分担違反を引き起こし続けるかどうか、またどのような時点で停止するかをチェックすることができる。この方法で、承認者は、さらに、役割分担違反の原因となる特定の役割または役割の組み合わせを特定することができる。他の実施例では、ステップ704により、感知アクセスは、その存在を認める管理なしでは導入されないことが確実であり、また機密扱いのアクセスは、役割が使用できるようになる前に必ず承認される。他の実施例では、オペレーション704は、機密扱いの役割を使用する場合に人員の活動を追跡する緊急「消防士」機能を備えることができる。

【００７４】

適宜、オペレーション704は、さらに、コンピュータ援用機能を備えることもでき、これにより、CBBAマネージャ102は、CBBAサブシステムユーザ(役割承認者など)がステップ705の分析において見つかったリスクを処理するのを助ける。改善では、CBBAマネージャ102は、ステップ705で見つかったリスク違反を引き起こした、要求または提案された役割追加または変更を取り除くこと、または緩和706の開始などのオプションを調整する。これらのオプションのうちの選択された1つを完了した後、結果として得られた役割変更は、ガイドライン160をより正確に満たすことになる。さらに、改善は、リスクを改善するために実行される処置をタイミングよく報告し、文書化することも含むことができ、また経営陣がリスクの管理および/または規制の順守に積極的に取り組んでいるという証拠ともなる。プロセス管理の場合、リスクのある条件の報告機能は、ルールにおける「許容範囲」を超えるトランザクションに基づくことができる。一実施例として、支払い期間は、通常30日であるが、一トランザクションでは、60日に変更される。担当者への通知により、例外に関連付けられている状況を評価させ、変更して元に戻すか、またはそれらの状況と不一致を正当とする理由を文書化することができる。これは、財務報告制限または規制に違反していないことを確認するためにレビューされる必要のあるビジネスの通常の過程を外れて作成される特別な1回限りのトランザクションに広く使用されている。

【００７５】

タスク705～708のいくつかの詳細な実施例について以下で説明する。

【００７６】

［リスク分析の実行］

ステップ705で、CBBAマネージャ102は、各要求された役割変更(704から)を分析し、リスクフレームワーク114に違反するかどうかを判定する。例えば、CBBAサブシステム104の場合、CBBAマネージャ102は、役割変更要求を分析して、提案されている役割変更が、もしそれが104bで実装されているのであれば、リスクフレーム114に違反しているかどうかを判定する。説明を簡単にするために、役割「変更」は、役割修正とともに役割追加をも含むものと理解しておく。

【００７７】

ステップ705は、ユーザまたは承認者から要求があったときに実行されるか、またはユーザが役割変更要求をサブシステムにサブミットする場合に必ず自動的に実行されうる。ステップ705では、CBBAマネージャ102は、該当するRTAを呼び出して、サブシステム104か

ら要求の内容、対象役割に関する情報などを含む、役割変更要求に関するすべての関係する情報を集める(そして報告として送り返す)。必要な情報は、例えば、リスクフレームワーク114により規定することができる。この情報を用いて、マネージャ102は、次に、集められた情報をローカルマニフェステーション114cと比較し、一致があるかどうかを調べる。集められた情報が関連するホストサブシステム104～108に適切なローカルマニフェステーション114cと一致する場合、提案されているような役割変更は、企業ガイドライン160に反する可能性を含む。

【００７８】

都合のよいことに、CBBAマネージャ102はすべてのサブシステム104～108にわたって役割管理を中心的に監督する立場にあるため、マネージャ102は、1つのCBBAサブシステムまたは他のCBBAサブシステム内にリスクが存在していない場合があっても、クロスアプリケーション分析を実行し、複数のCBBAサブシステム間で生じるリスク(つまり、ガイドライン160の違反の可能性)を検出することもできる。この点に関して、ステップ705では、各サブシステム104～108から関連するすべての情報を集めるようにRTA 104a～108aに指令し、このデータをバンドルし、バンドルされたデータを全体として、ローカルマニフェステーション114cの本体と突き合わせて分析することにより所定の役割変更要求を考察する。

【００７９】

こうして、CBBAマネージャ102は、サブシステム104～108間にある問題を検出することができる。一実施例では、CBBAマネージャ102は、各サブシステムを訪れ、そのシステム内の「ユーザid」を探し、技術情報を検出したらそれを集め、ルールネットワーク内でリスクのある組み合わせと比較する。一致がある場合、集められたソースデータで、どれがどのシステムに属しているかを追跡することができる。例えば、ユーザは、一方のサブシステムにおいてベンダーを更新し、他のサブシステムにおいて、支払いを行うことができる場合、CBBAマネージャ102は、両方とも発見し、どのシステムにおいてどの役割から一致が見つかったかを報告する。

【００８０】

この方法では、次いで、CBBAマネージャ102は、複数のCBBAサブシステム間で生じるリスク(114a)のどれかを検出することができる。他の利点として、ステップ705の分析を実施するために必要な情報は、RTA 104a～108aを使用して実質的にリアルタイムで得られ、CBBAサブシステム104～108から情報の時間のかかるダウンロードを待たなくて済む。

【００８１】

ステップ705は、以下のシーケンス800の説明においてさらに詳しく示される(図８)。一実施例では、ステップ705は、COMPLIANCE CALIBRATORバージョン5.0および/またはCONFIDENT COMPLIANCEバージョン1.2などのVirsa Systems, Inc.のソフトウェア製品のいくつかの機能を使用している。

【００８２】

［緩和］

ステップ706では、CBBAマネージャ102は、リスク緩和を実行する。一実施例では、このオペレーションは、CBBAマネージャ102が(ステップ705において)、ユーザの提案されている役割変更がリスクフレームワーク114に違反することを検出した場合に必ず自動的にトリガされる。

【００８３】

緩和は、リスクフレームワーク114の違反に対処するアクションである。緩和コントロールでは、識別されたリスクまたは予想される監査例外を免除または指定変更し、リスクフレームワーク114に違反するとしてもその例外が発生するようにできる。特定のリスクフレームワーク114違反を選択した場合、承認者は、監査証跡を維持するためにシステム内に取り込まれた管理承認で違反を指定変更することができる。緩和コントロールのいくつかの実施例は、新しいまたは変更された役割の存在期間を所定の期間(つまり、役割の予定有効期限)に制限すること、役割に関係する活動に関する報告を自動的に生成することなどを含む。

【００８４】
他の実施例は、リスクのあるタスクを分離することが可能でないため、リスクのある組み合わせの多くが1人によって実行されなければならない、小さな事務所で役立つものである。ここでは、CBBAマネージャ102が備える1つの例示的な緩和オペレーション706は、この担当者がそれらのリスクのある組み合わせを実行したときにCBBAマネージャ102に警告するようRTA 104a～108aをプログラムすることである。次に、CBBAマネージャ102は、この担当者の監督者に、その実行が合法的であることを保証するトランザクション支援文書を求めるよう促す。他の実施例では、マネージャ102およびRTAは、連携して、ルーチン作業に基づき、支援文書と比較して監督者(または役割がリスクのある組み合わせを含む他の人)によりレビューされうる変更の詳細報告書を生成する。他の実施例では、CBBAマネージャ102およびRTAは、例えば、被指定人がリスクのある組み合わせのうちの他方である他の人のタスクを請け負いながら、リスクのある組み合わせが限定された期間のみについて承認されることをのみを許す。この場合、CBBAマネージャ102およびRTAは、限定された期間が期限切れになったときに人に警告し、自動的にその人のアクセスを削除するようにプログラムされうる。

【００８５】
それに加えて、緩和プロシージャ706は、緩和アクションを開始するために、「監督者」またはイベントの第三者に通知するように構成することができる。これは、集められたシステム情報であるため、システムの場所とは無関係に組み合わせを誰が実行したかに基づき他方の場所とは反対に一方の場所のコントロールにおいて指定された人に通知する決定を下すことができる。これにより、1つの共通緩和コントロールを使用して、同じようにリスクを制御することができるが、組み合わせを実際に実行したのがわかっている人に基づいて実行するように異なる個人に通知することができる。他の実施例では、緩和706において、CBBAマネージャ102は、事前に承認されている代替えコントロールで検出されたリスクを管理するために現在ユーザの緩和コントロールを記録するコマンドを発行する。一実施例では、緩和オペレーション704の実装は、Virsa Systems, Inc.のCOMPLIANCE CALIBRATORソフトウェア製品の機能を使用する。

【００８６】
上述のように、プロシージャ706は、サブシステム104～108内のデータに実質的にリアルタイムでアクセスするなどのさまざまな方法でRTAアーキテクチャを利用する。さらに、RTAは、2つのリスクのある組み合わせが実際に実行される場合に、そのような組み合わせが理論上可能であるという報告とは反対に、生じる出来事を報告するために使用することができる。リアルタイムの態様により、システム100は、上述の特定のビジネス制限があるため存在していなければならないそれらのリスクのある組み合わせに対する組み込まれた改善ソリューションを実施することができる。他の利点は、個人がリスクのあるアクセスを行うことに対する例外を設けた後、発生したときにリアルタイムですぐにその例外の出来事を報告するために監視メカニズムが適所に置かれる。

【００８７】
［シミュレーション］
ステップ707では、CBBAマネージャ102はシミュレーションを実行する。一実施例では、このオペレーションは、CBBAマネージャ102が(ステップ705において)、ユーザの提案されている役割がリスクフレームワーク114に違反することを検出した場合に自動的にトリガされる。他のオプションとして、ユーザは、要求により手動でステップ707を開始できる。

【００８８】
シミュレーション707において、監督者、管理者、または他の役割承認者が、さまざまな仮説を承認し、CBBAマネージャ102は、これがリスクフレームワーク114に違反しているかどうかを判定する。例えば、これらの仮説は、与えられた役割追加、役割修正、役割任命、緩和条件などの詳細を指定することができる。都合のよいことに、ステップ705のクロスアプリケーション分析のように、ステップ707のシミュレーションでは、同様に、バ

ンドリングおよび他の技術を実行して、仮説の状況に関わるリスクのクロスアプリケーション分析を実行することができる。一実施例では、シミュレーションオペレーション707の実装は、Virsa Systems, Inc.のCONFIDENT COMPLIANCEおよびCOMPLIANCE CALIBRATORソフトウェア製品の機能を使用する。

【００８９】

プロシージャ707は、例えばサブシステム104～108内のデータに実質的にリアルタイムでアクセスすることにより上述のRTAアーキテクチャを利用し、したがって、いつも最新のきわめて正確なシミュレーションを行える。

【００９０】

［リスク終了］

ステップ708では、CBBAマネージャ102は、リスク終了プロセスを実行する。特に、ユーザ提案役割変更または追加がリスクフレームワーク104に違反する場合(ステップ705)、ステップ708において、(1)リスクがあるにもかかわらず役割変更が可能であるが、誰かに役割変更を通知するか、または(2)役割変更が完了しないようにする。ステップ708の特定のアクションは、以下のシーケンス800に関してさらに詳しく説明される(図８)。一実施例では、ステップ708において、Virsa Systems, Inc.のCOMPLIANCE CALIBRATORソフトウェア製品を使用することができる。

【００９１】

［信頼できる順守］

上述のように、役割管理オペレーション704およびそのサブプロセス705～708を使用することで、どれか1つのCBBAサブシステム104～106の役割104b～108bがリスクフレームワーク114に違反しないこと、および役割104b～108bがクロスプラットフォームのリスク暴露とならないことを保証することができる。しかしながら、ガイドライン160に違反する可能性を示すある種の状況において役割を定義することが可能であるとも考えられる。例えば、緩和コントロール(706)のせいで、他の何らかの方法で禁止されているトランザクションの組み合わせが許可されるが、経営管理側にそのようなトランザクションを監視させ、所定の許容差を決して超えないようにすることが望ましい。他の実施例は、多数の機能を含む役割が、非常事態のため許可されなければならない場合である。これらの場合、役割は、違反により構成されるが、緊急時のみ個人への任命について役割の承認を囲む緩和コントロールがある。

【００９２】

信頼できる順守プロセス712では、これらおよび他のそのような可能性を取り扱う。概して、信頼できる順守オペレーション712では、CBBAマネージャ102は、規定されている条件に関してサブシステム104～108を監視する。このレビューの結果に基づき、CBBAマネージャ102は、次に、1つまたは複数の報告を発行し、さらに、被指名者による指定フォローアップアクションを開始することができる。プロシージャ712は、サブシステム104～108内のデータに実質的にリアルタイムでアクセスすることにより上述のRTAアーキテクチャを利用する。

【００９３】

最初に、信頼できる順守712のトリガ(702)は、資格のある管理者などの認証されたユーザによるプロセスの呼び出しである。このときに、ユーザ-管理者は、CBBAマネージャ102と対話して、サブシステム104～108内で監視すべき条件を定義する。つまり、ユーザは、所望のタスク104c～108c、役割および任命104b～108b、マスターデータ(例えば、顧客およびベンダー)、サブシステム構成オプション、システム構成オプションへの変更などの監視すべき項目を指定する。ユーザは、さらに、これらの条件が発生した場合に必ず実行すべきアクション、例えば、(1)報告書、およびそのような報告書のフォーマット、内容、および受取人を生成するアクション、(2)作成すべきログまたは他の監査証跡を用意するアクション、(3)始まりの役割管理(704)または緩和(706)または他のプロセスなど、特定の条件が発生したときに必ずヒューマンワークフローを呼び出すアクション、および/または(4)サブシステム104～108のネイティブソフトウェアと連携して、特定のアクショ

ンを停止または実行されないようにするアクションを指定することもできる。
【００９４】
この初期セットアップの後に、指定された条件のどれかが発生した場合に、信頼できる順守712が再トリガされる(702)。つまり、RTA 104a～108a(CBBAマネージャ102によりプログラムされている)は、所定の条件を検出し、その発生をCBBAマネージャ102に報告し、その後、CBBAマネージャ102は、報告書を生成する、ログを作成する、ヒューマンワークフローを呼び出すなどの所定のアクションを実行する。
【００９５】
ユーザ指定条件に加えて、信頼できる順守712は、知られている弱点、典型的には厄介な領域、特に重大な結果をもたらす欠陥などのデフォルトまたはシステム指定条件が発生していないかサブシステム 104～108を監視することができる。これらの条件に応答して、プロセス712は、ユーザ指定条件の場合のような類似のフォローアップアクション、例えば、報告書を作成する、ログを作成する、ヒューマンワークフローを呼び出す、アクションを実行されないように停止するなどを実行することができる。
【００９６】
他の実施例として、指定された許容差または条件を検出したときに、RTAは、改善ケースを生成し、CBBAマネージャ102を介して指定された人またはグループにワークフローとして渡すことができる。次いで、CBBAマネージャ102は、このケースを例外に対するアクションまたは正当化理由について文書化する。ここでは、改善が開始され、信頼できる順守712において追跡され、これにより、ケースが閉じられる前に、例外が訂正されるか、または適切に正当化されることが保証される。
【００９７】
他の実施例として、管理者が、サブシステム104～108のうちの1つで二重払いの検出を停止する構成変更を開始した場合(企業ガイドライン160に違反して)、関連するRTA 104a～108bは、これを検出し、CBBAマネージャ102に報告し、自動的に、ローカルサブシステム内に実装される前にその変更を防止するアクションを実行する。
【００９８】
一態様によれば、次に、信頼できる順守712は、リアルタイムで連続して監視されるプロセスについて許容差およびしきい値を設定することにより、ビジネスプロセス内のボトルネックおよびチョークポイントをピンポイントで突き止めるために使用される。信頼できる順守712では、例えば、CBBA監視メカニズムにおける規定されたホットスポットおよび穴を監視し、さらに、追加の管理側指定基準を順守することができる。オペレーション712は、さらに、重要ビジネスプロセス内のマスターデータ、構成、およびトランザクションを監視することによりコントロールの有効性の見通しを高める。適宜、オペレーション712は、役割ベースのダッシュボードを備え、管理者および監査者がコントロールの不備に対し即座にアクセスできるようにすることが可能である。信頼できる順守712は、(1)調達から支払い、注文から現金、財務に対する組み込みのマスターコントロール、(2)自動化され、一貫している検査、(3)コントロールリポジトリとの統合、(3)例外および関係するトランザクションおよび文書のピンポイント指摘、(4)改善ワークフローおよび追跡、および(5)その他などの機能を備えるように実装されうる。
【００９９】
［報告書作成］
ステップ714では、CBBAマネージャ102は、1つまたは複数の出力報告を供給する。これは、ステータス、構成、トランザクション履歴、使用度、現在のタスク104c～108c、および/または役割および任命104b～108b、またはCBBAサブシステム104～108またはそのサブコンポーネントの他の特性、またはリスクフレームワーク114、構成122などに関する報告機能を伴うことができる。報告書716は、オンデマンドで、または指定された報告基準に応じて自動的に生成されうる。都合のよいことに、報告機能716は、サブシステム104～108内のデータに実質的にリアルタイムでアクセスすることにより、上述のRTAアーキテクチャを利用する。

【０１００】
［その他］
特に上で取りあげられているこれらのオペレーション712～714に加えて、CBBAマネージャ102は、所定の環境100内で多数のタスク716を実行するように拡張または修正することができる。
【０１０１】
［リスクターミネータ］
上述のように、CBBAマネージャ102は、時間の経過とともに役割を追加および変更するユーザの要求を受け取って処理し(ステップ704)、それにより、時間の経過とともに役割の集まり104b～106bを構築し、精密化し、改訂し、更新する。図8は、トリガ(702)、分析(705)、および終了(708)オペレーションのリンクされた実施例を与えるシーケンス800を示している。シーケンス800は、より広い背景状況において実装することが可能であるが、説明を簡単にするため、以下では、図１～2の特定の環境において説明する。
【０１０２】
ステップ802で、CBBAマネージャ102は、役割変更要求の通知、つまり、既存の役割を修正するか、または新しい役割をレコード104b～108bのうちの1つに追加する、許可データを変更する、プロファイルを追加または変更するなどのユーザ要求を受け取る。より具体的には以下のようになる。第1に、ユーザがインターフェイス(124など)を操作して、役割を変更または追加する要求をサブミットする。例えば、管理者、監督者、または他の役割承認者は、ユーザインターフェイス124を使用して要求をCBBAサブシステム104にサブミットし、新規雇用の役割を追加するか、または新しい職員を既存の役割に関連付けることができる。RTA 104aは、CBBAサブシステム104内の特定の活動を感知(ステップ610、図６)するためにsenseモジュール210(図２)を連続的に使用しながら、役割変更要求を検出する。感知された役割要求に応じて、プログラミング202は、役割変更要求をCBBAマネージャ102に報告(ステップ613、図６)するようモジュール213に指令する。CBBAマネージャ102は、ステップ802でこの報告を受け取る。都合のよいことに、CBBAマネージャ102は、役割変更要求の通知をリアルタイムで受け取るが、それは、CBBAサブシステム104のソフトウェア内に組み込まれている、RTA 104aにより報告されるからである。
【０１０３】
シーケンス800は、CBBAマネージャ102が、他の役割要求を受け取ると必ず802から再開し、したがって連続的に実行される。
【０１０４】
ステップ803で、CBBAマネージャ102は、要求を完全に処理するために、サブシステム104からすべての適用可能な情報を取得するようRTA 104aに指令する。CBBAマネージャ102は、この情報を、名前、型、機能、または他の高水準の指定により識別する。それに応答して、プログラミング202は、doモジュール212を呼び出して、マップ220と突き合わせて要求された情報を相互参照し、この情報が実際にサブシステム104内のどこに格納されているかを調べる。次いで、プログラミング202は、gatherモジュール211を呼び出して、そのように識別された情報を取り出す。この情報を手元に置いて、プログラミング202は、reportモジュール213を呼び出して、集めた情報をマネージャ102に送信する。
【０１０５】
ステップ804で、CBBAマネージャ102は、リスクフレームワーク114を、ステップ803で集めた情報に適用し、役割要求がリスクフレームワーク114に違反していないかどうかを評価する。このオペレーションは、上述のようにステップ705に従って実行される。
【０１０６】
ステップ805で、CBBAマネージャ102は、ステップ804の結果に基づいて取るべき適切なアクションを決定する。ステップ804で、要求された役割変更により課されるリスクが見つからなかった場合、ステップ805は、805aを経由してステップ806に進む。ステップ806で、CBBAマネージャ102は、役割104bに対する要求された変更を許可するか、実行するか、または連携して実装するようRTA 104aに命令する。

【０１０７】
対照的に、ステップ804で、リスク違反が見つかった場合、マネージャ102は、構成設定122に基づいて、(1)役割変更要求を許可し、誰かに通知するステップ(807)、または(2)役割変更要求を終了するステップ(808)のうちの1つを実行する。経路805bと805cの選択は、構成122におけるデフォルトまたはユーザ選択設定により決定される。一実施例では、これらの設定は、経路805b～805cの一方または他方を常に選択するという選択肢を規定することができる。他の実施例では、設定122では、リスクの性質、違反の種類、または他の条件もしくは背景状況に基づいて経路805b～805cを選択する方法を規定することができる。

【０１０８】
経路805bが選択された場合、CBBAマネージャ102は、ステップ807で要求された役割変更を許可する。つまり、CBBAマネージャ102は、要求された通り役割104bの更新を許可するようRTA 104aに命令する。したがって、プログラミング212は、doモジュール212を呼び出して要求された役割変更をブロックするのを差し控えるが、このブロック動作は、経路805cが選択された場合に実行される。役割変更を許可したにもかかわらず、CBBAマネージャ102は、役割、役割変更要求者、関係するビジネスユニット、ITシステムなどに適切である担当者を識別して、通知することにより追加のアクションを実行する。通知は、管理者、IT管理者、監督者、リスク管理要員などに送ることができる。ステップ807の報告は、例えば、114aまたは114cからの適用可能なリスティングなど、違反したすべてのリスクのリスティングを含むことができ、さらに、この報告を作成する際に、マネージャ102は、関連するRTA 104～108に、サブシステムから追加の必要情報を集めるよう指令することができる。

【０１０９】
さらに、ステップ807で、CBBAマネージャ102は、コメントをログ、トランザクション履歴、または役割変更に相関する他の監査証跡にコメントを入力することをユーザ(役割変更要求した)に義務付けるなどの、さらなるアクションを実行することができる。それとは別に、ステップ807で、そのようなログを自動的に作成または更新するようにRTA 104aに指令することができる。

【０１１０】
ステップ805b/807とは対照的に、CBBAマネージャ102は、ステップ808で、要求された役割変更の実行を禁止する。つまり、CBBAマネージャ102は、役割104bの更新をブロックするようRTA 104aに命令する。一実施例では、RTA 104aはdoモジュール212を呼び出すことによりこれを実行する。より具体的には、これは、104のネイティブシステムへの出口点と標準入口点を使用することにより、またはネイティブシステム全体を制御し、役割変更プロセスを完全に停止し、中断し、または切り詰めることにより実行することができる。SAPサブシステム104の背景状況において、RTA 104aは、SU01、SU10、およびPFCGなどのトランザクションが実行されるのを妨げる。

【０１１１】
他の実施例では、ステップ808において、リスクのある組み合わせまたは機密アクセス属性のビジネスルールに例外を管理者が入力するのをCBBAマネージャ102側で禁止する必要がある場合がある。他の実施例では、ステップ808において、一方のサブシステム104～108内の所定のユーザへの役割の提案された任命を停止することができるが、その役割は、他方のサブシステム内の同じユーザへの他の役割の既存の任命とともに考えた場合に、役割分担違反を生じることになるであろう。

【０１１２】
適宜、ステップ808において、CBBAマネージャ102は、上述のような適切な対象への、提案されたが、行われなかった役割変更の通知を送信する追加のステップを実行することができる。他のオプションとして、阻止された役割変更(ステップ808)の後に、CBBAマネージャ102は、ユーザを改善オペレーション810に導くことができる。改善については、上で詳しく説明されている(例えば、704、図７を参照)。

【０１１３】
［オプション:早期分析］
上述のようなステップ802の代替えとして、このステップ802は、ユーザが最終的に役割変更要求をサブミットする前に動作しうる。例えば、RTA 104aは、トランザクションが役割に追加されるときに感知し、許可対象が定義される前であってもCBBAマネージャ102に通知する(ステップ802)動作をすることができる。
【０１１４】
この場合、CBBAマネージャ102は、不完全な役割を、ユーザによって構築されるときに分析し(804)、ユーザ(示されていない)に対し潜在的違反を警告し、許可対象定義を続けるかどうかのオプションを与える。これにより、ユーザに、これまでの変更を破棄するオプションが与えられ、長い時間が費やされる前に、役割変更が最終的に失敗する。
【０１１５】
［代替え実装］
リスクターミネータ機能の代替えまたは追加実装として、CBBAマネージャ102は、役割および任命を変更する以外の活動を感知し、終了させることができる。例えば、CBBAマネージャ102は、ユーザが役割および任命により実行することを許可されているタスクを修正することを要求するか、またはユーザがガイドラインに違反する1つまたは複数のタスクを実行することを要求するか、またはユーザがユーザの既存の役割の範囲外のタスクを実行することを要求する状況を取り扱うことができる。ここでは、RTA 104a～108aは、CBBAサブシステム内でタスクを実行するユーザの要求について実質的にリアルタイムの通知を行う。さらに、これらの通知に応答して、CBBAマネージャ102は、リスクフレームワークを使用して、要求されたタスクがガイドラインに違反している可能性があるかどうか、および/または要求されたタスクが要求側ユーザの役割104b～108bの範囲外にあるかどうかを判定する。これらのいずれかが真である場合、CBBAマネージャ102は、実質的にリアルタイムで動作してCBBAサブシステムがタスクを実行するの阻止するよう1つまたは複数の適切なRTA 104a～108aに指令する。または、CBBAマネージャ102は、影響のあるCBBAサブシステムがタスクを実行するのを許可し、タスクの実質的にリアルタイムの通知を監督者または他の被指名人に送信する。
【０１１６】
［自動化ルール構築］
上述のように、システム100の一態様は、さまざまなユーザタスク(104c～108c)を実行し、しかも定義されている役割および任命(104b～108b)に従ってこれらのオペレーションのユーザ実行を規制することができるローカルCBBAサブシステム(104～108)を伴う。さらに、上述のように、システム100の他の態様は、中央コンポーネント(102)監視、ならびに役割および任命への変更を慎重に規制し、サポートし、補強することを伴う。この態様を実行する際に、リスクフレームワーク114が、役割/任命変更が実行されるかどうかを判定するために使用される。
【０１１７】
この背景状況を念頭に置くと、システム100の他の態様は、リスクフレームワーク114を構築するプロセスを伴っている。このプロセスは、最初にリスクフレームワーク114を生成するとともに、リスクフレームワーク114を改訂し、拡張し、または更新するために使用することができる。シーケンス900(図９)は、このプロセスの一実施例を示している。説明のため、シーケンス900は、システム100に関して説明される。シーケンス900は、しかしながら、制限することなく、多数の異なる実装設定で適用可能である。
【０１１８】
シーケンス900を説明しやすくするために、図10に、企業ガイドライン160、ビジネス活動、およびCBBAサブシステム特有のタスクの間の関係が例示されている。まず、図１０は、図1からの企業ガイドライン160の図を含む。ビジネス活動のライブラリ、コレクション、分類、メニュー、または他の選択が1002に示されている。大まかに言うと、ビジネス活動は、CBBAサブシステム104～108の特定のタスク104c～108cにより実行されることができ

る高水準の事業運営を指す。以下の表2には、ビジネス活動のいくつかの実施例が示されている。

【０１１９】

【表２】

表２ ビジネス活動 (1002 のいくつかの実施例)
ベンダーに支払う
ベンダーを作成する
請求書の支払いをする
発注書を変更する
配送を行う
商品を受け取る
...

【０１２０】

ビジネス活動1002の部分集合は、1006により示されており、これは、ビジネス活動のリスクのある組み合わせを表している。特に、活動1006は、同じ人に任せた場合にリスクのあることを示す2つまたはそれ以上のビジネス活動のさまざまな組み合わせを規定している。「リスク」は、より具体的には、規定されている企業ガイドライン160に違反する可能性のあることを意味する。表3(以下)は、リスクのある組み合わせ1006のいくつかの実施例、およびそれらの組み合わせにリスクがある理由(「違反の可能性...」)を示している。一実施例では、違反の可能性は、114aの履行における一般的リスクの例示的な集合を定める(図１)。

【０１２１】

【表３】

表３	
ビジネス活動のリスクを伴う組み合わせ (1006 の実施例)	これらの活動を同じ人が実行できる場合に、会社方針の考えられる違反 (114a の実施例)
ベンダーに支払う +商品を受け取る	受け取っていない商品またはサービスに対し支払う
GL マスターレコードを維持する +仕訳記入を転記する	架空の GL 勘定を作成し、仕訳活動を生成するか、または記入を転記することで活動を隠す。
原価中心点を維持する +原価振替処理	認可を受けずに原価中心点を変更し、この中心点への未許可原価振替を処理し、場合によっては CO 報告を歪曲する。
原価中心点を維持する +収益再転記	認可を受けずに原価中心点を変更し、この中心点への未許可収益記入を処理し、場合によっては CO 報告を歪曲する。
CC または CE グループを維持する +仕訳記入を転記する	原価中心点報告を操作し、不適切な仕訳記入転記を隠す。
...	...

【０１２２】

表3は、ビジネス活動のリスクのある組み合わせの要約した一覧であり、どの会社方針に違反する可能性があるかを示している。詳細な例は、この説明の後の付録-1に掲載した。付録-1に例示されているように、異なる会社方針違反に、低、中、および高などの異なるリスクレベルを割り当てることができる。これらの格付けは、つけ込まれた場合に事業体に及ぶリスクの重大度などの客観的要因、または個人の意見とは無関係な他の標準に基づくことができる。これらの格付けは、デフォルトにより、または事業主、またはそれらの組み合わせにより設定されうる。いくつかの例示的なリスクレベルとして以下のものがある。

・ 高-詐欺、システム障害、資産喪失などの物理的、もしくは金銭的損失、またはシステム規模の破壊が発生しうる。

・ 中-データ完全性または操作または複数システムの破壊が発生する可能性があり、いくつかの実施例として、マスターデータを上書きする、ビジネス承認をバイパスする、複数のビジネスプロセス領域を崩壊させるなどがある。

・ 低-単一ユニットまたはオペレーションに影響を及ぼす生産性損失またはシステム障害が発生する可能性があり、いくつかの実施例として、社内プロジェクト費用の虚偽表示または一プラントまたは場所に対するシステム機能停止がある。

【０１２３】

タスク1007～1009は、ビジネス活動1002を実行する際に場合によっては呼び出される可能性のあるCBBAサブシステム特有のタスクの領域全体を表す。本発明の実施例では、タスク1007～1009は、サブシステム104～108により実行することができるマシン実行可能タスク104c～108c(それぞれ)に対応する。大まかに言うと、これらのタスク1007～1009は、トランザクション(SAPサブシステム内の)、関数(ORACLEサブシステム内の)、コンポーネント(PEOPLESOFTサブシステム)、または使用されているサブシステムに適した他のタスクを含む。しかし、「タスク」1007～1009は、異なる粒度で定義することができる。例えば、CBBAサブシステムでSAPを使用する場合、「タスク」は、(1)アクション、または(2)アクションとさらに更新、作成、表示などのパーミッション、または(3)アクションとさらにパーミッションとさらに文書、フィールドなどのさらなる詳細の1つまたは複数の他の項目とすることができる。

【０１２４】

「ビジネス活動」1002の高水準の概念は、サブシステムが詳細タスク1007～1009を実行できる限り、サブシステム104～108において具体的意味を有するため、タスク1007～1009の部分集合は、したがって、ビジネス活動のリスクのある部分集合1006に対応する。リスクのあるタスク組み合わせは、1016により示されている。これらのリスクのあるタスク組み合わせ1016は、さまざまなサブシステム内タスク組み合わせ(1016～1018により例示されているような)と、さらにはサブシステム間タスク組み合わせ(1012～1014により例示されているような)から生じうる。一実施例では、リスクのあるタスク組み合わせ1016は、114cの履行におけるローカルマニフェステーションの例示的な集合を定める(図１)。

【０１２５】

図９を参照すると(図１０とともに)、ルーチン900は、リスクフレームワーク114を構築するための例示的なシーケンスを示している。ステップ902で、ビジネス活動1002が定義される。一実施例において、これは、CBBAサブシステム104～108がどのビジネス活動を実行できるかを決定することを伴う。ある場合には、ステップ902は、運用中のCBBAサブシステムの反映に基づいて実行されうる。他の場合には、ステップ902は、CBBAサブシステムをスクラッチから設計したときに初期段階で実行することができる。いずれの場合も、ステップ902は、手動で実行され、より具体的には、プログラマー、システムアドミニストレーター、デザイナー、ソフトウェアアーキテクト、または他の適切な担当者により実行される。一実施例では、ユーザは、インターフェイス129(例えば、GUI機能)を操作して、ビジネス活動1002をCBBAマネージャ102に入力する。

【０１２６】

ステップ904は、各ビジネス活動が各CBBAサブシステム内で実行できる可能な方法を含

む、ビジネス活動1002の技術的な解釈を示す。より具体的には、各CBBAサブシステムについて、ステップ904で、ビジネス活動を実行することができるすべてのCBBAサブシステム特有のマシン実装タスク1007～1009の一覧が作成される。所定のビジネス活動を実行するための異なる方法が多数ありえ、そのそれぞれについて考察する。ステップ904は、手動で実行され、より具体的には、プログラマー、システムアドミニストレーター、デザイナー、ソフトウェアアーキテクト、または他の適切な担当者により実行される。一実施例では、ユーザは、インターフェイス129(例えば、GUI機能)を操作して、タスク1007～1009を入力し、ビジネス活動1002と対応するタスク1007～1009とを相互に関連付ける。

【０１２７】

上述のように(図１０、1007～1009)、「タスク」は、異なる粒度で定義することができる。例えば、CBBAサブシステムでSAPを使用する場合、「タスク」は、(1)アクション、または(2)アクションとさらに更新、作成、表示などのパーミッション、または(3)アクションとさらにパーミッションとさらに文書、フィールドなどのさらなる詳細の1つまたは複数の他の項目とすることができる。ステップ904は、異なる形で動作し、次いで、システム100がセットアップされたタスク粒度に応じて動作する。したがって、ステップ904の技術的解釈を実行する際に、各ビジネス活動は、完全な粒度を得るために必要に応じて細かく分けられる。例えば、「タスク」が単にSAPアクションに対応する場合、ステップ904では、各ビジネス活動を複数のタスクに細分し、さらに、関連するパーミッション、文書、およびフィールドを指定する。「タスク」がSAPアクションとパーミッションと文書およびフィールド表す場合、ステップ904で、各ビジネス活動が複数のタスクに細分される。

【０１２８】

ステップ906で、リスクのあるビジネス活動1002の組み合わせ1006を識別する。つまり、ステップ906では、すべてが同じ人に任された場合に、その人は企業ガイドライン160に違反する形でシステム100を使用する能力を持つことになるビジネス活動の組み合わせを識別する。1人でそれらのビジネス活動を実行することができるとすれば、例えば、その人は、表3に記載の違反を行うことができ、したがって、規定された役割分担ルールに違反することができるであろう。ステップ906は、手動で実行され、より具体的には、プログラマー、システムアドミニストレーター、デザイナー、ソフトウェアアーキテクト、または他の適切な担当者により実行される。例えば、ユーザは、インターフェイス129のGUI機能を操作してCBBAマネージャ102と通信し、ステップ902でサブミットされたビジネス活動のさまざまな組み合わせを識別することによりステップ906を完了することができる。

【０１２９】

ステップ906の後に、ステップ908が実行される。ビジネス活動(906からの)識別された各リスクのある組み合わせ(1006)について、ステップ908は、これらの組み合わせの技術的解釈(904からの)を利用して、リスクのある組み合わせを実行することができるCBBAサブシステム特有のタスクの可能なすべての組み合わせを生成するコンピュータ駆動オペレーションを実行する。つまり、ステップ908で、ステップ904および906の結果を使用して、リスクのあるビジネス活動1006をCBBAサブシステム104～108でこれらの活動が実行されうるさまざまな方法のすべてにマップする。結果は、CBBAサブシステムタスクのリスクのある組み合わせのリスティング1016である。ステップ908では、各リスクのあるビジネス活動1006が所定のCBBAサブシステム(例えば、1016～1018)内で実行されうる可能性とともに、リスクのあるビジネス活動1006が複数のCBBAサブシステム(例えば、1012～1014)にまたがって実行されうる可能性を考慮する。具体的な一実施例では、ステップ908の一機能は、適切な機能レベルコードまたは許可対象に提案されている値を割り当てることであるとしてよい。

【０１３０】

ステップ902～906とは異なり、ステップ908は、コンピュータで実行される。本発明の実施例では、ステップ908は、CBBAマネージャ102により実行される。結果として得られるタスクリスティング1016は、膨大な大きさとなりうる。例えば、ほぼ200個のリスク1006がある場合、システムによっては、トランザクション組み合わせ1016の数は結果として20

,000に近いものとなりうる。

【０１３１】

ステップ908の後、ステップ910は、CBBAサブシステム内のユーザ活動を規制するマシン強制ルールを実行するが、これらのルールはタスクの生成された組み合わせのどれかを実行することができる所定の役割またはユーザの出現を禁止するものである。一実施例では、ステップ910は、リスクフレームワーク114を更新し、タスク906の結果を反映させることにより、より具体的には、タスク組み合わせ1016をローカルマニフェステーション114cに格納することにより実行される。単一のCBBAサブシステムの実施例(図に示されていない)では、ステップ910は、ローカルCBBAサブシステムをプログラムすることにより、より具体的には、そのサブシステムのローカルにあるリスクフレームワーク114を更新することにより実行できる。これにより、サブシステムは、CBBAサブシステム内のユーザ活動を規制することができ、タスクの生成された組み合わせを実行することができる所定の役割またはユーザの出現を禁止することができる。

【０１３２】

タスクの生成された組み合わせのどれかを実行することができる所定の役割またはユーザの出現を禁止するルールに関して、これは、そのような出現を妨げること、そのような出現の通知を行わせること、またはその両方を伴うことができる。この機能の他の詳細については、リスクターミネータ機能に関して上で説明されている(708、図７、および800、図８を参照)。

【０１３３】

（物理的プロビジョニング）

上記の実施例では、ERPサブシステム、政府の規制を順守するためのシステム、レガシーデータリポジトリなどのCBBAサブシステム104～108のさまざまな実施形態について説明した。

【０１３４】

他の実施例として、CBBAサブシステムの他の実施形態は、データ、プロセス、コンピューティングハードウェア、電子回路、デバイス、またはセキュリティもしくはいわゆる「物理的プロビジョニング」を構築することに関係するアクションを含む。この実施形態では、1つまたは複数のCBBAサブシステム104～108は、ドアロック、警報システム、アクセスゾーン、コントローラ、ブームゲート、エレベーター、読み取り装置(カード、バイオメトリック、RFIDなど)、登録者識別読み取り装置(PIR)、およびこれらのコンポーネントにより生成されるイベントまたはアラームなどのさまざまなリモート操作される設備セキュリティコンポーネントを含む。これは、さらに、コピー機、POSシステム、HVACシステムをおよびコンポーネント、輸送アクセス(料金)ポイント、および他のスマートカードまたは他の物理的アクセス技術に基づいて組み込むことができるそのような他のシステムなどの他のデバイスを含むことができる。

【０１３５】

物理的プロビジョニングの場合、タスク(例えば、104c)は、ドアロックを開ける動作、警報システムの作動を停止する動作、物理的領域でのアクセス権を得る動作、機器を操作する動作などを含む。タスク104c～108cを処理する際に、CBBAサブシステムは、124、126、128などのインターフェイスから個別ユーザ認証を受け取って、評価する。ユーザ認証では、キーパッドパスコード、バイオメトリック識別(例えば、指紋、虹彩/網膜スキャン)、ユーザ名およびパスワードのサブミット、磁気ストライプカードの提示、近接カード、スマートカード、無線ICタグ(RFID)などを使用することができる。CBBAサブシステムでは、ユーザの役割、任命、および他の特性(例えば、104b)などの情報を考慮し、ユーザに代わって要求されたタスクを実行するかどうかを決定する。セキュリティ構築の態様に関する限り、CBBAサブシステムは、CARDAX、GE、Honeywellなどの市販の製品などの技術を使用することができる。

【０１３６】

物理的プロビジョニングの場合、役割の管理(例えば、704、図７を参照)は、物理的領

域、機械などへのアクセス権を付与すること、および無効にすることに関係する。次いで、上述のような役割(例えば、104b)のように、物理的プロビジョニング役割は、役割分担違反を防止するように設計される。例えば、リスクは、同じ人が化学薬品貯蔵領域(例えば、硝酸アンモニウム)へのアクセス権だけでなく空港の接続施設のタールマック領域へのアクセス権をも保有している状況によって生じる可能性がある。物理的態様に加えて、CBBAマネージャ102は、さらに、物理的および論理的景観について同時に役割分担違反を予防するために役割を規制することもできる。例えば、リスクは、1人で一方の役割により期末棚卸保管領域にアクセスすることができ、それと同時にERPサブシステムにおいて在庫減価償却を実行できる役割に属している状況で生じる可能性がある。この物理的態様では、さらに、データをCBBAサブシステムに送出し、1人が1つの連続する期間内に物理的に1つの場所に長く留まりすぎているかどうか、または1人が物理的訪問と次の物理的訪問の間に作業場所から時間的に十分に離れていない場合、または1人に対し、例えば有毒または放射性物質への特定の規制暴露限度を超えた場合に関してルールを参照するようにできる。

【０１３７】

（他の実施形態）

前記の開示では多数の例示的な実施形態が示されているが、付属の請求項で定義されているように、本発明の範囲から逸脱することなく、さまざまな変更および修正を加えられることは当業者には明白なことであろう。したがって、開示されている実施形態は、概して本発明により考察されている主題を表しており、本発明の範囲は、当業者に明白であると思われる他の実施形態を完全に包含し、また本発明の範囲は、それに応じて、付属の請求項以外の何ものによっても制限されない。

【０１３８】

当業者に知られているか、または後から知られることになる上述の実施形態の要素に対するすべての構造的、および機能的等価物は、参照により本明細書に明確に組み込まれており、本発明の請求項に包含されることが意図されている。さらに、本発明の複数の請求項に包含されるので、1つのデバイスまたは方法で、本発明により解決されることが求められるありとあらゆる問題に対応することは必要でない。さらに、本開示の中の要素、コンポーネント、または方法ステップは、いっさい、その要素、コンポーネント、または方法ステップが請求項の中で明示的に記述されているかどうかに関係なく公衆に捧げられることを意図していない。この中の請求要素は、「する手段」、または方法クレームの場合「する段階」という語句を使用して明示的に引用されていない場合には、35 USC. 112、第6項の規定に従って解釈されないものとする。

【０１３９】

さらに、本発明の複数の要素は、単数形で説明または請求される場合があるが、単数形で要素を参照している場合でも、特に断りのない限り、「ただ1つの」を意味することを意図しておらず、「1つまたは複数」を意味するものとする。さらに、当業者であれば、操作順序は、説明および請求を目的としてある種の特定の順序で述べなければならないことを理解するであろうが、本発明では、そのような特定の順序を超えるさまざまな変更を考察している。

【０１４０】

それに加えて、当業者であれば、情報および信号は、さまざまな異なる技術および技法を使用して表すことができることを理解するであろう。例えば、本明細書で参照されているデータ、命令、コマンド、情報、信号、ビット、記号、およびチップは、電圧、電流、電磁波、磁場または磁気粒子、光場または光粒子、他の項目、または前記の組み合わせにより表すことができる。

【０１４１】

さらに、当業者であれば、本明細書で説明されている例示的な論理ブロック、モジュール、回路、およびプロセスステップは、電子ハードウェア、コンピュータソフトウェア、またはその両方の組み合わせとして実装することができることを理解するであろう。ハー

ドウェアとソフトウェアとを入れ替えて使用できることを明確に例示するために、上では、さまざまな例示的なコンポーネント、ブロック、モジュール、回路、およびステップが、一般的にその機能に関して説明されている。このような機能がハードウェアまたはソフトウェアとして実装されるかどうかは、特定の用途およびシステム全体に課せられる設計制約条件に左右される。当業者であれば、それぞれの特定の用途についてさまざまな方法により説明されている機能を実装することができるが、そのような実装決定は、本発明の範囲からの逸脱を引き起こすものとして解釈すべきではない。

【０１４２】

開示されている実施形態を前記のように提示したのは、当業者が本発明を製作または使用することができるようにするためである。これらの実施形態に対しさまざまな修正を加えられることは、当業者にとっては直ちに明白であろうし、また本明細書で定義されている一般原理は、本発明の精神または範囲から逸脱することなく他の実施形態にも適用することができる。したがって、本発明は、本明細書に示されている実施形態に限定されることを意図されておらず、本明細書で開示されている原理および新規性のある特徴と一致する最も広い範囲を適用されることを意図されている。

【０１４３】

【表４】

付録-1-1

ビジネス活動 #1	ビジネス活動 #2	ビジネス活動 #3	違反の説明	リスクレベル
GLマスタレコードを維持する	仕訳記入を転記する		架空のGL勘定を作成し、仕訳活動を生成するか、または記入を転記することで活動を隠す。	中
原価中心点を維持する	原価振替処理		認可を受けずに原価中心点を変更し、この中心点への未許可原価振替を処理し、場合によってはCO報告を歪曲する。	中
原価中心点を維持する	収益再転記		認可を受けずに原価中心点を変更し、この中心点への未許可収益記入を処理し、場合によってはCO報告を歪曲する。	中
CCまたはCEグループを維持する	仕訳記入を転記する		原価中心点報告を操作し、不適切な仕訳記入転記を隠す。	中
銀行マスタデータを維持する	AP支払い		本物でない銀行口座を作成し、そこから小切手を作成する。	高
資産書類を維持する	ベンダー請求書を処理する		請求書の支払いをし、時間の経過とともに減価償却される資産の中に隠す。	中
資産書類を維持する	POでの商品受領		ERS商品受領を通して請求書を作成し、時間の経過とともに減価償却される資産の中に隠す。	中
現金申し込み	銀行勘定調整		預金された現金と転記された現金徴収との差額の着服を許す。	高
原価中心点分配を維持する	原価中心点分配転記を実行する		原価を未許可原価中心点に割り当て、それにより、財務報告を歪曲する。	中
内部CO発注を維持する	内部発注決済		未許可発注からの支出を決済し、CO報告を歪曲する。	中
活動の種類を維持する	活動配分		架空データで原価配分を目的として使用される活動の種類を変更し、それにより、原価配分過程を歪曲する。	中
資産マスタを維持する	資産書類を維持する		資産マスタレコードを担当するユーザが、時間をかけてその資産を減価償却することを許すトランザクションを処理することが可能になる。	中
資産マスタを維持する	POでの商品受領		資産を作成し、関連する資産の受領を操作する。	高
間接費転記を処理する	プロジェクトを決済する		間接費支出をプロジェクトに転記し、決済承認プロセスを経ずにプロジェクトを決済する。	中
プロジェクト&WBS要素を維持する	プロジェクトを決済する		架空プロジェクトを使用し、決済承認プロセスを経ずに過剰な実プロジェクトを割り当て、プロジェクトを決済する。	中
プロジェクト&WBS要素を維持する	間接費転記を処理する		作業構成明細要素(プロフィットセンター、ビジネス領域、原価中心点、プラント)を操作し、間接費支出をプロジェクトに転記する。	中
銀行マスタデータを維持する	現金申し込み		本物でない銀行口座を維持し、そこへ入ってくる支払いを迂回する。	高
転記期間を維持する	仕訳記入を転記する		すでに締め切られている会計期間を開き、月末後に記入を不適切に転記する。	中
転記期間を維持する	AP支払い		すでに締め切られている会計期間を開き、月末後に支払いを不適切に転記する。	中
転記期間を維持する	現金申し込み		ユーザは、すでに締め切られている会計期間を開き、月末報告後に入ってくる支払いを記入する。	中
転記期間を維持する	商品移動		すでに締め切られている会計期間を開き、月末後に商品を不適切に受け取るか、または出す。	中

【０１４４】

【表５】

付録-1-2

ビジネス活動 #1	ビジネス活動 #2	ビジネス活動 #3	違反の説明	リスクレベル
GLマスタレコードを維持する	税金/通貨関係仕訳記入を転記する		架空のGL勘定を作成し、雑総勘定元帳活動を生成するか、または記入を転記することで不正活動を隠す。	中
CCまたはCEグループを維持する	税金/通貨関係仕訳記入を転記する		原価中心点報告を操作し、不適切な雑仕訳記入転記を隠す。	中
転記期間を維持する	税金/通貨関係仕訳記入を転記する		すでに締め切られている会計期間を開き、月末後に税金および通貨仕訳記入を不適切に転記する。	中
銀行マスタデータを維持する	手書き小切手処理		本物でない銀行口座を作成し、そこから小切手を作成する。	高
転記期間を維持する	手書き小切手処理		すでに締め切られている会計期間を開き、月末後に支払いを不適切に転記する。	中
財務項目を維持する	財務取引を確認する		ユーザは、架空の取引を作成し、その取引を粉飾して確認するか、または実行する。	高
生産指示処理	製品原価計算		原価差異を減らすために生産量を増やす。	低
生産指示処理	生産指示を確認する		生産指示処理および生産指示の確認	低
生産指示を確認する	製品原価計算		生産性により原価差異を減らすために生産量を増やす。	低
品質管理結果報告	配送処理		配送スケジュールに間に合わすため在庫品を一般リリースに移す。	低
品質管理結果報告	品目点数を記入する-WM	差異を消去する-WM	WM在庫一覧を使って調整することにより粗悪材料を取り除く。	中
商品移動	品目点数を記入する-WM	差異を消去する-WM	商品受領を介して商品を受け入れ、その後WM期末棚卸調整を実行する。	高
品質管理結果報告	生産指示を確認する		生産された材料をGR在庫品にリリースし、生産割当て量を維持する。	低
仕訳記入を転記する	品目点数を記入する-WM	差異を消去する-WM	帳簿記入を介してWM在庫調整を隠す。	中
品質管理結果報告	品目点数を記入する-IM	差異を消去する-IM	IM在庫一覧を使って調整することにより粗悪材料を取り除く。	中
品質管理結果報告	品目点数を記入し、差異を消去		IM在庫一覧を使って調整することにより粗悪材料を取り除く。	中
商品移動	品目点数を記入する-IM	差異を消去する-IM	商品受領を介して商品を受け入れ、その後IM期末棚卸調整を実行する。	高
商品移動	品目点数を記入し、差異を消去する-IM		商品受領を介して商品を受け入れ、その後IM期末棚卸調整を実行する。	高
仕訳記入を転記する	品目点数を記入し、差異を消去する-IM		帳簿記入を介してIM在庫調整を隠す。	中
仕訳記入を転記する	品目点数を記入する-IM	差異を消去する-IM	帳簿記入を介してIM在庫調整を隠す。	中
ベンダーマスタの維持	ベンダー請求書を処理する		架空のベンダーを維持し、自動支払いに対するベンダー請求書を記入する。	高
AP支払い	ベンダーマスタの維持		架空のベンダーを維持し、そのベンダーへの支払いを作成する。	高
ベンダー請求書を処理する	AP支払い		架空のベンダー請求書を記入し、次いで、そのベンダーに対し支払いをする。	高
発注書を維持する	ベンダー請求書を処理する		未許可品目を購入し、請求書作成により支払いを開始する。	高
発注書を維持する	POでの商品受領		個人使用のため架空の発注書を記入し、商品受領を通じて商品を受け取る。	高
ベンダー請求書を処理する	POでの商品受領		架空のベンダー請求書を記入し、商品受領を通じて商品を受け取る。	高

【０１４５】

【表６】

付録-1-3

ビジネス活動 #1	ビジネス活動 #2	ビジネス活動 #3	違反の説明	リスクレベル
発注書を維持する	AP支払い		架空の発注書を記入し、包括的支払いを記入する。	高
ベンダーマスタの維持	発注書を維持する		架空のベンダーを作成し、そのベンダーに対する購入を開始する。	高
ブロックされた請求書をリリースする	サービス受領		サービスを受け取るか、または受け入れ、すでにブロックされている請求書をリリースして、受領書を相殺する。	中
ブロックされた請求書をリリースする	発注書を維持する		未許可発注書を記入し、すでにブロックされている請求書をリリースして、発注書を相殺する。	中
発注書を維持する	品目点数を記入し、差異を消去する-IM		品目を不適切に調達し、IM期末棚卸点数を操作して隠す。	高
サービスマスタの維持	購買要求		サービスマスタデータを修正またはそれに追加し(通常は会社によって発注されない品目を追加する)、次いで購買要求を作成/変更する。	中
材料マスタの維持	発注書を維持する		材料マスタファイルに品目を追加し、それらの品目に関する詐欺的発注書を作成する。	中
銀行勘定調整	ベンダー請求書を処理する		銀行支払いと転記されたAPレコードとの差異を不適切に隠す。	高
ブロックされた請求書をリリースする	POでの商品受領		発注書と突き合わせて商品を受け取り、すでにブロックされている請求書をリリースして、受領書を相殺する。	中
サービス受領	AP支払い		サービスを受け取るか、または受け入れ、包括的支払いを記入する。	高
発注書を維持する	サービス受領		個人使用のため架空の発注書を記入し、サービス受領を通じてサービスを受け取る。	中
材料マスタの維持	購入契約		材料マスタファイルに品目を追加し、次いで、それらの品目を購入契約に不正に追加する。	中
PO承認	POでの商品受領		未許可商品の購入を承認し、発注を完全には受け取らないことにより在庫の悪用を隠す。	高
PO承認	AP支払い		会社に不正購入を任せ、未許可商品およびサービスの支払いを開始する。	高
PO承認	ベンダー請求書を処理する		本物でない発注書をリリースし、請求書を記入することにより発注の支払いを開始する。	高
PO承認	品目点数を記入する-IM	差異を消去する-IM	本物でない発注書をリリースするが、この行為はIM期末棚卸数を操作することにより検出されないままである。	高
PO承認	ベンダーマスタの維持		架空のベンダーを作成するか、または既存のベンダーマスタデータを変更し、このベンダーに対する購入を承認する。	高
PO承認	材料マスタの維持		材料マスタデータを追加または修正し、個人使用のため発注書をリリースする。	中
ブロックされた請求書をリリースする	購入契約		購入契約を修正し、すでにブロックされている請求書をリリースして、ベンダー勘定を相殺する。	中
AP支払い	購入契約		架空の購入契約を交わし、次いで支払いをする。	高
ベンダーマスタの維持	購入契約		架空の購入契約を交わすリスク、および架空のベンダーの入力または既存ベンダー特に勘定データの修正。	高

【０１４６】

【表７】

付録-1-4

ビジネス活動 #1	ビジネス活動 #2	ビジネス活動 #3	違反の説明	リスクレベル
購入契約	POでの商品受領		購入契約を修正し、次いで、詐欺目的で商品を受け取る。	高
ベンダー請求書を処理する	購入契約		未許可品目を購入契約に記入し、個人使用のためそれらの品目を得る請求書を作成する。	高
AP支払い	サービスマスタの維持		サービスマスタデータを修正する(通常は会社によって発注されないサービスを追加する)リスク、および包括的支払いの記入。	高
サービスマスタの維持	購買要求をリリースする		サービスマスタファイルにサービスを追加するリスク(ビジネス目的に関係しないサービス)、およびそれらのサービスに対する購買要求を作成することができること。	中
購買要求をリリースする	購入契約		購買契約を交わすか、または維持し、そのリリースを通じて関係する購買要求を許可するリスク。	中
購買要求	発注書を維持する		同じ人が1つの品目を要求し、その要求から発注書を作成するリスク。	中
発注書を維持する	サービスマスタの維持		サービスマスタファイルに品目を追加し、それらの品目に関する詐欺的発注書を作成する。	中
購入契約	品目点数を記入し、差異を消去する-IM		同じ人が材料に関する購入契約を交わし、次いで、それらの材料についてIM在庫を調整するリスク。	中
材料マスタの維持	購買要求		材料マスタデータを修正またはそれに追加し(通常は会社によって発注されない材料を追加する)、次いで材料要求をリリースするリスク。	中
購買要求	購買要求をリリースする		同じ人が1つの品目を要求し、次いで購買要求をリリースし、許可プロセスをバイパスするリスク。	中
AP支払い	銀行勘定調整		未許可支払いを記入し、同じ人を通して銀行と勘定調整を行うリスク。	高
ベンダー請求書を処理する	手書き小切手処理		架空のベンダー請求書を記入し、次いで、そのベンダーに対し手書き小切手処理をするか、支払いをする。	高
発注書を維持する	手書き小切手処理		架空の発注書を記入し、手書き小切手を処理し、包括的手書き小切手支払いの役目を果たすようにする。	高
サービス受領	手書き小切手処理		サービスを受け取るか、または受け入れ、包括的手書き小切手支払いを記入する。	高
PO承認	手書き小切手処理		会社に不正購入契約を交わさせ、未許可商品およびサービスの手書き小切手支払いを開始する。	高
手書き小切手処理	購入契約		架空の購入契約を交わし、次いで手書き小切手支払いをする。	高
手書き小切手処理	サービスマスタの維持		サービスマスタデータを修正する(通常は会社によって発注されないサービスを追加する)リスク、および包括的手書き小切手支払いの記入。	高
手書き小切手処理	銀行勘定調整		未許可手書き小切手支払いを記入し、同じ人を通して銀行と勘定調整を行う。	高
発注書を維持する	PO承認		リリース戦略が使用される場合、同じユーザは、発注書を保持し、それをリリースまたは承認することがあってはならない。	高
信用管理	販売注文、取り決め、または契約		販売書類を記入または修正し、顧客信用限度を承認する。	高

【０１４７】

【表８】

付録-1-5

ビジネス活動 #1	ビジネス活動 #2	ビジネス活動 #3	違反の説明	リスクレベル
販売注文、取り決め、または契約	顧客収支を消去する		販売書類を作成し、即座に、顧客の義務を消去する。	高
販売注文、取り決め、または契約	顧客マスタの維持		架空の顧客を作成し、不正販売書類の実施を開始する。	高
顧客マスタの維持	顧客請求書を処理する		マスタレコード(支払い条件、許容範囲レベル)未許可変更を、顧客に有利なように行い、不適切な請求書を記入する。	高
顧客マスタの維持	売上割り戻し		リベート契約を不適切に作成するか、または変更し、顧客の有利になるように顧客のマスタレコードを管理する。支払いが不適切な場所に行くように顧客のマスタレコードを変更することも可能であろう。	高
顧客収支を消去する	請求伝票を維持する		潜在的に、顧客の以前の収支を消去し、同じ顧客について請求伝票を作成するか同じ変更を加え、その顧客の義務を消去する。	高
販売注文、取り決め、または契約	請求伝票を維持する		販売書類を不適切に作成または変更し、それに対応する請求伝票を生成する。	高
信用管理	売上割り戻し		ユーザの信用限度を操作し、リベートを大盤振る舞いし、限界顧客の注文を実行する。	高
販売注文、取り決め、または契約	現金申し込み		架空の販売書類を記入し、次いで架空の支払いをする。	中
現金申し込み	請求伝票を維持する		顧客に対し請求伝票を作成し、同じ顧客から支払いを不適切に転記し、不払いを隠蔽する。	高
顧客マスタの維持	AR支払い		架空の顧客を作成し、未許可の顧客に対する支払いを開始する。	高
入金伝票を処理する	AR支払い		架空の入金伝票を記入することにより顧客への未許可支払いを開始する。	高
現金申し込み	売上送状リリース		売掛勘定レコードを変更し、顧客計算書との違いをカバーするようにする。	高
販売注文、取り決め、または契約	配送処理		架空の販売書類を作成することにより未許可出荷を隠す。	高
顧客請求書を処理する	販売価格の維持		売上送状に対する販売価格修正。	高
販売注文、取り決め、または契約	販売価格の維持		販売書類を記入し、詐欺による利益を得るため価格を下げる。	高
信用管理	現金申し込み		信用承認機能を実行し、詐欺目的で受け取った現金を修正する。	高
現金申し込み	売上割り戻し		架空の売上割り戻しを記入し、次いで架空の支払いをする。	高
現金申し込み	顧客マスタの維持		同じ人が顧客マスタファイルに変更を加え、顧客に対する受け入れ現金を修正するリスク。	高
販売注文、取り決め、または契約	販売注文書リリース		同じ人による販売書類の記入およびリリースのリスク。	中
販売注文、取り決め、または契約	売上割り戻し		販売書類を記入し、同じ人による売上割り戻しを与え、効果的に間接的値引きを与えるリスク。	中
顧客請求書を処理する	信用管理		売上送状を修正し、記入し、同じ人による信用限度を承認するリスク。	高
請求伝票を維持する	販売価格の維持		売上送状に対する販売価格修正のリスク。	高

【０１４８】

【表９】

付録-1-6

ビジネス活動 #1	ビジネス活動 #2	ビジネス活動 #3	違反の説明	リスクレベル
顧客マスタの維持	顧客収支を消去する		顧客マスタレコードを維持し、それと突き合わせて詐欺的支払いを転記する。	高
顧客マスタの維持	請求伝票を維持する		ユーザは、架空の顧客を作成し、次いで、顧客に請求書を発行することができる。	高
現金申し込み	顧客請求書を処理する		ユーザは、請求書を作成/変更し、その請求書と突き合わせて支払いを記入/変更することができる。	高
配送処理	現金申し込み		ユーザは、架空の/不正な配送を作成し、これらの潜在的不正流用商品に対し支払いを記入することができる。	高
販売注文、取り決め、または契約	顧客請求書を処理する		ユーザは、詐欺的販売契約を作成し、追加の商品を取り込み、不正な顧客請求書を記入して、詐欺を隠すことができる。	高
顧客収支を消去する	入金伝票を処理する		顧客に対し入金伝票を作成し、次いで同じ顧客を消去し、その顧客に対し支払いを促す。	高
従業員(PA)マスタデータを維持する	給与支払いを処理する		給与マスタデータを修正し、給与を処理する。詐欺活動の可能性がある。	高
HR手当	給与支払いを処理する		従業員HR手当を変更し、次いで、許可なく給与を処理する。詐欺活動の可能性がある。	高
第三者送金	ベンダーマスタの維持		マスタデータへの変更、および送金の実行の結果、詐欺的支払いが行われる可能性がある。	高
時間データを維持する	時間を承認する		給与マスタデータを変更し、不正設定に適用される時間データを入力する。	高
時間データを維持する	給与支払いを処理する		時間データを修正し、給与を処理した結果、詐欺的支払いが行われる。	高
給与構成を変更する	給与支払いを処理する		給与の構成を変更し、次いで、給与を処理し、その結果、詐欺的支払いが行われる。	高
従業員(PA)マスタデータを維持する	給与構成を変更する		給与の構成を変更し、次いで、給与マスタデータを修正し、その結果、詐欺的支払いが行われる。	高
PD構造の維持	従業員(PA)マスタデータを維持する		給与マスタデータを変更し、PD構造を修正する。	高
時間データを維持する	給与維持		偽りの時間データを入力し、給与維持を実行する。	高
給与維持	給与支払いを処理する		適切な許可なく給与を変更し、給与を処理する。	高
給与構成を変更する	給与維持		給与構成を変更し、給与設定に対し維持を実行する。	高
時間データを維持する	給与構成を変更する		給与構成を修正し、偽りの時間データを入力する。	高
時間データを維持する	PD構造を修正する		偽りの時間データを入力し、PD構造を維持する。	高
従業員(PA)マスタデータを維持する	時間データを維持する		ユーザは、偽りの時間データを入力し、給与を処理した結果、詐欺的支払いを行うことができる。	高
従業員(PA)マスタデータを維持する	給与維持		ユーザは、賃金を含む従業員マスタデータを維持し、給与結果を削除することができる。	高
給与体系	時間データを維持する		ユーザは、偽りの時間データを入力し、作業スケジュール評価を実行することができる。	高
時間評価	時間データを維持する		ユーザは、偽りの時間データを入力し、時間評価を実行することができる。	中

【０１４９】

【表１０】

付録-1-7

ビジネス活動 #1	ビジネス活動 #2	ビジネス活動 #3	違反の説明	リスクレベル
時間評価	PD構造を修正する		時間評価を実行し、承認のデータを間違った経路で送るようにPD構造を変更する。	中
時間評価	給与維持		時間評価を実行し、給与処理を混乱させる可能性のある給与結果を削除する。	中
時間評価	給与支払いを処理する		時価評価を実行し、給与を処理するユーザは、詐欺行為を隠すことが可能である。	中
時間評価	給与体系		両方の時価評価を実行し、給与体系を維持するユーザは、詐欺行為を隠す。	中
基本開発	システム管理		開発者は、生産において既存のプログラムを修正し、プログラムに対するトレースを実行し、そのプログラムを実行するように生産環境を構成することが可能である。これは、システム性能、データ完全性、不適切なプログラム修正に影響を及ぼす可能性があり、生産において不適切に修正されたこれらのプログラムを実行することができる。	中
基本開発	構成		開発者は、生産において既存のプログラムを修正し、プログラムに対するトレースを実行し、アラーム閾値を高くし、外部OSコマンドを通じて監査証跡をなくすことにより実行されるプログラムの監視を制限するように生産環境を構成することが可能である。	高
基本開発	クライアント管理		開発者は、生産におけるプログラムを作成または修正し、それらの変更を他のクライアントに複製することが可能である。これにより、トランスポートプロセスにおける固有の管理がバイパスされ、DVおよびQAクライアントに悪影響を及ぼす可能性がある。	中
基本開発	トランスポート管理		開発者は、生産におけるプログラムを作成または修正し、これらの変更のトランスポートを、不正な開発プラクティスを隠すため事後に強制することが可能である。これにより、さらに、生産において行われた変更を追跡せずにオリジナルバージョンのプログラムに戻すことが可能である。	高
基本ユーティリティ	システム管理		開発者は、R/3プログラムコンポーネント(メニュー、画面レイアウト、メッセージ、クエリ)を修正し、これらの変更とともにプログラムを実行するように生産環境を構成することが可能である。これは、システム性能、データ完全性、不適切なプログラム修正に影響を及ぼす可能性があり、生産において不適切に修正されたこれらのプログラムコンポーネントを実行することができる。	中
基本ユーティリティ	構成		開発者は、R/3プログラムコンポーネント(メニュー、画面レイアウト、メッセージ、クエリ)を修正し、アラーム閾値を高くし、外部OSコマンドを通じて監査証跡をなくすことにより修正されたプログラムコンポーネントを使用して実行されるプログラムの監視を制限するように生産環境を構成することが可能である。	高

【０１５０】

【表１１】

付録-1-8

ビジネス活動 #1	ビジネス活動 #2	ビジネス活動 #3	違反の説明	リスクレベル
基本ユーティリティ	クライアント管理		開発者は、R/3プログラムコンポーネント(メニュー、画面レイアウト、メッセージ、クエリ)を修正し、これらの変更を他のクライアントに複製することが可能である。これにより、トランスポートプロセスにおける固有の管理がバイパスされ、DVおよびQAクライアントに悪影響を及ぼす可能性がある。	中
基本ユーティリティ	トランスポート管理		開発者は、R/3プログラムコンポーネント(メニュー、画面レイアウト、メッセージ、クエリ)を修正し、これらの変更のトランスポートを、不正な開発プラクティスを隠すため事後に強制することが可能である。これにより、さらに、生産において行われた変更を追跡せずにオリジナルバージョンのプログラムコンポーネントに戻すことが可能である。	高
基本テーブル維持	システム管理		個人は、R/3テーブル中のデータを修正するか、または有効な構成値を修正し、不適切に修正されたデータを使用してR/3トランザクションおよびプログラムを実行するように生産環境をセットアップすることが可能である。これは、データ完全性、システム性能、および生産環境の適切な構成に影響を及ぼす可能性がある。	高
基本テーブル維持	クライアント管理		個人は、R/3テーブル中のデータを修正するか、または有効な構成値を変更し、これらの変更を他のクライアントに複製することが可能である。これは、クライアント管理トランザクションにクライアント独立の権限が付属し、クライアント独立のテーブルおよび構成パラメータを修正できる場合に特に影響を受けやすい。	高
セキュリティ管理	クライアント管理		個人は、役割および任命を不適切に修正し、この変更を生産のミラーコピーに反映させ、適切なセットアップに戻る可能性をなくすことが可能である。	高
セキュリティ管理	トランスポート管理		セキュリティ管理者は、未許可セキュリティ役割に不適切な変更を加え、トランスポートし、それらの役割を架空のユーザに任命して実行させることが可能である。	高
アーカイブ	システム管理		管理者は、エンドユーザのピーク時の使用に際してアーカイブトランザクションを実行し、システム性能に影響を及ぼす、アーカイブ機能を履行するために最大のシステム資源が得られるように生産システムを管理することが可能である。	中
アーカイブ	構成		ユーザは、アラーム閾値を高くし、外部OSコマンドを通じて監査証跡をなくすことにより、不適切なアーカイブ実行の監視を制限するように生産環境を構成することが可能である。	中
アーカイブ	クライアント管理		ユーザは、クライアント独立データおよび設定を不適切にアーカイブし、クライアント管理機能を使用して、そのような変更を他のクライアントに複製することが可能である。	中

【０１５１】

【表１２】

付録-1-9

ビジネス活動 #1	ビジネス活動 #2	ビジネス活動 #3	違反の説明	リスクレベル
アーカイブ	トランスポート管理		通常、アーカイブを担当する個人は、ビジネスプロセスおよびデータ維持ニーズを理解しているエンドユーザである。その職務は、トランスポート管理トランザクションを必要としない。トランスポート管理を受け持つユーザについては、その逆が言える。	中
トランスポートを作成する	トランスポートを実行する		トランスポートを作成し、オブジェクトをトランスポートに追加し、トランスポートを移動することができる。未許可オブジェクト変更を生産状態にし、変更管理プロセスをバイパスすることができる。	高
数値範囲を維持する	システム管理		数値範囲(1)をリセットし、ログ/監査証跡(2)を削除することができる。	高
ユーザマスタを維持する	プロファイル/役割を維持する		プロファイル/役割におけるアクセス権とユーザidの両方を管理するのが1人だと、不適切なアクセスのリスクが増大する。	高
モデルを維持する	需給計画		計画モデルおよびバージョンの未許可維持は、APOに格納されている生産計画データに悪影響を及ぼすことがある。このトランザクションは、選択された需要計画スーパーユーザまたはマネージャに制限されるべきである。	高
モデル&バージョン管理	需給計画		アクティブな計画バージョンの未許可削除は、APOに格納されている生産計画データに悪影響を及ぼすことがある。このトランザクションは、選択された需要計画スーパーユーザまたはマネージャに制限されるべきである。	高
バージョンを削除する(バージョン000～アクティブバージョン)	需給計画		計画モデルおよびバージョンの未許可維持は、APOに格納されている生産計画データに悪影響を及ぼすことがある。このトランザクションは、選択された需要計画スーパーユーザまたはマネージャに制限されるべきである。	高
DPにおけるコピー/バージョン管理	需給計画		「マスタデータを維持する」へのアクセスは、権限のある個人に制限されていない場合があり、非互換機能から分離されていない場合がある。マスタデータに対し不適切な変更を行うと、予定された指示書、プロセス指示書、およびスケジュールに悪影響が出ることがある。	中
計画立案に関連する特徴的な組み合わせを維持する	需給計画		「マスタデータを維持する」へのアクセスは、権限のある個人に制限されていない場合があり、非互換機能から分離されていない場合がある。マスタデータに対し不適切な変更を行うと、予定された指示書、プロセス指示書、およびスケジュールに悪影響が出ることがある。	中
時間バケットプロファイルを維持する	需給計画		「マスタデータを維持する」へのアクセスは、権限のある個人に制限されていない場合があり、非互換機能から分離されていない場合がある。マスタデータに対し不適切な変更を行うと、予定された指示書、プロセス指示書、およびスケジュールに悪影響が出ることがある。	中

【０１５２】

【表１３】

付録-1-10

ビジネス活動 #1	ビジネス活動 #2	ビジネス活動 #3	違反の説明	リスクレベル
予測プロファイルを維持する	需給計画		「マクロ/ルールを維持する」へのアクセスは、変更管理プロセスを介して制御されなければならない。未サポートの、または不正な調整が、マクロ/ルールに行われると、不正確な生産計画および生産スケジュールができあがる可能性がある。	中
上級マクロを定義する	需給計画		「マクロ/ルールを維持する」へのアクセスは、変更管理プロセスを介して制御されなければならない。未サポートの、または不正な調整が、マクロ/ルールに行われると、不正確な生産計画および生産スケジュールができあがる可能性がある。	高
統合ルール維持	需給計画		「マクロ/ルールを維持する」へのアクセスは、変更管理プロセスを介して制御されなければならない。未サポートの、または不正な調整が、マクロ/ルールに行われると、不正確な生産計画および生産スケジュールができあがる可能性がある。	中
転送プロファイルを維持する	需給計画		「転送プロファイルを維持する」-APOの需要計画からR/3の需要管理に需要計画がどのように転送されるかを決定する設定のグループへのアクセスは、需要計画スーパーユーザまたはマネージャに制限されるべきである。	中
需要計画をSNPにリリースする	需給計画		「需要計画をSNPにリリースする」へのアクセスは、需要計画スーパーユーザまたはマネージャに制限されるべきである。未サポートの、または不正な調整が、売上予測データに対し行われると、不正確な生産計画および詳細スケジュールができあがる可能性がある。	中
指示書を作成する	需給計画		「APOにおいて生産指示書に変更を加える」へのアクセスは、適切な生産計画要員に制限される。	中
指示書を処理する	需給計画		「APOにおいて生産指示書に変更を加える」へのアクセスは、適切な生産計画要員に制限される。	中
S＆DP管理	需給計画		「SDP管理(MSDP_ADMIN)を介して計画オブジェクト構造および計画領域を維持する」へのアクセスは、生産環境に制限されなければならない。これらの計画構造に対する未許可変更が行われると、需要計画および生産計画が不正確なものとなる可能性がある。	中
BW管理者ワークベンチ	需給計画		「BW（フィーダーシステム）を維持する」へのアクセスは、需要プランナーおよびエンドユーザから制限されなければならない。「インターフェイスを維持する」への未許可変更があると、データ転送が不正確になる可能性がある。	中
ライブキャッシュ監視	需給計画		ライブキャッシュ環境の再構成が未許可であるか、または誤りがあると、APOと他のフィーダーシステムとの間のデータ転送に影響が出る可能性がある。アクセスは、生産プランナーから制限されなければならない。	中

【０１５３】

【表１４】

付録-1-11

ビジネス活動 #1	ビジネス活動 #2	ビジネス活動 #3	違反の説明	リスクレベル
リードを生成し処理する	機会を維持する		機会を維持すること(リードをクォリファイする)は、リードを生成することとは独立していなければならない。販売/生産予測は、クォリファイドリードの数に基づくことが可能である。企業によっては、委託手数料を、クォリファイドリードの数に基づいて支払うことが可能である。	中
リードを生成し処理する	ビジネスパートナーを維持する		キービジネスパートナーデータの作成は、マーケティンググループのリードおよび機会管理から分離されなければならない。BPは、マスタデータグループによる適切なレビューの後になって作成されるべきである。	中
ビジネスパートナーを維持する	CRM販売注文を処理する		ユーザは、架空のビジネスパートナーを作成し、そのパートナーに対し詐欺的販売注文を開始することが可能である。ビジネスパートナーなどのマスタデータは、そのマスタデータを使用してトランザクションを処理する同じユーザによって維持されなければならない。	高
CRM販売注文を処理する	配送処理		ユーザは、架空の販売注文を作成して、未許可出荷を隠すことが可能である。	高
CRM販売注文を処理する	CRM請求伝票作成		販売書類を不適切に作成または変更し、CRMにおける対応する請求伝票を生成する。	高
CRM販売注文を処理する	R/3請求伝票作成		販売書類を不適切に作成または変更し、R/3における対応する請求伝票を生成する。	高
サービス注文処理	サービス確認		個人使用のため架空のサービス注文を行い、サービス受領を通じてサービスを受け取る。ユーザは、詐欺的支払いを促すことが可能である。それに加えて、スペアパーツを、確認の結果として在庫から詐欺として支給することが可能である。	高
CRM請求伝票作成	ビジネスパートナーを維持する		ユーザは、架空のビジネスパートナーを作成し、次いで、そのパートナーに対しCRMの請求伝票を処理することができる。	高
R/3請求伝票作成	ビジネスパートナーを維持する		ユーザは、架空のビジネスパートナーを作成し、次いで、そのパートナーに対しR/3の請求伝票を処理することができる。	高
サービス確認	CRM請求伝票作成		サービス注文を不適切に受け入れるか、または確認し、その注文書に対しCRMの対応する請求伝票を生成する。	高
サービス確認	R/3請求伝票作成		サービス注文を不適切に受け入れるか、または確認し、その注文書に対しR/3の対応する請求伝票を生成する。	高
入庫配送処理	入金伝票を処理する(苦情)		社内ユーザが、顧客と共謀し、架空の入庫配送(顧客によって記入された苦情に基づく)を処理し、顧客への入金伝票を処理することができる。	中
入金伝票を処理する(苦情)	CRM請求伝票作成		ユーザは、架空の入金伝票を作成し、CRMにおいて支払うべき課金を実行し、顧客への支払いを促すことが可能である。顧客は、社内ユーザにキックバックを提供することが可能である。	高

【０１５４】

【表１５】

付録-1-12

ビジネス活動 #1	ビジネス活動 #2	ビジネス活動 #3	違反の説明	リスクレベル
入金伝票を処理する(苦情)	R/3請求伝票作成		ユーザは、架空の入金伝票を作成し、R/3において支払うべき課金を実行し、顧客への支払いを促すことが可能である。顧客は、社内ユーザにキックバックを提供することが可能である。	高
顧客請求書	価格設定条件を維持する		価格設定条件を操作して、不正な請求書において実現される不適切な値引き/インセンティブを顧客に提供することが可能である。	高
CRM販売注文を処理する	価格設定条件を維持する		ユーザは、CRMの販売注文書に記入し、詐欺による利益に対する条件を介して価格を下げることが可能である。	高
機会を維持する	インセンティブ処理		委託手数料/インセンティブは、クォリファイドリードの数に基づいて支払うことができる。 クォリファイドリードが不適切だと、詐欺的委託手数料支払いが発生する可能性がある。	高
サービス注文処理	インセンティブ処理		委託手数料/インセンティブは、サービス注文の数に基づいて支払うことができる。 詐欺的注文は、大きな売上を達成して委託手数料を得るために行うことが可能である。	高
CRM販売注文を処理する	インセンティブ処理		委託手数料/インセンティブは、販売注文の数に基づいて支払うことができる。詐欺的注文は、大きな売上報告を達成して委託手数料を得るために行うことが可能である。	高
製品/カタログの維持	CRM販売注文を処理する		製品カタログに品目を追加し、それらの品目に関する架空の販売注文を作成する。	中
SRMベンダーマスタ	SRM請求書作成		架空のベンダーを維持し、自動支払い実行に入れる請求書を記入する。	高
SRM購入	SRM請求書作成		未許可品目を購入し、請求書作成により支払いを促す。	高
SRM購入	SRM商品受領/サービス受け入れ		個人使用のため架空の発注書を記入し、商品受領またはサービス受け入れを通じて商品またはサービスを受け取る。	高
SRM請求書作成	SRM商品受領/サービス受け入れ		架空の請求書を記入し、商品受領またはサービス受け入れを介して商品またはサービスを受け取る。	高
SRMベンダーマスタ	SRM購入		架空のベンダーを維持し、そのベンダーに対する購入を開始する。	高
SRM購入	R/3 WMで品目点数を記入する	R/3 WMで差異を消去する	品目を不適切に調達し、WM期末棚卸点数を操作して隠す。	中
SRM購入	R/3 IMで品目点数を記入する	R/3 IMで差異を消去する	品目を不適切に調達し、IM期末棚卸点数を操作して隠す。	中
SRM購入	R/3 IMで品目点数を記入し、差異を消去する		品目を不適切に調達し、IM期末棚卸点数を操作して隠す。	中
SRM製品の維持	SRM購入		カタログまたはマスタファイルに品目を追加し、それらの品目に関する詐欺的発注書を作成する。	中
R/3銀行勘定調整	SRM請求書作成		ユーザは、銀行支払いと転記されたAPレコードとの差異を隠すことができる。	高
SRM商品受領	R/3 WMで品目点数を記入する	R/3 WMで差異を消去する	SRM商品受領を介して商品を受け入れ、その後WM期末棚卸調整を実行する。	高
SRM商品受領	R/3 IMで品目点数を記入する	R/3 IMで差異を消去する	SRM商品受領を介して商品を受け入れ、その後IM期末棚卸調整を実行する。	高

【０１５５】

【表１６】

付録-1-13

ビジネス活動 #1	ビジネス活動 #2	ビジネス活動 #3	違反の説明	リスクレベル
SRM商品受領	R/3 IMで品目点数を記入し、差異を消去する		SRM商品受領を介して商品を受け入れ、その後強力なIMトランザクションを使用してIM期末棚卸調整を実行する。	高
SRM購入	POへのR/3商品受領		個人使用のため架空の発注書を記入し、商品受領を通じて商品またはサービスにアクセスする。	高
SRM購入	R/3サービス受け入れ		個人使用のため架空の発注書を記入し、サービス受け入れを通じて商品またはサービスにアクセスする。	高
ショッピングカートを維持する	SRM製品の維持		ショッピングカートに入れる商品を選択することにより架空の商品に対する購入を開始する。	中
ショッピングカートを維持する	SRMベンダーマスタ		架空のベンダーを維持し、ショッピングカートに入れる商品を選択することによりそのベンダーへの購入を開始する。	中
SRM PO承認	SRM商品受領/サービス受け入れ		未許可商品の購入を承認し、SRMにおいて発注を完全には受け取らないことにより在庫の悪用を隠す。	高
SRM PO承認	POへのR/3商品受領		未許可商品の購入を承認し、R/3において発注を完全には受け取らないことにより在庫の悪用を隠す。	高
SRM購入	SRM PO承認		リリース戦略が使用される場合、同じユーザは、発注書を保持し、それをリリースまたは承認することがあってはならない。	高
SRMベンダーマスタ	SRM PO承認		架空のベンダーを作成するか、または既存のベンダーマスタデータを変更し、このベンダーに対する購入を承認する。	高
整理統合階層を維持する	AP支払い		支払い処理、金銭の受領、GL勘定アクセスと連動するAP/AR/GLマスタデータ作成および転記機能、およびECCS階層および報告出力を修正する機能。	高
整理統合階層を維持する	ベンダー請求書を処理する		支払い処理、金銭の受領、GL勘定アクセスと連動するAP/AR/GLマスタデータ作成および転記機能、およびECCS階層および報告出力を修正する機能。	高
整理統合階層を維持する	手書き小切手処理		支払い処理、金銭の受領、GL勘定アクセスと連動するAP/AR/GLマスタデータ作成および転記機能、およびECCS階層および報告出力を修正する機能。	高
整理統合階層を維持する	現金申し込み		支払い処理、金銭の受領、GL勘定アクセスと連動するAP/AR/GLマスタデータ作成および転記機能、およびECCS階層および報告出力を修正する機能。	高
整理統合階層を維持する	顧客請求書を処理する		支払い処理、金銭の受領、GL勘定アクセスと連動するAP/AR/GLマスタデータ作成および転記機能、およびECCS階層および報告出力を修正する機能。	高
整理統合階層を維持する	原価中心点を維持する		支払い処理、金銭の受領、GL勘定アクセスと連動するAP/AR/GLマスタデータ作成および転記機能、およびECCS階層および報告出力を修正する機能。	高
整理統合階層を維持する	資産書類を維持する		支払い処理、金銭の受領、GL勘定アクセスと連動するAP/AR/GLマスタデータ作成および転記機能、およびECCS階層および報告出力を修正する機能。	高

【０１５６】

【表１７】

付録-1-14

ビジネス活動 #1	ビジネス活動 #2	ビジネス活動 #3	違反の説明	リスクレベル
整理統合階層を維持する	資産マスタを維持する		支払い処理、金銭の受領、GL勘定アクセスと連動するAP/AR/GLマスタデータ作成および転記機能、およびECCS階層および報告出力を修正する機能。	高
整理統合階層を維持する	収益再転記		支払い処理、金銭の受領、GL勘定アクセスと連動するAP/AR/GLマスタデータ作成および転記機能、およびECCS階層および報告出力を修正する機能。	高
整理統合階層を維持する	仕訳記入を転記する		支払い処理、金銭の受領、GL勘定アクセスと連動するAP/AR/GLマスタデータ作成および転記機能、およびECCS階層および報告出力を修正する機能。	高
整理統合階層を維持する	GLマスタレコードを維持する		支払い処理、金銭の受領、GL勘定アクセスと連動するAP/AR/GLマスタデータ作成および転記機能、およびECCS階層および報告出力を修正する機能。	高
整理統合階層を維持する	税金/通貨関係仕訳記入を転記する		支払い処理、金銭の受領、GL勘定アクセスと連動するAP/AR/GLマスタデータ作成および転記機能、およびECCS階層および報告出力を修正する機能。	高
整理統合階層を維持する	ベンダーマスタの維持		支払い処理、金銭の受領、GL勘定アクセスと連動するAP/AR/GLマスタデータ作成および転記機能、およびECCS階層および報告出力を修正する機能。	高
整理統合階層を維持する	顧客マスタの保持		支払い処理、金銭の受領、GL勘定アクセスと連動するAP/AR/GLマスタデータ作成および転記機能、およびECCS階層および報告出力を修正する機能。	高

【符号の説明】

【０１５７】

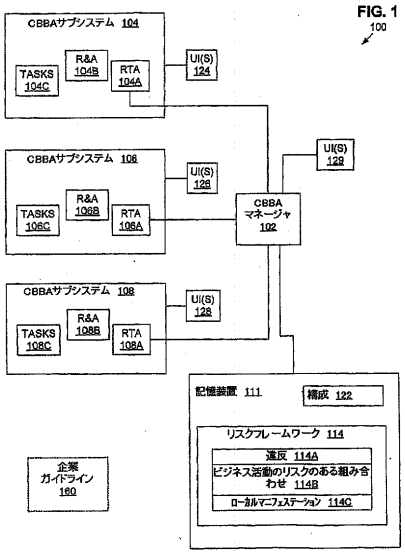
100 システム

102 CBBAマネージャ

104～108 ローカルCBBAサブシステム

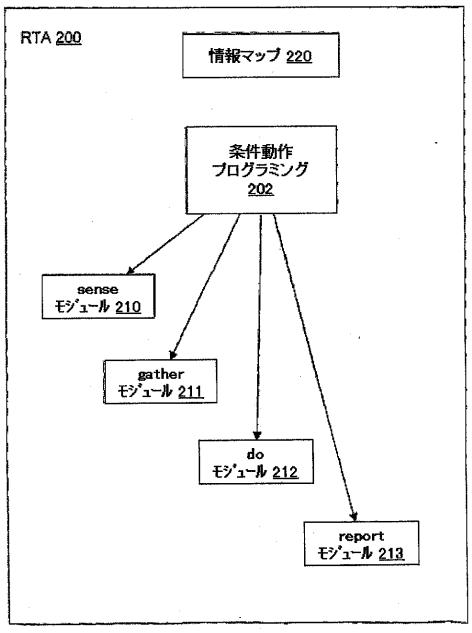
111 記憶装置

【図１】



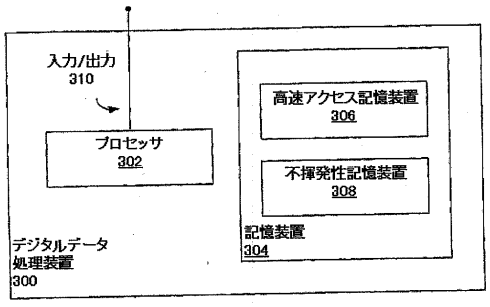
【図２】

FIG. 2



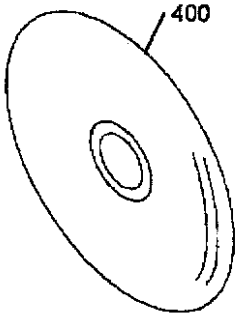
【図３】

FIG. 3



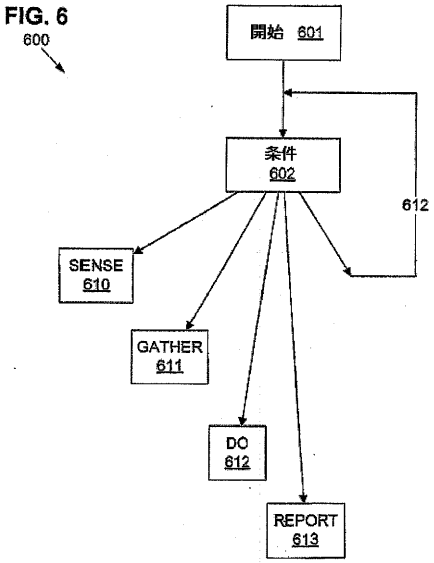
【図４】

FIG. 4



【図６】

FIG. 6



【図７】

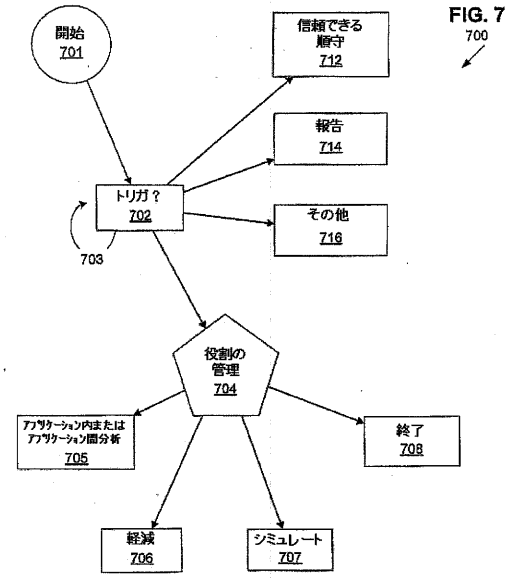


FIG. 7
700
開始
701
信頼できる
順守
712
報告
714
その他
716
トリガ？
702
703
役割の
管理
704
アプリケーション内または
アプリケーション間分析
705
終了
708
軽減
706
シミュレート
707

【図８】

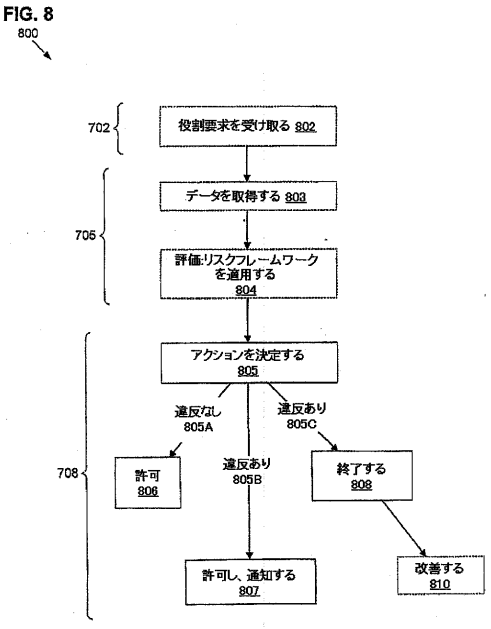


FIG. 8
800
702
役割要求を受け取る 802
705
データを取得する 803
評価リスクフレームワーク
を適用する
804
アクションを決定する
805
違反なし
805A
違反あり
805C
708
許可
806
違反あり
805B
終了する
808
許可し、通知する
807
改善する
810

【図９】

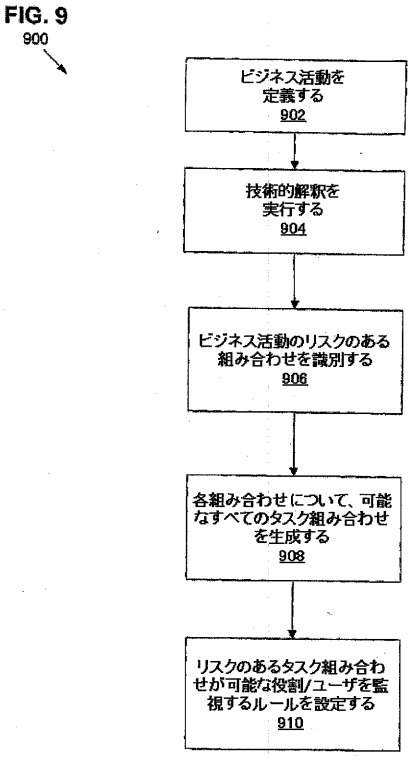


FIG. 9
900
ビジネス活動を
定義する
902
技術的解釈を
実行する
904
ビジネス活動のリスクのある
組み合わせを識別する
906
各組み合わせについて、可能
なすべてのタスク組み合わせ
を生成する
908
リスクのあるタスク組み合わ
せが可能な役割/ユーザを監
視するルールを設定する
910

【図１０】

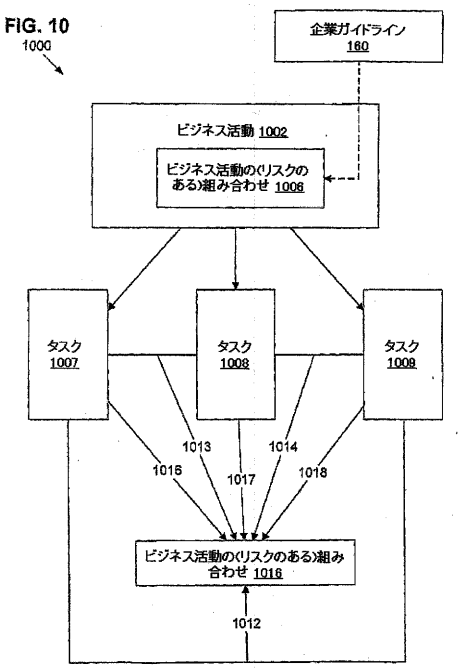
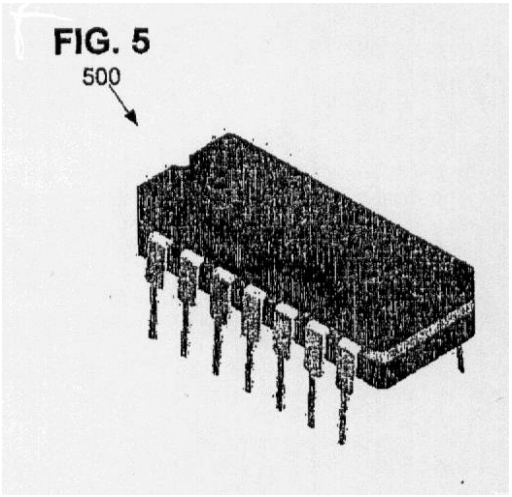


FIG. 10
1000
企業ガイドライン
160
ビジネス活動 1002
ビジネス活動のリスクの
ある組み合わせ 1006
タスク
1007
タスク
1008
タスク
1009
1013
1014
1015
1017
1018
ビジネス活動のリスクのある組み
合わせ 1016
1012

【図５】



フロントページの続き

(72)発明者　スーザン・ステイプルトン
アメリカ合衆国・ミズーリ・６３１２８・セント・ルイス・クリスタル・パーク・サークル・５８７１
(72)発明者　スリニヴァサ・カッケラ
アメリカ合衆国・カリフォルニア・９４５６０・ニューアーク・ポトレロ・ドライヴ・３９８９６

審査官　川崎　優

(56)参考文献　Guardium Solutions for Safeguading Databases, ２００５年　4月２５日, ＵＲＬ, http://web.archive.org/web/20050425100935/guardium.com/media/Data_Sheet_SQLG_111604.pdf

(58)調査した分野(Int.Cl., ＤＢ名)
Ｇ０６Ｑ　１０／００
Ｇ０６Ｆ　１１／３４, １３／００, ２１／３０－４６, ６０－８８