(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6050374号
(P6050374)
(45)発行日　平成28年12月21日(2016.12.21)　(24)登録日　平成28年12月2日(2016.12.2)

(51)Int.Cl.　F I
G06F 21/62 (2013.01)　G06F 21/62　３１８
G06F 12/00 (2006.01)　G06F 12/00　５３７Ａ

請求項の数 18　(全 21 頁)

(21)出願番号　特願2014-544786(P2014-544786)
(86)(22)出願日　平成24年11月21日(2012.11.21)
(65)公表番号　特表2015-505391(P2015-505391A)
(43)公表日　平成27年2月19日(2015.2.19)
(86)国際出願番号　PCT/US2012/066167
(87)国際公開番号　WO2013/081921
(87)国際公開日　平成25年6月6日(2013.6.6)
審査請求日　平成27年11月24日(2015.11.24)
(31)優先権主張番号　13/308,572
(32)優先日　平成23年12月1日(2011.12.1)
(33)優先権主張国　米国(US)

(73)特許権者　314015767
マイクロソフト　テクノロジー　ライセンシング，エルエルシー
アメリカ合衆国　ワシントン州　９８０５２　レッドモンド　ワン　マイクロソフト　ウェイ
(74)代理人　100140109
弁理士　小野　新次郎
(74)代理人　100075270
弁理士　小林　泰
(74)代理人　100101373
弁理士　竹内　茂雄
(74)代理人　100118902
弁理士　山本　修

最終頁に続く

(54)【発明の名称】安全なリソースへのアプリケーション・アクセスの認可

(57)【特許請求の範囲】
【請求項１】
ドキュメント・レポジトリ・システムにおける安全なリソースへのアクセスを認可するためのコンピューター実装方法であって、
ドキュメント・レポジトリ・システムにおいて安全なリソースに対するアクションを実行するための要求を受けるステップと、
前記要求を受けたことに応じて、前記要求が、ユーザーのみによって、アプリケーションのみによって、またはユーザーを代理するアプリケーションによってなされたかを判定するステップと、
前記要求が前記ユーザーを代理するアプリケーションによってなされたとの判定に応じて、前記アプリケーションおよび前記ユーザーの両方が前記安全なリソースにアクセスするためのパーミッションを有する場合にのみ前記要求を承諾するステップと、
前記要求がアプリケーションのみによってなされたことの判定に応じて、前記アプリケーションが、前記ユーザーを代理しない直接コールによる前記安全なリソースへのアクセスのためのパーミッションを承諾された場合に前記要求を承諾するステップと
についてのコンピューター実装動作を実行するステップを含む、コンピューター実装方法。
【請求項２】
請求項１記載のコンピューター実装方法であって、更に、
前記要求が前記アプリケーションのみによってなされたことの判定に応じて、前記要求

されたアクションの性能を前記アプリケーションのみに対して帰属させるデータを格納するステップを含む、コンピューター実装方法。
【請求項３】
請求項１記載のコンピューター実装方法であって、更に、
前記要求がユーザーを代理するアプリケーションによってなされたことの判定に応じて、前記要求されたアクションの性能を前記アプリケーションおよび前記ユーザーの両方に対して帰属させるデータを格納するステップを含む、コンピューター実装方法。
【請求項４】
請求項１記載のコンピューター実装方法において、前記安全なリソースが、前記ドキュメント・レポジトリ・システムによって維持されるコンテンツ・データベース内のアイテムを含む、コンピューター実装方法
【請求項５】
コンピューター実行可能命令を格納して有するコンピューター可読ストレージ媒体であって、コンピューターによって実行されると、前記コンピューターに、
ユーザーを代理して、ドキュメント・レポジトリ・システムによって維持される１つ以上の安全なリソースにアクセスするためのパーミッションを要求するアプリケーションからパーミッション要求を受け、前記パーミッション要求が、前記ユーザーのみによって、アプリケーションのみによって、または前記ユーザーを代理するアプリケーションによってなされ、
前記パーミッション要求を受けたことに応じて、前記１つ以上の安全なリソースに関連付けられる１つ以上のパーミッション・プロバイダーを識別し、関連する安全なリソースについて要求された前記パーミッションを記述するデータを、識別されたパーミッション・プロバイダーの各々から要求し、前記パーミッション・プロバイダーから受け取った前記データをユーザー・インターフェースにアグリゲートし、前記アプリケーションが前記１つ以上の安全なリソースにアクセスするパーミッションを承諾するために、ドキュメント・リポジトリ・システムの現在のユーザーが十分なパーミッションを有するかを判定し、前記ドキュメント・リポジトリ・システムの現在のユーザーに対し、前記ユーザー・インターフェースに表示させ、
前記アプリケーションおよび前記ユーザーの両方が前記安全なリソースにアクセスするためのパーミッションを有する場合に、前記ユーザーを代理して、前記アプリケーションが前記１つ以上の安全なリソースにアクセスするための前記要求されたパーミッションを承諾されたことを示す指標を、前記ユーザー・インターフェースにより前記ドキュメント・リポジトリ・システムの前記現在のユーザーから受け、前記パーミッション要求がアプリケーションのみによってなされた場合に前記アプリケーションが前記要求されたパーミッションを承諾されたこと、且つ前記アプリケーションが直接コールによる前記安全なリソースへのアクセスのためのパーミッションを承諾されたことを示す指標を受け、
前記アプリケーションが前記要求されたパーミッションを承諾されたことの前記指標を受けたことに応じて、前記安全なリソースについての前記アプリケーションによるランタイム要求を処理するのに用いる前記１つ以上の安全なリソースにアクセスするための前記要求されたパーミッションを前記アプリケーションが有することを示すデータを格納することを行わせる、コンピューター可読ストレージ媒体。
【請求項６】
請求項５記載のコンピューター可読ストレージ媒体であって、更なるコンピューター実行可能命令を格納して有し、前記コンピューターによって実行されると、前記コンピューターに、
前記アプリケーションが前記１つ以上の安全なリソースにアクセスするためのパーミッションを承諾するのに十分なパーミッションを現在のユーザーが有しないと判定するのに応じて、前記パーミッション要求を拒否する
ことを行わせる、コンピューター可読ストレージ媒体。
【請求項７】

請求項５記載のコンピューター可読ストレージ媒体において、前記パーミッション要求が更に、ユーザーを代理しない直接コールにより前記１つ以上の安全なリソースを利用するために、前記アプリケーションによる要求を含む、コンピューター可読ストレージ媒体。

【請求項８】

請求項７記載のコンピューター可読ストレージ媒体であって、更なるコンピューター実行可能命令を格納して有し、前記コンピューターによって実行されると、前記コンピューターに、

直接コールにより前記１つ以上の安全なリソースを利用するためのパーミッションを前記アプリケーションが承諾されたことを示す指標を、前記ユーザー・インターフェースにより前記現在のユーザーから受け、

前記安全なリソースについての前記アプリケーションからのランタイム要求を処理するのに用いるためのデータであって、前記アプリケーションが前記ユーザーを代理しない直接コールにより前記リソースを使用するためのパーミッションを有することを示すデータを格納する

ことを行わせる、コンピューター可読ストレージ媒体。

【請求項９】

前記パーミッション要求が、ハイパーテキスト転送プロトコル（ＨＴＴＰ）要求により、前記ドキュメント・レポジトリ・システムに供給される、請求項５記載のコンピューター可読ストレージ媒体。

【請求項１０】

前記パーミッション要求がアプリケーション・マニフェストにより前記ドキュメント・レポジトリ・システムに供給される、請求項５記載のコンピューター可読ストレージ媒体。

【請求項１１】

前記パーミッション要求が、前記ドキュメント・レポジトリ・システムによって提供されるユーザー・インターフェースにより、前記ドキュメント・レポジトリ・システムに供給される、請求項５記載のコンピューター可読ストレージ媒体。

【請求項１２】

前記パーミッション要求が、前記ドキュメント・レポジトリ・システムによって公表されるアプリケーション・プログラミング・インターフェース（ＡＰＩ）により、前記ドキュメント・レポジトリ・システムに供給される、請求項５記載のコンピューター可読ストレージ媒体。

【請求項１３】

請求項５記載のコンピューター可読ストレージ媒体であって、更なるコンピューター実行可能命令を格納して有し、前記コンピューターによって実行されると、前記コンピューターに、

前記パーミッション・プロバイダーの各々を、前記アプリケーションから前記パーミッション要求を受ける前に、安全なリソースの範囲に関連付けられているものとして登録する

ことを行わせる、コンピューター可読ストレージ媒体。

【請求項１４】

請求項１３記載のコンピューター可読ストレージ媒体において、前記パーミッション・プロバイダーの各々を登録することが更に、リソースに関連づけられる前記パーミッションを記述するデータを取得するために、前記パーミッション・プロバイダーの各々についてのコールバック機能を登録することを含み、要求された前記パーミッションを記述するデータを、識別されたパーミッション・プロバイダーの各々から要求することが、識別されたパーミッション・プロバイダーの各々についての前記コールバック機能へのコールを行うことを含む、コンピューター可読ストレージ媒体。

【請求項１５】

請求項１３記載のコンピューター可読ストレージ媒体において、前記パーミッション・プロバイダーの各々を登録することが更に、パーミッション要求が承諾されたことの通知を供給するために、前記パーミッション・プロバイダーの各々についてのコールバック機能を登録することを含む、コンピューター可読ストレージ媒体。

【請求項１６】

請求項１５記載のコンピューター可読ストレージ媒体であって、更なるコンピューター実行可能命令を格納して有し、前記コンピューターによって実行されると、前記コンピューターに、

前記アプリケーションが前記要求されたパーミッションを承諾されたことを示す指標を前記ユーザー・インターフェースにより現在のユーザーから受けたことに応じて、パーミッション要求が承諾されたことの通知を供給するために前記コールバック機能をコールする

ことを行わせる、コンピューター可読ストレージ媒体。

【請求項１７】

１つ以上のコンピューター・システムを備えるドキュメント・レポジトリ・システムであって、

ユーザーを代理して、ドキュメント・レポジトリ・システムによって維持される１つ以上の安全なリソースにアクセスするためのパーミッションを要求するアプリケーションからパーミッション要求を受け、

前記パーミッション要求を受けたことに応じて、ユーザーが前記パーミッション要求を承諾または拒否することを要求する前記ドキュメント・リポジトリ・システムの前記ユーザーに対して、ユーザー・インターフェースに表示させ、

前記アプリケーションが前記１つ以上の安全なリソースにアクセスするための前記要求されたパーミッションを承諾されたことを示す指標を、前記ユーザー・インターフェースにより前記ユーザーから受け、

前記アプリケーションが前記要求されたパーミッションを承諾されたことの前記指標を受けたことに応じて、前記安全なリソースについての前記アプリケーションによるランタイム要求を処理するのに用いる前記１つ以上の安全なリソースにアクセスするための前記要求されたパーミッションを前記アプリケーションが有することを示すデータを、ストレージ・デバイスを介して格納し、

前記ドキュメント・レポジトリ・システムにおいて安全なリソースに対するアクションを実行するためにランタイム要求を受け、

前記要求を受けたことに応じて、前記要求が、ユーザーにより、アプリケーションにより、またはユーザーを代理するアプリケーションによりなされたかを判定し、

前記要求が前記ユーザーを代理するアプリケーションによりなされたことの判定に応じて、前記アプリケーションおよび前記ユーザーの両方が前記安全なリソースにアクセスするためのパーミッションを有する場合にのみ、前記要求を承諾し、

前記要求が前記アプリケーションのみによりなされたことの判定に応じて、前記ユーザーを代理しない直接コールにより前記安全なリソースにアクセスするためのパーミッションを前記アプリケーションが承諾された場合に、前記要求を承諾する

ように構成される、ドキュメント・レポジトリ・システム。

【請求項１８】

請求項１７記載のドキュメント・レポジトリ・システムにおいて、前記１つ以上のコンピューター・システムが更に、

前記要求がアプリケーションのみによりなされたことの判定に応じて、前記要求されたアクションの性能を前記アプリケーションのみに対して帰属させるデータを格納し、

前記要求が前記ユーザーを代理するアプリケーションのみによりなされたことの判定に応じて、前記要求されたアクションの性能を前記アプリケーションおよび前記ユーザーの両方に対して帰属させるデータを格納する

ように構成される、ドキュメント・レポジトリ・システム。

【発明の詳細な説明】
【従来技術】
【０００１】
数多くのワールド・ワイド・ウェブ（「Ｗｅｂ」）アプリケーションでは、Ｗｅｂアプリケーションの機能を拡張するカスタム・サードパーティ・アプリケーションのインストールおよび使用を許可する。これらサードパーティ・アプリケーションは、通例、パーミッションの観点からＷｅｂアプリケーションの現在のユーザーとして実施する。その結果、このようなサードパーティ・アプリケーションは、現在のユーザーが実行できるであろう如何なるアクションをも、通例、Ｗｅｂアプリケーションに関連付けて実施するアプリケーションについての幾らかの制約された境界において実行可能である。このことは、サードパーティ・アプリケーションをインストールするシステム管理者が当該アプリケーションに重大な信頼を寄せることが義務付けられる。何故ならば、アプリケーションは、如何なるアプリケーションのユーザーがアクセス権を有するWebアプリケーション内の如何なる情報をも、読み出し、修正または削除可能だからである。
【０００２】
上記の課題に対する１つの解決策は、Ｗｅｂアプリケーションにより提供される特定の機能のみに対し、サードパーティ・アプリケーションによるアクセスを制限することである。例えば、サードパーティ・アプリケーションは、当該アプリケーションに公表(expose)されるアプリケーション・プログラミング・インターフェース（「ＡＰＩ」）を制限することによって、Ｗｅｂアプリケーションの特定の機能へのアクセス権のみを承諾することができる。上記課題に対する他のアプローチは、アプリケーションをインストールするシステム管理者によってなされる信頼決定(trust decision)の範囲を制限することである。例えば、Ｗｅｂアプリケーション内の環境を他のものから隔離することができ、その結果、サードパーティ・アプリケーションは、他の環境を破壊する危険性なしに別個の環境にインストールすることができる。この解決策は、例えば、センシティブなデータを公表する環境に対してアプリケーションのアクセス権を制限するのに利用することができる。しかしながら、サードパーティ・アプリケーションを利用する最もありふれた理由の１つが異なる環境にわたるデータをアグリゲートすることであるという所与の事実について、この解決策は過度に制限することになる。その結果、Ｗｅｂアプリケーションの配備にわたる全ての会社環境に適用するアプリケーションは、このシナリオにおいてインストールすることは困難となるか、または不可能となる。
【０００３】
上記のように、サードパーティ・アプリケーションは、通例、パーミッションの観点からＷｅｂアプリケーションの現在のユーザーとして実施する。このことは、アプリケーションが、それらユーザーが実行のためのパーミッションを有するアクションを実行することができるとすることのみを意味する。しかしながら、多くの状況では、ユーザーまたはユーザーのグループに、アプリケーションの使用を通じて、彼らのパーミッションが直接実行することを彼らに許可しないというアクションを実行させることが望ましい。例えば、支出レポート・アプリケーションは、特定の条件が満たされる（例えば小さい値）ときに支出レポートを承認することができるものの、ユーザーは、アプリケーションを通じて動作を行うことなく直接的に支出レポートを承認するパーミッションを有するべきではない。この種別の動作は、アプリケーションが現在のユーザーとして実施する場合は可能にならない。システムの中には、当該システム内でパーミッション制約を有しないシステム・アカウントに対するパーミッションを引き上げるのをアプリケーションが許可することにより、この制限に対処するものもある。しかしながら、この解決策は、システム管理者が、センシティブな情報を公表する環境内にアプリケーションをインストールするのを尚更望まないものとすることもある。
【０００４】
本明細書でなされる開示が提示されるのは、これらのおよび他の検討に関するものである。

【発明の概要】
【発明が解決しようとする課題】
【０００５】
アプリケーションが安全なリソースに対するアクセスを認可するための概念および技術を本明細書に説明する。本明細書において開示される技術の実施を通じて、安全なリソースの所有者は、安全なリソースを利用するために、アプリケーションに対して特権を承諾することができる。承諾された特権を利用して、アプリケーションは、リソースの所有者と同程度に、実行時において安全なリソースを直接（即ちユーザーなしで）利用することができる。しかしながら、ユーザーが安全なリソースにアクセスするためにアプリケーションを利用する場合は、リソースの使用はユーザーの特権程度にまで制限される。このようにして、アプリケーションが安全なリソースに直接アクセスするときに、アプリケーションの特権を安全なリソースの所有者レベルまで引き上げることができる。しかし、ユーザーがアプリケーションを利用してリソースにアクセスする場合は、安全なリソースへのアクセスは、ユーザーのパーミッションの程度にまで制限される。
【課題を解決するための手段】
【０００６】
本明細書において提示される一態様によれば、ドキュメント・レポジトリ・アプリケーションのようなＷｅｂアプリケーションは、当該Ｗｅｂアプリケーションの性能を拡張するカスタム・サードパーティ・アプリケーションを使用可能とするように構成される。コンテンツ・データベース内のアイテムのような、Ｗｅｂアプリケーションによって管理される安全なリソースに対するアクセスおよび利用するパーミッションを取得するために、アプリケーションは、最初に、Ｗｅｂアプリケーションの一部として実行するリソース・サーバーに対してパーミッション要求をサブミットする。パーミッション要求は、アプリケーションによって要求される範囲および権利を識別する。パーミッション要求はまた、アプリケーションがユーザーを代理せず直接コールすることより、１つ以上の安全なリソースを利用するためのパーミッションを承諾することもできる。パーミッション要求は、ハイパー・テキスト転送プロトコル（「ＨＴＴＰ」）要求、アプリケーション・マニフェスト、または、Ｗｅｂアプリケーションによって提供され、Ｗｅｂアプリケーションによって提供されるＡＰＩを通じた、若しくは他の方法による、ユーザー・インターフェース（「ＵＩ」）によってサブミットすることができる。
【０００７】
パーミッション要求を受けたことに応じて、リソース・サーバーは、パーミッションが要求された安全なリソースに関連付けられた１つ以上のパーミッション・プロバイダーを識別するように構成される。リソース・サーバーは、次いで、関連付けられた安全なリソースについて要求されたパーミッションを記述するデータを、各識別されたパーミッション・プロバイダーから要求する。データは、次いで、Ｗｅｂアプリケーションの現在のユーザーに表示されるＵＩにアグリゲートされる。このＵＩは、要求されたパーミッションをアプリケーションに承諾するかまたは拒否するかについて、ユーザーに尋ねる。要求されたパーミッションをユーザーがアプリケーションに承諾する場合は、アプリケーションは当該要求されたパーミッションを有することを示すデータを格納する。実行時には、このデータを利用して、Ｗｅｂアプリケーションによって管理される安全なリソースに対する、アプリケーションによってランタイム要求を処理する。
【０００８】
安全なリソースに対するアクションを実行するランタイム要求をリソース・サーバーから受け取ると、リソース・サーバーは、その要求が、ユーザーによってなされたものか、アプリケーションのみによってなされたものか、またはユーザーを代理するアプリケーションによってなされたものかについて判定する。要求がアプリケーションのみによってなされる場合は、リソース・サーバーは、ユーザーを代理せずに直接コールによって安全なリソースにアクセスするために、アプリケーションが上記の方法でパーミッションが承諾されたときのみ上記要求を承諾する。要求がユーザーを代理するアプリケーションによっ

てなされる場合は、リソース・サーバーは、ユーザーおよびアプリケーションの両方が要求されたアクションを実行するパーミッションを有しているときのみ、上記要求を承諾する。リソース・サーバーはまた、安全なリソースに対するアクションの性能を、ユーザー、アプリケーション、またはユーザーとアプリケーションの両方に対して帰属させる履歴データを格納する。

【０００９】

この摘要は特許請求する主題の主要な特徴や必須の特徴を特定することを意図するものではなく、また、この摘要は特許請求する主題の範囲を限定するのに用いることを意図するものでもない。更にまた、特許請求する主題は、この開示の如何なる部分で注記した不利な点の幾らかまたは全てを解決する実施態様に限定されるものではない。

【図面の簡単な説明】

【００１０】

【図１】図１は、本明細書に開示する一実施形態により、アプリケーションおよびドキュメント・レポジトリ・システムの動作態様を例示するソフトウェア・アーキテクチャーの概要図である。

【図２】図２は、本明細書に開示する一実施形態のパーミッション・プロバイダーを登録する１つのルーチンの態様について示すフロー図である。

【図３Ａ】図３Aは、本明細書に開示する一実施形態において、リソース・サーバーにアプリケーションを登録する１つのルーチンの態様について示すフロー図である。

【図３Ｂ】図３Bは、本明細書に開示する一実施形態において、リソース・サーバーにアプリケーションを登録する１つのルーチンの態様について示すフロー図である。

【図４Ａ】図４Ａは、本願明細書に開示する一実施形態において利用される例示のパーミッション要求のフォーマットおよび構造について示すデータ構造図である。

【図４Ｂ】図４Ｂは、本明細書に開示する一実施形態において、アプリケーションへのパーミッションを承諾する１つの例示的なユーザー・インターフェースについて示すユーザー・インターフェース図である。

【図５】図５は、リソース要求を処理するために本明細書に開示する一実施形態において利用される機構の態様について示すネットワーク図である。

【図６Ａ】図６Ａは、一実施形態による安全なリソースについての要求を処理するための１つのルーチンの態様について示すフロー図である。

【図６Ｂ】図６Ｂは、一実施形態による安全なリソースについての要求を処理するための１つのルーチンの態様について示すフローズである。

【図７】図７は、本明細書に開示する各種実施形態を実施できるコンピューター・システムの例示のコンピューター・ハードウェアおよびソフトウェア・アーキテクチャーについて示すコンピューター・アーキテクチャー図である。

【発明を実施するための形態】

【００１１】

以下の詳細な説明は、安全なリソースへのアプリケーションのアクセスを認可するための概念および技術に向けられる。本明細書に開示した技術を用いて上記に簡潔に説明したように、Ｗｅｂアプリケーションと連動して実行するアプリケーションは、実行時に、安全なリソースをリソースの所有者と同程度に直接利用することができる。安全なリソースを利用するためにユーザーがアプリケーションをしようする際、ユーザーおよびアプリケーションの両方は、当該安全なリソースを利用するために適切なパーミッションを有していなければならない。これらおよび他の特徴に関する追加の詳細説明について、図１～７に関して以下に提供する。

【００１２】

本明細書に説明する主題が、１つ以上のコンピューター・システム上のオペレーティング・システムおよび様々なプログラムの実行と連動して実行するコンピューター・モジュールの包括的なコンテキストで提示されると共に、当業者にとって、他の実施が、他の種別のプログラム・モジュールと連動して実行できることが認識されるであろう。一般的に

、プログラム・モジュールは、ルーチン、プログラム、コンポーネント、データ構造、および、特定のタスクを実行するかまたは特定の抽象データ型を実装する他のタイプの構造を含む。更に、当業者にとって、本明細書に説明する主題が、ハンドヘルド・デバイス、マルチプロセッサ・システム、マイクロプロセッサ・ベースまたはプログラム可能なコンシューマー電子機器、ミニコンピュータ、メインフレーム・コンピュータ等を含む他のコンピューター・システム構成を用いて実施できることが認められて然るべきである。

【００１３】

以下の詳細な説明において、その一部を形成する添付の図面を参照して、特定の実施形態または実施例について図示により示す。これより図面を参照する。同様の符号は幾らかの図面を通じた同様の要素を表し、安全なリソースへのアプリケーション・アクセスを認可するためのコンピューティング・システムおよび方法論の態様についてこれより説明する。

【００１４】

図１は、本明細書に開示する一実施形態におけるアプリケーション１０４およびドキュメント・レポジトリ・システム１０２の動作についての態様を例示するソフトウェア・アーキクチャー図である。ドキュメント・レポジトリ・システム１０２は、１つ以上のコンピューティング・システムであり、Ｗｅｂベースのドキュメント・レポジトリ・アプリケーション（図示せず）を実行するように構成される。ドキュメント・レポジトリ・システム１０２は、ドキュメント、および当該ドキュメント・レポジトリ・システム１０２において認可されたユーザー間での潜在的な他の種別のアイテムを格納、アクセスおよび共有するための機能を提供する。この点について、ドキュメント・レポジトリ・システム１０２は、ユーザーが、ドキュメントおよびコンテンツ・データ・ストア１２６内に格納される他の種別の電子的なアイテムを生成、修正、削除、およびさもなければ利用を可能にする機能を提供することができる。

【００１５】

ドキュメント・レポジトリ・システム１０２は、パーミッションに基づいてコンテンツ／データ・ストア１２６内のアイテムへのアクセスを制限することができる。パーミッションは、ドキュメント・レポジトリ・システム１０２のユーザーに対してセットすることができ、その結果、特定のユーザーのみがコンテンツ・データ・ストア１２６内の特定のアイテムにアクセスまたは修正できる。コンテンツ・データ・ストア１２６に格納されるアイテムは上記の方法によるパーミッションを用いて安全なものとされるので、これらのアイテムは、本明細書では、安全なリソース１２２Ａ～１２２Ｎ（総じて安全なリソース１２２）と称する。

【００１６】

なお、安全なリソース１２２が、主に、コンテンツ・データ・ストア１２６内のアイテムとして本明細書に説明される一方で、安全なリソース１２２は、アクセスがパーミッションに基づいて制御される如何なる種別の他のコンピューティング・リソースとしてもよいことが認められて然るべきである。また、本明細書に開示する実施形態は、主に、ドキュメント・レポジトリ・システム１０２のコンテキストで説明する一方で、本明細書に開示する実施形態はこのような実施に限定されないことが認められて然るべきである。寧ろ、本明細書に開示する実施形態は、アプリケーションが安全なリソースにアクセスするのを許可する如何なる種別のコンピューティング・システムをも用いて利用することができる。

【００１７】

一実施形態では、ドキュメント・レポジトリ・システム１０２は、安全なリソース１２２へのアクセスを制御するためのリソース・サーバー１１４を含む。リソース・サーバー１１４は、安全なリソース１２２にアクセスするために要求を受けて応じるように構成される１つ以上のソフトウェアおよび／またはハードウェア・コンポーネントである。リソース・サーバー１１４はまた、安全なリソース１２２を利用するために、アプリケーション１０４のようなアプリケーションを登録するための機能を提供する。

【００１８】
アプリケーション１０４は、ドキュメント・レポジトリ・システム１０２と共に使用するように構成されるアプリケーションである。例えば、アプリケーション１０４は、ドキュメント・レポジトリ・システム１０２により提供される機能を拡張することができる。アプリケーション１０４は、Ｗｅｂベースのアプリケーションとしてもよく、またはドキュメント・レポジトリ・システム１０２に対して直接実行してもよい。所望の機能を提供するために、アプリケーション１０４は、通例、安全なリソース１２２の内１つ以上を利用する。アプリケーション１０４、本明細書では主に、ドキュメント・レポジトリ・システム１０２により提供される機能を拡張するためのアプリケーションとして説明する一方、本明細書で利用する実施形態は、他の種別のアプリケーションと共に実施してもよい。
【００１９】
安全なリソース１２２を利用する認可を得るために、アプリケーション１０４は、一実施形態ではパーミッション要求をリソース・サーバー１１４に供給する。パーミッション要求１０６は、アプリケーション１０４によって要求されるアクセスの範囲１０８、および特定された範囲についての要求されたパーミッションを定める権利１１０を定義するデータである。パーミッション要求１０６はまた、「アプリケーションのみ」の要求１１２も含む。「アプリケーションのみ」の要求１１２は、アプリケーション１０４がユーザーを代理していない直接コールを行うことにより１つ以上の安全なリソース１２２を利用するためのパーミッションを承諾することを要求する。アプリケーション１０４は、ハイパーテキスト転送プロトコル（「ＨＴＴＰ」）要求、アプリケーション・マニフェスト１２４、ドキュメント・レポジトリ・システム１０２により提供されるＡＰＩを通じてドキュメント・レポジトリ・システム１０２によって提供されるユーザー・インタフェース（「ＵＩ」）によって、または他の方法で、パーミッション要求１０６をサブミットすることができる。パーミッション要求１０６の１つについては、図４Ａに関連して以降に説明する。
【００２０】
アプリケーション１０４からパーミッション要求１０６を受けるのに応じて、リソース・サーバー１１４は、１つ以上のパーミッション・プロバイダー１１６Ａ～１１６Ｎ（パーミッション・プロバイダー１１６と総称する。）を識別する。パーミッション・プロバイダー１１６は、安全なリソース１２２Ａ～１２２Ｎについてのパーミッションのプロバイダーとしてそれぞれ登録される。図１に示した例では、例えば、パーミッション・プロバイダー１１６Ａは安全なリソース１２２Ａについてのパーミッションのプロバイダーとして登録される。パーミッション要求１０６の範囲１０８として安全なリソース１２２Ａを含む場合は、リソース・サーバー１１４は、パーミッション・プロバイダー１１６Ａを、パーミッション要求１０６についての関連パーミッション・プロバイダーとして識別することになる。
【００２１】
リソース・サーバー１１４に登録するために、各パーミッション・プロバイダー１１６は、当該パーミッション・プロバイダーが関連付けられたリソースの範囲をリソース・サーバー１１４に示す。各パーミッション・プロバイダー１１６はまた、リソース・サーバー１１４を有するコールバック機能を登録することもある。例えば、各パーミッション・プロバイダー１１６は、リソース・サーバー１１４が有するコールバック機能を登録することができ、それを通じて、リソース・サーバー１１４は安全なリソース１２２に関連付けられたパーミッションを記述するデータを取得することができる。以下に詳述するように、リソース・サーバー１１４は、このデータを利用して、パーミッション要求１０６においてアプリケーション１０４によって要求されるパーミッションをユーザーに示すＵＩを構成するために、このデータを利用することができる。
【００２２】
各パーミッション・プロバイダー１１６はまた、コールバック機能を登録することができ、これを通じて、リソース・サーバー１１４はパーミッション要求１０６が承諾された

ことの通知を供給することができる。リソース・サーバー１１４は、パーミッション・プロバイダーのデータ・ストア１１８内に、コールバック機能を識別するデータを含む登録データを格納する。パーミッション・プロバイダー１１６を登録する１つのプロセスに関する追加の詳細説明について、以下に図２に関連して行う。

【００２３】

リソース・サーバー１１４は、一旦、パーミッション要求１０６に関連したパーミッション・プロバイダー１１６を識別すると、リソース・サーバー１１４は、要求されたそのパーミッションを記述するデータを取得するために各識別したプロバイダー１１６のコールバック機能をコールする。リソース・サーバー１１４は、パーミッション要求１０６の範囲１０８および権利１１０を、現在のユーザーを識別する現在のコンテキストと共に、識別したパーミッション・プロバイダー１１６に通すことができる。次に、コールされた各プロバイダー１１６は、現在のユーザーが、パーミッション要求１０６において要求されたアプリケーション１０４ひぇのパーミッションを承諾するのに十分な特権を有するかを判定する。

【００２４】

ユーザーがアプリケーション１０４に対する要求されたパーミッションを承諾するのに十分な特権を有していない場合は、パーミッション要求１０６は拒否されることになる。要求されたパーミッションをアプリケーション１０４に付与する十分な特権をユーザーが有する場合は、各パーミッション・プロバイダー１１６はデータをリソース・サーバーに戻すことになる。データは、アプリケーション１０４によって要求されたパーミッションをユーザーに示すＵＩを構成するのに利用できる。このデータは、ハイパーテキスト・マークアップ言語（「ＨＴＭＬ」）、プレーン・テキスト、またはダイアログ・ボックスのようなＵＩ要素に直接含むのに適した他のフォーマットの形態としてもよい。

【００２５】

リソース・サーバー１１４は、一旦、識別したパーミッション・プロバイダー１１６から応答を受け取ると、リソース・サーバー１１４は、受け取ったデータを現在のユーザーに表示するＵＩにアグリゲートする。ＵＩは、要求されたパーミッションについての説明を記載し、そして、パーミッション要求１０６においてアプリケーション１０４によって要求される許可を承諾または否定するかをユーザーに尋ねる。このような例示のＵＩの１つについて、図４Ｂに関連して後述する。ユーザーが、ＵＩを通じてアプリケーション１０４に対する要求されたパーミッションを承諾する場合は、リソース・サーバー１１４はパーミッション・データ・ストア１２０にアプリケーション１０４がパーミッションを要求したことを示すデータを格納する。実行時において、リソース・サーバー１１４は、このデータを利用して、アプリケーション１０４による要求を処理し、その結果、安全なリソース１２２へのアクションを実行することができる。リソース・サーバー１１４によって実行されるランタイム処理に関する追加の詳細説明について、以下に図５および図６Ａ～６Ｂに関連して行う。

【００２６】

図２は、本明細書に関する実施形態のパーミッション・プロバイダー１１６を登録する１つのルーチン２００の態様について示すフロー図である。図２および他の図面に関連して本明細書に説明する論理動作は、（１）コンピューティング・システム上で起動するコンピューター実装行為またはプログラム・モジュールのシーケンスとして、および／または（２）コンピューティング・システム内で相互接続されたマシン・ロジック回路若しくは回路モジュールとして実装されることが認められて然るべきである。実装は、コンピューター・システムの性能および他の要件に従った選択の問題である。したがって、本明細書において説明する論理動作とは、動作、構造デバイス、行為またはモジュールのような様々なものを指す。これらの動作、構造デバイス、行為およびモジュールは、ソフトウェア、ファームウェア、特定用途デジタル論理、およびそれらの如何なる組み合わせで実装することができる。また、図示され、本明細書に説明されるものよりも、より多くのまたはより少ない動作を実行できることも認められて然るべきである。これらの動作はまた、

本明細書において説明するものとは異なる順序で実行することができる。

【００２７】

ルーチン２００は、動作２０２で開始し、パーミッション・プロバイダー１１６は、当該パーミッション・プロバイダーが登録されるべき安全なリソースの範囲についての指標をリソース・サーバー１１４に供給する。ルーチン２００は、次いで動作２０４へと進み、パーミッション・プロバイダー１１６は、コールバック機能をリソース・サーバー１１４に提供する。当該リソース・サーバー１１４を通じて、要求されたパーミッションを記述するデータを取得することができる。先に簡潔に検討したように、リソース・サーバー１１４は、この情報を利用して、ユーザーがパーミッション要求１０６を承認または拒否することを要求するＵＩを生成することができる。

【００２８】

ルーチン２００は、動作２０４から動作２０６へと進み、パーミッション・プロバイダー１１６はリソース・サーバー１１４にコールバック機能を提供する。リソース・サーバー１１４は、パーミッション要求１０６が承諾されたことをパーミッション・プロバイダー１１６に通知するのに用いることができる。なお、動作２０２，２０４，２０６において供給される情報は１または複数のデータ構造として供給できることが認められて然るべきである。この情報はまた、拡張可能マークアップ言語（「ＸＭＬ」）を用いて、別の構造化された言語フォーマットを用いて、または概して別の方法を用いて、フォーマットしてもよい。

【００２９】

動作２０６から、ルーチン２００は動作２０８へと進み、リソース・サーバー１１４は、パーミッション・プロバイダー１１６によって識別される範囲およびコールバック機能をパーミッション・プロバイダーのデータ・ストア１１８内に格納する。データが一旦格納されると、ルーチン２００は動作２０８から動作２１０へと進み、終了する。

【００３０】

図３Ａ～３Ｂは、本明細書で開示する一実施形態において、リソース・サーバーにアプリケーションを登録する１つのルーチン３００の態様について示すフロー図である。ルーチン３００は、リソース・サーバー１１４がパーミッション要求１０６を受ける動作から開始する。ルーチン３００は、次いで動作３０４へと進み、リソース・サーバー１１４は、パーミッション要求１０６に記載されるパーミッションの範囲１０８に関連付けられたパーミッション・プロバイダー１１６を識別する。例えば、リソース・サーバー１１４は、範囲１０８に関連付けられたパーミッション・プロバイダー１１６を識別するために、パーミッション・プロバイダーのデータ・ストア１１８に格納された情報を通じてイテレートしてもよい。一旦パーミッション・プロバイダー１１６が識別されると、ルーチン３００は動作３０４から動作３０６へと進む。

【００３１】

動作３０６において、リソース・サーバー１１４は、要求された範囲１０８、権利１１０、アプリケーションのみの要求１１２、もしあれば、現在のコンテキストをパーミッションの要求元である、登録されたパーミッション・プロバイダー１１６の各々に通す。この情報を受け取ることに応じて、各パーミッション・プロバイダー１１６は、現在のユーザーが、要求されたパーミッションを承諾するのに十分な権威(authority)を有するかどうかを判定する。このことは、例えば、現在のユーザーによって保持される特権を示す、パーミッション・データ・ストア内に格納されたデータを参照することによって達成できる。アプリケーション１０４への要求されたパーミッションをユーザーが承諾することができない場合は、ルーチン３００は、動作３１０から動作１２へと進み、パーミッション要求１０６は拒否される。加えて、ＵＩは、パーミッションが承諾できないことを示して、ユーザーに提示することができる。ルーチン３００は、次いで、動作３１２から動作３１４へと進み、終了する。

【００３２】

ユーザーがパーミッション要求１０６を承諾するのに十分な特権を所有する場合は、ル

ーチン３００は動作３１０から（図３Ｂに示す）動作３１６へと進む。動作３１６では、リソース・サーバー１１４は、識別されたパーミッション・プロバイダー１１６の各々が有するコールバック機能をコールして、各パーミッション・プロバイダー１１６について要求されたパーミッションを記述したデータを取得する。次に、コールされたパーミッション・プロバイダー１１６の各々は、要求された情報をリソース・サーバー１１４に供給する。ルーチン３００は、次いで、動作３１６から動作３１８へと進む。

【００３３】

動作３１８では、リソース・サーバー１１４は、パーミッション・プロバイダー１１６から受け取ったデータをＵＩにアグリゲートし、該ＵＩを現在のユーザーに提示する。先に述べたように、このＵＩはまた、パーミッション要求１０６に記載されるアプリケーション１０４に対する特権の付与を承認または拒否することをユーザーに尋ねる。そのような１つのＵＩについて、図４Ｂに関連して後に説明する。

【００３４】

ユーザーがアプリケーション１０４への特権の承諾を拒否する場合は、ルーチン３００は動作３２０から動作３２２へと進む。動作３２２では、パーミッション要求１０６が拒否される。加えて、ＵＩをユーザーに提示して、要求されたパーミッションを承諾できないことを示してもよい。ルーチン３００は、次いで動作３２２から動作３２８へと進み、終了する。

【００３５】

ユーザーがパーミッション要求１０６を承認する場合は、ルーチン３００は動作３２０から動作３２４へと進む。動作３２４では、リソース・サーバーは、パーミッション要求１０６が承諾されたことを示すために、識別されたパーミッション・プロバイダー１１６の各々によって公表されるコールバック機能をコールする。ルーチン３００は、次いで、動作３２６へ進み、アプリケーション１０４への要求されたパーミッションの承諾を示すデータをパーミッション・データ・ストアに格納する。先に述べたように、このデータは、実行時に利用されて、アプリケーション１０４から受け取る安全なリソース１２２の要求が承認または拒否されるべきかについて判定する。ルーチン３００は、動作３２６からどうさ３２８へと進み、終了する。

【００３６】

図４Ａは、本明細書に開示する一実施形態において利用される例示のパーミッション要求１０６のフォーマットおよび構造について示したデータ構造図である。特に、図４Ａに示したパーミッション要求１０６の例では、アプリケーション１０４は、４つの異なる安全なリソースへのパーミッションを要求している。従って、パーミッション要求１０６は、各リソースに対応するＸＭＬ要素を含む。特に、１つの要素はドキュメント・ライブラリへの特権の要求に対応し、１つの要素はユーザー・プロファイル・ストアへの特権の要求に対応し、１つの要素はカレンダーへの特権の要求に対応し、そして、他の１つの要素はコンタクトへの特権の要求に対応する。

【００３７】

特権が要求される安全なリソース毎に、パーミッション要求１０６は要求された権利も特定する。例えば、図４Ａに示されるパーミッション要求１０６は、コンタクトを読み出す、カレンダーを読み出す、およびドキュメント・ライブラリに書き込むための権利を要求する。なお、他のタイプの権利がまた要求されてもよいことが認められて然るべきである。また、図４Ａに示されるパーミッション要求がＸＭＬを利用して表現される一方、他の構造化されたまたは構造化されていない言語についても利用できることが理解されて然るべきである。他の要素、構成、およびデータの配置はまた、範囲１０８、権利１１０、アプリケーションのみの要求１１２，および如何なる他の要素のパーミッション要求１０６をも利用することもできる。

【００３８】

図４Ｂは、本明細書で開示する一実施形態における、アプリケーション１０４に対するパーミッションを承諾する１つの例示のユーザー・インターフェース４００について示す

ユーザー・インターフェース図である。先に検討したように、リソース・サーバー１１４は、パーミッション要求１０６の受け取りに続いて、ユーザー・インターフェース４００を生成する。図４Ｂに示すＵＩ４００は、図４Ａに示すパーミッション要求１０６に基づいて生成される。

【００３９】

ユーザー・インターフェース４００は、アプリケーションが安全なリソース１２２へのアクセスを要求したユーザーへの説明を行うテキストを含む。ユーザー・インターフェース４００はまた、パーミッション要求１０６においてアプリケーション１０４によって要求される様々なパーミッションについて記述するテキストを含む。先に検討したように、この情報は、コールバック機能によってパーミッション要求１０６に記載した範囲１０８に関連付けられるパーミッション・プロバイダー１１６から取得することができる。パーミッション・プロバイダー１１６から受ける情報は、一実施形態では、フィールド４０２Ａ～４０２Ｄ内に表示される。

【００４０】

図４Ｂに示した例では、例えば、要求されたパーミッションを記述するドキュメント・ライブラリについてパーミッション・プロバイダー１１６から受けたデータを、フィールド４０２Ａに表示するのがよい。ユーザー・プロファイルについてパーミッション・プロバイダー１１６から受けたデータは、フィールド４０２Ｂに表示するのがよい。要求されたパーミッションを記述するカレンダーについてパーミッション・プロバイダー１１６から受けたデータは、フィールド４０２Ｃに表示するのがよい。コンタクトについてパーミッション・プロバイダー１１６から受けたデータは、フィールド４０２Ｄに表示するのがよい。現在のユーザーは、ＵＩ制御４０４Ｂを選択して、要求された特権を承諾することができる。代替として、ユーザーは、ＵＩ制御４０４Ａを選択して、パーミッション要求１０６を拒否することができる。

【００４１】

なお、図４Ｂに示したユーザー・インターフェースは単に例示のものであり、より多くのおよび少ないデータを提示してもよいことが認められて然るべきである。例えば、アプリケーションのみの要求１１２がなされたことを示すフィールドを含む付加フィールド４０２を提示してもよい。加えて、提示されるデータは、図４Ｂに示したものとは異なる方法で、または異なるＵＩ制御を利用して提示してもよい。当業者にとって、他の変更態様が明らかであろう。

【００４２】

図５は、実行時においてリソース要求を処理するために、本明細書に開示する一実施形態で利用される機構の態様について示すネットワーク概要図である。図５に示す例では、ユーザー５０２およびアプリケーション１０４は、リソース・サーバー１１４に安全なリソースについての要求（「リソース要求５０４」）を開始することができる。特に、ユーザー５０２は、アプリケーション１０４を用いることなく、ドキュメント・レポジトリ・システム１０２を通じて直接的に安全なリソース１２２Ａのリソース要求５０４Ａを生成することができる。同様に、アプリケーション１０４は、直接的に且つユーザー５０２を代理せずに、安全なリソース１２２Ａについてのリソース要求５０４Ｃを生成することができる。加えて、ユーザー５０２は、アプリケーション１０４を利用して、アプリケーション１０４およびユーザー５０２によってなされたリソース要求５０４Ｂを生成することができる。

【００４３】

リソース要求５０４が、ユーザー５０２のみによって、アプリケーション１０４のみによって、またはユーザー５０２に代理してアプリケーション１０４によってなされたかを判定するために、適切な認可メカニズムを利用することができる。このような機構を通じて、リソース要求５０４Ａがユーザー５０２のみによってなされたときに、ユーザー識別５０６Ａがリソース・サーバー１１４に提示される。アプリケーション識別５０６Ｃは、リソース要求５０４Ｃがアプリケーション１０４のみによってなされたときに、リソース

・サーバー１１４に提示される。同様に、アプリケーションおよびユーザー識別５０６Ｂは、リソース要求５０４Ｂがユーザー５０２を代理してアプリケーション１０４によってなされたときに、リソース・サーバー１１４に提示される。適切なプロトコルは、リソース要求５０４がなされたときに、識別５０６をリソース・サーバー１１４に提示するのに利用することができる。他の機構がまた、ユーザー５０２およびアプリケーション１０４を認証するために、また、リソース要求５０４がユーザー５０２のみによって、アプリケーション１０４のみによって、またはユーザー５０２を代理してアプリケーション１０４によってなされたときに、リソース・サーバー１１４に示すために利用することもできる。

【００４４】

リソース要求５０４を受け取ることに応じて、リソース・サーバー１１４は、リソース要求５０４がユーザー５０２によって、アプリケーション１０４のみによって、または、ユーザー５０２を代理してアプリケーション１０４によってなされたかを判定する。リソース・サーバー１１４は、次いで、パーミッション・データ・ストア１２０からデータを抽出して、リソース要求５０４を承諾できるか、または拒否すべきかについて判定する。リソース要求５０４がアプリケーション１０４のみによってなされた場合は、リソース・サーバー１１４は、上記の方法でユーザーを代理しない直接コールによる安全なリソースへのアクセスするためのパーミッションをアプリケーション１０４が承諾したときのみ、要求５０４を承諾する。リソース要求５０４がユーザー５０２を代理したアプリケーション１０４によってなされた場合は、リソース・サーバー１１４は、ユーザー５０２およびアプリケーション１０４の両方が、要求された動作を実行するパーミッションを有するときのみ、要求５０４を承諾する。リソース・サーバー１１４はまた、データを履歴データ・ストア５０８に格納することもでき、安全なリソース１２２へのアクションの性能を、ユーザー５０２に、アプリケーション１０４に、またはユーザー５０２およびアプリケーション１０４の両方に、適切に帰属させる。これらプロセスに関する付加的な詳細説明について、図６Ａ～６Ｂに関連して以下に行う。

【００４５】

図６Ａ～６Ｂは、一実施形態による、安全なリソース１２２についてのランタイム要求５０４を処理するための１つのルーチン６００の態様について示すフロー図である。ルーチン６００は動作６０２で開始し、リソース・サーバー１１４はリソース要求５０４を受け取る。リソース要求５０４の受け取りに応じてルーチン６００は動作６０４へと進み、リソース・サーバー１１４は、受け取った要求５０４がユーザー５０２のみを代理してなされたものかについて判定する。要求５０４がユーザー５０２のみを代理してなされた場合は、ルーチン６００は動作６０４から動作６１０へと進む。

【００４６】

動作６１０では、リソース・サーバー１１４は、その要求を行ったユーザー５０２が、受け取ったリソース要求において要求されたアクションを実行するための十分な特権を有するかについて判定する。ユーザー５０２が充分な特権を有しない場合は、ルーチン６００は動作６１２から動作６１４へと進み、受け取ったリソース要求５０４は拒否される。ルーチン６００は、次いで、動作６１４から動作６２０へと進み、終了する。

【００４７】

ユーザー５０２が充分な特権を有する場合は、ルーチン６００は動作６１２から動作６１６へと進み、受け取ったリソース要求５０４で要求される動作が実行される。例えば、読み出し動作、書き込み動作、または他の如何なる種別の動作が、安全なリソース１２２上で実行されるのがよい。一旦アクションを完了すると、ルーチン６００は動作６１８へと進み、リソース・サーバー１１４は、データを履歴データ・ストア５０８に格納して、実行したアクションをユーザー５０２に帰属させる。例えば、データは、ユーザー５０２が安全なリソース１２２への書き込み動作を実行したことを示すデータを格納することができる。ルーチン６００は、動作６１８から動作６２０へと進み、終了する。

【００４８】

動作６０４において、リソース・サーバー１１４は、受け取ったリソース要求５０４がユーザー５０２のみによりなされなかったと判定する場合は、ルーチン６００は動作６０６へと進む。動作６０６において、リソース・サーバー１１４は、受け取ったリソース要求５０４がユーザー５０２を代理してアプリケーション１４０によりなされたかどうかを判定する。受け取ったリソース要求５０４が、ユーザー５０２を代理してアプリケーション１４０によってなされた場合は、ルーチン６００は動作６０６から動作６２２へと進む。

【００４９】

動作６２２では、リソース・サーバー１１４は、パーミッション・データ・ストア１２０を利用して、アプリケーション１０４およびユーザー５０２が、受け取ったリソース要求５０４において要求されたアクションを実行するのに充分な特権があるかどうかを判定する。アプリケーション１０４またはユーザー５０２が充分な特権は有しない場合は、ルーチン６００は動作６２４から動作６１４へと進み、受け取ったリソース要求５０４は否定される。ルーチン５００は、次いで、動作６１４から動作６２０へと進み、終了する。

【００５０】

アプリケーション１０４およびユーザー５０２が充分な特権を有する場合は、ルーチン６００は動作６２４から動作６２６へと進み、受け取ったリソース要求５０４において要求されたアクションが実行される。一旦アクションを完了すると、ルーチン６００は動作６２８へと進み、リソース・サーバー１１４は、データを履歴データ・ストア５０８に格納して、実行したアクションをアプリケーション１０４およびユーザー５０２の両方に帰属させる。例えば、アプリケーション１０４が、ユーザー５０２を代理して、安全なリソース１２２に対する削除動作を実行したことを示すデータを格納することができる。ルーチン６００は動作６２８から動作６２０へと進み、終了する。

【００５１】

動作６０６において、リソース・サーバー１１４が、受け取ったリソース要求がユーザ５０２およびアプリケーション１０４の両方を代理してなされなかったと判定する場合は、ルーチン６００は動作６０６から動作６０８へと進む。動作６０８において、リソース・サーバー１１４は、受け取ったリソース要求５０４がアプリケーション１０４のみを代理してなされたかを判定する。受け取ったリソース要求５０４がアプリケーション１０４のみを代理してなされなかった場合は、ルーチン６００は、動作６０８から動作６１４へ進み、受け取ったリソース要求５０４を拒否する。ルーチン６００は、次いで、動作６１４から動作６２０へ進み、終了する。

【００５２】

リソース・サーバー１１４は、受け取ったリソース要求５０４がアプリケーション１０４だけを代理してなされたと判定する場合は、ルーチン６００は動作６０８から（図６Ｂに示す）動作６３０へと進む。動作６３０では、アプリケーション１０４が、受け取ったリソース要求５０４において要求されたアクションを実行するのに充分な特権を有するかを判定するために、リソース・サーバー１１４はパーミッション・データ・ストア１２０を利用する。アプリケーション１０４が充分な特権を有しない場合は、ルーチン６００は動作６３２から動作６３４へと進み、受け取ったリソース要求が否定される。ルーチン６００は、次いで、動作６３４から動作６４０へと進み、終了する。

【００５３】

アプリケーション１０４が充分な特権を有する場合は、ルーチン６００は動作６３２から動作６３６へと進み、受け取ったリソース要求５０４において要求されたアクションが実行される。一旦アクションが完了すると、ルーチン６００は動作６３８へと進み、リソース・サーバーは、データを履歴データ・ストア５０８に格納して、実行したアクションをアプリケーション１０４のみに帰属させる。ルーチン６００は、動作６３８から動作６４０へと進み、終了する。

【００５４】

図７は、本明細書に示した各種実施形態を実施することができるコンピューター・シス

テムのための例示のコンピューター・ハードウェアおよびソフトウェア・アーキテクチャーについて示すコンピューター・アーキテクチャー図である。図７に示すコンピューター・アーキテクチャーは、従来型のデスクトップ、ラップトップ・コンピューター、またはサーバー・コンピューターを例示しており、本明細書に開示した機能を提供するために上記説明した様々なソフトウェア・コンポーネントを実行するのに利用することができる。

【００５５】

図７に示すコンピューター・アーキテクチャーは、中央演算処理ユニット７０２（「ＣＰＵ」）、ランダム・アクセス・メモリ７１４（「ＲＡＭ」）およびリード・オンリ・メモリ（「ＲＯＭ」）７１６を含むシステム・メモリ７０８、並びに当該メモリをＣＰＵ７０２に結合するシステム・バス７０４を含む。起動中のようにコンピューター７００内において要素間で情報を移送するのを支援する基本ルーチンを収容する基本入／出力システム（「ＢＩＯＳ」）（図示せず）は、ＲＯＭ７１６に格納される。コンピューター７００は更に、オペレーティング・システム７１８、アプリケーション・プログラム、および他のプログラム・モジュールを格納するための大容量ストレージ・デバイス７１０を含み、より詳細は以下に説明する。

【００５６】

大容量ストレージ・デバイス７１０は、バス７０４に接続される大容量ストレージ・コントローラー（図示せず）を通じてＣＰＵ７０２に接続される。大容量ストレージ・デバイス７１０およびそれに付随するコンピューター可読ストレージ媒体により、不揮発性ストレージがコンピューター７００に提供される。本明細書に含まれるコンピューター可読媒体の説明は、ハードディスクまたはＣＤ－ＲＯＭドライブのような大容量ストレージ・デバイスに関連するものであるが、当業者にとって、コンピューター可読ストレージ媒体は、コンピューター７００によってアクセスすることができる如何なる利用可能なコンピューター・ストレージ媒体とすることができることが認められて然るべきである。

【００５７】

一例として、これに限定されないが、コンピューター可読ストレージ媒体は、コンピューター可読命令、データ構造、プログラム・モジュールまたは他のデータのような情報をストレージするための如何なる方法または技術で実施される揮発性および不揮発性の、並びに着脱可能および着脱不能な媒体を含むことができる。例えば、コンピューター可読ストレージ媒体は、これに限定されないが、ＲＡＭ、ＲＯＭ、ＥＰＲＯＭ、ＥＥＰＲＯＭ、フラッシュ・メモリ若しくは他のソリッド・ステート・メモリ技術、ＣＤ－ＲＯＭ、デジタル多用途ディスク（「ＤＶＤ」）、ＨＤ－ＤＶＤ、ＢＬＵ－ＲＡＹ若しくは他の光デバイス、磁気カセット、磁気テープ、磁気ディスク・ストレージ、若しくは他の磁気記憶デバイス、または所望の情報を格納するのに用いることができ、コンピューター７００によってアクセス可能な他の如何なる非一時的媒体をも含む。

【００５８】

なお、本明細書に開示したコンピューター可読媒体は通信媒体を含むことが認められて然るべきである。通信媒体は、通例、コンピューター可読命令、データ構造、プログラム・モジュール、または他のデータを搬送波のような変調データ信号若しくは他の転送機構で実現し、如何なる情報搬送媒体をも含む。「変調データ信号」なる用語は、その特徴セットの内１つ以上を有する信号、または情報を信号にコード化するような方法で変更される信号のことを意味する。一例として、これに限定されないが、通信媒体は、有線ネットワークまたはダイレクト通信接続のような有線媒体、並びに音響、無線周波数、赤外線および他の無線媒体のような無線媒体を含む。上記の如何なる組合せはまた、コンピューター可読媒体の範囲内として含まれなければならない。コンピューター可読ストレージ媒体は、通信媒体を含まない。

【００５９】

各種実施形態によれば、コンピューター７００は、ネットワーク７２０のようなネットワークを通じた遠隔コンピューターへの論理接続を用いて、ネットワーク化した環境において動作することができる。コンピューター７００は、バス７０４に接続されるネットワ

ーク・インターフェース・ユニット７０６を通じてネットワーク７２０に接続することができる。なお、ネットワーク・インターフェース・ユニット７０６はまた、他の種別のネットワークおよび遠隔コンピューター・システムに接続するために利用できることも認められて然るべきである。コンピューター７００はまた、キーボード、マウスまたは電子スタイラス（図７に図示せず）を含む、数多くの他のデバイスからの入力を受け取り且つ処理するために、入／出力コントローラ７１２を含むこともできる。同様に、入／出力コントローラは、ディスプレイ・スクリーン、プリンター、または他の種別の出力デバイス（図７に図示せず）に出力を供給することができる。

【００６０】

先に簡潔に述べたように、数多くのプログラム・モジュールやデータ・ファイルが、ネットワーク化されたデスクトップ、ラップトップまたはサーバー・コンピューターの動作を制御するのに適したオペレーティング・システム７０４を含む、コンピューター７００の大容量ストレージ・デバイス７１０およびＲＡＭ７１４に格納することができる。大容量ストレージ・デバイス７１０およびＲＡＭ７１４はまた、１つ以上のプログラム・モジュールを格納することもできる。特に、大容量ストレージ・デバイス７１０およびＲＡＭ７１４は、アプリケーション１０４またはリソース・サーバー１１４のような、先に説明した機能を提供する１つ以上のソフトウェア・コンポーネント、または他の種別のプログラム若しくはサービスを格納することができる。大容量ストレージ・デバイス７１０およびＲＡＭ７１４はまた、本明細書に開示した他のプログラム・モジュールおよびデータを格納することもできる。

【００６１】

一般に、ソフトウェア・アプリケーションまたはモジュールは、ＣＰＵ７０２にロードされ実行されると、ＣＰＵ７０２およびコンピューター７００全体を、一般用途のコンピューティング・システムから、本明細書に提示される機能を実行するのにカスタマイズされた特定用途のコンピューティング・システムへと変換させることができる。ＣＰＵ７０２は、如何なる数のトランジスターまたは他の別個の回路要素から構成することができ、それは如何なる状態の数を、個々にまたは集合的に想定することができる。より具体的には、ＣＰＵ７０２は、ソフトウェアまたはモジュール内に収容された実行可能命令に応じて、１つ以上の有限状態マシンとして動作させることができる。これらコンピューター実行可能命令は、如何にＣＰＵ７０２が状態間を遷移するかを特定することによってＣＰＵ７０２を変更させることができ、これにより、ＣＰＵ７０２を構成するトランジスターまたは他の別々のハードウェア要素を物理的に変更させる。

【００６２】

ソフトウェアまたはモジュールを大容量ストレージ・デバイス上にコード化することはまた、大容量ストレージ・デバイスまたは付随するコンピューター可読ストレージ媒体の物理的な構造を変化させることもできる。

物理的な構造の特定の変更は、本説明における異なる実施態様では様々な要因に依存することがある。このような要因の例として、これに限定されないが以下を含むことができる。即ち、コンピューター可読ストレージ媒体を実装するのに使用される技術や、コンピューター可読ストレージ媒体がプライマリまたはセカンダリのストレージとして特徴付けられるか等である。例えば、コンピューター可読ストレージ媒体が半導体ベース・メモリとして実装される場合は、ソフトウェアがコード化されると、ソフトウェアまたはモジュールは、半導体メモリの物理的な状態を変更することができる。例えば、ソフトウェアは、トランジスター、コンデンサー、または半導体メモリを構成する他の別個の回路要素を変更することができる。

【００６３】

別の例として、コンピューター可読ストレージ媒体は、磁気または光学的技術を用いて実装することができる。このような実装において、ソフトウェアまたはモジュールは、ソフトウェアがコード化されると、磁気または光学式媒体の物理的状態を変更することができる。これらの変更は、所与の磁気媒体内において特定の位置の磁気特性を変更すること

を含むことができる。これらの変更はまた、所与の光学式媒体内において特定の位置の物理的な特徴または特性を変更して、それらの位置についての光特性を変更することを含むこともできる。物理媒体の他の変更が、本説明の範囲および趣旨から逸脱することなく、本検討を容易にするためにのみ提供される上記の例を用いて可能である。

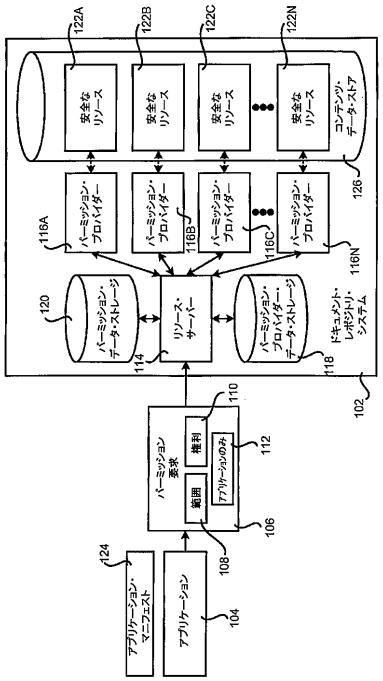
【００６４】

以上のことから、安全なリソースへのアプリケーションによるアクセスを認可する技術について本明細書に開示したことが認められて然るべきである。本明細書に提示した主題について、コンピューターの構造上の特徴、方法論的な行為、およびコンピューター可読媒体に特化した言語で記載したものの、添付の特許請求の範囲に規定される発明が、本明細書に説明する特定の特徴、行為、または媒体には必ずしも限定されないことが理解されるべきである。むしろ、特定の特徴、行為および媒体は、特許請求の範囲を実施する例示の形態として開示されるものである。

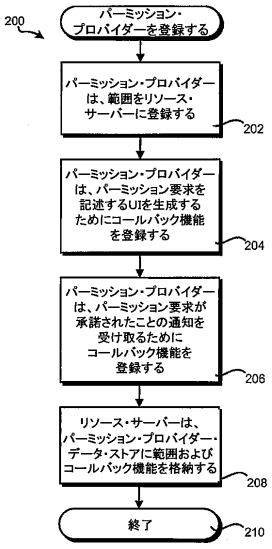
【００６５】

先に説明した主題は、例示目的のみによって提供されたものであり、限定するものとして解釈されてはならない。様々な修正や変更が、図示および説明した例示の実施形態や適用に従うことなく、また、以降の特許請求の範囲に記載した本発明の真の趣旨および範囲から逸脱することなく、本明細書に記載した主題に対して行うことができる。

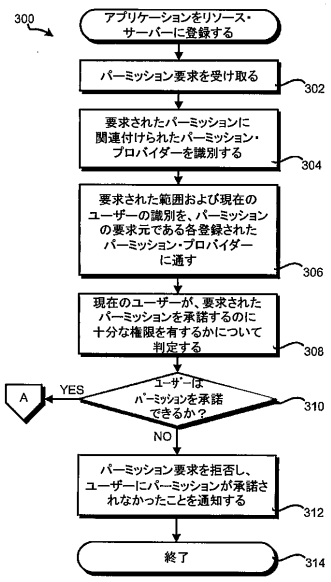
【図１】



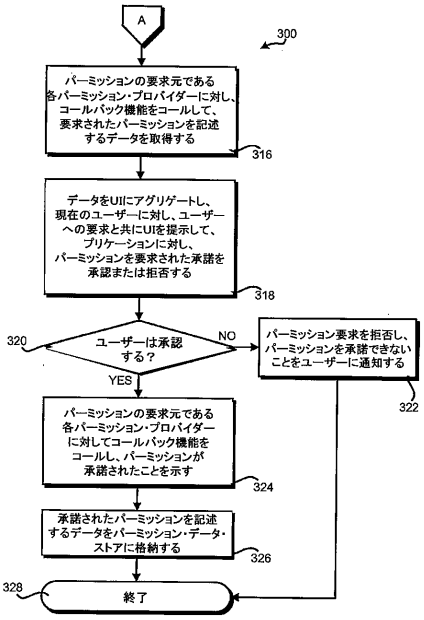
【図２】



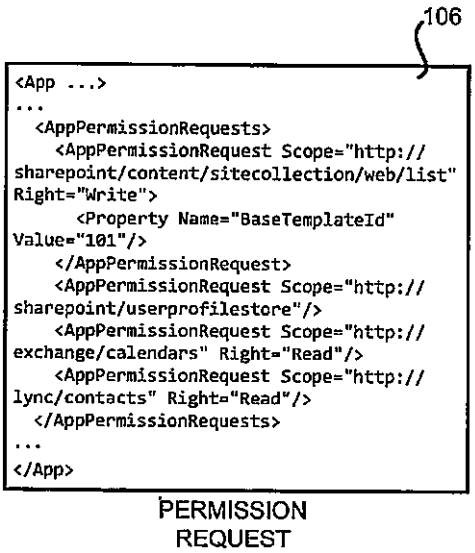
【図３Ａ】



【図３Ｂ】



【図４Ａ】



【図４Ｂ】

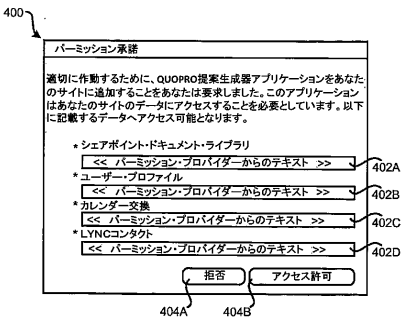
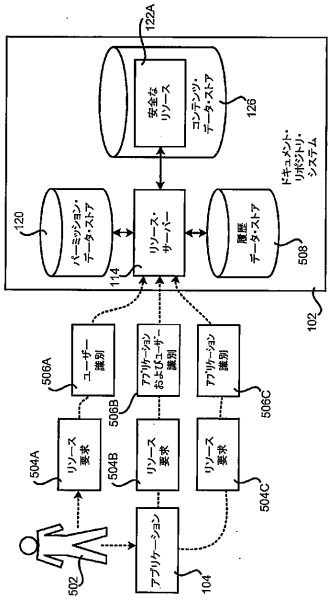
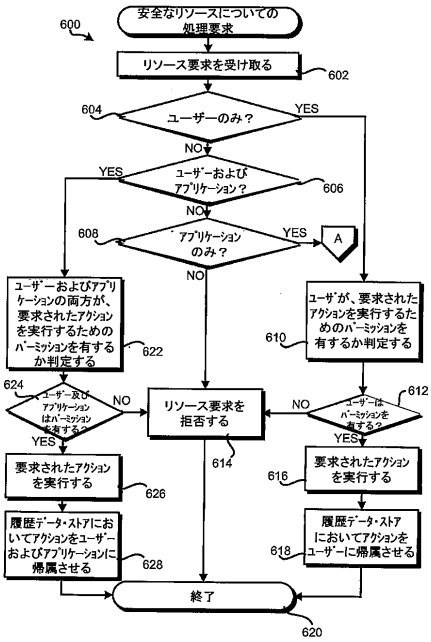


FIG. 4B

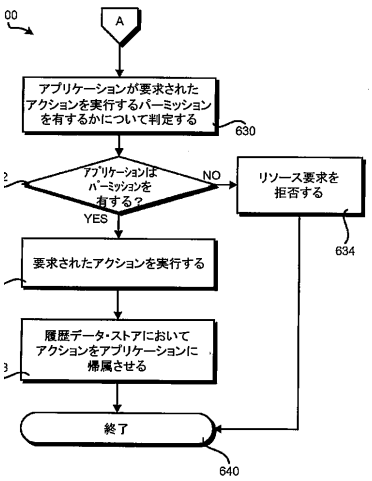
【図５】


122A
安全なリソース
コンテンツ・データ・ストア
126
ドキュメント・リポジトリ・システム
パーミッション・データ・ストア
120
リソース・サーバー
114
履歴データ・ストア
508
102
ユーザー識別
506A
アプリケーションおよびユーザー識別
506B
アプリケーション識別
506C
リソース要求
504A
リソース要求
504B
リソース要求
504C
アプリケーション
104
502

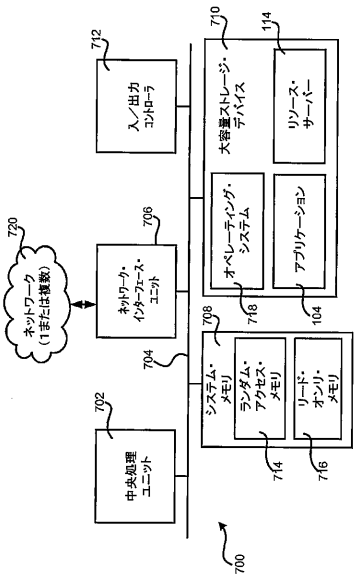
【図６Ａ】


600
安全なリソースについての処理要求
リソース要求を受け取る
602
ユーザーのみ？
604
YES
NO
ユーザーおよびアプリケーション？
606
YES
NO
アプリケーションのみ？
608
YES
NO
A
ユーザーおよびアプリケーションの両方が、要求されたアクションを実行するためのパーミッションを有するか判定する
622
ユーザーが、要求されたアクションを実行するためのパーミッションを有するか判定する
610
ユーザー及びアプリケーションはパーミッションを有する？
624
NO
YES
リソース要求を拒否する
614
ユーザーはパーミッションを有する？
612
NO
YES
要求されたアクションを実行する
626
要求されたアクションを実行する
616
履歴データ・ストアにおいてアクションをユーザーおよびアプリケーションに帰属させる
628
履歴データ・ストアにおいてアクションをユーザーに帰属させる
618
終了
620

【図６Ｂ】


A
アプリケーションが要求されたアクションを実行するパーミッションを有するかについて判定する
630
アプリケーションはパーミッションを有する？
NO
YES
リソース要求を拒否する
634
要求されたアクションを実行する
履歴データ・ストアにおいてアクションをアプリケーションに帰属させる
終了
640

【図７】


712
入／出力コントローラ
710
大容量ストレージ・デバイス
114
リソース・サーバー
オペレーティング・システム
718
アプリケーション
104
720
ネットワーク（1または複数）
706
ネットワーク・インターフェース・ユニット
708
704
システム・メモリ
ランダム・アクセス・メモリ
714
リード・オンリ・メモリ
716
702
中央処理ユニット
700

フロントページの続き

(74)代理人 100153028
弁理士 上田 忠
(74)代理人 100120112
弁理士 中西 基晴
(74)代理人 100196508
弁理士 松尾 淳一
(74)代理人 100147991
弁理士 鳥居 健一
(74)代理人 100119781
弁理士 中村 彰吾
(74)代理人 100162846
弁理士 大牧 綾子
(74)代理人 100173565
弁理士 末松 亮太
(74)代理人 100138759
弁理士 大房 直樹
(72)発明者 ハワード，ロバート・マッキー
アメリカ合衆国ワシントン州９８０５２－６３９９，レッドモンド，ワン・マイクロソフト・ウェイ，マイクロソフト コーポレーション，エルシーエイ－インターナショナル・パテンツ
(72)発明者 ミロン，タイタス・コンスタンティン
アメリカ合衆国ワシントン州９８０５２－６３９９，レッドモンド，ワン・マイクロソフト・ウェイ，マイクロソフト コーポレーション，エルシーエイ－インターナショナル・パテンツ
(72)発明者 テイラー，ウィリアム・デーヴィッド
アメリカ合衆国ワシントン州９８０５２－６３９９，レッドモンド，ワン・マイクロソフト・ウェイ，マイクロソフト コーポレーション，エルシーエイ－インターナショナル・パテンツ
(72)発明者 ジュウ，シャオフェン
アメリカ合衆国ワシントン州９８０５２－６３９９，レッドモンド，ワン・マイクロソフト・ウェイ，マイクロソフト コーポレーション，エルシーエイ－インターナショナル・パテンツ
(72)発明者 アイディン，エレイ
アメリカ合衆国ワシントン州９８０５２－６３９９，レッドモンド，ワン・マイクロソフト・ウェイ，マイクロソフト コーポレーション，エルシーエイ－インターナショナル・パテンツ
(72)発明者 ヴィーララガヴァン，ヴェンカテシュ
アメリカ合衆国ワシントン州９８０５２－６３９９，レッドモンド，ワン・マイクロソフト・ウェイ，マイクロソフト コーポレーション，エルシーエイ－インターナショナル・パテンツ

審査官 岸野 徹

(56)参考文献 国際公開第２００７／０４３６５９（WO，Ａ１）
特開２００１－３３７８６４（ＪＰ，Ａ）
米国特許出願公開第２０１０／０２４２０９７（ＵＳ，Ａ１）
国際公開第２０１１／０８８９００（WO，Ａ１）
特開平１１－２７２７６９（ＪＰ，Ａ）
特開２００８－０１６０１３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／６２
Ｇ０６Ｆ １２／００