(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5083042号
(P5083042)
(45)発行日　平成24年11月28日(2012.11.28)　(24)登録日　平成24年9月14日(2012.9.14)

(51)Int.Cl.　　F I
G06F 21/00 (2006.01)　　G06F 21/00　157D
G06F 21/20 (2006.01)　　G06F 21/20　146
G06F 21/24 (2006.01)　　G06F 21/24　163J

請求項の数 7　(全 68 頁)

(21)出願番号　特願2008-142646 (P2008-142646)
(22)出願日　平成20年5月30日 (2008.5.30)
(65)公開番号　特開2009-289137 (P2009-289137A)
(43)公開日　平成21年12月10日 (2009.12.10)
審査請求日　平成23年2月17日 (2011.2.17)

（出願人による申告）平成１９年度、経済産業省、「セキュア・プラットフォームプロジェクト」委託研究、産業技術力強化法第１９条の適用を受ける特許出願

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100074099
弁理士　大菅　義之
(74)代理人　100133570
弁理士　▲徳▼永　民雄
(72)発明者　徳谷　崇
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　畠山　卓久
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

最終頁に続く

(54)【発明の名称】アクセス制御ポリシーの遵守チェック用プログラム

(57)【特許請求の範囲】
【請求項１】
リソースに対するアクセスを一括してまたは部分的に制限するアクセス権情報を記憶するアクセス権情報記憶手段から該アクセス権情報を取得する取得処理と、
前記リソースに対してまたは該リソースに対するアクセスに対して設定された複数のポリシーを記憶するポリシー記憶手段から前記複数のポリシーのそれぞれに対して、前記アクセス権情報が適合しているか否かを検査し、ポリシーに適合しないものを違反として検出する検出処理と、
検出された前記違反内容に応じたリスクに基づき、前記アクセス権情報の適正度を出力する出力処理と、
を情報処理装置に実行させるプログラム。
【請求項２】
前記複数のポリシーに、前記アクセス権情報に含まれるユーザ情報が、使用していないユーザアカウント、利用者を特定できないユーザアカウント、または削除されるべきアカウントであったがまだ残っているユーザアカウントの何れかに該当する場合に違反とすることが含まれる、
ことを特徴とする請求項１に記載のプログラム。
【請求項３】
前記複数のポリシーに、前記アクセス権情報に含まれるロール割当てが、使用していないロール割当て、または、あらかじめ決められたロール割当て禁止ルールに違反するロー

ル割当て、の何れかに該当する場合に違反とすることが含まれる、
ことを特徴とする請求項１に記載のプログラム。
【請求項４】
前記複数のポリシーに、前記アクセス権情報に含まれるパーミッション割当てが、使用していないパーミッション割当て、または、あらかじめ決められたパーミッション割当て禁止ルールに違反するパーミッション割当て、の何れかに該当する場合に違反とすることが含まれる、
ことを特徴とする請求項１に記載のプログラム。
【請求項５】
前記複数のポリシーに、前記アクセス権情報に含まれるロールが、使用されていないロール、あらかじめ決められたユーザへのロール割当て禁止ルールに違反するロール、または、あらかじめ決められたロールへのパーミッション割当て禁止ルールに違反するロール、の何れかに該当する場合に違反とすることが含まれる、
ことを特徴とする請求項１に記載のプログラム。
【請求項６】
前記複数のポリシーに、ユーザへのロール割当て禁止ルールに違反するロール割当て、ロールへのパーミッション割当て禁止ルールに違反するパーミッション、または、ユーザへのパーミッション割当て禁止ルールに違反するパーミッション、の何れかに該当する場合に違反とすることが含まれる、
ことを特徴とする請求項１に記載のプログラム。
【請求項７】
リソースに対するアクセスを一括してまたは部分的に制限するアクセス権情報を記憶するアクセス権情報記憶手段から取得するアクセス権情報取得手段と、
前記リソースに対してまたは該リソースに対するアクセスに対して設定された複数のポリシーを記憶するポリシー記憶手段から前記複数のポリシーのそれぞれに対して、前記アクセス権情報が適合しているか否かを検査し、ポリシーに適合しないものを違反として検出する検出手段と、
検出された前記違反内容に応じたリスクに基づき、前記アクセス権情報の適正度を出力する出力手段と、
を備える情報処理装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理システムにおいて内部統制等に基づくアクセス制御ポリシーが適切に遵守されているか否かをチェックするプログラムに関する。
【背景技術】
【０００２】
近年日本版ＳＯＸ法（金融商品取引法）の施行に伴い、内部統制やコンプライアンスへの対応が求められており、ＩＤ，アクセス権についても統制を厳密に実施し、強化していくことが求められている。
【０００３】
従来この分野において、Ｓｕｎ　Ｊａｖａ　Ｉｄｅｎｔｉｔｙ　Ｍａｎａｇｅｒなどの企業内の各システムが管理するＩＤ情報を統合的に管理する機能を持つ製品や、Ｏｒａｃｌｅ　Ｒｏｌｅ　Ｍａｎａｇｅｒなどの企業内のシステムで管理しているロールを統合的に管理するシステムが、提供されており、統制強化のために、セキュリティポリシー（職務分掌）をチェックする機能が組み込まれている。
【０００４】
この仕組みは、以下のようなマトリクスを利用して、チェックを行う方式である。
【０００５】

【表１】

	ロールA	ロールB	ロールC	ロールD
ロールA				
ロールB	×			
ロールC	○	×		
ロールD	○	×	○	

表中の○印は、ユーザが行と列で示されている2つのロールを同時に利用（所属）することがセキュリティポリシー上許されている。×は、ユーザが行と列で示されている２つのロールを同時に利用することが、セキュリティポリシー上禁止されていることを示している。

【０００６】

例えば、ユーザは、ロールＡとロールＢを同時に利用することができない。また、ユーザは、ロールＡとロールＣは同時に利用することができる。このような定義に基づいて、ＩＤやロールの統合管理するシステムは、自身で管理しているだれがどのロールに所属しているかという「ユーザ－ロール割当て情報」を使ってチェックを行う。

【０００７】

上記技術に関連して、特許文献１には、ＲＢＡＣ（Ｒｏｌｅ Ｂａｓｅｄ Ａｃｃｅｓｓ Ｃｏｎｔｒｏｌ）モデルおよびＴＥ（Ｔｙｐｅ Ｅｎｆｏｒｃｅｍｅｎｔ）モデルに基づく強制アクセス制御の設定が適切であることを検証する情報処理装置について開示されている。また、特許文献２には、２ポリシー集合の置き換えに用いることのできるポリシー集合を生成するポリシー集合生成装置について開示されている。

【特許文献１】特開２００７－０４１８８１号公報

【特許文献２】特開２００７－０７２５８１号公報

【発明の開示】

【発明が解決しようとする課題】

【０００８】

現在、多くのシステムでは、ＲＢＡＣといったアクセス制御モデルが採用されている。このモデルには、ユーザとロールの関係、ロールとパーミッションの関係、ロールの階層関係や職務分掌の関係などを管理している。

【０００９】

このようなＲＢＡＣシステムを想定した場合に、上記従来の技術の製品が提供している機能は、ＩＤとロールの関係の関係について、セキュリティポリシーをチェックしており、その他の関係についてチェックしておらず、そのためポリシー遵守が徹底されていない。

【００１０】

また、内部統制の実施において、企業内のシステム管理やセキュリティ管理の担当といったシステムに精通している人ばかりでなく、監査担当、コンプライアンス担当や、あるいは経営層といったシステムに精通していない人も係わってくるため、システムのＩＤ・アクセス権の統制が行われているかどうかについてだれが見てもわかるようにシステム毎に数値化することが必要である。

【００１１】

これは、組織内のシステムにおいてどのシステムが、他のシステムに比べて、ＩＤ・アクセス権に関してどれだけちゃんと管理している／管理していないということがわかるようになり、管理していないシステムについて徹底を促すことができることや、数値化することにより、各システムの管理目標を明確化することができるといった効果がある。これらの効果は、組織内の統制強化につながる。

【００１２】

本発明は、上述した問題に鑑みてなされたものであり、その解決しようとする課題は、アクセス制御のためのポリシーに対する多面的かつ網羅的なチェックを可能にし、チェック結果を容易かつ客観的に把握することを可能にするアクセス制御ポリシーの遵守チェックを実現することである。

【課題を解決するための手段】

【００１３】

上記課題を解決するために、情報処理装置に、リソースに対するアクセスを一括してまたは部分的に制限するアクセス権情報を記憶するアクセス権情報記憶手段から該アクセス権情報を取得する取得処理と、前記リソースに対してまたは該リソースに対するアクセスに対して設定された複数のポリシーを記憶するポリシー記憶手段から前記複数のポリシーのそれぞれに対して、前記アクセス権情報が適合しているか否かを検査し、ポリシーに適合しないものを違反として検出する検出処理と、検出された前記違反内容に応じたリスクに基づき、前記アクセス権情報の適正度を出力する出力処理と、を実行させる。

【００１４】

上記処理によると、アクセス権情報がポリシーに適合しないものを違反として検出し、検出された違反内容に応じたリスクに基づき、アクセス権情報の適正度を表示装置に出力し、表示データとして記憶装置に出力する。

【発明の効果】

【００１５】

以上に説明した処理により、アクセス制御のためのポリシーに対して多面的かつ網羅的なチェックを可能にし、チェック結果を容易かつ客観的に把握することを可能にするアクセス制御ポリシーの遵守チェックが実現される。

【発明を実施するための最良の形態】

【００１６】

以下、本発明の実施形態について、図１～図５３に基づいて説明する。

１．　本実施例の概要

図１は、本実施例に係るアクセス制御ポリシー遵守のチェック機構を備える統合セキュリティ管理システム１００の構成例を示す図である。

【００１７】

図１に示す統合セキュリティ管理システム１００は、各サーバＡ、ＢおよびＣに対してアクセス制御を行なうアクセス制御ポリシー（以下、必要に応じて「ポリシー」という）の配布・収集を行なう統合アクセス制御情報管理部１１０と、各サーバＡ、ＢおよびＣにおけるユーザアカウント等を統合的に管理する統合ＩＤ管理部１２０と、を備える。

【００１８】

なお、各サーバＡ、ＢおよびＣから出力されるログの全部または一部は、監査ログとして監査ログ記憶部１３０に記憶される。必要に応じて、監査ログ記憶部１３０を統合セキュリティ管理システム１００の構成要素としてもよい。また、図１では、サーバＡ、ＢおよびＣからなるサーバシステムを示しているが、サーバの数を限定する趣旨でないのは当然である。

【００１９】

統合アクセス制御情報管理部１１０は、各サーバＡ、ＢおよびＣに対してポリシーの配布・収集を行なう設定アダプタ１１１と、ポリシーを生成するポリシー生成部１１２と、生成したポリシーやＲＢＡＣポリシー等を記憶するＲＢＡＣポリシー記憶部１１３と、各サーバＡ、ＢおよびＣにおけるリソースの構成情報を各サーバから取得・管理するリソース構成情報管理部１１４と、ポリシーをチェックするルール等を記憶するポリシーチェックルール記憶部１１５と、ポリシーチェックルール記憶部１１５に記憶されているポリシーチェックルールにしたがってポリシーのチェック・修正を行なうポリシーチェック・修

正部１１６と、を備えることにより、システム全体で一貫したアクセス制御を行うためのアクセス権を管理（生成、編集、削除等）し、各サーバシステムのアクセス制御機構で可読な形式でアクセス権を配付する。

【００２０】

ポリシーチェック・修正部１１６は、例えば、ＲＢＡＣポリシー記憶部１１３に記憶されたＲＢＡＣポリシーやＲＢＡＣポリシー記憶部１１３若しくは統合ＩＤ管理部１２０に記憶されたアクセス権設定情報を取得し、監査ログ記憶部１０３から監査ログとして記憶されているアクセスログを取得する。

【００２１】

アクセス権設定情報とは、例えば、後述するロール－ユーザ対応表などのユーザ情報、ユーザ－ロール割当て情報、パーミッション－ロール割当て情報、ロール情報、などをいい、必要に応じて職務分掌ルール情報等を含めてもよい。

【００２２】

ロールとは、論理的な中間体であって、例えばリソースなどのオブジェクトに対するアクセスに関する設定等をグループ化したものである。例えば、ＲＢＡＣシステムでは、アクセス権（読み取り、書き込み、変更、削除など）などをグループ化したものをいう。

【００２３】

また、ポリシーチェック・修正部１１６は、ポリシーチェックルール記憶部１１５から所定のポリシーチェックルールを取得する。そして、ポリシーチェックルールに違反した設定があるかどうかを検知し、ポリシー遵守レベルを算出する（数値化する）。また、ポリシーチェック・修正部１１６は、検出した違反に対して修正案を提示する。

【００２４】

ポリシーチェックルールとは、例えば、後述するユーザへのロール割当て禁止ルール、ロールへのパーミッション割当て禁止ルール、ユーザへのパーミッション割当て禁止ルールなどである。

【００２５】

リソース構成情報管理部１１４は、統合的なアクセス制御実現に必要な、アクセス制御対象となるリソースの構成情報を各サーバＡ、ＢおよびＣから収集し、ポリシー作成のために統合アクセス情報管理で管理する。

【００２６】

リソースとは、本実施例に係る統合セキュリティ管理システム１００の管理対象であって、各サーバを構成し若しくはサーバ上で動作する構成要素をいう。例えば、各サーバに備わるメモリやデータファイル、各サーバ上で動作するアプリケーション等である。

【００２７】

また、アクセスとは、リソースに対して行なう操作のことをいう。例えば、任意のサーバ上またはサーバが備える記憶装置等に記憶されたファイルに対するＲｅａｄ／Ｗｒｉｔｅ処理などである。

【００２８】

統合ＩＤ管理部１２０は、統合的なアクセス制御を実現するために、サーバＡ、ＢおよびＣからなるサーバシステムや統合セキュリティ管理システム１００を含むシステム全体で一意なユーザＩＤとその属性情報（資格、役割等）とを一元管理し、管理対象システムと同期をとると共に、ポリシー作成に必要なユーザＩＤ等を統合アクセス制御情報管理部１１０に通知する。

【００２９】

また、統合ＩＤ管理部１０２は、ロール－ユーザ対応表等のユーザ情報を管理し、必要に応じて統合アクセス制御情報管理部１１０に配付する。

２．　ポリシー遵守レベル測定対象

本実施例に係る統合アクセス制御情報管理部１１０は、アクセス権の管理対象であるユーザ情報、ユーザ－ロール割当て情報、パーミッション－ロール割当て情報、ロール情報、職務分掌ルール情報（以下、これらの情報を「アクセス権管理情報」という）について

、ポリシーを遵守しているかどうかを検知し、検知された設定情報等のリスクの強弱に応じて得点化を行なう。さらに、サーバや保護されるリソース集合の単位で、その総合得点を計算することで、他のサーバやリソース集合の管理におけるポリシー遵守度合いを比較可能にする。

【００３０】

本実施例に係る統合セキュリティ管理システム１００では、ＲＢＡＣシステムにおけるポリシーの遵守レベルを計測する場合について説明する。なお、ＲＢＡＣシステムについては、従来技術であるので、詳細な説明は省略する。

【００３１】

図２は、本実施例に係る統合セキュリティ管理システム１００におけるポリシー遵守レベルのチェック対象を説明する図である。図２に示すように、次の項目についてポリシーチェックルールに違反した件数を取得し、その結果を用いて遵守のレベルを数値化する。

【００３２】

（１）不適切なユーザアカウントの検出

不適切なユーザアカウントとしては、例えば、利用者を特定できないユーザ、使用されていないユーザ、職制移動したが残っているユーザについてのアカウントなどが考えられる。

【００３３】

（２）不適切なユーザ－ロール割当ての検出

不適切なユーザ－ロール割当てとしては、例えば、使用されていないユーザ－ロール割当て、ユーザの同時割当てが禁止されたロールについてユーザ－ロール割当てが行なわれている、などが考えられる。

【００３４】

（３）不適切なパーミッション－ロール割当ての検出

不適切なパーミッション－ロール割当てとしては、使用されていないパーミッション－ロール割当て、ユーザの同時割当てが禁止されているパーミッションについてパーミッション－ロール割当てが行なわれている、などが考えられる。

【００３５】

（４）不要なロールの検出

不要なロールとしては、例えば、使用されていないロール、親子関係が禁止されたロール、などが考えられる。

【００３６】

（５）職務分掌違反の検出

職務分掌違反としては、例えば、ユーザの同時割当てが禁止されたロールについてユーザ－ロール割当てが行なわれている、パーミッションの同時割当てが禁止されているロールまたはユーザについてパーミッション－ロール割当てが行なわれている、などが考えられる。

【００３７】

３．　本実施例に係る処理の概要

図３は、本実施例に係る統合セキュリティ管理システム１００の処理の概要を示すフローチャートである。

【００３８】

ステップＳ３００において、統合セキュリティ管理システム１００は、アクセス制御ポリシーの遵守をチェックする処理を開始すると、ステップＳ３０１に移行する。

ステップＳ３０１において、統合セキュリティ管理システム１００は、必要に応じて、統合ＩＤ管理部１２０、ＲＢＡＣポリシー記憶部１１３またはポリシーチェックルール記憶部１１５からアクセス権管理情報を取得する。

【００３９】

本実施例では、アクセス権管理情報のうちユーザＩＤ等のユーザ情報は、統合ＩＤ管理部１２０に記憶されている。また、ユーザ－ロール割当て情報、パーミッション－ロール

割当て情報およびロール情報は、ＲＢＡＣポリシー記憶部１１３に記憶され、職務分掌ルール情報は、ポリシーチェックルール記憶部１１５に記憶されている。

【００４０】

ステップＳ３０２において、統合セキュリティ管理システム１００は、ステップＳ３０１で取得したアクセス権管理情報に応じて、ポリシーチェックルール記憶部１１５からポリシーチェックルールを取得し、当該ルール等に関する違反を検出する。

【００４１】

本実施例では、図２で説明したように、ステップＳ３０１で取得したアクセス権管理情報に応じて、（１）不適切なユーザアカウント、（２）不適切なユーザ－ロール割当て、（３）不適切なパーミッション－ロール割当て、（４）不要なロール、（５）職務分掌違反を違反として検出する。これらの（１）～（５）の処理については、後述する。

【００４２】

ステップＳ３０３において、統合セキュリティ管理システム１００は、ステップＳ３０２で検出した違反の件数等に基づいて、ポリシー遵守レベルを算出する。

ステップＳ３０４において、統合セキュリティ管理システム１００は、ステップＳ３０３の算出結果を表示装置等に出力して表示する。そして、統合セキュリティ管理システム１００は、ステップＳ３０５に移行して処理を終了する。

【００４３】

以下、ステップＳ３０２～Ｓ３０４の具体的な処理について説明する。

３．１　不適切なユーザアカウントの検出処理

アクセス権管理の中で、不適切なユーザＩＤがあると、不正なアクセスや、情報漏洩・情報の改ざんの原因となるため、ユーザＩＤを適切に管理することが必要となる。

【００４４】

本実施例では、アクセス権管理の管理対象であるユーザ情報を使って、使っていないユーザＩＤ、利用者を特定できないユーザＩＤ、または、異動したがアカウントが残っているユーザを、不適切なユーザと定義し、それを検出し、検出結果を、そのリスクの強弱に応じて分類し、得点化することで、ユーザＩＤを適切に管理することを可能にする。

【００４５】

図４は、本実施例に係る不適切なユーザＩＤの検出処理の概要を示す図である。

ポリシーチェック・修正部１１６は、統合ＩＤ管理部１２０から表２１に示すロール－ユーザ対応表を取得する。また、ポリシーチェック・修正部１１６は、人事システム４１０などの例えば異動者情報記憶部４１１に記憶されている従業員に関する情報から作成された異動や退職したユーザリスト（以下、「異動者リスト」という）を取得する。

【００４６】

異動者情報記憶部４１１は、例えば、必要に応じて統合セキュリティ管理システム１００に備えてもよいし、人事システム４１０を構成するサーバＡ、Ｂ、またはＣ等に備えられていてもよい。

【００４７】

また、ポリシーチェック・修正部１１６は、統合ＩＤ管理部１２０からユーザ情報４０２を取得する。そして、ポリシーチェック・修正部１１６は、取得した情報を利用し、不適切なユーザアカウントを検出する。さらに、ポリシーチェック・修正部１１６は、検出結果を、表３に示す不適切なユーザのリスク得点表５０１に基づいて数値化する。

【００４８】

図５は、本実施例に係る不適切なユーザアカウントの定義を説明する図である。

図５に示すように、本実施例に係る不適切なユーザアカウントは、

（ａ）「利用者を特定できないユーザＩＤ」∪

（ｂ）「使用されていないユーザＩＤ」∪

（ｃ）「職制異動したがＩＤが残っているユーザＩＤ」

と定義する。

【００４９】

ここで、本実施例では、システムのユーザＩＤリスト（以下、「ユーザリスト」という）を、ユーザ情報３０２として使用する。表２にその具体例を示す。表２では、ユーザＩＤとメールアドレス、最終利用日時という項目をもつテーブルである。

【００５０】

【表２】

	ユーザID	メールアドレス	最終利用日時
1	aaaaa	aaaaa@○○○○.com	2008/1/22 20:08
2	bbbbb		2008/1/20 14:28
3	ccccc	ccccc@○○○○.com	2000/9/1 12:22
4	ddddd	ddddd@○○○○.com	2007/12/26 11:34
5	eeeee	eeeee@○○○○.com	2008/1/13 12:02
	・・・	・・・	・・・

表２を用いた場合、（ａ）「利用者を特定できないユーザＩＤ」は、メールアドレスがないユーザと定義することができる。例えば、表２では２行目の「ｂｂｂｂｂ」は、メールアドレスがないため、利用者を特定できないＩＤとなる。

【００５１】

なお、本実施例では、メールアドレスがないユーザを「利用者を特定できないユーザＩＤ」と定義しているが、これに限定する趣旨ではない。例えば、内線番号や外線番号、Ｆａｘ番号など利用者との連絡手段がない場合に「利用者と特定できないユーザＩＤ」と定義してもよい。

【００５２】

また、表２を用いた場合、（ｂ）「使用されていないユーザＩＤ」は、最終利用日時が現在時刻よりも所定期間以前のユーザＩＤと定義することができる。

また、表２を用いた場合、（ｃ）「職制異動（退職含む）したがＩＤが残っているユーザＩＤ」は、人事システム４１０などの従業員に関する情報などから作成された異動や退職したユーザリスト（異動者リスト）に載っているユーザのユーザＩＤと定義することができる。

【００５３】

以上の定義にしたがって、不適切なユーザアカウントを検出する処理を以下に説明する。

図６は、本実施例に係る不適切なユーザアカウントを検出する具体的な処理を示すフローチャートである。

【００５４】

例えば、図３に示したステップＳ３０１において、統合ＩＤ管理部１２０から表２に示したユーザ情報（ユーザリスト）を取得し、人事システム４１０から異動者リストを取得すると、ポリシーチェック・修正部１１６は、処理をステップＳ６０１に移行する。そして、不適切なユーザアカウントの検出処理を開始する。

【００５５】

ステップＳ６０２において、ポリシーチェック・修正部１１６は、ユーザリストのｉ（ｉは１以上の自然数）番目のユーザＩＤのＵｉをチェック対象のユーザＩＤに設定する。

そして、ポリシーチェック・修正部１１６は、ユーザリストにおけるメールアドレスを参照し、ユーザＩＤＵｉにメールアドレスが登録されているか否かをチェックする。また

、ポリシーチェック・修正部１１６は、ユーザリストにおける最終利用日時を参照し、当該最終利用日時が現在時刻よりも所定期間以上前であるか否かをチェックする。また、ポリシーチェック・修正部１１６は、異動者リストを参照し、ユーザＩＤＵｉ（または、Ｕｉに該当するユーザ）が当該異動者リストに登録されているか否かをチェックする。

【００５６】

ステップＳ６０３において、ユーザＩＤＵｉにメールアドレスが登録されている場合、ポリシーチェック・修正部１１６は、処理をステップＳ６０４に移行する。そして、ポリシーチェック・修正部１１６は、該当するユーザＩＤＵｉを、特定できないユーザアカウントとして記憶装置等に記憶する。

【００５７】

ステップＳ６０５において、当該最終利用日時が現在時刻よりも所定期間以上前である場合、ポリシーチェック・修正部１１６は、処理をステップＳ６０６に移行する。そして、ポリシーチェック・修正部１１６は、該当するユーザＩＤＵｉを、利用されていないユーザアカウントとして記憶装置等に記憶する。

【００５８】

ステップＳ６０７において、ユーザＩＤＵｉが異動者リストに登録されている場合、ポリシーチェック・修正部１１６は、処理をステップＳ６１０に移行する。そして、ポリシーチェック・修正部１１６は、該当するユーザＩＤＵｉを、異動したが残っているユーザアカウントとして記憶装置等に記憶する。

【００５９】

ステップＳ６０９において、ポリシーチェック・修正部１１６は、ユーザＩＤＵｉが表３に示す分類（Ａ）～（Ｇ）の何れに該当するかを判断する。そして、表３に該当する分類がある場合、ポリシーチェック・修正部１１６は、処理をステップＳ６１０に移行する。

【００６０】

ステップＳ６０１において、ポリシーチェック・修正部１１６は、ユーザＩＤＵｉとリスク分類とリスク得点を、記憶装置等に用意したユーザリスク検出リストに記録する。

ステップＳ６１１において、ポリシーチェック・修正部１１６は、全てのユーザＩＤについてチェックが完了したか否かを確認する。そして、チェックすべきユーザＩＤがユーザリストにある場合、ポリシーチェック・修正部１１６は、処理をステップＳ６１２に移行する。

【００６１】

ステップＳ６１２において、ポリシーチェック・修正部１１６は、ｉを１だけインクリメントし、処理をステップＳ６０２に移行する。ステップＳ６０２では、ユーザリストにおける次のユーザＩＤをチェック対象のユーザＩＤに設定する。

【００６２】

一方、ステップＳ６１３において、全てのユーザＩＤについてチェックが完了した場合、ポリシーチェック・修正部１１６は、処理をステップＳ６１３に移行し、不適切なユーザアカウントの検出処理を終了する。

【００６３】

ここで、（ａ）「利用者を特定できないユーザＩＤ」と、（ｂ）「使用されていないユーザＩＤ」と、（ｃ）「職制異動したがＩＤが残っているユーザＩＤ」の集合の関係を図７に示す。

【００６４】

図７に示す集合（Ａ）は、「利用者を特定できないユーザＩＤ」かつ「使用されているユーザＩＤ」かつ「職制異動していないユーザＩＤ」の集合を示し、集合（Ｂ）は、「利用者を特定できるユーザＩＤ」かつ「使用されていないユーザＩＤ」かつ「職制異動していないユーザＩＤ」の集合を示し、集合（Ｃ）は、「利用者を特定できるユーザＩＤ」かつ「使用されているユーザＩＤ」かつ「職制異動したがＩＤが残っているユーザＩＤ」の集合を示す。

【００６５】
また、集合（Ｄ）は、「利用者を特定できないユーザＩＤ」かつ「使用されていないユーザＩＤ」かつ「職制異動したがＩＤが残っているユーザＩＤ」の集合を示す。
また、集合（Ｅ）は、「利用者を特定できないユーザＩＤ」かつ「使用されていないユーザＩＤ」かつ「職制異動していないユーザＩＤ」の集合を示し、集合（Ｆ）は、「利用者を特定できるユーザＩＤ」かつ「使用されていないユーザＩＤ」かつ「職制異動したがＩＤが残っているユーザＩＤ」の集合を示し、集合（Ｇ）は、「利用者を特定できないユーザＩＤ」かつ「使用されているユーザＩＤ」かつ「職制異動したがＩＤが残っているユーザＩＤ」の集合を示す。
【００６６】
この図の各集合についてのリスクを考慮することにより、例えば、表３に示すリスク得点（リスクが高ければ高い点数）テーブルが得られる。
【００６７】
【表３】

検出した不適切なユーザの分類	説明	リスク	得点
(A)	使用しており、異動していないまたは、ユーザリストに残っていない、かつ利用者を特定できないユーザ	特定できない利用者がシステムを利用している状況はリスクが高い	3
(B)	使っていない、異動していないまたはユーザリストに残っていない、かつ利用者を特定できるユーザ	利用者を特定できるが、使っていないユーザで、ゴーストIDにもなっていないので、リスクは低い	1
(C)	使っており、異動したがユーザリストに残っており、かつ利用者を特定できるユーザ	ゴーストIDが使われていることからリスクは高い	3
(D)	使っていない、異動したがユーザリストに残っており、かつ利用者を特定できないユーザ	ゴーストIDで、利用者は特定できないのでリスクは高い。	3
(E)	使っていない、異動していないまたはユーザリストに残っていない、かつ利用者を特定できないユーザ	利用者が特定できないが、使われていないのでリスクは中程度	2
(F)	使っていない、異動したがユーザリストに残っている、かつ利用者を特定できるユーザ	ゴーストIDだが、使われておらず、しかも利用者が特定できるので、リスクは中程度	2
(G)	使っており、異動したがユーザリストに残っている、かつ利用者を特定できないユーザ	ゴーストIDが使われていて、しかもそれが誰かわからないことからリスクが最も高い	4

なお、表３に示した得点は、点数が大きいほど検出した不適切なユーザアカウントの分類のリスクが高いことを示している。ただし、表３に示した得点は、これに限定する趣旨ではなく、必要に応じてリスクの高いと思われるものに高い特定を設定すればよい。
【００６８】
以上に説明した処理によって、ユーザＩＤ毎のリスク値と、全てのリスク値の合計を算出すると、ポリシーチェック・修正部１１６は、処理結果を、ポリシー遵守レベルとして表示装置等に出力して表示する。
【００６９】
図８は、不適切なユーザアカウントの検出処理におけるポリシー遵守レベルの表示例を示す図である。本実施例では、ユーザＩＤ毎のリスク点数と、その合計点をリスク評価値

として表示している。

【００７０】

３．２　不適切なユーザ－ロール割当ての検出処理

アクセス権管理において、不適切なユーザ－ロール割当てがあると、不正なアクセスや、情報漏洩・情報の改ざんの原因となる。そのため、ユーザ－ロール割当てを適切に管理する必要がある。

【００７１】

本実施例では、アクセス権管理の管理対象であるユーザ－ロール割当て情報に関し、不適切なユーザ－ロール割当て情報を、使用していないユーザ－ロール割当てとユーザへのロール割当て禁止の違反割当てとで定義し、それを検出し、検出結果を、そのリスクの強弱に応じて分類し、得点化することで、ユーザ－ロール割当てを適切に管理する。

【００７２】

図９は、本実施例に係る不適切なユーザ－ロール割当ての検出処理の概要を示す図である。

ポリシーチェック・修正部１１６は、統合ＩＤ管理部１２０からユーザ情報９０１（例えば、表２１に示すロール－ユーザＩＤ対応表）を取得する。また、ポリシーチェック・修正部１１６は、監査ログ記憶部１３０から例えば表２２に示すアクセスログ９０２を取得する。

【００７３】

そして、ポリシーチェック・修正部１１６は、ユーザ情報９０１とアクセスログ９０２とから使用していないユーザロール割当てを検出する。また、ポリシーチェック・修正部１１６は、例えば表５に示すあらかじめ設定されたロール割当て禁止ルール９０３に基づいて、ユーザ－ロール割当てに関するロール割当て禁止違反を検出する。そして、ポリシーチェック・修正部１１６は、検出結果を、表７に示すあらかじめ用意された不適切なユーザ－ロール割当てのリスク得点表９０４を用いて数値化する。

【００７４】

本実施例では、不適切なユーザ－ロール割当てを、

（ａ）「使用されていないユーザ－ロール割当て」∪

（ｂ）「ユーザへのロール割当て禁止の違反割当て」

と定義する。

【００７５】

図１０は、本実施例に係る不適切なユーザ－ロール割当ての検出処理の概要を示すフローチャートである。

例えば、図３に示したステップＳ３０１において、統合ＩＤ管理部１２０からユーザ情報９０１（例えば、表２１に示すロール－ユーザ対応表）を取得し、監査ログ記憶部１３０から例えば表２２に示すアクセスログ９０２を取得すると、ポリシーチェック・修正部１１６は、処理をステップＳ１００１に移行する。そして、不適切なユーザ－ロール割当ての検出処理を開始する。

【００７６】

ステップＳ１００１において、ポリシーチェック・修正部１１６は、ユーザ情報９０１とアクセスログ９０２とから使用していないユーザロール割当てを検出する。

ステップＳ１００２において、ポリシーチェック・修正部１１６は、あらかじめ設定されたロール割当て禁止ルール９０３に基づいて、ユーザ－ロール割当てに関するロール割当て禁止違反を検出する。

【００７７】

ステップＳ１００３において、ポリシーチェック・修正部１１６は、ステップＳ１００１およびステップＳ１００２における検出結果から、不適切なユーザ－ロール割当てのリスク得点表９０４に基づいてリスク評価値を算出する。

【００７８】

以上の処理が終了すると、ポリシーチェック・修正部１１６は、処理をステップＳ３０

４に移行し、ポリシー遵守レベルとして算出したリスク評価値を出力装置等に出力して表示する。

【００７９】

ここで、ステップＳ１００１における「使用されていないユーザ－ロール割当て」の検出では、表４に示すユーザ－ロール対応表（表２１をユーザをキーにソートしたもの）と、表２２に示すアクセスログと、から使用されていないユーザ－ロール割当てを検出する。

【００８０】

【表４】

ユーザID(UID)	ロール
U1	R1
U1	R3
・ ・ ・	・ ・ ・
U2	R1
U2	R5
・ ・ ・	・ ・ ・

【００８１】

３．２．１　使用されていないユーザ－ロール割当ての検出処理

図１１は、本実施例に係る使用されていないユーザ－ロール割当て検出処理（ステップＳ１００１）の具体的な処理を示すフローチャートである。

【００８２】

ステップＳ１１０１において、ポリシーチェック・修正部１１６は、ユーザ－ロール対応表のｉ番目のユーザＩＤであるＵｉを取得する。そして、ポリシーチェック・修正部１１６は、アクセスログ９０２を参照し、当該Ｕｉについてのアクセスログが記録されているアクセスログを抽出する。

【００８３】

ステップＳ１１０２において、ポリシーチェック・修正部１１６は、ユーザ－ロール対応表のＵｉにおけるｊ（ｊは１以上の自然数）番目のロールＲｊを取得する。そして、ポリシーチェック・修正部１１６は、ステップＳ１１０１で抽出したアクセスログのうち、当該Ｒｊに対するアクセスログが記録されているか否かを確認する。

【００８４】

ステップＳ１１０３において、ポリシーチェック・修正部１１６は、ステップＳ１１０２の確認の結果、ＵｉがＲｊを使用したアクセスログを確認できなかった場合、処理をステップＳ１１０４に移行し、当該ＵｉのＲｊを記憶装置等に記憶する。

【００８５】

ステップＳ１１０５において、ポリシーチェック・修正部１１６は、ユーザ－ロール対応表にＵｉに所属する未チェックのロールがあるか否かを判断する。そして、未チェックのロールがあると判断した場合、ポリシーチェック・修正部１１６は、処理をステップＳ１１０６に移行する。

【００８６】

そして、ポリシーチェック・修正部１１６は、ｊを１だけインクリメントすると、処理をステップＳ１１０２に移行する。

ステップＳ１１０７において、ポリシーチェック・修正部１１６は、ユーザ－ロール対応表に未チェックのユーザがあるか否かを判断する。未チェックのユーザがあると判断した場合、ポリシーチェック・修正部１１６は、処理をステップＳ１１０８に移行する。

【００８７】

そして、ポリシーチェック・修正部１１６は、ｉを１だけインクリメントすると、処理をステップＳ１１０１に移行する。

一方、ステップＳ１１０７において、未チェックのユーザがないと判断した場合、ポリシーチェック・修正部１１６は、ユーザが使用していないロールを検出する処理を終了し（ステップＳ１１０９）、ステップＳ１００２に移行する。

【００８８】

以上の処理によって、ユーザが使用していないロールのリストが得られる。

なお、ステップＳ１００２における「ユーザへのロール割当て禁止の違反割当て」の検出において、ユーザへのロール割当て禁止のルール９０３は、例えば表５のようにロールのペアとして定義される。以下の例の１番目は、Ｒ１とＲ２を同じユーザに割当ててはいけないことを意味する。２番目は、Ｒ１とＲ５を同じユーザに割当ててはいけないことを意味している。

【００８９】

【表５】

番号	ロール割当て禁止ルール
1	R1 , R2
2	R1 , R5
・・・	・・・

【００９０】

３．２．２　ユーザへのロール割当て禁止の違反割当ての検出処理

図１２は、本実施例に係るロール割当て禁止に違反するロール割当て検出処理（ステップＳ１００２）の具体的な処理を示すフローチャートである。なお、図１２に示す処理では、入力として、表４に示したユーザ－ロール対応表と、表５に示したロール割当て禁止ルール９０３と、が入力される。

【００９１】

ステップＳ１００１の処理が終了すると、ポリシーチェック・修正部１１６は、処理をステップＳ１２０１に移行し、ユーザ－ロール割当てがロール割当て禁止ルール９０３に違反しているか否かをチェックする処理を開始する。

【００９２】

ステップＳ１２０１において、ポリシーチェック・修正部１１６は、記憶装置等にあらかじめ記憶されたロール割当て禁止ルール９０３を取得する。

ステップＳ１２０２において、ポリシーチェック・修正部１１６は、ユーザ－ロール対応表を参照し、チェック対象のユーザＩＤを特定する。以下、ユーザ－ロール対応表のｉ番目のユーザＩＤをＵｉとして説明する。

【００９３】

ステップＳ１２０３において、ポリシーチェック・修正部１１６は、ユーザ－ロール対応表を参照し、Ｕｉに対して割当てられているロールを特定する。以下、ユーザ－ロール対応表において、Ｕｉに対してｊ番目に割当てられているロールをＲｊとする。

【００９４】

ステップＳ１２０４において、ポリシーチェック・修正部１１６は、例えば、表５に示したロール割当て禁止ルールを参照し、ステップＳ１２０３で特定したロールＲｊが、当該ロール割当て禁止ルールに登録されているか否かをチェックする。

【００９５】

そして、Ｒｊがロール割当て禁止ルールに登録されていた場合、ポリシーチェック・修正部１１６は、処理をステップＳ１２０５に移行する。

ステップＳ１２０５において、ポリシーチェック・修正部１１６は、ロール割当て禁止ルールにＲｊとともに登録されているロール（以下、「Ｒｊ’」とする）を取得する。そして、ポリシーチェック・修正部１１６は、ユーザ－ロール対応表を参照し、Ｕｉに対してＲｊ’が割当てられているか否かをチェックする。

【００９６】

そして、ユーザ－ロール対応表において、Ｕｉに対してＲｊ’が割当てられている場合、ポリシーチェック・修正部１１６は、処理をステップＳ１２０６に移行し、違反しているＵｉ、ＲｊおよびＲｊ’を１組のデータとして、記録装置等に記憶する。

【００９７】

ステップＳ１２０７において、ポリシーチェック・修正部１１６は、ユーザ－ロール対応表を参照し、Ｕｉに対して割当てられているロールであってチェックしていないものがあるか否かをチェックする。チェックしていないロールがある場合、ポリシーチェック・修正部１１６は、処理をステップＳ１２０８に移行し、ｊを１だけインクリメントする。そして、処理をステップＳ１２０３に移行する。

【００９８】

また、ステップＳ１２０７において、チェックしていないロールがない場合、ポリシーチェック・修正部１１６は、処理をステップＳ１２０９に移行する。

ステップＳ１２０９において、ポリシーチェック・修正部１１６は、ユーザ－ロール対応表を参照し、チェックすべきユーザＩＤが他にあるか否かをチェックする。チェックすべきユーザＩＤがある場合、ポリシーチェック・修正部１１６は、処理をステップＳ１２１０に移行し、ｉを１だけインクリメントする。そして、処理をステップＳ１２０２に移行する。

【００９９】

また、ステップＳ１２０９において、チェックすべきユーザＩＤがない場合、ポリシーチェック・修正部１１６は、ステップＳ１２１１に移行し、ユーザ－ロール割当てがロール割当て禁止ルールに違反しているかのチェック処理を終了する。

【０１００】

以上の処理により出力される違反リストは表６のようなものになる。例えば、ユーザＩＤがＵ２の場合、Ｒ１とＲ２の同時割当てが禁止されているルールに違反していることを示している。

【０１０１】

【表６】

ユーザID	ロール割当て禁止ルール
U2	R1 , R2
U5	R1 , R5
・・・	・・・

【０１０２】

図１１および１２で詳細したように、ステップＳ１００１およびＳ１００２の処理により、使用されていないユーザ－ロール割当てとロール割当て禁止ルールに違反した割当てが検出される。そして、ポリシーチェック・修正部１１６は、この検出結果から、次表に示すケースの場合分けに応じて、リスク評価値を計算する。なお、表７に示すリスク得点は、これに限定する趣旨でないのは当然である。

【０１０３】

【表７】

No	ケース	リスク	得点
1	違反しているロール禁止割当ての２つのロール両方とも使っている	職務分掌違反であるためリスクは高い	3
2	違反しているロール禁止割当ての２つのロールのうち一つを使っている	違反設定にはなっているが、使用されていないのでリスクは中程度。	2
3	違反しているロール禁止割当ての２つのロール両方とも使っていない	違反しているが、両方のロールとも使っているのでリスクは高い。	1
4	違反割当てにはなっていないが、使われていない	違反はしていないが、使っていないのでリスクは低い	1

ポリシーチェック・修正部１１６は、ステップＳ１００１およびＳ１００２の処理結果を表７に示す分類にしたがって分類し、得点を算出する。

【０１０４】

例えば、表６のユーザＩＤがＵ２の場合、表５に示したロール割当て禁止ルールの番号１に違反していることを示している。一方、表４に示したユーザ－ロール対応表には、Ｕ２に対してＲ１およびＲ５が設定されている。

【０１０５】

すなわち、Ｕ２は、ロール割当て禁止ルールの番号１に規定されているロール（Ｒ１、Ｒ５）のうちの１つのロールを使用している。したがって、ポリシーチェック・修正部１１６は、表７に示すＮｏ．２のケースに該当すると判断し、リスク評価値として得点２を取得する。

【０１０６】

さらに、ポリシーチェック・修正部１１６は、ユーザＩＤ毎に得られた得点の合計値を計算し、表示装置等に出力して一定のフォーマットにしたがって表示する。

図１３は、不適切なユーザ－ロール割当ての検出処理におけるポリシー遵守レベルの表示例を示す図である。本実施例では、ユーザＩＤ毎に、ロール割当て禁止ルールに違反したロール、使用してないロール、違反の説明、リスク点数を表示し、また、その合計点をリスク評価値として表示している（図１３では、リスク評価値が「３９」の場合を示している）。

【０１０７】

３．３　不適切なパーミッション－ロール割当ての検出処理

アクセス権管理において、不適切なパーミッション－ロール割当てがあると、不正なアクセスや、情報漏洩・情報の改ざんの原因となる。そのため、パーミッション－ロール割当ては適切に管理される必要がある。

【０１０８】

本実施例では、アクセス権管理の管理対象であるパーミッション－ロール割当て情報に関し、アクセス権管理の管理対象であるパーミッション－ロール割当て情報を使って、不適切なパーミッション－ロール割当てを、使用していないパーミッション－ロール割当てとパーミッション割当て禁止の違反割当てと定義し、それを検出し、検出結果を、そのリスクの強弱に応じて分類し、得点化することで、ユーザ－ロール割当てを適切に管理する。

【０１０９】

ポリシーチェック・修正部１１６は、監査ログ記憶部１０３から、例えば表２２に示すアクセスログ１４０１を取得する。また、ポリシーチェック・修正部１１６は、ＲＢＡＣポリシー記憶部１１３からから、例えば表２０に示すパーミッション－ロール情報１４０

２を取得する。
【０１１０】
また、ポリシーチェック・修正部１１６は、アクセスログ１４０１とパーミッション－ロール情報１４０２とから使用していないパーミッションを検出する。
そして、ポリシーチェック・修正部１１６は、検出した使用していないパーミッションと、例えば表８に示すあらかじめ設定されたパーミッション割当て禁止ルール１４０３と、に基づいて、不適切なパーミッション－ロール割当てを検出する。そして、ポリシーチェック・修正部１１６は、検出結果を、例えば表１１に示すあらかじめ用意された不適切なパーミッション割当てのリスク得点表１４０４を用いて数値化する。
【０１１１】
本実施例では、不適切なパーミッション－ロール割当てを、
（ａ）「使用されていないパーミッション」∪
（ｂ）「職務分掌上（業務オペレーション上）ロールが同時に持つことが禁止されているパーミッション」
と定義する。
【０１１２】
図１５は、本実施例に係る不適切なパーミッション－ロール割当ての検出処理の概要を示すフローチャートである。
例えば、図３に示したステップＳ３０１において、監査ログ記憶部１０３から例えば表２２に示すアクセスログ１４０１を取得し、ＲＢＡＣポリシー記憶部１１３から例えば表２０に示すパーミッション－ロール情報１４０２を取得すると、ポリシーチェック・修正部１１６は、処理をステップＳ１５０１に移行する。そして、不適切なパーミッション－ロール割当ての検出処理を開始する。
【０１１３】
ステップＳ１５０１において、ポリシーチェック・修正部１１６は、アクセスログ１４０１とパーミッション－ロール情報１４０２から使用していないパーミッションを検出する。
【０１１４】
ステップＳ１５０２において、ポリシーチェック・修正部１１６は、例えば表８に示すあらかじめ設定されたパーミッション割当て禁止ルール１４０３に基づいて、パーミッション－ロール割当てに関するパーミッション割当て禁止違反を検出する。
【０１１５】
ステップＳ１５０３において、ポリシーチェック・修正部１１６は、ステップＳ１５０１およびＳ１５０２における検出結果から、不適切なパーミッション－ロール割当てのリスク得点表１４０４に基づいてリスク評価値を算出する。
【０１１６】
以上の処理が終了すると、ポリシーチェック・修正部１１６は、処理をステップＳ３０４に移行し、ポリシー遵守レベルとして算出したリスク評価値を出力装置等に出力して表示する。
【０１１７】
３．３．１　使用されていないパーミッションの検出処理
「使用されていないパーミッション」の検出処理は、図１１に示した「使用されていないユーザ－ロール割当て」の検出処理と同様の処理によって行なうことができる。この場合、ユーザ情報９０１に替えてパーミッション－ロール情報１４０２を使用し、アクセスログ９０２に替えてアクセスログ１４０１を使用すればよい。
【０１１８】
また、本実施例では、パーミッション割当て禁止ルール１４０３の例として、職務分掌上同時に持つことが禁止されているパーミッションについてのルールを使用する。このルールの例を表８に示す。表８は、職務分掌上同時に持つことが禁止されているパーミッションの組として定義されている。

【０１１９】
例えば、ルール番号１は、パーミッションｐ１とｐ３とを同時に持つことが禁止されていることを示している。
【０１２０】
【表８】

ルール番号	パーミッション割当て禁止
1	p1, p3
2	p2, p4
3	p1, p6
・・・	・・・

【０１２１】
以下では、ＲＢＡＣシステム上において、（ｂ）「職務分掌上（業務オペレーション上）ロールが同時に持つことが禁止されているパーミッション」が設定されているかどうかを検出する処理について説明するが、ＲＢＡＣシステム以外のシステムであっても同様の処理である。
【０１２２】
また、ここで使用するロールとパーミッションの対応表（以下、「ロール－パーミッション対応表」という）の例を以下の表９に示す。表中、「０」は割当てなしを示し、「１」は割当て有りを示す。例えば、Ｒ１は、パーミッションｐ１、ｐ４およびｐ５が割当てられていることを示す。
【０１２３】
【表９】

ロール	p1	p2	p3	p4	p5	p6
R1	1	0	0	1	1	0
R2	0	0	1	0	0	0
R3	0	1	1	1	0	1
・・・	・・・	・・・	・・・	・・・	・・・	・・・

【０１２４】
３．３．２　職務分掌上ロールが同時に持つことが禁止されているパーミッションの検出処理
図１６は、本実施例に係るロールが同時使用禁止のパーミッションを所有しているか否かのチェック処理（ステップＳ１５０２）の具体的な処理を示すフローチャートである。
【０１２５】
ステップＳ１５０１の処理が終了すると、ポリシーチェック・修正部１１６は、処理をステップＳ１６０１に移行し、パーミッション割当て禁止ルール１４０３に違反したパーミッション（ロールが同時所有禁止パーミッション）を所有しているか否かをチェックする処理を開始する。
【０１２６】
ステップＳ１６０１において、ポリシーチェック・修正部１１６は、記憶装置等にあらかじめ記憶されたパーミッション割当て禁止ルール１４０３を取得する。同様に、ポリシーチェック・修正部１１６は、統合ＩＤ管理部１２０などから、例えば表２１に示すロール－ユーザ対応表、例えば表９に示すロール－パーミッション対応表を取得する。
【０１２７】

ステップＳ１６０２において、ポリシーチェック・修正部１１６は、ロール－パーミッション対応表を参照し、チェック対象のロールを特定する。以下、ロール－パーミッション対応表のｉ番目のロールをＲｉとして説明する。

【０１２８】

ステップＳ１６０３において、ポリシーチェック・修正部１１６は、ロール－パーミッション対応表を参照し、Ｒｉに対して割当てられているパーミッションを特定する。以下、ロール－パーミッション対応表において、Ｒｉに対してｊ番目に割当てられているパーミッションをＰｊとする。

【０１２９】

ステップＳ１６０４において、ポリシーチェック・修正部１１６は、ステップＳ１６０１で取得したパーミッション割当て禁止ルール１４０３の同時所有禁止パーミッションリストを参照し、ステップＳ１６０３で特定したパーミッションＰｊが、当該パーミッション割当て禁止ルール１４０３に登録されているか否かをチェックする。

【０１３０】

そして、Ｐｊがパーミッション割当て禁止ルール１４０３に登録されている場合、ポリシーチェック・修正部１１６は、処理をステップＳ１６０５に移行する。

ステップＳ１６０５において、ポリシーチェック・修正部１１６は、パーミッション割当て禁止ルール１４０３にＰｊとともに登録されているパーミッション（以下、「Ｐｊ’」という）を取得する。そして、ポリシーチェック・修正部１１６は、ロール－パーミッション対応表を参照し、Ｒｉ対してパーミッションＰｊ’が割当てられているか否かをチェックする。

【０１３１】

そして、ロール－パーミッション対応表おいて、Ｒｉに対してＰｊ’が割当てられている場合、ポリシーチェック・修正部１１６は、処理をステップＳ１６０６に移行し、違反しているＲｉ、ＰｊおよびＰｊ’を１組のデータとして、記録装置等に記憶する。

【０１３２】

ステップＳ１６０７において、ポリシーチェック・修正部１１６は、ロール－パーミッション対応表を参照し、Ｒｉに対して割当てられているパーミッションであってチェックしていないものがあるか否かをチェックする。チェックしていないパーミッションがある場合、ポリシーチェック・修正部１１６は、処理をステップＳ１６０８に移行し、ｊを１だけインクリメントする。そして、処理をステップＳ１６０３に移行する。

【０１３３】

また、ステップＳ１６０７において、チェックしていないパーミッションがある場合、ポリシーチェック・修正部１１６は、処理をステップＳ１６０９に移行する。

ステップＳ１６０９において、ポリシーチェック・修正部１１６は、ロール－パーミッション対応表を参照し、チェックすべきロールが他にあるか否かをチェックする。チェックすべきロールがある場合、ポリシーチェック・修正部１１６は、処理をステップＳ１６１０し、ｉを１だけインクリメントする。そして、処理をステップＳ１６０２に移行する。

【０１３４】

また、ステップＳ１６０９において、チェックすべきロールがない場合、ポリシーチェック・修正部１１６は、ステップＳ１６１１に移行し、パーミッション割当て禁止ルール１４０３に違反したパーミッション（ロールが同時所有禁止パーミッション）を所有しているか否かをチェックする処理を終了する。

【０１３５】

以上の処理により出力される違反リストは表１０のような結果が得られる。例えば、Ｒ３は、パーミッションｐ２とｐ４の同時割当てが禁止されたルールに違反していることを示している。

【０１３６】

【表１０】

ロール	パーミッション
R3	p2, p4
R5	p6, p12
・・・	・・・
Ri	pj, pj'
・・・	・・・

【０１３７】

以上に説明したように、ステップＳ１５０１およびＳ１５０２の処理により、使用されていないパーミッション割当てとパーミッション割当て禁止ルール１４０３に違反した割当てが検出される。そして、ポリシーチェック・修正部１１６は、この検出結果から、表１１に示すケースの場合分けに応じて、リスク評価を算出する。なお、表１１に示すリスク得点は、これに限定する趣旨でないのは当然である。

【０１３８】

【表１１】

No	ケース	リスク	得点
1	パーミッション割当て禁止ルールのに違反している2つのパーミッション両方とも使っている	職務分掌違反であるためリスクは高い	3
2	パーミッション割当て禁止ルールの違反している2つのパーミッションのうち一つを使っている	違反設定にはなっているが、使用されていないのでリスクは中程度。	2
3	パーミッション割当て禁止ルールの違反している2つのパーミッション両方とも使っていない	違反しているが、両方のロールとも使っているのでリスクは高い。	1
4	違反割当てにはなっていないが、使われていない	違反はしていないが、使っていないのでリスクは低い	1

例えば、表１１に示すケースＮｏ．１は、ステップＳ１５０２の処理によって検出したパーミッション割当て禁止ルール１４０３に違反しているパーミッション（例えば、表１０に示すパーミッション）のうち、２つのパーミッションが両方とも使用されている場合、リスク得点を３とすることを示している。

【０１３９】

さらに、ポリシーチェック・修正部１１６は、ロール毎に得られた得点の合計値を計算し、表示装置等に出力して一定のフォーマットにしたがって表示する。

図１７は、不適切なパーミッション－ロール割当て処理におけるポリシー遵守レベルの表示例を示す図である。本実施例では、ロール毎に、パーミッション割当て禁止ルール１４０３に違反したパーミッション、使用していないパーミッション、違反の説明、リスク点数を表示し、また、その合計点をリスク評価値として表示している（図１７では、リスク評価値が「７」の場合を示している）。

【０１４０】

３．４　不適切なロールの検出処理

ポリシーチェック・修正部１１６は、監査ログ記憶部１０３から例えば表２２に示すアクセスログ１８０１を取得する。また、ポリシーチェック・修正部１１６は、ＲＢＡＣポリシー記憶部１１３から、例えば表２０に示すパーミッション－ロール情報１８０２と、

例えば表１２に示すロール階層情報１８０３と、を取得する。

【０１４１】

そして、ポリシーチェック・修正部１１６は、アクセスログ１８０１、パーミッション－ロール情報１８０２およびロール階層情報１８０３から使用していないロールを検出する。

【０１４２】

そして、ポリシーチェック・修正部１１６は、検出した使用していないロールと、例えば表５に示すロール割当て禁止ルール１８０４と、例えば表８に示すパーミッション割当て禁止ルール１８０５と、に基づいて、不適切なロールを検出する。そして、ポリシーチェック・修正部１１６は、検出結果を、例えば表３に示すあらかじめ用意された不適切なロールのリスク得点表１８０６を用いて数値化する。

【０１４３】

本実施例では、不適切なロールを、

（ａ）「使用されていないロール」∪

（ｂ）「ロール割当て禁止ルールに違反するロール」∪

（ｃ）「パーミッション割当て禁止ルールに違反するロール」

と定義する。

【０１４４】

図１９は、本実施例に係る不適切なロールの検出処理の概要を示すフローチャートである。

例えば、図３に示すステップＳ３０１において、監査ログ記憶部１０３から例えば表２２に示すアクセスログ１８０１を取得し、ＲＢＡＣポリシー記憶部１１３から、例えば表２０に示すパーミッション－ロール情報１８０２と、例えば表１２に示すロール階層情報１８０３と、を取得すると、ポリシーチェック・修正部１１６は、処理をステップＳ１９０１に移行する。そして、不適切なロールの検出処理を開始する。

【０１４５】

ステップＳ１９０１において、ポリシーチェック・修正部１１６は、アクセスログ１８０１とパーミッション－ロール情報１８０２とから使用していないロールを検出する。

ステップＳ１９０２において、ポリシーチェック・修正部１１６は、あらかじめ設定されたロール割当て禁止ルール１８０４に基づいて、ロール階層情報１８０３において当該ルールに違反するロールを検出する。

【０１４６】

ステップＳ１９０３において、ポリシーチェック・修正部１１６は、あらかじめ設定されたパーミッション割当て禁止ルール１８０５に基づいて、当該ルールに違反するロールを検出する。

【０１４７】

ステップＳ１９０４において、ポリシーチェック・修正部１１６は、ステップＳ１９０１、Ｓ１９０２およびＳ１９０３における検出結果から、不適切なロールのリスク点数表１８０６に基づいてリスク評価値を算出する。

【０１４８】

以上の処理が終了すると、ポリシーチェック・修正部１１６は、処理をステップＳ３０４に移行し、ポリシー遵守レベルとして算出されたリスク評価値を出力装置等に出力して表示する。

【０１４９】

３．４．１　使用されていないロールの検出処理

図２０は、本実施例に係る使用されていないロールの検出処理（ステップＳ１９０１）の具体的な処理を示すフローチャートである。

【０１５０】

ステップＳ２００１において、ポリシーチェック・修正部１１６は、パーミッション－ロール情報１８０２を参照し、当該パーミッション－ロール情報１８０２のｉ番目に登録

されているロールＲｊを取得する。

【０１５１】

ステップＳ２００２において、ポリシーチェック・修正部１１６は、アクセスログ１８０１を参照し、ステップＳ２００１で取得したＲｊに対するアクセスログが記録されているか否かをチェックする。そして、Ｒｊに対するアクセスログが記録されていない場合、ポリシーチェック・修正部１１６は、処理をステップＳ２００３に移行する。また、Ｒｊに対するアクセスログが記録されている場合、ポリシーチェック・修正部１１６は、処理をステップＳ２００４に移行する。

【０１５２】

ステップＳ２００３において、ポリシーチェック・修正部１１６は、Ｒｊを使用されていないロールとして、記憶装置等に記憶する。

ステップＳ２００４において、ポリシーチェック・修正部１１６は、パーミッション－ロール情報１８０２を参照し、チェックすべきロールが他にあるか否かをチェックする。そして、チェックすべきロールが他にある場合、ポリシーチェック・修正部１１６は、処理をステップＳ２００５に移行する。そして、ポリシーチェック・修正部１１６は、ｉを１だけインクリメントし、ステップＳ２００１に移行する。

【０１５３】

また、ステップＳ２００４において、チェックすべきロールが他にない場合、ポリシーチェック・修正部１１６は、ステップＳ２００６に移行し、使用されていないロールの検出処理を終了する。

【０１５４】

３．４．２　ロール割当て禁止ルールに違反するロールの検出処理

本実施例に係るロールの構成例を図２１に示す。本実施例に係るロールは、ＮＩＳＴ（Ｎａｔｉｏｎａｌ　Ｉｎｓｔｉｔｕｔｅ　ｏｆ　Ｓｔａｎｄａｒｄ　ａｎｄ　Ｔｅｃｈｎｏｌｏｇｙ）が提案するＲＢＡＣシステムのロール階層を有するロールを使用している。したがって、上位のロールは下位のパーミッションを所有し、下位のロールは上位のロールに所属するユーザがメンバーとなるように定義されている。

【０１５５】

なお、ＮＩＳＴが提案するＲＢＡＣシステムのロール階層については、従来技術なので詳細な説明は省略する。また、以後の説明では、必要に応じて、特定のロールに対して上位のロールを「祖先」、下位のロールを「子孫」という。

【０１５６】

図２１に示したロール階層は、表１２に示すロール階層情報１８０３としてＲＢＡＣポリシー記憶部１１３に記憶される。なお、簡単のために、ＲｉをＲｉと表している。

【０１５７】

【表１２】

senior（親）	junior（子）
－	R7
R7	R5
R7	R6
R5	R1
R5	R2
R6	R3
R6	R4
R1	－
R2	－
R3	－
R4	－

本実施例に係るユーザに対するロール割当て禁止ルール違反の検出処理では、表１２に示したロール階層情報１８０３から、表５のしたロール割当て禁止ルールに違反するロールを検出する。

【０１５８】

検出すべきロールを図２２に示す。すなわち、ロール割当て禁止ルール１８０４に定義されている２つのロールの組が、子孫－祖先の関係であるようなものを検出する。例えば、図２２に示すＲｏｌｅＡ、ＲｏｌｅＢである。

【０１５９】

これは、ＮＩＳＴが提案するロール階層の定義では、上位のロールは、下位のパーミッションを継承するので、上位ロールは下位ロールのパーミッションを含んでしまう。したがって、この２つのロールがロール割当て禁止ルール１８０４に違反するロールであれば、上位のロール（または、上位のロールよりさらに上位のロール）に人を割当てることができなくなる 。人が割当てられないロールに意味はないので、このようなロールをロール割当て禁止ルール１８０４に違反するロールとして検出する。

【０１６０】

また、図２２に示すように、子孫－祖先の関係にないＲｏｌｅＣ、ＲｏｌｅＤは、ロール割当て禁止ルール１８０４に違反しないロールとする。

本実施例に係るロール割当て禁止ルールに違反するロールの検出処理は、ロールの同時割当て禁止ルールで定義されるロールの組みの１つのロールについて、ロール階層木を走査し、そのロールを基準に子孫、および祖先にもう一つのロールが存在するかをチェックする。

【０１６１】

図２３は、本実施例に係るロール割当て禁止ルールに違反するロールの検出処理（ステップＳ１９０２）の具体的な処理を示すフローチャートである。

ステップＳ２３０１において、ポリシーチェック・修正部１１６は、ロール割当て禁止ルール１８０４を参照し、ｉ番目に登録されているロールＲｉｌ、Ｒｉｍを取得する。

【０１６２】

ステップＳ２３０２において、ポリシーチェック・修正部１１６は、ロール階層情報１８０３を参照し、ステップＳ２３０１で取得したＲｉｌについてロール階層木を操作して

検索する。

【０１６３】

ステップＳ２３０３において、ポリシーチェック・修正部１１６は、Ｒｉｌの子孫にＲｉｍが存在するか否かをチェックする。そして、Ｒｉｌの子孫にＲｉｍが存在する場合、ポリシーチェック・修正部１１６は、処理をステップＳ２３０５に移行する。

【０１６４】

ステップＳ２３０４において、ポリシーチェック・修正部１１６は、Ｒｉｌの祖先にＲｉｍが存在するか否かをチェックする。そして、Ｒｉｌの祖先にＲｉｍが存在する場合、ポリシーチェック・修正部１１６は、処理をステップＳ２３０５に移行する。

【０１６５】

ステップＳ２３０５において、ポリシーチェック・修正部１１６は、ステップＳ２３０３またはＳ２３０４の処理によってＲｉｍを検出すると、該当するロール割当て禁止ルール１８０４のルール番号ｉ、ロールＲｉｌおよびＲｉｍを、記憶装置等に記憶する。

【０１６６】

ステップＳ２３０６において、ポリシーチェック・修正部１１６は、ロール割当て禁止ルール１８０４を参照し、チェックすべきルールが他にあるか否かをチェックする。そして、チェックすべきルールが他にある場合、ポリシーチェック・修正部１１６は、処理をステップＳ２３０７に移行する。そして、ポリシーチェック・修正部１１６は、ｉを１だけインクリメントし、処理をステップＳ２３０１に移行する。

【０１６７】

一方、ステップＳ２３０６において、チェックすべきロールが他にない場合、ポリシーチェック・修正部１１６は、ロール階層からロール割当て禁止ルールに違反しているロールの検出処理を終了する。例えば、表１３に示すような結果が得られる。

【０１６８】

【表１３】

ルール番号	ロール割当て禁止ルール
1	R1 , R5
4	R1 , R7
・・・	・・・

【０１６９】

３．４．３　パーミッション割当て禁止ルールに違反するロールの検出処理

本実施例に係るパーミッション割当て禁止ルールに違反するロールの検出処理では、例えば表１２に示したロール階層情報１８０３から親子関係にあるロールを抽出し、例えば表２３に示すロール－パーミッション対応表から、該当するロールのパーミッションを取得する。

【０１７０】

そして、取得したパーミッションが、例えば表８に示すパーミッション割当て禁止ルール１８０５に違反しているか否かをチェックする。具体的には、後述するように、ロール階層木の中で親子関係にあるＲｉとＲｊの各々が持つパーミッションが違反しているかをチェックする。そして、例えば表１４に示すように、違反しているパーミッション割当て禁止ルールを出力する。

【０１７１】

ここで、パーミッション割当て禁止ルールに違反するロールについて、以下に示す（１）～（４）の場合が考えられる。

（１）ロールＲｉとＲｊがともにパーミッション割当て禁止ルールに違反している場合

図２４は、ロールＲｉとＲｊがともにパーミッション割当て禁止ルールに違反している場合のロール階層について説明する図である。図２４に示すロール階層は、パーミッショ

ンｐｉおよびｐｊに関し、（ｐｉ∈Ｒｉ）かつ（ｐｊ∈Ｒｉ）の関係にあるＲｉと、（ｐｉ∈Ｒｉ）かつ（ｐｊ∈Ｒｉ）の関係にあるＲｊと、が親子関係にある場合を示している。

【０１７２】

例えば、パーミッション割当て禁止ルール１８０５のルール番号ｋのルールに、ｐｉとｐｊの同時割当て禁止が定義されていた場合、ポリシーチェック・修正部１１６は、当該ルールに違反するＲｉの子孫であるＲｊがロール階層木の葉であるかをチェックし、葉である場合Ｒｊがルール違反の原因の１つと判断する。

【０１７３】

したがって、図２４に示すロール階層の場合、ＲｉとＲｊはいずれもパーミッション割当て禁止ルール１８０５に違反すると判断する。また、Ｒｊが葉でない場合、ポリシーチェック・修正部１１６は、Ｒｊの子孫について同様のチェックを行なう。

【０１７４】

（２）ロールＲｉがパーミッション割当て禁止ルールに違反し、Ｒｊが違反していない場合

図２５は、ロールＲｉがパーミッション割当て禁止ルールに違反し、Ｒｊが違反していない場合のロール階層について説明する図である。図２５に示すロール階層は、パーミッションｐｉおよびｐｊに関し、（ｐｉ∈Ｒｉ）かつ（ｐｊ∈Ｒｉ）の関係にあるＲｉと、（ｐｉ∈Ｒｉ）でも（ｐｊ∈Ｒｉ）でもないＲｊと、が親子関係にある場合を示している。

【０１７５】

例えば、パーミッション割当て禁止ルール１８０５のルール番号ｋのルールに、ｐｉとｐｊの同時割当て禁止が定義されていた場合、Ｒｉはパーミッション割当て禁止ルールに違反し、Ｒｊは違反しないと判断する。

【０１７６】

ここで、Ｒｊにおけるパーミッションとの関係は、以下に示す（ａ）～（ｃ）の３つの場合が考えられる。

（ａ）「Ｒｊがｐｉを所有し」、　かつ、「Ｒｊがｐｊを所有しない」

（ｂ）「Ｒｊがｐｉを所有しない」、かつ、「Ｒｊがｐｊを所有する」

（ｃ）「Ｒｊがｐｉを所有しない」、かつ、「Ｒｊがｐｊを所有しない」

（ａ）または（ｂ）の場合、Ｒｊがルール違反の原因の１つと考えられる。これは、ＲＢＡＣシステムのロール階層構造において、Ｒｊに割当てられているルール違反のパーミッションｐｉまたはｐｊを取り除けば、当該ｐｉまたはｐｊを親のＲｉからも取り除いてルール違反を解消することができるからである。

【０１７７】

例えば、図２６に示すように、Ｒｊにｐｊが割当てられていた場合、Ｒｊからｐｊを削除することにより、Ｒｊの祖先（Ｒｎ、Ｒｎ＋１、・・・、Ｒｉ）のうちルールに違反するロールＲｉとＲｎからｐｊを削除することが可能となり、ＲｉとＲｎのルール違反を解消することができる。

【０１７８】

また、（ｃ）の場合、Ｒｊ（または、Ｒｊより下位の部分木）がルール違反の原因ではないので、Ｒｊの親であるＲｉ、または、Ｒｊ以外のＲｉの子孫にルール違反の原因があると考えられる。

この場合、図２７に示すパーミッション違反の原因の範囲２７０１について、パーミッション割当て禁止ルール１８０５に違反するパーミッションのチェックを行なう。

【０１７９】

（３）ＲｉおよびＲｊがパーミッション割当て禁止ルールに違反していない場合、

この場合、違反がないのでロールに対するパーミッション割当てに問題はないと判断することができる。

【０１８０】

（４）ロールＲｉがパーミッション割当て禁止ルールに違反せず、Ｒｊが違反している場合

この場合、のＲＢＡＣシステムの仕様に違反していると判断することができる。

【０１８１】

図２８は、本実施例に係るパーミッション割当て禁止ルールに違反するロールを検出する処理である。

ステップＳ２８０１において、ポリシーチェック・修正部１１６は、パーミッション割当て禁止ルール１８０５を参照し、当該パーミッション割当て禁止ルールのｉ番目のルールに登録されているパーミッションｐｉｌおよびｐｉｍを取得する。

【０１８２】

ステップＳ２８０２において、ポリシーチェック・修正部１１６は、ロール階層情報１８０３を参照し、ルート階層木のルートを取得する。そして、ポリシーチェック・修正部１１６は、パーミッション－ロール情報１８０２を参照し、当該ルートのロールに対してｐｉｌまたはｐｉｍが割当てられているか否かをチェックする。

【０１８３】

ルートのロールに対してｐｉｌまたはｐｉｍが割当てられていない場合、ポリシーチェック・修正部１１６は、パーミッション割当て禁止ルール１８０５に違反するロールはないと判断し、処理をステップＳ２８０３に移行する。

【０１８４】

ステップＳ２８０３において、ポリシーチェック・修正部１１６は、パーミッション割当て禁止ルール１８０５を参照し、他にチェックすべきルールがあるか否かをチェックする。他にチェックすべきルールがある場合、ポリシーチェック・修正部１１６は、処理をステップＳ２８０４に移行する。そして、ｉを１だけインクリメントし、処理をステップＳ２８０１に移行する。

【０１８５】

また、ステップＳ２８０３において、他にチェックすべきルールがない場合、ポリシーチェック・修正部１１６は、処理をステップＳ２８１５に移行し、パーミッション割当て禁止ルールに違反するロールを検出する処理を終了する。

【０１８６】

一方、ステップＳ２８０２において、ルートのロールに対してｐｉｌまたはｐｉｍが割当てられている場合、ポリシーチェック・修正部１１６は、ルートのロールがパーミッション－ロール情報１８０２に違反していると判断し、処理をステップＳ２８０５に移行する。

【０１８７】

ステップＳ２８０５において、ポリシーチェック・修正部１１６は、ロール階層を深さ優先し、親ロールＲｉａがパーミション違反し、かつ、子ロールＲｉｂがパーミッション違反していないＲｉａ、Ｒｉｂまでロール階層を走査する。そして、違反しているロールと、違反しているルール番号、違反しているパーミッションを違反リストに記憶する。

【０１８８】

ステップＳ２８０６において、ポリシーチェック・修正部１１６は、Ｒｉｂに対してｐｉｌとｐｉｍの両方とも割当てられていないか否かを確認する。Ｒｉｂに対してｐｉｌとｐｉｍの両方とも割当てられていない場合、ポリシーチェック・修正部１１６は、処理をステップＳ２８０７に移行する。

【０１８９】

ステップＳ２８０７において、ポリシーチェック・修正部１１６は、親ロールＲａｉに他の未調査のロールがあるか否かを確認する。他の未調査のロールがある場合、ポリシーチェック・修正部１１６は、処理をステップＳ２８０８に移行する。

【０１９０】

ステップＳ２８０８において、ポリシーチェック・修正部１１６は、Ｒｉａをルートとするサブツリー（例えば、図２７に示したパーミッション違反の原因の範囲２７０１）を

操作対象にセットする。そして、処理をステップＳ２８０３に移行する。

【０１９１】

また、ステップＳ２８０７において、他の未調査のロールがない場合、ポリシーチェック・修正部１１６は、処理をステップＳ２８０９に移行する。

ステップＳ２８０９において、ポリシーチェック・修正部１１６は、ルール番号ｉと、Ｒｉａと、Ｒｉａに割当てられたルールに違反したｐｉｌ、ｐｉｍを違反リストに記憶する。そして、処理をステップＳ２８１０に移行する。

【０１９２】

ステップＳ２８１０において、ポリシーチェック・修正部１１６は、Ｒｉａの親ロールは、ルートのロールか否かをチェックする。そして、Ｒｉａの親ロールがルートのロールである場合、ポリシーチェック・修正部１１６は、処理をステップＳ２８０３に移行する。また、Ｒｉａの親ロールがルートのロールでない場合、ポリシーチェック・修正部１１６は、処理をステップＳ２８１１に移行する。

【０１９３】

ステップＳ２８１１において、ポリシーチェック・修正部１１６は、Ｒｉａの親ロールをＲｉａにセットする。そして、ポリシーチェック・修正部１１６は、処理をステップＳ２８１３に移行する。

【０１９４】

一方、ステップＳ２８０６において、Ｒｉｂに対してｐｉｌまたはｐｉｍが割当てられている場合、ポリシーチェック・修正部１１６は、処理をステップＳ２８１２に移行する。

【０１９５】

ステップＳ２８１２において、ポリシーチェック・修正部１１６は、ルール番号ｉと、Ｒｉｂと、Ｒｉｂに割当てられたルールに違反したパミッション（ｐｉｌまたはｐｉｍ）を違反リストに記憶する。そして、処理をステップＳ２８１３に移行する。

【０１９６】

ステップＳ２８１３において、ポリシーチェック・修正部１１６は、親ロールＲａｉについて他に未調査の子ロールがあるか否かをチェックする。おして、他に未調査の子ロールがある場合、ポリシーチェック・修正部１１６は、処理をステップＳ２８１４に移行する。

【０１９７】

ステップＳ２８１４において、ポリシーチェック・修正部１１６は、Ｒａｉをルートとするサブセットを操作対象にセットし、処理をステップＳ２８０５に移行する。

以上の処理によって、パーミッション割当て禁止ルールに違反するロールについて、表１４に示すような結果が得られる。

【０１９８】

【表１４】

違反しているルール番号	違反の原因となっているロール	違反の原因となっているパーミッション
3	Ri	P3i, P3j
3	Rj	P3i, P3j
・・・	・・・	・・・
5	Rj	P5i
・・・	・・・	・・・

以上に説明したように、ステップＳ１９０１、Ｓ１９０２およびＳ１９０３の処理から、使われていないロール、違反しているユーザーロール割当て（例えば、表１３）、違反

しているロール－パーミッション割当て（例えば、表１４）が検出される。ポリシーチェック・修正部１１６は、この検出結果から次表に示すケースの場合分けに応じて、リスク評価を算出する。なお、表１５に示すリスク得点は、これに限定する趣旨でないのは当然である。

【０１９９】

【表１５】

No	ロールの使用	ロール割当て禁止設定違反	パーミッション割当て禁止設定		説明	リスク得点
			設定違反	設定違反原因※		
1	未使用	－	－	－	違反はしていないが、使っていないため、リスクは低い。	1
2	未使用	－	－	原因	違反はしていないが、上位ロールの設定違反の原因となっているため、リスクは中程度。	2
3	未使用	－	違反	－	パーミッションの割当て違反をしているので、リスクは高い	3
4	未使用	－	違反	原因	このパーミッションの割当てが原因で違反をしている。	3
5	未使用	違反	－	－	ロール割当て設定違反をしている	3
6	未使用	違反	－	原因	ロール割当て禁止違反はしているが、パーミッション割当て違反はしていないが、上位ロールのパーミッション割当て違反の原因になっている。 ただしロールは使っていない。	3
7	未使用	違反	違反	－	ロール割当、パーミッション割当て両方とも違反をしている。ただしロールは使っていない。	4
8	未使用	違反	違反	原因	ロール割当、パーミッション割当て両方とも違反をしている。さらに、パーミッション割当ては、上位のロールの違反原因になっている。 ただしロールは使っていない。	4
9	使用	－	－	－	ロールが使われている。	0
10	使用	－	－	原因	違反はしていないが、上位ロールの設定違反の原因となっているため、リスクは中程度。	2
11	使用	－	違反	－	パーミッションの割当て違反をしており、さらに使用されているためリスクは高い	4
12	使用	－	違反	原因	このパーミッションの割当てが原因で違反をしており、さらに使用されている。	4
13	使用	違反	－	－	ロール割当て設定違反をしており、さらに使用されている。	4
14	使用	違反	－	原因	ロール割当て禁止違反はしているが、パーミッション割当て違反はしていないが、上位ロールのパーミッション割当て違反の原因になっている。 さらにそのロールを使用している。	4
15	使用	違反	違反	－	ロール割当、パーミッション割当て両方とも違反をしている。さらにそのロールを使用している。	5
16	使用	違反	違反	原因	ロール割当、パーミッション割当て両方とも違反をしている。さらに、パーミッション割当ては、上位のロールの違反原因になっている。 さらにそのロールを使用している。	5

なお、表１５において、ロールに割当てられているパーミッション設定が原因で、そのロール自身の設定が違反となっている場合、または、そのロール自身は違反していないが、そのロールの上位ロールのパーミッション割当てが違反となっている場合、を設定違反の”原因”としている。

【０２００】
さらに、ポリシーチェック・修正部１１６は、ロール毎に得られた得点の合計を計算し、法事装置等に出力して一定のフォーマットにしたがって表示する。
図２９は、不適切なロールの検出処理におけるポリシー遵守レベルの表示例を示す図である。本実施例では、ロール毎に、ロールの使用／未使用、ロール割当て禁止ルール１８０４で禁止されるロール、パーミッション割当て禁止ルール１８０５で禁止されるパーミッション、違反の説明、リスク点数を表示し、また、その合計点をリスク評価値として表示している（図２９では、リスク評価値が「７２」の場合を示している）。
【０２０１】
３．５　職務分掌違反の検出処理
アクセス権管理の中で、職務分掌に違反しているような不適切な設定があると、不正なアクセスや、情報漏洩・情報の改ざんの原因となる。そのため、アクセス権の設定を適切に管理する必要がある。
【０２０２】
本実施例では、例えば表５に示したロール割当て禁止ルール３００１と、例えば表８に示したロールに対するパーミッション割当て禁止ルール３００２と、後述するユーザに対するパーミッション割当て禁止ルール３００３と、を利用して職務分掌ルールを定義し、アクセス権設定情報（ユーザ－ロール割当て情報、パーミッション－ロール割当て情報）の中から、ルール違反を検出することによりアクセス権の設定を適切に管理する。
【０２０３】
本実施例では、職務分掌ルールを、
（ａ）「ユーザに対するロール割当て禁止ルールに違反する割当て」∪
（ｂ）「ロールに対するパーミッション割当て禁止ルールに違反する割当て」∪
（ｃ）「ユーザに対するパーミッション割当て禁止ルールに違反する割当て」
と定義する。
【０２０４】
なお、（ａ）「ユーザに対するロール割当て禁止ルールに違反する割当て」の検出処理、（ｂ）「ロールに対するパーミッション割当て禁止ルールに違反する割当て」の検出処理は、それぞれ既に２．２および２．３で説明しているので省略する。
【０２０５】
３．５．１　ユーザに対するパーミッション割当て禁止ルールに違反する割当ての検出処理
ポリシーチェック・修正部１１６は、ＲＢＡＣポリシー記憶部１１３からパーミッション－ロール情報３００１を読み出し、統合ＩＤ管理部１２０からユーザ情報３００２を読み出す。なお、パーミッション－ロール情報３００１とは、例えば、表９に示したロール－パーミッション対応表であり、ユーザ情報３００２とは、例えば、表２１に示すロール－ユーザ対応表である。
【０２０６】
そして、ポリシーチェック・修正部１１６は、パーミッション－ロール情報３００１とユーザ情報３００２とから、例えば、表１６に示すユーザ毎のパーミッションリスト（ＡＣＬ）を作成する。そして、ポリシーチェック・修正部１１６は、ＡＣＬについて、例えば表１７に示すパーミッション割当て禁止ルールに基づいて、ユーザに対するパーミッション割当て禁止ルールに違反する割当てを検出する。
【０２０７】

【表１６】

ユーザID	p1	p2	p3	p4	p5
U1	1	0	0	1	1
U2	1	1	0	1	1
U3	0	1	1	0	1
・・・	・・・	・・・	・・・	・・・	・・・

【０２０８】

【表１７】

ルール番号	割当て禁止パーミッション
1	p2, p4
2	p3, p8
3	p7, p8
・・・	・・・

【０２０９】

図３１は、本実施例に係る職務分掌違反の検出処理の概要を示すフローチャートである。

例えば、図３に示したステップＳ３０１において、ＲＢＡＣポリシー記憶部１１３からパーミッション－ロール情報３００１を取得し、統合ＩＤ管理部１２０からユーザ情報３００２を取得すると、ポリシーチェック・修正部１１６は、処理をステップＳ３１０１に移行する。そして、職務分掌違反の検出処理を開始する。

【０２１０】

ステップＳ３１０１において、ポリシーチェック・修正部１１６は、あらかじめ設定されたロール割当て禁止ルール９０３に基づいて、ユーザ－ロール割当てに関するロール割当て禁止違反を検出する。

【０２１１】

ステップＳ３１０２において、ポリシーチェック・修正部１１６は、ポリシーチェック・修正部１１６は、あらかじめ設定されたロールに対するパーミッション割当て禁止ルール１４０３に基づいて、ロールに対するパーミッション－ロール割当てに関するパーミッション割当て禁止違反を検出する。

【０２１２】

ステップＳ３１０３において、ポリシーチェック・修正部１１６は、パーミッション－ロール情報３００１とユーザ情報３００２とから、ユーザ毎のパーミッションリスト（ＡＣＬ）を作成する。

【０２１３】

ステップＳ３１０４において、ポリシーチェック・修正部１１６は、あらかじめ設定されたユーザに対するパーミッション割当て禁止ルールに基づいて、ユーザに対するパーミッション－ユーザ割当てに関するパーミッション割当て禁止違反を検出する。

【０２１４】

ステップＳ３１０５において、ポリシーチェック・修正部１１６は、ステップＳ３１０１、Ｓ３１０２およびＳ３１０４における検出結果について、リスク得点を設定する。

以上の処理が終了すると、ポリシーチェック・修正部１１６は、処理をステップＳ３０４に移行し、ポリシー遵守レベルとして設定したリスク評価値を出力装置等に出力して表

示する。

【０２１５】

図３２は、本実施例に係るＡＣＬの作成処理を示すフローチャートである。

ステップＳ３２０１において、ポリシーチェック・修正部１１６は、ロール－ユーザ対応表を参照し、ロール－ユーザ対応表のユーザＩＤ毎にソートし、ユーザＩＤ毎にユーザが所属するロールのリストを作成する。

【０２１６】

ステップＳ３２０２において、ポリシーチェック・修正部１１６は、以降の処理の対象となるユーザＩＤとしてＵｉをセットする。

ステップＳ３２０３において、ポリシーチェック・修正部１１６は、Ｕｉが所属する全てのロールが持つパーミッションをユーザに割当ててＡＬＣに記憶する。例えば、表１６において、Ｕ１はパーミッションｐ１、ｐ４およびｐ５が割当てられる。

【０２１７】

ステップＳ３２０４において、ポリシーチェック・修正部１１６は、ステップＳ３２０１で生成したリストを参照し、チェックすべきユーザが他に存在するか否かをチェックする。チェックすべきユーザＩＤが他に存在する場合、ポリシーチェック・修正部１１６は、処理をステップＳ３２０５に移行する。そして、ｉを１だけインクリメントして処理をステップＳ３２０２に移行する。

【０２１８】

また、ステップＳ３２０４において、チェックすべきユーザＩＤが他に存在しない場合、ポリシーチェック・修正部１１６は、ステップＳ３２０６に移行し、ＡＣＬの作成処理を終了する。

【０２１９】

図３３は、本実施例に係るユーザに対するパーミッション割当て禁止ルールに違反する割当ての検出処理を示すフローチャートである。

ステップＳ３３０１において、ポリシーチェック・修正部１１６は、ＡＣＬを参照し、以降の処理対象のユーザＩＤをＵｉにセットする。さらに、ステップＳ３３０２において、ポリシーチェック・修正部１１６は、ＡＣＬを参照し、以降の処理対象を、ＵｉのパーミッションＰｊにセットする。

【０２２０】

ステップＳ３３０３において、ポリシーチェック・修正部１１６は、ユーザに対するパーミッション割当て禁止ルール３００３を参照し、Ｐｊが当該ルールに登録されている同時所有禁止のパーミッションとして登録されているか否かをチェックする。

【０２２１】

Ｐｊが同時所有禁止のパーミッションとして登録されている場合、ポリシーチェック・修正部１１６は、処理をステップＳ３３０４に移行する。

ステップＳ３３０４において、ポリシーチェック・修正部１１６は、ユーザに対するパーミッション割当て禁止ルール３００３を参照し、Ｐｊと対で登録されているパーミッションＰｊ’を取得する。そして、ポリシーチェック・修正部１１６は、ＡＣＬを参照し、Ｕｉに対してＰｊ’が登録されているか否かをチェックする。

【０２２２】

Ｕｉに対してＰｊ’が登録されている場合、ポリシーチェック・修正部１１６は、処理をステップＳ３３０５に移行する。そして、違反しているＵｉ、ＰｊおよびＰｊ’を１組のデータとして記憶装置等に記憶する。

【０２２３】

ステップＳ３３０６において、ポリシーチェック・修正部１１６は、ＡＬＣを参照する。そして、Ｕｉに対して他にパーミッションが登録されているか否かをチェックする。他にパーミッションが登録されている場合、ポリシーチェック・修正部１１６は、処理をステップＳ３３０７に移行する。そして、ｊを１だけインクリメントして処理をステップＳ３３０２に移行する。

【０２２４】
また、ステップＳ３３０６において、他にパーミッションが登録されていない場合、ポリシーチェック・修正部１１６は、処理をステップＳ３３０８に移行する。
ステップＳ３３０８において、ポリシーチェック・修正部１１６は、ＡＣＬを参照し、チェックすべきユーザが他に存在するか否かをチェックする。チェックすべきユーザが他に存在する場合、ポリシーチェック・修正部１１６は、処理をステップＳ３３０９に移行する。そして、ｉを１だけインクリメントして処理をステップＳ３３０１に移行する。
【０２２５】
また、ステップＳ３３０８において、チェックすべきユーザが他に存在しない場合、ポリシーチェック・修正部１１６は、ステップＳ３３１０に移行し、ユーザに対するパーミッション割当て禁止ルール３００３に違反する割当ての検出処理を終了する。
【０２２６】
以上の処理によって、例えば、表１８に示すユーザ－パーミッション割当てリストが得られる。
【０２２７】
【表１８】

ユーザ	パーミッション
U2	p2, p4
U7	p3, p8
・・・	・・・
Ui	pj, pj'
・・・	・・・

【０２２８】
以上に説明したようにステップＳ３１０１、Ｓ３１０２およびＳ３１０４による検出結果え得ると、ポリシーチェック・修正部１１６は、その検索結果に対して各々に点数を設定してリスクの計算をできるようにする。
【０２２９】
本処理で得られた検出結果は、どれも高いリスクのものであると考えられるため、本実施例では検出結果それぞれのリスク得点を３点としている。そして、ポリシーチェック・修正部１１６は、その合計値を計算し、表示装置等に出力して一定のフォーマットにしたがって表示する。
【０２３０】
図３４は、職務分掌違反の検出処理におけるポリシー遵守レベルの表示例を示す図である。本実施例では、違反ルール種別（ロールに対するパーミッション割当て禁止ルール３００２またはユーザに対するパーミッション割当て禁止ルール３００３）、違反ユーザ、ロール割当て禁止ルール１８０４による割当て禁止ロール、違反したロール、パーミッション割当て禁止ルール３００２若しくは３００３による割当て禁止パーミッション、違反の説明、リスク点数を表示し、また、その合計点をリスク評価値として表示している（図３４では、リスク評価値が「８４」の場合を示している）。
【０２３１】
４．１　ポリシー遵守レベルの測定方法
上述した３．１から３．５までの検出までの検出方法およびリスクの得点化を利用して、システムのポリシー遵守レベルの測定方法について説明する。以下の手順を踏むことで、ユーザ数やアクセス権設定情報数が異なるシステム同士でも比較可能なリスクの総合点を計算できるようになる。
【０２３２】

４．１．１　不適切なユーザアカウント

各システムの利用者数（表２のようなユーザリストのユーザ数）で割ることで、システム間の数値を比較できるようにしておく。これにより、ここの値域は０から４の間の実数となる。

【０２３３】

４．１．２　不適切なユーザ－ロール割当て

入力となるユーザ－ロール対応表のサイズをｍ（ｍは１以上の自然数）とし（ただし、サイズとは行数のことをいう）、ユーザ数をｎ（ｎは１以上の自然数）とし、ロール割当て禁止ルール数をｋ（ｋは１以上の自然数）とした場合、３．２で説明した計算結果を取りえる違反数ｍ＋ｋ＊ｎで割ることでシステム間で数値を比較可能にする。図３５は、ユーザ－ロール対応表の例を示す。

【０２３４】

４．１．３　不適切なパーミッション－ロール割当て

入力となるロールとパーミッションの対応表のサイズをｑ（ｑは１以上の自然数）とし（ただし、サイズとは行数のことをいう）、ロール数をｒ（ｒは１以上の自然数）とし、パーミッション割当て禁止ルール数をｌ（ｌは１以上の自然数）とした場合、３．３で説明した計算結果を取り得る違反数ｑ＋ｌ＊ｒで割ることでシステム間で数値を比較可能にする。図３６は、ロール－パーミッション対応表の例を示す。

【０２３５】

４．１．４　不要なロール

入力となるロールとパーミッションの対応表のサイズをｑ（ｑは１以上の自然数）とすし（ただし、サイズとは行数のことをいう）、ロール数をｒとし、ロール割当て禁止ルール数ｋとし、パーミッション割当て禁止ルール数をｌとした場合、出力結果を取りえる違反数ｒ＋ｋ＊ｒ＋ｌ＊ｒで割ることでシステム間での数値比較を可能にする。

【０２３６】

４．１．５　職務分掌違反

ユーザ数をｎとし、ロール割当て禁止ルール数をｋとし、ロール数をｒとし、パーミッション割当て禁止ルール数をｌとし、ユーザへのパーミッション割当て禁止ルール数をｓ（ｓは１以上の自然数）とした場合、３．５で説明した計算結果取りえる違反数をｋ＊ｎ＋ｌ＊ｒ＋ｓ＊ｎで割ることで、システム間で数値比較可能にする。

【０２３７】

４．２　アクセス権管理の総合評価値の計算方法

アクセス権管理における総合的な評価値を、上記４．１．１から４．１．５までの結果の和をとることで、管理の徹底度合いを比較することができる。また、次のような重み付けをして和を計算することも可能である。

【０２３８】

総合管理評価値 ＝ Ｋ１×ａ／４＋Ｋ２×ｂ／３＋Ｋ３×ｃ／１＋Ｋ４×ｄ／３＋Ｋ５×ｅ／３

ただし、Ｋ１、Ｋ２、Ｋ３、Ｋ４およびＫ５は係数、ａは不適切なユーザアカウントのリスク評価値、ｂは不適切なユーザ－ロール割当てのリスク評価値、ｃは不要なロールのリスク評価値、ｄは不適切なパーミッション－ロール割当てのリスク評価値、ｅは職務分掌違反のリスク評価値とする。

【０２３９】

例えば、｛Ｋ１，Ｋ２，Ｋ３，Ｋ４，Ｋ５｝＝｛３，２，１，２，３｝として場合、表１９が得られる。

【０２４０】

【表１９】

	a.不適切なユーザアカウント	b. 不適切なユーザ-ロール割当て	c. 不要なロール	d. 不適切なパーミッション-ロール割当て	e. 職務分掌違反	アクセス権管理の総合管理評価値
サーバA	1.2	1.5	0.3	2.1	1.5	5.1
サーバB	3	2	0.4	1.7	1.2	6.3
・・・	・・・	・・・	・・・	・・・	・・・	・・・

【０２４１】

図３７は、サーバ毎のポリシー遵守レベルの計測結果の画面の構成例を示している。

また、図３７に示した画面の「詳細」ボタンを押下することにより、各システムの詳細な情報を表示することも可能である。図３８には、「詳細」ボタンを押下したときに表示される各システムのポリシー遵守レベル評価結果の画面を示している。

さらに、上記の画面では「月間推移表示」ボタンを押下したときに、図３９に示す各項目のリスク値の推移を表示してもよい。

【０２４２】

５．　アクセス権設定に無駄がないかのチェック方法

アクセス権設定の中に、設定はされているが使われていないアクセス権情報がある。これは、セキュリティの最小特権の原理や管理コストの観点から不要と考えられる。以下、このような無駄な設定を検出する方法を説明する。

【０２４３】

図４０は、無駄なアクセス権設定を検出する場合の構成例の概要を示している。

ポリシーチェック・修正部１１６は、ＲＢＡＣポリシー記憶部１１３から、例えば表２０に示すパーミッション－ロール情報を、統合ＩＤ管理部１２０から例えば表２１に示すロール－ユーザ対応表を、監査ログ記憶部１３０から例えば表２２に示すアクセスログを取得し、以下で説明する検出方法を用いて、以下の２つを検出する。

【０２４４】

（ａ）ユーザやロールに設定された使われていないパーミッション割当て

（ｂ）使用されていないロール

検出方法としては、アクセスログを利用する。（ａ）については、ユーザやロールに与えられているが使用されていないアクセス権を検出する。（ｂ）については、使われていないロールを検出する。これらを検出することで、無駄なアクセス権設定が存在するかチェックする。

【０２４５】

５．１　使われていないユーザやロールに設定されたパーミッション

ここでは、使用されていないユーザやロールに設定されたパーミッションを検出する方法を説明する。アクセス権の設定情報は、表２０、表２１に示すようなデータとなっている。また、アクセスログには、表２２に示す情報が得られるものとする。

【０２４６】

【表２０】

ロール	リソース	アクション
R1	X1	r
R1	X2	r
R1	X3	r/w
・ ・ ・	・ ・ ・	・ ・ ・
R2	Y1	r
・ ・ ・	・ ・ ・	・ ・ ・

【０２４７】

【表２１】

ロール	ユーザID(UID)
R1	taro
R1	jiro
R1	hanako
・ ・ ・	・ ・ ・
R2	maeda
・ ・ ・	・ ・ ・

【０２４８】

【表２２】

日時	主体		場所	リソース	アクション	アクセス制御結果
	UID	ロール				
2008/03/26/1200	taro	R1	server1	X1	write	deny
2008/03/26/0903	taro	R1	server1	X3	write	allow
・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・

なお、対象となるアクセスログの期間としては、例えば１ヶ月、４半期、半期などある程度の時間間隔のログ情報を利用することが望ましい。

【０２４９】

図４１は、ユーザやロールに設定された使用されていないパーミッションの検出処理を示すフローチャートである。なお、パーミッションは、リソースとアクションとで構成さ

れた１組の情報である。

【０２５０】

ステップＳ４１０１において、ポリシーチェック・修正部１１６は、ＲＢＡＣポリシー記憶部１１３からアクセス権設定情報を取得し、監査ログ記憶部１３０からアクセスログを取得する。

【０２５１】

ステップＳ４１０２において、ポリシーチェック・修正部１１６は、アクセス権設定情報を参照し、当該アクセス権設定情報に登録されているｉ番目のロールＲｉを以降の処理対象にセットする。なお、以降の処理では、説明を簡単にするために表２０の表現を変えた表２３を使用する。

【０２５２】

【表２３】

ロール	パーミッション
R1	P11
R1	P12
R1	P13
・ ・ ・	・ ・ ・
Ri	Pi1
・・・	・・・
Ri	Pij
・ ・ ・	・ ・ ・

ステップＳ４１０３において、ポリシーチェック・修正部１１６は、アクセス権設定情報を参照し、Ｒｉに対して登録されているｊ番目のパーミッションＰｉｊを以降の処理対象にセットする。

【０２５３】

ステップＳ４１０４において、ポリシーチェック・修正部１１６は、アクセスログを参照し、Ｐｉｊに関するアクセスログがアクセスログに記憶されているか否かをチェックする。そして、Ｐｉｊのアクセスログが存在しない場合、ポリシーチェック・修正部１１６は、処理をステップＳ４１０５に移行する。

【０２５４】

ステップＳ４１０５において、ポリシーチェック・修正部１１６は、ＲｉとＰｉｊを記憶装置等に記憶する。そして、処理をステップＳ４１０６に移行する。

ステップＳ４１０６において、ポリシーチェック・修正部１１６は、アクセス権設定情報を参照し、Ｒｉに対して他にチェックすべきパーミッションが登録されているか否かをチェックする。そして、他にチェックすべきパーミッションが登録されている場合、ポリシーチェック・修正部１１６は、処理をステップＳ４１０７に移行する。

【０２５５】

ステップＳ４１０７において、ポリシーチェック・修正部１１６は、ｊを１だけインクリメントし、処理をステップＳ４１０３に移行する。

また、ステップＳ４１０６において、他にチェックすべきパーミッションが登録されていない場合、ポリシーチェック・修正部１１６は、処理をステップＳ４１０８に移行する

。そして、ポリシーチェック・修正部１１６は、アクセス権設定情報を参照し、他にチェックすべきロールが存在するか否かをチェックする。

【０２５６】

他にチェックすべきロールが存在する場合、ポリシーチェック・修正部１１６は、処理をステップＳ４１０９に移行する。そして、ｉを１だけインクリメントして処理をステップＳ４１０２に移行する。

【０２５７】

また、ステップＳ４１０８において、他にチェックすべきロールが存在しない場合、ポリシーチェック・修正部１１６は、処理をステップＳ４１１０に移行し、ユーザやロールに設定された使用されていないパーミッションの検出処理を終了する。

【０２５８】

以上の処理によって、例えば、表２４に示すように、使用されていないパーミッションのリストが得られる。

【０２５９】

【表２４】

ロール	パーミッション
R1	p13
R1	p14
・・・	・・・
Ri	・・・
Ri	pij
・・・	・・・

なお、使用されていないロールの検出処理については、図２０で詳細に説明をしているので省略する。

【０２６０】

６．組織間のアクセス権設定の違いや経時的変化を視覚化し、設定ミスを検出支援する方法

各組織が管理している情報に対して、アクセス権の設定情報を組織毎に割合を表示し、設定ミスや不審な設定だと考えられる情報を以下に説明する。

【０２６１】

図４２は、組織間のアクセス権設定の違いや変化の視覚化を実現するための構成例を示している。ポリシーチェック・修正部１１６は、ＲＢＡＣポリシー記憶部１１３から例えば表２０に示すパーミッション－ロール情報を取得し、統合ＩＤ管理部１２０から例えば表２５に示す組織－ユーザ－ロール対応表を取得し、以下で説明するアクセス権設定割合を組織毎に計算する。

【０２６２】

【表２５】

組織	ユーザ	ロール
A部門	U_{A1}	R1
A部門	U_{A1}	R2
・・・	・・・	・・・
X部門	U_{Xi}	Rx
・・・	・・・	・・・

【０２６３】

６．１　組織毎のアクセス権設定割合の計算

ポリシーチェック・修正部１１６は、各組織が管理するシステムのアクセス権設定情報から、組織毎のアクセス権の設定割合を算出する。そして、ポリシーチェック・修正部１１６は、算出結果を表示するとともに記憶装置等に記録する。

【０２６４】

例えば、組織ｘのユーザの集合をＵ（ｘ）、システムＡにおけるユーザｕのパーミッションの集合をＰＲＭ（Ａ，ｕ）、システムＡにおける組織ｘに所属するユーザが持つパーミッションの和集合をＰＲＭ（Ａ，ｘ）、システムＡが管理するリソースの集合をＲ（Ａ）、システムＡの管理するリソースに対するアクションの集合をＡＣＴ（Ａ）とするとき、システムＡにおける組織ｘのアクセス権設定割合は、次式で定義することができる。

【０２６５】

【数１】

$$ACRate(A,x) := \frac{\left|PRM(A,x)\right|}{\left|U(x)\right| \times 2^{R(A)ACT(A)}} \times 100 \quad (\%) \quad \cdots\cdots\cdots \quad (1)$$

なお、ＰＲＭ（Ａ，ｕ）は、例えば表２０に示すパーミッション－ロール情報と、システムＡにおける例えば表２５に示す組織－ユーザ－ロール対応表から計算することができ、ＰＲＭ（Ａ，ｘ）は、ＰＲＭ（Ａ，ｕ）と例えば表２５に示す組織－ユーザ－ロール対応表から組織ｘにおけるパーミッションの和集合を計算することができる。また、ＡＣＴ（Ａ）は、例えばリソースがファイルのみならば、｛ｒｅａｄ，ｗｒｉｔｅ｝となる。

【０２６６】

ここで、ある特定のアクションに関して割合が出したい場合は、３つの引数を持つＰＲＭを次のように定義する。すなわち、ＰＲＭ（Ａ，ｕ）の中で、アクションがａ１のパーミッションの集合をＰＲＭ（Ａ，ｕ，ａ１）、ＰＲＭ（Ａ，ｘ）の中で、アクションがａ１のパーミッションの集合をＰＲＭ（Ａ，ｘ，ａ１）と定義すると、システムＡにおける組織ｘのアクションａ１のアクセス権設定割合は、次式で定義することができる。

【数２】

$$ACRate(A,x,a1) := \frac{\left|PRM(A,x,a1)\right|}{\left|U(x)\right| \times 2^{R(A)}} \times 100 \quad (\%) \quad \cdots\cdots\cdots \quad (2)$$

【０２６７】

６．２　定期的な組織毎のアクセス権設定割合の計算結果の記録

アクセス権の設定の追加や変更の時間的変化を記録するために、ポリシーチェック・修正部１１６は、定期的に組織毎のアクセス権設定割合ＡＣＲａｔｅを計算し記憶装置等に記録することもできる。この時、その変化の出力装置等に表示し、記憶装置等に記憶してもよい。表２６は、システム毎にＡＣＲａｔｅを算出した結果の例を示している。

【０２６８】

【表２６】

	システムA	システムB	システムC	システムD	システムE
A部門	R:70% W:70%	R:35% W:20%	R:1% W:1%	R:3% W:1%	R:80% W:10%
B部門	R:40% W:15%	R:70% W:70%	―	―	R:80% W:5%
C部門	R:50% W:20%	―	R:80% W:80%	―	R:80% W:3%
D部門	―	―	―	R:80% W:75%	R:80% W:5%

【０２６９】

６．３　組織毎のアクセス権設定割合の大きな変化の検知とアラーム

また、ポリシーチェック・修正部１１６は、経時的な組織毎のアクセス権設定割合ＡＣＲａｔｅ値の変化の中から、大きな変化があった組織を検知し、組織のアクセス権設定がおかしくないか確認を促す通知を行なってもよい。

【０２７０】

図４３は、各システムにおける各組織のアクセス権設定数や利用率を計算した結果を表示した画面の構成例を示す図である。図４３に示す使用率は、ロールがシステム上で利用されているかどうかを表す尺度である。例えば、次式を用いて使用率を算出することができる。

【０２７１】

使用率　＝　アクセスログに記録されているあるロールでアクセスしたログレコードの件数÷（（アクセスログレコードの総数×あるロールのユーザ数）÷（システム上に存在するロールのユーザ数の和））×１００

このとき、アクセスログは、１日、１週間、１ヶ月、３ヶ月、半年のように適当な期間のアクセスログを使用することが望ましい。例えば、システムに３つのロールＲｏｌｅＡ、ＲｏｌｅＢ、ＲｏｌｅＣがあり、各々のユーザ数、アクセスログレコードの件数および総数が表２７の場合について考える。

【０２７２】

【表２７】

	RoleA	RoleB	RoleC	合計
ユーザ数	50	80	60	100
ログレコード件数	500	200	300	1000

なお、表２７において、ユーザはロールに重複して所属することが可能なため、必ずしもＲｏｌｅＡ、ＲｏｌｅＢおよびＲｏｌｅＣのユーザ数の和にならない。

【０２７３】

この時、ＲｏｌｅＡの使用率は、５００÷（（１０００×５０）÷（５０＋８０＋６０））×１００＝１９０となる。ＲｏｌｅＢ、ＲｏｌｅＣについても同様に使用率を算出すると、それぞれ４７．５、９５となる。

【０２７４】

図４４は、本実施例に係る組織毎のアクセス権設定割合の表示画面の例を示す図である

。
図４３で示した画面の「アクセス権設定割合」ボタンを押下することにより、上述した手法によりＡＣＲａｔｅを算出し、図４４に示す組織毎のアクセス権設定割合表示画面を表示するようにしてもよい。また、図４３に示した画面の「月間推移表示」ボタンを押下することにより、図４５に示す各システムのアクセス権設定の平均割合推移を表示してもよい。なお、平均とは、たとえば、システムを利用している各部門のアクセス権割合の平均である。

【０２７５】

図４６は、本実施例に係るシステム毎のアクセス権設定・使用率情報の表示画面の例を示す図である。

図４３に示した各システムのアクセス権設定・使用率情報表示画面例で、各システムの「詳細」ボタンをクリックすることにより、図４６に示すシステム毎のアクセス権設定・使用率情報の表示画面を表示してもよい。図４６に示す「ロール割合」は、アカウント数に対するロール数の割合を示したものであり、ロール数÷アカウント数×１００で求められる。

【０２７６】

７．　一致や類似したロールを発見し、修正案を提示する方法

ロール管理では、管理コストの観点から冗長なロールを管理しない工夫が必要となる。そこで、現在のロール設定（ユーザとロールの関係、ロールとパーミッションの関係）情報から、一致や類似したロールを発見し、最適なロール設定に近づけるような修正案を提示する方法について説明する。

【０２７７】

図４７は、一致や類似したロールを発見するための構成例を示している。

ポリシーチェック・修正部１１６は、ＲＢＡＣポリシー記憶部１１３から例えば表２０に示すパーミッション－ロール情報を取得し、統合ＩＤ管理部１２０から例えば表２１に示すロール－ユーザ対応表を取得し、以下で説明する類似度を計算し、計算結果を、表３１が示す６つのケースに分類し、各々のケースの修正案を提示する。

【０２７８】

７．１　類似度計算

類似度は、例えば一致係数の計算法を用いて計算する。本実施例ではロールの属性として、ユーザ、パーミッションを使用し、ロール毎に一致係数を算出する。以下、ユーザに関する一致係数をユーザ類似度ｕｓｍｃ、パーミッションに関する一致係数をパーミッション類似度ｐｓｍｃという。

【０２７９】

ここで、ユーザ類似度は、ロールＲ１、Ｒ２の両方に所属するユーザ数をａ、Ｒ１のみに所属するユーザ数をｂ、Ｒ２のみに所属するユーザ数をｃ、Ｒ１、Ｒ２のいずれにも所属しないユーザ数をｄ、全ユーザ数をｎ（ｎ＝ａ＋ｂ＋ｃ＋ｄ）とすると、次式で定義することができる。

ユーザ類似度ｕｓｍｃ　＝　（ａ＋ｄ）／ｎ　　・・・・・　（３）

【０２８０】

また、パーミッション類似度は、ロールＲ１、Ｒ２の両方に割当てられているパーミッション数をｏ、Ｒ１のみに割当てられているパーミッション数をｐ、Ｒ２のみに割当てられているパーミッション数をｑ、Ｒ１、Ｒ２のいずれにも割当てられていないパーミッション数をｒ、全パーミッション数をｍ（ｍ＝ｏ＋ｐ＋ｑ＋ｒ）とすると、次式で定義することができる。

【０２８１】

パーミッション類似度ｐｓｍｃ　＝　（ｏ＋ｐ）／ｍ　・・・・・　（４）

例えば、ロールとユーザが表２８に示す関係にあり、ロールとパーミッションが表２９に示す関係にある場合、式（３）および式（４）を用いると、表３０に示す類似度（ｕｓｍｃ、ｐｓｍｃ）を算出することができる。

【０２８２】
【表２８】

ロール	taro	jiro	hanako	maeda	saito
R1	1	1	0	0	0
R2	1	0	1	0	0
R3	1	0	1	1	1
R4	0	1	1	1	1

【０２８３】
【表２９】

ロール	p1	p2	p3	p4	p5
R1	1	0	0	1	1
R2	1	1	0	1	1
R3	0	1	1	0	1
R4	1	0	1	1	0

【０２８４】
【表３０】

ロール	R1		R2		R3		R4	
	us_{mc}	ps_{mc}	us_{mc}	ps_{mc}	us_{mc}	ps_{mc}	us_{mc}	ps_{mc}
R1	–	–	–	–	–	–	–	–
R2	0.6	0.8	–	–	–	–	–	–
R3	0.2	0.2	0.6	0.4	–	–	–	–
R4	0.2	0.6	0.2	0.4	0.6	0.2	–	–

【０２８５】

【表３１】

No	ケース	修正案
1	ロールのユーザのみが一致	2つのパーミッションを合わせたロールにマージすべき。 注意：今後どちらかのロールのみユーザに変化があるかもしれない。
2	ロールのユーザ類似度のみ高い	どちらか一方のロールにしか所属しないユーザを提示し、削除するか、もう一方のロールに所属させれば、(ケース1と同じになり)ロールをマージすることができることを提示する。
3	ロールのパーミッションのみが一致	2つのユーザグループを合わせたロールを提示する。 ユーザグループ同士が同じ部署である場合などは、このようにしたほうがいいかもしれない。
4	ロールのパーミッション類似度のみ高い	どちらか一方のロールにしか割当てられていないパーミッションを提示し、削除するか、もう一方のロールに割当てれば、(ケース3と同じとなり)ユーザグループを合わせたロールを提示することができることを通知する。
5	ロールのユーザ、パーミッションが一致	同じロールが2重にある。必要がないため削除すべきことを提示する。
6	ロールのユーザ類似度、パーミッション類似度ともに高い	次の2つのロール構成を提示する。 (1)ユーザをベースにしたロール構成 ケース2と同様。 (2)パーミッションをベースにしたロール構成 ケース4と同様。

【０２８６】

図４８は、本実施例に係る類似度計算の具体的な処理を示すフローチャートである。

ステップＳ４８０１において、ポリシーチェック・修正部１１６は、カウント用変数ｉに１をセットする。そして、ポリシーチェック・修正部１１６は、処理をステップＳ４８０２に移行し、変数ｊにｉ＋１をセットする。

【０２８７】

ステップＳ４８０３において、ポリシーチェック・修正部１１６は、式（３）および式（４）に示した定義にしたがって、ＲｉとＲｊについて、ユーザ類似度ｕｓｍｃとパーミッション類似度ｐｓｍｃを算出する。そして、ポリシーチェック・修正部１１６は、記憶装置等に算出結果を記憶する。

【０２８８】

ステップＳ４８０４において、ポリシーチェック・修正部１１６は、ｊがｎ以下か否かを判別する。ｊがｎ以下の場合、ポリシーチェック・修正部１１６は、処理をステップＳ４８０５に移行する。そして、ｊを１だけインクリメントして処理をステップＳ４８０３に移行する。

【０２８９】

ステップＳ４８０６において、ポリシーチェック・修正部１１６は、ｉがｎ以下か否かを判別する。ｉがｎ以下の場合、ポリシーチェック・修正部１１６は、処理をステップＳ４８０７に移行する。そして、ｉを１だけインクリメントして処理をステップＳ４８０２に移行する。

【０２９０】

また、ステップＳ４８０６において、ｉがｎより大きい場合、ポリシーチェック・修正部１１６は、処理をステップＳ４８０７に移行し、類似度計算処理を終了する。

ロールに所属するユーザ数が低い若しくは使用率が低いものは、他のロールと比較して、システムに影響があまりなく無駄なロールである可能性が高いと考えられる。そこで、図４９に示すように、フィルター項目として、「ユーザ数」と「使用率」を設けて、条件に合う検索結果を表示するようにしてもよい。「ロール類似度計算」ボタンが押下された場合に、当該フィルター処理により得られた数値の小さなロールに対して類似度計算を行なうようにしてもよい。

【０２９１】

図４８に示した類似計算が完了すると、ポリシーチェック・修正部１１６は、例えば図５０に示す計算結果を表示装置等に出力して表示する。さらに、「修正案表示」ボタンが押下されると、ポリシーチェック・修正部１１６は、例えば表３１に示した類似度計算結果に対する修正案提示ルールを参照し、計算結果に該当するケースＮｏ．の修正案を表示装置等に出力して表示する。図５１は、ロール修正案提示の表示画面の構成例を示している。

【０２９２】

また、図５１に示す「詳細」ボタンの押下に応じて、各ロールの組の修正案の詳細を示すようにしてもよい。図５２は、ロール修正案の詳細の表示画面の構成例を示している。

図５３は、本実施例に係る統合セキュリティ管理システム１００の具体的な構成例を示す図である。

【０２９３】

図５３に示す統合セキュリティ管理システム１００は、周辺機器や各種ソフトウェアを実行する他に本実施例に係るポリシーチェック・修正処理を実現するプログラムを実行するＣＰＵ５３０１と、プログラムを実行するために使用される揮発性のメモリ５３０２（例えば、ＲＡＭ）と、外部からのデータ入力手段である入力装置５３０３（例えば、キーボードやマウス）と、データ等を表示する出力装置５３０４と、統合セキュリティ管理システム１００が動作するために必要なプログラムやデータの他に本実施例に係るポリシーチェック・修正処理を実現するプログラムを記憶する外部記憶装置５３０５と、メモリ５３０２や外部記憶装置５３０５のデータを可搬記憶媒体５３０７（例えば、フロッピイディスクやＭＯディスク、ＣＤ－ＲやＤＶＤ－Ｒなど）に出力し、或は可搬記憶媒体５３０７からプログラムやデータ等を読み出す媒体駆動装置５３０６と、ネットワークを介して他のシステム等に接続するネットワーク接続装置５３０８と、を有し、これらの装置がバス５３００に接続されて相互にデータの受け渡しが行える構成となっている。

【０２９４】

なお、本実施例に係るポリシーチェック・修正処理を実現するプログラムは、外部記憶装置５３０５でなく可搬記憶媒体５３０７に記憶されていてもよい。

以上に説明したように、本実施例に係る統合セキュリティ管理システム１００は、制御対象となるシステム（例えば、図１に示したサーバＡ、ＢおよびＣからなるサーバシステムなど）が備えるリソースに対するアクセス権設定情報について、１または２以上のポリシーチェックルール（例えば、３．１に示した不適切なユーザアカウントの検出、３．２に示した不適切なユーザ－ロール割当ての検出、３．３に示した不適切なパーミッション－ロール割当ての検出、３．４に示した不要なロールの検出、３．５に示した職務分掌違反の検出など）にしたがって、ルール違反を検出する。その結果、アクセス制御のためのポリシーに対して多面的かつ網羅的にチェックを行なうことが可能となる。

また、検出結果に応じて全体または所定の違反項目毎にポリシー遵守レベルを算出し表示するので、チェック結果を容易かつ客観的に把握すること可能となる。

【０２９５】

以上の実施例１～ｎを含む実施形態に関し、さらに以下の付記を開示する。

（付記１）　任意のリソースに対するアクセスを一括してまたは部分的に制限するアクセス権管理情報を記憶するアクセス権管理情報記憶手段から該アクセス権管理情報を取得するアクセス権管理情報取得処理と、

前記リソースに対してまたは該リソースに対するアクセスに対して設定されたポリシーを記憶するポリシー記憶手段から該ポリシーを取得し、前記アクセス権管理情報が前記ポリシーに適合しているか否かを検査し、前記ポリシーに適合しないものを違反として検出する違反検出処理と、

該違反のリスクの度合いに応じてリスク得点を算出し、該算出結果から前記ポリシーに対する遵守レベルを算出するポリシー遵守レベル算出処理と、

該ポリシー遵守レベル算出処理の算出結果を出力する結果出力処理と、

を情報処理装置に実行させるプログラム。

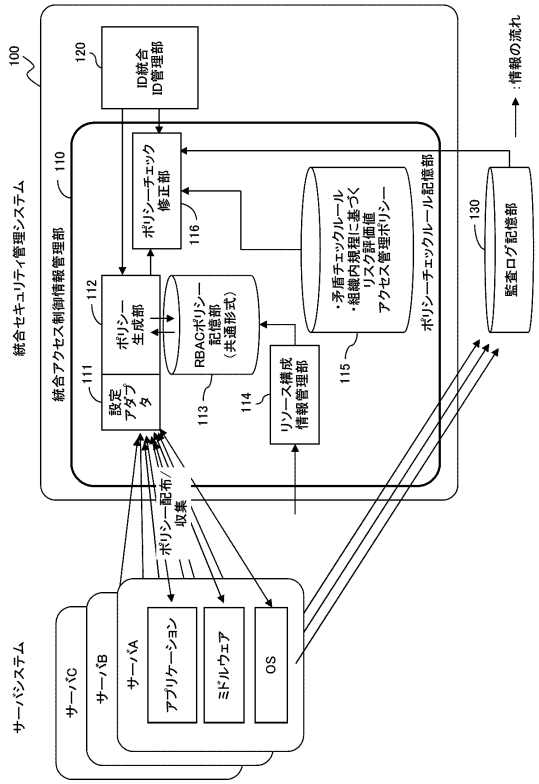
（付記２）　前記違反検出処理は、サーバ毎若しくは所定のリソース毎に、該サーバが備えるリソース若しくは前記所定のリソースに対して設定されたポリシーに前記アクセス権管理情報が適合しているか否かを検査する、
　ことを特徴とする付記１に記載のプログラム。
（付記３）　前記ポリシー遵守レベル算出処理は、前記サーバ毎若しくは所定のリソース毎にリスク得点を算出し、該算出結果から前記ポリシーに対する遵守レベルを算出する、
　ことを特徴とする付記２に記載のプログラム。
（付記４）　前記ポリシーは、前記アクセス権管理情報に含まれるユーザ情報が、使用していないユーザアカウント、利用者を特定できないユーザアカウント、または削除されるべきアカウントであったがまだ残っているユーザアカウントの何れかに該当する場合に違反とする、
　ことを特徴とする付記１に記載のプログラム。
（付記５）　前記ポリシーは、前記アクセス権管理情報に含まれるロール割当てが、使用していないロール割当て、または、あらかじめ決められたロール割当て禁止ルールに違反するロール割当て、の何れかに該当する場合に違反とする、
　ことを特徴とする付記１に記載のプログラム。
（付記６）　前記ポリシーは、前記アクセス権管理情報に含まれるパーミッション割当てが、使用していないパーミッション割当て、または、あらかじめ決められたパーミッション割当て禁止ルールに違反するパーミッション割当て、の何れかに該当する場合に違反とする、
　ことを特徴とする付記１に記載のプログラム。
（付記７）　前記ポリシーは、前記アクセス権管理情報に含まれるロールが、使用されていないロール、あらかじめ決められたユーザへのロール割当て禁止ルールに違反するロール、または、あらかじめ決められたロールへのパーミッション割当て禁止ルールに違反するロール、の何れかに該当する場合に違反とする、
　ことを特徴とする付記１に記載のプログラム。
（付記８）　前記ロールは階層構造を有する、ことを特徴とする付記７に記載のプログラム。
（付記９）　前記ポリシーは、ユーザへのロール割当て禁止ルールに違反するロール割当て、ロールへのパーミッション割当て禁止ルールに違反するパーミッション、または、ユーザへのパーミッション割当て禁止ルールに違反するパーミッション、の何れかに該当する場合に違反とする、
　ことを特徴とする付記１に記載のプログラム。
（付記１０）　任意のリソースに対するアクセスを一括してまたは部分的に制限するアクセス権管理情報を記憶するアクセス権管理情報記憶手段から取得するアクセス権管理情報取得手段と、
　前記リソースに対してまたは該リソースに対するアクセスに対して設定されたポリシーを記憶するポリシー記憶手段から該ポリシーを取得し、前記アクセス権管理情報が前記ポリシーに適合しているか否かを検査し、前記ポリシーに適合しないものを違反として検出する違反検出手段と、
　該違反のリスクの度合いに応じてリスク得点を算出し、該算出結果から前記ポリシーに対する遵守レベルを算出するポリシー遵守レベル算出手段と、
　該ポリシー遵守レベル算出処理の算出結果を出力する結果出力手段と、
　を備える情報処理装置。
【図面の簡単な説明】
【０２９６】
【図１】本実施例に係るアクセス制御ポリシー遵守のチェック機構を備える統合セキュリティ管理システムの構成例を示す図である。
【図２】本実施例に係る統合セキュリティ管理システムにおけるポリシー遵守レベルの計測対象を説明する図である。

【図３】本実施例に係る統合セキュリティ管理システムの処理の概要を示すフローチャートである。
【図４】本実施例に係る不適切なユーザアカウントの検出処理の概要を示す図である。
【図５】本実施例に係る不適切なユーザアカウントの定義を説明する図である。
【図６】本実施例に係る不適切なユーザアカウントを検出する具体的な処理を示すフローチャートである。
【図７】本実施例に係るユーザアカウントの分類を説明する図である。
【図８】不適切なユーザアカウント検出処理におけるポリシー遵守レベルを表示する画面の構成例を示す図である。
【図９】本実施例に係る不適切なユーザ－ロール割当ての検出処理の概要を示す図である。
【図１０】本実施例に係る不適切なユーザ－ロール割当ての検出処理の概要を示すフローチャートである。
【図１１】本実施例に係る使用されていないユーザ－ロール割当て検出処理（ステップＳ１００１）の具体的な処理を示すフローチャートである。
【図１２】本実施例に係るロール割当て禁止に違反するロール割当て検出処理（ステップＳ１００２）の具体的な処理を示すフローチャートである。
【図１３】不適切なユーザ－ロール割当ての検出処理におけるポリシー遵守レベルを表示する画面の構成例を示す図である。
【図１４】本実施例に係る不適切なパーミッション－ロール割当ての検出を行なうための構成例を示す図である。
【図１５】本実施例に係る不適切なパーミッション－ロール割当ての検出処理の概要を示すフローチャートである。
【図１６】本実施例に係るロールが同時使用禁止のパーミッションを所有しているか否かのチェック処理（ステップＳ１５０２）の具体的な処理を示すフローチャートである。
【図１７】不適切なパーミッション－ロール割当て処理におけるポリシー遵守レベルを表示する画面の構成例を示す図である。
【図１８】本実施例に係る不適切なロールの検出を行なうための構成例を示す図である。
【図１９】本実施例に係る不適切なロールの検出処理の概要を示すフローチャートである。
【図２０】本実施例に係る使用されていないロールの検出処理（ステップＳ１９０１）の具体的な処理を示すフローチャートである。
【図２１】本実施例に係る階層構造を有するロールの構成例を示す図である。
【図２２】本実施例に係る階層構造を有するロールのチェック範囲を説明する図である。
【図２３】本実施例に係るロール割当て禁止ルールに違反するロールの検出処理（ステップＳ１９０２）の具体的な処理を示すフローチャートである。
【図２４】ロールＲｉとＲｊがともにパーミッション割当て禁止ルールに違反している場合のロール階層について説明する図である。
【図２５】ロールＲｉがパーミッション割当て禁止ルールに違反し、Ｒｊが違反していない場合のロール階層について説明する図である。
【図２６】違反の原因となるロールを説明する図である。
【図２７】違反の原因となるロールを説明する図である。
【図２８】本実施例に係るパーミッション割当て禁止ルールに違反するロールを検出する処理である。
【図２９】本実施例に係る不適切なロールの検出処理におけるポリシー遵守レベルを表示する画面の構成例を示す図である。
【図３０】本実施例に係る職務分掌違反の検出を行なうための構成例を示す図である。
【図３１】本実施例に係る職務分掌違反の検出処理の概要を示すフローチャートである。
【図３２】本実施例に係るＡＣＬの作成処理を示すフローチャートである。
【図３３】本実施例に係るユーザに対するパーミッション割当て禁止ルールに違反する割

当ての検出処理を示すフローチャートである。
【図３４】本実施例に係る職務分掌違反の検出処理におけるポリシー遵守レベルを表示する画面の構成例を示す図である。
【図３５】本実施例に係るユーザ－ロール対応表のサイズを説明する図である。
【図３６】本実施例に係るロール－パーミッション対応表のサイズを説明する図である。
【図３７】本実施例に係るサーバ毎のポリシー遵守レベルの計測結果の画面の構成例を示している。
【図３８】「詳細」ボタンを押下したときに表示される各システムのポリシー遵守レベル評価結果の画面の構成例を示す図である。
【図３９】「月間推移表示」ボタンを押下したときに表示されるリスク値の推移の画面の構成例を示す図である。
【図４０】本実施例に係る無駄なアクセス権設定を検出するための構成例の概要を示している。
【図４１】本実施例に係るユーザやロールに設定された使用されていないパーミッションの検出処理を示すフローチャートである。
【図４２】本実施例に係る組織間のアクセス権設定の違いや変化の視覚化を実現するための構成例を示している。
【図４３】各システムにおける各組織のアクセス権設定数や利用率を計算した結果を表示した画面の構成例を示す図である。
【図４４】本実施例に係る組織毎のアクセス権設定割合を表示する画面の構成例を示す図である。
【図４５】各システムのアクセス権設定の平均割合推移を表示する画面の構成例を示す図である。
【図４６】本実施例に係るシステム毎のアクセス権設定・使用率情報を表示する画面の構成例を示す図である。
【図４７】本実施例に係る一致や類似したロールを発見するための構成例を示している。
【図４８】本実施例に係る類似度計算の具体的な処理を示すフローチャートである。
【図４９】本実施例に係る類似度計算画面の構成例を示す図である。
【図５０】本実施例に係る類似度の計算結果を表示する画面の構成例を示す図である。
【図５１】本実施例に係るロール修正案提示を表示する画面の構成例を示す図である。
【図５２】本実施例に係るロール修正案の詳細を表示する画面の構成例を示す図である。
【図５３】本実施例に係る統合セキュリティ管理システムの具体的な構成例を示す図である。
【符号の説明】
【０２９７】
１００　　統合セキュリティ管理システム
１１０　　統合アクセス制御情報管理部
１１３　　ＲＢＡＣポリシー記憶部
１１５　　ポリシーチェックルール記憶部
１１６　　ポリシーチェック・修正部
１２０　　統合ＩＤ管理部
１３０　　監査ログ記憶部

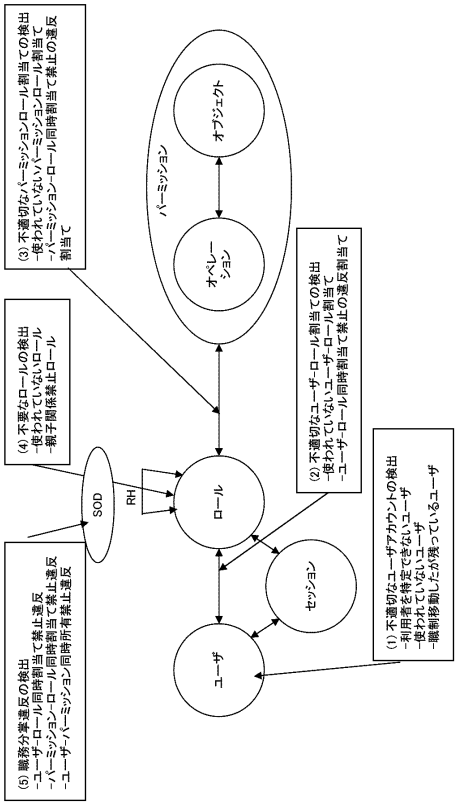
【図１】

本実施例に係るアクセス制御ポリシー遵守のチェック機構を備える統合セキュリティ管理システムの構成例を示す図



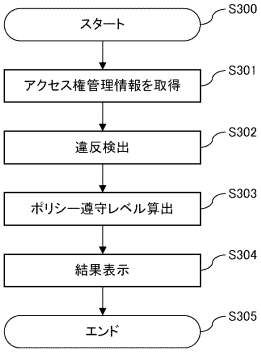
【図２】

本実施例に係る統合セキュリティ管理システムにおけるポリシー遵守レベルの計測対象を説明する図



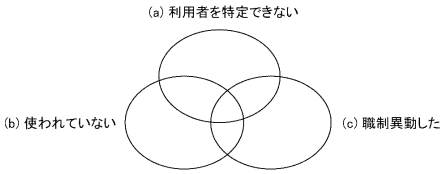
【図３】

本実施例に係る統合セキュリティ管理システムの処理の概要を示すフローチャート



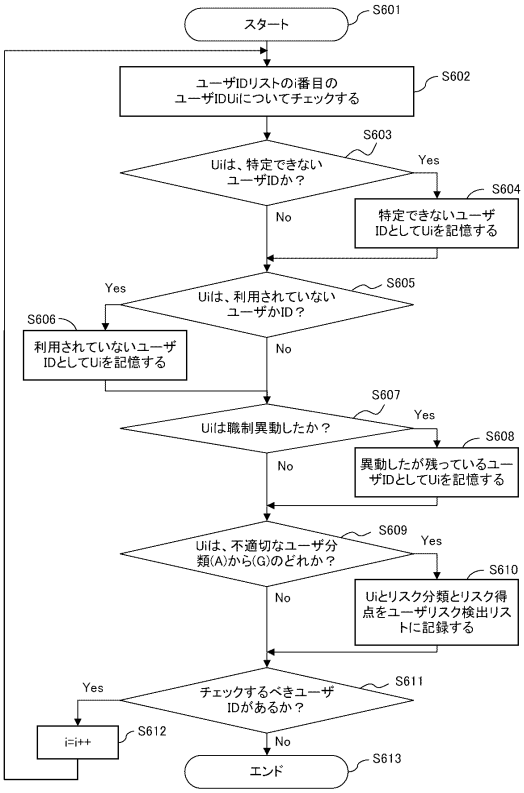
【図５】

本実施例に係る不適切なユーザアカウントの定義を説明する図



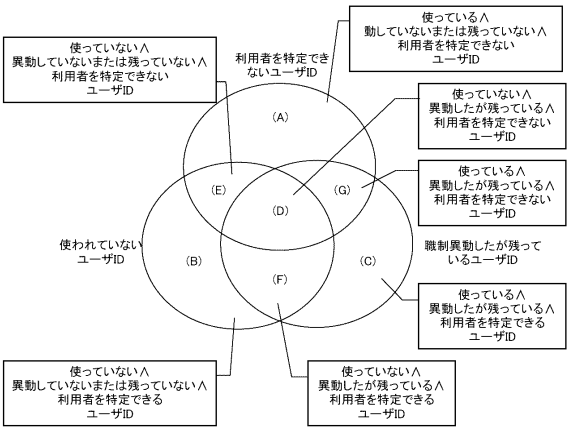
【図６】

本実施例に係る不適切なユーザアカウントを
検出する具体的な処理を示すフローチャート



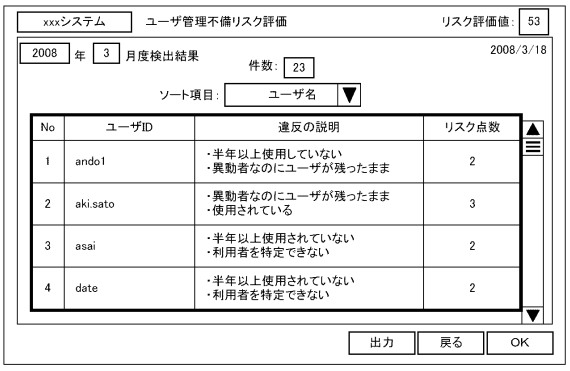
【図７】

本実施例に係るユーザアカウントの
分類を説明する図



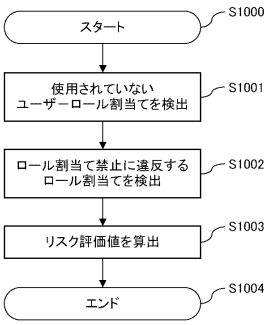
【図８】

不適切なユーザアカウント検出処理における
ポリシー遵守レベルを表示する
画面の構成例を示す図



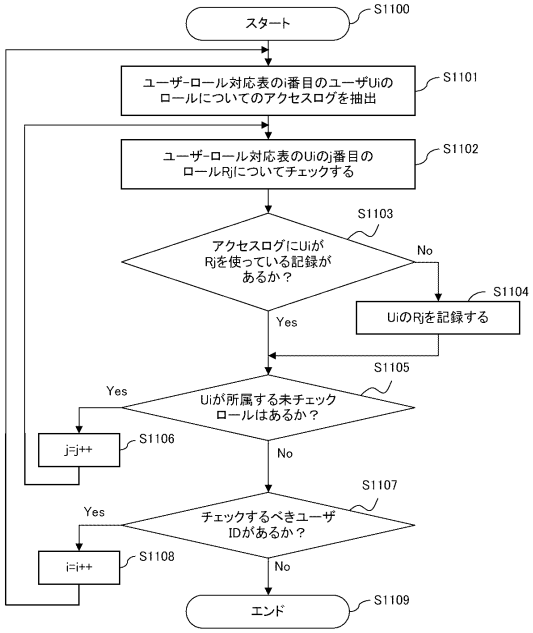
【図１０】

本実施例に係る不適切な
ユーザーロール割当ての検出
処理の概要を示すフローチャート



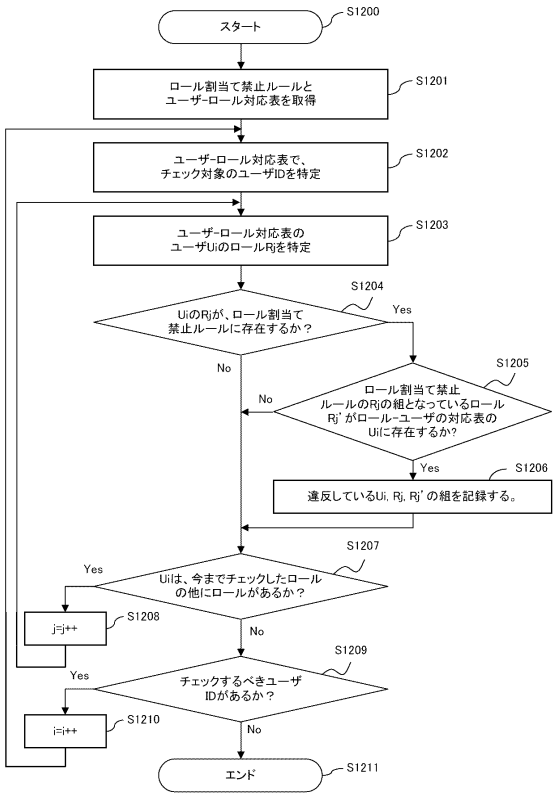
【図１１】

本実施例に係る使用されていないユーザーロール割当て検出処理（ステップS1001）の具体的な処理を示すフローチャート



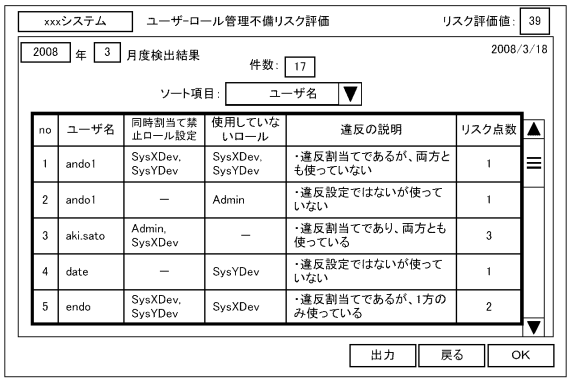
【図１２】

本実施例に係るロール割当て禁止に違反するロール割当て検出処理（ステップS1002）の具体的な処理を示すフローチャート



【図１３】

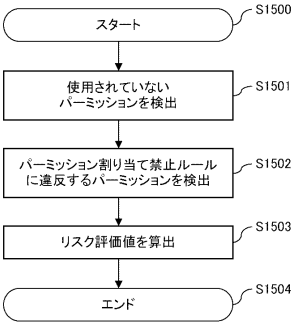
不適切なユーザーロール割当ての検出処理におけるポリシー遵守レベルを表示する画面の構成例を示す図



no	ユーザ名	同時割当て禁止ロール設定	使用していないロール	違反の説明	リスク点数
1	ando1	SysXDev, SysYDev	SysXDev, SysYDev	・違反割当てであるが、両方とも使っていない	1
2	ando1	—	Admin	・違反設定ではないが使っていない	1
3	aki.sato	Admin, SysXDev	—	・違反割当てであり、両方とも使っている	3
4	date	—	SysYDev	・違反設定ではないが使っていない	1
5	endo	SysXDev, SysYDev	SysXDev	・違反割当てであるが、1方のみ使っている	2

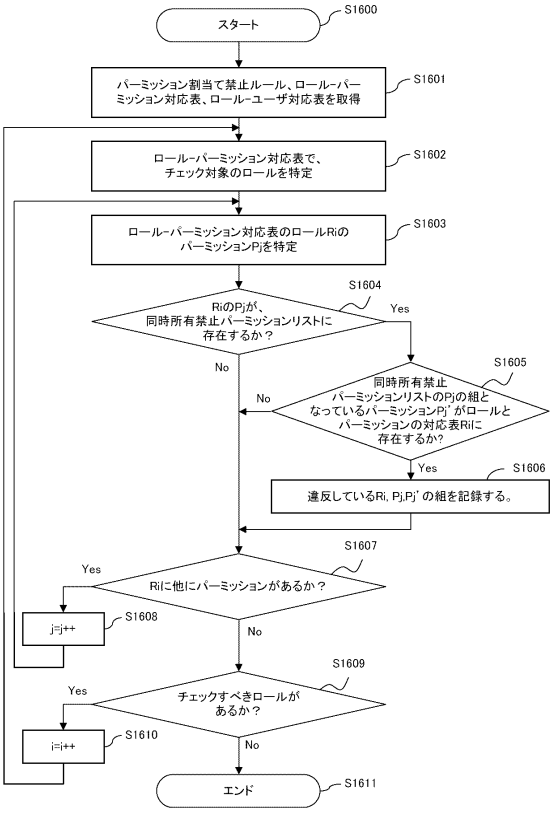
【図１５】

本実施例に係る不適切なパーミッション－ロール割当ての検出処理の概要を示すフローチャート



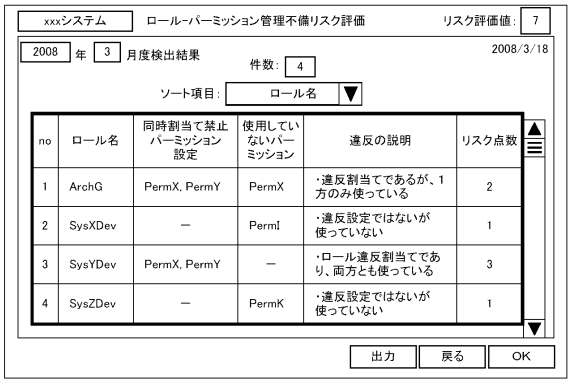
【図１６】

本実施例に係るロールが同時使用禁止のパーミッションを所有しているか否かのチェック処理（ステップS1502）の具体的な処理を示すフローチャート



【図１７】

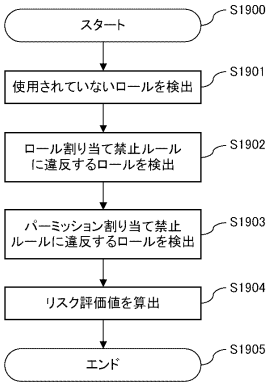
不適切なパーミッション－ロール割当て処理におけるポリシー遵守レベルを表示する画面の構成例を示す図



no	ロール名	同時割当て禁止パーミッション設定	使用していないパーミッション	違反の説明	リスク点数
1	ArchG	PermX, PermY	PermX	・違反割当てであるが、1方のみ使っている	2
2	SysXDev	−	PermI	・違反設定ではないが使っていない	1
3	SysYDev	PermX, PermY	−	・ロール違反割当てであり、両方とも使っている	3
4	SysZDev	−	PermK	・違反設定ではないが使っていない	1

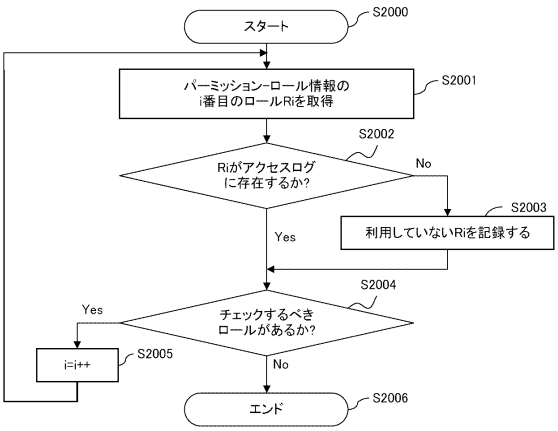
【図１９】

本実施例に係る不適切なロールの検出処理の概要を示すフローチャート



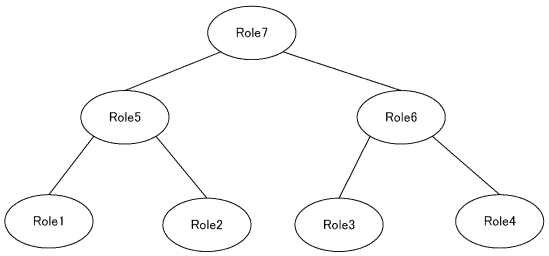
【図２０】

本実施例に係る使用されていないロールの検出処理（ステップS1901）の具体的な処理を示すフローチャート



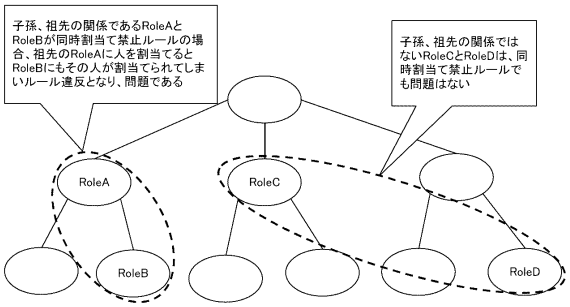
【図２１】

本実施例に係る階層構造を有する
ロールの構成例を示す図



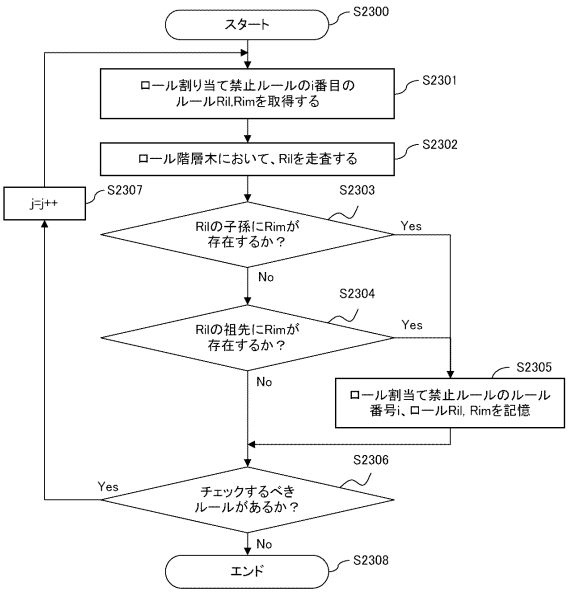
【図２２】

本実施例に係る階層構造を有する
ロールのチェック範囲を説明する図



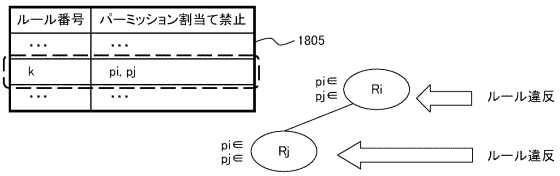
【図２３】

本実施例に係るロール割当て禁止ルールに違反する
ロールの検出処理（ステップS1902）の具体的な
処理を示すフローチャート



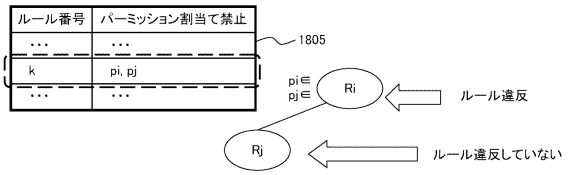
【図２４】

ロールRiとRjがともにパーミッション
割当て禁止ルールに違反している場合の
ロール階層について説明する図



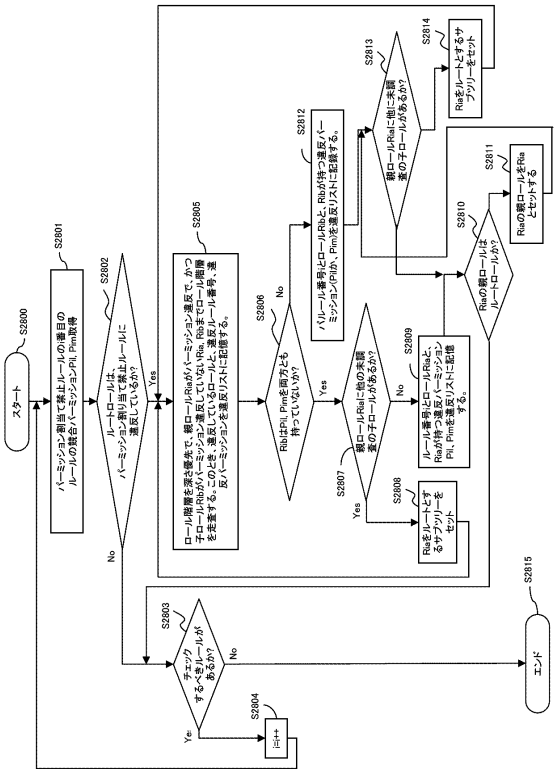
【図２５】

ロールRiがパーミッション割当て禁止ルールに
違反し、Rjが違反していない場合の
ロール階層について説明する図



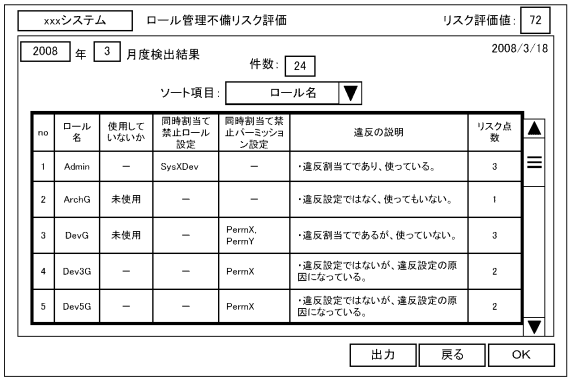
【図２８】

本実施例に係るパーミッション割当て禁止ルールに違反するロールを検出する処理



【図２９】

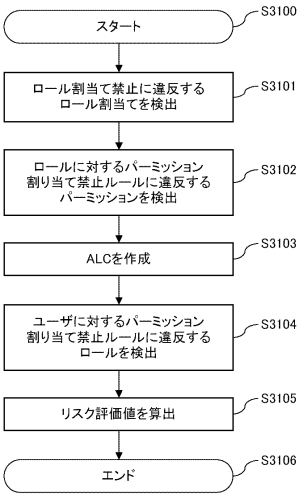
本実施例に係る不適切なロールの検出処理におけるポリシー遵守レベルを表示する画面の構成例を示す図



no	ロール名	使用していないか	同時割当て禁止ロール設定	同時割当て禁止パーミッション設定	違反の説明	リスク点数
1	Admin	−	SysXDev	−	・違反割当ててあり、使っている。	3
2	ArchG	未使用	−	−	・違反設定ではなく、使ってもいない。	1
3	DevG	未使用	−	PermX, PermY	・違反割当ててあるが、使っていない。	3
4	Dev3G	−	−	PermX	・違反設定ではないが、違反設定の原因になっている。	2
5	Dev5G	−	−	PermX	・違反設定ではないが、違反設定の原因になっている。	2

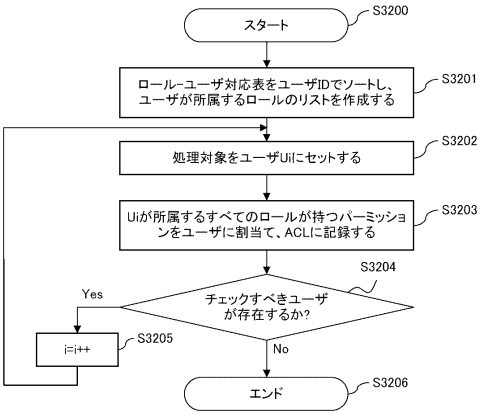
【図３１】

本実施例に係る職務分掌違反の検出処理の概要を示すフローチャート



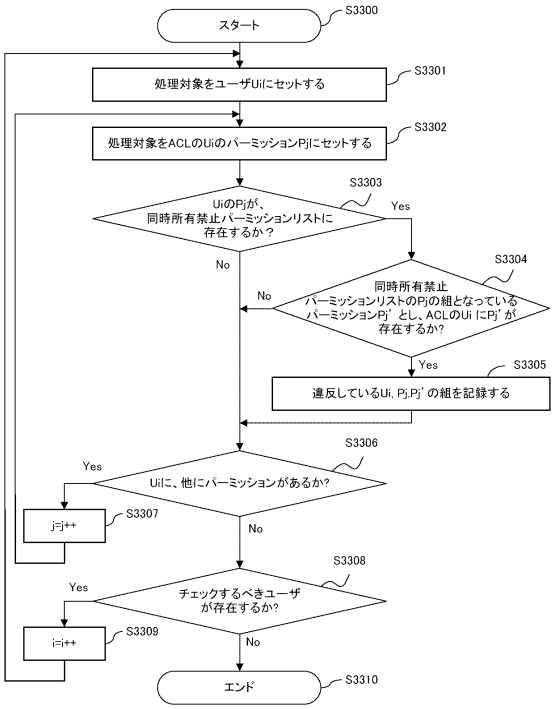
【図３２】

本実施例に係るACLの作成処理を示すフローチャート



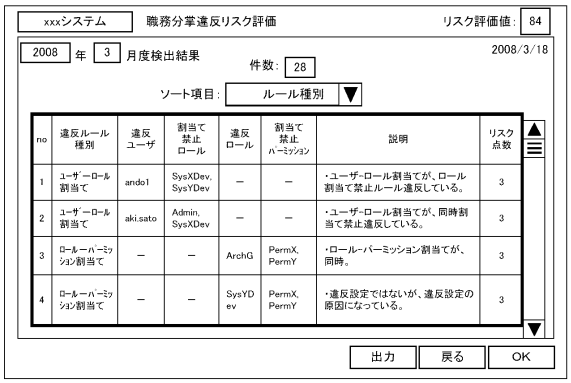
【図３３】

本実施例に係るユーザに対するパーミッション割当て禁止ルールに違反する割当ての検出処理を示すフローチャート



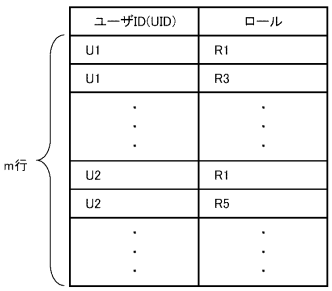
【図３４】

本実施例に係る職務分掌違反の検出処理におけるポリシー遵守レベルを表示する画面の構成例を示す図



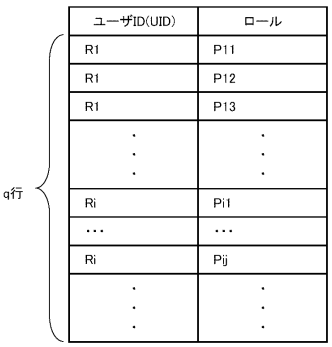
【図３５】

本実施例に係るユーザーロール対応表のサイズを説明する図



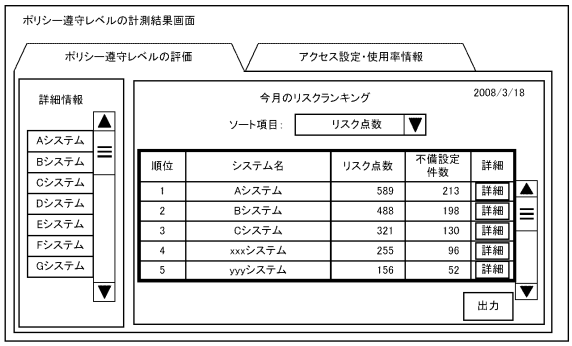
【図３６】

本実施例に係るロールーパーミッション対応表のサイズを説明する図



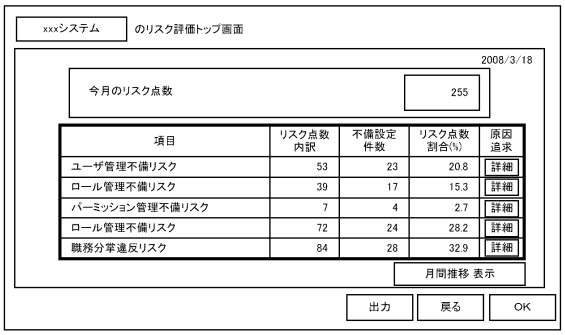
【図３７】

本実施例に係るサーバ毎の
ポリシー遵守レベルの計測結果の
画面の構成例を示している



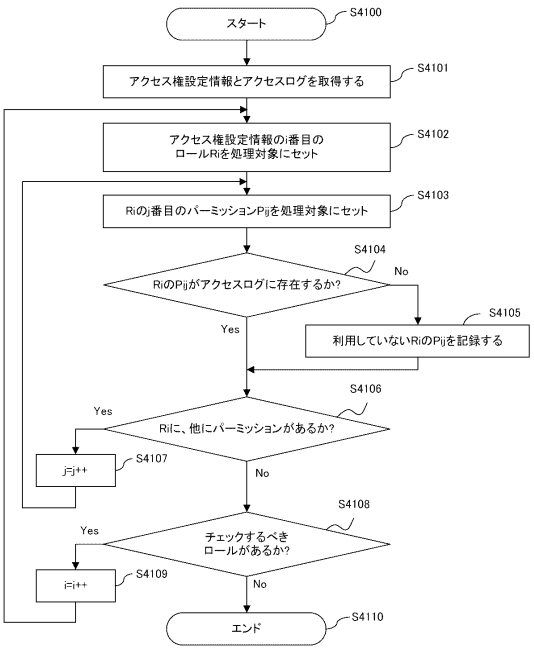
【図３８】

「詳細」ボタンを押下したときに表示される
各システムのポリシー遵守レベル評価結果の
画面の構成例を示す図



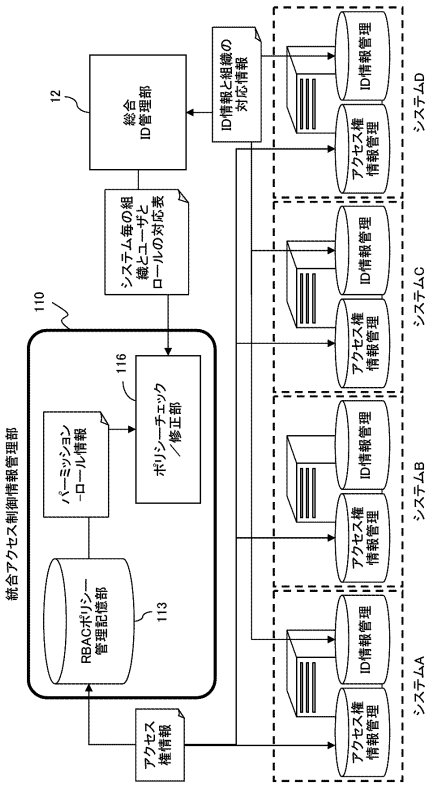
【図４１】

本実施例に係るユーザやロールに設定された使用されていない
パーミッションの検出処理を示すフローチャート



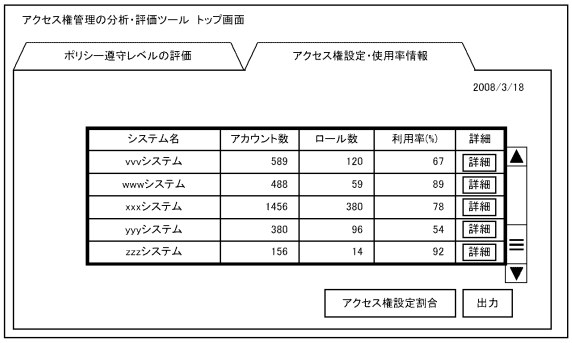
【図４２】

本実施例に係る組織間のアクセス権設定の違いや
変化の視覚化を実現するための構成例を示している



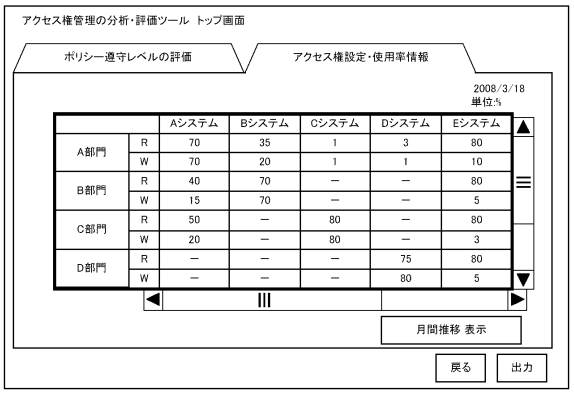
【図４３】

各システムにおける各組織の
アクセス権設定数や利用率を計算した
結果を表示した画面の構成例を示す図



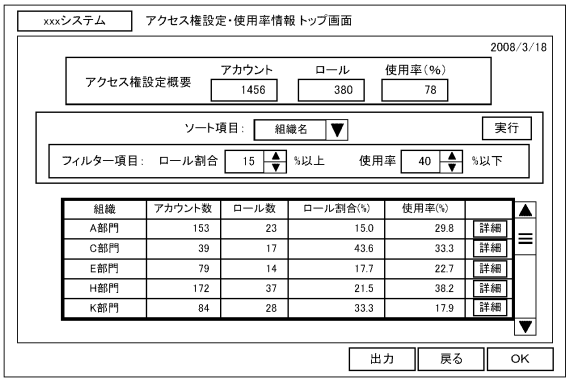
【図４４】

本実施例に係る組織毎の
アクセス権設定割合を表示する
画面の構成例を示す図



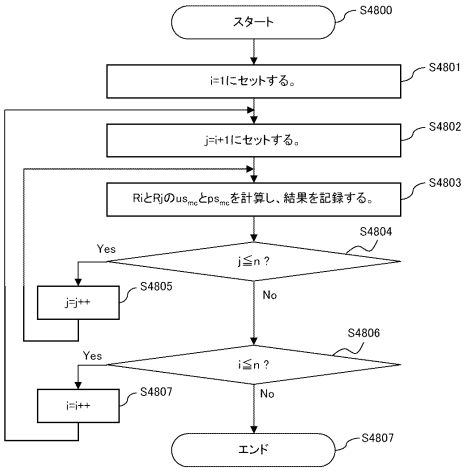
【図４６】

本実施例に係るシステム毎の
アクセス権設定・使用率情報を
表示する画面の構成例を示す図



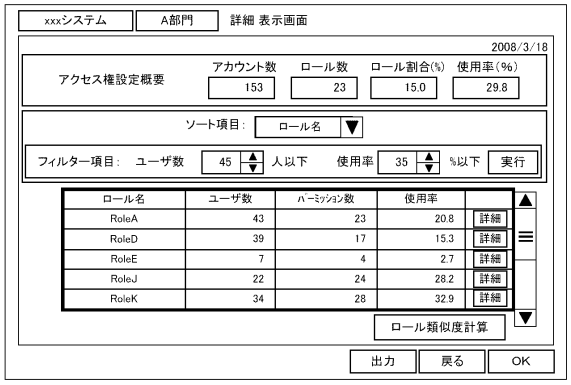
【図４８】

本実施例に係る類似度計算の具体的な
処理を示すフローチャート



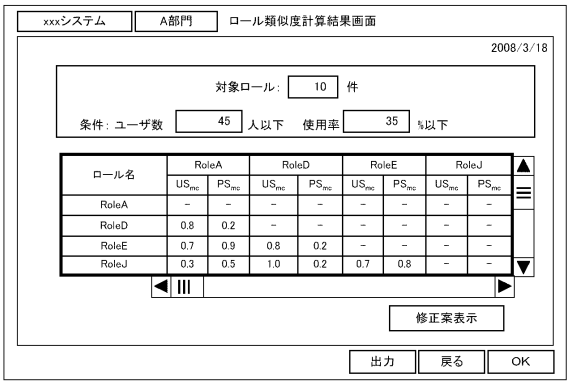
【図４９】

本実施例に係る類似度計算
画面の構成例を示す図



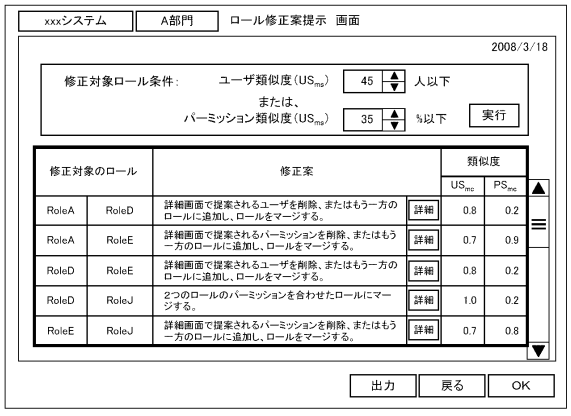
【図５０】

本実施例に係る類似度の計算結果を
表示する画面の構成例を示す図



【図５１】

本実施例に係るロール修正案提示を
表示する画面の構成例を示す図

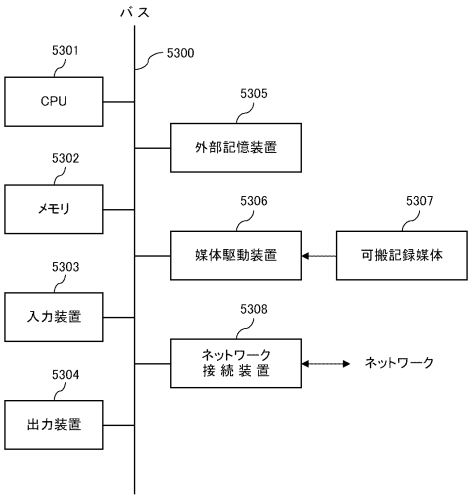


【図５２】

本実施例に係るロール修正案の詳細を
表示する画面の構成例を示す図

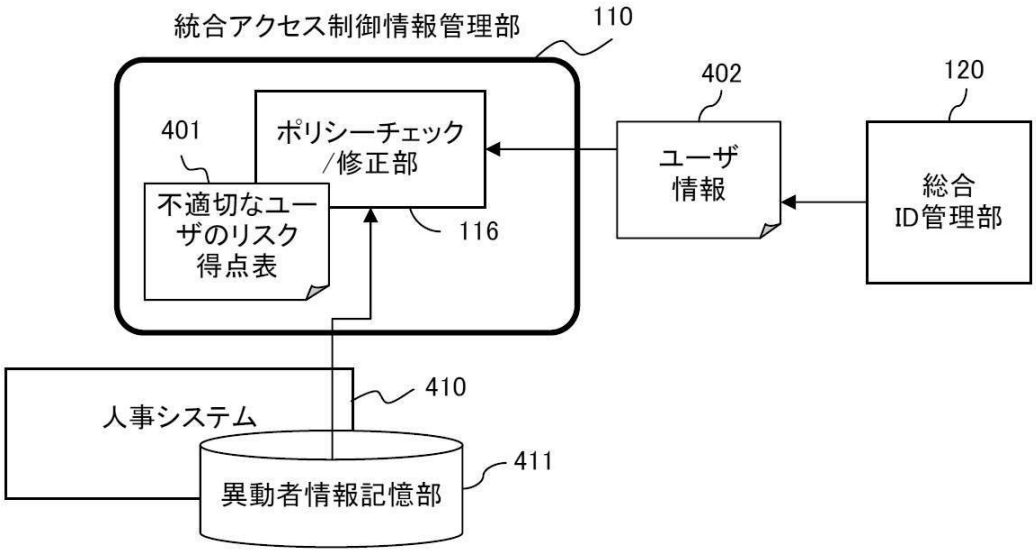
【図５３】

本実施例に係る
統合セキュリティ管理システムの
具体的な構成例を示す図



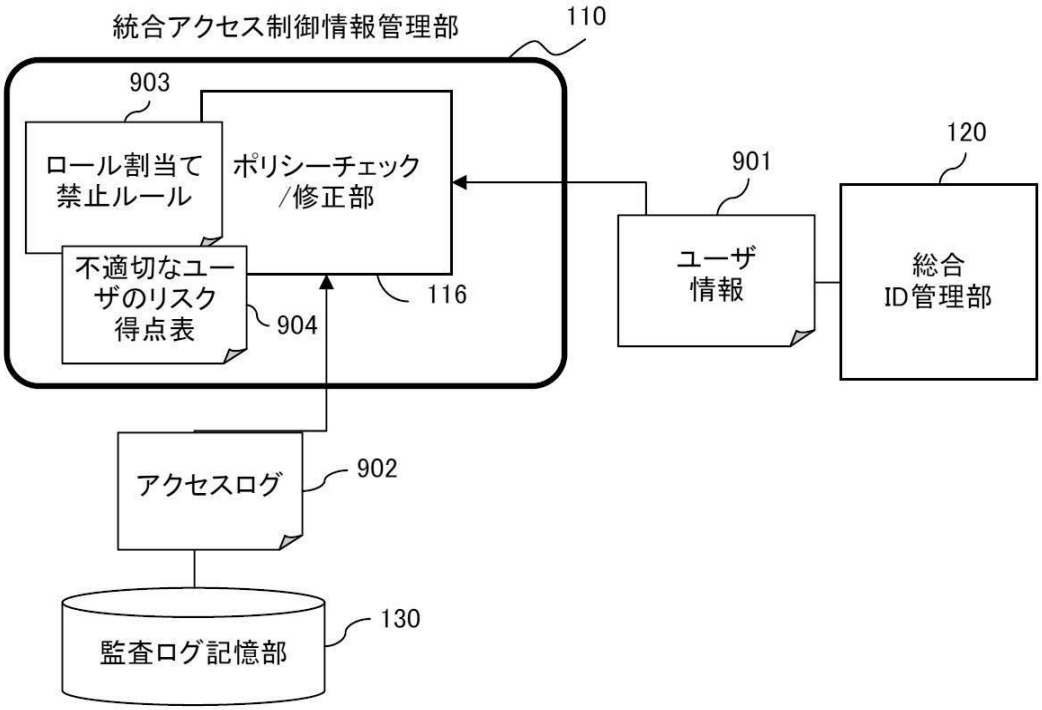
【図４】

本実施例に係る不適切な
ユーザアカウントの検出処理の概要を示す図



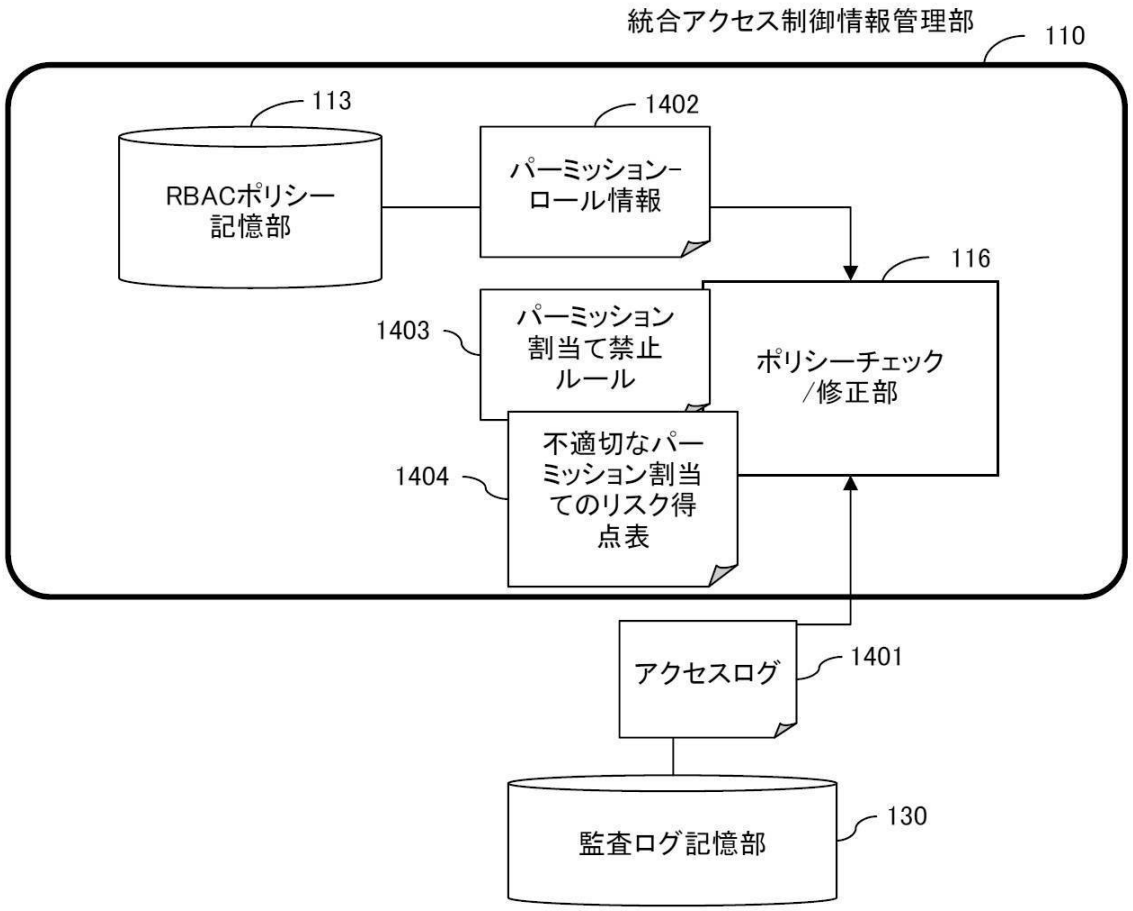
【図９】

本実施例に係る不適切なユーザーロール割当ての検出処理の概要を示す図



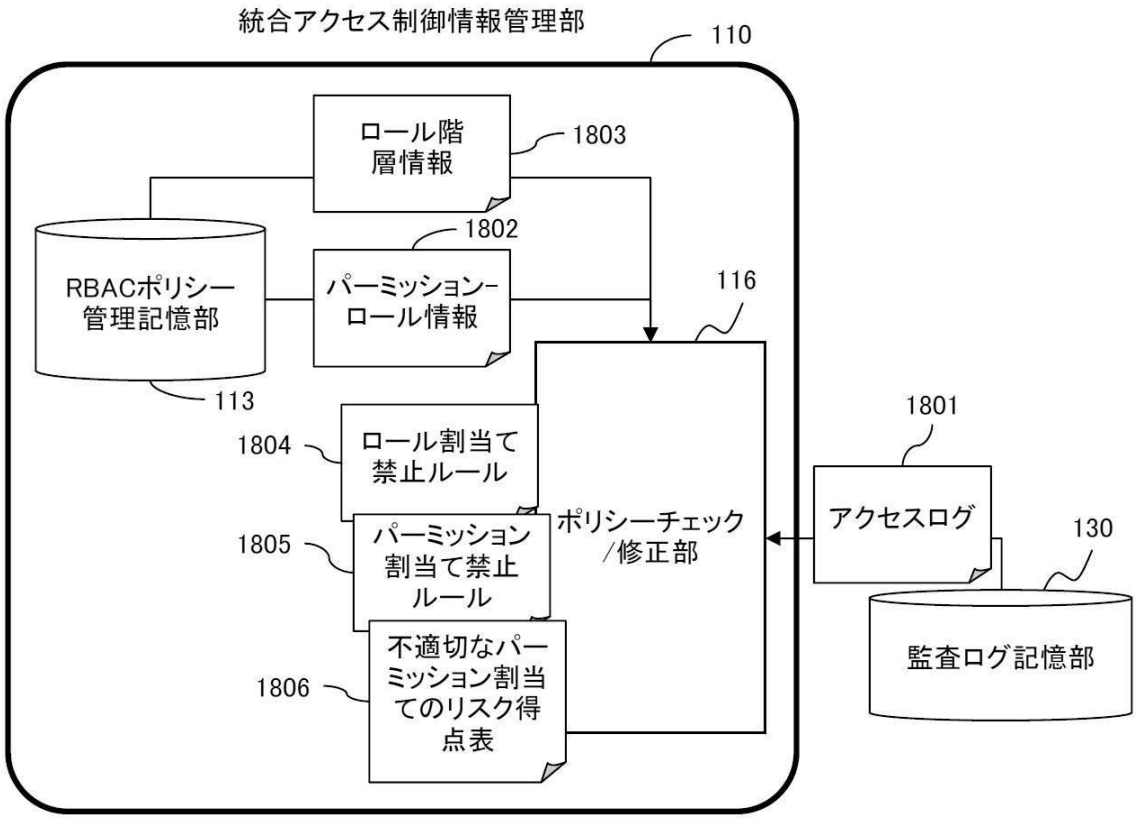
【図１４】

本実施例に係る不適切な
パーミッション－ロール割当ての
検出を行なうための構成例を示す図



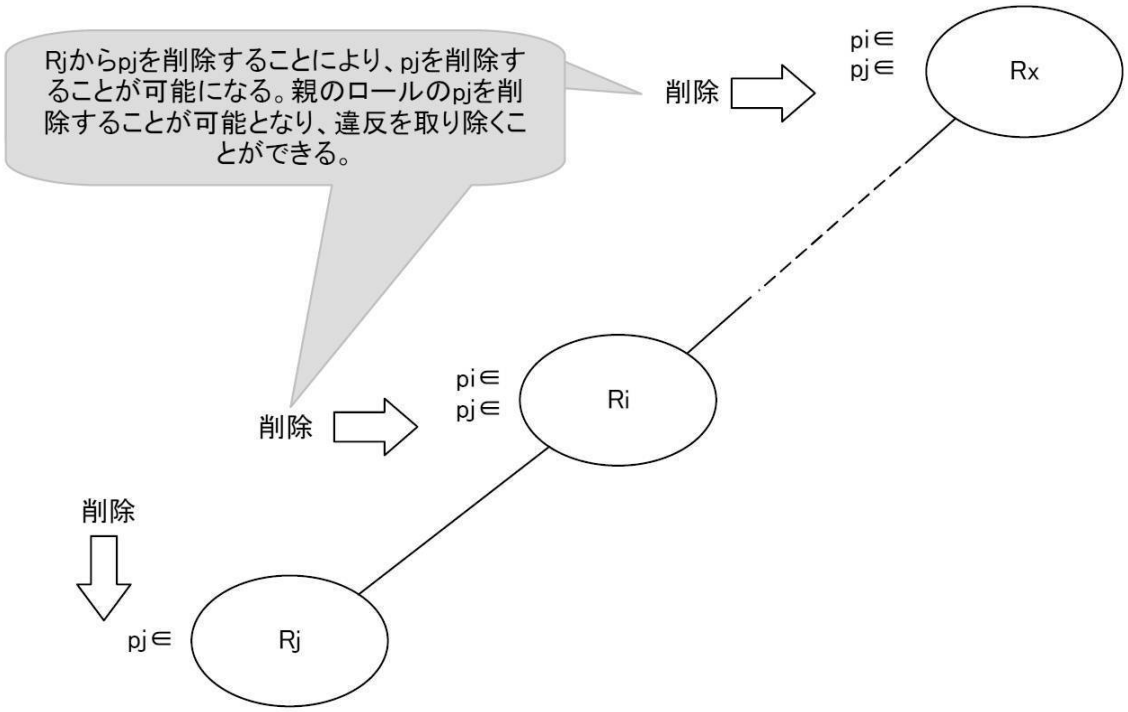
【図１８】

本実施例に係る不適切なロールの
検出を行なうための構成例を示す図



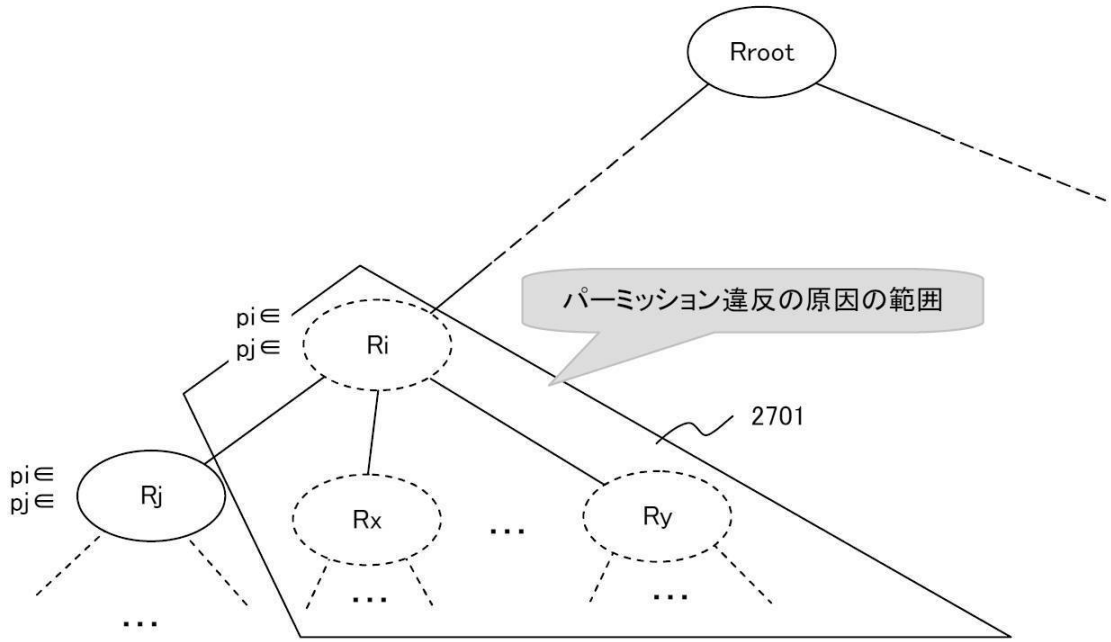
【図２６】

違反の原因となるロールを説明する図



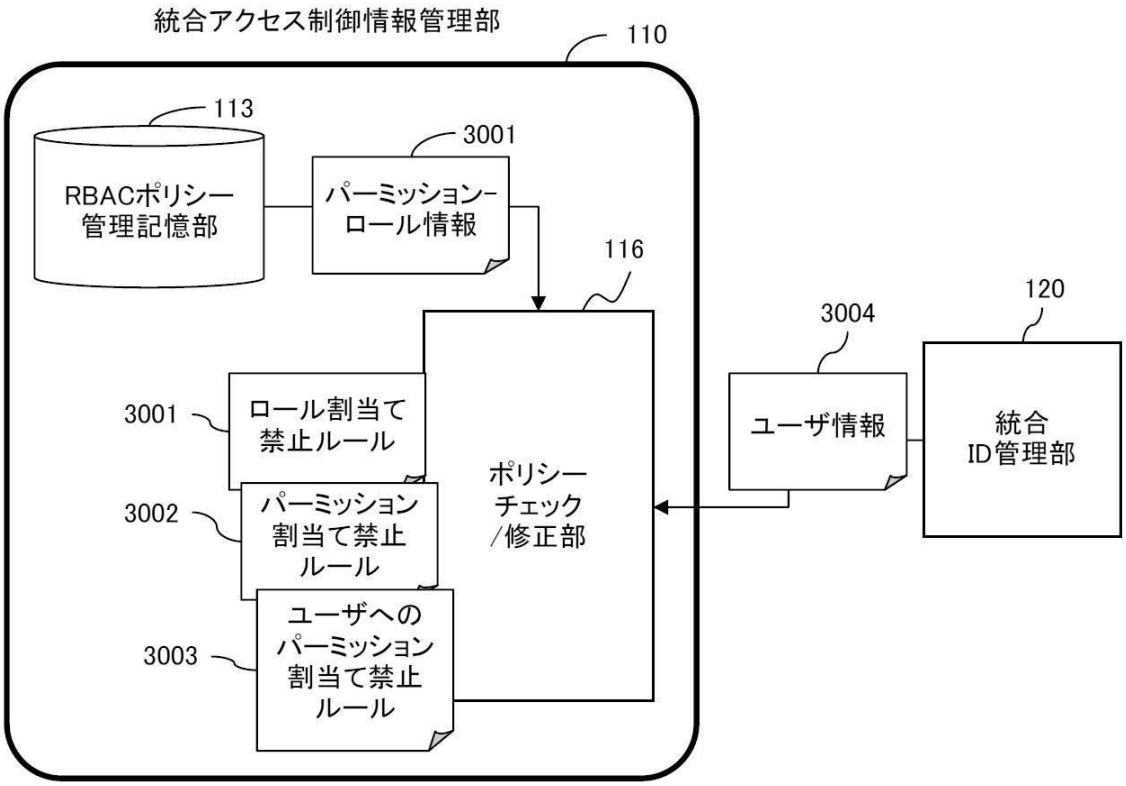
【図２７】

違反の原因となるロールを説明する図



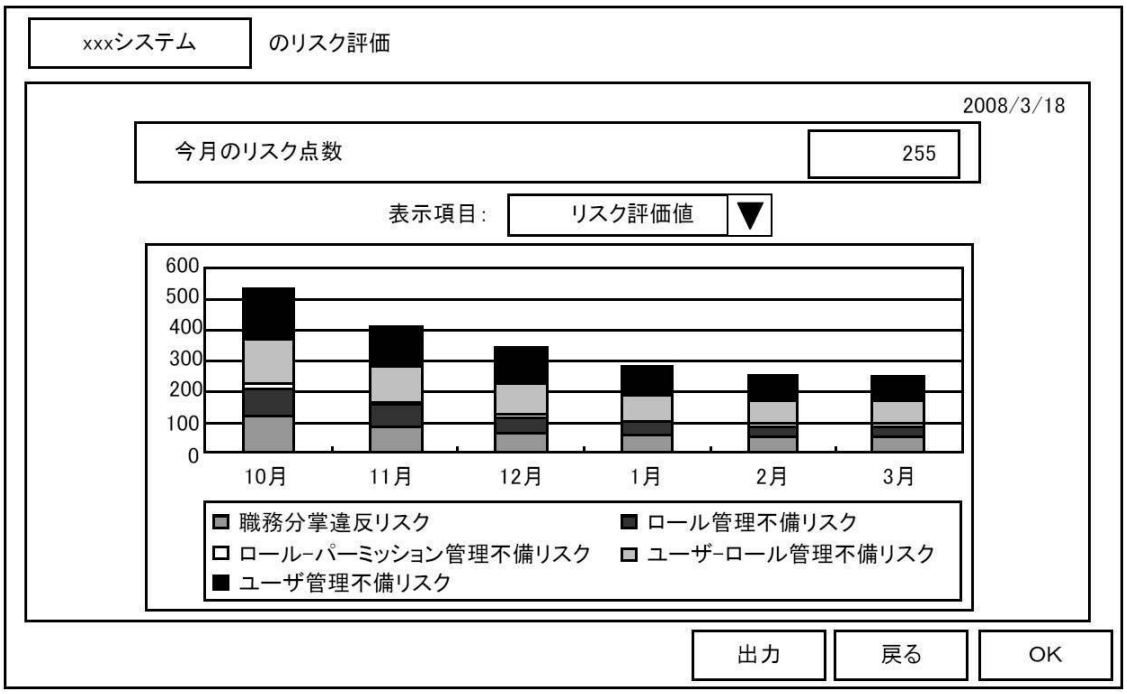
【図３０】

本実施例に係る職務分掌違反の検出を
行なうための構成例を示す図



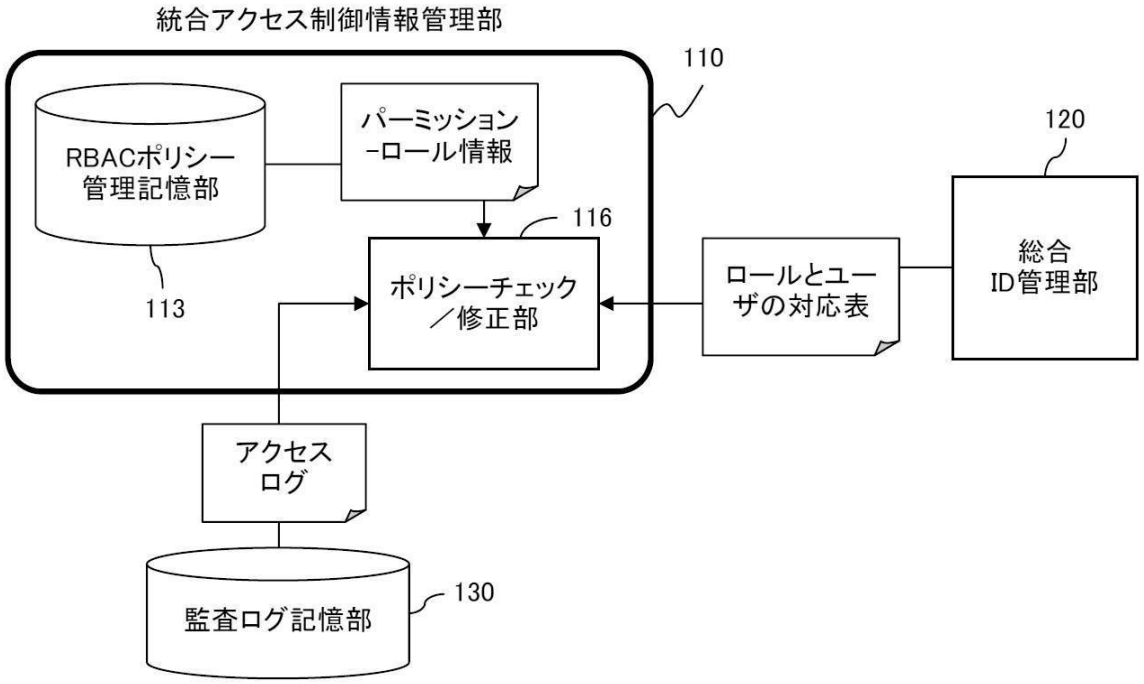
【図３９】

「月間推移表示」ボタンを押下したときに
表示されるリスク値の推移の
画面の構成例を示す図



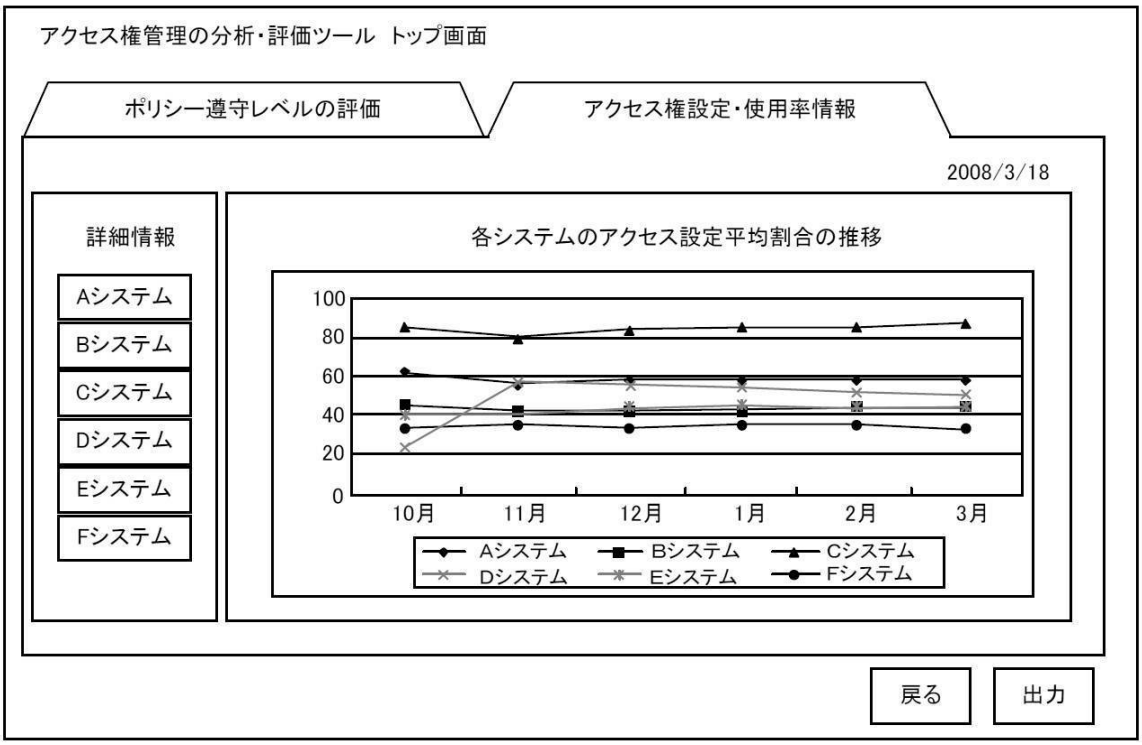
【図４０】

本実施例に係る無駄なアクセス権設定を
検出するための構成例の概要を示している



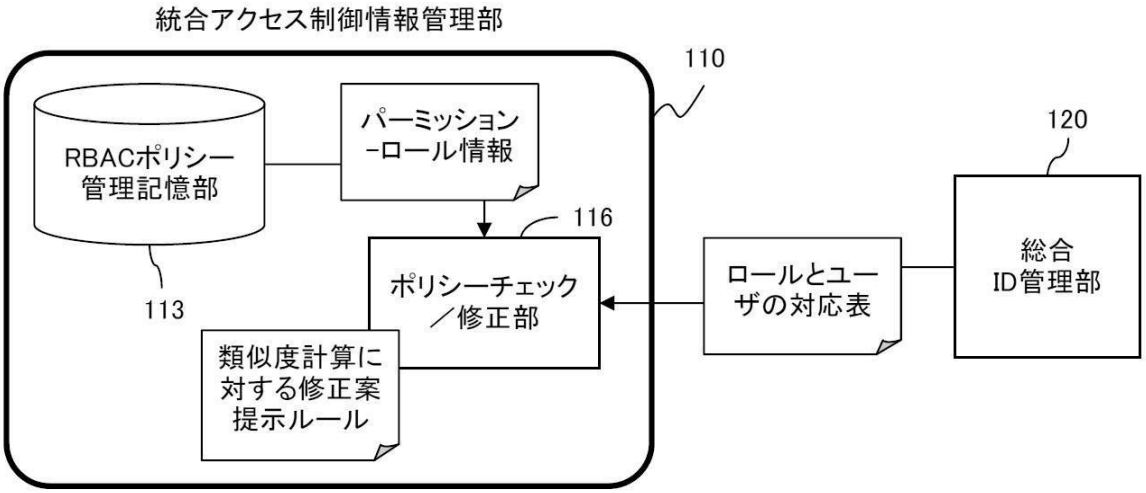
【図４５】

各システムのアクセス権設定の
平均割合推移を表示する画面の
構成例を示す図



【図４７】

本実施例に係る一致や類似したロールを
発見するための構成例を示している



フロントページの続き

(72)発明者　長谷部　高行
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　寺田　剛陽
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

審査官　平井　誠

(56)参考文献　特開２００２－３５２０６２（ＪＰ，Ａ）
米国特許出願公開第２００７／０１４３８５１（ＵＳ，Ａ１）
米国特許出願公開第２００６／０００５２５４（ＵＳ，Ａ１）
米国特許出願公開第２００７／０１４３８２７（ＵＳ，Ａ１）
米国特許出願公開第２００８／００７２３２８（ＵＳ，Ａ１）
あなたは狙われている！セキュリティ２４時第１回，Ｗｉｎｄｏｗｓ　ＮＴ　Ｗｏｒｌｄ　Ｖｏｌ．４　Ｎｏ．４，日本，株式会社ＩＤＧコミュニケーションズ，１９９９年　４月　１日，第4巻，p.166-169
ウイルス・不正侵入に強いネットワークを目指そう！　ゼロから始める“安全”社内ＬＡＮの作り方，ＮＥＴＷＯＲＫ　ＭＡＧＡＺＩＮＥ　第１０巻　第４号，日本，株式会社アスキー，２００５年　４月　１日，第10巻，p.150-153

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１