明　細　書

発明の名称 ：

アクセス制御装置、アクセス制御方法、およびプログラム

技術分野

[0001] 本発明は、アクセス制御装置、アクセス制御方法、およびプログラムに関する。

背景技術

[0002] 企業や公共施設などの運用を支える業務情報システム、いわゆるエンタープライズシステム（Enterprise System）は、今や、大小さまざまな組織の基盤となっている。業務情報システムは、ノード端末やデータベースから得られるデータを集計、蓄積、解析、加工した上でより付加価値の高い情報を出力することにより、複雑化する組織マネジメントを支えている。

[0003] このような業務情報システムは、稼働後も、アクセスルール監視、障害対応、機能拡張や機能変更などのさまざまなメンテナンス作業を必要とする。通常、業務情報システムを導入するクライアント企業は、外部の管理会社にこのメンテナンス作業を委託する。外部の管理会社のＳＥ（System Engineer）は、業務情報システムにリモートログインしてメンテナンス作業を行うことが多い。

[0004] ところで、近年、アメリカで成立したＳＯＸ（Sarbanes‐Oxley）法は、企業経営者や会計監査人に対して公開情報の正当性を保証するように強く求めている。これに倣って、日本でも日本版ＳＯＸ法が導入されたため、日本版ＳＯＸ法に対応できる態勢の確立が急務となっている。

[0005] このような社会背景に鑑みて、特許文献１～５に示すように、業務情報システムの情報セキュリティを高めるための様々な技術が提案されている。

先行技術文献

特許文献

[0006] 特許文献1：特開２０１２－２０３６２４号公報

特許文献2：特開２００８－２２６０５７号公報

特許文献3：特開２００８－２２６０５８号公報

特許文献4：特許２００８－１１７３１６号公報

特許文献5：特許２００８－１１７３１７号公報

発明の概要

発明が解決しようとする課題

[0007] 特許文献１～５に示す技術を用いた業務情報システムのシステム管理者は、ユーザの所属する会社、所属部署、役職（担当ロール）、ノード名（端末名）、ノードグループ名（システム名）およびポリシー（たとえば、ログ取得の有無、接続元ＩＰアドレス規制の有無、接続可能プロトコルの指定、事前承認の有無等の様々なアクセスルール）などを指定して業務情報システムを利用するユーザに対して詳細なアクセス制御を実現している。

[0008] ところで、システム管理者は、ユーザの作業内容に応じてユーザに設定したアクセスルールを追加したり、変更する場合がある。そのため、結果として多くのアクセスルールをユーザに対して設定することになり、これらのアクセスルールの組み合わせが複雑に絡み合ってアクセス制御を実行することになると、設定したシステム管理者自身であってもアクセス制御の管理が困難になるという状況がある。また、このような状況は、監査を実施する者にとっても、実際にユーザに設定されたアクセスルールに基づいて適切なアクセス制御がなされているのか否かについて把握することが困難である。

[0009] 本発明は、上述した課題を鑑みてなされたものであり、アクセス制御の管理が容易であると共に、適切なアクセス制御で運用されているか否かについて容易に確認することができるアクセス制御装置、アクセス制御方法、およびプログラムを提供することを目的とする。

課題を解決するための手段

[0010] 本発明の一側面は、アクセス制御装置に関するものである。すなわち、本発明に係るアクセス制御装置は、所定のシステムを構成するサーバに対するクライアント端末のアクセスを制御するアクセス制御装置であって、所定の

システムの管理者により作成された１または複数のアクセスルールから、クライアント端末にログインしたユーザが利用するアクセスルールを選択させるための選択画面情報を生成する画面生成部と、選択画面情報に基づいて表示されるアクセスルールから選択されたアクセスルールに従ってユーザのアクセス制御を実行するアクセス制御部と、を有することを特徴とする。

[0011] また、上述した構成に加えて、所定のシステムの管理者により作成された１または複数のアクセスルールを記憶する第１の記憶部と、画面生成部により生成された選択画面情報に基づいて表示される１または複数のアクセスルールからユーザが選択したアクセスルールをユーザのアクセス制御を実行する際に適用するアクセスルールとして記憶する第２の記憶部とを有することができる。

[0012] また、上述した構成に加えて、画面生成部は、クライアント端末からユーザが利用可能となっているアクセスルールについて問い合わせ要求がなされた場合に、第２の記憶部を参照してユーザが利用可能となっているアクセスルールを特定すると共に、問い合わせ要求をしてきたユーザもしくはユーザが所属する所定のユーザグループと関連付けられているアクセスルールを特定可能な名称を示す特定画面情報を生成することができる。

[0013] また、上述した構成に加えて、第１の記憶部に記憶されているアクセスルールを検索するルール検索支援部を有し、ルール検索支援部は、ユーザからアクセスルールの検索を要求された際に、アクセスルール名または接続先ノード名を指定してアクセスルールの検索ができる画面情報を生成することができる。

[0014] また、上述した構成に加えて、第１の記憶部に記憶されているアクセスルールを検索するルール検索支援部を備えており、ルール検索支援部は、ユーザもしくはユーザが所属する所定のユーザグループが過去に使用したアクセスルールを示す画面情報を生成することができる。

[0015] また、本発明の一側面は、アクセス制御方法に関するものである。すなわち、本発明に係るアクセス制御方法は、所定のシステムを構成するサーバに

対するクライアント端末からのアクセスを制御するアクセス制御方法であって、所定のシステムの管理者により作成された１または複数のアクセスルールから、クライアント端末にログインしたユーザが利用するアクセスルールを選択させるための選択画面情報を生成する画面生成ステップと、選択画面情報に基づいて表示されるアクセスルールから選択されたアクセスルールに従ってユーザのアクセス制御を実行するアクセス制御ステップと、を有することを特徴とする。

[0016] 本発明の一側面は、プログラムに関するものである。すなわち、本発明に係るプログラムは、所定のシステムを構成するサーバに対するクライアント端末からのアクセスを制御するアクセス制御装置としてコンピュータを機能させるためのプログラムであって、コンピュータを、所定のシステムの管理者により作成された１または複数のアクセスルールから、クライアント端末にログインしたユーザが利用するアクセスルールを選択させるための選択画面情報を生成する画面生成手段と、選択画面情報に基づいて表示されるアクセスルールから選択されたアクセスルールに従ってユーザのアクセス制御を実行するアクセス制御手段として機能させることを特徴とする。

発明の効果

[0017] 本発明によれば、アクセス制御の管理が容易であると共に、適切なアクセス制御で運用されているか否かについて容易に確認することができるアクセス制御装置、アクセス制御方法、およびプログラムを提供することができる。

図面の簡単な説明

[0018] [図1]本発明のアクセス制御装置の一実施の形態を含む業務情報システムの構成例を示すブロック図である。

[図2]図１に示す業務情報防護装置の機能構成例を示すブロック図である。

[図3]図２に示す実行条件保持部における実行条件情報のデータ構成の例を示す図である。

[図4]ログ保持部で保持されるアクセスログの記録内容の例を示す図である。

[図5]ログイン画面例を示す図である。

[図6]アクセス申請画面例を示す図である。

[図7]アクセス申請者がポリシー名を検索する際に表示される画面例を示す図である。

[図8]アクセス承認画面例を示す図である。

[図9]システム管理者がポリシー名を検索する際に表示される画面例を示す図である。

[図10]図６および図８において選択可能なアクセスルールの具体例について説明するための図である。

[図11]図１０に示すアクセスルールのうち、社員に関するロールに着目したアクセスルールを説明するための図である。

[図12]図１０に示すアクセスルールのうち、協力会社に関するロールに着目したアクセスルールを説明するための図である。

[図13]図１０に示すアクセスルールのうち、ベンダに関するロールに着目したアクセスルールを説明するための図である。

[図14]アクセスログ検索画面例を示す図である。

[図15]検索結果画面例を示す図である。

[図16]アクセスチェック処理について説明するフローチャートである。

発明を実施するための形態

[0019] ［業務情報システムの構成］

図１は、本発明のアクセス制御装置の一実施の形態を含む業務情報システムの構成例を示すブロック図である。同図に示す業務情報システムは、業務情報防護装置１０と作業用端末２０がネットワーク３０を介して接続されているとともに、クライアント環境４０が、業務情報防護装置１０を介してネットワーク３０に接続されている。また業務情報防護装置１０には、ログ管理装置１５も接続されている。

[0020] 図１に示す業務情報システムにおいて、クライアント環境４０は、ある企業Ａの業務環境を示す。クライアント環境４０の各種業務システムは、稼働

後も、適宜メンテナンス作業を受ける。このメンテナンス作業は、クライアント環境４０内で行われることもあるが、多くは作業用端末２０からのリモートアクセスにより実行される。このリモートのメンテナンス作業を行うユーザのことを、以下、単に「作業者」とよぶ。作業者は、通常、企業Ａとメンテナンス作業契約を交わした管理会社のＳＥ（Systems Engineer）であることが多いが、企業Ａの社員であることもある。作業者は、作業用端末２０に自己に割り振られたユーザを使用してログインし、ネットワーク３０および業務情報防護装置１０を介して、クライアント環境４０の各種業務情報システムにリモートログインする。作業用端末２０と業務情報防護装置１０の間の通信経路は、ＶＰＮ（Virtual Private Network）などによりセキュアな通信経路であることが望ましい。

[0021] 以下において、ネットワーク３０は、インターネットやローカルエリアネットワーク（ＬＡＮ）等の公用回線を介したリモートアクセスを前提として説明するが、業務情報防護装置１０やクライアント環境４０、作業用端末２０は、互いに専用回線にて接続されてもよい。

[0022] また、本明細書においては、各種の業務情報システムの運用により組織業務を実行する側の企業であって、外部の作業用端末２０からメンテナンス作業というサービスを受けるクライアントという意味で「クライアント企業」や「クライアント環境」という用語を使用するものとする。また、本明細書における「アクセス制御」とは、主にコンピュータセキュリティによるアクセス制御を意図しており、あるサブジェクト（能動体、クライアント端末など）が、どのオブジェクト（システム、ファイル、サーバなど）に対する処理（たとえばファイルであれば読み取り／書き込み／実行など）を許可するか否か、あるいは許可する接続手段（たとえば、サーバであれば使用可能なプロトコル、ポートなど）について制御することを指す。なお、コンピュータセキュリティによるアクセス制御は、一般的には、認証（authentication）、認可（authorization）、監査（audit）からなるが、これ以外の処理が含まれてもよいし、これらをすべて含んでいなくてもよい。

[0023] 業務情報防護装置１０は、作業用端末２０からクライアント環境４０へのリモートログイン要求を一元的に受け付ける装置であって、ネットワークセキュリティ境界に設置される。業務情報防護装置１０は、TELNET（Telecommunication network）、SSH（Secure SHell）、FTP（File Transfer Protocol）、HTTP（HyperText Transfer Protocol）、HTTPS（Hypertext Transfer Protocol Security）、WindowsRDP（Remote Desktop Protocol）、CIFS（Common Internet File System）などの通信プロトコルのアクセス制御、およびログ取得による監査を行う。

[0024] 業務情報防護装置１０は、以下の２段階の判定が共に肯定判定となったことを条件として、作業用端末２０からクライアント環境４０へのリモートログインを許可する。

１．作業者があらかじめ登録されているユーザであるか（以下、「ユーザ認証」とよぶ）

２．作業者がメンテナンス作業を実行することを事前に（正しく）申請済みであるか（以下、「申請判定」とよぶ）

[0025] 業務情報防護装置１０は、中継装置１１、ユーザ認証装置１２、およびアクセス制御装置１４を含む。なお、業務情報防護装置１０は、中継装置１１、ユーザ認証装置１２、およびアクセス制御装置１４の各機能を一体として備える単一の装置で構築されていてもよい。

[0026] 中継装置１１は、作業用端末２０よりネットワーク３０を介してアクセスされると、作業用端末２０のＩＰアドレスやホスト名などを確認し、接続許可対象外であった場合には、直ちに切断し、接続を許可しない。一方、接続許可対象であった場合には、中継装置１１は、作業用端末２０にユーザＩＤとパスワードを要求し、その要求に応じて送信されてきたユーザＩＤとパスワードを、ユーザ認証装置１２、およびアクセス制御装置１４に供給し、確認を依頼する。

[0027] ユーザ認証装置１２は、中継装置１１に代わって「ユーザ認証」を実行する。まず、作業用端末２０のユーザは、中継装置１１にリモートログインす

る。このときユーザＩＤとパスワードがネットワーク３０を介して中継装置１１に送信される。ユーザ認証装置１２は、中継装置１１からユーザＩＤとパスワードを受け取ってユーザ認証を実行し、その結果を中継装置１１に返す。

[0028] アクセス制御装置１４は、中継装置１１からユーザＩＤとパスワードを受け取って「申請判定」を実行する。作業者は、業務情報システムへのリモートログインに先立って、どのような作業をいつ実行する予定であるかをあらかじめ申請しなければならない。アクセス制御装置１４は、このような作業予定を一元的に管理しており、作業者からのリモートログイン要求を受け付けると、その作業者がなんらかのメンテナンス作業を事前に申請しているか否かを確認する。

[0029] また、アクセス制御装置１４は、中継装置１１に代わって「アクセス権認証」を実行する。つまり、アクセス制御装置１４は、中継装置１１からユーザＩＤとパスワード、およびアクセス先を示す情報（ＩＰアドレスやホスト名など）を受け取って、ユーザがアクセス先へ接続を許可されているか（アクセス権があるか）否かの認証を実行し、その結果を中継装置１１に返す。業務情報システムへのアクセスが許可される条件は、ユーザ認証に成功し、かつ、作業申請済みであることである。

[0030] なお、作業者はクライアント環境４０でのメンテナンス作業を開始する前に、作業用端末２０を介してアクセス制御装置１４に作業申請情報を送信する処理（この処理を以下、「アクセス申請」という。）を行う。ここでいう作業申請情報とは、たとえば作業目的、作業日時、件名、アクセス対象となるシステム名、適用するアクセスルール名などの入力データの集合であるが、このほかにも、申請者のメールアドレス、申請日時など、入力されたデータ以外の付帯情報が含まれてもよい。なお、上述のアクセスルールとは、メンテナンス作業をするユーザ名、メンテナンス作業をするユーザが属しているユーザグループ名（ロール名）、メンテナンス作業が実行されるノード名、メンテナンス作業が実行されるノードが属しているノードグループ名（シ

ステム名）、ログ取得のＯＮ／ＯＦＦ、接続元のＩＰアドレス規制、接続可能プロトコル、事前承認の有無などのいずれか１つ、またはこれらを複数組み合わせて作成されるポリシーをそれぞれ組み合わせて構成される制御ルールのことである。

[0031] なお、「アクセス申請」は、作業用端末２０から実行されるとしたが、これに限らず、たとえば、作業用端末２０とは異なる申請用端末（図示せず）から実行されるようにしてもよい。

[0032] また、アクセス制御装置１４は、ユーザからの「アクセス申請」で申請されたアクセスルールに基づいてそのユーザのアクセス制御を実行することができる。なお、このアクセスルールはクライアント環境４０のシステム管理者により予め作成、設定されている。ユーザはシステム管理者により作業内容、職位などに応じて作成、設定されたアクセスルールの中から適用するアクセスルールを選択することができる（詳細は後述）。

[0033] 中継装置１１、ユーザ認証装置１２、およびアクセス制御装置１４は、それぞれ正系と副系の２台のサーバからなり、フェールオーバー機能を有している。すなわち、何らかの理由で正系のサーバに障害が発生した場合、副系のサーバに正系のサーバのＩＰアドレスが付加されるように構成されている。具体的には、正系のサーバと副系のサーバには、それぞれ実ＩＰとバーチャルＩＰを所有しており、副系のサーバが正系のサーバを監視し、異常を検知したときに、正系のバーチャルＩＰを取得する。作業者は、バーチャルＩＰに対してアクセスするようになされており、異常発生時には、正系から副系のサーバへのアクセスに自動的に切り替わる。これにより、作業者は、正系のサーバに障害が発生したことを意識することなく、副系のサーバを利用してサービスを継続することができる。

[0034] ログ管理装置１５は、中継装置１１で行われるアクセスの内容を取得し、管理する。例えば、アクセス日時やＩＰアドレスといった「サマリーログ」や送受信されたデータの「全文ログ」が取得され、管理される。

[0035] ログ管理装置１５は、アクセス制御装置１４で管理される作業申請内容と

ログ管理装置１５で管理されるアクセスログを紐付けて管理しており、アクセスチェックを容易に行うことができる。アクセスチェックとは、アクセスログを捜査し、申請された通りのアクセスを行っているか否かのログ監査を行うことである。なお、ログ管理装置１５と業務情報防護装置１０が単一の装置で構成されていてもよい。

[0036] 作業用端末２０は、作業者によって、クライアント環境４０へリモートログインするためのユーザＩＤとパスワードが入力されると、そのユーザＩＤとパスワードをリモートログイン要求として、ネットワーク３０を介して業務情報防護装置１０に送信する。

[0037] クライアント環境４０は、財務情報システム４１、顧客情報システム４２、在庫管理システム４３という３種類の業務情報システムと、１以上の承認用端末４４を含む。財務情報システム４１は、企業Ａの財務情報を管理するシステムである。顧客情報システム４２は、企業Ａの顧客情報を管理するシステムである。在庫管理システム４３は、企業Ａの商品の在庫状態を管理するシステムである。承認用端末４４は、ウェブブラウザを搭載した一般的なＰＣ端末である。承認用端末４４は、必ずしもクライアント環境４０に属する必要はなく、ノートＰＣなどの携帯端末であってもよい。

[0038] 図２は、業務情報防護装置１０およびログ管理装置１５の機能構成例を示すブロック図である。

[0039] 図２に示す各ブロックは、ハードウエア的には、コンピュータのＣＰＵをはじめとする素子やＲＡＭ，ＲＯＭ，ＨＤＤなどの記憶装置で実現でき、ソフトウエア的にはコンピュータプログラム等によって実現されるが、ここでは、それらの連携によって実現される機能ブロックを示している。したがって、これらの機能ブロックはハードウエア、ソフトウエアの組合せによっていろいろなかたちで実現することができる。

[0040] Ａ：中継装置１１

中継装置１１のログインインタフェース処理部１１１は、作業用端末２０からのリモートログイン要求を受け付ける。このリモートログイン要求には

、ユーザＩＤとパスワードが含まれる。中継装置１１は、受け付けたユーザＩＤとパスワードを、ユーザ認証装置１２によるユーザ認証処理、アクセス制御装置１４による申請判定処理、アクセス権認証処理のために転送する。またログインインタフェース処理部１１１は、作業用端末２０からアクセス先を示す情報（ＩＰアドレスやホスト名など）を取得したとき、取得した情報をアクセス制御装置１４によるアクセス権認証処理のために転送する。そしてログインインタフェース処理部１１１は、ユーザ認証装置１２、アクセス制御装置１４から、それぞれの判定結果を受け取る。以下、ユーザＩＤやパスワードのように、ユーザを識別するためのデータのことを「ユーザ識別情報」とよぶ。変形例として、ユーザ識別情報は、指紋や虹彩などの生体情報であってもよい。

[0041] 中継装置１１は、単一の装置でなくてもよい。たとえば、財務情報システム４１用の中継装置１１と、顧客情報システム４２用の中継装置１１は別々であってもよい。あるいは、作業者は、複数の中継装置１１のうち任意の中継装置１１を介して目的とする業務情報システムにアクセスしてもよい。中継装置１１を複数設けることは、負荷分散や可用性の面からも好ましい。同様に、ユーザ認証装置１２、アクセス制御装置１４も、負荷分散や可用性の面から複数設けるようにしてもよい。

[0042] Ｂ：ユーザ認証装置１２

ユーザ認証装置１２は、ユーザ認証部１２１と正規ユーザ情報保持部１２２を含む。ユーザ認証部１２１は、中継装置１１のログインインタフェース処理部１１１がリモートログイン要求を受け付けたとき、ログインインタフェース処理部１１１からそのユーザＩＤとパスワードを取得する。そして、その送信元のユーザが正規のユーザとして正規ユーザ情報保持部１２２に登録されているか否かを判定することによりユーザ認証を行う。正規ユーザ情報保持部１２２は、ユーザＩＤとパスワードを対応づけた正規ユーザ情報を保持する。この正規ユーザ情報に登録されているユーザのことを「正規ユーザ」とよぶ。ユーザ認証部１２１は、作業者だけでなく承認者についてもユ

ーザ認証を実行するが、詳細は後述する。なお、ユーザ情報保持部１２２は、ユーザ認証装置１２の内部に実装されているが、これに限らず、たとえば、ＬＤＡＰ（Lightweight Directory Access Protocol）サーバなどの外部装置であってもよい。

[0043] 本実施の形態におけるユーザ認証装置１２は単一の装置であり、ユーザ識別情報を一元的に管理する。複数の業務情報システムと複数の関係者をつなぐユーザ認証を単一のユーザ認証装置１２にて実行することにより、ユーザ認証ポリシー（policy）を管理しやすい構成となっている。しかしながら、ユーザ認証装置１２で管理している正規ユーザと、クライアント環境４０における財務情報システム４１、顧客情報システム４２、在庫管理システム４３におけるユーザとは異なるユーザとして管理、構成するようにしてもよい。

[0044] Ｃ：アクセス制御装置１４

アクセス制御装置１４は、ユーザからの「アクセス申請」を受け付けると共に、この「アクセス申請」に基づいて登録された作業申請情報に基づいて「申請判定」を行う機能を有している。

[0045] アクセス制御装置１４は、申請状態管理部１３１、アクセスルール選択画面生成部１３２、アクセスルール特定画面生成部１３３、申請状態判定部１３４、アクセス制御部１３５、アクセス権認証部１３６、実行条件保持部１３７、実行履歴保持部１３８、作業予定保持部１３９、アクセスルール保持部１４０、アクセス権情報保持部１４１とを含む。

[0046] 申請状態管理部１３１は、「アクセス申請」に関する処理を担当する。申請状態管理部１３１は、作業用端末２０から作業申請情報を受信すると、実行条件保持部１３７に登録されている実行条件情報（不図示）と適合しているかを判定する。申請状態管理部１３１は、作業申請情報が実行条件情報と適合していないと判定した場合、申請を却下し、その旨を作業用端末２０の作業者に通知する。申請状態管理部１３１は、作業申請情報が実行条件情報と適合していると判定した場合、作業予定保持部１３９の作業予定情報に、

申請された作業を登録する。こうして作業予定情報に登録された作業申請のことを「有効な作業申請」とよぶ。作業予定情報の内容は、作業申請情報の内容と実質的に同等であってもよい。すなわち、受信された作業申請情報のうち、有効な作業申請としての要件を満たす作業申請情報だけが「作業予定情報」として作業予定保持部１３９に正式登録されることになる。

[0047] 申請状態管理部１３１は、有効な作業申請がなされると、作業を一意に識別するための申請ナンバー（作業ＩＤ）を付与する。作業予定情報では、申請ナンバー、作業予定日時、作業内容、作業者名、承認状態、適用するアクセスルールの名称等が対応づけられる。有効な作業申請さえ行えば作業開始可能なタイプのメンテナンス作業だけでなく、承認がなされなければ作業開始できないタイプのメンテナンス作業もある。実行条件情報の一部として、このような定義がなされていてもよい。なお、作業予定保持部１３９に登録されている作業予定情報のうち、作業予定日時を経過した作業については、過去に出された申請履歴の状態になり、却下された申請については、申請状態が「却下」として記録された状態になる。

[0048] 申請状態管理部１３１は、有効な作業申請が作業予定保持部１３９に登録されると、その申請された作業内容が承認を必要とするものであるか否かを、実行条件保持部１３７に登録されている実行条件情報を参照して判定する。申請状態管理部１３１は、メンテナンス作業が申請された場合、その申請ナンバーを承認者に通知する。本実施の形態における申請状態管理部１３１は、申請ナンバーを示す電子メールを承認用端末４４に送信する。承認者は、通知を受けると、承認用端末４４の図示せぬ入力部を操作し、申請ナンバーに基づいて業務情報防護装置１０のアクセス制御装置１４にアクセスし、承認可否を入力する。

[0049] 申請状態管理部１３１は、承認可否を承認用端末４４から受け付ける。申請状態管理部１３１は、承認がなされると、作業予定保持部１３９に登録されている作業予定情報における承認状態を「未承認」から「承認」に変更する。却下の場合には、申請状態管理部１３１は、作業者に申請却下の旨を通

知すると共に、作業予定保持部１３９に登録されている作業予定情報の申請状態を「却下」として記録する。

[0050] アクセスルール選択画面生成部１３２は、アクセスルールを選択するための画面情報を生成する。システム管理者は、アクセスルール選択画面生成部１３２が生成した画面情報に基づいて表示された１または複数のアクセスルールからユーザに対して利用可能とするアクセスルールを選択することができる。なお、アクセスルール選択画面生成部１３２は、システム管理者の管理負担を更に軽減させるために、アクセスルール毎の管理者を設定させるための設定画面情報の生成する機能、システム管理者からの認知度が高い「ポリシー名」、「ユーザ名」、「接続ノード名」等でアクセスルールを検索するための支援画面情報の生成する機能を有する。

[0051] アクセスルール特定画面生成部１３３は、申請状態管理部１３１が「アクセス申請」を受け付ける際に、ユーザが利用可能となっているアクセスルールを示す特定画面情報を生成する。この特定画面情報に基づいて表示されるアクセスルールは、上述したアクセスルール選択画面生成部１３２が生成した選択画面情報に基づいて表示されるアクセスルールからシステム管理者によって選択されることにより決定される。アクセスルールからユーザによって特定のアクセスルールが選択されると、後述する実行条件保持部１３７に実行条件情報として保持される。そして、この特定のアクセスルールに従ってユーザのアクセス制御が実行される。なお、アクセスルール特定画面生成部１３３は、ユーザがポリシー名をキーとして特定のアクセスルールを検索できるポリシー検索機能を有する。

[0052] 申請状態判定部１３４は、「申請判定」を実行する。作業者からリモートログイン要求が受け付けられたとき、ログインインタフェース処理部１１１から取得したユーザ識別情報と作業予定保持部１３９に登録されている作業予定情報を参照して、作業申請済か否かを判定する。また、申請状態判定部１３４は、リモートログイン要求の受信日時が、申請された作業時間内にあるか否かについても判定する。たとえば、「１０：００～１１：００」とい

う作業予定時間を指定して申請されているときには、１０：００以前や１１：００以後にリモートログイン要求をしてきても申請判定の結果は「否定」となり、リモートログインは許可されない。

[0053] アクセス制御部１３５は、「ユーザ認証」と「申請判定」が共に肯定判定となると、作業用端末２０からクライアント環境４０へアクセスするための通信経路を許可する。もちろん、承認が必要なメンテナンス作業が申請されているときには、承認済みでなければアクセス許可されない。なお、アクセス制御部１３５は、通信経路を許可した後の作業用端末２０のアクセス制御については、後述する実行条件保持部１３７に保持されている実行条件情報に基づいて随時アクセス制御を実行する。これにより、システム管理者により許可されたアクセスルールに従ったアクセス制御を実現している。

[0054] アクセス権認証部１３６は、中継装置１１のログインインタフェース処理部１１１がリモートログイン要求を受け付けたとき、ログインインタフェース処理部１１１からユーザＩＤとパスワード、およびアクセス先を示す情報（ＩＰアドレスやホスト名など）を取得し、その送信元のユーザがアクセス先に接続を許可されているか（アクセス権があるか）否かを、アクセス権情報保持部１４１に登録されているアクセス申請状況をもとに判定する。

[0055] 実行条件保持部１３７は、上述したアクセスルール特定画面生成部１３３により生成された画面情報に基づいて示される画面から選択されたアクセスルールを、メンテナンス作業での実行条件情報として保持する。図３に図２に示す実行条件保持部１３７における実行条件情報のデータ構成の例を示す。

[0056] 図３は、実行条件保持部１３７における実行条件情報のデータ構成の例を示す図である。実行条件情報は、各業務情報システムの管理者により定められたアクセスルールである。アクセスルールＩＤ欄１３７Ａには、アクセスルールを一意に識別するためのＩＤ（以下、「アクセスルールＩＤ」とよぶ）が示されている。アクセスルールＩＤは、アクセスルールが登録されるときに、割り当てられる。年月日欄１３７Ｂには、アクセスルールの適用日が

示されている。時間欄１３７Ｃには、アクセスルールの適用時間が示されている。たとえば、アクセスルールＩＤ「１」のアクセスルールは、企業Ａの営業日であって「６：００～１６：００」の時間帯に適用されることを意味している。

[0057] 作業種別欄１３７Ｄには、アクセスルールが適用されるメンテナンス作業の作業種別が示されている。承認要否欄１３７Ｅには、該当作業の実行をするために承認が必要か否かが示されている。この図３の例では、承認が必要な場合には「○」が記載されており、不要な場合には何も記載されていない。アクセスルール名欄１３７Ｆには、このアクセス申請による作業に適用されるアクセスルールの名称が示されている。なお、このアクセスルールの名称は後述するポリシー名であってもよい。図３の例では、たとえば、アクセスルールＩＤ「１」のアクセスルールＡが適用されるのは、「営業日」の「６：００～１６：００」における作業種別「０１」の「障害対応」を目的としたメンテナンス作業と、作業種別「０２」の「調査」を目的としたメンテナンス作業であり、これらについては承認不要である。すなわち、営業日の「６：００～１６：００」中を作業予定日時として障害対応を目的としたメンテナンス作業を行う場合には、作業者はあらかじめその旨を示す作業申請行うだけでよく、承認は不要である。

[0058] またアクセスルールＩＤ「２」のアクセスルールＢが適用されるのは、「営業日」の「６：００～１６：００」における作業種別「０３」の「稼働監視」を目的としたメンテナンス作業と、作業種別「０４」の「リリース作業」を目的としたメンテナンス作業であり、これらについては承認が必要である。すなわち、営業日の「６：００～１６：００」において、「稼働監視」や「リリース作業」を目的とするメンテナンス作業を実行する場合には、作業申請だけでなく承認がなされていなければアクセスできない。たとえば、ある作業者が、営業日の「６：００～１６：００」中の日時Ｔにリモートアクセス要求をしてきたとする。このとき、図３の例で示す実行条件情報に基づく申請判定の結果は以下の通りである。

[0059] １．日時Ｔを作業予定時間として含むような作業の申請がなされていない場合、否定判定となる。

２．日時Ｔを作業予定時間として含む障害対応作業が申請されていた場合、肯定判定となる。

３．日時Ｔを作業予定時間として含む稼働監視作業が申請されていた場合、申請状態判定部１３４は、作業予定保持部１３９を参照し、申請された稼働監視作業が承認済みであれば肯定判定する。未承認や却下の場合には、否定判定となる。

[0060] アクセス制御装置１４は、この図３に示すような実行条件情報を参照することで、ユーザに対応するアクセスルールを特定し、アクセス制御を実行することができる。

[0061] 実行履歴保持部１３８は、メンテナンス作業時に使用されたアクセスルール名とこのアクセスルール名を示すデータを基データとして算出されたハッシュ値の組み合わせを実行履歴情報として保持する。これにより、仮にメンテナンス作業後に実行履歴情報として記録されているアクセスルール名が変更された場合であっても、このアクセスルール名の組み合わせとして記録されているハッシュ値を確認することで、実際に利用されたアクセスルール名であるか否かについて確認することができる。すなわち、実行履歴情報の完全性を確保することができる。また、実行履歴保持部１３８が保持している実行履歴情報を参照するだけでどのようなアクセス制御がなされていたのかを確認することができる。すなわち、ユーザのアクセス制御の監査が容易になる。なお、実行履歴保持部１３８が保持している実行履歴情報は、後述するログ管理装置１５にて保存されるようにしてもよい。

[0062] 作業予定保持部１３９は、申請状態管理部１３１により正式登録された、有効な作業申請としての要件を満たす作業予定情報を保持する。

[0063] アクセスルール保持部１４０は、システム管理者により事前に作成されたアクセスルール情報を保持している。

[0064] アクセス権情報保持部１４１は、ユーザＩＤおよびアクセス先を示す情報

に対応づけたアクセス申請状況を保持する。

[0065] Ｄ：ログ管理装置１５

ログ管理部１５１は、作業用端末２０からクライアント環境４０へのアクセスログを管理する。ログ管理部１５１は、ログ記録部１５１Ａと作業検証部１５１Ｂを含む。ログ記録部１５１Ａは、リモートログイン要求の実行、作業用端末２０と業務情報システムの間で送受されるコマンドやデータ、その実行日時および適用しているアクセスルール名などをアクセスログとして記録する。記録時、ログ記録部１５１Ａは、申請状態管理部１３１で付与された申請ナンバーと、その申請ナンバーに対応する作業申請内容のアクセスログを結びつける。またログ記録部１５１Ａは、認証失敗や未申請、アクセス権無し等の拒否履歴のログも記録する。

[0066] 作業検証部１５１Ｂは、ログ保持部１５２で保持されているアクセスログの内容と、そのアクセスログに紐付けられた申請ナンバーに対応する、作業予定保持部１３９に登録されている作業予定情報とを比較して、不正アクセスがなされていないかをチェックする。

[0067] たとえば、「稼働監視」を目的とした作業申請がなされているときに、ファイルの書き換え処理の実行がなされたときには、作業検証部１５１Ｂは、ログ保持部１５２で保持されているアクセスログを参照して、このような不正アクセスを検出する。作業検証部１５１Ｂは、承認用端末４４に対して、不正アクセス、あるいは、不正アクセスの疑いのあるアクセスがあった旨を通知する。あるいは、不正アクセスが検出された時点で、アクセス制御部１３５はリモートアクセスを強制的に禁止してもよい。

[0068] ログ保持部１５２は、申請状態管理部１３１で付与された申請ナンバーと、その申請ナンバーに対応する作業申請内容のアクセスログを紐付けて保持する。ログ保持部１５２で保持するアクセスログの記録内容については、図４を参照して後述する。

[0069] 図４は、ログ保持部１５２で保持されるアクセスログの記録内容の例を示す図である。ログ保持部１５２は、サマリーログ記録領域１５２Ａと全文ロ

グ記録領域１５２Ｂを含み、サマリーログと全文ログの２種類のログを保持している。サマリーログは、アクセスの開始、終了時刻、利用端末、アクセス先サーバのＩＰアドレスやホスト名、利用ＩＤ、接続時間などを含む。全文ログは、実際にコマンドなどを実行・操作した内容を含む。

[0070] 図４の例の場合、サマリーログ記録領域１５２Ａと全文ログ記録領域１５２Ｂには、それぞれプロトコル毎に主な記録内容が保持されている。たとえば、「ＴＥＬＮＥＴ」のプロトコルの場合、サマリーログ記録領域１５２Ａには、アクセス開始日時、ポート、接続元ＩＰアドレス、ユーザＩＤ、接続先ＩＰアドレス、接続時間が記録され、全文ログ記録領域１５２Ｂには、受信データが記録される。

[0071] 以上示したアクセスログの記録内容が、申請ナンバーに紐付けてログ保持部１５２で保持される。なお、WindowsRDPで取得されるアクセスログは動画形式で記録される。なお、ログ管理装置１５側でアクセスルール名、アクセスルールＩＤなどを記録するようにしてもよい。

[0072] 図５は、ログイン画面例を示す図である。図５に示すログイン画面５０は、作業用端末２０から中継装置１１にリモートログイン要求するときに、作業用端末２０に表示される。中継装置１１は、リモートログイン要求を受け付けると、ログインウィンドウ５１を作業用端末２０のログイン画面５０内に表示させる。すなわち、中継装置１１のログインインタフェース処理部１１１が、作業用端末２０のユーザインタフェース画面を提供することになる。作業用端末２０のユーザは、ログイン画面５０内に表示されたログインウィンドウ５１上でユーザＩＤやパスワードを入力する。ユーザからみたユーザインタフェースは従来のターミナルサーバが提供するものと同じであるが、入力されたユーザ識別情報はユーザ認証装置１２、アクセス制御装置１４によってそれぞれユーザ認証、申請判定、アクセス権認証に供給される。

[0073] 図６は、アクセス申請画面例を示す図である。図６に示すアクセス申請画面６０は、作業者が作業申請のために、作業用端末２０からアクセス制御装置１４にアクセスするときに作業用端末２０に表示される。すなわち、申請

状態管理部１３１は、作業用端末２０からアクセスされると、作業用端末２０にアクセス申請画面６０を表示させる。

[0074] ポリシー検索ボタン６１は、申請者が利用可能なポリシー名を検索することができる。なお、ここでいうポリシー名は、図３で説明したアクセスルール名欄１３７Ｆにて記録されているアクセスルール名と同一の記載のものであってもよい。なお、申請者は、自分が作業をするときに適用されるポリシー名を直接入力することもできる。件名領域６２には、申請する作業の件名を入力する。システム分類領域６３からは、対象とする業務情報システムのタイプが選択される。ここでは、財務情報システム６４が選択されている。アクセス制御部１３５は、申請日時において、選択された業務情報システム以外へのユーザのアクセスを禁止するように制御してもよい。

[0075] システム名領域６４は、業務情報システムの名前を示し、作業種別領域６５は、作業種別を示す。内容入力領域６６は、作業内容などを自由記述するための領域である。添付ファイル領域６７は、利用する手順書等の電子ファイルを添付するための領域である。アクセス予定日時領域６８は、作業予定日時を示す。作業者は、申請画面６０に示される各項目にデータを入力した後、申請ボタン６９をクリックする。すると、作業用端末２０は、入力されたデータを作業申請情報としてアクセス制御装置１４に送信する。

[0076] アクセス申請時に、申請者名、件名、システム分類、システム名、作業種別、内容、およびアクセス予定日時、実際に利用する手順書等が記載された電子ファイルの添付、および適用するポリシー名を選択することにより、作業申請情報とともに付随する電子ファイルを一元管理することが可能となる。

[0077] 図７は、アクセス申請をするユーザがポリシー名を検索する際に表示される画面例を示す図である。この図７に示すポリシー検索画面７０は、図６で説明したポリシー検索ボタン６１が押下されると作業用端末２０側にて表示される画面例である。このポリシー検索画面７０では、ユーザがポリシー名の一部を入力して検索ボタン７１を押下すると、このユーザが利用可能でか

つ該当するポリシー名がリスト表示領域７２にリストアップされる。なお、リストアップされているポリシー名の横に配置されている詳細ボタン７３，７４を押下することで、該当するポリシーの詳細情報が別画面（不図示）で表示される。なお、ポリシー名の検索名が入力されずに、ただ単に検索ボタン７１が押下された場合には、このユーザ、またはこのユーザが所属するユーザグループで過去に使用されたポリシー名が検索されるようにしてもよい。

[0078] 図８は、アクセス承認画面例を示す図である。図８に示すアクセス承認画面８０は、承認が必要な作業申請がなされた場合、承認用端末４４に表示される。すなわち、申請状態管理部１３１は、承認が必要な作業申請がなされたとき、申請ナンバーを承認用端末４４に通知する。承認者が、申請ナンバーを指定してアクセス制御装置１４にアクセスすると、申請状態管理部１３１は承認用端末４４にアクセス承認画面８０をウェブページとして表示させる。

[0079] 申請情報領域８１は、アクセス申請画面６０に入力された申請内容を示す。承認者名領域８２は、承認者名を入力するための領域である。承認依頼者名領域８３は、承認を依頼したユーザ名を入力するための領域である。たとえば、承認権限のあるユーザＢが、ユーザＣに承認を依頼したときには、ユーザＣはユーザＢに代理して承認判断を行う。これは、ユーザＢの休暇中など、特殊な状況に対応するための措置である。

[0080] 通信欄８４は、作業申請者に対するメッセージを記述する欄であり、申請却下の理由を記述したり、申請承認するときには作業内容に条件や注文をつけるための記述がなされてもよい。承認ボタン８５は承認用、却下ボタン８６は却下用のボタンである。承認ボタン８５から却下ボタン８６のいずれかがクリックされると、入力内容と承認可否を示すデータがアクセス制御装置１４に送信される。申請状態管理部１３１は、このデータを作業用端末２０に、たとえば、電子メールにより送信する。

[0081] 図９は、システム管理者がポリシー名を検索する際に表示される画面例を

示す図である。図９に示すポリシー一覧画面９０に示すように、システム管理者から認知度の高い項目（たとえばポリシー名、接続システムなど）の一部または全部を入力することによって該当するアクセスルールを検索することができる。図９に示す例では、アクセスルールを構成する要素別に部分一致するものからポリシー名を検索することができるように構成されている。なお、検索結果として表示されるポリシーはポリシー検索結果表示領域９１に表示される。そして、ポリシー検索結果表示領域９１に表示されたポリシー名をクリックすると、そのポリシーの詳細情報が別画面（不図示）で表示される。なお、この図９に示すポリシー一覧画面９０は、システム管理者がポリシー名を検索する際だけではなく、ユーザがポリシー（またはアクセスルール）を検索する際に表示されるものであってもよい。ユーザがポリシー名を検索する際（たとえば図６で説明したアクセス申請の際）には、そのユーザもしくはそのユーザが所属する所定のユーザグループが過去に使用したアクセスルールをポリシー検索結果表示領域９１に表示させるようにしてもよい。

[0082] 図１０～図１３は、図６および図８において選択可能なアクセスルールの具体例について説明するための図である。アクセスルールは、たとえば図１０に示すように、所属する会社、所属する部署、役職などにより決定されるロール、ログ取得の有無、接続元ＩＰアドレス規制の有無、接続可能プロトコルの指定、事前承認の有無等の様々なルールの組み合わせで構成されるポリシー、ノードグループ名（システム名）、ノード名（端末名）などで構成されている。なお、図１０に示す「ユーザ」オブジェクトは、ユーザ自体を示し、「ノード」オブジェクトは、アクセス先のサーバ自体を示している。

[0083] 「ロール」オブジェクトには、社員管理者ロール、社員承認者ロール、協力管理者ロール、監査者ロール、一般ユーザ（社員）ロール、一般ユーザ（協力）ロール、一般ユーザ（ベンダ）ロールが定義されている。これらの各ロールとして定義されているオブジェクトを「ユーザ」オブジェクトに設定することにより、作業対象となるサーバにあるフォルダやファイルなどのア

クセス制御をユーザ単位ではなく、ロール単位で設定したり、変更したりすることができる。なお、「ユーザ」オブジェクトに対しては複数の「ロール」オブジェクトを設定することが可能である。

[0084] また、「ポリシー」オブジェクトには、社員ポリシー、協力会社ポリシー、システムポリシー、システム緊急ポリシーが定義されている。「ポリシー」オブジェクトでは、作業内容や役職などに応じて操作ログの取得のＯＮ／ＯＦＦ、事前承認の有無、使用可能となっているプロトコルが定義されている。たとえば、社員ポリシーは、社員管理者ロール、社員承認者ロール、監査者ロール、一般ユーザ（社員）ロールに関連づけられており、これらの各ロールを使用する際に社員ポリシーに定義されている内容に従ったアクセス制御を実行することができるようになる。なお、「ロール」オブジェクトに対しては複数の「ポリシー」オブジェクトを設定することが可能である。

[0085] また、「ノードグループ」オブジェクトには、企業Ａで使用される情報システム名が定義されており、図１０に示す例ではsystem_Ａ，system_Ｂ，system_Ｃの３つの情報システム名が定義されている。「ノードグループ」オブジェクトは、情報システムを構成するノード（サーバ）単位で定義されている。たとえば、system_Ａでは、Server01とserver02が関連づけられている。なお、「ノード」オブジェクトに対しては複数の「ノードグループ」オブジェクトを設定することが可能である。

[0086] 図１１は、図１０に示したアクセスルールのうち、社員に関するロールに着目したアクセスルールを説明するための図である。図１１に示すように、「ユーザ」オブジェクトのuser01には社員管理者ロール、社員認証者ロールおよび監査者ロールが設定されている。また、「ユーザ」オブジェクトのuser03には一般ユーザ（社員）ロールが設定されている。また、これらのロールすべてに社員ポリシーが設定されている。社員ポリシーにはsystem_Ａ，system_Ｂ，system_Ｃすべてに対して接続可能に設定されている。社員ポリシーでは、操作ログ取得がＯＮ（操作ログを取得する）、事前承認が必要、ＳＳＨ、ＲＤＰ、ＦＴＰ、ＳＣＰ、ＳＦＴＰの利用が可能である。なお、system_

Ａは、server01、server02により構成され、system_Ｂは、server03により構成され、system_Ｃはserver01，server02，server03，server04により構成されているため、それぞれがシステム単位で組分けされている。

[0087] これらの設定がなされているアクセスルールからは、次のことがわかる。すなわち、「ユーザ」オブジェクトのuser03は、system_Ａ，system_Ｂ，system_Ｃのすべてのシステムに対してアクセス可能であるが、何らかの作業を行う際には事前申請が必要となる。そして、user01は、user03の事前申請に対して管理、承認、監査を実施する必要がある。つまり、user01は、user03の上長であるが、一般ユーザ（社員）ロールが設定されていないため、system_Ａ，system_Ｂ，system_Ｃのすべてのシステムに対してはアクセスが不可である。

[0088] 図１２は、図１０に示したアクセスルールのうち、協力会社に関するロールに着目したアクセスルールを説明するための図である。図１２に示すように、user01には、監査者ロールが設定されている。また、user02には協力管理者ロールおよび協力承認者ロールが設定されている。User04，User05，User06には一般ユーザ（協力）ロールが設定されている。また、これらのロールすべてに協力会社ポリシーが設定されている。協力会社ポリシーでは、操作ログ取得がＯＮ（操作ログを取得する）、事前承認が必要、ＳＳＨの利用が可能となっている。また、協力会社ポリシーにはsystem_Ｂ，system_Ｃに対してアクセス可能に設定されている。なお、system_Ｂは、server03により構成されており、system_Ｃはserver01，server02，server04により構成されているため、それぞれがシステム単位で組分けされている。

[0089] これらの設定がなされているアクセスルールからは、次のことがわかる。一般ユーザ（協力）ロールが設定されているUser04，User05，User06は、system_Ｂ，system_Ｃに対してアクセスする際にはuser02の事前承認が必要である。つまり、協力会社ポリシーに関わる管理・承認については、協力管理者ロールおよび協力承認者ロールが設定されているuser02が実施する必要がある。また、協力会社ポリシーに関わるログ監査についてはuser02では行えず

、監査者ロールが設定されているuser01により実施する必要がある。

[0090] 図１３は、図１０に示したアクセスルールのうち、ベンダに関するロールに着目したアクセスルールを説明するための図である。図１３に示すように、user01には、社員管理者ロール、社員承認者ロール、および監査者ロールが設定されている。また、user02には協力承認者ロールが設定されている。User07，User08には一般ユーザ（ベンダ）ロールが設定されている。また、これらのロールすべてにシステムＡポリシーおよびシステムＡ緊急ポリシーが設定されている。システムＡポリシーでは、操作ログ取得がＯＦＦ（操作ログを取得しない）、事前承認が必要、ＲＤＰおよびＦＴＰの利用が可能となっている。また、システムＡ緊急ポリシーでは、操作ログ取得がＯＮ（操作ログを取得する）、事前申請が必要、ＲＤＰおよびＦＴＰの利用が可能となっている。また、これらのポリシーにはsystem_Ａに対してアクセス可能に設定されている。なお、system_Ａはserver01，server02により構成されているため、これらのノードをグルーピングして設定されている。

[0091] これらの設定がなされているアクセスルールからは、次のことがわかる。一般ユーザ（ベンダ）ロールが設定されているUser07，User08は、system_Ａに対してアクセスする際には２つのポリシーのいずれかを選択することができる。システムＡポリシーを選択した場合には、user02の事前承認が必要である。一方、システムＡ緊急ポリシーを選択した場合には、user02の事前申請が必要なだけであり、承認は不要である。すなわち、緊急時には事前申請のみで通常業務を行うことができる。なお、User07，User08からの申請は、User01，User02共に承認を行うことができる。

[0092] なお、図１０～図１３に示したようなアクセスルールは、システム管理者が承認用端末４４からアクセス制御装置１４に接続し、アクセス制御装置１４によって表示される不図示のアクセス申請・承認レベル設定画面で予め定義することで使用可能となっている。

[0093] 図１４は、アクセスログ検索画面例を示す図である。図１４に示すアクセスログ検索画面９０は、承認者が、アクセスチェック（ログ監査）を行う場

合に、承認用端末４４に表示される。承認者は、許可したアクセスの内容が、事前に申請された作業内容通りに行われているか否かを確認するために、アクセスログ検索画面９０上で、検索したいアクセスログの検索条件を設定する。検索ボタン９１は、設定された検索条件でアクセスログの検索を実行するためのボタンである。検索ボタン９１がクリックされると、検索条件を示すデータがログ管理装置１５に送信される。ログ管理装置１５のログ管理部１５１（の作業検証部１５１Ｂ）は、検索条件を示すデータに基づいて、ログ保持部１５２に登録されているアクセスログを抽出するとともに、アクセス制御装置１４の作業予定保持部１３９に登録されている作業予定情報を抽出する。

[0094] 図１５は、検索結果画面例を示す図である。図１５に示す検索結果画面１００は、アクセスログ検索画面９０の検索ボタン９１がクリックされた場合に、承認用端末４４に表示される。すなわち、承認者によってアクセスログ検索画面９０で設定された検索条件を満たすアクセスログがアクセス制御装置１４とログ管理装置１５で検索され、その検索結果（アクセスログと作業予定情報）が承認用端末４４に送信され、サマリーとして検索結果画面１００上に一覧表示される。

[0095] ファイルアイコン１０１は、具体的な作業内容をダウンロードするためのボタンである。ファイルアイコン１０１がクリックされると、具体的な実行コマンドの内容が、テキストファイルとして取得されて表示される。またファイルコマンド１０２は、申請内容をダウンロードするためのボタンである。ファイルアイコン１０１がクリックされると、具体的な申請内容が取得されて表示される。すなわち承認者は、アクセスログと申請内容を容易に見比べることができるので、ログ監査を効率よく行うことができる。

[0096] なお、申請内容に応じて不要だと思われる禁止コマンドなどをキーワードとして予め登録しておくと、そのキーワードが含まれるレコード行数とレコードを抽出することができる。たとえば、アクセス申請時、アクセス分類に「一般ＩＤ作業」を申請した場合、一般ＩＤによるアクセスであれば、特権

ＩＤを取得するようなコマンドが不要であるだけでなく、ユーザを追加するコマンドは本来発行されないことがわかっている。そこで、「一般ＩＤ作業」に対して禁止されている、あるいは不要である、「SU-」（特権ＩＤを取得するためのコマンド）、および「useradd」（ユーザを追加するコマンド）をキーワードとして事前に登録しておく。これにより、申請内容に応じて不要だと思われる禁止コマンドなどを含むアクセスログを抽出し、承認者に提供できるので、不正使用を効率よく見つけ出すことができる。

[0097] またメール通知の機能を利用すれば、キーワードに合致する操作が行われた場合、管理者へ電子メールを通知することができる。このように、アクセスチェックを行うだけでログ監査を効率良く行うことができる。

[0098] なおここでは、アクセスログと申請内容を見比べることができるように、検索結果を表示するようにしたが、ログ管理部１５１の作業検証部１５１Ｂが、検索条件を示すデータに基づいて、アクセス制御装置１４の作業予定保持部１３９に登録されている作業予定情報と、ログ保持部１５２に登録されているアクセスログとを対比して、前記ログ情報に示されるアクセスの中の、前記作業予定情報で申請されたメンテナンス作業用アクセスに合致しないアクセスを、不正アクセスとして検出することもできる。

[0099] ［作業申請処理について］

ここで、作業用端末２０の作業者が行う作業申請処理について説明する。作業者は、まず、作業用端末２０に表示される図５に示すログイン画面５０上でユーザＩＤとパスワードを入力する。作業用端末２０は、入力されたユーザ識別情報と共に、中継装置１１を経由することなく、直接、アクセス制御装置１４にアクセスする。アクセス制御装置１４は、ユーザ識別情報をユーザ認証装置１２に転送する。ユーザ認証装置１２のユーザ認証部１２１は、正規ユーザ情報保持部１２２の正規ユーザ情報を参照してユーザ認証を行い、認証に失敗した場合、以降の処理は実行されない。

[0100] 認証に成功した場合、ユーザ認証装置１２は、認証成功の旨をアクセス制御装置１４に通知する。アクセス制御装置１４の申請状態管理部１３１は、

申請画面用データを作業用端末２０に送信する。作業用端末２０は、図６に示すアクセス申請画面６０を表示させる。ユーザは、アクセス申請画面６０にデータを入力し、入力されたデータが作業申請情報としてアクセス制御装置１４に送信される。

[0101] アクセス制御装置１４の申請状態管理部１３１は、申請された作業内容と実行条件保持部１３７の実行条件情報を比較し、登録可否を判定する。有効な作業申請でなければ、申請状態管理部１３１は申請を却下した上で、作業用端末２０に却下通知し、以降の処理は実行されない。一方、有効な作業申請であると判定した場合、申請状態管理部１３１は、申請されたメンテナンス作業を作業予定保持部１３９の作業予定情報に登録する。承認が必要な作業であれば、申請状態管理部１３１は承認を求める旨の電子メールを承認用端末４４に送信する。

[0102] 以上の処理により、作業申請情報のうち、有効な作業申請としての要件を満たす作業申請情報だけが「作業予定情報」として作業予定保持部１３９に正式に登録される。

[0103] ［作業承認処理について］

次に、作業申請処理によって申請された作業内容の承認処理について説明する。承認用端末４４は、申請が出された旨の電子メールを受け取ったあと、アクセス制御装置１４にアクセスする。承認者は任意のタイミングにて、図５に示したログイン画面５０上でユーザＩＤとパスワードを入力する。また、承認者は、ユーザＩＤとパスワードの入力時、申請ナンバーも指定する。承認用端末４４は、入力された承認者のユーザＩＤとパスワードをユーザ認証装置１２に送信する。ユーザ認証装置１２のユーザ認証部１２１は、承認用端末４４からユーザＩＤとパスワードを取得し、正規ユーザ情報保持部１２２に登録されている正規ユーザ情報を参照して、承認者のユーザ認証を行う。ユーザ認証に失敗した場合、以降の処理は実行されない。

[0104] 認証に成功した場合、アクセス制御装置１４の申請状態管理部１３１は、承認用端末４４から取得した申請ナンバーに基づいて、作業予定保持部１３

９に登録されている作業申請情報を検索する。アクセス制御装置１４の申請状態管理部１３１は、検索した作業申請情報に基づいて、アクセス承認画面８０のためのＨＴＭＬ（HyperText Markup Language）データを承認用端末４４に送信する。承認用端末４４は、申請ナンバーで指定された作業に関するアクセス承認画面８０（図８）を表示させる。承認者は、アクセス承認画面８０を確認し、承認ボタン８５または却下ボタン８６をクリックすると、入力されたデータがアクセス制御装置１４に送信される。アクセス制御装置１４の申請状態管理部１３１は、承認可否に応じて作業予定保持部１３９の作業予定情報を更新する。申請状態管理部１３１は、作業用端末２０に承認可否を通知する。

[0105] 以上の処理により、有効に申請された作業について承認がなされる。なお、承認者が、アクセス制御装置１４にアクセスすると、アクセス制御装置１４は承認待ちの作業申請を一覧表示させ、承認者はその中から承認対象となる作業申請を選択するというユーザインタフェースであってもよい。また、複数の作業申請を一括して承認または却下を行うことも可能である。

[0106] ［リモートログイン処理について］

次に、業務情報システムへのリモートログイン処理について説明する。作業者は、作業用端末２０から、まず、中継装置１１にアクセスする。中継装置１１は、アクセスされた作業用端末２０のＩＰアドレスを確認し、接続を許可するか否かを判断し、許可しない場合には接続を切断する。一方、作業用端末２０からの接続を許可する場合には、中継装置１１は、作業用端末２０に対し、プロトコルに適した形でユーザ識別情報（ユーザＩＤおよびパスワード）を要求する。作業用端末２０は、ログイン画面５０（図５）を表示させ、作業者からユーザＩＤとパスワードの入力を受け付ける。作業用端末２０は、入力されたユーザＩＤとパスワードを中継装置１１に送信する。

[0107] 中継装置１１は、作業用端末２０から受信したユーザＩＤとパスワードをユーザ認証装置１２、アクセス制御装置１４に供給する。ユーザ認証装置１２のユーザ認証部１２１は、中継装置１１からユーザＩＤとパスワードを取

得し、正規ユーザ情報保持部１２２に登録されている正規ユーザ情報を参照して、作業者のユーザ認証を行う。ユーザ認証に失敗した場合、以降の処理は実行されない。

[0108] 認証に成功した場合、中継装置１１は、作業用端末２０にアクセス先の入力を要求する。作業用端末２０は、作業者からアクセス先の入力を受け付け、アクセス先を示す情報（ＩＰアドレスやホスト名など）を中継装置１１に送信する。中継装置１１は、作業用端末２０から受信したアクセス先を示す情報をアクセス制御装置１４に供給する。アクセス制御装置１４のアクセス権認証部１３６は、アクセス先を示す情報に基づいて、アクセス権情報保持部１４１に登録されているアクセス申請状況を参照し、アクセス先へのユーザのアクセス権を確認する。アクセス権認証部１３６は、不適切なアクセスと判断した場合には、アクセス先へのユーザのアクセスを拒否する。一方、適切なアクセスと判断した場合には、アクセス先へのユーザのアクセスを許可する。そして全ての判定が肯定となった場合、作業者は、メンテナンス作業の対象となる業務情報システムにアクセス可能となる。

[0109] 以上の処理により、業務情報システムへリモートログインした場合に、不正なアクセスと判断されると、ログインに失敗し、アクセスを禁止することができる。

[0110] ［アクセスチェック処理について］

次に、図１６のフローチャートを参照して、アクセスチェック処理について説明する。承認者は、許可したアクセスの内容が、事前に申請された作業内容通りに行われているか否かを確認するために、承認用端末４４の入力部（図示せず）を用いて、アクセスチェック（ログ監査）の実行を指示する。

[0111] ステップＳ１において、承認用端末４４は、承認者からの指示に基づいて、図１４に示したアクセスログ検索画面９０を表示する。承認者は、アクセスログ検索画面９０上で、検索したいアクセスログの検索条件を設定する。ステップＳ２において、承認用端末４４は、承認者により設定されたアクセスログの検索条件の入力を受け付ける。そして、検索ボタン９１がクリック

されると、ステップＳ３において、承認用端末４４は、入力を受け付けたアクセスログの検索条件データをログ管理装置１５に送信する。

[0112] ステップＳ４において、ログ管理装置１５の作業検証部１５１Ｂは、承認用端末４４から検索条件データを受信すると、アクセス制御装置１４の作業予定保持部１３９から、検索条件データに含まれる申請ナンバーに対応する作業予定情報を読み出し、ログ保持部１５２から申請ナンバーに紐付けされているアクセスログを読み出し、両者を突き合わせ、不正アクセスがなされていないかをチェックする。たとえば、上述したように、「稼働監視」を目的とした作業申請がなされているときに、ファイルの書き換え処理の実行がなされたときには、不正アクセスとなる。ステップＳ５において、作業検証部１５１Ｂは、ログ保持部１５２から検索条件に合致するアクセスログを読み出し、アクセスチェック結果として承認用端末４４に通知する。

[0113] ステップＳ６において、承認用端末４４は、ログ管理装置１５から受信したアクセスチェック結果に基づいて、図１５に示した検索結果画面１００を表示させる。なお、申請内容に応じて不要だと思われる禁止コマンドをキーワードとして予め登録してある場合、キーワードに合致するアクセスログが検索された場合には、検索されたキーワードに合致するレコード行数とレコードを、管理者へメール通知することができる。

[0114] ［発明の実施の形態における効果］

以上のように、業務情報システム（所定のシステム）を構成するサーバに対する作業用端末２０（クライアント端末）のアクセスを制御するアクセス制御装置１４であって、業務情報システムの管理者により作成された１または複数のアクセスルールから、作業用端末２０にログインしたユーザが利用するアクセスルールを選択させるための選択画面情報を生成するアクセスルール特定画面生成部１３３（画面生成部）と、選択画面情報に基づいて表示されるアクセスルールから選択されたアクセスルールに従ってユーザのアクセス制御を実行するアクセス制御部１３５とを有する構成となっている。

[0115] これにより、システム管理者は、１または複数のアクセスルールをユーザ

に対して提示することができ、かつユーザに対して使用するアクセスルールを選択させることができる。そのため、システム管理者はユーザに対して必要なアクセスルールを作成して設定しておくだけでよく、作業内容に応じてアクセスルールの設定を逐一変更する必要がなくなるのでアクセス制御の管理がしやすくなる。また、ユーザにとっても、自分が選択できるアクセスルールが１または複数が提示されると共に、その提示されたアクセスルールが複数ある場合には、提示されたアクセスルールから自己の作業内容に応じて選択することができるため、どのようなアクセスルールが自分に適用されるのかが具体的に把握して選択することが可能となる。さらに、アクセス制御について監査をする者にとっては、ユーザが選択したアクセスルールに従ってアクセス制御が行われるため、選択されたアクセスルールのみに着目して確認するだけでよい。そのため、ユーザ毎に複数のアクセスルールが組み合わされて設定されている場合であっても、実際に想定した制御でアクセスされているのか否かについて把握しやすくなり、監査する者の負荷を軽減させることができる。

[0116] また、上述した構成に加え、アクセスルール保持部１４０（第１の記憶部、第２の記憶部）には、業務情報システムの管理者により作成された１または複数のアクセスルールを記憶し、アクセスルール特定画面生成部１３３により生成された選択画面情報に基づいて表示される１または複数のアクセスルールからユーザが選択したアクセスルールをユーザのアクセス制御を実行する際に適用するアクセスルールとして記憶するように構成されている。

[0117] これにより、ユーザに適用されるアクセスルールについても記録されるため、この記録を見るだけでどのようなアクセス制御がなされていたのかを容易に確認することができる。このため、クライアント企業としても、自システムについてのコンプライアンス（compliance）を証明しやすいというメリットがある。このような特徴により、業務情報防護装置１０に含まれるアクセス制御装置１４は、ＳＯＸ法が求める「内部統制の強化」に資することができる。

[0118] また、上述した構成に加え、アクセスルール特定画面生成部１３３は、ユーザが利用可能となっているアクセスルールについて問い合わせ要求がなされた場合に、アクセスルール保持部１４０を参照してユーザが利用可能となっているアクセスルールを特定すると共に、その特定されたアクセスルールのうち、問い合わせ要求をしてきたユーザもしくはユーザが所属する所定のユーザグループと関連付けられているアクセスルール名を示す特定画面情報を生成する構成となっている。

[0119] これにより、利用可能なアクセスルールをリストアップしてユーザに対して提示することができるため、アクセスルールを選択する際の負荷を軽減させることができる。

[0120] また、上述した構成に加え、アクセスルール保持部１４０に記憶されているアクセスルールを検索するアクセス制御部１３５（ルール検索支援部）を有し、アクセス制御部１３５は、ユーザからアクセスルールの検索を要求された際に、アクセスルール名または接続先ノード名を指定してアクセスルールの検索ができる画面情報を生成する構成となっている。

[0121] これにより、ユーザがアクセス申請をする際にメンテナンス作業対象となるサーバ名などをキーとしてアクセスルールを容易に検索することが可能となる。

[0122] また、上述した構成に加え、アクセスルール保持部１４０に記憶されているアクセスルールを検索するアクセス制御部１３５を備えており、アクセス制御部１３５は、ユーザもしくはユーザが所属する所定のユーザグループが過去に使用したアクセスルールを示す画面情報を生成する構成となっている。

[0123] これにより、同一のユーザ、またはユーザが所属するユーザグループが過去に利用したアクセスルールが、選択可能となるアクセスルールとして提示されることになるため、ユーザが選択可能なアクセスルールが非常に多くある場合には、ユーザがアクセスルールを選択する際の負荷を軽減させることができる。

[0124] また、上述したアクセス制御装置１４のアクセスルールとして説明したアクセス制御方法、およびアクセス制御装置１４としてコンピュータを機能させるためのプログラムは上述したアクセス制御装置１４が奏する効果と同様の効果を奏するものである。

[0125] 以上においては、「メンテナンス作業」を例に挙げ説明したが、本発明は、これに限らず、たとえば、社員が外出先からアクセスする場合にも適用することが可能である。

[0126] 上述した一連の処理は、ハードウエアにより実行することもできるし、ソフトウエアにより実行することもできる。一連の処理をソフトウエアにより実行する場合には、そのソフトウエアを構成するプログラムが、専用のハードウエアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、プログラム記録媒体からインストールされる。

[0127] この発明は、上記実施の形態そのままに限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で構成要素を変形して具体化したり、上記実施の形態に開示されている複数の構成要素を適宜組み合わせたりすることにより種々の発明を形成できる。例えば、実施の形態に示される全構成要素から幾つかの構成要素を削除してもよい。さらに、異なる実施の形態に亘る構成要素を適宜組み合わせても良い。

符号の説明

[0128] １４…アクセス制御装置、

２０…作業用端末（クライアント端末）、

４１…財務情報システム（所定のシステムの一例）、

４２…顧客情報システム（所定のシステムの一例）、

４３…在庫管理システム（所定のシステムの一例）、

１３３…アクセスルール特定画面生成部（画面生成部の一例）、

１３５…アクセス制御部（アクセス制御部、ルール検索支援部の一例）、

１４０…アクセスルール保持部（第１の記憶部、第２の記憶部の一例）、

請求の範囲

［請求項1］ 所定のシステムを構成するサーバに対するクライアント端末のアクセスを制御するアクセス制御装置であって、

前記所定のシステムの管理者により作成された１または複数のアクセスルールから、前記クライアント端末にログインしたユーザが利用するアクセスルールを選択させるための選択画面情報を生成する画面生成部と、

前記選択画面情報に基づいて表示されるアクセスルールから選択されたアクセスルールに従って前記ユーザのアクセス制御を実行するアクセス制御部と、

を有することを特徴とするアクセス制御装置。

［請求項2］ 請求項１に記載のアクセス制御装置であって、

前記所定のシステムの管理者により作成された１または複数のアクセスルールを記憶する第１の記憶部と、

前記画面生成部により生成された選択画面情報に基づいて表示される１または複数のアクセスルールから前記ユーザが選択したアクセスルールを前記ユーザのアクセス制御を実行する際に適用するアクセスルールとして記憶する第２の記憶部と、

を有することを特徴とするアクセス制御装置。

［請求項3］ 請求項２に記載のアクセス制御装置であって、

前記画面生成部は、

前記クライアント端末から前記ユーザが利用可能となっているアクセスルールについて問い合わせ要求がなされた場合に、前記第２の記憶部を参照して前記ユーザが利用可能となっているアクセスルールを特定すると共に、問い合わせ要求をしてきたユーザもしくは前記ユーザが所属する所定のユーザグループと関連付けられているアクセスル

ールを特定可能な名称を示す特定画面情報を生成する、ことを特徴とするアクセス制御装置。

［請求項4］ 請求項２または３に記載のアクセス制御装置であって、

前記第１の記憶部に記憶されているアクセスルールを検索するルール検索支援部を有し、

前記ルール検索支援部は、

前記ユーザから前記アクセスルールの検索を要求された際に、前記アクセスルール名または接続先ノード名を指定して前記アクセスルールの検索ができる画面情報を生成することを特徴とするアクセス制御装置。

［請求項5］ 請求項２から３のいずれか１項に記載のアクセス制御装置であって、

前記第１の記憶部に記憶されているアクセスルールを検索するルール検索支援部を備えており、

前記ルール検索支援部は、

前記ユーザもしくは前記ユーザが所属する所定のユーザグループが過去に使用したアクセスルールを示す画面情報を生成することを特徴とするアクセス制御装置。

［請求項6］ 所定のシステムを構成するサーバに対するクライアント端末からのアクセスを制御するアクセス制御方法であって、

前記所定のシステムの管理者により作成された１または複数のアクセスルールから、前記クライアント端末にログインしたユーザが利用するアクセスルールを選択させるための選択画面情報を生成する画面生成ステップと、

前記選択画面情報に基づいて表示されるアクセスルールから選択さ

れたアクセスルールに従って前記ユーザのアクセス制御を実行するアクセス制御ステップと、
を有することを特徴とするアクセス制御方法。

［請求項7］ 所定のシステムを構成するサーバに対するクライアント端末からのアクセスを制御するアクセス制御装置としてコンピュータを機能させるためのプログラムであって、
前記コンピュータを
前記所定のシステムの管理者により作成された１または複数のアクセスルールから、前記クライアント端末にログインしたユーザが利用するアクセスルールを選択させるための選択画面情報を生成する画面生成手段と、
前記選択画面情報に基づいて表示されるアクセスルールから選択されたアクセスルールに従って前記ユーザのアクセス制御を実行するアクセス制御手段、
として機能させるためのプログラム。