(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5460681号
(P5460681)
(45)発行日　平成26年4月2日(2014.4.2)　(24)登録日　平成26年1月24日(2014.1.24)

(51)Int.Cl.　　F I
G06F 21/62 (2013.01)　　G06F 21/24 163C
G06Q 50/24 (2012.01)　　G06Q 50/24

請求項の数 4　(全 15 頁)

(21)出願番号　特願2011-262588 (P2011-262588)
(22)出願日　平成23年11月30日 (2011.11.30)
(65)公開番号　特開2013-114598 (P2013-114598A)
(43)公開日　平成25年6月10日 (2013.6.10)
審査請求日　平成24年10月18日 (2012.10.18)

(73)特許権者　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100080285
弁理士　小出　俊實
(74)代理人　100075672
弁理士　峰　隆司
(74)代理人　100103034
弁理士　野河　信久
(72)発明者　倉　恒子
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

最終頁に続く

(54)【発明の名称】情報流通システムとそのアクセス制御方法

(57)【特許請求の範囲】
【請求項１】
サービスの要求側となる第１の情報処理装置と、サービスの提供側となる第２の情報処理装置と、これら第１及び第２の情報処理装置間をネットワークを介して連携させる第３の情報処理装置とを具備する情報流通システムにおいて、
前記第２の情報処理装置は、
前記第１の情報処理装置からサービス対象となるデータとその登録要求を受信し、当該受信されたサービス対象となるデータと、当該データに係るユーザが差出人、受取人及び対象者の何れであるかを表す役割情報と、当該ユーザの所属組織と資格を表す属性情報と、当該データに対するアクセスの状況の変化を表すステータス情報とを相互に関連づけて記憶する記憶手段と、
前記記憶手段に記憶されたサービス対象となるデータに対する、前記第１の情報処理装置からのアクセスによる閲覧又は編集の結果に応じて、前記記憶されているステータス情報を更新する更新手段と、
前記第１の情報処理装置からのアクセス要求に応じ、サービス対象となるデータに対するアクセス制御に先立ち、前記アクセス要求の内容と、前記記憶された役割情報、属性情報及び更新後のステータス情報に基づいて、前記サービス対象となるデータに対するアクセス制御ルールを決定する決定手段と、
前記決定されたアクセス制御ルールに従い、前記サービス対象となるデータに対するアクセス制御を実行する実行手段と

を具備することを特徴とする情報流通システム。
【請求項２】
前記記憶手段は、サービス対象となるデータ又はその電子フォーマットが複数種類存在する場合に、この種類ごとにユーザの役割を表す役割情報、当該ユーザの属性情報及びアクセスの状況を表すステータス情報を記憶することを特徴とする請求項１記載の情報流通システム。
【請求項３】
サービスの要求側となる第１の情報処理装置と、サービスの提供側となる第２の情報処理装置と、これら第１及び第２の情報処理装置間をネットワークを介して連携させる第３の情報処理装置とを具備する情報流通システムで使用されるアクセス制御方法において、
前記第１の情報処理装置が、ユーザによるサービス対象となるデータとその登録要求を送信させるための入力操作を受付け、当該受け付けたサービス対象となるデータとその登録要求を前記ネットワークを介して前記第２の情報処理装置へ送信する過程と、
前記第２の情報処理装置が、前記第１の情報処理装置から送られたサービス対象となるデータとその登録要求を受信し、当該受信されたサービス対象となるデータと、当該データに係るユーザが差出人、受取人及び対象者の何れであるかを表す役割情報と、当該ユーザの所属組織と資格を表す属性情報と、当該データに対するアクセスの状況の変化を表すステータス情報とを相互に関連づけて記憶手段に記憶させる過程と、
前記第２の情報処理装置が、前記記憶手段に記憶されたサービス対象となるデータに対する、前記第１の情報処理装置からのアクセスによる閲覧又は編集の結果に応じて、前記記憶手段に記憶されているステータス情報を更新する過程と、
前記第１の情報処理装置が、ユーザによるデータアクセス要求を受付け、当該データアクセス要求を前記ネットワークを介して前記第２の情報処理装置へ送信する過程と、
前記第２の情報処理装置が、前記アクセス要求元のユーザについての認証要求を前記ネットワークを介して前記第３の情報処理装置へ送信し、その認証結果を表す情報を受信する過程と、
前記第２の情報処理装置が、前記認証結果をもとに要求元のユーザの正当性が確認された場合に、前記サービス対象となるデータに対するアクセス制御に先立ち、前記アクセス要求の内容と、前記記憶された役割情報、属性情報及び更新後のステータス情報に基づいて、前記サービス対象となるデータに対するアクセス制御ルールを決定する過程と、
前記第２の情報処理装置が、前記決定されたアクセス制御ルールに従い、前記サービス対象となるデータに対するアクセス制御を実行する過程と
を具備することを特徴とするアクセス制御方法。
【請求項４】
前記記憶させる過程は、サービス対象となるデータ又はその電子フォーマットが複数種類存在する場合には、この種類ごとに前記ユーザの役割を表す役割情報、当該ユーザの属性情報及びアクセスの状況を表すステータス情報を記憶することを特徴とする請求項３記載のアクセス制御方法。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、複数の情報処理装置間でサービス対象データを流通させる情報流通システムとそのアクセス制御方法に関する。
【背景技術】
【０００２】
近年、複数の医療機関がネットワークを介して連携し、医療サービスを市民に提供するサービスシステムが普及している。この種のシステムでは、個々の病院がそれぞれサーバを運用し、これらのサーバ間で情報をやり取りする。例えば、中核病院により検査した結果であるレントゲン写真やカルテの情報を、診療所等のかかりつけ医に開示することにより、中核病院とかかりつけ医が連携しながら治療を行なう場合には、双方で患者の情報を

閲覧できなければならない。しかし、患者の情報は個人情報であるため、取り扱いを慎重にしなければならない。このため、個人情報に対して様々なアクセス制御方法が提案されている（例えば特許文献１、２又は３を参照）。

【０００３】

また、中核病院と診療所で同じ患者の治療にあたるにしても、対象病原以外の情報を見せる必要はなく、適切なアクセス制御を設定することによってデータの開示範囲を絞ることが求められる。さらに、ガイドライン等により方針を制定されている例もある（例えば非特許文献１を参照）。

【０００４】

一方、医療のＩＴ化は益々進んでおり、取り扱える書類の種類も増え続けている。電子化するにあたり、フォーマットをどのようにしたらよいかといった議論が進んでおり、現時点ではフォーマット化されていなくても、近い将来正式フォーマットとしてシステムで取り扱わざるを得なくなる可能性もある（例えば非特許文献２を参照）。

【０００５】

また、一般にユーザが様々なデータを作成して特定のサーバに格納し、この格納されたデータを別のユーザが閲覧するといったサービスはよく知られている。ブログやTwitter（登録商標）はその一例である。医療分野においても、ある病院で撮影されたレントゲン写真や診療カルテの情報を他の病院に開示してその閲覧権限を与えることにより、医療の質を向上させる試みがなされている（例えば非特許文献３を参照）。

【０００６】

例えば、紹介状は紹介元の病院の医師によって作成され、紹介先の病院の医師が閲覧できる文書であるが、紹介先の病院の医師は自由に閲覧できても、書き込むことはできないといったアクセス制御が必要となる。現在の運用では、紹介状は封書により紹介元の医師から患者に渡される。ここで、患者は紹介状の中身を閲覧することはできないと仮定すると、紹介状サービスをＩＴにより実現するには、患者に対しては自分宛の紹介状の有無を検索できても中身を閲覧できないようにするアクセス制御を行う必要がある。

【０００７】

一方、処方箋については、発行された時点では患者がどの調剤薬局から薬を購入するかが分からないため、特定の人を指定することができない。すなわち、薬剤師という資格を持った人であれば、誰でも処方箋の電子データを閲覧できるようにしておかなければならない。また、長期に渡って服用する薬の場合には、量を分けて複数回に渡り購入できるようにすることも必要である。このとき、常に同じ薬剤師から購入しなければならないといった制約はないため、ここでも薬剤師という資格を持った人であれば誰でも処方箋の電子データにアクセスできるようにしなければならないし、薬を渡すたびに量や具体的な薬名を追記できるようにしなければならない。また、処方量をすべて渡し終わった後には、それ以上薬が渡らないような制約をかけなければならない。すなわち、閲覧や書き込みに対するアクセス制御も必要となる。処方箋は、処方されている期間には患者が閲覧できるようにしておかなければならないが、すべての薬を受領した後の処方箋は薬剤師が管理することになっているため、患者からは閲覧できないようにする必要がある。

【０００８】

すなわち、紹介状や処方箋といったサービス対象データの種類によって、当該サービス対象データに対するアクセス制御ルールを異ならせる必要がある。また、アクセス制御ルールは、データの種類に止まらず、アクセスするユーザの役割や属性等によっても異ならせる必要がある。

【０００９】

このうち、ユーザの役割に応じてアクセス制御を実施する方法としては、ロールベースアクセス制御が知られている。この技術は、会社等の組織内におけるロールに対するアクセスを割り当てるものとなっている。このため、紹介状や処方箋等のように、同一組織に所属しているとは限らないユーザについては適用できない。

【００１０】

またアクセス制御ルールは、時間の経過、つまりデータをやり取りする段階によっても変化する。そのため、依頼された要求に対して、適切なアクセス権限を判断する処理を実施したうえで、本来やるべき処理を実行しなければならない。例えば紹介状であれば、受取人が紹介状を開封し、患者の治療を引き受ける状況になった時点で、紹介先病院の医師は紹介元病院の診療カルテやレントゲン撮影画像等の治療に必要な関係文書にアクセスできるようにしなければならない。しかし現状では、紹介元の医師が患者に対して紹介状と共に治療に必要なデータを手渡しし、患者が紹介状とこのデータを自ら紹介先の医師に持参することが一般的である。このため、診療データは個人情報であるにもかかわらず、紹介先病院の医師に安全に提示することが困難である。

【先行技術文献】

【特許文献】

【００１１】

【特許文献１】特開２０１１－１００３６１号公報

【特許文献２】特開２０１１－１００３６２号公報

【特許文献３】特開２０１１－１０７７７９号公報

【非特許文献】

【００１２】

【非特許文献１】「保存が義務付けられた診療録等の電子保存ガイドライン（第３版）」、一般社団法人　保健医療福祉情報システム工業会　セキュリティ委員会　電子保存ＷＧ、２０１１年４月、［平成２３年１０月３１日検索］、インターネット＜URL: http://www.jahis.jp/wp-content/uploads/st11-001.pdf＞

【非特許文献２】「処方せんの電子化について」、厚生労働省　医療情報ネットワーク基盤検討会、平成２０年７月、［平成２３年１０月３１日検索］、インターネット＜URL: http://www.mhlw.go.jp/shingi/2008/08/dl/s0801-6a.pdf＞

【非特許文献３】ＮＰＯ法人長崎地域医療連携ネットワークシステム、［平成２３年１０月３１日検索］、インターネット＜URL: http://www.ajisai-net.org/ajisai/＞

【発明の概要】

【発明が解決しようとする課題】

【００１３】

以上述べたように既存の技術では、サービス対象のデータをネットワークを介して流通させようとする際に、アクセスするユーザの役割や属性、さらには上記データの状況変化に対して適切なアクセス制御を行うことができない。

この発明は上記事情に着目してなされたもので、その目的とするところは、ユーザの役割と属性、さらには上記データの状況変化に応じて、当該データに対し適切なアクセス制御ルールに従いアクセス制御できるようにした情報流通システムとそのアクセス制御方法を提供することにある。

【課題を解決するための手段】

【００１４】

上記目的を達成するためにこの発明の１つの観点は、サービスの要求側となる第１の情報処理装置と、サービスの提供側となる第２の情報処理装置と、これら第１及び第２の情報処理装置間をネットワークを介して連携させる第３の情報処理装置とを具備する情報流通システムにおいて、上記第２の情報処理装置により、はじめに上記第１の情報処理装置からサービス対象となるデータとその登録要求を受信し、当該受信されたサービス対象となるデータと、当該データに係るユーザが差出人、受取人及び対象者の何れであるかを表す役割情報と、当該ユーザの所属組織と資格を表す属性情報と、当該データに対するアクセスの状況の変化を表すステータス情報とを相互に関連付けて記憶する。また上記サービス対象となるデータに対する、上記第１の情報処理装置からのアクセスによる閲覧又は編集の結果に応じて、上記記憶されているステータス情報を更新する。そしてこの状態で、上記第１の情報処理装置からアクセス要求が送信されると、サービス対象となるデータに対するアクセス制御に先立ち、上記アクセス要求の内容と、上記記憶された役割情報、属

性情報及び更新後のステータス情報に基づいて、上記サービス対象となるデータに対するアクセス制御ルールを決定し、この決定されたアクセス制御ルールに従い上記サービス対象となるデータに対するアクセス制御を実行するようにしたものである。

【００１６】

またこの発明は、サービス対象となるデータの種類又はその電子フォーマットの種類が異なる場合には、この種類ごとにユーザの役割を表す役割情報、当該ユーザの属性情報及びアクセスの状況を表すステータス情報を記憶することも特徴とする。

【発明の効果】

【００１７】

したがって、ユーザの操作に応じて要求側の情報処理装置からサービス対象データに対するアクセス要求が発生すると、予め記憶されたユーザの役割を表す情報と当該ユーザの属性情報をもとに適切なアクセス制御ルールが決定され、サービス対象データに対するアクセス制御が実行される。このため、ユーザの役割、例えば差出人、受取人及び対象者の何れであるのかと、属性、例えば所属組織又は資格を考慮してアクセス制御ルールが決定され、このアクセス制御ルールに従いサービス対象データに対するアクセス制御を実行することが可能となる。このアクセス制御の種類には、例えば記憶された情報リストの検索のみ、内容の閲覧のみ、或いは閲覧＋編集が考えられる。

【００１８】

また、アクセス制御ルールを決定する際には、サービス対象データに対する最新のアクセス状況を表すステータス情報も考慮される。このため、ユーザの役割や属性が変わらなくても、サービス対象データに対する現在のアクセス状況（例えば作成済、閲覧済、編集済）が変化した場合には、この変化に応じてその時々で適切なアクセス制御を実行することが可能となる。

【００１９】

さらに、サービス対象データ又はその電子フォーマットが複数種類ある場合には、これらの種類ごとにユーザの役割、属性及びステータス情報が記憶され、アクセス制御ルールが決定されるので、サービス対象データ又はその電子フォーマットの種類が異なる場合でも、それに応じた適切なアクセス制御を実行することが可能となる。

【００２０】

すなわちこの発明によれば、ユーザの役割と属性、さらには上記データの状況変化に応じて、当該データに対し適切なアクセス制御ルールに従いアクセス制御できるようにした情報流通システムとそのアクセス制御方法を提供することができる。

【図面の簡単な説明】

【００２１】

【図１】この発明の一実施形態に係る情報流通システムの機能構成を示すブロック図。

【図２】図１に示したシステムのサーバに記憶される紹介状管理データの一例を示す図。

【図３】図１に示したシステムのサーバに記憶される紹介状属性データの一例を示す図。

【図４】図１に示したシステムの連携サーバに記憶される紹介状アプリケーションアクセス制御ファイルの一例を示す図。

【図５】図１に示したシステムの要求側サーバに記憶される紹介状アプリケーションアクセス制御ファイルの一例を示す図。

【図６】図１に示したシステムの提供側サーバに記憶される紹介状アプリケーションアクセス制御ファイルの一例を示す図。

【図７】紹介状アプリケーション設定ファイルの一例を示す図。

【図８】図１に示したシステムによる紹介状サービスの概要を示す図。

【図９】図１に示したシステムにおいて実行される、医師による紹介状登録・閲覧権限付与処理のシーケンスを示す図。

【図１０】図１に示したシステムにおいて実行される、患者に対する紹介状サービス処理のシーケンスを示す図。

【発明を実施するための形態】

【００２２】
以下、図面を参照してこの発明に係わる実施形態を説明する。
［構成］
図１は、この発明の一実施形態に係る情報流通システムの機能構成を示すブロック図である。
情報流通システムは、クライアント端末４が接続される複数の要求側サーバ１と、サービスを提供する複数の提供側サーバ２と、連携サーバ３とを具備し、これらのサーバ１，２，３はネットワーク５を介して相互に通信可能となっている。
【００２３】
クライアント端末４は、例えば医師や患者等のユーザが使用するパーソナル・コンピュータからなり、Ｗｅｂブラウザ４１を有している。ユーザは、Ｗｅｂブラウザ４１を使って要求側サーバ１及び提供側サーバ２にアクセスする。
【００２４】
要求側サーバ１は、例えば病院のポータルサーバ或いは患者が利用する医療ポータルサーバからなり、クライアント端末４からの要求を受け付けると、この要求を自サーバが処理できる場合には対応するサービスを実行し、処理できない場合には該当する提供側サーバ２に上記要求を転送する。
【００２５】
この機能を実現するために要求側サーバ１は、送受信部１１と、アクセス制御部１２と、データアクセス部１３と、ユーザ情報格納部１４と、アプリケーションデータ格納部１５を備える。送受信部１１は、クライアント端末４、提供側サーバ２及び連携サーバ３との間でネットワーク５を介して各種データの送受信を行う。
【００２６】
アクセス制御部１２は、Ｗｅｂアクセス抽出部１２１及びアクセス制御判定部１２２を有する。Ｗｅｂアクセス抽出部１２１は、クライアント端末４のＷｅｂブラウザ４１から要求されたＨＴＴＰリクエストを受け付け、リクエストの内容を解析する。アクセス制御判定部１２２は、ユーザのデータへのアクセス可否を判断する。このアクセス可否の判断のため、データアクセス部１３を介してユーザ情報格納部１４に対し問い合わせを行う。ユーザ情報格納部１４は、上記アクセス可否の判断に必要なユーザの個人情報を格納しており、上記問い合わせに対する回答をデータアクセス部１３を介してアクセス制御判定部１２２に返す。アプリケーションデータ格納部１５には、自サーバ上で実行されるアプリケーションが用いるアクセス制御ファイル、設定ファイル及び個別データが格納されている。
【００２７】
提供側サーバ２は、例えば医療情報の流通サービスを提供するサービス事業者が運用するサーバであり、上記要求側サーバ１とほぼ同じ機能、つまり送受信部２１と、アクセス制御部２２と、データアクセス部２３と、ユーザ情報格納部２４と、アプリケーションデータ格納部２５を備えている。
【００２８】
連携サーバ３は、上記要求側サーバ１と提供側サーバ２との間を連携させるためのもので、送受信部３１と、アクセス制御判定部３２と、データアクセス部３３と、ユーザ情報格納部３４と、アプリケーションデータ格納部３５と、システム情報格納部３６と、マスタ情報格納部３７を備えている。
【００２９】
システム情報格納部３６には、情報流通システムを構成する各サーバが有するシステム情報や使用する認証方式を表す情報が格納されている。マスタ情報格納部３７には、情報流通システムに対し利用登録した全てのユーザについて、そのユーザＩＤに関連付けて当該ユーザが所属する組織や資格を表す属性情報がマスタ情報として格納される。登録済のユーザが新たに資格を取得した場合には、上記マスタ情報が更新される。ユーザ情報格納部３４には、上記マスタ情報格納部３７に格納されたマスタ情報のうちユーザの属性情報

が格納され、さらにユーザが利用できるサービスのリストが格納される。アプリケーションデータ格納部３５には、自サーバ上で実行されるアプリケーションが用いるアクセス制御ファイル、設定ファイル及び個別データが格納される。

【００３０】

連携サーバ３は、要求側サーバ１又は提供側サーバ２から、ユーザが利用可能なサービスについての問い合わせを受信すると、上記ユーザ情報格納部３４に格納されたサービスリストを検索して、当該ユーザが要求するサービスを利用可能か否かを判断し、その結果を要求元の要求側サーバ１又は提供側サーバ２へ回答する。

【００３１】

なお、以上述べた要求側サーバ１、提供側サーバ２及び連携サーバ３による基本的な機能とその動作については、特開２０１０－８６０８０号公報「分散情報連携システムおよび分散情報連携方法」に詳しく記載されている。

【００３２】

次に、本実施形態に係る情報流通システムが例えば医療従事者用インターネットサービスを実施する上で使用する各種管理データの構成を説明する。

提供側サーバ２がサービスを提供する医療従事者用インターネットサービスのうち、紹介状に関するサービスを利用するユーザは、紹介状を発行する医師、紹介状を受領する医師、紹介状を発行される患者の３ユーザである。

【００３３】

紹介状サービスでは、医師にはその属性として組織と資格が付与される。一方、患者は個人ではあるもののある組織に所属していたり資格を持っていることもあるが、紹介状サービスを利用するに当たっては、どこの組織にも属さずまた資格の有無も関係しないため、これらの情報を属性として持たない。また、医療従事者用インターネットサービスには様々なサービスがあるが、そのうちの紹介状サービスを利用するユーザには当該紹介状サービスのみを利用可能な権限を与える。このユーザを自動認証ユーザと呼称する。紹介状サービスを提供するシステムが信頼するのはこの自動認証ユーザだけであり、自動認証ユーザは組織も資格も持たない特別なユーザという扱いとする。

【００３４】

紹介状管理データ、紹介状属性データ及びアプリケーション検索設定ファイルといった、特定のアプリケーションを実行するときに用いる設定ファイルは、提供するサービス種別に依存するため提供側サーバ２のアプリケーションデータ格納部２５に格納される。これに対しアクセス制御ファイルは、要求側サーバ１、提供側サーバ２及び連携サーバ３がそれぞれアクセス制御判定処理を実施するときに用いるため、それぞれのサーバ１，２，３のアプリケーションデータ格納部１５，２５，３５に格納される。こちらのアプリケーションデータ格納部１５，２５，３５に格納される各管理データは、紹介状サービスを提供するに際に事前にユーザにより設定され、必要に応じて適宜アクセス制御項目の登録、更新、削除が行なわれる。

【００３５】

図２及び図３は、それぞれ紹介状サービスを提供する提供側サーバ２に格納される紹介状管理データ及び紹介状属性データの記述例を示すものである。同図に示すように紹介状管理データは、データの状態を表すステータスと、実行ユーザ名と、文書ＩＤと、シーケンス番号と、フォーマット種別と、実データと、署名者のユーザＩＤと、登録日時及び更新日時と、削除フラグとから構成される。また紹介状属性データは、データの状態を表すステータスと、実行ユーザ名と、文書ＩＤと、差出人のユーザＩＤと、差出人の組織ＩＤと、受取人のユーザＩＤと、受取人の組織ＩＤと、対象者のユーザＩＤと、対象者の組織ＩＤと、状態と、発行日時と、登録日時及び更新日時と、アクセス制御ルール番号とから構成される。

【００３６】

一方図４、図５及び図６は、それぞれ連携サーバ３、病院Ｘのサーバ（要求側サーバ１）及び提供側サーバ２に格納される紹介状アプリケーションアクセス制御ファイルの記述

例を示すものである。同図に示すように紹介状アプリケーションアクセス制御ファイルは、データの状態を表すステータスと、実行ユーザ名と、アクセス制御ルール名と、ルール格納場所と、アクセス対象のデータ名と、開示先となる条件ユーザと、開示先となる条件組織と、開示先の資格と、検索の可否及び更新の可否を表すフラグとを含む。なお、このうち図４及び図５に記述されている、ユーザの役割や属性、ステータス等の前提条件に対するアクセス制御ルールは、紹介状データを閲覧する許可を与えたタイミングで更新される。また、図６に記述されているアクセス制御ルールは、紹介状管理データを提供側サーバ２に登録するタイミングで更新される。

【００３７】

［動作］

次に、以上のように構成された情報流通システムによるアクセス制御動作を説明する。

ここでは、例えば図８に示すように、病院Ｘの医師Ｂが患者Ａの紹介状を作成して紹介状サービスに登録し、この紹介状を紹介先の病院Ｙの医師Ｃが紹介状サービス受け取ると共に、患者Ａが自身の紹介状の流通状態を確認する場合を例にとって説明を行う。

【００３８】

（１）紹介状データの登録・閲覧権限付与

図９は、医師Ｂが患者Ａの紹介状を発行し登録する場合の処理手順と処理内容を示すフローチャートである。なお、システムを起動すると、連携サーバ３、要求側サーバ１及び提供側サーバ２では、先ず図４、図５及び図７に示した紹介状アプリケーションアクセス制御ファイル及び紹介状アプリケーション設定ファイルが各格納部から読込まれる。

【００３９】

この状態で、医師Ｂが自身のクライアント端末４において患者Ａの紹介状を作成し、病院Ｘのポータルサーバ（要求側サーバ１）に対しＷｅｂアクセスすると、要求側サーバ１から提供側サーバ２に対して紹介状を登録するために必要となる文書ＩＤの払い出し要求が送られる。提供側サーバ２は、要求された文書ＩＤを払い出した後、図２に示す照会状管理データに当該文書ＩＤと重複するＩＤが登録されていないか否かを確認する。その結果、重複があればエラーメッセージを要求側サーバ１へ返送して処理を終了する。

【００４０】

これに対し重複がないことが確認されると、提供側サーバ２は紹介状属性データ（図３に例示）に、文書ＩＤ、実行ユーザ名、ステータス及び紹介状の中身である実データ等の必要な項目データを書き込む。また、この作成した紹介状に対して誰がアクセスしてよいかを判断するためのアクセス制御ルールを、紹介状アプリケーションアクセス制御ファイル（図６）に追記する。さらに、ユーザの役割を表す紹介状の差出人、受取人及び対象者のユーザＩＤとその所属組織のＩＤを、紹介状属性データ（図３）に登録する。そして、最後に要求側サーバ１が、個々の紹介状に対して、関連のある診療データや検査結果を閲覧してもよいかどうかを制御するためのアクセス制御ルールを、紹介状アプリケーションアクセス制御ファイル（図５）に追記する。

【００４１】

以上の処理をもう少し詳しく説明する。

紹介元の医師Ｂが、自身が使用するクライアント端末４のＷｅｂブラウザ４１を操作して、病院Ｘのポータルサーバ（要求側サーバ１）にログインし、Ｗｅｂメニューから紹介状サービスを選択したとする。そうすると要求側サーバ１は、紹介状サービスを利用するために連携サーバ３に医師Ｂのユーザ情報を転送する。連携サーバ３は、転送された医師Ｂのユーザ情報をユーザ情報格納部３４に格納されているユーザ情報と照合することにより医師Ｂが当該紹介状サービスを利用可能か否かを判定し、この判定結果を要求側サーバ１に返送する。要求側サーバ１は、上記判定の結果医師Ｂの正当性が確認されると、紹介状サービスを提供する提供側サーバ１に対し紹介状サービスの提供を依頼する。

【００４２】

この実施形態では、図８に例示したように紹介状の差出人が医師Ｂ、受取人が医師Ｃ、対象者は患者Ａであるため、紹介状属性データ（図３）には差出人のユーザＩＤと組織Ｉ

Ｄ、受取人のユーザＩＤと組織ＩＤ、対象者のユーザＩＤからなる５種類のデータが事前に記述される。なお、患者Ａは組織に属さないため、紹介状属性データ（図３）には患者Ａの組織ＩＤは記述されていない。

【００４３】

また、紹介状アプリケーションアクセス制御ファイル（図６）には、アクセス権限として、差出人にはデータ登録・更新・削除を、また受取人にはデータ検索・参照をそれぞれ許可し、かつ対象者には紹介状データの検索権限のみを許可するように設定されたアクセス制御ルールが記述される。なお、このアクセス制御ルールは、紹介状サービスに対し事前に利用登録された自動認証ユーザに対してのみ設定される。

【００４４】

なお、処方箋の場合は、例えば差出人は医師Ｂ、受取人は調剤薬局Ｚの薬剤師Ｄ、対象者は患者Ａとなる。処方箋属性データは、紹介状属性データと同じデータ構造となる。処方箋に対しては、アクセス権限として、差出人にはデータ登録・更新・削除を、また受取人にはデータ検索・更新・参照をそれぞれ許可し、対象者にはデータ検索・参照のみを許可するように設定されたアクセス制御ルールが、アプリケーションアクセス制御ファイル（図６）に記述される。なお、紹介状の場合と同じく、差出人のデータ削除は状態によって変更する必要がある。

【００４５】

提供側サーバ２は、要求側サーバ１において紹介状が作成され、当該紹介状データが転送されると、紹介状アプリケーション設定ファイルに、上記紹介状データの受け渡しに必要な情報を記述する。図７はその一例を示すものである。すなわち、紹介状を受け渡す準備として、先ずcheckポイントにおいて、差出人と受取人の情報に基づき現在のステータスに対するアクセス権限を確認する処理を呼び出す。checkポイントの時点では、まだ紹介状アプリケーションアクセス制御ファイル（図６）への登録は行なわれていない。アクセス権限が確認された後に、以下のregistポイントへ遷移し、紹介状管理データ及び紹介状属性データに関連する情報と、紹介状アプリケーションアクセス制御ファイル（図６）にデータが登録される。

【００４６】

なお、他サーバから要求が来たときに独自のアクセス権限を設定する方法について以下に述べる。

提供側サーバ２では、様々なアプリケーションを提供しており、一般に他サーバ（要求側サーバ１）からの依頼に対して、アクセス制御ルールを用いて処理を実行している。しかし、要求側サーバ１からの要求に対し、信頼できるかどうか疑わしい場合がある。そこで、要求を実施する前に判定する方法として、サービスタイプという概念を導入する。これは使用したいサービスを表す識別子のことを指す。紹介状サービスのサービスタイプを"ReferralService"とする。

【００４７】

サービス提供者は、紹介状独自のアクセス権限に基づき処理をすることをサービスタイプリストに記述する。ユーザがＷｅｂブラウザ４１から紹介状サービスを利用する場合は、ユーザが入力する情報に加えてサービスタイプも合わせて提供側サーバ２に転送する。提供側サーバ２は、アクセス制御判定部２２２においてサービスタイプリストを検索し、"ReferralService"に対応する処理を呼び出して実行する。なお、サービスタイプリストの中に上記要求されたサービスタイプが存在しなければ、サービスタイプリストが途中で書き換えられた可能性があるため、処理を中断する。

【００４８】

以上のように登録を行うことで、紹介状データを閲覧した紹介先の医師Ｃが、必要に応じて患者Ａの診療データを見ながら、より詳細な診断を行なうことが可能となる。

【００４９】

（３）患者による紹介状の閲覧

図１０は、患者Ａが自身についての紹介状を閲覧しようとする場合の処理手順と処理内

容を示すフローチャートである。なお、このサービスを利用するに当たり、サーバ１を起動した時点で図４、図５及び図７に示した各ファイルが読み込まれる。

【００５０】

紹介元病院Ｘの医師Ｂに罹っている患者Ａが、自身のクライアント端末を操作して医療ポータルサーバ（要求側サーバ１）に対しＷｅｂアクセスし、これにより自身の紹介状の検索要求を入力したとする。このとき、紹介状検索要求の入力項目としては、患者自身の名前、紹介元病院Ｘにおける患者番号（診察券に印字されている番号）、医師情報（病院Ｘの担当医師Ｂ）が入力される。上記検索要求を受け取ると要求側サーバ１は、当該紹介状の検索要求を、紹介状サービスを提供している提供側サーバ２に転送する。

【００５１】

上記紹介状検索要求を受け取った提供側サーバ２は、先ず連携サーバ３に対し要求元の患者Ａについて問い合わせる。連携サーバ３は、上記問い合わせに対しユーザ情報格納部３４を検索することにより要求元の患者Ａの資格を確認する。そして、その結果を提供側サーバ２に返送する。

【００５２】

提供側サーバ２は、上記連携サーバ３から問い合わせに対する確認結果を受け取り、この情報により患者Ａが医師の資格を持たないと判定すると、続いてアクセス制御判定部２２２において紹介状アプリケーションアクセス制御ファイル（図６）をもとにアクセス制御ルールの記載内容を確認する。このとき、アクセス制御ルールとしては、「医師の資格を持たないユーザからのアクセス権限は検索結果リストのみ表示で内容は閲覧させない」旨が記載されている。このため提供側サーバ２は、図２に示した紹介状管理データから紹介状が発行されているかどうかのみを検索し、その検索結果をリスト化して要求側サーバ１に送信する。要求側サーバ１は、上記検索結果を表すリストを受け取ると、このリストを要求元の患者Ａのクライアント端末４へ送信して表示させる。

【００５３】

すなわち、提供側サーバ２は、検索を依頼したユーザの資格やアクセス権限の情報を最初に調べ、その結果に基づき紹介状データの検索を実行する。検索を行なう前のチェックで実行する処理と確認結果後の処理はデータの種類（電子フォーマット）に依存することから、電子フォーマットの種類を指定することで、実行処理の中で振り分けることが可能となる。

【００５４】

［実施形態の効果］

以上詳述したようにこの実施形態では、要求側サーバ１からの登録要求に対し、提供側サーバ２がサービス対象となる紹介状等のデータに関連付けて、当該データに係るユーザが差出人、受取人、対象者の何れであるかを表す役割情報と、当該ユーザの所属組織と資格を表す属性情報と、当該データに対するアクセスの状況の変化を表すステータスを記憶する。またそれと共に、上記役割情報、属性情報及び更新後のステータスに基づいて設定されたアクセス制御ルールを記憶する。そしてこの状態で、要求側サーバ１からアクセス要求が送信されると、サービス対象となるデータに対するアクセス制御に先立ちアクセス制御ルールを確認し、このアクセス制御ルールに従い上記サービス対象となるデータに対するアクセス制御を実行するようにしている。

【００５５】

したがって、ユーザの操作に応じて要求側サーバ１から紹介状データに対するアクセス要求が発生すると、ユーザの役割が差出人、受取人及び対象者の何れであるのかと、所属組織又は資格を考慮して設定されたアクセス制御ルールに従い、紹介状データに対するアクセス制御を適切に実行することができる。しかも、アクセス制御ルールは、紹介状データに対する最新のアクセス状況を表すステータスも考慮される。このため、ユーザの役割や属性が変わらなくても、紹介状データに対するアクセス状況（例えば作成済、閲覧済、編集済）が変化した場合には、この変化に応じて適切なアクセス制御を実行することが可能となる。さらに、サービス対象データの電子フォーマット種別を記憶しておくことで、

サービス対象データ（紹介状、処方箋など）が複数種類ある場合でも、これらの種類ごとに、それに応じた適切なアクセス制御を実行することが可能となる。

【００５６】

なお、この発明は上記実施形態に限定されるものではない。例えば、この発明のシステムは医療情報を流通するシステムに限るものではなく、サービス対象データについても紹介状や処方箋に限定されるものではない。例えば、会社で決裁文書を起案した場面において、起案者から自部署の部長に決裁確認をとるのであれば、差出人と対象者が起案者、受取人が自部署の部長になる。さらに自部署の部長決裁が完了した後で、次に総務部長に決裁を依頼する処理フローであれば、差出人が自部署の部長、受取人が総務部長、進捗を確認する起案者が対象者となる。すなわち、様々な場面で適用できるモデルであり、このモデルを適用することで、様々な種類の電子フォーマットに対して関係する人々の属性データおよび、各々の人に対するファイルのアクセス制御ルールを設定できる。

【００５７】

その他、ネットワークの種類、各情報処理装置の種類や構成、その処理手順及び処理内容、図２乃至図６に示したデータの構成や項目の内容（電子フォーマットの構成）等についても、この発明の要旨を逸脱しない範囲で種々変形して実施可能である。

【００５８】

要するにこの発明は、上記実施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できる。また、上記実施形態に開示されている複数の構成要素の適宜な組み合せにより種々の発明を形成できる。例えば、実施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、異なる実施形態に亘る構成要素を適宜組み合せてもよい。

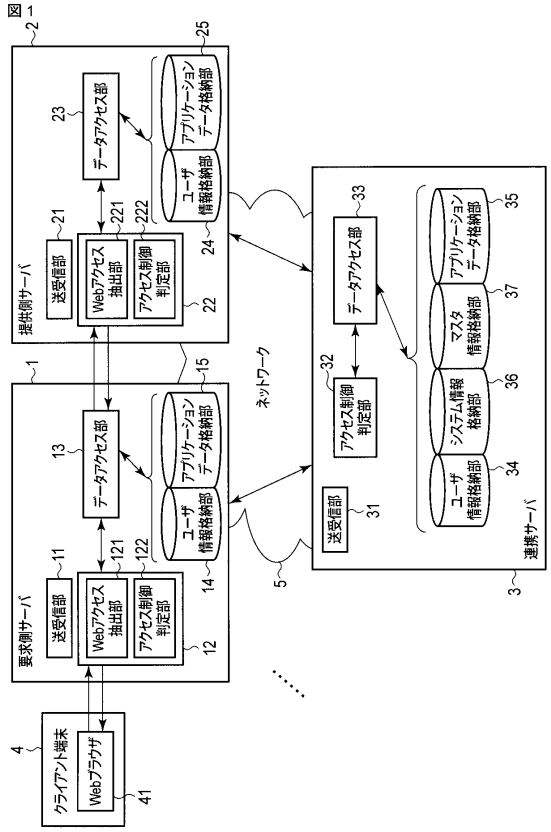
【符号の説明】

【００５９】

１…要求側サーバ、２…提供側サーバ、３…連携サーバ、４…クライアント端末、５…ネットワーク、１１，２１，３１…送受信部、１２，２１…アクセス制御部、１２１，２２１…Ｗｅｂアクセス抽出部、１２２，２２２，３２…アクセス制御判定部、１３，２３，３３…データアクセス部、１４，２４，３４…ユーザ情報格納部、１５，２５，３５…アプリケーションデータ格納部、３６…システム情報格納部、３７…マスタ情報格納部。

【図１】

図１



【図２】

図２

ステータス	実行ユーザ	文書ID	シーケンス番号	フォーマット種別	実データ	署名者ユーザID	登録日時	更新日時	削除フラグ
作成	医師B	0001	1	紹介状	<?xml version="1.0"> <Referral Data> …	DR_B	2011/09/18 13:34:00	2011/09/18 14:12:23	—
閲覧	医師C	0001	1	紹介状	<?xml version="1.0"> <Referral Data> …	DR_B	2011/09/20 10:23:21	2011/09/20 10:23:21	—
作成	医師B	0002	1	紹介状	<?xml version="1.0"> <Referral Data> …	DR_B	2011/09/20 10:54:03	2011/09/20 10:54:03	—
…									

＜紹介状管理データ＞

【図３】

図３

ステータス	実行ユーザ	文書ID	差出人ユーザID	差出人組織ID	受取人ユーザID	受取人組織ID	対象者ユーザID	対象者組織ID	状態	発行日付	登録日時	更新日時	アクセス制御ルールNo.
作成	医師B	0001	DR_B	Host_x	DR_C	Host_Y	PT_A	—	作成	2011/09/18 13:34:00	2011/09/18 13:34:00	2011/09/18 14:12:23	—
作成	自動認証ユーザ	0001											0004
作成	自動認証ユーザ	0001											0005
作成	自動認証ユーザ	0001											0006
作成	医師B	0001											0007
閲覧	医師C	0001	DR_B	Host_x	DR_C	Host_Y	PT_A	—	閲覧	2011/09/18 13:34:00	2011/09/18 13:34:00	2011/09/20 11:42:56	—
…													

＜紹介状属性データ＞

【図４】

図４

ステータス	実行ユーザ	アクセス制御ルールNo.	ルール名	ルール格納場所	対象データ	開示先条件ユーザ	開示先条件組織	開示先資格	検索可否	更新可否	…
前提条件	—	0001	自動認証ユーザが保有資格データを検索できる	連携サーバ		自動認証サーバ上のユーザID			1	0	
前提条件	—	0003	医師Cが組織データを検索できる	連携サーバ				医師Cの資格	1	0	
…											

＜紹介状アプリケーションアクセス制御ファイル（連携サーバに格納されるもの）＞

【図５】

図5

ステータス	実行ユーザ	アクセス制御ルールNo.	ルール名	ルール格納場所	対象データ	開示先条件ユーザ	開示先条件組織	開示先資格	検索可否	更新可否	…
前提条件	—	0002	病院Xの医師Bがアクセス制御ファイルに診察データの検索、更新設定ができる	病院Xのサーバ	病院Xの診察データ	病院Xの医師BのユーザID			1	1	
作成	医師B	0007	病院Yが患者Aの診察データを検索できる	病院Yのサーバ	病院Yの患者AのユーザID		病院Yの組織ID		1	0	
…											

＜紹介状アプリケーションアクセス制御ファイル（病院Xのポータル(要求側サーバ)に格納されるもの）＞

【図６】

図6

ステータス	実行ユーザ	アクセス制御ルールNo.	ルール名	ルール格納場所	対象データ	開示先条件ユーザ	開示先条件組織	開示先資格	検索可否	更新可否	…
作成	自動認証ユーザ	0004	病院Yの医師Cが文書ID(0001)の属性データを検索できる	医療従事者用サービス提供サーバ	文書ID(0001)	医師CのユーザID	病院Yの組織ID		1	0	
作成	自動認証ユーザ	0005	医師Bが文書ID(0001)の属性データを検索できる	医療従事者用サービス提供サーバ	文書ID(0001)	医師BのユーザID	病院Xの組織ID		1	0	
作成	自動認証ユーザ	0006	患者Aが文書ID(0001)の属性データを検索できる	医療従事者用サービス提供サーバ	文書ID(0001)	患者AのユーザID			1	0	
…											

＜紹介状アプリケーションアクセス制御ファイル（医療従事者用サービス提供サーバ）に格納されるもの）＞

【図７】

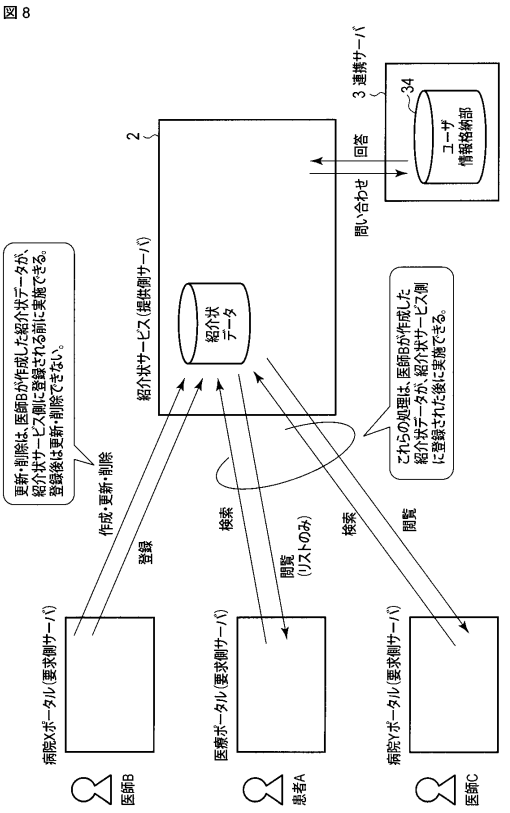
図7

```
<?xml version="1.0" encoding="UTF-8">
<DocumentConfigurationFile xmlns="http://...">
  <Map>
    <Point>check</Point>
    <ActionName>insert</ActionName>
    <DocType>紹介状</DocType>
    <ClassName>紹介状データアクセス権限確認</ClassName>
  </Map>
  <Map>
    <Point>regist</Point>
    <ActionName>insert</ActionName>
    <DocType>紹介状</DocType>
    <ClassName>紹介状データアクセス権限更新</ClassName>
  </Map>
    .  .  .  .
</DocumentConfigurationFile>
```

＜紹介状アプリケーション設定ファイル＞

【図８】

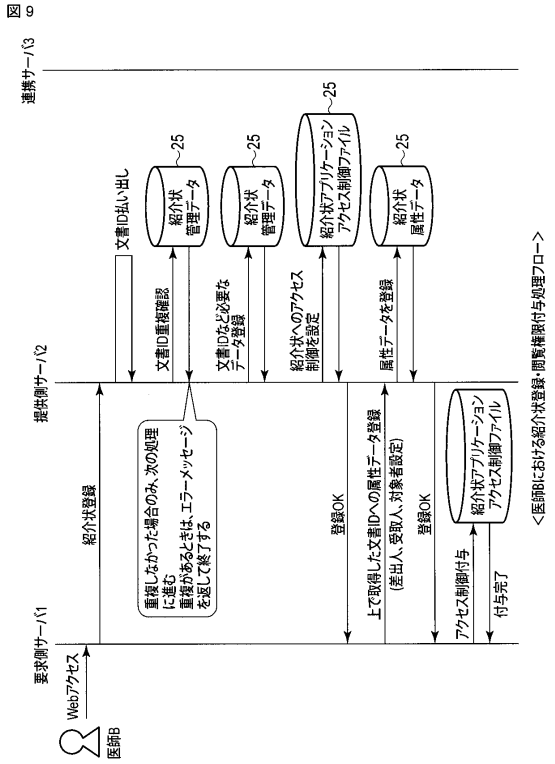
図8



＜紹介状サービスのイメージ＞

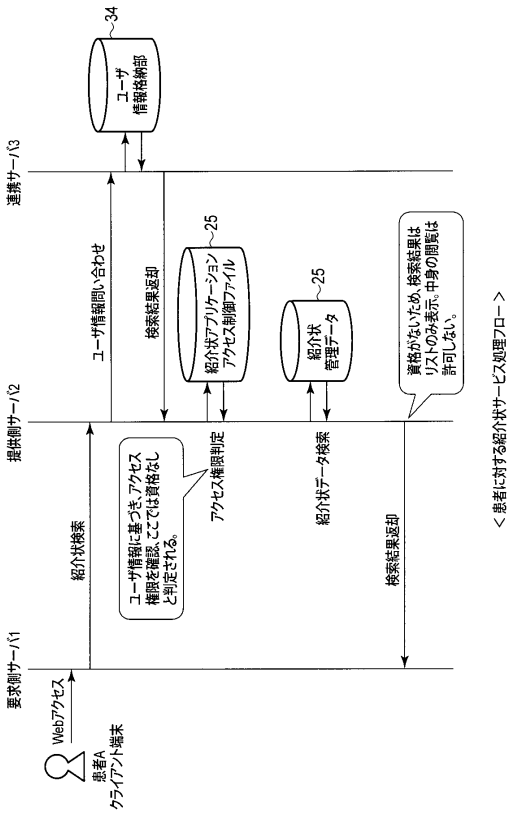
【図９】

図 9


連携サーバ3
提供側サーバ2
要求側サーバ1
Webアクセス
医師B
紹介状登録
文書ID払い出し
文書の重複確認
重複しなかった場合のみ、次の処理に進む
重複がある場合は、エラーメッセージを返して終了する
文書IDなど必要なデータ登録
紹介状への
アクセス制御を設定
属性データを登録
登録OK
上で取得した文書IDへの属性データ登録
(差出人、受取人、対象者設定)
登録OK
アクセス制御付与
付与完了
紹介状
管理データ
紹介状
管理データ
紹介状アプリケーション
アクセス制御ファイル
紹介状
属性データ
紹介状アプリケーション
アクセス制御ファイル
25
25
25
25
<医師Bにおける紹介状登録・閲覧権限付与処理フロー>

【図１０】

図 10


連携サーバ3
提供側サーバ2
要求側サーバ1
Webアクセス
患者A
クライアント端末
紹介状検索
ユーザ情報問い合わせ
検索結果返却
ユーザ
情報格納部
紹介状アプリケーション
アクセス制御ファイル
紹介状
管理データ
ユーザ情報に基づき、アクセス権限を確認。ここでは資格なしと判定される。
アクセス権限判定
紹介状データ検索
資格がないため、検索結果はリストのみ表示。中身の閲覧は許可しない。
検索結果返却
34
25
25
<患者に対する紹介状サービス処理フロー>

フロントページの続き

(72)発明者　橋本　順子
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　宮島　麻美
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　白石　将浩
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　吉田　芳浩
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　爰川　知宏
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　前田　裕二
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

審査官　木村　励

(56)参考文献　特開２００１－２９７１５３（ＪＰ，Ａ）
特開２０１１－１００３６２（ＪＰ，Ａ）
特開２０１０－０８６０８０（ＪＰ，Ａ）
特開２００５－１２２３８０（ＪＰ，Ａ）
特開２０１０－２３７８３４（ＪＰ，Ａ）
特開平１１－３３８９５０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／６０　－　２１／６４
Ｇ０６Ｑ　５０／２４