(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3566478号
(P3566478)
(45)発行日　平成16年9月15日(2004.9.15)　(24)登録日　平成16年6月18日(2004.6.18)

(51)Int.Cl.[7]	F I		
G06F 12/14	G06F	12/14	520F
G06F 12/00	G06F	12/14	530D
G06F 17/30	G06F	12/14	560B
	G06F	12/00	537A
	G06F	17/30	110F

請求項の数 10　(全 13 頁)　最終頁に続く

(21)出願番号　特願平8-358607
(22)出願日　平成8年12月27日(1996.12.27)
(65)公開番号　特開平10-187542
(43)公開日　平成10年7月21日(1998.7.21)
審査請求日　平成12年6月28日(2000.6.28)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100081880
弁理士　渡部　敏彦
(72)発明者　椎山　弘隆
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

審査官　高橋　克

最終頁に続く

(54)【発明の名称】文書セキュリティ管理システム、文書セキュリティ管理方法および文書検索装置

(57)【特許請求の範囲】
【請求項１】
ネットワークを介してクライアント端末に接続された文書検索サービスサーバと、
該文書検索サービスサーバを通じて前記ネットワークに接続され、文書を蓄積するデータサーバとを備え、
前記文書検索サービスサーバは前記クライアント端末から指定された文字列にしたがって前記データサーバに蓄積されている文書を検索する文書セキュリティ管理システムにおいて、
前記データサーバには、アクセス制限文字列およびそのパスワードのテーブルが格納されており、
前記文書検索サービスサーバは、
前記アクセス制限文字列およびそのパスワードを設定する設定手段と、
検索時、前記クライアント端末から前記テーブルに格納された前記アクセス制限文字列およびそのパスワードの指定がない場合、該アクセス制限文字列を含む文書へのアクセスを禁止する禁止手段とを備えたことを特徴とする文書セキュリティ管理システム。
【請求項２】
前記文書検索サービスサーバと前記データサーバとの間にファイアウォールを設けたことを特徴とする請求項１記載の文書セキュリティ管理システム。
【請求項３】
前記アクセス制限文字列およびそのパスワードの登録を要求した者のＩＰアドレスが前記

テーブルに格納されていることを特徴とする請求項１記載の文書セキュリティ管理システム。
【請求項４】
前記アクセス制限文字列は、前記登録を要求した者から削除要求が合った場合、あるいは異なるＩＰアドレスを有する者から所定数以上の削除要求があった場合に前記テーブルから削除されることを特徴とする請求項３記載の文書セキュリティ管理システム。
【請求項５】
検索結果を表示する表示装置を備え、
該表示装置は、前記検索された文書に前記アクセス制限文字列が含まれている場合、該アクセス制限文字列に対するパスワードの入力を要求する画面を表示することを特徴とする請求項１記載の文書セキュリティ管理システム。
【請求項６】
前記データサーバは、前記文書がイメージデータである場合、該イメージデータをＯＣＲ処理によってテキストデータに変換し、該変換されたテキストデータを前記イメージデータと対応付けて蓄積することを特徴とする請求項１記載の文書セキュリティ管理システム。
【請求項７】
前記文書検索サービスサーバは、前記検索された文書が前記アクセス制限文字列を含まない場合、該検索された文書に属性を付加して前記クライアント端末に検索結果を通知することを特徴とする請求項１記載の文書セキュリティ管理システム。
【請求項８】
前記ネットワークおよび前記文書検索サービスサーバ間にファイアウォールが設けられたことを特徴とする請求項１記載の文書セキュリティ管理システム。
【請求項９】
ネットワークを介してクライアント端末に接続された文書検索サービスサーバと、
該文書検索サービスサーバを通じて前記ネットワークに接続され、文書を蓄積するデータサーバとを備え、
前記文書検索サービスサーバは前記クライアント端末から指定された文字列にしたがって前記データサーバに蓄積されている文書を検索する文書セキュリティ管理方法において、
前記データサーバには、アクセス制限文字列およびそのパスワードのテーブルが格納されており、
前記文書検索サービスサーバは、
前記アクセス制限文字列およびそのパスワードを設定し、
検索時、前記クライアント端末から前記テーブルに格納された前記アクセス制限文字列およびそのパスワードの指定がない場合、前記アクセス制限文字列を含む文書へのアクセスを禁止することを特徴とする文書セキュリティ管理方法。
【請求項１０】
文書を蓄積するとともに、アクセス制限文字列およびそのパスワードが格納されたテーブルを有するデータサーバから文書を検索する文書検索装置であって、
前記アクセス制限文字列およびそのパスワードを設定する設定手段と、
検索時、クライアント端末から前記テーブルに格納された前記アクセス制限文字列およびそのパスワードの指定がない場合、該アクセス制限文字列を含む文書へのアクセスを禁止する禁止手段とを有することを特徴とする文書検索装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、文書セキュリティ管理システム、文書セキュリティ管理方法および文書検索装置に関する。
【０００２】
【従来の技術】

従来、文書セキュリティ管理システムでは、外部に対してファイアウォールを形成することで実現されてきた。その内部のセキュリティはデータの暗号化という手段で対応していた。

【０００３】

また、機密度の高い文書データを共有システムで管理する場合、予めアクセス権を制限したグループ単位で文書管理を行ったり、文書個々にアクセス権やキーワードを付与することが行われていた。

【０００４】

【発明が解決しようとする課題】

しかしながら、前者の場合、文書データの効率的な共有を阻害していた。また、後者の場合、機密文書のアクセス権範囲の柔軟性を欠いたり、また、機密性が無くなり公に開示する際の運用を柔軟に対応できなかった。

【０００５】

そこで、本発明は文書データを効率よく共有しつつ、機密文書のアクセス権範囲を柔軟に対応することができる文書セキュリティ管理システム、文書セキュリティ管理方法および文書検索装置を提供することを目的とする。

【０００６】

また、本発明は機密性が無くなり公に開示する際の運用を柔軟に対応できる文書セキュリティ管理システム、文書セキュリティ管理方法および文書検索装置を提供することを他の目的とする。

【０００７】

【課題を解決するための手段】

上記目的を達成するために、請求項１に記載の文書セキュリティ管理システムは、ネットワークを介してクライアント端末に接続された文書検索サービスサーバと、該文書検索サービスサーバを通じて前記ネットワークに接続され、文書を蓄積するデータサーバとを備え、前記文書検索サービスサーバは前記クライアント端末から指定された文字列にしたがって前記データサーバに蓄積されている文書を検索する文書セキュリティ管理システムにおいて、前記データサーバには、アクセス制限文字列およびそのパスワードのテーブルが格納されており、前記文書検索サービスサーバは、前記アクセス制限文字列およびそのパスワードを設定する設定手段と、検索時、前記クライアント端末から前記テーブルに格納された前記アクセス制限文字列およびそのパスワードの指定がない場合、該アクセス制限文字列を含む文書へのアクセスを禁止する禁止手段とを備えたことを特徴とする。

【０００８】

請求項２に記載の文書セキュリティ管理システムは、請求項１に係る文書セキュリティ管理システムにおいて前記文書検索サービスサーバと前記データサーバとの間にファイアウォールを設けたことを特徴とする。

【００１０】

請求項３に記載の文書セキュリティ管理システムでは、請求項１に係る文書セキュリティ管理システムにおいて前記アクセス制限文字列およびそのパスワードの登録を要求した者のＩＰアドレスが前記テーブルに格納されていることを特徴とする。

【００１１】

請求項４に記載の文書セキュリティ管理システムでは、請求項３に係る文書セキュリティ管理システムにおいて　前記アクセス制限文字列は、前記登録を要求した者から削除要求が合った場合、あるいは異なるＩＰアドレスを有する者から所定数以上の削除要求があった場合に前記テーブルから削除されることを特徴とする。

【００１２】

請求項５に記載の文書セキュリティ管理システムは、請求項１に係る文書セキュリティ管理システムにおいて検索結果を表示する表示装置を備え、該表示装置は、前記検索された文書に前記アクセス制限文字列が含まれている場合、該アクセス制限文字列に対するパスワードの入力を要求する画面を表示することを特徴とする。

【００１３】
請求項６に記載の文書セキュリティ管理システムでは、請求項１に係る文書セキュリティ管理システムにおいて前記データサーバは、前記文書がイメージデータである場合、該イメージデータをＯＣＲ処理によってテキストデータに変換し、該変換されたテキストデータを前記イメージデータと対応付けて蓄積することを特徴とする。
【００１４】
請求項７に記載の文書セキュリティ管理システムでは、請求項１に係る文書セキュリティ管理システムにおいて前記文書検索サービスサーバは、前記検索された文書が前記アクセス制限文字列を含まない場合、該検索された文書に属性を付加して前記クライアント端末に検索結果を通知することを特徴とする。
【００１５】
請求項８に記載の文書セキュリティ管理システムでは、請求項１に係る文書セキュリティ管理システムにおいて前記ネットワークおよび前記文書検索サービスサーバ間にファイアウォールが設けられたことを特徴とする。
【００１６】
請求項９に記載の文書セキュリティ管理方法は、ネットワークを介してクライアント端末に接続された文書検索サービスサーバと、該文書検索サービスサーバを通じて前記ネットワークに接続され、文書を蓄積するデータサーバとを備え、前記文書検索サービスサーバは前記クライアント端末から指定された文字列にしたがって前記データサーバに蓄積されている文書を検索する文書セキュリティ管理方法において、前記データサーバには、アクセス制限文字列およびそのパスワードのテーブルが格納されており、前記文書検索サービスサーバは、前記アクセス制限文字列およびそのパスワードを設定し、検索時、前記クライアント端末から前記テーブルに格納された前記アクセス制限文字列およびそのパスワードの指定がない場合、前記アクセス制限文字列を含む文書へのアクセスを禁止することを特徴とする。
請求項１０に記載の文書検索装置は、文書を蓄積するとともに、アクセス制限文字列およびそのパスワードが格納されたテーブルを有するデータサーバから文書を検索する文書検索装置であって、前記アクセス制限文字列およびそのパスワードを設定する設定手段と、検索時、クライアント端末から前記テーブルに格納された前記アクセス制限文字列およびそのパスワードの指定がない場合、該アクセス制限文字列を含む文書へのアクセスを禁止する禁止手段とを有することを特徴とする。
【００１７】
【発明の実施の形態】
本発明の文書セキュリティ管理システム、文書セキュリティ管理方法および文書検索装置の実施の形態について説明する。図１は実施の形態における文書セキュリティ管理システムの構成を示すブロック図である。
【００１８】
この文書セキュリティ管理システム１は、文書データを蓄積するデータサーバ５、ＬＡＮ３に接続された全文検索サービス（ＦＴＳ）サーバ７、および全文検索サービスサーバ７およびデータサーバ５間に配置されたファイアウォール９を有する。
【００１９】
このような文書セキュリティ管理システム１では、ファイアウォール９の外側に全文検索サービスサーバ７が設けられているので、ＬＡＮ３に接続されたどのクライアント端末１２からも全文検索サービスサーバ７にアクセス可能である。
【００２０】
文書セキュリティ管理システム１では、セキュリティ管理上、検索用ファイル（全文検索インデックス）やアクセス制限文字列・パスワードの情報はファイアウォール９の内側にあるデータサーバ５に設けられている。
【００２１】
全文検索サービスサーバ７では全文検索サービスソフトウェアが動作しており、ファイア

ウォール９を越えて行われるデータのやり取りは全て全文検索サービスソフトウェアを経由し、データサーバ５に蓄積された文書テキストデータ（文書）・文書イメージデータに対してのアクセスは全文検索サービスソフトウェアが実行することとなる。

【００２２】

全文検索方式としては、文字インデックス方式（特開平８－７０３３号公報参照）、単語インデックス方式のいずれでもよいが、アクセス制限文字列が特殊な言葉になる可能性があるので、検索漏れのおそれのない文字インデックス方式の方が好ましい。

【００２３】

図２はデータサーバ５に管理されているデータの構成を示す図である。データサーバ５は検索用ファイル（全文検索インデックス）、ＯＣＲテキスト情報、文書・文書イメージデータ本体、アクセス制限文字列管理情報などのデータを格納している。

【００２４】

使用者はデータサーバ５に蓄積されている文書・文書イメージデータを参照したい場合、文書・文書イメージに含まれる文字列を指定することにより文書・文書イメージデータを参照することができる。ここで、機密文書のアクセスを防ぐために文書に含まれる文字列の指定が制限されるが、この制限された文字列をアクセス制限文字列という。

【００２５】

つぎに、文書セキュリティ管理システム１における（Ａ）アクセス制限文字列登録処理、（Ｂ）アクセス制限文字列削除処理、（Ｃ）文書・データ登録処理、（Ｄ）文書・データ検索処理について説明する。

【００２６】

（Ａ）アクセス制限文字列登録処理

図３はアクセス制限文字列の登録処理手順を示すフローチャートである。機密文書に関わるアクセス制限文字列を指定したい場合、クライアント端末１２はアクセス制限文字列設定の要求を開始し（ステップＳ１）、全文検索サービスソフトウェアに対してそのアクセス制限文字列とアクセス制限文字列へのパスワードを設定するコマンドを送信する（ステップＳ２）。全文検索サービスサーバ７はアクセス制限文字列およびパスワードの登録要求者のＩＰアドレスをデータサーバ５に格納されたアクセス制限文字列管理情報テーブルに記憶する（ステップＳ３）。

【００２７】

図４はアクセス制限文字列管理情報テーブルを示す図である。全文検索サービスソフトウェアにより、アクセス制限文字列管理情報テーブルにアクセス制限文字列、パスワード、登録要求者のＩＰアドレスが書き込まれる。アクセス制限文字列管理情報テーブルはファイアウォール９より後方のデータサーバ５に格納されているので、セキュリティが確保される。

【００２８】

このアクセス制限文字列の登録要求は普通、機密事項を含む文書を登録する前に行われるべきであり、システム管理者との相談で行われるべきものである。また、アクセス制限文字列は日常使用する語は適当でなく、新語や造語に類する語であることが望ましい。したがって、日常用語辞書と比較して存在しないものを選ぶことが考えられる。

【００２９】

（Ｂ）アクセス制限文字列削除処理

機密性が無くなりその言葉を含む文書・文書イメージデータを開示したい場合、クライアント端末１２はアクセス制限文字列のアクセス制限解除依頼を全文検索サービスサーバ７に送信し、全文検索サービスソフトウェアに対してアクセス制限文字列とパスワードを渡す。

【００３０】

図５はアクセス制限文字列の解除処理手順を示すフローチャートである。登録要求を行ったＩＰアドレスを持つ者が原則としてそのアクセス制限文字列に対する情報を削除することができる。まず、削除要求された文字列がアクセス制限文字列のリストにあるか否かを

判別する（ステップＳ１１）。アクセス制限文字列のリストにある場合、パスワードが一致しているか否かを判別する（ステップＳ１２）。パスワードが一致している場合、登録要求者のＩＰアドレスであるか否かを判別する（ステップＳ１３）。登録要求者のＩＰアドレスである場合、そのアクセス制限文字列をアクセス制限文字列管理情報テーブルから削除する（ステップＳ１４）。

【００３１】

一方、登録要求者のＩＰアドレスでない場合、削除要求者のＩＰアドレスのリストにあるか否かを判別する（ステップＳ１５）。削除要求者のＩＰアドレスのリストにない場合、削除要求数＋１が削除開始しきい値（本実施形態では値３）を越えたか否かを判別する（ステップＳ１６）。削除開始しきい値を越えた場合、ステップＳ１４に移行し、アクセス制限文字列をアクセス制限文字列管理情報テーブルから削除する。

【００３２】

また一方、ステップＳ１１でアクセス制限文字列のリストにない場合、ステップＳ１２でパスワードが一致しない場合、ステップＳ１５で削除要求者のＩＰアドレスリストにある場合、ステップＳ１６で削除開始しきい値を越えていない場合、そのまま処理を終了する。

【００３３】

このように、登録者以外の者が削除する手段として、安全のために異なる複数の削除要求があった場合のみ削除することができるようにされている。この場合、データサーバ５のアクセス制限文字列管理情報テーブルにアクセス制限文字列削除要求を行った削除要求者のＩＰアドレスが記憶される場所を設けておく。また、異なるＩＰアドレスから同一のアクセス制限文字列に対して正しいパスワードで削除開始しきい値以上の削除要求があった場合、削除を許可する機能をデータサーバ５に設けておく。

【００３４】

（Ｃ）文書・文書イメージデータの登録処理

ＬＡＮ３に接続されたクライアント端末１２から文書・文書イメージデータの登録が指示された場合、全文検索サービスサーバ７上で動作している全文検索サービスソフトウェアにより文書・文書イメージデータがＬＡＮ３を通じてデータサーバ５に格納されると共に文書アドレスが決定される。

【００３５】

全文検索サービスソフトウェアは文書（テキストデータ）を文字キーに分解し、分解された文字キーを文書アドレスが記述された検索用ファイル（全文検索インデックス）に追加記録する（特開平８－７０３３号公報参照）。

【００３６】

文書イメージデータの場合、ＯＣＲ処理を行いその認識で得たテキストデータを文書（テキストデータ）の登録と同様文字キーに分解し、分解された文字キーを文書イメージアドレスが記述された検索用ファイル（全文検索インデックス）に追加記録する。このとき、ＯＣＲ処理から得られるテキストデータは元の文書イメージデータと対応付けて記憶される。

【００３７】

図６は文書・文書イメージデータの登録処理手順を示すフローチャートである。まず、クライアント端末１２から文書・文書イメージデータを転送してデータサーバ５に格納する（ステップＳ２１）。文書イメージデータが格納されたか否かを判別し（ステップＳ２２）、文書イメージデータでない場合、検索用ファイルを作成する（ステップＳ２３）。一方、文書イメージデータである場合、ＯＣＲ処理を行ってテキストデータを抽出し（ステップＳ２４）、ＯＣＲの誤認識を考慮して検索用ファイルを更新する（ステップＳ２５）。抽出されたテキストデータを元の文書イメージデータと対応付けて格納する（ステップＳ２６）。

【００３８】

（Ｄ）文書・データ検索処理

データサーバ５が蓄積している文書・文書イメージデータを参照したい場合、クライアント端末１２は参照したい文書・文書イメージデータに含まれる文字列を指定することにより検索処理を行う。全文検索ソフトウェアにより検索したい文字列（検索語）を文字キーに分解し、それらの文字キーを全て含む文書の文書アドレスを得た後、それらの分解キーが連続している文書データを調べて確定する。これにより高速に検索処理が行われる。

【００３９】

また、アクセス制限文字列を検索語に指定したい場合、同時にそれへのパスワードを指定することとなる。図７は検索時の検索条件入力画面を示す図である。必要があれば検索語にパスワードを指定できるような形となっている。

【００４０】

アクセス制限文字列とそのパスワードの指定が無い場合、そのアクセス制限文字列を含む文書は検索結果として表示されず、あたかもそのアクセス制限文字列を含む文書は存在しないようにみえる。

【００４１】

図９および図１０は文書・文書イメージデータの検索処理手順を示すフローチャートである。アクセス制限文字列へのパスワードが正しくない場合、指定する検索条件の中からそのアクセス制限文字列に該当する部分の演算を行わないことによりアクセス制限文字列およびパスワードを解析するための情報を使用者に与えないようにする。

【００４２】

まず、検索条件が入力されると（ステップＳ３１）、入力された検索語（パスワード）を１つ読み出す（ステップＳ３２）。読み出された検索語は「アクセス制限文字列＋パスワード指定」による検索語であるか否かを判別する（ステップＳ３３）。「アクセス制限文字列＋パスワード指定」による検索語でない場合、検索語を全文検索し、その結果を記憶する（ステップＳ３４）。

【００４３】

一方、「アクセス制限文字列＋パスワード指定」による検索語である場合、アクセス制限文字列管理情報テーブルからアクセス制限文字列であるか否かを判別する（ステップＳ３５）。アクセス制限文字列である場合、パスワードが合っているか否かを判別する（ステップＳ３６）。パスワードが合っている場合、検索語を全文検索し、その結果を記憶する（ステップＳ３７）。一方、アクセス制限文字列あるいはパスワードが合っていない場合、後述する論理演算時に考慮したいように設定する（ステップＳ３８）。

【００４４】

未処理の検索語があるか否かを判別し（ステップＳ３９）、未処理の検索語がある場合、ステップＳ３２の処理に戻る。一方、未処理の検索語がない場合、指定された論理演算で個々の検索語に対する全文検索結果を演算する（ステップＳ４０）。但し、アクセス制限文字列、パスワード指定ミスの部分の演算は無効として処理される。

【００４５】

該当する文書が存在するか否かを判別し（ステップＳ４１）、該当する文書が存在しない場合、ヒットしなかった旨を返す（ステップＳ４２）。一方、該当する文書が存在する場合、今回検索語に出てきたアクセス制限文字列でパスワードが合っているものの検索結果同士の論理和をとる（ステップＳ４３）。今回検索語に出てこなかったアクセス制限文字列および今回検索語に出てきたがパスワードがあっていなかったアクセス制限文字列の検索結果同士の論理和をとる（ステップＳ４４）。

【００４６】

ステップＳ４３およびステップＳ４４の処理結果の論理積をとる（ステップＳ４５）。ステップＳ４１およびステップＳ４４の処理結果の論理積をとる（ステップＳ４６）。ステップＳ４５およびステップＳ４６の処理結果の論理和をとる（ステップＳ４７）。ステップＳ４３およびステップＳ４４の処理結果の論理積をとる（ステップＳ４８）。

【００４７】

ステップＳ４７の処理結果にステップＳ４８の処理結果を加えたヒット件数を返すが、ス

テップＳ４８の処理結果についてはそのヒット件数に「アクセス制限文書」という文言を付加して返し、ステップＳ４７の処理結果についてはそのヒット件数にタイトル等の属性を付加して返す（ステップＳ４９）。

【００４８】

図１１は検索結果から使用者が文書・文書イメージデータを参照する場合の処理手順を示すフローチャートである。まず、クライアント端末１２から文書・文書イメージデータのうち参照したいものを指示する（ステップＳ５１）。他にアクセス制限文字列を含んでいるか否かを判別する（ステップＳ５２）。他にアクセス制限文字列を含んでいない場合、指示された文書・文書イメージデータを送信する（ステップＳ５３）。

【００４９】

一方、ステップＳ５２で他にアクセス制限文字列を含んでいる場合、含まれるアクセス制限文字列を提示し、そのパスワードを入力させる（ステップＳ５４、図８参照）。入力されたパスワードが一致するか否かを判別し（ステップＳ５５）、一致する場合、他にアクセス制限文字列があるか否かを判別する（ステップＳ５６）。他にアクセス制限文字列がある場合、ステップＳ５４に戻り、他にアクセス制限文字列がない場合、ステップＳ５３に移行する。

【００５０】

一方、ステップＳ５５で入力されたパスワードが一致しない場合、データ開示を拒否する旨を通知する（ステップＳ５７）。

【００５１】

検索処理結果は大きく分けて２通りある。その１つはアクセス制限文字列でない検索語でヒットしたもの、およびアクセス制限文字列を検索語に選んで正しいパスワードを与えたものでその文書内に他のアクセス制限文字列を含んでいない場合である。もう１つはアクセス制限文字を検索語に選んで正しいパスワードを与えたものでその文書内に他のアクセス制限文字列を含んでいる場合である。

【００５２】

文書・文書イメージデータを参照する際、前者の場合にはヒットした文書データを一括で送信してもよいが、後者の場合には後述するように個別にアクセス制限文字列とパスワードを聞いて条件を満たしてから参照させることとなる。前者の場合、ヒット数、文書タイトルなどの属性情報を、後者の場合、提示しても差し支えない属性情報だけを通知する。また、クライアント端末１２のアプリケーションの要求に応じて必要なデータだけを送信してもよい。

【００５３】

また、後者の場合、他のアクセス制限文字列を複数含む文書に対しては質問ダイアログが提示される。図８はアクセス制限文字列を複数含むヒット文書に対しパスワードを入力する画面を示す図である。順次アクセス制限文字列を提示し、全ての正しいパスワードが入力された場合に参照可能とするが、途中でパスワードの指定を誤った場合、その時点で参照不可能となる。

【００５４】

尚、全文検索サービスサーバ７がクライアント端末１２から指定された検索語をシソーラス（同義語・類義語）に展開する機能を有する場合、アクセス制限文字列がシソーラス展開結果に含まれていないかをチェックし、存在した場合、このアクセス制限文字列と一致したシソーラスを無効にする処理を行う。

【００５５】

また、本実施の形態では文書イメージデータに含まれる文字列イメージに対してアクセス制限を加えるものであるが、文字列イメージでなく、その内容・機密度を表すキーワード・記号列・暗号に対して文字列によりアクセス制限を加えるようにしてもよい。また、使用者がインターネットブラウザを使用し、ホームページ上で処理を行う形での運用も可能である。

【００５６】

さらに、上記実施の形態では、ＬＡＮ３から各種データへの直接アクセスを防ぐためにファイアウォール９を全文検索サービスサーバ７およびデータサーバ５間に設けているが、ファイアウォール９を他の位置に設けてもよい。図１２は他の文書セキュリティ管理システムの構成を示すブロック図である。この文書セキュリティ管理システムはＬＡＮ５３に直にファイアウォール５９が接続され、その後に全文検索サービスサーバ５７、データサーバ５５が設けられている。ＬＡＮ５３に近い側から全文検索サービスサーバ５７、データサーバ５５が直列に接続されていればよく、この場合、ファイアウォール５９を通過できるＬＡＮ５３上のクライアント端末６２は制限を受けることになる。セキュリティ上、図１に示した構成の方が好ましいが、アクセスできるクライアント端末が制限を受ける分、図１２に示した構成の方が運用に柔軟性がある。

【００５７】

またさらに、データサーバが全文検索サービスサーバからのパケットであるか否かを同定し、全文検索サービスサーバからのパケットでない場合、内部ファイルを参照できなくする機能を有しているときには、必ずしもファイアウォールを設ける必要がない。

【００５８】

また、近年、繁栄を続けているインターネットやイントラネットなどのネットワークを介したデータ共有管理システムに適用することで、単純なアクセス権によるセキュリティでなく蓄積した文書に含まれる文字列によってセキュリティを確保することができる。

【００５９】

さらに、ネットワークを介さないスタンドアローン型のデータ管理システムでも文書に含まれる文字列によりアクセスを制限する概念は利用可能である。

以上示したように、上記実施形態によれば、文書データを効率よく共有しつつ、機密文書のアクセス権範囲を柔軟に対応することができる。また、機密性が無くなり公に開示する際の運用を柔軟に対応することができる。

さらに、データサーバが全文検索サービスサーバからのパケットであるか否かを同定し、全文検索サービスサーバからのパケットでない場合、内部ファイルを参照できなくする機能を有していない場合など、クライアント端末からデータサーバに直接アクセスすることを防ぐことができ、文書セキュリティを向上できる。

また、機密性を高めることができる。さらに、登録要求者のＩＰアドレスの管理を容易に行うことができ、アクセス制限文字列およびそのパスワードを削除する際の確認を簡単に行うことができる。

また、誤って機密文書が公に開示されてしまうおそれを無くすことができる。さらに、操作性を向上することができる。また、テキストデータと同様の処理をイメージデータに対して行うことができる。

さらに、機密文書でない場合、検索結果に対する多くの情報を使用者に通知することができる。また、ファイアウォールを通過できるネットワーク上のクライアント端末は制限を受けることになり、アクセスできるクライアント端末が制限を受ける分、運用の柔軟性を高めることができる。

【００６０】

【発明の効果】

本発明によれば、文書データを効率よく共有しつつ、機密文書のアクセス権範囲を柔軟に対応することができる。また、機密性が無くなり公に開示する際の運用を柔軟に対応することができる。

【図面の簡単な説明】

【図１】実施の形態における文書セキュリティ管理システムの構成を示すブロック図である。

【図２】データサーバ５に管理されているデータの構成を示す図である。

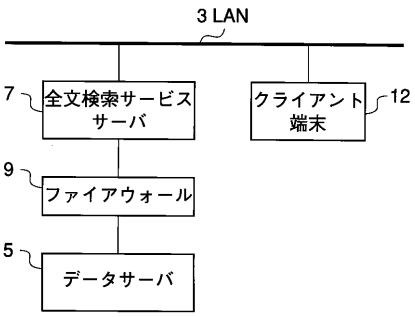
【図３】アクセス制限文字列の登録処理手順を示すフローチャートである。

【図４】アクセス制限文字列管理情報テーブルを示す図である。

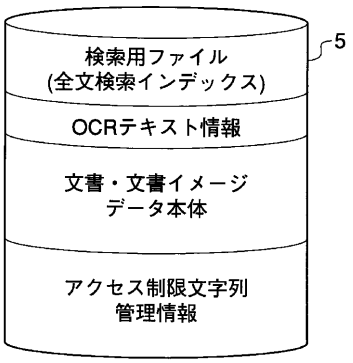
【図５】アクセス制限文字列の解除処理手順を示すフローチャートである。

【図６】文書・文書イメージデータの登録処理手順を示すフローチャートである。
【図７】検索時の検索条件入力画面を示す図である。
【図８】アクセス制限文字列を複数含むヒット文書に対しパスワードを入力する画面を示す図である。
【図９】文書・文書イメージデータの検索処理手順を示すフローチャートである。
【図１０】図９につづく文書・文書イメージデータの検索処理手順を示すフローチャートである。
【図１１】検索結果から使用者が文書・文書イメージデータを参照する場合の処理手順を示すフローチャートである。
【図１２】他の文書セキュリティ管理システムの構成を示すブロック図である。
【符号の説明】
１　文書セキュリティ管理システム
５　データサーバ
７　全文検索サービスサーバ
９　ファイアウォール
１２　クライアント端末

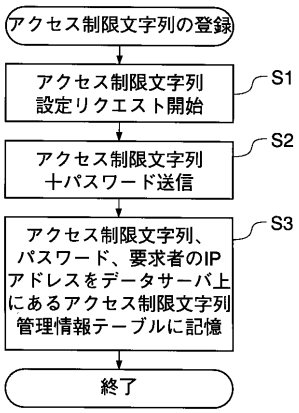
【図１】



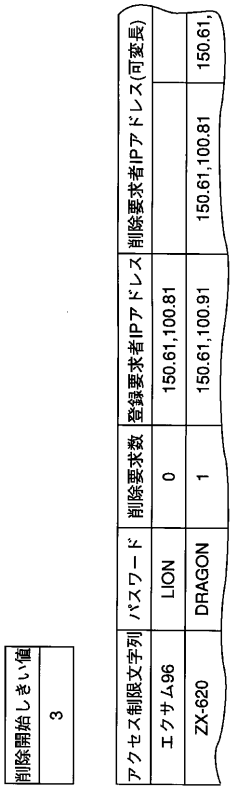
【図２】



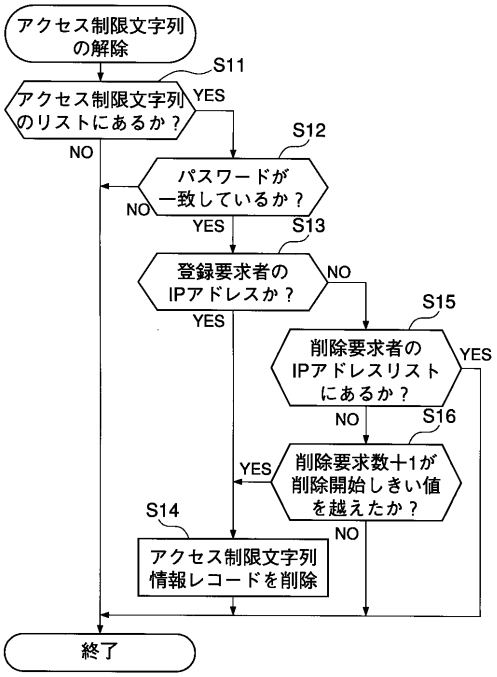
【図３】



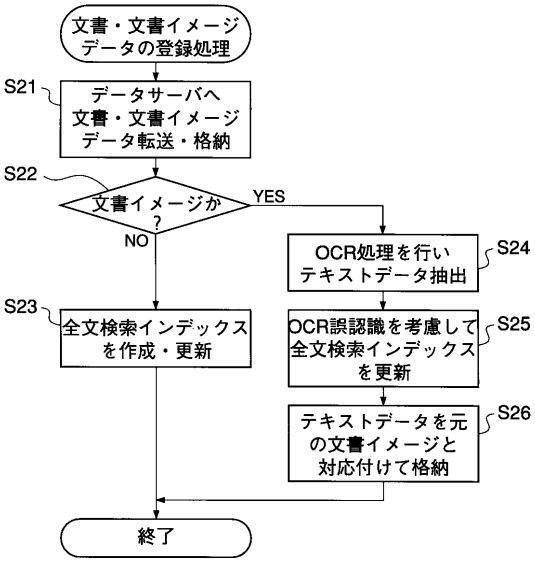
【図４】


削除開始しきい値
3
アクセス制限文字列
エクサム96
ZX-620
パスワード
LION
DRAGON
削除要求数
0
1
登録要求者IPアドレス
150.61,100.81
150.61,100.91
削除要求者IPアドレス(可変長)
150.61,100.81
150.61,

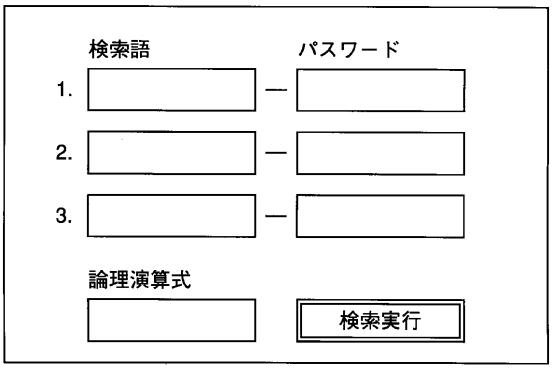
【図５】


アクセス制限文字列の解除
S11
アクセス制限文字列のリストにあるか？
YES
NO
S12
パスワードが一致しているか？
NO
YES
S13
登録要求者のIPアドレスか？
NO
YES
S15
削除要求者のIPアドレスリストにあるか？
YES
NO
S16
削除要求数＋1が削除開始しきい値を越えたか？
YES
NO
S14
アクセス制限文字列情報レコードを削除
終了

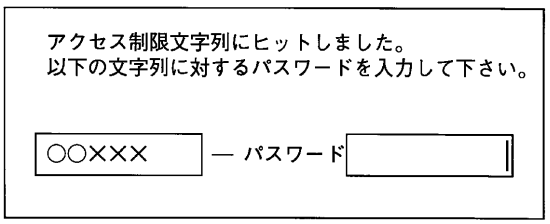
【図６】


文書・文書イメージデータの登録処理
S21
データサーバへ文書・文書イメージデータ転送・格納
S22
文書イメージか？
YES
NO
S23
全文検索インデックスを作成・更新
S24
OCR処理を行いテキストデータ抽出
S25
OCR誤認識を考慮して全文検索インデックスを更新
S26
テキストデータを元の文書イメージと対応付けて格納
終了

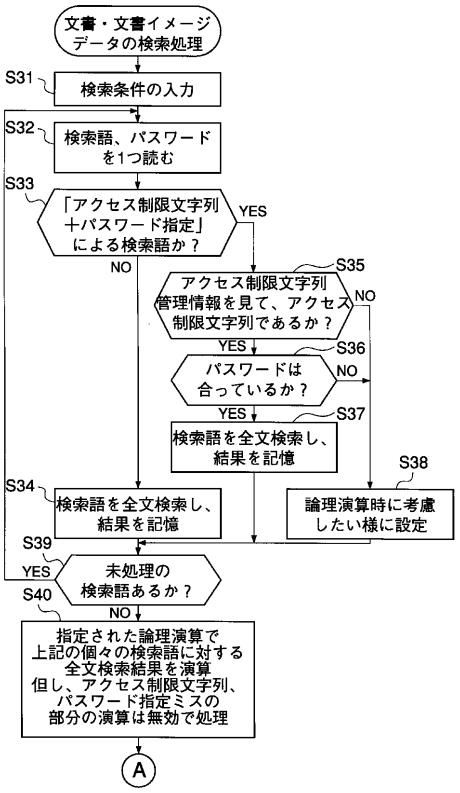
【図７】


検索語
パスワード
1.
2.
3.
論理演算式
検索実行

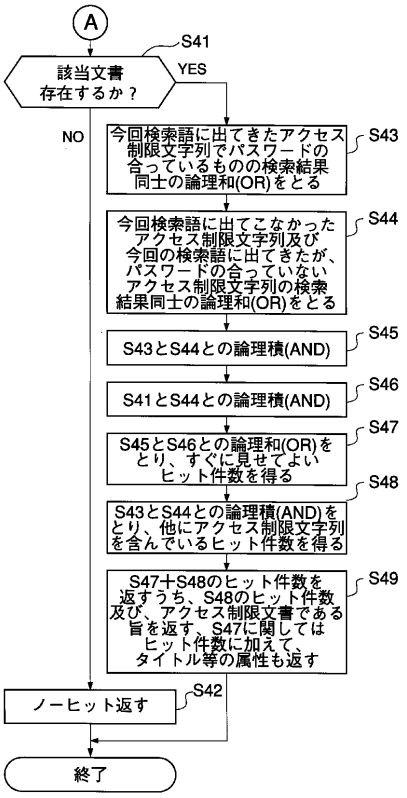
【図８】


アクセス制限文字列にヒットしました。
以下の文字列に対するパスワードを入力して下さい。
○○×××
パスワード

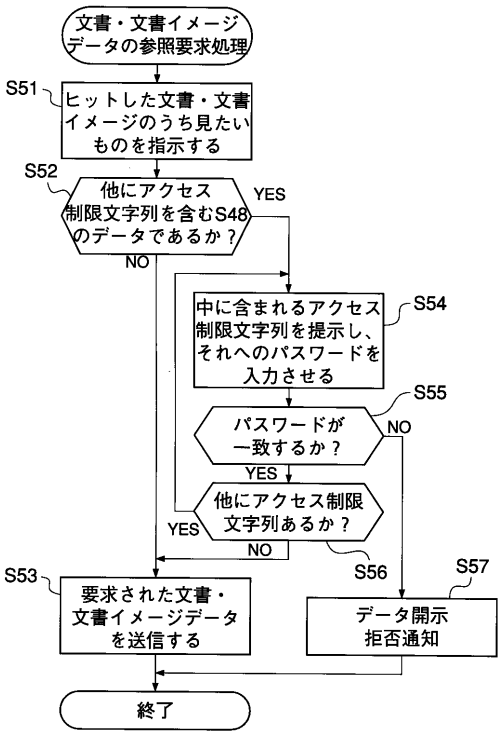
【図９】



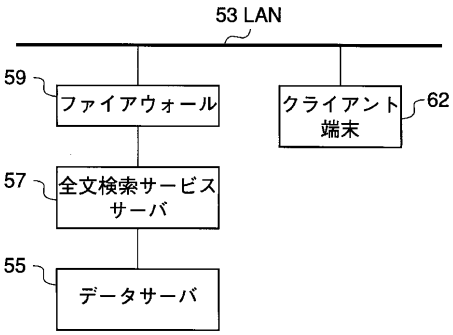
【図１０】



【図１１】



【図１２】



フロントページの続き

(51)Int.Cl.[7] FI
G06F 17/30 １２０Ｂ
G06F 17/30 １７０Ａ

(56)参考文献 特開平０５－００２６０９（ＪＰ，Ａ）
特開平０６－０３５９７０（ＪＰ，Ａ）
特開昭５７－１３０１７７（ＪＰ，Ａ）
特開昭６２－０２６５５５（ＪＰ，Ａ）
特開昭６２－１５０４４９（ＪＰ，Ａ）
特開平０２－２９７１８７（ＪＰ，Ａ）
特開平０７－２９６０００（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.[7]，ＤＢ名)
G06F 12/14
G06F 12/00 537
G06F 17/30