(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2011-138340
(P2011-138340A)
(43)公開日　平成23年7月14日(2011.7.14)

(51)Int.Cl.	F I	テーマコード（参考）
G06F 3/12 (2006.01)	G06F 3/12 K	

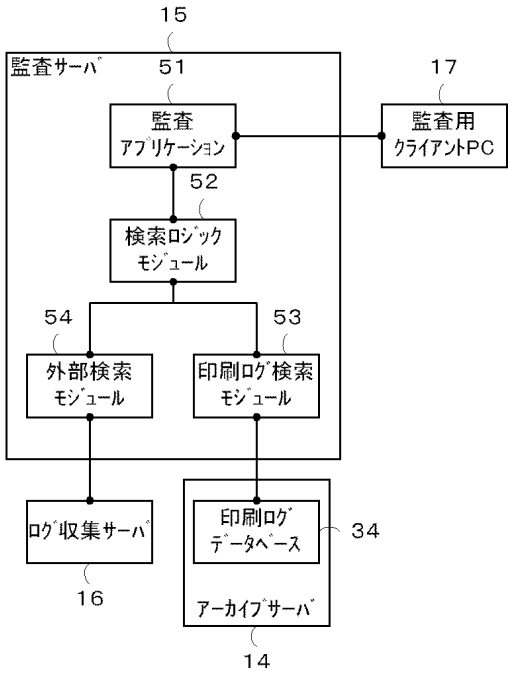
審査請求 未請求　請求項の数 7　ＯＬ　（全 14 頁）

(21)出願番号　特願2009-298348 (P2009-298348)
(22)出願日　平成21年12月28日 (2009.12.28)

(71)出願人　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　100145827
弁理士　水垣　親房
(72)発明者　松ヶ下　勇人
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

(54)【発明の名称】サーバ装置、サーバ装置のログ監査方法およびプログラム

(57)【要約】
【課題】　蓄積された印刷ログの中から不正処理された印刷ログを優先して表示する。
【解決手段】
監査サーバ１５は、監査用クライアントＰＣ１７から印刷ログデータベース３４に蓄積された印刷ログに対する検索条件と、検索条件に従い検索された印刷ジョブのログに対して、ログ管理サーバで管理されるログに紐付ける関連ログ設定とを受け付ける。そして、監査サーバ１５は、検索要求に対する検索結果をアーカイブサーバ１４から取得し、さらに、関連ログ設定に応じた関連ログ検索要求に対するヒット件数をログ収集サーバ１６から取得する。そして、監査サーバ１５は取得した検索結果と取得したヒット件数とに応じて、検索結果に含まれる印刷ログの表示態様を制御する。
【選択図】　図５



【特許請求の範囲】
【請求項１】
印刷装置で処理された印刷ジョブのログを蓄積して管理する印刷ログ管理サーバおよびクライアント装置にログインするユーザのログを収集して管理するログ管理サーバと通信するサーバ装置であって、
蓄積された前記印刷ジョブのログに対する検索条件、および前記検索条件に従い検索される印刷ジョブのログに対して、前記ログ管理サーバで管理されるログに紐付ける関連ログ設定とを前記クライアント装置から受け付ける受付手段と、
前記受付手段により受け付けられた検索条件に応じた検索要求を前記印刷ログ管理サーバに出力し、当該検索要求に対する検索結果を前記印刷ログ管理サーバから取得する印刷ログ検索結果取得手段と、
前記受付手段により受け付けられた関連ログ設定に応じた関連ログ検索要求を前記ログ管理サーバに出力し、当該関連ログ検索要求に対するヒット件数を前記ログ管理サーバから取得するログ検索結果取得手段と、
前記印刷ログ検索結果取得手段が取得した検索結果と前記ログ検索結果取得手段が取得したヒット件数とに応じて、前記検索結果に含まれる印刷ログの表示態様を制御する制御手段と、
を備えることを特徴とするサーバ装置。
【請求項２】
前記制御手段は、ヒット件数が少ない印刷ログを優先して表示することを特徴とする請求項１記載のサーバ装置。
【請求項３】
前記受付手段は、前記ログ管理サーバで管理されるログに紐付ける関連ログ設定とともに、ログ検索に際して、前記関連ログ設定よりも優先すべき検索項目を受け付け可能であることを特徴とする請求項１記載のサーバ装置。
【請求項４】
前記受付手段は、前記ログ管理サーバで管理されるログに紐付ける関連ログ設定として、ユーザ名、マシン名、アドレス、ドキュメント名、日時のいずれかまたはこれらの組み合わせを受け付け可能であることを特徴とする請求項１または３のいずれか１項に記載のサーバ装置。
【請求項５】
前記関連ログ設定よりも優先すべき検索項目は、ドメインの認証ログであることを特徴とする請求項３記載のサーバ装置。
【請求項６】
印刷装置で処理された印刷ジョブのログを蓄積して管理する印刷ログ管理サーバおよびクライアント装置にログインするユーザのログを収集して管理するログ管理サーバと通信するサーバ装置のログ監査方法であって、
蓄積された前記印刷ジョブのログに対する検索条件、および前記検索条件に従い検索される印刷ジョブのログに対して、前記ログ管理サーバで管理されるログに紐付ける関連ログ設定とを前記クライアント装置から受け付ける受付工程と、
前記受付工程により受け付けられた検索条件に応じた検索要求を前記印刷ログ管理サーバに出力し、当該検索要求に対する検索結果を前記印刷ログ管理サーバから取得する印刷ログ検索結果取得工程と、
前記受付工程により受け付けられた関連ログ設定に応じた関連ログ検索要求を前記ログ管理サーバに出力し、当該関連ログ検索要求に対するヒット件数を前記ログ管理サーバから取得するログ検索結果取得工程と、
前記印刷ログ検索結果取得工程が取得した検索結果と前記ログ検索結果取得工程が取得したヒット件数とに応じて、前記検索結果に含まれる印刷ログの表示態様を制御する制御工程と、
を備えることを特徴とするサーバ装置のログ監査方法。

【請求項７】
請求項６に記載のサーバ装置のログ監査方法をコンピュータに実行させることを特徴とするプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、蓄積された印刷ログを検査するサーバ装置、サーバ装置のログ監査方法およびプログラムに関する。
【背景技術】
【０００２】
プリンタやMFPなどの画像処理装置において、顧客情報や設計資料といった機密文書が不正に印刷され、情報漏洩が生じることがある。
従来、それら情報漏洩の発生源の特定や漏洩経路の追跡といった監査のために、印刷した証跡として印刷ログを保管するシステムが知られている。
例えば、特許文献１では、印刷データと共に、日時、ジョブ名、ユーザ名、画像の特徴量などの情報を印刷ログとして保存し、それら条件をキーに検索することで不正な印刷を監査することが提案されている。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開２００７－２８０３６２号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
前述の方法では、不正な印刷のログだけでなく正当な印刷のログも蓄積されるため、日々の印刷ボリュームが多い状況下では印刷ログの量が膨大になる。そのため、監査するうえで印刷ログに保存されている情報だけでは不正な印刷を特定するのが大変困難な場合がある。
【０００５】
本発明は、上記の課題を解決するためになされたもので、本発明の目的は、蓄積された印刷ログの中から不正処理された印刷ログを優先して表示できる仕組みを提供することである。
【課題を解決するための手段】
【０００６】
上記目的を達成する本発明のサーバ装置は以下に示す構成を備える。
印刷装置で処理された印刷ジョブのログを蓄積して管理する印刷ログ管理サーバおよびクライアント装置にログインするユーザのログを収集して管理するログ管理サーバと通信するサーバ装置であって、蓄積された前記印刷ジョブのログに対する検索条件、および前記検索条件に従い検索された印刷ジョブのログに対して、前記ログ管理サーバで管理されるログに紐付ける関連ログ設定とを前記クライアント装置から受け付ける受付手段と、前記受付手段により受け付けられた検索条件に応じた検索要求を前記印刷ログ管理サーバに出力し、当該検索要求に対する検索結果を前記印刷ログ管理サーバから取得する印刷ログ検索結果取得手段と、前記受付手段により受け付けられた関連ログ設定に応じた関連ログ検索要求を前記ログ管理サーバに出力し、当該関連ログ検索要求に対するヒット件数を前記ログ管理サーバから取得するログ検索結果取得手段と、前記印刷ログ検索結果取得手段が取得した検索結果と前記ログ検索結果取得手段が取得したヒット件数とに応じて、前記検索結果に含まれる印刷ログの表示態様を制御する制御手段とを備えることを特徴とする。
【発明の効果】
【０００７】

本発明によれば、印刷ログだけでなく、合わせてコンピュータの操作が記録されている証跡を関連付けて監査することで、不正な印刷をより高い精度で特定することが可能になる。

【図面の簡単な説明】

【０００８】

【図１】データ処理システムの構成を示すブロック図である。

【図２】データ処理システムのハードウエア構成を説明する図である。

【図３】データ処理システムのソフトウェアモジュールの構成図である。

【図４】データ処理システムの他のソフトウェアモジュールの構成図である。

【図５】監査サーバ上で動作するソフトウェアモジュール構成図である。

【図６】印刷ログのデータ構造を示す図である。

【図７】ログ収集サーバで保存されるログのデータ構造を示す図である。

【図８】監査アプリケーションにて構成される監査ＵＩを示す図である。

【図９】サーバ装置のデータ処理手順を示すフローチャートである。

【図１０】監査ＵＩによる検索結果表示例を示す図である。

【発明を実施するための形態】

【０００９】

次に本発明を実施するための最良の形態について図面を参照して説明する。

〔第１実施形態〕

図１は、本発明の実施形態を示すデータ処理システムの構成を示すブロック図である。

図１において、１０は各構成要素を接続するネットワークである。１１はプリンタ（印刷装置）で、印刷データを出力する。１２はプリントサーバで、プリンタ１１を含む図示しない各種のプリンタと通信して印刷指示を行う。１３はクライアント装置（クライアント）で、ユーザの操作によりアプリケーションから印刷指示をプリントサーバ１２に対して出力する。

また、１４は印刷ログ管理サーバとして機能するアーカイブサーバで、印刷ログを蓄積して管理する。１５は監査サーバで、アーカイブサーバ１４に蓄積された印刷ログを検索する。１６はログ管理サーバとして機能するログ収集サーバで、各クライアント１３にて行われる各ユーザの操作ログを収集して管理する。１７は監査用クライアントで、監査サーバ１５にアクセスし、印刷ログを監査する。監査用クライアント１７は、Ｗｅｂブラウザ機能を備え、監査サーバ１５が提供する監査ＵＩを表示可能に構成されている。後述スル図８に示す監査ＵＩでは、当該監査ＵＩに介して設定された印刷ログの検索条件や、ログ収集サーバ１６が管理するログに紐付ける関連ログ設定を行えるように構成され、設定された内容が監査サーバ１５に受付られる。

【００１０】

また、上記各構成要素はネットワーク１０により通信可能に接続されており、通信手段としては、ＨＴＴＰや、ＨＴＴＰ上のＳＯＡＰ、つまりＷｅｂサービスが用いられる他、ＴＣＰ／ＩＰによる相互通信を用いて行われる。

なお、プリントサーバ１２には対象となるプリンタ１１用のプリンタドライバおよび印刷ログを取得するためのＡｄｄ－ｉｎモジュールがインストールされている。また、ポイント・アンド・プリント機能によりクライアント１３にも同等のプリンタドライバおよびＡｄｄ－ｉｎモジュールがインストールされている。

【００１１】

印刷時には印刷データがクライアント１３からプリントサーバ１２を経由してプリンタ１１に送られて印刷処理が実行される。

なお、クライアント１３にはプリンタ１１用のドライバ、印刷ログを取得するためのＡｄｄ－ｉｎモジュールをインストールし、クライアント１３から直接プリンタ１１へ印刷することも可能に構成されている。

図２は、図１に示したプリントサーバ１２、クライアント１３、アーカイブサーバ１４、監査サーバ１５、ログ収集サーバ１６、あるいは監査用のハードウエア構成を示すブロ

ック図である。
図２において、２１はＣＰＵで、内部バスで接続される各デバイス（後述のＲＯＭ、ＲＡＭ他）を直接或いは間接的に制御し、本発明を実現するためのプログラムを実行する。２２はＲＯＭで、ＢＩＯＳが格納されている。２３はＲＡＭ（直接記憶装置）で、ＣＰＵ２１のワーク領域として利用されたり、本発明を実現するためのソフトウェアモジュールをロードするための一時記憶として利用されたりする。
【００１２】
２４はＨＤＤ（ハードディスクドライブ）で、基本ソフトウェアであるＯＳ（オペレーティングシステム）やソフトウェアモジュールが記憶されている。なお、ＨＤＤ２４に代えて、ＳＳＤ（ソリッドステートドライブ）などで構成されていてもよい。
２５は入力装置であり、不図示のキーボードやポインティングデバイスなどで構成されている。２６は出力装置であり、ディスプレイが接続される。２７はネットワーク１０に接続するためのＩ／Ｆである。
これらハードウエアでは、起動後ＣＰＵ２１によりＢＩＯＳが実行されＯＳがＨＤＤ２４からＲＡＭ２３に実行可能にロードされる。ＣＰＵ２１はＯＳの動作に従って後述する各種ソフトウェアモジュールをＨＤＤ２４からＲＡＭ２３に随時、実行可能にロードする。各種ソフトウェアモジュールは上記各デバイスの協調によりＣＰＵ２１によって実行され動作する。
【００１３】
図３は、図１に示したデータ処理システムのソフトウェアモジュールの構成図である。以下、図１に示したクライアント１３、プリントサーバ１２およびアーカイブサーバ１４上で動作するソフトウェアモジュールの構成について説明する。
なお、各ソフトウェアモジュールは、図２で示したＨＤＤ２４に記憶されており、前述したようにＣＰＵ２１によってＲＡＭ２３にロードされて実行される。
クライアント１３、プリントサーバ１２にはプリンタ１１用のプリンタドライバ３０と印刷ログ取得のためのＡｄｄ－ｉｎモジュール３１を備える。またプリントサーバ１２および、印刷経路によってはクライアント１３においても、Ａｄｄ－ｉｎモジュール３１から渡された印刷ログをアーカイブサーバ１４に送信するためのドライバエージェント３２を備える。
【００１４】
アーカイブサーバ１４は、ドライバエージェント３２から送信される印刷ログを受信し、印刷ログデータベース３４に蓄積するためのアーカイブサービス３３が動作している。また、印刷ログデータベース３４はアーカイブサーバ１４内にソフトウェアモジュールとして構成してもよいし、ネットワーク１０により通信可能に接続されたハードウエアとして構成してもよい。
印刷ログデータベース３４は、ＳＱＬと呼ばれる問い合わせ言語を解するリレーショナルデータベースが一般的に利用され、アーカイブサービス３３はＳＱＬ文を印刷ログデータベース３４に対して発行することで印刷ログを登録する。
【００１５】
図４は、図１に示したログ収集サーバ１６、およびクライアント１３上で動作するソフトウェアモジュール構成図である。
なお、各ソフトウェアモジュールは、図２で示したＨＤＤ２４に記憶されており、前述したようにＣＰＵ２１によってＲＡＭ２３にロードされ実行される。
ログ収集サーバ１６には、ネットワーク１０にて通信可能に接続されているクライアント１３から所定のログを定期的に収集する収集モジュール４１を備えている。
また、ログを登録するためのＩ／Ｆである登録Ｉ／Ｆ４２を備えており、前記収集モジュール４１や、後述するクライアント１３のログエージェント４７からのログ登録の要求を受け付ける。登録Ｉ／Ｆ４２で受け付けた各種ログは登録ロジックモジュール４３を介して所定のフォーマットに変換され、ログデータベース４４に検索可能に登録される。
【００１６】

上記収集モジュール４１は、クライアント１３にて実行されているＯＳが備えるログ収集用のインタフェースを介してＯＳが記録するログを収集したり、もしくは既定の箇所に保存されているログファイルをＯＳが備えるファイルアクセスインタフェースを介して収集したりする。

【００１７】

ここで、収集モジュール４１は、クライアント１３だけでなく、ネットワーク１０に接続された不図示の他の汎用ＰＣやワークステーション、サーバなどからも同様にログを収集可能である。

ログデータベース４４は、ログ収集サーバ１６内にソフトウェアモジュールとして構成してもよいし、ネットワーク１０により通信可能に接続されたハードウエアに構成されてもよい。

ログデータベース４４は、ＳＱＬと呼ばれる問い合わせ言語を解するリレーショナルデータベースが一般的に利用され、登録ロジックモジュール４３はＳＱＬ文をログデータベース４４に対して発行することでログを登録する。

また、登録Ｉ／Ｆ４２はＳＯＡＰメッセージをＨＴＴＰにて送信する所謂ＷｅｂＳｅｒｖｉｃｅとして備えてもよいし、ＳｙｓＬｏｇプロトコルを備えてもよい。

【００１８】

また、ログ収集サーバ１６にはログデータベース４４に登録されているログを所定の条件で検索するための検索ロジックモジュール４５を備える。またログの検索は検索Ｉ／Ｆ４６を介してネットワーク１０に接続される各ハードウエアから実行可能に構成される。

検索Ｉ／Ｆ４６は、ＳＯＡＰメッセージをＨＴＴＰにて送信する所謂ＷｅｂＳｅｒｖｉｃｅとして備えてもよいし、ＳＱＬコマンドを受け付けるよう構成されてもよい。検索Ｉ／Ｆ４６で受け付けた検索条件を検索ロジックにてログデータベース４４が解する言語（たとえばＳＱＬ）に変換して発行することで検索を実行する。

【００１９】

クライアント１３は、ログエージェント４７を備えることができる。ログエージェント４７は、クライアント１３上で動作するＯＳを監視し所定の条件にてログを生成する。ログエージェント４７は、例えばＯＳのファイルシステムへのアクセス時や、ネットワーク通信時にログを生成する。

【００２０】

ログエージェント４７は、ネットワーク１０を介して生成されたログを前述したログ収集サーバ１６の登録Ｉ／Ｆ４２に対して定期的に送信する。また、ログエージェント４７は、既定の箇所に生成されるログを定期的に送信するよう構成することもできる。ここでログエージェント４７は、クライアント１３だけでなく、ネットワーク１０に接続された不図示の他の汎用ＰＣやワークステーション、サーバなどでも同様に構成可能である。

【００２１】

図５は、図１に示した監査サーバ１５上で動作するソフトウェアモジュール構成を説明する図である。

なお、以下に示す各ソフトウェアモジュールは、図２で示した監査サーバ１５のＨＤＤ２４に記憶されており、前述したようにＣＰＵ２１によってＲＡＭ２３にロードされ実行される。

監査サーバ１５は、監査アプリケーション５１を備えている。監査アプリケーション５１は、いわゆるＷｅｂアプリケーションとして構成されており、監査用クライアント１７はＷｅｂブラウザを用いてアクセスする。

なお、Ｗｅｂアプリケーションとしての構成は一例であり、ＵＩを備えたローカルアプリケーションとしての構成も可能である。その場合は、監査は監査サーバ１５上で実行される。

【００２２】

また、監査サーバ１５は、監査アプリケーション５１にて設定された検索条件を解釈し、検索を順次実行する検索ロジックモジュール５２、および前述の印刷ログデータベース

３４に検索を実行する印刷ログ検索モジュール５３、および前述のログ収集サーバ１６に検索を実行する外部検索モジュール５４を備える。ここで、印刷ログ検索モジュール５３は、アーカイブサーバ１４から印刷ログの検索結果を取得する印刷ログ検索結果取得処理を行う。

【００２３】

また、外部検索モジュール５４は、ネットワーク１０を介して接続するログ収集サーバ１６の検索Ｉ／Ｆ４６に対応したソフトウェアモジュールを追加アダプターとして追加することができる。なお、検索条件に対応する検索ロジックモジュール５２の動作の詳細については後述する。ここで、外部検索モジュール５４は、ログ収集サーバ１６からログ検索結果を取得するログ検索結果取得処理を行う。

【００２４】

図６は、図５に示した印刷ログデータベース３４で管理される印刷ログのデータ構造を示す図である。

図６において、印刷ログ６０はユーザ名６１、ドメイン名６２、コンピュータ名６３、ＩＰアドレス６４、ＭＡＣアドレス６５、ドキュメント名６６、印刷開始日時６７、テキスト情報６８、画像特徴量６９からなる。

ユーザ名６１は、印刷を実行したユーザ名であり、クライアント１３にログインしたユーザを特定する情報が記録される。ドメイン名６２は、クライアント１３にログインする際にログイン先となるドメインを特定する情報が記録される。

【００２５】

コンピュータ名６３、ＩＰアドレス６４、ＭＡＣアドレス６５は印刷を実行したクライアント１３の情報が記録される。ドキュメント名６６は、印刷したドキュメントのファイル名が記録される。

印刷開始日時６７は、クライアント１３にてユーザが印刷を行った開始日時が記録される。テキスト情報６８はアーカイブサーバ１４にて収集した印刷ログの画像データに含まれるテキスト情報が格納される。ここで、テキスト情報は、Ａｄｄ－ｉｎモジュール３１にて抽出されるか、もしくはアーカイブサービス３３にて画像データをＯＣＲ処理して抽出される。

【００２６】

これら処理は、各ソフトウェアモジュールが図２で示したＨＤＤ２４に記憶され、ＣＰＵ２１によってＲＡＭ２３にロードされ実行される。

画像特徴量６９は、アーカイブサーバ１４にて収集した印刷ログの画像データから計算される画像の特徴を示す数値であり、アーカイブサービス３３に備えた計算式をもってアーカイブサーバ１４のＣＰＵ２１によって計算される。

【００２７】

図７は、図１に示したログ収集サーバ１６で保存されるログのデータ構造を示す図である。

図７において、ログ７０は、ログの種類を特定するためのログ種別７１、ユーザ名７２、ドメイン名７３、コンピュータ名７４、ＩＰアドレス７５、ＭＡＣアドレス７６、記録日時７７等からなる。

ログ種別７１は"ログイン"、"プリント"といった文字列情報でもよいし、また、それらに対応したＩＤとしてマッピングした情報でもよい。ユーザ名７２は、ログに記録される操作を実行したユーザ名であり、クライアント１３にログインしたユーザを特定する情報が記録される。

【００２８】

ドメイン名７３はクライアント１３にログインする際にログイン先となるドメインを特定する情報が記録される。コンピュータ名７４、ＩＰアドレス７５、ＭＡＣアドレス７６はログに記録される操作が実行されたクライアント１３の情報が記録される。記録日時７７はクライアント１３にてログが記録された日時である。

【００２９】

図８は、図１に示した監査用クライアント１７のＷｅｂブラウザ上に表示される、監査サーバ１５の監査アプリケーション５１にて構成される監査ＵＩ８０の一例を示す図である。監査ＵＩ８０は、監査用クライアント１７から印刷ジョブのログに対する検索条件と、当該検索条件に従い検索される印刷ジョブのログに対して紐付ける関連ログ設定とを監査サーバ１５が受け付ける際に監査用クライアント１７で表示される。

図８において、監査ＵＩ８０は大きく画面左の検索条件ペイン８１０と画面右の検索結果ペイン８２０に分かれる。

検索条件ペイン８１０は、検索実行ボタン８１１、類似画像検索ペイン８１２、全文検索ペイン８１３、属性検索ペイン８１４、関連ログ設定ペイン８１５、および必須ログ設定ペイン８１６に分かれる。

類似画像検索ペイン８１２では、比較する画像を選択し、その画像による類似画像検索条件が設定できる。類似画像検索条件は、選択した画像の画像特徴量と保存されている印刷ログの画像特徴量の比較によって、類似する印刷ログを抽出する条件である。

全文検索ペイン８１３では、比較するテキストを入力し、そのテキストによる全文検索条件が設定できる。

全文検索条件は、比較するテキストと保存されている印刷ログのテキスト情報の比較によって印刷ログを抽出する条件である。全文検索条件には、すべての語句を含むＡＮＤ条件、どれかの語句を含むＯＲ条件、語句を含まないＮＯＴ条件を組み合わせて指定することが可能である。

【００３０】

属性検索ペイン８１４では、比較する各属性値を入力し、その属性値による属性検索条件が設定できる。属性検索条件は、設定した各属性値と対応する印刷ログの属性値の比較により印刷ログを抽出する条件である。

属性としては、ユーザ名、ドメイン名、コンピュータ名、ＩＰアドレス、ＭＡＣアドレス、ドキュメント名および印刷時間帯が指定可能である。図示の監査ＵＩ８０では、ユーザ名、アドレス、印刷時間帯のみを例示している。

【００３１】

各属性値は、すべての条件が合致するＡＮＤ条件、どれかの条件が合致するＯＲ条件、条件が合致しないＮＯＴ条件を組み合わせて指定することが可能である。図示の属性に条件を入力した場合はすべての条件のＡＮＤ条件として設定される。

その他の属性設定や組み合わせの設定は図示詳細設定ボタンを押下することで表示される詳細設定画面（不図示）により行うことができる。なお印刷時間帯は"年月日（時分）"から"年月日（時分）"までの範囲指定が可能であり、その範囲に印刷ログの印刷開始日時が含まれる印刷ログが抽出される。

【００３２】

各検索ペインに条件を設定後、検索ボタンを押下すると、類似画像検索条件、全文検索条件、属性検索条件は各条件のすべてをＡＮＤ条件として印刷ログの抽出を行う。この印刷ログの抽出は、監査サーバ１５のＣＰＵ２１によってＲＡＭ２３にロードされている検索ロジックモジュール５２から、印刷ログ検索モジュール５３を介して、印刷ログデータベース３４にて解釈可能な問い合わせ言語に変換され実行される。

【００３３】

関連ログ設定ペイン８１５では、本発明の特徴である、抽出した印刷ログの優先順位付けを行うための設定を行うことができる。より具体的には、抽出された各印刷ログとログ収集サーバ１６に保存されている操作ログを、どの属性によって関連付けるかを設定できる。属性としては、ユーザ名、ドメイン名、マシン名、ＩＰアドレス、ＭＡＣアドレス、および日時（期間）を設定できる。

【００３４】

ここで、ユーザ名、ドメイン名、コンピュータ名、ＩＰアドレス、ＭＡＣアドレスは印刷ログおよびログで説明したものであり、互いが完全一致するログが対象となる。期間は、抽出された印刷ログの印刷開始日時の前後の期間を設定可能であり、その期間に保存さ

れたログが対象となる。関連付けによる優先順位付けの処理についての詳細は後述する。

【００３５】

必須ログ設定ペイン８１６は、関連ログ設定ペイン８１５の設定よりも優先すべき検索項目（必須ログ設定項目）を設定する。本実施形態では、監査アプリケーション５１が、検索項目に応じて順位付けされた印刷ログに対して、さらに優先して強調表示するための設定を行うことができる。ここで、監査アプリケーション５１は、検索した印刷ログの検索結果と、ログ収集サーバ１６から通知されるヒット件数に応じて、印刷ログの表示態様を制御する。また、表示態様として、本実施形態では、以下の強調表示処理を行うものとするが、ユーザが識別可能であれば、いれら以外の表示態様であってもよい。

ここで、設定としては必須ログを設定するか否か、および、図示詳細設定ボタンを押下することで不図示の必須ログ詳細設定画面により詳細設定することができる。詳細設定画面では、必須ログ項目の指定をすることができ、より具体的にはログのログ種別と対応した値を、一つないしは複数個設定することができる。必須ログ項目による強調表示処理についての詳細は後述する。

【００３６】

以下、本発明の特徴である、保存されている印刷ログの監査処理フローについてフローチャートを用いて説明する。なお、本実施形態では、必須ログ設定項目として、ドメインの認証ログを例とするが、他の項目であってもよい。さらに、必須ログ設定項目を設定する場合には、ログ収集サーバ１６に対するクエリ条件にログの種類を絞り込むキーワードを備えているものとする。

監査処理は、上述した監査用クライアント１７のＷｅｂブラウザ上に表示される監査ＵＩ８０の検索条件ペイン８１０に対する押下を、監査サーバ１５の監査アプリケーション５１が受け付けた場合に開始される。

監査用クライアントＰＣ１７に表示された監査ＵＩ８０を介して検索条件ペイン８１０の押下を受けた監査アプリケーション５１は、検索ロジックモジュール５２に対して検索処理を指示する。その際、監査ＵＩ８０に設定されている各検索条件、関連ログ設定、必須ログ設定を引数として渡す。

これら処理は、監査サーバ１５のＣＰＵ２１によってＲＡＭ２３にロードされている監査アプリケーション５１、検索ロジックモジュール５２によって実行される。

【００３７】

図９は、本実施形態を示すサーバ装置におけるデータ処理手順の一例を示すフローチャートである。本例は、図１に示した監査サーバ１５の検索ロジックモジュール５２にて行われる検索処理のフローである。以下、検索した印刷ログのうち、不正な印刷ログを特定して、当該不正な印刷ログを他の印刷ログとの表示態様を変更して強調表示する制御について説明する。

監査サーバ１５の検索ロジックモジュール５２は、監査アプリケーション５１からの検索指示を受け、検索処理を実行し、検索結果を監査アプリケーション５１に返却する。本明細書では、図９のフローチャートで示す手順が、検索ロジックモジュール５２として監査サーバ１５のＲＡＭ２３にロードされＣＰＵ２１により実行される。

【００３８】

Ｓ９０１にて検索ロジックモジュール５２は、監査アプリケーション５１より検索指示を受付る。このとき、例えば図８に示した監査UI８０で設定可能な引数として検索条件、関連ログ設定、必須ログ設定が指定される。Ｓ９０２にて検索ロジックモジュール５２は印刷ログ検索モジュール５３に対するクエリ（印刷ログ検索クエリ）を生成し、指定された各検索条件をクエリに設定する。

【００３９】

次に、Ｓ９０３にて検索ロジックモジュール５２は、ユーザが図８に示した監査UI８０の関連ログ設定ペイン８１５を用いて、関連ログ設定が指定されているかを判断する。ここで、設定されていないと検索ロジックモジュール５２が判断した場合はＳ９０４へ、設定されていると判断した場合はＳ９０７へ処理を分岐する。

Ｓ９０４にて検索ロジックモジュール５２は、前述の印刷ログ検索クエリに対して検索結果のソート順序の指定であるソート条件を設定する。ソート条件としては印刷ログ項目の各項目順が指定可能であり、監査アプリケーション５１から指定する方法と、検索ロジックモジュール５２にあらかじめデフォルト値として設定することも可能である。

【００４０】

次に、Ｓ９０５にて検索ロジックモジュール５２は、印刷ログ検索モジュール５３へ印刷ログ検索クエリを発行する。印刷ログ検索クエリを受けた印刷ログ検索モジュール５３は、印刷ログデータベース３４に対して、印刷ログデータベース３４が解釈可能なクエリに変換して発行する。

【００４１】

印刷ログ検索モジュール５３は、検索結果を印刷ログデータベース３４より受け付け、検索ロジックモジュール５２に検索結果を通知する。ここで、印刷ログ検索モジュール５３は、監査サーバ１５のＲＡＭ２３にロードされＣＰＵ２１により実行される。

Ｓ９０６にて検索ロジックモジュール５２は、印刷ログ検索モジュール５３より通知される検索結果を受け付け、Ｓ９１７へ移行する。

以下、検索ロジックモジュール５２が、Ｓ９０３にて関連ログ設定が指定されていると判断した場合の処理を説明する。

Ｓ９０７にて検索ロジックモジュール５２は、印刷ログ検索モジュール５３へ印刷ログ検索クエリ（検索要求）を発行する。印刷ログ検索クエリを受け付けた印刷ログ検索モジュール５３は、印刷ログデータベース３４に対して、印刷ログデータベース３４が解釈可能なクエリに変換して発行する。印刷ログ検索モジュール５３は、検索結果を印刷ログデータベース３４より受け付け、検索ロジックモジュール５２に検索結果を通知する。ここで、印刷ログ検索モジュール５３は、監査サーバ１５のＲＡＭ２３にロードされＣＰＵ２１により実行される。

【００４２】

Ｓ９０８にて検索ロジックモジュール５２は、印刷ログ検索モジュール５３より検索結果を受け付け結果から印刷ログを逐次１件選択し、以下のフローを件数分繰り返す。

そして、Ｓ９０９にて検索ロジックモジュール５２は、選択した印刷ログから、関連ログ設定されている属性値を取得する。次に、Ｓ９１０にて外部検索モジュール５４に対するクエリ（関連ログ検索クエリ）を生成し、設定された各条件値をクエリに設定する。

次に、Ｓ９１１にて検索ロジックモジュール５２は、ユーザが監査ＵＩ８０の必須ログ設定ペイン８１６を用いて、必須ログ設定が指定されているかを判断する。ここで、必須ログ設定が設定されていると検索ロジックモジュール５２が判断した場合はＳ９１２へ、設定されていないと判断した場合はＳ９１３へ処理を分岐する。

Ｓ９１２にて検索ロジックモジュール５２は、前述の関連ログ検索クエリに対して必須ログ設定に対応するログ種別の値を追加設定する。ここで、本実施形態では、関連ログ検索クエリは、検索ヒット件数のみを返却するクエリで構成されている。また、必須ログ設定が有効な場合は、関連ログ設定に対応した件数取得クエリと、関連ログ設定および必須ログ設定の積にて設定された件数取得クエリをそれぞれ取得するクエリが構成される。

【００４３】

次に、Ｓ９１３にて検索ロジックモジュール５２は、外部検索モジュール５４へ前述のログ検索クエリ（関連ログ検索要求）を発行する。関連ログ検索クエリを受けた外部検索モジュール５４は、ログ収集サーバ１６に対して、ログ収集サーバ１６が解釈可能なクエリに変換して発行する。外部検索モジュール５４は、検索結果をログ収集サーバ１６より受け付け、検索ロジックモジュール５２に検索結果を通知する。ここで、外部検索モジュール５４は、監査サーバ１５のＲＡＭ２３にロードされＣＰＵ２１により実行される。

【００４４】

Ｓ９１４にて、検索結果を受けた検索ロジックモジュール５２は、結果の検索ヒット件数を該選択した印刷ログに追加属性値として設定する。この際、必須ログ設定がなされている場合には、関連ログ設定のみによるクエリのヒット件数（ログヒット件数）と、必須

ログ設定が反映されたクエリのヒット件数（必須ログヒット件数）の２項目追加される。上記Ｓ９０８～Ｓ９１４のステップを印刷ログ検索結果件数分繰り返す。

【００４５】

次に、Ｓ９１５にて検索ロジックモジュール５２は、印刷ログ検索結果の件数分、処理が完了したと判断すると、Ｓ９１６にて印刷ログ検索結果を前述のログヒット件数の昇順でソーティングする。

ここで、ソート条件として、ログヒット件数ではなく、必須ログヒット件数を選択するよう構成することも可能である。また、もしくは必須ログヒット件数を第一のソート条件、ログヒット件数を第二のソート条件とした複合条件を設定することも可能であるが、本実施の形態ではログヒット件数に設定されているとして説明する。

【００４６】

最後に、Ｓ９１６にて検索ロジックモジュール５２は、印刷ログ検索結果として設定に従ってソートされた結果を監査アプリケーション５１に通知し、処理を終了する。この際、ログヒット件数および必須ログヒット件数が追加属性値に設定されている場合は、それらを含んだ結果を通知する。

【００４７】

図１０は、図８に示した監査ＵＩ８０の検索結果ペイン８２０に表示される検索結果画面の一例を示す図である。

図１０に示す画面は、監査ＵＩ８０は前述したように、監査サーバ１５の監査アプリケーション５１にて構成され、監査用クライアント１７のＷｅｂブラウザ上に表示される。

監査アプリケーション５１は、検索ロジックモジュール５２より受け取った検索結果を検索結果ペイン８２０の検索結果リスト１００１に反映する。監査アプリケーション５１は、監査サーバ１５のＲＡＭ２３にロードされＣＰＵ２１により実行され、Ｗｅｂブラウザで解釈可能に画面情報を生成する。その情報を監査用クライアント１７のＷｅｂブラウザからの検索ボタン押下のリクエストに対するレスポンスとして通知する。

【００４８】

図１０にて、検索結果リスト１００１の表示順は上述した検索ロジックモジュール５２の処理フローにて決定されたソート順序に従う。

そのため、検索時に関連ログ設定がなされている場合は、ログヒット件数が少ないものからソートされて表示される。

ログヒット件数が少ない、つまり、ログ収集・管理の対象にない方法や手段により印刷された印刷ログである。そのため、より疑わしい印刷ログから優先して表示することが可能となる。

【００４９】

また、検索ロジックモジュール５２より受け取った検索結果に、必須ログヒット件数が設定されている場合、監査アプリケーション５１は必須ログヒット件数がゼロ件のものを強調表示するよう構成することができる。

図１０では、検索結果リスト１００１の上位２件が該当する必須ログヒット件数がゼロ件である例であり、他の印刷ログとは背景色を変えることで強調表示している。その結果、より疑わしい印刷ログを容易に特定することが可能となる。

【００５０】

以上の方法により、不正な印刷のログだけでなく正当な印刷のログも蓄積される膨大な印刷ログの中から、ログ収集・管理の対象にない方法や手段によって印刷された印刷ログを優先的に確認することが可能になる。つまり、印刷ログと共にコンピュータの操作が記録されているログを監査することで不正な印刷の特定の精度を向上することが可能となる。

【００５１】

また、本発明は、以下の処理を実行することによっても実現される。即ち、上述した実施形態の機能を実現するソフトウェア（プログラム）を、ネットワーク又は各種記憶媒体を介してシステム或いは装置に供給し、そのシステム或いは装置のコンピュータ（または

ＣＰＵやＭＰＵ等）がプログラムを読み出して実行する処理である。

【００５２】

本発明は上記実施形態に限定されるものではなく、本発明の趣旨に基づき種々の変形（各実施形態の有機的な組合せを含む）が可能であり、それらを本発明の範囲から除外するものではない。

本発明の様々な例と実施形態を示して説明したが、当業者であれば、本発明の趣旨と範囲は、本明細書内の特定の説明に限定されるのではない。

【符号の説明】

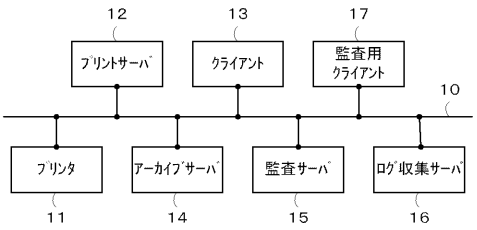
【００５３】

１４　アーカイブサーバ

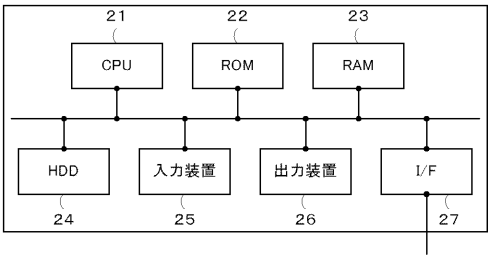
１５　検査サーバ

１６　ログ収集サーバ

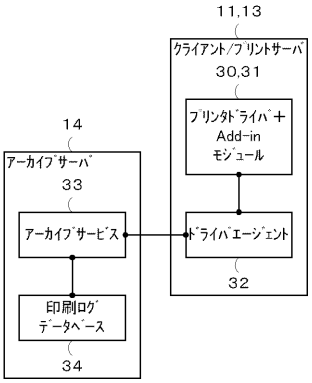
【図１】



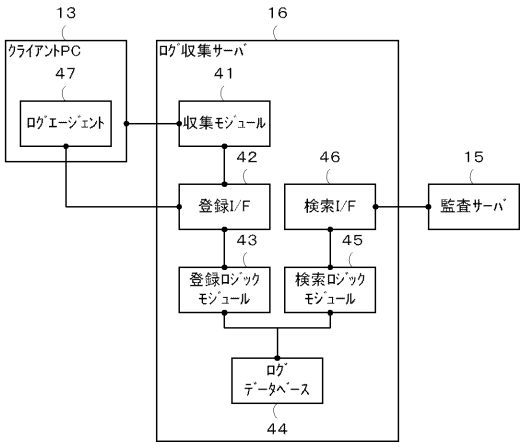
【図２】



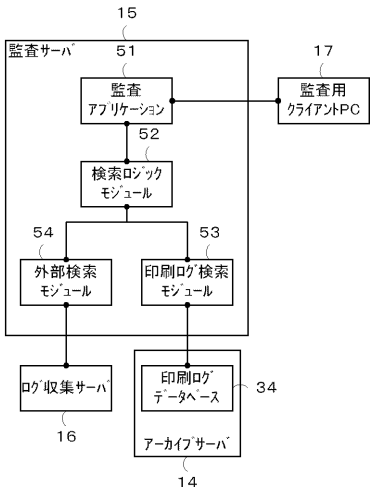
【図３】



【図４】


13
16
ｸﾗｲｱﾝﾄPC
47
ﾛｸﾞｴｰｼﾞｪﾝﾄ
ﾛｸﾞ収集ｻｰﾊﾞ
41
収集ﾓｼﾞｭｰﾙ
42
登録I/F
46
検索I/F
15
監査ｻｰﾊﾞ
43
45
登録ﾛｼﾞｯｸ
ﾓｼﾞｭｰﾙ
検索ﾛｼﾞｯｸ
ﾓｼﾞｭｰﾙ
ﾛｸﾞ
ﾃﾞｰﾀﾍﾞｰｽ
44

【図５】


15
監査ｻｰﾊﾞ
51
監査
ｱﾌﾟﾘｹｰｼｮﾝ
17
監査用
ｸﾗｲｱﾝﾄPC
52
検索ﾛｼﾞｯｸ
ﾓｼﾞｭｰﾙ
54
53
外部検索
ﾓｼﾞｭｰﾙ
印刷ﾛｸﾞ検索
ﾓｼﾞｭｰﾙ
ﾛｸﾞ収集ｻｰﾊﾞ
16
印刷ﾛｸﾞ
ﾃﾞｰﾀﾍﾞｰｽ
34
ｱｰｶｲﾌﾞｻｰﾊﾞ
14

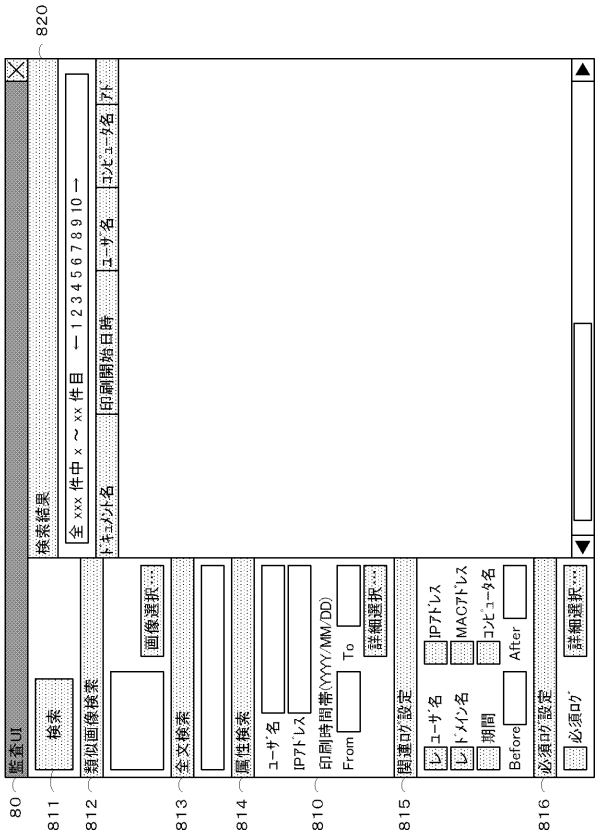
【図６】


60
ユーザ名
61
ドメイン名
62
コンピュータ名
63
IPアドレス
64
MACアドレス
65
ドキュメント名
66
印刷開始日時
67
テキスト情報
68
画像特徴量
69

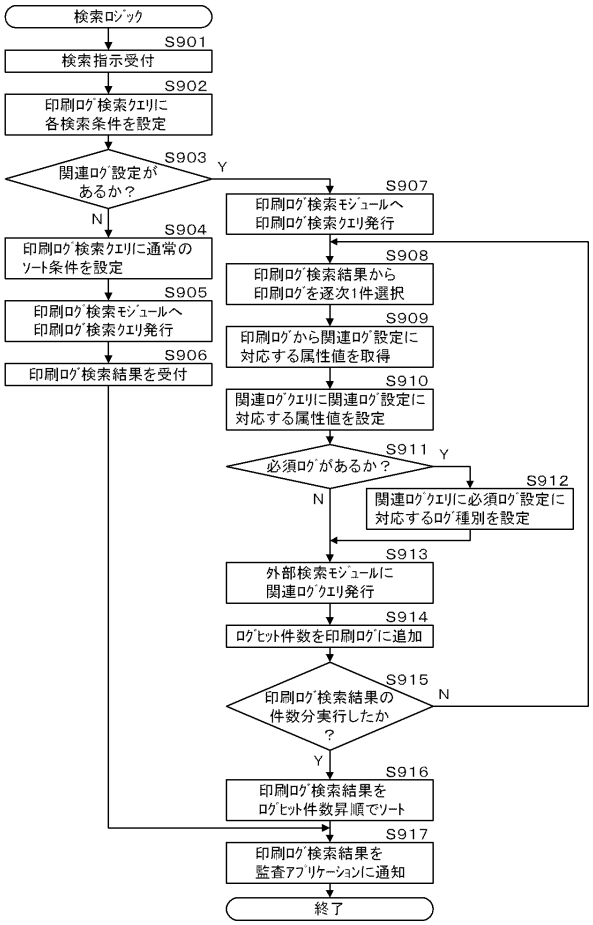
【図７】


70
ログ種別
71
ユーザ名
72
ドメイン名
73
コンピュータ名
74
IPアドレス
75
MACアドレス
76
記録日時
77

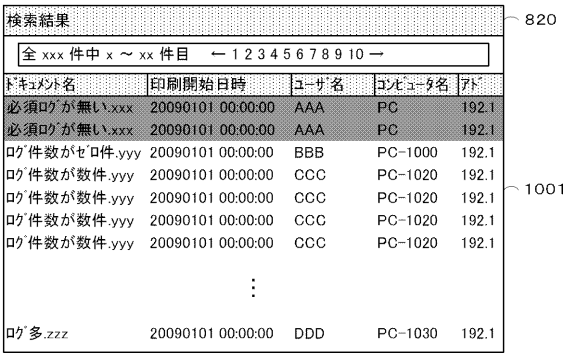
【図８】


820
検索結果
全 xxx 件中 x ～ xx 件目 ←1 2 3 4 5 6 7 8 9 10→
ﾄﾞｷｭﾒﾝﾄ名
印刷開始日時
ﾕｰｻﾞ名
ｺﾝﾋﾟｭｰﾀ名
ｱﾄﾞ
監査UI
検索
類似画像検索
画像選択…
全文検索
属性検索
ユーザ名
IPアドレス
印刷時間帯(YYYY/MM/DD)
From
To
詳細選択…
関連ﾛｸﾞ設定
ユーザ名
ドメイン名
IPアドレス
MACアドレス
コンピュータ名
期間
Before
After
必須ﾛｸﾞ設定
必須ﾛｸﾞ
詳細選択…
80
811
812
813
814
810
815
816

【図９】


検索ﾛｼﾞｯｸ
S901
検索指示受付
S902
印刷ﾛｸﾞ検索ｸｴﾘに
各検索条件を設定
S903
関連ﾛｸﾞ設定が
あるか？
Y
N
S904
印刷ﾛｸﾞ検索ｸｴﾘに通常の
ｿｰﾄ条件を設定
S905
印刷ﾛｸﾞ検索ﾓｼﾞｭｰﾙへ
印刷ﾛｸﾞ検索ｸｴﾘ発行
S906
印刷ﾛｸﾞ検索結果を受付
S907
印刷ﾛｸﾞ検索ﾓｼﾞｭｰﾙへ
印刷ﾛｸﾞ検索ｸｴﾘ発行
S908
印刷ﾛｸﾞ検索結果から
印刷ﾛｸﾞを逐次1件選択
S909
印刷ﾛｸﾞから関連ﾛｸﾞ設定に
対応する属性値を取得
S910
関連ﾛｸﾞｸｴﾘに関連ﾛｸﾞ設定に
対応する属性値を設定
S911
必須ﾛｸﾞがあるか？
Y
N
S912
関連ﾛｸﾞｸｴﾘに必須ﾛｸﾞ設定に
対応するﾛｸﾞ種別を設定
S913
外部検索ﾓｼﾞｭｰﾙに
関連ﾛｸﾞｸｴﾘ発行
S914
ﾛｸﾞﾋｯﾄ件数を印刷ﾛｸﾞに追加
S915
印刷ﾛｸﾞ検索結果の
件数分実行したか
？
N
Y
S916
印刷ﾛｸﾞ検索結果を
ﾛｸﾞﾋｯﾄ件数昇順でｿｰﾄ
S917
印刷ﾛｸﾞ検索結果を
監査ｱﾌﾟﾘｹｰｼｮﾝに通知
終了

【図１０】


検索結果
820
全 xxx 件中 x ～ xx 件目 ←1 2 3 4 5 6 7 8 9 10→
ﾄﾞｷｭﾒﾝﾄ名
印刷開始日時
ﾕｰｻﾞ名
ｺﾝﾋﾟｭｰﾀ名
ｱﾄﾞ
必須ﾛｸﾞが無い.xxx 20090101 00:00:00 AAA PC 192.1
必須ﾛｸﾞが無い.xxx 20090101 00:00:00 AAA PC 192.1
ﾛｸﾞ件数がｾﾞﾛ件.yyy 20090101 00:00:00 BBB PC-1000 192.1
ﾛｸﾞ件数が数件.yyy 20090101 00:00:00 CCC PC-1020 192.1
ﾛｸﾞ件数が数件.yyy 20090101 00:00:00 CCC PC-1020 192.1
ﾛｸﾞ件数が数件.yyy 20090101 00:00:00 CCC PC-1020 192.1
ﾛｸﾞ件数が数件.yyy 20090101 00:00:00 CCC PC-1020 192.1
1001
ﾛｸﾞ多.zzz 20090101 00:00:00 DDD PC-1030 192.1