(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2007-142930
(P2007-142930A)
(43)公開日　平成19年6月7日(2007.6.7)

(51)Int.Cl.			F I			テーマコード（参考）
H04N	1/44	(2006.01)	H04N	1/44		5C062
H04N	1/00	(2006.01)	H04N	1/00	106C	5C075
H04N	1/32	(2006.01)	H04N	1/32	Z	5J104
H04L	9/32	(2006.01)	H04L	9/00	675D	

審査請求 未請求　請求項の数 7　OL　（全 11 頁）

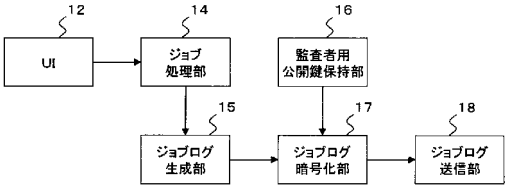
(21)出願番号　特願2005-335566 (P2005-335566)
(22)出願日　平成17年11月21日 (2005.11.21)

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂九丁目７番３号
(74)代理人　100075258
弁理士　吉田　研二
(74)代理人　100096976
弁理士　石田　純
(72)発明者　益井　隆徳
神奈川県海老名市本郷２２７４番地　富士ゼロックス株式会社内

Fターム(参考)　5C062 AA29 AB38 AB42 AC22 AC24
AC34 BA00
5C075 CF09 EE03
5J104 AA12 AA16 EA01 EA15 JA21
MA01 NA02 NA27 NA38 PA14

(54)【発明の名称】画像処理装置、ジョブログ生成方法、およびプログラム

(57)【要約】
【課題】ジョブ処理の対象となった画像を表す画像データを含むジョブログを生成する画像処理装置において、該ジョブログに対するセキュリティ強化を図る。
【解決手段】ジョブ処理部１４がジョブ処理を行い、ジョブログ生成部１５がジョブ処理の対象となった画像を表す画像データを含むジョブログを生成する。さらに、ジョブログ暗号化部１７は、監査者用公開鍵保持部１６から監査者の公開鍵を取得して、その公開鍵を用いてジョブログを暗号化する。ジョブログ送信部１８は、監査者の公開鍵で暗号化されたジョブログを監視サーバに送信する。
【選択図】図２



【特許請求の範囲】
【請求項１】
ジョブ処理を行うジョブ処理部と、
前記ジョブ処理の対象となった画像を表す画像データを含むジョブログを生成するログ生成部と、
予め定められた監査者が復号可能な暗号化処理を前記生成したジョブログに対して行って、その結果得られる暗号化ログをログ蓄積装置に蓄積させるログ暗号化部と、
を備える画像処理装置。
【請求項２】
請求項１に記載の画像処理装置において、
前記ジョブ処理は、指定された閲覧者の宛先に前記画像を送信する処理であって、
前記ジョブ処理部が送信する画像に対して前記閲覧者の公開鍵を用いて暗号化処理を行う画像暗号化部を備え、
前記ログ暗号化部は、
前記公開鍵に関する情報を前記暗号化ログと関連づけて前記ログ蓄積装置に蓄積させることを特徴とする画像処理装置。
【請求項３】
請求項１に記載の画像処理装置において、
前記ジョブ処理は、指定された閲覧者の宛先に前記画像を送信する処理であって、
前記ジョブ処理部が送信する画像に対して前記閲覧者の公開鍵を用いて暗号化処理を行う画像暗号化部を備え、
前記ログ暗号化部は、
前記閲覧者の公開鍵を用いて暗号化処理された画像を前記暗号化ログと関連づけて前記ログ蓄積装置に蓄積させることを特徴とする画像処理装置。
【請求項４】
請求項１に記載の画像処理装置において、
前記ジョブ処理は、指定された閲覧者の宛先に前記画像を送信する処理であって、
前記ジョブ処理部が送信する画像に対して前記閲覧者の暗号化パスワードを用いて暗号化処理を行う画像暗号化部を備え、
前記ログ暗号化部は、
前記暗号化パスワードを前記暗号化ログと関連づけて前記ログ蓄積装置に蓄積させることを特徴とする画像処理装置。
【請求項５】
請求項１に記載の画像処理装置において、
前記ジョブ処理は、指定された閲覧者の宛先に前記画像を送信する処理であって、
前記ジョブ処理部が送信する画像に対して前記閲覧者および前記監査者が復号可能な暗号化処理を行う画像暗号化部を備えることを特徴とする画像処理装置。
【請求項６】
画像処理装置がジョブ処理の対象となった画像を表す画像データを含むジョブログを生成するジョブログ生成方法であって、
前記画像処理装置が、
ジョブ処理を行い、
前記ジョブ処理の対象となった画像を表す画像データを含むジョブログを生成し、
予め定められた監査者により復号可能な暗号化処理を前記生成したジョブログに対して行って、その結果得られる暗号化ログをログ蓄積装置に蓄積させる、
ことを特徴とするジョブログ生成方法。
【請求項７】
コンピュータを画像処理装置として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、
ジョブ処理を行うジョブ処理部と、

前記ジョブ処理の対象となった画像を表す画像データを含むジョブログを生成するログ生成部と、
予め定められた監査者により復号可能な暗号化処理を前記生成したジョブログに対して行って、その結果得られる暗号化ログをログ蓄積装置に蓄積させるログ暗号化部と、
して機能させるためのプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、ジョブ処理を行う画像処理装置に関し、特にジョブ処理の対象となった画像を表す画像データを含むジョブログを生成し、該ジョブログをログ蓄積装置に蓄積させる画像処理装置に関する。

【背景技術】

【０００２】

近年、個人情報や社内情報などの機密情報の漏洩に対する防止策への意識が企業などで高まっている。画像の複写やスキャンなどのジョブ処理を行う画像処理装置においても、画像に示される情報の漏洩に対して防止策を講ずる必要がある。

【０００３】

画像処理装置における情報漏洩の防止策の１つとして、例えば、ジョブ処理の対象となった画像を表す画像データを含むジョブログを監視サーバに蓄積して、監査者が監視サーバに蓄積されたジョブログを監視する監視システムが知られている。

【０００４】

このような監視システムにおいて、画像処理装置から監視サーバに提供されるジョブログには特定の監査者のみが閲覧できるような暗号化を施すことは考慮されていない。そのため、例えば、第三者が監視サーバに不正にアクセスしてジョブログに含まれる画像データを閲覧することで情報が漏洩する場合がある。

【発明の開示】

【発明が解決しようとする課題】

【０００５】

本発明は、ジョブ処理の対象となった画像を表す画像データを含むジョブログを生成する画像処理装置において、該ジョブログに対するセキュリティ強化を図ることを目的とする。

【課題を解決するための手段】

【０００６】

本発明に係る画像処理装置は、ジョブ処理を行うジョブ処理部と、前記ジョブ処理の対象となった画像を表す画像データを含むジョブログを生成するログ生成部と、予め定められた監査者により復号可能な暗号化処理を前記生成したジョブログに対して行って、その結果得られる暗号化ログをログ蓄積装置に蓄積させるログ暗号化部と、を備えることを特徴とする。

【０００７】

ジョブログに含まれる画像データは、ジョブ処理の対象となった画像そのものでもよいし、その画像の縮小画像（サムネイル画像）や拡大画像でもよい。また、ログ暗号化部は少なくとも画像データに対して暗号化を行えばよい。

【０００８】

本発明に係る画像処理装置の１つの態様では、前記ジョブ処理は、指定された閲覧者の宛先に前記画像を送信する処理であって、前記ジョブ処理部が送信する画像に対して前記閲覧者の公開鍵を用いて暗号化処理を行う画像暗号化部を備え、前記ログ暗号化部は、前記公開鍵に関する情報を前記暗号化ログと関連づけて前記ログ蓄積装置に蓄積させることを特徴とする。ここで、公開鍵に関する情報とは、公開鍵で暗号化された画像について監査者がセキュリティ上の追跡調査を行う際に利用する情報であり、例えば、公開鍵のアルゴリズムや鍵長、証明書のシリアル番号、証明書を発行した認証局情報、証明書の有効期

間などいわゆる公開鍵証明書に記述される情報である。

【０００９】

また、本発明に係る画像処理装置の１つの態様では、前記ジョブ処理は、指定された閲覧者の宛先に前記画像を送信する処理であって、前記ジョブ処理部が送信する画像に対して前記閲覧者の公開鍵を用いて暗号化処理を行う画像暗号化部を備え、前記ログ暗号化部は、前記閲覧者の公開鍵を用いて暗号化処理された画像を前記暗号化ログと関連づけて前記ログ蓄積装置に蓄積させることを特徴とする。

【００１０】

さらに、本発明に係る画像処理装置の１つの態様では、前記ジョブ処理は、指定された閲覧者の宛先に前記画像を送信する処理であって、前記ジョブ処理部が送信する画像に対して前記閲覧者の暗号化パスワードを用いて暗号化処理を行う画像暗号化部を備え、前記ログ暗号化部は、前記暗号化パスワードを前記暗号化ログと関連づけて前記ログ蓄積装置に蓄積させることを特徴とする。

【００１１】

加えて、本発明に係る画像処理装置の１つの態様では、前記ジョブ処理は、指定された閲覧者の宛先に前記画像を送信する処理であって、前記ジョブ処理部が送信する画像に対して前記閲覧者および前記監査者が復号可能な暗号化処理を行う画像暗号化部を備えることを特徴とする。

【発明の効果】

【００１２】

本発明によれば、ジョブ処理の対象となった画像を表す画像データを含むジョブログを生成する画像処理装置において、該ジョブログに対するセキュリティ強化を図ることができる。

【発明を実施するための最良の形態】

【００１３】

本発明を実施するための最良の形態（以下、実施形態と称す。）について、以下図面を用いて説明する。

【００１４】

図１は、本実施形態に係る監視システムの全体のシステム構成を示す図である。図１において、監視システムは、ローカルエリアネットワーク（ＬＡＮ）１００とインターネット１１０との２つのネットワーク網から構成される。ＬＡＮ１００には、画像処理装置１０、監視サーバ２０、監査用端末３０、文書格納サーバ４０、閲覧用端末５０－１が接続されている。インターネット１１０には閲覧用端末５０－２が接続されている。以下、閲覧用端末５０－１，５０－２については区別する必要がなければ単に「閲覧用端末５０」と称する。

【００１５】

画像処理装置１０は、ジョブ処理を行う。ジョブ処理としては、ユーザから指定された文書を電子的に読み取って電子画像（以下、単に「画像」と称する）を生成するスキャン処理や、ユーザから指定された画像を用紙に印字する印刷処理などがある。また、スキャン処理により得られた画像を用紙に印字するコピー処理もジョブ処理の１つである。さらに、画像を電子メールに添付して送信したり、ＦＡＸ通信により送信することで閲覧用端末５０に送信する処理や、画像を文書格納サーバ４０に蓄積させる処理も画像処理装置１０が行うジョブ処理の１つである。

【００１６】

さらに、画像処理装置１０が上記のようなジョブ処理を行ったことが原因で情報漏洩することを防止するために、画像処理装置１０は各種ジョブ処理の対象となった画像を表す画像データを含むジョブログを生成し、監視サーバ２０に送信する。監査者は、監査用端末３０を介して監視サーバ２０にアクセスしてジョブログを参照することでジョブ処理の対象となった画像の内容を確認することができる。よって、監査者は、ジョブログを参照することで、画像処理装置１０がジョブ処理を行ったことが原因で起こりうる情報漏洩の

兆候を察知したり、情報漏洩が起きた原因について追跡調査をすることができる。

【００１７】

ここで、ジョブ処理の対象となった画像を表す画像データとは、画像に示される情報が含まれる画像データである。この画像データは、ジョブ処理の対象となった画像にどのような情報が示されているのかを監査者が確認できるデータである。例えば、画像データは、文書を電子的に読み取って得られた画像そのものや、その画像を縮小したサムネイル画像や拡大した拡大画像である。したがって、ジョブログを参照することができれば、ユーザはジョブ処理の対象となった画像に示される情報を確認することができる。そのため、監査者以外のユーザが監視サーバ２０にアクセスして、監視サーバ２０に蓄積されているジョブログを参照することができれば、情報の漏洩が起きてしまう。このような情報漏洩は、たとえ画像処理装置１０と監視サーバ２０とがＳＳＬなどの暗号化プロトコルを用いてジョブログの送受信を行っていたとしても、ジョブログ自体に暗号化がされていないため、起こりうるものである。

【００１８】

そこで、本実施形態では、画像処理装置１０は、予め定められた監査者のみが復号可能な暗号化処理をジョブログに対して行って、その結果得られる暗号化ログを監視サーバ２０に蓄積させる。

【００１９】

ここで、さらに画像処理装置１０について詳しく説明する。

【００２０】

図２は、画像処理装置１０の機能ブロックを示す図である。図２において、ユーザインタフェース（ＵＩ）１２は、所望のジョブ処理をさせるためにユーザが画像処理装置１０に対して指示を出す際に利用する操作ユニットである。ジョブ処理部１４は、ＵＩ１２やネットワークを介して受け取った指示に基づいて、各種ジョブ処理を行う。

【００２１】

ジョブログ生成部１５は、ジョブ処理の対象となった画像を表す画像データを含むジョブログを生成する。図３Ａは、ジョブログの一例を示す図である。図３Ａに示す通り、ジョブログは、テキスト領域２００と画像領域２１０とから構成される。テキスト領域２００には、実行されたジョブ処理の種別や、ジョブ処理の実行を指示したユーザの識別情報、ジョブ処理の実行日時、ジョブ処理の対象となった画像の画像フォーマットなどが示される。また、ジョブ処理が、画像を閲覧者の宛先に送信する処理の場合には、その宛先の情報などが示される。さらに、画像処理装置１０または監視サーバ２０が文字認識（OCR）の機能を有する場合には、画像で認識した文字列を検索キーワードとして、このテキスト領域２００に入れてもよい。また、画像領域２１０には、画像データとして、ジョブ処理の対象となった画像そのもの、もしくはその画像のサムネイル画像や拡大画像が示される。

【００２２】

監査者用公開鍵保持部１６は、ジョブログを監査者のみが復号可能なように暗号化するために用いる監査者用の公開鍵を保持する。公開鍵とは、いわゆる公開鍵暗号化方式で用いられる１対の鍵の一方であり、一般に公開されるほうの鍵である。監査者の公開鍵は予め認証局から取得して監査者用公開鍵保持部１６に登録しておけばよい。

【００２３】

ジョブログ暗号化部１７は、監査者用公開鍵保持部１６から監査者用の公開鍵を取得し、ジョブログ生成部１５が生成したジョブログに対してその公開鍵を用いて暗号化処理を施し、暗号化ログを生成する。ジョブログ暗号化部１７は、少なくとも画像領域２１０に対して暗号化を行う。もちろんジョブログ暗号化部１７は、ジョブログ全体に対して暗号化を行っても構わない。また、ジョブログ暗号化部１７がジョブログに含まれる画像データに示される情報を非公開情報と公開情報とに識別できる場合には、少なくとも非公開情報に対応する領域のみ暗号化を行っても構わない。

【００２４】

ジョブログ送信部１８は、暗号化ログを監視サーバ２０に送信する。監視サーバ２０は、ジョブログを蓄積するためのデータベースを備え、画像処理装置１０から送信された暗号化ログをそのデータベースに登録する。

【００２５】

以上のように、本実施形態では、画像処理装置１０が、生成したジョブログに対して監査者用の公開鍵を用いて暗号化し、その結果得られる暗号化ログを監視サーバ２０に蓄積させる。これにより、たとえ監視サーバ２０に対して第三者が不正にアクセスしてジョブログを取得したとしても、そのジョブログは、秘密鍵を有する監視者のみが復号可能な暗号化が施されているため、第三者はそのジョブログに含まれる画像データを閲覧することができない。よって、ジョブログが不正にアクセスされたとしても情報漏洩を未然に防ぐことができる。

【００２６】

また、監視サーバ２０に蓄積されるジョブログは監視者のみが復号可能なため、監視サーバ２０にアクセス可能な他のユーザが存在する場合にも、他のユーザはジョブログの内容を参照することはできない。よって、ジョブログに対するセキュリティを強化することができる。

【００２７】

ここで、図４に示すフローチャートを用いて、画像処理装置１０がユーザの指示に応じてジョブ処理を行う際の処理手順について説明する。

【００２８】

画像処理装置１０は、ユーザからの指示に応じて、文書のスキャン処理などのジョブ処理を実行する（Ｓ１００）。さらに、画像処理装置１０は、ジョブ処理の対象となった画像を表す画像データを含むジョブログを生成する（Ｓ１０２）。例えば、画像処理装置１０は、文書をスキャンすることで得られる画像のサムネイル画像を生成して、ジョブログの画像領域２１０に埋め込む。さらに、画像処理装置１０は、指示を行ったユーザを特定するための情報（ユーザ名やユーザＩＤ）や、ジョブ処理の種別などをジョブログのテキスト領域２００に記述する。

【００２９】

続いて、画像処理装置１０は、生成されたジョブログに対して監査者用の公開鍵を用いて暗号化処理を施す（Ｓ１０４）。その後、画像処理装置１０は、暗号化されたジョブログ（暗号化ログ）を監視サーバ２０に向けて送信する（Ｓ１０６）。

【００３０】

以上により、監視サーバ２０には、監査者のみが復号可能なジョブログが蓄積されることになる。よって、監視サーバ２０に蓄積されたジョブログが不正にアクセスされたとしても情報漏洩を未然に防ぐことができる。また、監視サーバ２０に蓄積されたジョブログは監視者のみが復号可能なため、監視サーバ２０にアクセス可能な他のユーザが存在する場合にも、他のユーザはジョブログの内容を参照することはできない。よって、ジョブログに対するセキュリティを強化することができる。

【００３１】

なお、上記の実施形態では、ジョブログ暗号化部１７が公開鍵暗号化方式によりジョブログを暗号化する例について説明した。しかし、監査者のみが復号可能な暗号化であれば、公開鍵暗号化方式以外の方式に基づいてジョブログを暗号化してもよい。よって、例えば、ジョブログ暗号化部１７は、監視者のみが知っている暗号化パスワードを用いてジョブログを暗号化してもよい。

【００３２】

また、上記の実施形態では、監査者は一人の場合を想定して説明しているが、監査者が複数いる場合には、画像処理装置１０は各監査者が復号可能なようにジョブログに対して暗号化を行う。より具体的には、画像処理装置１０は、まずジョブログを暗号化するためのコンテンツ暗号化鍵（乱数）を生成する。そして、画像処理装置１０は、そのコンテンツ暗号化鍵を用いてジョブログを暗号化した後、そのコンテンツ暗号化鍵を各監査者の公

開鍵でそれぞれ暗号化して、暗号化された各コンテンツ暗号化鍵を暗号化されたジョブログと関連づけて監視サーバ２０に送信する。これにより、ジョブログに対して各監査者が復号可能なように暗号化を行うことができる。

【００３３】

続いて、本実施形態の第１の変形例について説明する。

【００３４】

第１の変形例は、画像処理装置１０がジョブ処理の対象となった画像を、指定された閲覧者の宛先に送信する場合であって、送信する画像に対して閲覧者が復号可能なように閲覧者の公開鍵を用いて暗号化する場合に好適な例である。

【００３５】

従来は、閲覧者に送信する画像に対して閲覧者の公開鍵を用いて暗号化を行ったとしても、その時用いた公開鍵に関する情報をログとして管理していなかった。そのため、例えば閲覧者の秘密鍵が漏洩したことなどが原因で、画像処理装置１０から送信された画像が漏洩したとしても、実際にその画像が暗号化されていたのか、そして、画像を送信する時点で有効な公開鍵で暗号化されていたかを監査者が追跡して調査することが困難であった。また、公開鍵を用いて暗号化を行って送信された画像が存在するかどうかを追跡するのが困難だったため、閲覧者の秘密鍵が漏洩するなどして、いわゆる証明書失効リスト（ＣＲＬ）に登録された場合に、以前にその秘密鍵に対応する公開鍵を使って暗号化された画像が存在するかどうかや、その公開鍵を使って暗号化された画像をどの閲覧者に送信したのかを監査者が特定し、情報漏洩の波及を未然に防ぐことが困難であった。

【００３６】

そこで、第１の変形例では、画像を閲覧者に送信する際に閲覧者の公開鍵を用いて暗号化を行っていた場合にはその公開鍵に関する情報（以下、公開鍵情報と称す。）を画像処理装置１０は暗号化ログとともに監視サーバ２０に送信する。監視サーバ２０は、画像処理装置１０から送信された暗号化ログと公開鍵情報とを関連づけてデータベースに蓄積する。

【００３７】

ここで、公開鍵情報とは、公開鍵で暗号化された画像について監査者がセキュリティ上の追跡調査を行う際に利用する情報であり、例えば、公開鍵のアルゴリズムや鍵長、証明書のシリアル番号、証明書を発行した認証局情報、証明書の有効期間などいわゆる電子証明書に記述される情報である。よって、ジョブログと公開鍵情報とを参照することで、監査者は、公開鍵を使って暗号化された画像が存在するかどうかや、その公開鍵を使って暗号化された画像をどの閲覧者に送信したのかを把握することができる。さらに、監査者は、画像を暗号化する際に用いた公開鍵が暗号化する時点において有効な公開鍵であったかどうかを把握することができる。なお、画像処理装置１０は、ジョブログのテキスト領域２００に公開鍵情報を追加して監視サーバ２０に送信してもよい。図３Ｂは、ジョブログのテキスト領域２００に公開鍵情報を追加した場合の一例である。

【００３８】

ここで、第１の変形例における画像処理装置１０がユーザの指示に応じて文書をスキャンして、その結果得られる画像を指定された閲覧者の宛先に送信する場合の処理手順について、図５に示すフローチャートを用いて説明する。

【００３９】

まず、画像処理装置１０は、ユーザからの指示に応じて文書のスキャン処理を実行する（Ｓ２００）。次いで、画像処理装置１０は、上記の実施形態と同様にジョブログを生成する（Ｓ２０２）。さらに、画像処理装置１０は、画像に対して暗号化を行う際に用いる閲覧者の公開鍵の公開鍵情報を取得して、ジョブログのテキスト領域２１０に追加する（Ｓ２０４）。そして、画像処理装置１０は、ジョブログを監査者の公開鍵で暗号化した後（Ｓ２０６）、暗号化ログを監視サーバ２０に送信する（Ｓ２０８）。

【００４０】

以上、第１の変形例によれば、画像処理装置１０は、画像を閲覧者に送信する際に閲覧

者の公開鍵を用いて暗号化を行っていた場合にはその公開鍵の公開鍵情報を暗号化ログとともに監視サーバ２０に送信する。よって、ジョブログと公開鍵情報とを参照することで、監査者は、公開鍵を使って暗号化された画像が存在するかどうかや、その公開鍵を使って暗号化された画像をどの閲覧者に送信したのかを把握することができる。さらに、監査者は、画像を暗号化する際に用いた公開鍵が暗号化する時点において有効な公開鍵であったかどうかを把握することができる。

【００４１】

なお、第１の変形例では、画像を暗号化する際に用いた閲覧者の公開鍵の公開鍵情報をジョブログと関連づけて監視サーバ２０に送信する例について説明した。しかし、送信した画像に対してどのような公開鍵で暗号化されたのかを監査者が把握することができればよい。したがって、閲覧者の公開鍵で暗号化された画像そのものをジョブログと関連づけて監視サーバ２０に送信して、監視サーバ２０にそれらを蓄積させてもよい。このようにしても、監査者は、閲覧者の公開鍵で暗号化された画像を参照することで、閲覧者の公開鍵の公開鍵情報を取得することができる。よって、監査者は、画像を暗号化する際に用いた公開鍵が暗号化する時点において有効な公開鍵であったかどうかを把握することができる。

【００４２】

続いて、第２の変形例について説明する。

【００４３】

第２の変形例では、画像処理装置１０は、閲覧者宛に暗号化して画像を送信する場合に、閲覧者のみではなく監査者もその画像を復号可能なように暗号化する。

【００４４】

画像処理装置１０が、例えば文書をスキャンして得られた画像を閲覧者の公開鍵で暗号化して閲覧者に送信した場合、送信された画像は、閲覧者の秘密鍵を用いなければ復号化することができない。しかし、情報漏洩の追跡調査などを目的として、監査者が送信された画像を復号して調査する必要が生じる場合がある。この時、監査者が閲覧者の秘密鍵を入手できなければ、その送信された画像を復号することができず、情報漏洩の追跡調査に支障をきたす場合がある。

【００４５】

そこで、第２の変形例では、たとえ閲覧者が秘密鍵を紛失したり、秘密鍵を監査者へ提供することを拒否した場合でも、閲覧者に送信した画像を監査者が復号化できるように、画像処理装置１０は送信する画像に対して暗号化を行う。より具体的には、画像処理装置１０は、画像を暗号化するために用いるコンテンツ暗号化鍵を、閲覧者の公開鍵で暗号化したものと、監査者の公開鍵で暗号したものを、画像と関連づけて閲覧者宛に送信する。これにより、閲覧者宛に送信した画像は、閲覧者のほかに監査者も復号することができる。

【００４６】

なお、画像処理装置１０は、閲覧者宛に送信する画像に対して暗号化を行う際に用いた監査者の公開鍵の公開鍵情報についてもジョブログに追加してもよい。

【００４７】

図６は、第２の変形例における画像処理装置１０が、スキャン処理の結果得られた画像を閲覧者に送信する際の処理手順を示すフローチャートである。

【００４８】

図６に示す通り、第２の変形例における画像処理装置１０は、スキャン処理の結果得られた画像に対して閲覧者の他に監査者も復号可能なように暗号化を行う（Ｓ２０４－２）。ジョブログの生成に関しては、上記の実施形態もしくは第１の変形例における画像処理装置１０と同様でよいため説明を省略する。

【００４９】

以上、第２の変形例によれば、閲覧者に送信する画像に対して暗号化を行った場合に、たとえ閲覧者が秘密鍵を紛失したり、秘密鍵を監査者へ提供することを拒否した場合でも

、監査者が閲覧者に送信した画像を容易に復号化することができる。

【００５０】

なお、第２の変形例では、画像処理装置１０が閲覧者の公開鍵を用いて画像の暗号化を行う場合を例に説明した。しかし、上記の通り、画像処理装置１０は、閲覧者用の暗号化パスワードを用いて画像を暗号化する場合もある。この場合は、図７のフローチャートに示すように、画像処理装置１０は、ジョブログのテキスト領域２００に画像を暗号化する際に用いた閲覧者用の暗号化パスワードを記述して（Ｓ２０４－３）、監視サーバ２０に送信する（Ｓ２０８）。これにより、監査者は、ジョブログを参照することで閲覧者用の暗号化パスワードを取得することができるため、たとえ閲覧者が暗号化パスワードを忘れたり、暗号化パスワードを監査者へ伝えることを拒否した場合でも、監査者が閲覧者に送信した画像を容易に復号化することができる。

【００５１】

なお、上記の実施形態及び第１～２の変形例では、画像処理装置１０と監視サーバ２０とを別々の装置として説明した。しかし、監視サーバ２０の機能を画像処理装置１０に追加してもよい。つまり、画像処理装置１０が備えるデータベースにジョブログを蓄積してもよい。

【図面の簡単な説明】

【００５２】

【図１】実施形態及び第１～２の変形例における監視システム全体のシステム構成を示す図である。

【図２】実施形態及び第１～２の変形例における画像処理装置の機能ブロックを示す図である。

【図３Ａ】画像処理装置が生成するジョブログの一例を示す図である。

【図３Ｂ】画像処理装置が生成するジョブログの一例を示す図である。

【図４】実施形態における画像処理装置が行う処理手順を示すフローチャートを示す。

【図５】第１の変形例における画像処理装置が行う処理手順を示すフローチャートを示す。

【図６】第２の変形例において、閲覧者に送信する画像に対して閲覧者の公開鍵で暗号化を行う場合に画像処理装置が行う処理手順を示すフローチャートを示す。

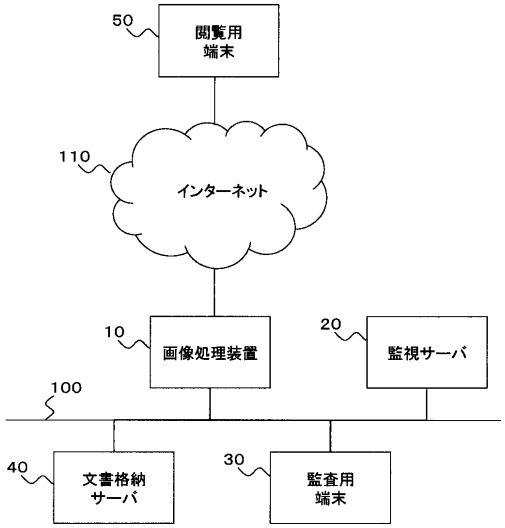
【図７】第２の変形例において、閲覧者に送信する画像に対して閲覧者の暗号化パスワードで暗号化を行う場合に画像処理装置が行う処理手順を示すフローチャートを示す。

【符号の説明】

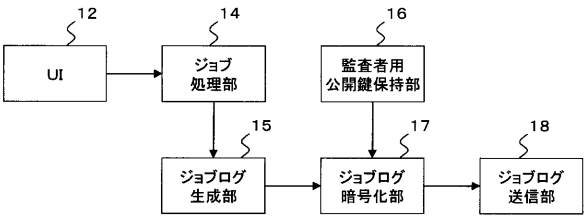
【００５３】

１０　画像処理装置、１２　ユーザインタフェース、１４　ジョブ処理部、１５　ジョブログ生成部、１６　監査者用公開鍵保持部、１７　ジョブログ暗号化部、１８　ジョブログ送信部、２０　監視サーバ、３０　監査用端末、４０　文書格納サーバ、５０　閲覧用端末。

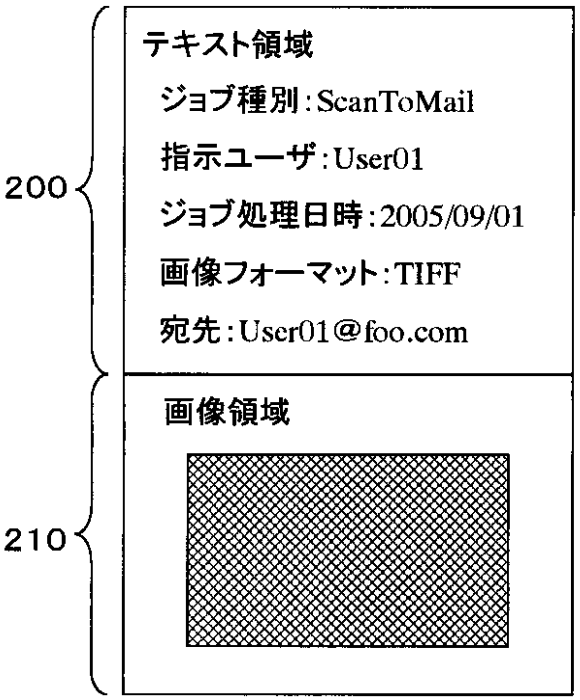
【図１】



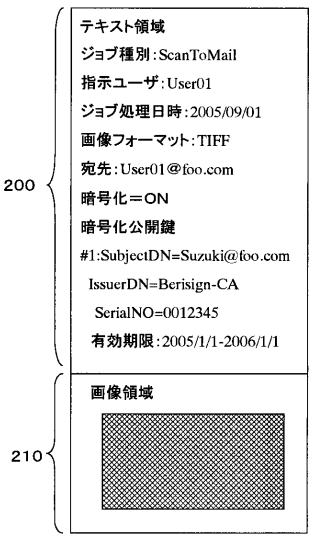
【図２】



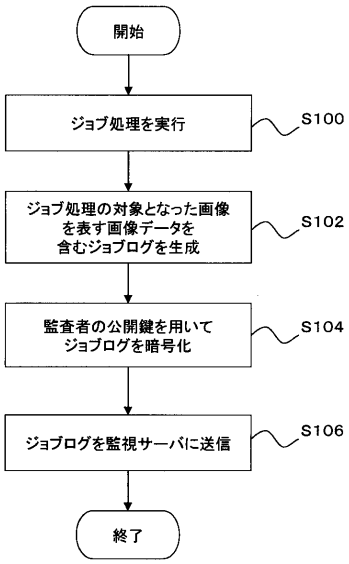
【図３Ａ】



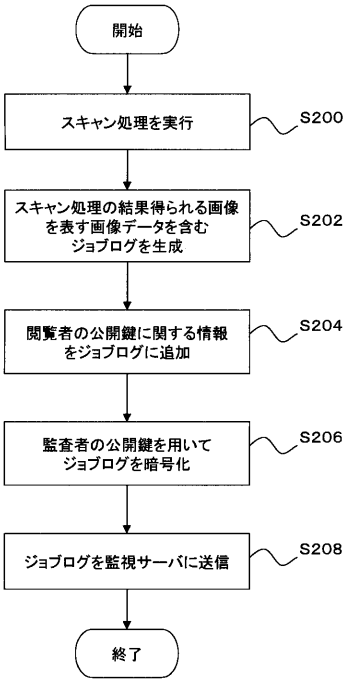
【図３Ｂ】



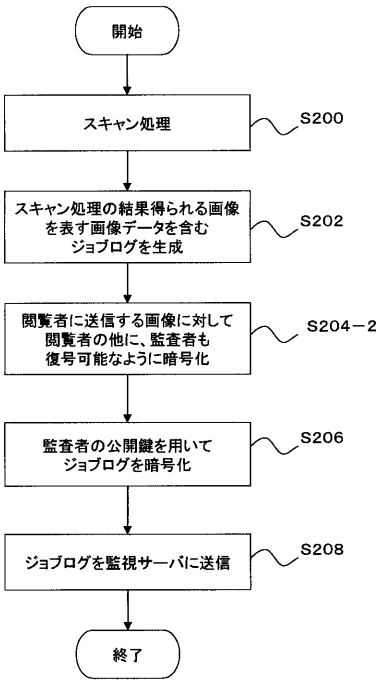
【図４】



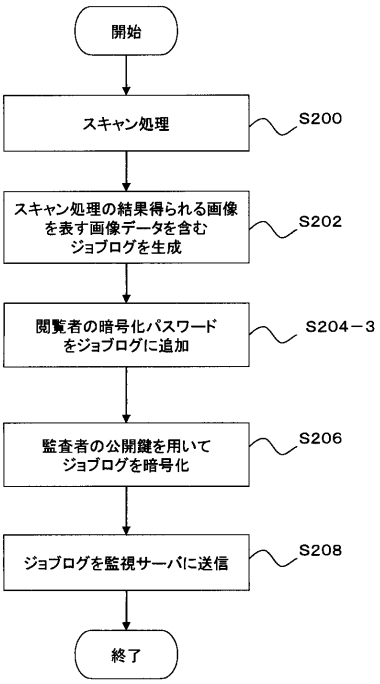
【図５】


開始
スキャン処理を実行
S200
スキャン処理の結果得られる画像を表す画像データを含むジョブログを生成
S202
閲覧者の公開鍵に関する情報をジョブログに追加
S204
監査者の公開鍵を用いてジョブログを暗号化
S206
ジョブログを監視サーバに送信
S208
終了

【図６】


開始
スキャン処理
S200
スキャン処理の結果得られる画像を表す画像データを含むジョブログを生成
S202
閲覧者に送信する画像に対して閲覧者の他に、監査者も復号可能なように暗号化
S204－2
監査者の公開鍵を用いてジョブログを暗号化
S206
ジョブログを監視サーバに送信
S208
終了

【図７】


開始
スキャン処理
S200
スキャン処理の結果得られる画像を表す画像データを含むジョブログを生成
S202
閲覧者の暗号化パスワードをジョブログに追加
S204－3
監査者の公開鍵を用いてジョブログを暗号化
S206
ジョブログを監視サーバに送信
S208
終了