(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4442583号
(P4442583)

(45)発行日　平成22年3月31日(2010.3.31)　(24)登録日　平成22年1月22日(2010.1.22)

(51)Int.Cl.			F I		
H04L	9/08	(2006.01)	H04L	9/00	601A
H04N	1/44	(2006.01)	H04N	1/44	
G09C	1/00	(2006.01)	H04L	9/00	601E
			G09C	1/00	660D

請求項の数 13　(全 14 頁)

(21)出願番号　特願2006-119120 (P2006-119120)
(22)出願日　平成18年4月24日 (2006.4.24)
(65)公開番号　特開2007-295167 (P2007-295167A)
(43)公開日　平成19年11月8日 (2007.11.8)
審査請求日　平成18年4月24日 (2006.4.24)

前置審査

(73)特許権者　303000372
コニカミノルタビジネステクノロジーズ株式会社
東京都千代田区丸の内一丁目６番１号
(74)代理人　100101454
弁理士　山田　卓二
(74)代理人　100081422
弁理士　田中　光雄
(72)発明者　岡本　知幸
東京都千代田区丸の内一丁目６番１号　コニカミノルタビジネステクノロジーズ株式会社内

審査官　青木　重徳

最終頁に続く

(54)【発明の名称】画像処理装置、画像処理方法及び画像処理用プログラム

(57)【特許請求の範囲】

【請求項１】

それぞれの公開鍵で対応付けられた複数の個別記憶領域を有する記憶部と、

画像データに対応する共通鍵を生成する共通鍵生成部と、

前記共通鍵で前記画像データを暗号化することにより暗号化画像データを生成する暗号化画像データ生成部と、

前記共通鍵を前記複数の個別記憶領域のうちの所定の個別記憶領域に対応付けられた公開鍵で暗号化することにより暗号共通鍵情報を生成する暗号共通鍵情報生成部と、を有し、

前記記憶部は、前記暗号化画像データを記憶する画像データ記憶領域を備え、前記暗号共通鍵情報を、前記暗号共通鍵情報を生成する際に使用した前記公開鍵に対応する前記所定の個別記憶領域に格納することを特徴とする画像処理装置。

【請求項２】

前記個別記憶領域には、格納されている前記暗号共通鍵情報と対応する前記暗号化画像データとを関係付けるリンク情報を格納することを特徴とする請求項１に記載の画像処理装置。

【請求項３】

前記共通鍵で前記暗号化画像データを復号して画像データを取得する暗号化画像データ復号部を有することを特徴とする請求項１又は２に記載の画像処理装置。

【請求項４】

前記画像処理装置は、復号された画像データに基づいてプリントするプリント部を有することを特徴とする請求項３に記載の画像処理装置。

【請求項５】

前記暗号化画像データ復号部は、前記公開鍵と対をなす秘密鍵を用いて復号化を行うことを特徴とする請求項３に記載の画像処理装置。

【請求項６】

前記個別記憶領域として第１個別記憶領域と第２個別記憶領域とを有し、前記第１個別記憶領域に格納された第１暗号共通鍵情報を、前記第２個別記憶領域にコピー又は移動させる際は、前記第１暗号共通鍵情報を前記第１個別記憶領域に対応する第１公開鍵と対をなす第１秘密鍵で復号し、前記第２個別記憶領域に対応する第２公開鍵で暗号化した第２暗号共通鍵情報を、前記第２個別記憶領域に格納することを特徴とする請求項１～５のいずれかに記載の画像処理装置。

【請求項７】

前記第１個別記憶領域に格納された第１暗号共通鍵情報を、前記第２個別記憶領域にコピー又は移動させる際は、前記第２暗号共通鍵情報に、前記第１個別記憶領域に対応する電子署名又はコピーもしくは移動を指示したユーザの電子署名を付与することを特徴とする請求項６に記載の画像処理装置。

【請求項８】

前記個別記憶領域として第１個別記憶領域と第２個別記憶領域とを有し、前記第１個別記憶領域および前記第２個別記憶領域に前記暗号共通鍵情報を格納する際は、前記共通鍵の情報を、前記第１個別記憶領域に対応する第１公開鍵で暗号化した第１暗号共通鍵情報を前記第１個別記憶領域に格納し、前記第２個別記憶領域に対応する第２公開鍵で暗号化した第２暗号共通鍵情報を前記第２個別記憶領域に格納することを特徴とする請求項１～５のいずれかに記載の画像処理装置。

【請求項９】

前記画像処理装置は装置秘密鍵と装置公開鍵とを有しており、前記暗号化画像データ生成部は、前記装置公開鍵で前記画像データを暗号化して装置暗号化画像データを生成することを特徴とする請求項１～８のいずれかに記載の画像処理装置。

【請求項１０】

前記画像処理装置に接続された情報処理端末からの指示に基づいて、前記暗号化画像データ及び暗号共通鍵情報を前記情報処理端末へ送信するか、又は前記装置暗号化画像データを前記装置秘密鍵で復号して得られた画像データを前記情報処理端末へ送信する通信手段を有することを特徴とする請求項９に記載の画像処理装置。

【請求項１１】

前記画像処理装置は、原画像を読み取って画像データを生成するスキャナ部を有し、前記暗号化画像データ生成部は、前記スキャナ部で生成した画像データを前記共通鍵で暗号化することにより暗号化画像データを生成することを特徴とする請求項１～１０のいずれかに記載の画像処理装置。

【請求項１２】

前記記憶部は、公開鍵が対応付けられていない個別記憶領域を有し、

前記スキャナ部で生成した画像データを格納する個別記憶領域に公開鍵が対応付けられているか否かを判断する判断部を備えていて、

公開鍵が対応付けられていない場合は、共通鍵で暗号化することなく前記画像データを前記公開鍵が対応付けられていない個別記憶領域に記憶することを特徴とする請求項１１に記載の画像処理装置。

【請求項１３】

前記記憶部は、前記画像データに関する文書タイトル、作成日時、文書の作成者のうちの少なくとも１つの文書情報を、前記暗号共通鍵情報に対応付けて記憶することを特徴とする請求項１～１２のいずれかに記載の画像処理装置。

【発明の詳細な説明】

【技術分野】
【０００１】
本発明は、ネットワークに接続可能な画像処理装置と、該画像処理装置における画像処理方法と、該画像処理をコンピュータに実行させるための画像処理用プログラムとに関するものである。
【背景技術】
【０００２】
一般に、コンピュータ、プリンタ、スキャナ装置、複合機等がネットワークを介して互いに接続されたネットワークシステムにおいて、文書、画像等のデジタルデータをやり取りし又は保存する場合、データの内容が第３者に漏洩するおそれがある。そこで、このようなデジタルデータを暗号化してやり取りし又は保存し、データを使用する際に復号化するようにした暗号化技術が種々提案されている（例えば、特許文献１～４参照）。
【０００３】
具体的には、特許文献１は、送信先フォルダに公開鍵がある場合はデータを暗号化して保存することによりデータのセキュリティを確保するようにしたネットワークシステムを開示している。特許文献２は、プリントジョブを公開鍵で暗号化し秘密鍵で復号化するようにした上で、音声情報に関連付けられた鍵の対を用いることによりプリント時のデータの漏洩を低減するようにした印刷システムを開示している。特許文献３は、フォルダ内のファイルを暗号化する際に、ネットワークワークサーバから公開鍵を取得してファイルを暗号化し、暗号化されたファイルはアイコンを変えて表示するようにした文書管理システムを開示している。特許文献４は、ファイルを暗号化することによりセキュリティを保ちつつ、他の端末装置との間で暗号化ファイルを共有することができるようにしたネットワークシステムを開示している。
【特許文献１】特開２００３－２４４１２６号公報（段落［００２７］、図５）
【特許文献２】特開２００３－０２９９５５号公報（段落［００３０］、図３）
【特許文献３】特開２００３－２４２００５号公報（段落［００４３］、図４）
【特許文献４】特開２００４－０７２１５１号公報（段落［００３２］、図１）
【発明の開示】
【発明が解決しようとする課題】
【０００４】
しかしながら、この種のネットワークシステムにおける従来の暗号化技術では、例えば、スキャナ装置のようなデバイスにおいて、対称鍵暗号化方式による処理を行う場合、情報処理量が非常に多くなるので、処理速度が低下したり、処理効率が低下したりするといった問題がある。
【０００５】
本発明は、上記従来の問題を解決するためになされたものであって、ネットワークを介して画像処理装置等が互いに接続されたネットワークシステムにおいて、処理速度及び処理効率を低下させることなく、文書、画像等のデジタルデータを暗号化・復号化することを可能にする手段を提供することを目的ないしは解決すべき課題とする。
【課題を解決するための手段】
【０００６】
上記課題を解決するためになされた本発明に係る画像処理装置は、記憶部と、共通鍵生成部と、暗号化画像データ生成部と、暗号共通鍵情報生成部とを有している。記憶部は、それぞれの公開鍵で対応付けられた複数の個別記憶領域（ボックス）を有する。共通鍵生成部は、画像データ（イメージデータ）に対応する共通鍵を生成する。暗号化画像データ生成部は、共通鍵で画像データを暗号化することにより暗号化画像データを生成する。暗号共通鍵情報生成部は、共通鍵を複数の個別記憶領域のうちの所定の個別記憶領域に対応付けられた公開鍵で暗号化することにより暗号共通鍵情報を生成する。記憶部は、暗号化画像データを記憶する画像データ記憶領域（イメージストア）を備えている。ここで、暗号共通鍵情報は、暗号共通鍵情報を生成する際に使用した公開鍵に対応する前記所定の個

別記憶領域に格納されている。

【０００７】

本発明に係る上記画像処理装置においては、個別記憶領域に、格納されている暗号共通鍵情報と対応する暗号化画像データとを関係付けるリンク情報を格納するのがさらに好ましい。

【０００８】

本発明に係る上記各画像処理装置は、共通鍵で暗号化画像データを復号して画像データを取得する暗号化画像データ復号部を有するのが好ましい。この場合、画像処理装置は、復号された画像データに基づいてプリントするプリント部を有するのがさらに好ましい。また、暗号化画像データ復号部は、公開鍵と対をなす秘密鍵を用いて復号化を行ってもよい。

【０００９】

本発明に係る上記各画像処理装置は、個別記憶領域として第１個別記憶領域と第２個別記憶領域とを有していてもよい。この画像処理装置においては、第１個別記憶領域に格納された第１暗号共通鍵情報を、第２個別記憶領域にコピー又は移動させる際は、第１暗号共通鍵情報を第１個別記憶領域に対応する第１公開鍵と対をなす第１秘密鍵で復号し、第２個別記憶領域に対応する第２公開鍵で暗号化した第２暗号共通鍵情報を、第２個別記憶領域に格納するのが好ましい。

【００１０】

ここで、第１個別記憶領域に格納された第１暗号共通鍵情報を、第２個別記憶領域にコピー又は移動させる際は、第２暗号共通鍵情報に、第１個別記憶領域に対応する電子署名又はコピーもしくは移動を指示したユーザの電子署名を付与するのがさらに好ましい。

【００１１】

また、個別記憶領域として第１個別記憶領域と第２個別記憶領域とを有している場合において、第１個別記憶領域および第２個別記憶領域に暗号共通鍵情報を格納する際は、共通鍵の情報を、第１個別記憶領域に対応する第１公開鍵で暗号化した第１暗号共通鍵情報を第１個別記憶領域に格納し、第２個別記憶領域に対応する第２公開鍵で暗号化した第２暗号共通鍵情報を第２個別記憶領域に格納するようにしてもよい。

【００１２】

本発明に係る上記各画像処理装置は、装置秘密鍵と装置公開鍵とを有していてもよい。ここで、暗号化画像データ生成部は、装置公開鍵で画像データを暗号化して装置暗号化画像データを生成するのが好ましい。この場合、画像処理装置に接続された情報処理端末からの指示に基づいて、暗号化画像データ及び暗号共通鍵情報を情報処理端末へ送信するか、又は装置暗号化画像データを装置秘密鍵で復号して得られた画像データを情報処理端末へ送信する通信手段を有するのがさらに好ましい。

【００１３】

本発明に係る上記各画像処理装置は、原画像を読み取って画像データを生成するスキャナ部を有していてもよい。ここで、暗号化画像データ生成部は、スキャナ部で生成した画像データを共通鍵で暗号化することにより暗号化画像データを生成するのが好ましい。この画像処理装置は、記憶部が公開鍵が対応付けられていない個別記憶領域を有するときは、スキャナ部で生成した画像データを格納する個別記憶領域に公開鍵が対応付けられているか否かを判断する判断部を備えていてもよい。ここで、公開鍵が対応付けられていない場合は、共通鍵で暗号化することなく画像データを公開鍵が対応付けられていない個別記憶領域に記憶するのが好ましい。

【００１４】

本発明に係る上記各画像処理装置においては、記憶部は、画像データに関する文書タイトル、作成日時、文書の作成者のうちの少なくとも１つの文書情報を、暗号共通鍵情報に対応付けて記憶していてもよい。

【発明の効果】

【００１７】

本発明に係る画像処理装置、画像処理方法又は画像処理用プログラムによれば、画像データ全体を共通鍵で暗号化した後、共通鍵だけを公開鍵で暗号化する。このため、画像データ全体を公開鍵で暗号化する場合に比べて、データ処理量が大幅に軽減される。さらに、画像データ自体は、秘密鍵でしか復号（解読）できないので、セキュリティを十分に確保することができる。また、暗号化された共通鍵のみに対して処理を行う場合は、画像データ全体の復号と再暗号化を繰り返す場合に比べて、より効率的な処理を行うことができ、ひいては高度なデータの暗号化を行うことができる。したがって、処理速度及び処理効率を低下させることなく、文書、画像等のデジタルデータを暗号化・復号化することができる。

【発明を実施するための最良の形態】

【００１８】

以下、添付の図面を参照しつつ、本発明を実施するための最良の形態（実施の形態）を具体的に説明する。なお、この実施の形態では、典型的な画像処理装置であるスキャナ装置について説明を行っているが、本発明の対象となる画像処理装置はスキャナ装置に限定される訳ではなく、その他の種々の画像処理装置、例えばプリンタ、複合機等であってもよいのはもちろんである。また、以下で説明する画像処理方法ないしは処理手順は、本発明に係るプログラムを用いてコンピュータで実行することができる。

【００１９】

図１は、本発明の実施の形態に係るスキャナ装置の構成を模式的に示すブロック図である。図１に示すように、スキャナ装置１０１（ネットワークスキャナ装置）はネットワーク１０２に接続され、該ネットワーク１０２に接続された他の端末機器（例えば、パソコン、プリンタ、複合機等）とデータのやり取りないしは送受信を行うことができるようになっている。ここで、ネットワーク１０２は、例えば企業などに構築されたローカルネットワーク（ＬＡＮ）であり、１０／１００Ｂａｓｅ－Ｔや１０００Ｂａｓｅ－Ｔ等のインターフェースを用いて実現することができる。

【００２０】

スキャナ装置１０１には、スキャナ部１０１ａと、プリンタ部１０１ｂと、操作パネル部１０１ｃと、記憶部（記憶媒体）１０１ｄと、ネットワーク通信部１０１ｅと、演算処理部１０１ｆとが組み込まれている。スキャナ部１０１ａは、詳しくは図示していないが、光源、プリズム、ＣＣＤなどを有し、文書原稿あるいは画像原稿を所定の解像度で読み取り、所定の画像処理を施して電子データに変換する。プリンタ部１０１ｂは、詳しくは図示していないが、例えば電子写真機構、インクジェット機構あるいは熱転写機構を備えたものであり、印刷ジョブ等の電子データを画像化して紙面に出力する。

【００２１】

操作パネル部１０１ｃは、例えばタッチパネル式のものであり、ユーザがスキャナ装置１０１に種々の指示を入力するための機構を有するとともに、ユーザへのメッセージをパネルに表示する。記憶部１０１ｄは、詳しくは図示していないが、ハードディスク（ＨＤＤ）や不揮発性メモリなどを有し、スキャナ装置１０１に係る各種のデータやソフトウェアを格納している。ネットワーク通信部１０１ｅはネットワーク１０２に接続され、ネットワーク１０２に接続された他の装置と通信を行うためのものであり、ネットワーク・インターフェース・カード（ＮＩＣ）などによって実現することができる。演算処理部１０１ｆは、詳しくは図示していないが、マイクロプロセッサ（ＣＰＵ）やランダム・アクセス・メモリ（ＲＡＭ）などを組み合わせることによって実現することができ、スキャナ装置１０１全体における各種制御処理を実行する。

【００２２】

演算処理部１０１ｆは、スキャナ装置１０１の各部を制御するとともに、種々の演算処理を行う。また、演算処理部１０１ｆは、共通鍵生成部ｆ１と、暗号化画像データ生成部ｆ２と、暗号共通鍵情報生成部ｆ３と、暗号化画像データ復号部ｆ４と、判断部ｆ５とを有している。ここで、共通鍵生成部ｆ１は、画像データ（イメージデータ）に対応する共通鍵Ｋを生成する。暗号化画像データ生成部ｆ２は、共通鍵Ｋで画像データを暗号化する

ことにより暗号化画像データを生成する。暗号共通鍵情報生成部ｆ３は、共通鍵Ｋを公開鍵Ａで暗号化することにより暗号共通鍵データを生成する。暗号化画像データ復号部ｆ４は、共通鍵Ｋで暗号化画像データを復号して画像データを取得する。判断部ｆ５は、スキャナ部１０１ａで生成した画像データを格納する個別記憶領域（ボックス）に公開鍵Ａが対応付けられているか否かを判断する。

【００２３】

図２は、図１に示すスキャナ装置１０１がその記憶部１０１ｄに保持している、複数の使用者（ユーザ）のボックス（使用者別記憶部）を管理するための情報を模式的に示す図である。図２に示すように、記憶部１０１ｄ内には仮想的なボックス群２０１が存在し、この仮想的なボックス群２０１は、各使用者にそれぞれ割り当てられた一列に並ぶ複数（図２に示す例では５つ）のボックスを有している。仮想的なボックス群２０１の各ボックスは、ボックス管理テーブル２０２によって管理される。

【００２４】

ボックス管理テーブル２０２において、「ＩＤ」の項目は、各ボックスの通し番号を示し、この番号は実際の物理的なボックスの位置を一意にあらわす。「名前」の項目は、各ボックスに関連付けられた使用者の名前を示す文字列であり、ユーザ認証機能のユーザ（使用者）に関連付けられた文字列を示す。「パスワード」の項目は、ボックスに関連付けられたパスワードを示し、またユーザ認証機能のユーザに関連付けられたパスワードでもある。「鍵」の項目は、ボックスに関連付けられた公開鍵を示す。公開鍵は、５１２バイトから１０２４バイト程度のバイナリデータであり、電子証明書と呼ばれるデータを保持している。例えば「ＩＤ」の項目が００１であり、「名前」の項目が岡本であるボックスは、パスワード「＊＊＊」と、「２５ＡＤ．．」から始まる文字列の公開鍵とを有している。

【００２５】

図３は、本発明に係るスキャナ装置１０１で使用される暗号化技術を模式的に示す図であり、イメージデータ３０１の暗号化及び復号の態様を示している。なお、イメージデータ３０１は、スキャンして得た画像を電子データに変換したものである。共通鍵３０２（Ｋ）は、イメージデータ３０１を暗号化するために生成された一時的な鍵であり、３ＤＥＳ、ＡＳＥ等の共通鍵方式の暗号化アルゴリズムに使用される。この共通鍵３０２（Ｋ）は、スキャン毎に生成される共通鍵、すなわちスキャン毎に異なる共通鍵である。公開鍵３０３（Ａ）は、秘密鍵３０４（Ａ’）と対で使用され、ＲＳＡ、ＤＳＡ等の対称鍵方式の暗号化アルゴリズムに使用される。公開鍵３０３で暗号化したデータは秘密鍵３０４によってのみ復号することができ、逆に秘密鍵３０４で暗号化したデータは公開鍵３０３によってのみ復号することができる。これらの鍵３０３、３０４がこのような性質を有しているので、一般に、前者の暗号化はデータの秘匿に使用され、後者の暗号化はデータへの電子署名と認証に使用される。前記のとおり、本実施の形態では、スキャン毎に異なる共通鍵を生成するようにしているが、スキャン毎にランダムに発生させる共通鍵としてもよい。また、所定回数毎に、あるいは、ユーザ毎に、異なる共通鍵またはランダムな共通鍵を生成するようにしてもよい。

【００２６】

イメージデータ３０１を共通鍵３０２で暗号化した暗号データ３０５（暗号画像データ）は、その暗号化に共通鍵方式の暗号化アルゴリズムを用いる。これにより、イメージデータ３０１の暗号化処理の効率化を図ることができる。共通鍵３０２を公開鍵３０３で暗号化した暗号データ３０６（暗号共通鍵データ）は、その暗号化に対称鍵方式の暗号化アルゴリズムを用いる。このため、秘密鍵３０４のみが、共通鍵３０２の暗号データ３０６の復号を行うことができる。したがって、暗号データ３０５と暗号データ３０６とを対にして保持することにより、秘密鍵３０４を用いなければイメージデータ３０１を入手することができないといった安全性の高い環境を提供することができる。

【００２７】

図４は、図１に示すスキャナ装置１０１がスキャンして得たイメージデータを暗号化す

る際の処理手順ないしは処理方法を示すフローチャートである。以下、図４に示すフローチャートに従って、この暗号化の処理手順を具体的に説明する。この暗号化処理においては、まず、使用者がスキャン装置１０１の操作パネル部１０１ｃを操作して、文書ないしは画像（以下「文書等」という。）のスキャンと、スキャンして得たイメージデータの所定のボックスへの格納（保存）とを指示すると（ボックススキャン開始）、スキャナ装置１０１は該ボックスに関連付けられた公開鍵３０３が存在するか否かを調査し（ステップＳ４０１）、公開鍵３０３が存在するか否かを判定する（Ｓ４０２）。

【００２８】

ステップＳ４０２で、該ボックスに関連付けられた公開鍵３０３が存在しないと判定した場合は（ＮＯ）、スキャンした文書等のイメージデータを暗号化せずにそのまま該ボックスに保存し（ステップＳ４０３）、今回のスキャン処理を終了する。逆に、該ボックスに関連付けられた公開鍵３０３が存在すると判定した場合は（ＹＥＳ）、該ボックスに関連付けられた公開鍵３０３を操作パネル部１０１ｃに表示し、使用者に対して、イメージデータを暗号化するか否かの確認を促す（ステップＳ４０４）。そして、使用者の暗号化についての指示の内容を判定し（ステップＳ４０５）、使用者がイメージデータの暗号化を指示していない場合は（ＮＯ）、スキャンした文書のデータを暗号化せずにそのまま該ボックスに保存し（ステップＳ４０３）、今回のスキャン処理を終了する。

【００２９】

他方、ステップＳ４０５で、使用者が暗号化を指示していると判定した場合は（ＹＥＳ）、文書等をスキャンして得たイメージデータ３０１用の共通鍵３０２を、例えば乱数生成手段などを用いて生成する（ステップＳ４０６）。次に、イメージデータ３０１全体を共通鍵３０２（Ｋ）で暗号化して保存する（ステップＳ４０７）。さらに、共通鍵３０２を公開鍵３０３（Ａ）で暗号化して保存し（ステップＳ４０８）、今回のスキャン処理を終了する。

【００３０】

以下、図５～図１１を参照しつつ、本発明に係るイメージデータの暗号化処理のいくつかの具体例を説明する。

図５は、本発明に係るスキャナ装置１０１がスキャンして得たイメージデータを暗号化した後、暗号データを効率的に配置した場合におけるデータ配置形態の一例を模式的に示したものであり、記憶部１０１ｄにおける仮想的なデータ配置形態を示している。図５において、イメージストア５０１（画像データ記憶部）は、イメージデータ５０８、又は該イメージデータ５０８を共通鍵５０９（Ｋ）で暗号化した暗号データ５１０を保存する領域である。ボックス５０２及びボックス５０３は、いずれもスキャナ装置１０１が有しているボックス情報を保持する領域である。両ボックス５０２、５０３には、それぞれ、公開鍵５０４（Ａ）及び公開鍵５０６（Ｂ）が関連付けられている。

【００３１】

また、秘密鍵５０５（Ａ’）及び秘密鍵５０７（Ｂ’）は、それぞれ、公開鍵５０４及び公開鍵５０６と対になっている鍵であり、これらの秘密鍵５０５、５０７は対称鍵暗号化アルゴリズムに使用される。イメージデータ５０８は、文書等をスキャンして得たイメージの電子データである。このイメージデータ５０８は、スキャン毎ないしはスキャン時に作成される共通鍵５０９により暗号化された暗号データ５１０として、イメージストア５０１に格納（保存）されている。ここで、スキャン毎に生成される共通鍵５０９とは、１ジョブ毎に生成される共通鍵を意味しているが、１ジョブ内であっても１頁ごとに異なる共通鍵を生成するようにしてもよい。

【００３２】

共通鍵５０９は、一方では公開鍵５０４により暗号化された暗号データ５１１としてボックス５０２に格納され、他方では公開鍵５０６により暗号化された暗号データ５１３としてボックス５０３に格納されている。また、ボックス５０２及びボックス５０３には、それぞれ、イメージストア５０１内の暗号データ５１０とリンクするためのリンク情報５１２及びリンク情報５１４が格納されている。したがって、ボックス５０２及びボックス

５０３に、それぞれ、イメージデータ５０８を暗号化した暗号データ５１０が格納されているのと実質的には同じことになる。このようにデータを配置することにより、ボックス５０２及びボックス５０３に、それぞれ、秘密鍵５０５及び秘密鍵５０７でしか復号（解読）することができないイメージデータを提供することができる。また、イメージデータ５０８を暗号化した暗号データ５１０をイメージストア５０１に１つ格納するだけで済むので、データ配置の効率化を実現することができる。また、リンク５１２及びリンク５１４に併せて、文書タイトル、作成日時、文書の作成者（スキャンであればスキャンを実行した人）などの文書情報を、ボックス内に暗号データ５１１と関連付けて、ボックス５０２に格納することにより、ボックス５０２内の文書の一覧を表示する際に、わざわざ、暗号データ５１０を復号化する必要がなくなり、保存した文書情報に基づいて表示することが可能になる。

【００３３】

図６は、本発明に係るネットワークスキャナ装置において、本発明に係る暗号化方式により公開されている暗号化された電子文書を、別のボックスへ公開（移動／コピー）する場合の処理手順を模式的に示す図である。図６に示すように、本発明に係るスキャナ装置６０１は、ネットワーク６０３を介して、クライアント端末６０２に接続されている。スキャナ装置６０１は、例えばＨＴＴＰサーバ機能を搭載したものである。使用者は、クライアント端末６０２上で動作するＷｅｂブラウザからアクセスすることにより、スキャナ装置６０１の種々の機能を利用することができる。

【００３４】

スキャナ装置６０１において、イメージストア６０８は、イメージデータ６１６、又は該イメージデータ６１６を共通鍵６１５（Ｋ）で暗号化した暗号データ６１７を保存している。そして、スキャナ装置６０１は、公開鍵６０５（Ａ）に関連付けられたボックス６０４と、公開鍵６１０（Ｂ）に関連付けられたボックス６０９とを公開している。共通鍵６１５は、公開鍵６０５により暗号化された暗号データ６０７としてボックス６０４に格納されている。また、ボックス６０４には、イメージストア６０８内の暗号データ６１７とリンクするためのリンク情報６１８が格納されている。したがって、ボックス６０４に、イメージデータ６１６を暗号化した暗号データ６１７が格納されているのと実質的には同じことになる。一方、クライアント端末６０２は秘密鍵６０６（Ａ'）を有しており、この秘密鍵６０６を用いて、公開鍵６０５により暗号化した暗号データ６０７を復号して、共通鍵６１５を取得することができる。

【００３５】

ここで、イメージデータ６１６を暗号化した暗号データ６１７は、次の手順でボックス６０９に公開することができる。すなわち、クライアント端末６０２は、一方では、ネットワーク６０３を経由して、共通鍵６１５を暗号化した暗号データ６０７を取得し、この暗号データ６０７を秘密鍵６０６で復号して共通鍵６１５を得る（ステップＳ６１１）。他方では、ネットワーク６０３を経由して公開鍵６１０を取得し、共通鍵６１５を公開鍵６１０で暗号化する（ステップＳ６１２）。そして、この暗号化した共通鍵６１５をボックス６０９に送信（送付）する（ステップＳ６１３）。その結果、ボックス６０９においては、該ボックス６０９に関連づけられた公開鍵６１０に対応する秘密鍵（図示せず）を用いて、暗号化された共通鍵６１５を復号化することができ、さらに暗号データ６１７を復号してイメージデータ６１６を得ることができる。なお、これらの一連の処理は、Ｗｅｂブラウザで動作するスクリプトプログラム等で自動的に行うことができる。このように鍵データだけをハンドリング（転送）することにより、あるボックスの文書を別のボックスに公開（移動／コピー）することができる。

【００３６】

なお、クライアント端末６０２で、イメージデータ６１６を閲覧する際は、クライアント端末６０２から、ボックス６０４にアクセスして、スキヤナ装置６０１に対して、選択されたイメージデータ６１６（上述したように、文書情報に基づいて選択する）を送信するよう指示を出すと、スキャナ装置６０１は、暗号データ６０７（暗号化された共通鍵６

１５）と、リンク情報６１８に基づいて特定される暗号データ６１７（暗号化されたイメージデータ６１６）とを、指示を出したクライアント端末６０２へと送信する。クライアント端末６０２では、自身の持つ秘密鍵６０６で、暗号データ６０７を復号して共通鍵６１５を取り出し、この取り出した共通鍵６１５で、暗号データ６１７を復号することにより、安全にイメージデータ６１６（文書等）の取得／閲覧を行うことができる。

【００３７】

図７は、本発明に係るネットワークスキャナ装置において、本発明に係る暗号化方式により公開されている暗号化された電子文書を印刷する場合における処理手順を模式的に示す図である。図７に示すように、スキャナ装置７０１は、図６の場合と同様に、ネットワーク７０３を介して、クライアント端末７０２に接続されている。スキャナ装置７０１において、イメージストア７０８は、イメージデータ７１６、又は該イメージデータ７１６を共通鍵７１５（Ｋ）で暗号化した暗号データ７１７を保存している。そして、スキャナ装置７０１は、公開鍵７０５（Ａ）に関連付けられたボックス７０４を有している。共通鍵７１５は、公開鍵７０５により暗号化された暗号データ７０７としてボックス７０４に格納されている。また、ボックス７０４には、イメージストア７０８内の暗号データ７１７とリンクするためのリンク情報７１８が格納されている。したがって、ボックス７０４に、イメージデータ７１６を暗号化した暗号データ７１７が格納されているのと実質的には同じことになる。一方、クライアント端末７０２は秘密鍵７０６（Ａ'）を有しており、この秘密鍵７０６を用いて公開鍵７０５により、暗号データ７０７を復号して共通鍵７１５を取得することができる。

【００３８】

ここで、イメージデータ７１６（文書）の印刷を、クライアント端末７０２からスキャナ装置７０１に指示する場合の処理手順は、次のとおりである。すなわち、まず、ネットワーク７０３を経由して、共通鍵７１５を暗号化した暗号データ７０７を取得し、この暗号データ７０７を秘密鍵７０６で復号して共通鍵７１５を得る（ステップＳ７１１）。そして、復号された共通鍵７１５をボックス７０４に送信する。この後、スキャナ装置７０１は、受信した共通鍵７１５を用いて暗号データ７１７を復号し、この復号されたイメージデータ７１６をプリンタ部１０１ｂで紙面に出力する（ステップＳ７１２）。このように、共通鍵７１５ないしはその暗号データ７０７だけをネットワーク７０３上でやり取りするだけでイメージデータ７１６（電子文書）を印刷することができ、イメージデータ７１６の保護と処理の高速化とを実現することができる。

【００３９】

図８は、図６に示す処理手順に、文書を公開した人の履歴を記録する（たどる）ことができる機能を付加した場合の処理手順を模式的に示す図である。図８に示す処理手順では、図６に示す処理手順において暗号化された文書を別のボックスへ公開する際に、暗号化された鍵情報と共に電子署名を追加することにより、文書を公開した人の履歴を記録する（たどる）ことができるようにしている。

【００４０】

図８に示すように、この場合も図６の場合と同様に、スキャナ装置８０１は、ネットワーク８０４を介して、クライアント端末８０２とクライアント端末８０３とに接続されている。そして、スキャナ装置８０１は、各クライアント端末８０２、８０３に、それぞれ個別のボックスを提供している。あるボックスの暗号化された文書を別のボックスへ公開するための処理手順は次のとおりである。

【００４１】

すなわち、ボックスＡ中の暗号化された文書を、図６に示す処理手順と同様のステップによりクライアント端末８０２からボックスＢに公開する際に（ステップＳ８１１）、公開するデータに秘密鍵Ａ'を用いて電子署名８１２を施す。同様に、ボックスＢ中の暗号化された文書を、図６に示す処理手順と同様のステップによりクライアント端末８０３からボックスＣに公開する際も（ステップＳ８１３）、前記の電子署名８１２に重ねる形で電子署名８１４を施す。このように、転送が複数回にわたる場合は、電子署名を入れ子に

することにより、転送元の履歴を電子署名で保証することができる。

【００４２】

図９は、２台のスキャナ装置を用いてネットワーク上の連携を行うようにした場合における暗号化処理の処理手順を模式的に示す図である。図９に示すように、スキャナ装置９０１及びスキャナ装置９０２は、図６の場合と同様に、ネットワーク９０５を介して、クライアント端末９０３及びクライアント端末９０４に接続されている。そして、スキャナ装置９０１及びスキャナ装置９０２は、それぞれ、クライアント端末９０３及びクライアント端末９０４に、対応する個別のボックスを提供している。前記のとおり、スキャナ装置９０１のボックスＡ内の暗号化された文書を、クライアント装置９０３から別のボックスに公開する際に、使用者はネットワーク９０５に接続された別のスキャナ装置９０２のボックスＢを選択することができる。したがって、前記の手順でもって、共通鍵Ｋをボックスに保存するとともに、イメージデータに対するネットワーク９０５越しのリンク情報９０６を付加することにより、ネットワーク９０５上の連携を簡単に実現することができる。

【００４３】

図１０は、スキャナ装置がそれ自体の対称鍵を持つことにより、前記の各処理手順を効率化するようにした場合における暗号化処理の処理手順を模式的に示す図である。図１０に示すように、スキャナ装置１００１は、図６の場合と同様に、ネットワーク１００４を介して、クライアント端末１００２及びクライアント端末１００３に接続されている。そして、スキャナ装置１００１は、各クライアント端末１００２、１００３に、それぞれ、対応する個別のボックスを提供している。また、スキャナ装置１００１はそれ自体が対称鍵１００５を有し、全てのイメージデータについて、共通鍵Ｋをそれ自体の公開鍵Ｍで暗号化した暗号データ１００６を保持している。

【００４４】

このため、スキャナ装置１００１は、クライアント端末１００２、１００３の秘密鍵Ａ’、Ｂ’を用いることなく、それ自体の秘密鍵Ｍ’で全ての暗号化されたイメージデータを復号することができる。また、これにより、スキャナ装置１００１は、クライアント端末１００２、１００３に対して、暗号化されたイメージと暗号化された共通鍵Ｋの対とをダウンロードすることにより（ステップＳ１０１１）、それ自体の秘密鍵を用いて安全にデータを復号することができる。さらに、スキャナ装置１００１は、イメージの復号をスキャナ装置１００１に依頼して復号済みのイメージデータをダウンロードするといった方式（ステップＳ１０１２）を選択することができる。また、印字する際には、クライアント端末１００２からの指示を受けるだけで、自身のもつ秘密鍵で共通鍵Ｋを取り出すことができ、プリントを行うことができるので、安全にプリントを行うことができる。

【００４５】

図１１は、スキャナ装置に一時的な対称鍵を生成することにより、一時的なボックス機能を提供するようにした場合における暗号化処理の処理手順を模式的に示す図である。図１１に示すように、スキャナ装置１１０１は、ネットワーク１１０４を介して、クライアント端末１１０２及びクライアント端末１１０３に接続されている。また、スキャナ装置１１０１は、その記憶部に一時的に対称鍵を生成し、それに関連付けられた一時的なボックス１１０５を公開している。さらに、スキャナ装置１１０１は、一時的なボックス１１０５を使用する使用者に対して、一時的な公開鍵を含む一時的な電子証明書１１０６を送信（送付）する。電子証明書の有効期限は、一時的なボックスを利用することができる有効期限と同一である。このため、一時的なボックス１１０５に保存されている文書は、前記の各ネットワークスキャナ装置の場合とは逆に、一時的な電子証明書１１０６に含まれる公開鍵で解読することができる。これにより、使用者にとって煩雑な鍵の設定を省略することができる、一時的にセキュアな文書機能をもたせることができる。

【００４６】

以上、本発明の実施の形態によれば、対称鍵暗号化方式を用いることにより、使用者の秘密鍵でしかスキャンしたデータを復号することができないセキュアなスキャナ装置ない

しは画像処理装置を提供することができる。また、使用者が煩雑な鍵の設定を省略することを希望する場合は、一時的な電子証明書に含まれる公開鍵で解読することができるスキャナ装置ないしは画像処理装置を提供することができる。

【図面の簡単な説明】

【００４７】

【図１】本発明の実施の形態に係るスキャナ装置の構成を模式的に示すブロック図である。

【図２】図１に示すスキャナ装置が有するボックスの情報を模式的に示す図である。

【図３】本発明に係るスキャナ装置が使用するデータの暗号化技術を模式的に示す図である。

【図４】本発明に係るスキャナ装置がスキャンしたデータを暗号化するための処理手順を示すフローチャートである。

【図５】本発明に係るスキャナ装置が暗号化したデータを保持する際のデータ配置形態を模式的に示す図である。

【図６】本発明に係るスキャナ装置が暗号化したデータを別のボックスへ公開する場合のデータ配置形態を模式的に示す図である。

【図７】本発明に係るスキャナ装置が暗号化したデータを印刷する場合のデータ配置形態を模式的に示す図である。

【図８】本発明に係るスキャナ装置が電子署名技術を利用して転送履歴を保存する場合のデータ配置形態を模式的に示す図である。

【図９】本発明に係るスキャナ装置がネットワークに複数台接続されて連携する場合のデータ配置形態を模式的に示す図である。

【図１０】本発明に係るスキャナ装置がそれ自体の対称鍵を持つことにより処理を効率化する場合のデータ配置形態を模式的に示す図である。

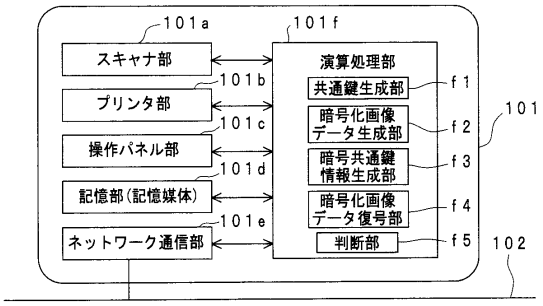
【図１１】本発明に係るスキャナ装置が一時的な対称鍵を生成する場合におけるデータ配置形態を模式的に示す図である。

【符号の説明】

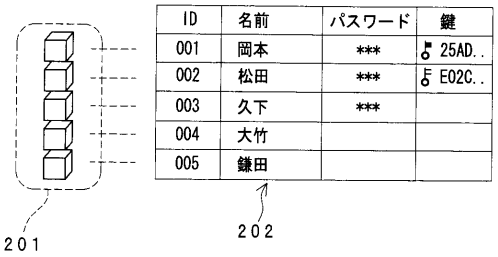
【００４８】

１０１　スキャナ装置、１０ａ　スキャナ部、１０１ｂ　プリンタ部、１０１ｃ　操作パネル部、１０１ｄ　記憶部、１０１ｅ　ネットワーク通信部、１０１ｆ　演算処理部、１０２　ネットワーク、３０１　イメージデータ、３０２　共通鍵、３０３　公開鍵、３０４　秘密鍵、３０５　暗号データ、３０６　暗号データ、５０１　イメージストア、５０２　ボックス、５０３　ボックス、５０４　公開鍵、５０５　秘密鍵、５０６　公開鍵、５０７　秘密鍵、５０８　イメージデータ、５０９　共通鍵、５１０　暗号データ、５１１　暗号データ、５１２　リンク、５１３　暗号データ、５１４　リンク、６０１　スキャナ装置、６０２　クライアント端末、６０３　ネットワーク、６０４　ボックス、６０５　公開鍵、６０６　秘密鍵、６０７　暗号データ、６０８　イメージストア、６０９　ボックス、６１０　公開鍵、６１５　共通鍵、６１６　イメージデータ、６１７　暗号データ、６１８　リンク情報、７０１　スキャナ装置、７０２　クライアント端末、７０３　ネットワーク、７０４　ボックス、７０５　公開鍵、７０６　秘密鍵、７０７　暗号データ、７０８　イメージストア、７１５　共通鍵、７１６　イメージデータ、７１７　暗号データ、７１８　リンク情報、８０１　スキャナ装置、８０２　クライアント端末、８０３　クライアント端末、８０４　ネットワーク、８１２　電子署名、８１３　電子署名、９０１　スキャナ装置、９０２　スキャナ装置、９０３　クライアント端末、９０４　クライアント端末、９０５　ネットワーク、９０６　リンク、１００１　スキャナ装置、１００２　クライアント端末、１００３　クライアント端末、１００４　ネットワーク、１００５　対称鍵、１００６　暗号データ、１１０１　スキャナ装置、１１０２　クライアント端末、１１０３　クライアント端末、１１０４　ネットワーク、１１０５　一時的なボックス、１１０６　一時的な電子証明書。

【図１】

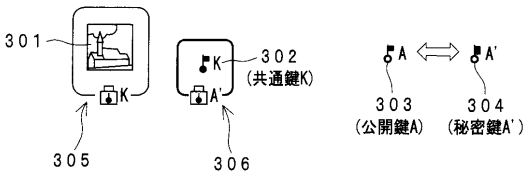


【図２】

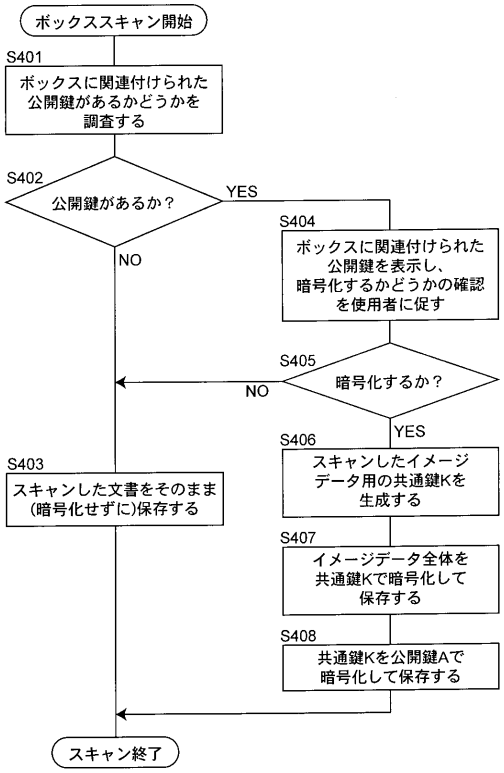


ID	名前	パスワード	鍵
001	岡本	***	25AD..
002	松田	***	E02C..
003	久下	***	
004	大竹		
005	鎌田		

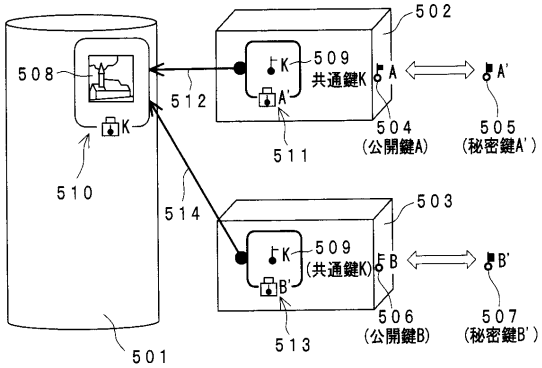
【図３】



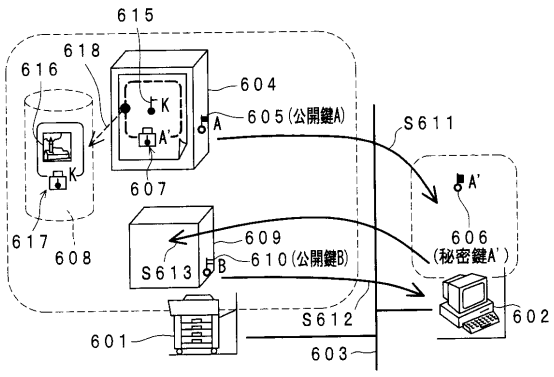
【図４】



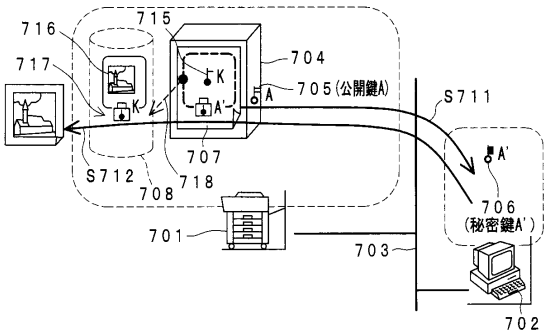
【図５】



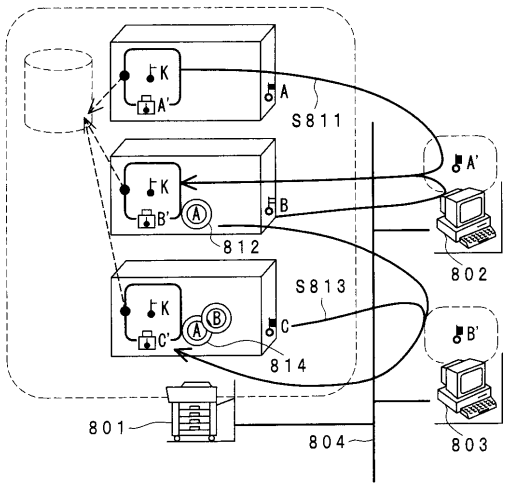
【図６】



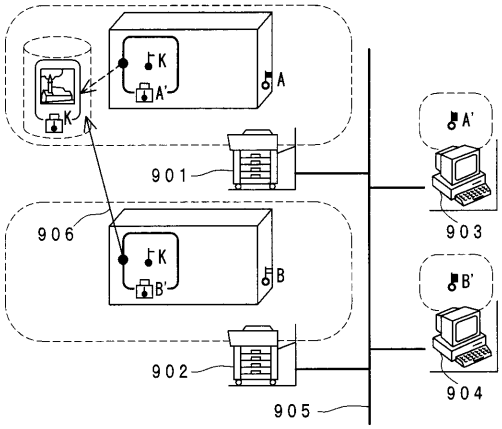
【図７】



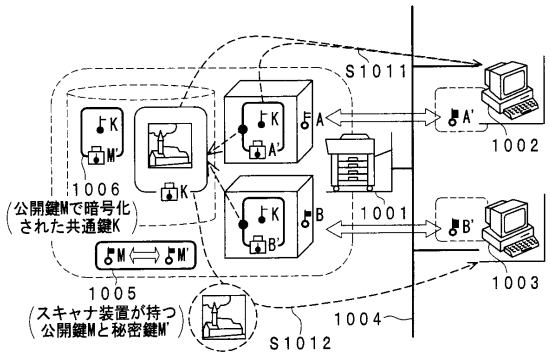
【図８】



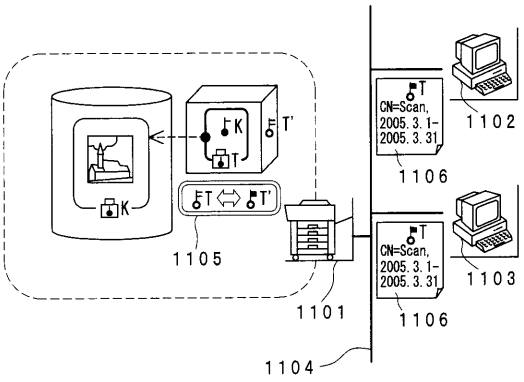
【図９】


K
A'
A
901
906
K
B'
B
902
905
A'
903
B'
904

【図１０】


S1011
K
M'
K
A'
A
1002
1006
(公開鍵Mで暗号化
された共通鍵K
K
B'
B
1001
M
M'
1003
1005
(スキャナ装置が持つ
公開鍵Mと秘密鍵M'
1004
S1012

【図１１】


K
T'
T
T
T'
1105
1101
1104
T
CN=Scan,
2005.3.1-
2005.3.31
1106
1102
1106
1103

フロントページの続き

(56)参考文献 特開２００６－１３７７６（ＪＰ，Ａ）
特開２００５－２５６３０１（ＪＰ，Ａ）
特開２００４－３３４５４２（ＪＰ，Ａ）
特開２００３－１７３３９４（ＪＰ，Ａ）
特開２０００－３０７５６４（ＪＰ，Ａ）
特開平１１－２１５３８４（ＪＰ，Ａ）
特開平１０－１５０５４１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／０８
Ｇ０９Ｃ　　１／００
Ｈ０４Ｎ　　１／４４