

(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2007-267296  
(P2007-267296A)

(43) 公開日 平成19年10月11日(2007.10.11)

(51) Int. Cl.		F I		テーマコード (参考)
HO4L	9/32	(2006.01)	HO4L 9/00 675D	5J104
HO4L	9/08	(2006.01)	HO4L 9/00 601F	

審査請求 有 請求項の数 3 O L (全 12 頁)

(21) 出願番号	特願2006-92767 (P2006-92767)	(71) 出願人	000006297 村田機械株式会社
(22) 出願日	平成18年3月30日 (2006.3.30)	(74) 代理人	100097892 弁理士 西岡 義明
		(74) 代理人	100103791 弁理士 川崎 勝弘
		(72) 発明者	石山 勝則 京都市伏見区竹田向代町136番地 村田 機械株式会社内
		Fターム(参考)	5J104 AA09 AA16 EA01 EA04 EA15 EA16 JA21 LA03 LA06 MA01 MA05 NA02 NA27 NA37 NA38

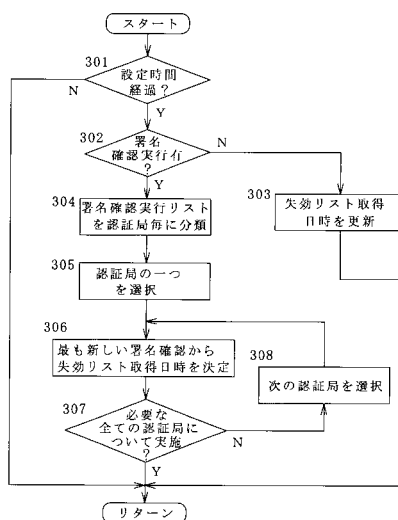
(54) 【発明の名称】 失効リスト取得機能付き通信装置

(57) 【要約】

【課題】 証明書失効リスト取得のための認証局への無駄なアクセスを減らすことが可能な失効リスト取得機能付き通信装置を提供する。

【解決手段】 前回の失効リスト取得日時から48時間が経過すると、署名確認実行リストに署名確認事象が記憶されているか否かを判定し、署名確認事象が記憶されている場合、署名確認実行リストの内容を認証局ごとに分類し、認証局の一つを選択する(ステップ301~305)。次に、選択した認証局について、最も新しい署名確認実行日時から48時間後をその認証局の失効リスト取得日時に決定し、以降、必要な全ての認証局について失効リスト取得日時を決定する(ステップ306~308)。そして、決定した失効リスト取得日時になると、自動的に認証局にアクセスして失効リストが取得される。

【選択図】 図13



**【特許請求の範囲】****【請求項 1】**

証明書失効リスト保存手段と、認証局から証明書失効リストを取得して上記証明書失効リスト保存手段に保存する制御手段とを備えた失効リスト取得機能付き通信装置であって、

上記制御手段が、あらかじめ設定した期間ごとに、失効リストが必要な事象の有無に応じて証明書失効リストの取得日時を決定することを特徴とする失効リスト取得機能付き通信装置。

**【請求項 2】**

請求項 1 に記載された失効リスト取得機能付き通信装置において、

失効リストが必要な事象が複数個あった場合、上記制御手段が、最後の事象から所定期間経過時を証明書失効リストの取得日時と決定することを特徴とする失効リスト取得機能付き通信装置。

**【請求項 3】**

請求項 2 に記載された失効リスト取得機能付き通信装置において、

上記制御手段が、失効リストが必要な事象を認証局ごとに分類し、認証局ごとに証明書失効リストの取得日時を決定することを特徴とする失効リスト取得機能付き通信装置。

**【発明の詳細な説明】****【技術分野】****【0001】**

本発明は、認証局から証明書失効リストを取得する機能を備えた失効リスト取得機能付き通信装置に関する。

**【背景技術】****【0002】**

複写機能、ファクシミリ機能、プリント機能、スキャナ機能等を有するデジタル複合機では、最近、スキャナによりスキャンした文書画像にタイムスタンプを付与して e - 文書として保存することが行われている。

すなわち、紙文書と比較してデジタルデータは改ざん等が容易であるため、タイムスタンプ技術が用いられており、このタイムスタンプは、電子文書の確定時刻を証明する技術で、その文書がいつから存在しているのか、ということと、その時点から第三者だけでなく作成者本人にも改ざんされていないことを証明するものである。

**【0003】**

このようなタイムスタンプ技術を採用する場合、電子文書のハッシュ値を時刻証明機関 (Time Stamping Authority、以下 T S A という) に送信し、T S A が送られたハッシュ値と原子時計を用いた正確な時刻の情報とを暗号化してタイムスタンプを作成するとともに、作成したタイムスタンプを電子署名とともに返送し、このタイムスタンプと電子署名を電子文書とともに e - 文書として保管するようにしている (例えば、特許文献 1 参照)。

**【特許文献 1】特開 2005 - 267083 号公報****【0004】**

そして、e - 文書を検証する場合、タイムスタンプを復号し、タイムスタンプ時刻情報の確認、及び、別途計算した当該電子文書のハッシュ値とタイムスタンプに含まれているハッシュ値とを比較することにより、改ざんの検知を行うことができる。

なお、ハッシュ値とは、与えられた原文から不可逆な一方向関数 (ハッシュ関数) を用いて生成された固定長の値で、メッセージダイジェストなどとも呼ばれる。ハッシュ値から原文を求めることや、同じハッシュ値を持つ異なった文章を作成することは極めて困難であるため、ハッシュ値を比較することで原文が同一であるかどうかの確認が可能となる。

**【0005】**

一方、上記のような時刻証明機関で暗号化を行う場合、公開鍵暗号化方式 ( P K I 、 Pu

10

20

30

40

50

blic Key Infrastructure)等の暗号化方法を利用しており、この公開鍵暗号化方式は、メッセージを暗号化するときと復号化するときとで、同一鍵(暗号アルゴリズム)を用いる共通鍵暗号方法と、異なる鍵(暗号化は公開鍵、復号化は秘密鍵)を用いる公開鍵暗号方法とが一般に知られている。

【0006】

公開鍵は、例えば認証局(CA: Certificate Authority)で正式にその保有者であるユーザとの関係が認証され不特定多数に公開された暗号鍵であり、秘密鍵は公開鍵と対をなす暗号鍵である。そして、公開鍵で暗号化したものは秘密鍵でしか復号化することができず、逆に秘密鍵を利用して暗号化したものは公開鍵でしか復号化することができない。したがって、公開鍵暗号方法を利用している時刻証明機関は秘密鍵を利用してタイムスタンプの作成及び電子署名を行っている。 10

【0007】

また、上記の認証局が発行する電子証明書は公開鍵が真正であることを証明するデータであり、真正を証明する対象の公開鍵も含んでおり、その証明書により真正が証明されている公開鍵によって、その公開鍵と対を成す秘密鍵を用いて施された電子署名をチェックすることにより、データの改ざんの有無を検出することができる。

【0008】

そして、電子署名を行う場合には、電子証明書を送信先に送信し、受信者が電子署名のチェックを行う場合、公開鍵を使用して電子署名の認証を行うと同時に、電子証明書の有効性を確認するが、電子証明書は、本人の申告、認証局の処分、法定の理由等により失効する。例えば、秘密鍵を格納したICカード等が盗難にあたり、紛失した場合には、本人の通告により電子証明書は失効し、また、電子証明書に記載されている内容に変更があった場合には、認証局が電子証明書を失効させる。 20

【0009】

したがって、電子署名をチェックする場合には、電子証明書が失効していないか確認する必要があり、また、電子署名を実行する場合にも電子証明書が失効していないか確認する必要がある。

このため、一般的な認証局では、CRLと呼ばれる電子証明書の失効リストを定期的に発行しており、証明書失効リストを利用して電子証明書の有効性の検証を行う者は、通常、認証局が発行した証明書失効リストを端末装置にダウンロードし、ローカルに保存した証明書失効リストから検証対象の電子証明書の状態を検索し、電子証明書の有効性を検証するようにしている。 30

【発明の開示】

【発明が解決しようとする課題】

【0010】

上記のように、e-文書を検証する場合、認証局の発行する証明書失効リストにより電子証明書の有効性を確認しなければならないが、証明書失効リストを取得する場合、ほとんどが同じ認証局へのアクセスが予想され、必要な時に認証局へアクセスすると、無駄が多くなるという問題があった。

また、認証局での証明書失効リストの発行は1日1回程度と間隔が長いため、複数の確認要求に対して同じデータを取得することになり、同様に、無駄が多くなるという問題があった。 40

【0011】

本発明は、上記の問題に鑑みてなされたもので、証明書失効リスト取得のための認証局への無駄なアクセスを減らすことが可能な失効リスト取得機能付き通信装置を提供することを目的とする。

【課題を解決するための手段】

【0012】

上述の目的を達成するため、請求項1に係る発明の失効リスト取得機能付き通信装置は、証明書失効リスト保存手段と、認証局から証明書失効リストを取得して上記証明書失効 50

リスト保存手段に保存する制御手段とを備えた失効リスト取得機能付き通信装置であって、上記制御手段が、あらかじめ設定した期間ごとに、失効リストが必要な事象の有無に応じて証明書失効リストの取得日時を決定することを特徴とする。

【0013】

また、請求項2に係る発明の失効リスト取得機能付き通信装置は、請求項1に記載された失効リスト取得機能付き通信装置において、失効リストが必要な事象が複数個あった場合、上記制御手段が、最後の事象から所定期間経過時を証明書失効リストの取得日時と決定することを特徴とし、

請求項3に係る発明の失効リスト取得機能付き通信装置は、請求項2に記載された失効リスト取得機能付き通信装置において、上記制御手段が、失効リストが必要な事象を認証局ごとに分類し、認証局ごとに証明書失効リストの取得日時を決定することを特徴とする。

10

【発明の効果】

【0014】

本発明の請求項1に係る発明の失効リスト取得機能付き通信装置によれば、あらかじめ設定した期間ごとに、失効リストが必要な事象の有無に応じて証明書失効リストの取得日時が決定されるので、証明書失効リスト取得のための認証局への無駄なアクセスを減らすことができる。

【0015】

また、本発明の請求項2、請求項3に係る発明の失効リスト取得機能付き通信装置によれば、失効リストが必要な事象が複数個あった場合、認証局ごとに事象を分類し、各認証局について最後の事象から所定期間経過時が証明書失効リストの取得日時と決定されるので、さらに証明書失効リスト取得のための認証局への無駄なアクセスを減らすことが可能となる。

20

【実施例】

【0016】

以下、本発明の失効リスト取得機能付き通信装置をデジタル複合機に適用した実施例について説明する。図1はデジタル複合機を備えたシステムのネットワーク構成例を示す図であり、図2はデジタル複合機のハードウェア構成を示すブロック図である。

【0017】

図1に示すネットワーク構成図において、1はデジタル複合機、2、3、4・・・はパソコン、5は公衆交換電話網(PSTN)、6はLAN(Local Area Network)、7はインターネット網、8はTSA、9は認証局である。デジタル複合機1はコピーモード、プリンタモード、ファクスモードの各機能を備えるとともに、メール送信機能も備え、PSTN5及びLAN6に接続されており、このLAN6に端末装置として複数のパソコン2、3、4・・・が接続されている。このLAN6はインターネット網7にも接続されており、デジタル複合機1はこのインターネット網7を介してメールの送受信を行うことが可能である。

30

【0018】

また、TSA8は時刻証明機構であり、インターネット網7を介してデジタル複合機1からスキャンデータのハッシュ値を受信すると、受信したハッシュ値を原子時計を用いた正確な時刻の情報とともに、TSA8の秘密鍵を用いて暗号化してタイムスタンプを作成し、作成したタイムスタンプ、電子署名、及びタイムスタンプ用秘密鍵の電子証明書をデジタル複合機1に返送する。

40

また、認証局9は、TSA等の利用者と公開鍵の対を認証局の秘密鍵によって電子署名した「電子証明書」を発行し、電子署名を検証する側では、電子証明書の署名を検証して公開鍵が正当なものであるかどうかを確認する。なお、この認証局9は、CRLと呼ばれる電子証明書の失効リストを定期的に発行している。

【0019】

デジタル複合機1は、図2に示すように、CPU11、ROM(Read Only Memory)

50

12、RAM (Random Access Memory) 13、表示・操作部 14、読取部 15、画像メモリ 16、記録部 17、コーデック 18、モデム 19、ネットワーク制御ユニット NCU 20、LAN インターフェース (I/F) 21 及び e - 文書保存部 22 から構成され、各部がバス 23 を介して接続されている。

【0020】

CPU 11 はバス 23 を介してデジタル複合機 1 のハードウェア各部を制御するとともに、ROM 12 に記憶されたプログラムに基づいて各種のプログラムを実行し、ROM 12 はデジタル複合機の動作に必要な種々のプログラムや操作メッセージ等を予め記憶している。また、RAM 13 はSRAM 等で構成され、プログラムの実行時に発生する一時的なデータを記憶する。

10

【0021】

表示・操作部 14 は、デジタル複合機 1 の動作状態を表示したり、種々の機能の操作画面の表示を行う表示部と、デジタル複合機 1 を操作するための複数のキーよりなり、図 3 に示すように、表示部を構成するLCD 表示部 31 と多数の操作キーから構成されている。LCD 表示部 31 には、タッチパネルスイッチが配設され、LCD 表示部 31 に表示された項目部分を押下することで、対応する項目の選択や機能の実行を行うことができる。また、操作キーとして、テンキー 32、スタートキー 33、リセットキー 34、ストップキー 35、複数のワンタッチダイヤルキー 36、十字キー 37、リターンキー 38、セットキー 39、FAX 切替キー 40、コピー切替キー 41、スキャナ切替キー 42 等の各種キーが設けられている。なお、LCD 表示部 31 によりこれらの操作キーの一部又は全部を代用することも可能である。

20

【0022】

読取部 15 はオートドキュメントフィーダー (ADF) やフラットベッドスキャナ (FBS) 等の読取り用原稿載置台を備え、CCD 等を利用したスキャナで原稿を読み取り、ドットイメージデータを出力する。

また、画像メモリ 16 は、DRAM 等を用いて構成され、送信すべき画像データまたは受信した画像データあるいは読取部 15 で読み取った画像データを記憶し、記録部 17 は電子写真方式等のプリンタ装置を備え、受信したデータ、コピー原稿データあるいは外部のパソコン 2、3、4 等から送信されたプリントデータをプリントアウトする。

【0023】

コーデック 18 は所定のプロトコルに対応して符号化・復号するものであり、読み取った原稿の画像データを送信するために MH、MR または MMR 方式により符号化し、外部から受信した画像データを復号するとともに、電子メールに添付可能なファイルとして一般的に利用される画像フォーマットである TIFF 方式等にも対応して符号化、復号する。

30

【0024】

モデム 19 はバス 23 に接続されており、ファクシミリ通信が可能なファクスモデムとしての機能を有し、このモデム 19 は同様にバス 23 に接続された NCU 20 と接続されている。NCU 20 はアナログ回線の閉結及び開放の動作を行うハードウェアであり、必要に応じてモデム 19 を PSTN 5 に接続する。

40

LAN インターフェース 21 は LAN 6 に接続され、インターネット網 7 からの信号を受信する一方、LAN 6 に対して信号やデータを送信するものであり、信号変換やプロトコル変換などのインターフェース処理を実行する。

【0025】

一方、e - 文書保存部 22 は、e - 文書を文書の種類ごとに保存する記憶部であり、図 4 に示すように、e - 文書の管理ファイルと、帳簿、見積書、注文書、議事録等の文書毎のフォルダとを備え、各文書フォルダには、文書名を識別できる文字列と日付、通番を組み合わせたファイル名が付与されたファイルに、スキャン文書、タイムスタンプ及び電子署名が保存される。また、管理ファイルには、図 5 に示す、各 e - 文書のファイル名と、タイムスタンプの有効期限、当該 e - 文書の保存期限が記憶されたファイルと、図 6 に示

50

す、各 T S A の公開鍵、電子証明書名、認証局名が記憶されたファイルと、図 7 に示す、各認証局が発行する失効リストのファイル、及び、図 8 に示す、電子署名確認の実行日時、e - 文書名、証明書名、認証局名を記憶する署名確認実行リストのファイルとを備えている。

#### 【 0 0 2 6 】

デジタル複合機 1 は上記のような構成を備えており、ファクシミリ送信時には、原稿の画像データが読取部 1 5 で読み取られ、コーデック 1 8 で圧縮されて画像メモリ 1 6 に蓄積される。この圧縮された画像データが画像メモリ 1 6 から読み出されてモデム 1 9 で変調され、N C U 2 0 から P S T N 5 を通して通信相手先に送信される。また、ファクシミリ受信時には、受信した画像データがモデム 1 9 で復調され、画像メモリ 1 6 に蓄積された後、コーデック 1 8 で復号されて記録部 1 7 により印刷される。

10

#### 【 0 0 2 7 】

一方、このデジタル複合機は、上記のように文書をスキャンして e - 文書として保存することができるようになっており、以下、e - 文書スキャン時の作用について説明する。

ユーザが表示・操作部 1 4 の L C D 表示部 3 1 で e - 文書スキャンを指示すると、表示・操作部 1 4 の L C D 表示部 3 1 に図 9 に示す e - 文書スキャンの文書種類選択画面が表示される。

この画面には、帳簿 e - 文書スキャン、見積書 e - 文書スキャン、注文書 e - 文書スキャン等の e - 文書スキャンを行う文書の種類を選択する画面が表示されており、いずれかの e - 文書スキャンを押下して選択した後、「実行」ボタンを押下することにより、デジタル複合機 1 が e - 文書スキャンを実行する。

20

#### 【 0 0 2 8 】

図 1 0 は e - 文書スキャン実行時の C P U 1 1 の作用を示すフローチャートであり、いずれかの文書種類の e - 文書スキャンを選択した後、「実行」ボタンを押下すると、C P U 1 1 は図 1 0 のフローチャートに示す e - 文書スキャンプログラムを開始し、原稿の画像データを読取部 1 5 で読み取り、コーデック 1 8 で圧縮して画像メモリ 1 6 に蓄積する（ステップ 1 0 1 ）。

次に、C P U 1 1 は、画像メモリ 1 6 に蓄積したデータのハッシュ値を算出した後、このハッシュ値データを L A N インターフェース 2 1、L A N 6、インターネット網 7 を介して T S A 8 に送信することにより、タイムスタンプの発行を依頼する（ステップ 1 0 2 ）。

30

#### 【 0 0 2 9 】

そして、タイムスタンプの発行を依頼した後、C P U 1 1 は、T S A 8 からタイムスタンプを受信したか否かを判定し（ステップ 1 0 3 ）、T S A 8 からタイムスタンプを受信すると、当該文書の種類に応じたファイル名、例えば、図 9 の e - 文書スキャンの文書種類選択画面で、帳簿 e - 文書スキャンを選択していた場合、ファイル名を「chobo」+「日付」+「連番」により作成し、作成したファイル名によりスキャンデータ、タイムスタンプ及び電子署名を帳簿フォルダに保存するとともに、管理ファイルにファイル名、タイムスタンプの有効期限、e - 文書の保存期限を記憶する（ステップ 1 0 4 ）。

なお、文書の保存期間は、文書の種類ごとに、例えば、帳簿 1 0 年間、注文書 5 年間等と指定できるので、保存期限は e - 文書の作成日とその種類の文書の保存期間とにより自動的に決定することができる。

40

#### 【 0 0 3 0 】

次に、ユーザが、e - 文書保存部 2 2 に保存された文書をプリント出力する場合の作用について説明する。

ユーザが表示・操作部 1 4 の L C D 表示部 3 1 で e - 文書のプリント出力を指示すると、表示・操作部 1 4 の L C D 表示部 3 1 に e - 文書の種類選択画面が表示され、この画面で例えば、帳簿 e - 文書を指定すると、図 1 1 に示すように、帳簿 e - 文書の一覧リストが表示される。

この画面には、帳簿 e - 文書に含まれる文書の一覧が表示されているので、この中から

50

所望の文書を押下して選択した後、「実行」ボタンを押下することにより、当該文書のプリントを行うことができる。なお、多数の帳簿 e - 文書が保存されている場合には、「次頁」ボタンを押下することにより、次の頁の帳簿 e - 文書を表示することができる。

**【0031】**

図12は e - 文書プリント実行時の CPU 11 の作用を示すフローチャートであり、いずれかの e - 文書を選択した後、「実行」ボタンを押下すると、CPU 11 は図12のフローチャートに示す e - 文書プリントプログラムを開始し、まず、当該文書のタイムスタンプを e - 文書保存部 22 から読み出し、復号した（ステップ 201）後、当該 e - 文書の検証を行う（ステップ 202）。

**【0032】**

すなわち、当該 e - 文書の検証を行う場合、復号されたタイムスタンプ時刻情報の確認、及び、別途計算した当該 e - 文書データのハッシュ値とタイムスタンプに含まれているハッシュ値とを比較することにより、改ざんの検知を行うとともに、電子署名のチェックを行う。この電子署名のチェックは、公開鍵を使用して電子署名の認証を行うと同時に、e - 文書保存部 22 の管理ファイルに保存されている、図7の失効リストを参照することにより、タイムスタンプを発行した TSA の電子証明書が失効していないかを確認することにより電子証明書の有効性を確認する。

**【0033】**

次に、CPU 11 は、当該 e - 文書が有効か否かを判定し（ステップ 203）、当該 e - 文書のハッシュ値とタイムスタンプに含まれているハッシュ値とが異なっている場合、あるいは、電子証明書が失効していた場合には、LCD 表示部 31 に、当該 e - 文書が無効である旨を表示した（ステップ 204）後、プログラムを終了する。

一方、当該 e - 文書が有効であると判定した場合、CPU 11 は、当該 e - 文書のデータをコーデック 18 で復号して記録部 17 により印刷した（ステップ 205）後、e - 文書保存部 22 の管理ファイルに、図8に示すように、署名確認の実行日時、e - 文書名、電子証明書名、認証局名を記憶し（ステップ 206）、プログラムを終了する。

**【0034】**

一方、デジタル複合機 1 は、定期的に証明書失効リストの取得が必要か否かを判定しており、証明書失効リストの取得が必要となった場合には、各認証局ごとに失効リスト取得日時を決定する。

すなわち、デジタル複合機 1 の CPU 11 は、常時、図13のフローチャートに示す失効リスト取得日時決定プログラムを実行しており、このプログラムを開始すると、設定時間、例えば、RAM 13 に記憶されている前回の失効リスト取得日時から 48 時間が経過したか否かを判定し（ステップ 301）、前回の失効リスト取得日時から 48 時間が経過していないと判定した場合、プログラムを終了する。

**【0035】**

一方、ステップ 301 で前回の失効リスト取得日時から 48 時間が経過したと判定した場合、CPU 11 は、署名確認実行リストに署名確認事象が記憶されているか否かを判定し（ステップ 302）、署名確認実行リストに署名確認事象が記憶されていないと判定した場合、失効リスト取得日時をその時点の日時に更新して RAM 13 に記憶した（ステップ 303）後、プログラムを終了する。

**【0036】**

ステップ 302 で署名確認実行リストに署名確認事象が記憶されていると判定した場合、CPU 11 は、図8の署名確認実行リストの内容を認証局ごとに分類した（ステップ 304）後、認証局の一つを選択する（ステップ 305）。次に、CPU 11 は、選択した認証局について、最も新しい署名確認実行日時からその認証局の失効リスト取得日時を決定する（ステップ 306）。

例えば、ある認証局について、図14に示すように、「3月27日13時」、「3月27日17時」、「3月28日10時」に署名確認を行っていた場合、CPU 11 は「3月28日10時」から 48 時間後、すなわち、「3月30日10時」をその認証局の失効リ

10

20

30

40

50

スト取得日時と決定し、当該認証局の名称とともに R A M 1 3 に記憶する。

【 0 0 3 7 】

次に、C P U 1 1 は、必要な全ての認証局について失効リスト取得日時を決定したか否かを判定し（ステップ 3 0 7）、未だ失効リスト取得日時を決定していない認証局が残っている場合には、次の認証局を選択した（ステップ 3 0 8）後、ステップ 3 0 6 に戻ってその認証局の失効リスト取得日時を決定し、失効リスト取得日時を決定していない認証局が残っていない場合には、プログラムを終了する。

【 0 0 3 8 】

また、デジタル複合機 1 は、上記の証明書失効リストの取得日時決定プログラムとは別個に、常時、証明書失効リストの取得プログラムを実行し、必要な場合には、認証局にアクセスして証明書失効リストを取得する。 10

すなわち、デジタル複合機 1 の C P U 1 1 は、常時、図 1 5 のフローチャートに示す失効リスト取得プログラムを実行しており、このプログラムを開始すると、現在時刻と R A M 1 3 に記憶されている失効リスト取得日時とを比較することにより、失効リスト取得日時になったか否かを判定し（ステップ 4 0 1）、失効リスト取得日時になっていないと判定した場合、プログラムを終了する。

【 0 0 3 9 】

一方、ステップ 4 0 1 で現在時刻が失効リスト取得日時であると判定した場合、C P U 1 1 は、R A M 1 3 に記憶されている失効リストの取得先の認証局 9 に L A N インターフェース 2 1、L A N 6、インターネット網 7 を介してアクセスし、証明書失効リストの取得を要求する（ステップ 4 0 2）。この後、C P U 1 1 は、認証局 9 から証明書失効リストを取得したか否かを判定し（ステップ 4 0 3）、失効リストを取得したと判定すると、取得した失効リストを e - 文書保存部 2 2 の管理ファイルの当該認証局の失効リスト記憶領域に保存する（ステップ 4 0 4）。 20

【 0 0 4 0 】

次に、C P U 1 1 は、失効リスト取得日時をその時点の日時に更新した（ステップ 4 0 5）後、署名確認実行リストに含まれている e - 文書の証明書が失効リストに含まれているか否かを判定することにより、当該 e - 文書が無効か否かを判定する（ステップ 4 0 6）。当該 e - 文書が無効であると判定した場合、C P U 1 1 は、該当する T S A 及び該当する e - 文書が無効である旨のテキストデータを作成して記録部 1 7 によりプリント出力する（ステップ 4 0 7）。 30

また、ステップ 4 0 6 で署名確認実行リストに含まれている e - 文書の証明書が失効リストに含まれていないと判定した場合、または、ステップ 4 0 7 で該当する T S A、e - 文書が無効である旨をプリント出力した後、C P U 1 1 は、署名確認実行リストの内容の内、失効リストを取得した認証局に関するものを削除し（ステップ 4 0 8）、プログラムを終了する。

【 0 0 4 1 】

以上のように、失効リストの取得が必要な署名確認が実行されていた場合、あらかじめ設定した期間ごとに、証明書失効リストの取得日時が決定されるので、証明書失効リスト取得のための認証局への無駄なアクセスを減らすことができ、また、失効リストの取得が必要な署名確認が複数実行されていた場合には、認証局ごとに署名確認を分類し、各認証局について最後の署名確認から所定期間経過時が証明書失効リストの取得日時と決定されるので、さらに証明書失効リスト取得のための認証局への無駄なアクセスを減らすことができる。 40

【 0 0 4 2 】

なお、上記の実施例では、署名確認を実行した e - 文書が無効であると判定した場合、該当する T S A 及び該当する e - 文書が無効である旨をプリント出力したが、デジタル複合機の表示部に該当する T S A 及び e - 文書が無効である旨を表示するようにしてもよい。

【 0 0 4 3 】

また、上記の実施例では、前回の失効リスト取得日時から48時間が経過したときに証明書失効リストの取得が必要か否かを判定したが、前回の失効リスト取得日時から24時間が経過したときに証明書失効リストの取得が必要か否かを判定してもよく、さらに、上記の実施例では、最も新しい署名確認実行日時から48時間後を失効リスト取得日時と決定したが、最も新しい署名確認実行日時から1時間後を失効リスト取得日時とする等、時間間隔は適宜変更することが可能である。

【0044】

また、上記の実施例では、本発明の失効リスト取得機能付き通信装置をデジタル複合機に適用した例について説明したが、本発明の失効リスト取得機能付き通信装置はファクシミリサーバー装置やe-文書サーバー等にも適用することが可能である。

10

さらに、上記の実施例では、e-文書の検証実施に失効リストを使用する場合の例について説明したが、電子メールの送信時や受信時の署名検証時に失効リストを使用するメールサーバー等にも、本発明の失効リスト取得機能付きサーバー装置を適用することが可能である。

【図面の簡単な説明】

【0045】

【図1】デジタル複合機を備えたシステムのネットワーク構成例を示す図である。

【図2】デジタル複合機のハードウェア構成を示すブロック図である。

【図3】表示・操作部の詳細な構成を示す図である。

【図4】e-文書を保存する記憶部のファイル構造を示す図である。

20

【図5】管理ファイルに保存されるe-文書データの一例である。

【図6】管理ファイルに保存されるTSAの情報の一例である。

【図7】管理ファイルに保存される各認証局の失効リストの一例である。

【図8】管理ファイルに保存される署名確認実行リストの一例である。

【図9】e-文書スキャンの文書種類選択画面の一例である。

【図10】e-文書スキャンプログラムの作用を示すフローチャートである。

【図11】帳簿e-文書の一覧リストの表示例である。

【図12】e-文書プリント実行時の作用を示すフローチャートである。

【図13】失効リスト取得日時決定プログラムの作用を示すフローチャートである。

【図14】署名確認実行の時間経過の一例である。

30

【図15】失効リスト取得プログラムの作用を示すフローチャートである。

【符号の説明】

【0046】

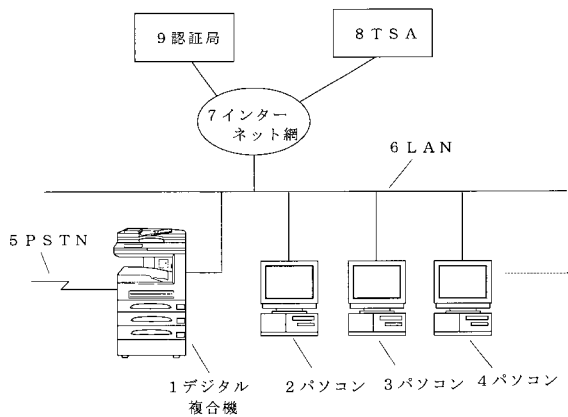
- 1 デジタル複合機
- 2、3、4 パソコン
- 5 P S T N
- 6 L A N
- 7 インターネット網
- 8 T S A
- 9 認証局
- 11 C P U
- 12 R O M
- 13 R A M
- 14 表示・操作部
- 15 読取部
- 16 画像メモリ
- 17 記録部
- 18 コーデック
- 19 モデム
- 20 N C U

40

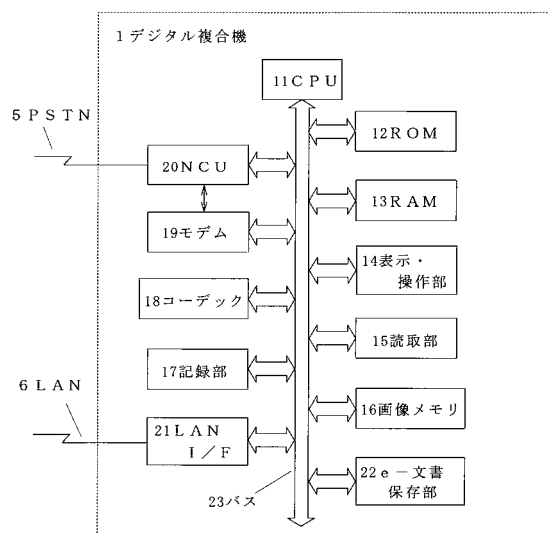
50

- 2 1 LAN I / F
- 2 2 e - 文書保存部
- 2 3 バス

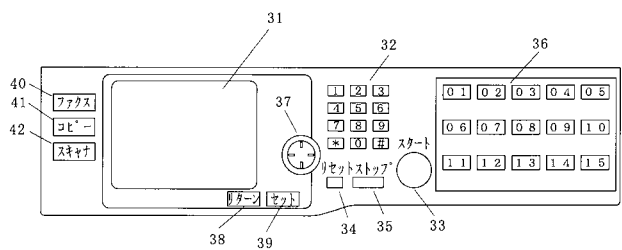
【 図 1 】



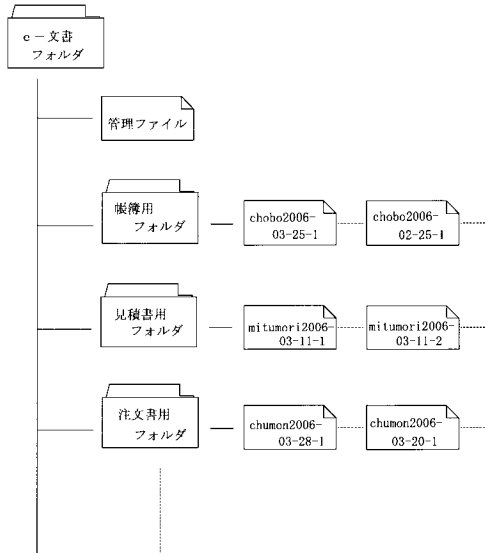
【 図 2 】



【 図 3 】



【 図 4 】



【 図 5 】

No	File名	有効期限	保存期限
1	Chobo2006-03-25-1	2009.03.25	2016.03.25
2	Chobo2006-02-25-1	2009.02.25	2016.02.25

【 図 6 】

時刻証明機関	公開鍵	電子証明書	認証局
T S A a	123456789	aaaaaaa	xxxセキュリティ
T S A b	987654321	bbbbbbb	ootセキュリティ
T S A c	102030405	ccccccc	ssセキュリティ

【 図 7 】

認証局	失効リスト
xxxセキュリティ	-----
ootセキュリティ	-----
ssセキュリティ	-----

【 図 8 】

	日付	e-文書	証明書	認証局
1	2006.03.28 10:00	Chobo2006-03-25-1	aaaaaaa	xxxセキュリティ
2	2006.03.27 17:00	Chobo2006-02-25-1	aaaaaaa	xxxセキュリティ
	2006.03.27 13:00	Chobo2006-01-25-1	aaaaaaa	xxxセキュリティ

【 図 9 】

e-文書スキャンを実行します。

帳簿 e-文書スキャン

見積書 e-文書スキャン

注文書 e-文書スキャン

実行      取消し

【 図 1 1 】

帳簿 e-文書リスト

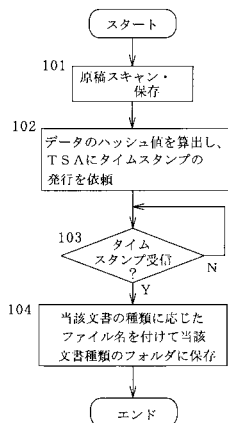
chobo2006-03-25-1

chobo2006-02-25-1

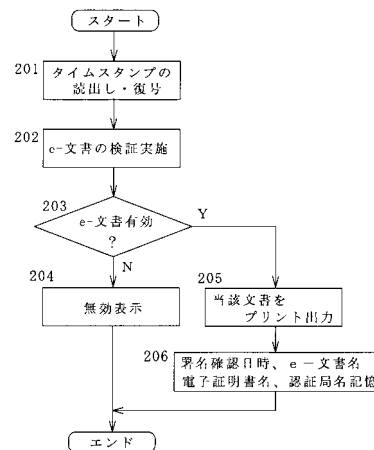
chobo2006-01-25-1

実行      次頁      取消し

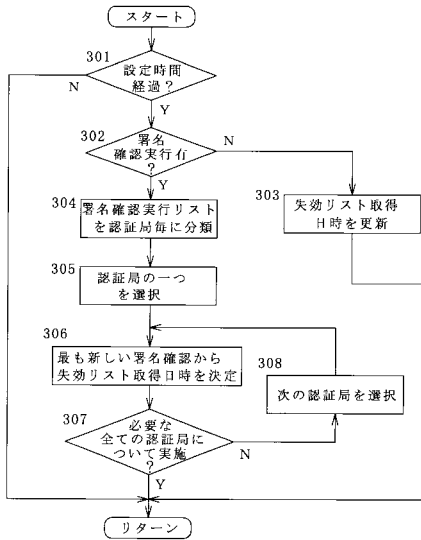
【 図 1 0 】



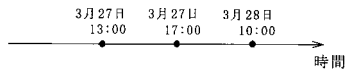
【 図 1 2 】



【図13】



【図14】



【図15】

