

(51)Int.Cl. <sup>6</sup>	識別記号	F I	
H 0 4 N	1/40	H 0 4 N	1/40 Z
G 0 3 G	21/04	G 0 6 F	15/66 B
G 0 6 T	1/00	G 0 3 G	21/00 5 5 4

審査請求 未請求 予備審査請求 有 (全 48 頁)

(21)出願番号 特願平8-529025  
 (86)(22)出願日 平成8年(1996)3月29日  
 (85)翻訳文提出日 平成9年(1997)9月29日  
 (86)国際出願番号 PCT/FR96/00481  
 (87)国際公開番号 WO96/31049  
 (87)国際公開日 平成8年(1996)10月3日  
 (31)優先権主張番号 95/03668  
 (32)優先日 1995年3月29日  
 (33)優先権主張国 フランス (FR)  
 (81)指定国 EP(AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), JP, US

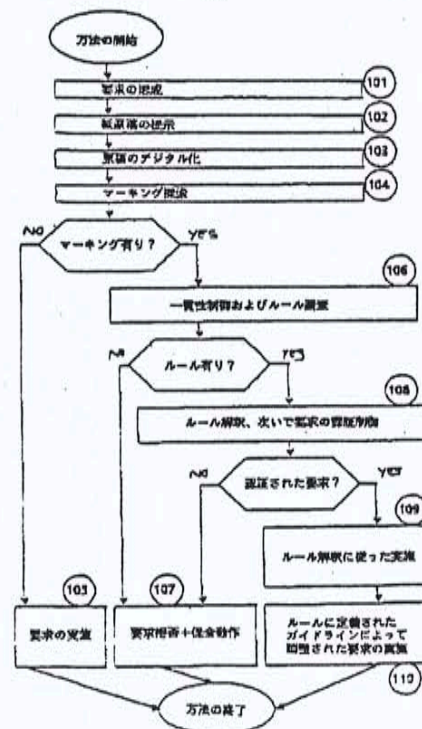
(71)出願人 ランク ゼロックス エスアー  
 フランス国、93586 サーン カーン セ  
 デ、リュ トゥーゼ 7  
 (72)発明者 ラーミ ポール  
 フランス国、91160 ラーンジュモー、リ  
 ユ アドルフ アダム 25  
 (74)代理人 弁理士 山本 亮一

(54)【発明の名称】 機密文書の安全な複製方法

(57)【要約】

本発明は、エンコードされた「ルール」によって完成された文書の機密性を同定する一方、複製制限を定義する「マーキング」の定義と、機密文書(102)の複製要求(101)中におけるマーキング(104)の存在の決定および複製制限(106)の探索のための前記文書(103)のデジタル化とからなる。認証制御(108)の後の複製はこれらの制限(109)に従って実施される(110)。複製は前記文書の発行者に関連した電子的原稿の探索によって得ることができる。本発明は特に文書の複製によるハッキングおよびある種の文書の同一の複製を妨げ、著作権管理を認証する。これは発行者が改竄の心配をすることなく、あらゆる作成された機密文書の使用を管理し続けることを可能にする。

図1





## 【特許請求の範囲】

1. 文書を複製するための方法であって、機密と考えられる文書に予め付加的な特定のグラフィック要素である「マーキング」および「ルール」を付加すること、および以下の工程

- 実施すべき複製作業の定義要求(101)、
- 原稿文書の提示(102)、
- 原稿文書のデジタル化(103)、
- 文書の「通常性」もしくは「機密性」を決定するための文書の可能な「マーキング」を検出するためのデジタル化の結果の分析(104)、
- 前工程後に文書が「機密文書」と同定された場合、「ルール」を探索および解読するための補完的な分析(106)、異常時には要求の拒絶(107)

-前工程後に文書が「機密文書」と同定された場合、「ルール」に定義された要素と要求および要求者の特徴づける要素に関する要求の認証管理(108)、異常時には要求の拒絶(107)、

-前工程後に、文書が「機密文書」と同定され、要求が認証された場合、要求者によって与えられる補完的要素と組み合わせられた、「ルール」で定義された動作もしくはそれらに由来する動作の実行(109)、

-提示された文書が「通常文書」(105)である場合および、提示された文書が、「ルール」の解釈に由来するガイドラインによれば「機密文書」(110)であって複製が認証される場合、要求された複製の作成を順に実施することを特徴とする方法。

2. 請求項1による方法を実施するための装置であって、以下の機能モジュール

-利用者がその要求および自身を正確に定義することを可能にする「ユーザインタフェースモジュール」(11)、

-提示された文書のコンピュータ操作を可能にするために基本的な黒色お

よび白色の点への分解もしくは場合によってはカラーもしくは赤外線属性の付与

モジュール(20)とを含むことを特徴とする請求項4記載の装置。

6. さらに、「認証可能な文書」の提示および提示された文書にリンクされた「保管サーバ」(73)への要求に際して「文書サーバ」上で発現された要求の実行中に、認証されたコピーもしくは取引を受信しなければならない任意のコンピュータシステム上に組み込まれた「処理モジュール」(87)を含むことを特徴とする請求項5記載の装置。

を行う「デジタル化モジュール」(12)、

-認証された時に、利用者によって定義された紙コピーを対応する電子手段から構築する「印刷モジュール」(14)、

-コンピュータモジュールである「分析モジュール」(16)、「制御モジュール」(15)および「形成モジュール」(17)であって、分析モジュールはデジタル化された文書からの「マーキング」および「ルール」の検出および解読に適したアルゴリズムを含み、「制御モジュール」は全モジュールの駆動制御および結合を保証し、「形成モジュール」は、(認証された場合に)原稿文書のデジタル画像から、原稿のルールに含まれた変形ガイドラインを尊重しながら、「マーキング」および「ルール」のない作成すべき文書のデジタル化画像を形成し、このように構築された文書はそれ自体の「マーキング」および「ルール」を備えているものを組み合わせたことを特徴とする装置。

3. さらに、文書の複製に要する任意の電子ファイルを2つの同一の「文書サーバ」(1)間で対話および交換させることを可能にする「通信モジュール」(18)および、要求されたコピーがコピーを作成する「文書サーバ」の外部からの要求に由来する場合に作動されるコンピュータモジュールであって、作成されるべき文書を保持し、受信先が受信側「文書サーバ」であることを自ら同定した場合のみ、これを解放する「出力管理モジュール」(19)を含むことを特徴とする請求項2記載の装置。

4. 機密文書を印刷しなければならない任意のコンピュータシステム(72)に付加された「ドライバ」(82)をさらに含み、前記ドライバは所望の紙文書の構築に必要な全ファイルおよび特徴を「文書サーバ」(1)の「通信モジュール」(18)に送られるために提供されていることを特徴とする請求項3記載の装置。

5. さらに、「認証可能な文書」(92)の作成中に前記「認証可能な文書」からの認証されたコピーの作成のための要求が発現された時に復元用にその電子的同等物(91)を保存する「保管サーバ」(73)と、任意の「文書サーバ」(

3)から任意の「保管サーバ」(73)へのアクセスを管理する「ディレクトリ

## 【発明の詳細な説明】

## 機密文書の安全な複製方法

本発明は文書複製または遠隔頒布装置による産業スパイ等の容易性を妨げることのできるものである。本発明は文書中における補完的なグラフィック要素の形成と、適合させた方法の概念とを組み合わせることによって、ある種の機密文書の作成もしくは頒布を禁止または管理し、原稿とそのコピーとの区別を容易にするために固有の値を有するいくつかの文書のコピーを所定のガイドラインに従って変更し、著作権に関する経費の支払いがある場合にいくつかの文書の複製もしくは頒布を認可し、原稿発行者によって留保された電子的原稿の直接の複製によって紙の原稿もしくはそのコピーを認証し、紙の原稿から電子的コピーを作成し、あるいは原稿文書の発行者によって管理された電子的取引を行い、全体的な文書の全体もしくはその一部のコピーをその技幹から作成することを可能にする。

これらの目的のため、本発明の中核は以下の機能、すなわち、文書を獲得し、複製要求を発現し、文書中の機密性を検出するために獲得文書の処理を行い、場合によっては文書に関連した複製規則を抽出し、複製規則を管理および適用し、もし電子的原稿の探索によって要求されれば、コピーされた文書を作成し、場合によっては、複製規則および発現された要求に従って、電子的コピーを作成し、もしくは電子的取引を実行することにある。

現在、文書作成もしくは複製の様々な特徴的要素においては文書に含まれた情報の機密性もしくは作成された文書の使用に関して、以下のような、いくつかの危険性が存在する。

A-企業に由来する紙原稿はいずれもその企業内のコピー機で簡易かつ迅速にコピーすることができる。原稿が消失しないため、そのコピーはいかなる痕跡も残すことなく容易に社外に運んで企業に損害を与えることができる。

B-企業に由来する原稿はいずれもファクシミリシステムを用いて、その簡

便のいかなる痕跡も残すことなく遠隔複製して企業に極めて大きな損害を与えることができる。

C-カラー複写システムは現在でも、また将来はより効率的な技術の統合に



よってますます、原稿に極めて忠実なコピーを作成することが可能であり、かなり豊富な専門的技術に頼ることなくコピーと原稿との区別を行うことは困難である。

D-管理、財務もしくは取引に関する文書は、検知不可能な修正もしくは改竄によって、元の文書の粉飾をもたらす変造を伴う権利の悪用（納税書式、出生証明書、徴収書、契約書、請求書、小切手等）を可能にする。

E-現在原稿の頒布のみに関して報酬を受け、これら原稿のコピーについては報酬を受けていない著者は、ある種の文書については多大な労力を強いられている。

F-ある種の文書もしくはそれらが抽出される全体的な文書はそれらの性質（製本、切り抜き等）もしくはそれらの劣化（不完全な文書、部分的頒布）のため、それらの所有者によって容易にコピーできない。

G-共同プリンタで作成されるコンピュータ関連文書はいずれも機密性の高いものであったとしても、その作成時とその所有者による回収時の間に第三者によって故意もしくは偶然に見られてしまうことがある。

これら文書の頒布および使用の安全性に関する問題の全てに対して現在適用されている以下の従来の解決法はあまり効率的ではないが、取り扱いにくいものである。

A/B-これらの点は企業の戦略的文書の過剰な管理（錠と鍵）もしくは複製手段へのアクセス制限によってのみ解決される。これは、ある種の文書の戦略的重要性評価が低いこと、もしくはその保護にまれにしか適用されない困難な規律のため、効果的でないことが多い。

C-保護は、高度なグラフィック性あるいは適用が困難なもしくは高価な特定の媒体もしくは技術（金属線、磁気インクもしくは軌跡、ホログラム等）の使用によって確保される。これらの解法の複雑性によって、それらの使用は制限され、熟練者のみが正偽を区別可能であることが多い。

D-現在、発行当局に対して文書で確認要求を行った場合にのみ絶対的なものになる認証済みコピーのみが相対的な安全性を与える。このプロセスは困難で

(8) 特表平11-509995

と称する。

一第5のカテゴリはそれと同一なコピー（もしくはほぼ同一な）コピーによって、可能なコピーの派生的使用により、原稿の発行者に損害が生じ得るあらゆる文書に関する。実際の文書のみが価値を有するが、それが含む情報には価値がない。このカテゴリは銀行券、チケットおよび他の固有の価値を有する文書が含まれる。このカテゴリは以下「価値のある文書」と称する。

「通常文書」以外の文書の全カテゴリを総称するため、「機密文書」という一般的なカテゴリを使用する。

さらに、以下、紙媒体上の通常文書に関する紙文書と、紙文書への印刷要求後に対応する文書の電子ファイル形式にある全ての定義に対応する電子的要素を特徴づける電子文書とを区別する。

本発明を記載するにあたり、文書のデジタル形式を参照する。紙文書に関し、これは黒色もしくは白色の基本点への分解を意味するか、もしくはカラー属性によって定義される。この分解により、ファイルの電子的保存が可能になり、論理的処理の機会が得られる。

本発明の主な特徴は、処理すべき文書の付加的な特定のグラフィック要素の定義と実際の処理の定義とに基づく以下の方法にある。

文書において、新たな要素は

- マーキングと
- ルールである。

「マーキング」とは「機密文書」と「通常文書」とを区別することを可能にする要素である。この「マーキング」は、実際の文書の可読性を妨げないが文書の縮小部分でも検知可能でなければならない全文書の特有のグラフィック性（可視か否か）によって達成される。この「マーキング」は「機密文書」と考えられる

任意の文書上に存在し、したがって、任意の「通常文書」に欠けている。

ルールは全ての「機密文書」に関する要素であって、その関連する文書の複製に関するルールおよび制限を定義するものである。この要素は以下「ルール」と称する。複製ルールおよび制限には「ルール」として統合されるべき与えられた

あり、例外的に、また既に疑惑のある場合にのみ実施されることが多い。

E-著者の保護に関する法律のみがこのようなコピーの禁止を可能にするが、罰則は容易に適用できず懲罰的なものでないため、このような侵害を実際に防止するものはない。

F-現在、その制限の結果、利用者は文書の著者が同定可能であって要求に回答するための手段を有している時には自らの手で著者に要求を行うが、さもなければ、文書の「分解」もしくは改変されたコピーの作成をしなければならない。

G-個人用プリンタの普及は組織および保守の面で問題を伴うものであり、より精巧な仕事用に主な組織に共同プリンタを備えることを妨げるものではない。

本方法および本方法を実施するための装置は機密文書の作成、頒布および使用の安全性に関するこの問題を解決することのできるものである。本発明を定義するに先立ち、装置によって処理可能な様々な種類の文書（これらのカテゴリは重複し得る）を定義するのが有用であろう。

-第1のカテゴリは、その特徴により、機密性、法的価値、および固有の価値のいずれも有しておらず、以下の分類のいずれにも属さない、自由に頒布可能なあらゆる文書に関する。このタイプの文書は以下「通常文書」と称する。

-第2のカテゴリは機密性のある、すなわち、自由に開示してはならない情報を含む文書に関する。この第2のカテゴリは以下「機密文書」と称する。

-第3のカテゴリは取引もしくは権利能力を証明する文書に関するものであり、これらの文書にはその信憑性が欠かれない。このカテゴリは、請求書、公文書、契約書、法令もしくは管理文書、租税報告書、小切手、食券等を含むことができる。このカテゴリは以下「認証可能な文書」と

称する。

-第4のカテゴリはある種の仕事の結果として生じ、その頒布がその著作者に権利を支払うことによって正当化されるあらゆる文書に関する。このカテゴリは書籍、雑誌等を含むことができる。この第4のカテゴリは以下「著者の文書

(9) 特表平11-509995

文書の参照および同定要素に関する知識が必要となることがある。これらの「ルール」は文書に、複製の機会に関する表示や文書のコピーが要求された時に処理装置が達成しなければならない動作を関連づけることができる。この要素は「マーキング」と補完的なものである（「マーキング」を有していない文書には「ルール」がなく、「マーキング」を有する要素は「ルール」を保有しなければならない）。「ルール」は実際の文書の可読性の改変を最小とするような方法で文書上にエンコードされる。もしも「ルール」が文書の複製を可能にするが、原稿の改変を伴うものである場合は、適当な（既存のもしくはこの目的で特に定義された）言葉を用いて改変ガイドラインを「ルール」に含有させる。

「マーキング」および「ルール」の定義に使用される方法は実際の文書の探索および抽出の観点から文書のデジタル化に適合するものでなければならない。

文書複製が要求された場合の対応する方法は以下の工程、すなわち、

- 実施すべき複製作業の定義要求、
- 複製要求に係る原稿紙文書の提示、
- 原稿文書のデジタル化、

-文書の「通常性」もしくは「機密性」を決定するための文書の可能な「マーキング」を検出するためのデジタル化の結果の分析、および提示された文書が「通常文書」である場合の要求の実施、

-前工程で文書が「機密文書」と同定された場合、「ルール」を探索および抽出するための付加的な分析。異常時には可能な保全動作とともに要求の拒絶、

-前工程後に文書が「機密文書」と同定された場合、「ルール」に定義された要素と要求および要求者を特徴づける要素に対する要求の認証管理、および、この要求が認証されない場合には可能な保全動作とともに要求の拒絶、

-前工程後に文書が「機密文書」と同定され、要求が認証された場合、要求者によって与えられる補完的要素と組み合わせられた、「ルール」で定義された動作もしくはそれらに由来する動作の処理。提示された文書が機密文書であって複製が認証された場合、「ルール」の解釈に由来するガイドラインに従った、要



ればYES、論理ページ上で「マーキング」が検出されなければNOである。この値は後続の処理工程を条件づける。

－「マーキング」が検出されない場合の処理(105)

処理されたページ上で「マーキング」が検出されなかった場合、このページは「通常文書」であるため、当初の要求がこのページについてなされる。しかしながら、同一の要求のために提示された全ページが「通常文書」である場合のみ、全体的な要求は一体的に考慮される。

－「マーキング」が検出された場合の処理：「ルール」の探索および一貫性制御(106) 「マーキング」が存在する場合、文書は「機密文書」と考えられる。この場合、複製制限が定義され、「ルール」の形式で文書中に挿入される。本工程の目的は前記ルールを検出しかつそれらの正当性をチェックすること、ならびにそれらを検出することにある。ルールは所定のかつ正規化されたグラフィックバイナリコーディングの形式にあり、検出および抽出アルゴリズムは、エンコーディングに必要であればバイナリ正当性制御を含んで定義することができる。エンコーディングがページ内の数カ所に与えられている場合、多様な出現の解釈一貫性制御が実施される。エンコーディングが実際の文書の内容に関連する統計値によって調整されている場合、これらの統計値は抽出された「ル

ール」の値の有効性を調べるために再計算される。この工程の結果は論理値であり、処理されたページ上で正当な「ルール」が検出されればYES、文書が「ルール」を含んでいないか不当な「ルール」を含んでいればNOである。この値と同時に、適切な処理のためにより詳細な診断を与えることもできる。

－「マーキング」が存在し、正当な「ルール」が存在しない場合の処理(107)。この場合は異常(本方法は「マーキング」と「ルール」との補完的存在を定義する)と考えられ、処理されたページに関する当初の要求は拒絶される。さらに、警報、原稿の捕捉、要求および著者の記録等、保全動作を起こすことができる。

－「マーキング」が存在し、正当な「ルール」が存在する場合の処理(108) 発現された要求が認証されていること、および要求者に対する付加的な

まれた情報による著作権課金に関して、または機密文書の作成管理の全体(日時、作成された文書の参照、要求者の同定等)について付加的な作用を適当な管理者との協議の上で行うことができる。

－要求の実施(110)

デジタル形式の文書を紙文書に変換する。

この方法の実施のためには予め定められ、かつ正規化された「マーキング」を確立しなければならない。このため、本発明は様々な典型的な「マーキング」を推奨する。

図2～4はこれらの「マーキング」を示すものである。

以下の定義において、基本的厚さが示された場合、これは印刷可能であり、かつ次にデジタル化が選択された後に検出可能な最小の厚さを意味する(これらの制限を部分的に補償するアルゴリズムによって調整することが可能である)。

第1の好ましい「マーキング」は、段落もしくはグラフィックである数個の一貫した部分からなる典型的な文書(201)に関する(本例ではこの文書は2つ

の段落(202)および(203)である2つの一貫した部分を有する)。一貫した部分の他に、文書は2つの主要なマージン(204)および一貫した部分を分離するマージン(205)を有する。文書を構成する文字(207)もしくはグラフィックの外側の一貫した部分にのみ、独立した点(206)が予め確立された密度標準に従って、テキストおよびグラフィックの印刷成分上に重なることなく、全一貫部分内に記されている。図2とは異なり、点は十分に薄く、文書の可読性を変化させない(ここでは図示の便宜上、これらは強調されており、また、使用された密度は正規化に使用されるものとして代表的ではない)。好ましくは、点は(文書の可読性を損なわないような基本的厚さを有する)より複雑なシンボルで置き換えることができる。

第2の好ましい「マーキング」は典型的な文書(210)であって、パターンを重ねるようなテキストとグラフィック要素(211)との組を含む。本例では、パターンは平行な斜線(212)からなり、これらは文書の可読性を損なわないような基本的厚さを有して所定の間隔に沿って文書の一端から多端へ延びてい

制御が行われていること(認証は要求者もしくは要求自体の特性に依存し得、例えば、局所複製は認証されるが、遠隔複製は認証されない)を確認するため、「ルール」を解釈する。発現された要求が認証済みコピーを得ることに関する場合、あらゆる機密文書に対して体系的になされる認証制御とは独立して、提示された文書が実際に「認証可能な文書」であることをチェックするために付加的な制御が行われる。この場合、要求者が必要に応じてその要求の定義を達成し、あるいは放棄することさえもできるように、提示された「認証可能な文書」に対応する全体的な文書の電子的原稿を特徴づける要素が探索される。これらの制御の末に論理値が更新される。すなわち、発現された要求が認証されないか維持されない場合にはNOであり、要求が認証されかつ維持される場合(制御工程は要求者が受諾もしくは拒否できる使用料を提示することができる)にはYESである。

－要求が認証されないか、維持されない場合の処理(107)

「マーキング」が存在しかつ正当な「ルール」が存在しない場合と同様に、要求は拒否され、当初の要求が制限のない者による「機密文書」型文書を侵害する企てに対応する時には保全システムを起動させることが

できる。

－「機密文書」に対する認証された要求の場合の処理(109)

作成すべき文書のデジタル化された画像が、要求の特質および「ルール」の作用に由来し、さらに原稿に対する変更(マスキング、重ね印刷、カラー抑制、グラフィック変更等)を含むガイドラインに従って生成される。この結果、提示された文書に由来するデジタル画像に関するものではなく、認証済みのコピーを要求した時に提示された文書にリンクされた電子的原稿に由来する実際のコピーの画像を構築することができる。これらのガイドラインは適当な言葉で表現された基本的な命令により、ルールに従ってエンコードしておくことができる。このようにして作成された画像は、原稿文書の「マーキング」に依存しない適当な「マーキング」および当初の「ルール」とは異なってもよい適当な「ルール」(特に、得られたコピーの複製権は原稿のものとは異なってもよい)を含む。作成された文書に対するこれらの直接的な作用に加え、「ルール」に含

る。

第3の好ましい「マーキング」は典型的な文書(図示せず)であって、各文字(221)を、基本的厚さを有する矩形の網目で囲ったものである。

好ましい「ルール」はいくつかの同一の出現部の形式で文書上にエンコードされる。各出現部はヘディング(231)およびデータ部(232)からなる。ヘディング(231)は出現部の同定およびその読み取り方向の決定を可能にする。この目的で、好ましいヘディングは、基本的厚さの「+」記号(233)と、それに続く基本的厚さの配向バー(234)を備えている。このヘディング(231)データ部(232)の同定および解釈を可能にし、データ部(232)では所定の間隔で基本的厚さのバーがその存在(235)もしくはその不在(236)によってバイナリ値0もしくは1を与えている。これらのバイナリ値を組み合わせることによって、「ルール」の解釈可能な値の再構築が可能になる。同一の文書に数個の「ルール」が挿入され、したがって、例えば、ぼかし点型の「マーキング」を用いる典型的な文書(241)において、文書を囲む主要なマージンと、文書(242)の段落、グラフィック等からなる各一貫部分を分離

する中間マージンとを定義することが可能である。主要なマージンのそれぞれについて、その各端および得られる領域の中央(243)に「ルール」を挿入する。同様に、中間的なマージン(244)のそれぞれについて、その各端および得られる領域の中央に「ルール」を挿入する。

使用される「マーキング」がパターンタイプの「マーキング」である場合、「ルール」のグラフィック性は2つのパターン要素(251)の間に挿入されるように適合させる。ここでも「ルール」はヘディング(252)およびデータ部(253)からなり、これらの要素(254)(255)(256)および(257)のエンコーディングを構成する記号およびバーはそれらの間の、そして妥当であれば、それらとパターンとの間の平行性を維持するように適合させる。

局所複製に使用するべく本方法を実施するために提案される装置は「文書サーバ」(1)によって実現され、これは主として以下の機能モジュール、すなわち



、「ユーザインタフェースモジュール」(11)、「デジタル化モジュール」(12)、「制御モジュール」(15)、「分析モジュール」(16)、「形成モジュール」(17)および「印刷モジュール」(14)を含む。この「文書サーバ」(1)は利用者(31)が原稿文書(41)から紙コピー文書(43)を要求することを可能にする。このために、利用者(31)はその原稿(41)を「デジタル化モジュール」(12)に導入し、そのコピー作業を「ユーザインタフェースモジュール」(11)に対して定義する。この要求に続いて、「ユーザインタフェースモジュール」(11)はこれを「制御モジュール」(15)に送る。このモジュール(15)は「デジタル化モジュール」(12)をこれら原稿(41)から電子型手段の使用可能なデジタル化された文書(42)を与えるように制御する。提示された文書(41)の最初のデジタル化文書(42)画像が得られたら、「制御モジュール」は「分析モジュール」(16)に要求を行う。このモジュール(16)は実際的基本文書(44)、すなわち、いかなる「マーキング」も「ルール」に対応するいかなる要素も含まないものを最初のデジタル文書(42)から抽出する。この結果と同時に、分析モジュールは「マーキング」が存在するか否かを決定し、この検出が陽性である場合には「ルール」を探索

し、これらを読み出して、それらから使用可能な電子的ファイル(45)を形成する。このモジュール(16)はこのレベルで「ルール」と提示された文書(41)との間の合一性を検査する。この合一性に関する診断は使用可能な「ルール」(45)に組み込まれる。「マーキング」が検出されない場合は、原稿(41)が「通常文書」型文書であることを意味し、「制御モジュール」(15)は「形成モジュール」(17)に基本デジタル化文書(44)から直接に最終的なデジタル化文書(47)を形成するよう要求する。次いで、「制御モジュール」(15)は「形成モジュール」(17)に最終的なデジタル化文書(47)から、要求されたコピー(43)を直接得るよう要求する。「マーキング」が検出され、かつ「ルール」が読み取り不能である場合もしくは読み取り「ルール」の異なった出現部がそれらの中で一貫していないか提示された文書(41)に対応していない場合、「制御モジュール」(15)は分析(42)および(45)に由来

一前回の結果から、マーキング密度は式 $D = \text{NMARQ} / (\text{NDOT} - \text{NUTL})$ で計算される。この密度は「マーキング」を特徴づける正規化された密度と比較される。この比較の結果は提示された文書の機密性もしくは通常性を定義するための診断に用いられる。

第2の好ましい「マーキング」(パターン)について、探索はパターン(212)のビットの全出現を検出するために全文書(210)上で実施される(この例では、例えば、パターンの1つのビットを基本的厚さと少なくとも1cmの長さを有する斜めのバーとして定義することができる)。このようにして見出された要素の数およびそれらのページ中における地理的分布に従って、正規化されたパターン存在の診断を行うことができ、この結果、提示されたページの「機密文書」もしくは「通常文書」の特性に関する診断を実施することができる。

第3の好ましい「マーキング」(網掛け)について、探索はページ全体においてそれを構成する文字(221)を同定するために実施される。各同定された文字について、その文字が基本的網目(222)によって囲まれているかどうかチェックされる。文書がそのページ中にこのような囲みを有する文字を所定数より多く有している場合、その文書は「機密文書」あるいは逆に「通常文書」と考

えられる。

文書が「マーキング」の検出後に「機密文書」と考えられる場合、「ルール」のあらゆる出現が探索される。このために、配向バー(234)もしくは(255)によって妥当性が明らかにされる「ルール」(233)もしくは(254)のグラフィック識別子の探索がある。このように定義されたヘディング(231)もしくは(252)の検出後、データ(232)もしくは(253)が探索される。このために、各基本的間隔において、バーの存在(235)／(255)もしくは不在(236)／(257)の検出が行われる。完全な検出によって、出現のエンコーディングの解釈、さらにその妥当性の確認も可能になる。エンコーディング統一性制御値(例えば総制御バイナリ)が定義されれば、この妥当性は制御される。数個の「ルール」が検出される場合には、それらの一貫性が確認される。エンコードされた値が、提示された文書にリンクされた統計値に

するファイルを破壊することによってコピーの達成を拒絶し、また、「ユーザインタフェースモジュール」(11)への要求もしくは警告、原稿の捕捉等の保全動作の開始によって利用者(31)に警告することができる。「マーキング」が検出され、かつ一貫した「ルール」が読み取られた場合、制御モジュールはこれらの「ルール」を処理して、対応する処理を達成する。コピー(43)を作成しなければならず、かつ原稿が「機密文書」である場合、「制御モジュール」は作成すべき文書(43)に関連した新たな「ルール」(46)を構築し、これを「形成モジュール」(17)に渡す。このモジュール(17)は基本デジタル化文書(44)および新たな「ルール」(46)から、実際の文書、「マーキング」、およびこの文書にリンクした可能な「ルール」を含む、作成すべき文書(43)のデジタル化文書(47)の形式にある画像を形成する。次いで、「印刷モジュール」がこの電子的モデル化(47)から、作成すべき文書(43)を構築する。

第1の好ましい「マーキング」(ぼかし点)について、「マーキング」探索は以下のように行うことができる。

一提示された文書の一貫した領域、例えば領域(202)および(203)の探索。このために、文書中の、基本点(「ドット」)の幅が所定の幅よりも大きく、また高さも同様に大きな白色の矩形部分(提示された

独立点の密度が所定値よりも低い場合にその部分は白色と考えられる)を全て除去する。この結果、図2の例ではマージン(204)および(205)が除去される。「ルール」(好ましくは+記号もしくはバー)の出現部に属する可能性のある任意のグラフィック要素はこの探索で「白色部」と考えられる。

一前段階で得られる領域から、例えば部分(202)および(203)の場合、可能性のある表面を全領域の基本的印刷点で計測する。これによって数NDOTが得られる。この領域では数個の基本的印刷点の配置で特徴づけられるあらゆる印刷要素が探索される。これは、例えば文字の場合、例えば図3の場合、(207)と同様な文字である。これら全要素の全体的な表面をドットで計測し、NUTLを得る。新たな探索によって、全ての独立した印刷基本点の計測が可能になり、NMARQが得られる。

によって調整される場合、これらの統計値は読み取られた「ルール」と提示された文書との合一性をチェックするために再計算される。

文書が制限を伴って複製される場合、「制御モジュール」は文書(41)の「ルール」(45)の解釈に由来する処理にリンクする。この処理は例えば、以下のものを含む。

一利用者(31)が「ルール」で定義されたアクセスを行う認証のための「ユーザインタフェースモジュール」(11)への制御要求、

一文書が「著者の文書」である場合の著作権料、

一複製が認証された場合に、作成すべき文書(43)に関連づけられた「ルール」である「最終ルール」(46)を「最初のルール」(45)から形成すること、

一基本デジタル化文書の変形のためのガイドラインの可能な送出手を「形成モジュール」(17)に要求すること、これらのガイドラインは最初の文書(41)の「ルール」の解釈に対応する。

「形成モジュール」(17)が「最終デジタル化文書」(47)の形成を終了した時に「制御モジュール」(15)は「印刷モジュール」(14)に要求を行う。

(「分析モジュール」の診断後もしくは「ユーザインタフェースモジュール」(11)に対する利用者(31)同定の要求が失敗した後に)複製が認証されない全体的な場合、「制御モジュール」は保全システム(警告、原稿の捕捉等)を作動し、装置中における最初の文書(41)から構築されたあらゆる内部要素、すなわち「内部デジタル化文書」(42)、「内部ルール」(45)および「基本デジタル化文書」(44)を破壊することができる。

複製すべき文書(41)が「通常文書」型の文書である場合、「形成モジュール」(17)は「基本デジタル化文書」から直接「最終デジタル化文書」(47)を構築する。他の場合、「最終デジタル化文書」(47)は「基本デジタル化文書」(44)、「最終ルール」(46)、および「制御モジュール」(15)から送られる可能性のある変形ガイドラインから構築される。「形成モジュール」



ル」(17)はこれらの要素に新たな「マーキング」を導入する。

本方法を遠隔複製に使用するべく実施するために提案された装置は、さらに遠隔複製に用いられるモジュール、すなわち「通信モジュール」(18)および「出力管理モジュール」(19)を含む「文書サーバ」(1)によって実現される。

利用者(31)がその「文書サーバ」(1)に、文書(41)をその相手先に相手先(31)の遠隔「文書サーバ」(2)を介して伝送することを要求する場合、その利用者(31)は局所コピーのためにその文書(41)をその「文書サーバ」(1)に導入する。利用者(31)と相手先(32)の2つの「文書サーバ」(1)および(2)は同一である。モジュールの駆動は関係する「文書サーバ」の「制御モジュール」(15)によって達成される。送信側「文書サーバ」(1)の「ユーザインタフェースモジュール」(11)を介した要求の発現後、送信側(1)の「デジタル化モジュール」(12)はデジタル形式にある文書(42)を作成する。この文書(42)は局所コピーを得るためのものと同一の原則に従って送信側(1)の「分析モジュール」(16)によって分析される。この送信側(1)のモジュール(16)は、局所操作の場合と同様に、基本デジタル文書(44)(いかなる「マーキング」もいかなる「ルール」も含まないもの

)、および原稿文書(41)にリンクした「最初のルール」(45)を形成する。このレベルにおいて、「制御モジュール」は最終「ルール」(46)の制御、計測、形成もしくは最初の「ルール」(44)の作用に由来するコピー変形ガイドラインの形成に関して同じ作業を達成する一方、「ルール」に含まれた情報に従って文書(41)が遠隔的に複製できるかをチェックし、次いで、送信側「文書サーバ」(1)の「ユーザインタフェースモジュール」(11)を介して、利用者(31)に、受信側「文書サーバ」(2)の同意および受信側(2)に対する相手先(32)の識別子もしくは同等ないずれかの情報を得るための要求を行う。「文書サーバ」(2)の同意は電話型リンクの場合においては電話番号、コンピュータリンクが使用される場合にはコンピュータネットワークアドレスによって行われる。相手先(32)の識別子は局所コピーの場合に利用者が自身

3)の有効な配布時のみ行われる。

本方法をコンピュータシステムからの印刷に使用するべく実施するために提案される装置は遠隔複製のための機能成分と同じものに加えて、「機密文書」を作成しなければならない任意のコンピュータシステムに存在する「ドライバ」(82)を含む「文書サーバ」(1)によって実現される。コンピュータ利用者(33)はコンピュータシステム(72)に存在するアプリケーション(81)を用いて文書を構想する。この構想の結果はデジタル形式の文書(48)である。実際、この結果はページ記述言語の基本を用いることによる記述的な形式の文書画像である。この場合、コンピュータシステム(72)のレベルもしくは「文書サーバ」(1)のレベルで解釈用サブモジュールを導入しなければならない。単純化するため、図9ではアプリケーションの結果はデジタル化された形式の文書であると単純に仮定する。「文書サーバ」上の文書を送出するため、コンピュータシステム(72)にはドライバ(82)が組み込まれる。このドライバは、最初のパラメータ化により、もしくは利用者(33)との会話により、もしくはシステム(72)に保存された要素の探索により、もしくはこれらの手段の組み合わせにより、作成すべき文書に関連した「ルール」(49)を確立するために必要な要素を集めることを可能にする。これらの「ルール」は、エンコードされた値がこの新たなソースに適合されていることを除き、装置から通常由来する文書について定義されるものと同じである。文書(48) + 「ルール」(49) + 利用

者(33)の組は2つの関係するシステムの通信モジュール(83)次いで(18)を用いることによってコンピュータネットワーク(71)を介して「文書サーバ」(1)に伝送される。「文書サーバ」(1)上のこれらの要素(48)(49)および識別子を受信した後、「制御モジュール」(15)は「形成モジュール」(17)に、受信した文書(44)および受信した「ルール」(46)からデジタル形式の最終文書(47)を作成するよう要求する。この文書(47)は、「出力管理モジュール」(19)によって、特定の待ち行列(図示せず)で保存されかつ利用者(33)の識別子にリンクされるように処理される。印刷は利用者(33)の存在下においてのみ解放される。所望のコピーを得るため

を「文書サーバ」に対して同意するものと同じである。この識別子は選択された例の場合、パスワードを伴うものでなければならない(これは相手先が磁気バッチやその同等品のような他の安全な識別手段を有する場合には不要である)。利用者(31)が受信側(2)の同意および受信側(2)に対する相手先(32)の識別を提供した後に遠隔コピーが認証された場合、制御モジュールは送信側(1)の「通信モジュール」(18)に、遠隔コピーを可能にする要素を受信側(2)に伝送するよう要求する。送信側(1)の「通信モジュール」(18)は、場合により、電話網もしくはコンピュータネットワーク(71)を使用して、受信側(2)の「通信モジュール」(18)との間に通信セッションを確立する。基本デジタル文書(44)、最終「ルール」(45)、さらに場合によっては原稿に対するコピーの変形に関するガイドラインがこの通信で伝送される。これは受信側(2)に対する相手先(32)の識別子で完了する。この受信後、受信側(2)の「制御モジュール」(15)は受信側(2)の「形成モジュール」(17)に対して、受信側(2)で受信側(2)の「基本デジタル化文書」(44)と、場合によっては原稿に対するコピーの変形に関するガイドラインとから「最終デジタル化文書」(47)を構築するよう要求する。次いで、「最終デジタル化文書」(47)は、これを送信側利用者(31)によって指定された相手先(32)の識別子とリンクすることによって(図示しない)特定の待ち行列で保

存する受信側(2)の「出力管理モジュール」(19)により、処理される。所望のコピーを得るためには、相手先はその識別子およびそのパスワードを獲得することによって(もしくは場合によっては磁気バッチ等によって)自身を受信側(2)に対して同意しなければならない。この同意後、受信側の「文書サーバ」(2)で受信され、同意済みの相手先(32)にリンクされた全文書がリストされる。次いで、相手先(32)は獲得したい文書(複数でも可)を解放し、この場合、受信側の「出力管理モジュール」(14)は、所望のコピー(複数でも可)(43)を得るために、その待ち行列から対応する文書(複数でも可)をその受信側(2)の「印刷モジュール」(14)に返送する。提供された「機密文書」のコピーに関して管理作業が必要な場合、この作業は文書(複数でも可)(4

に、利用者(33)はその識別子およびそのパスワード(もしくは場合によっては磁気バッチ等)を獲得することによって「ユーザインタフェースモジュール」(11)を介して「文書サーバ」(1)に対して自身を同意しなければならない。この同意後、「文書サーバ」(1)上で受信され、かつ利用者(33)にリンクされた全ての文書がリストされる。次いで、利用者(33)は自身が得たい文書(複数でも可)を解放し、この場合、所望の印刷物(複数でも可)を得るために「出力管理モジュール」(19)はその待ち行列に対応する文書(複数でも可)を「印刷モジュール」(14)に返送する。識別子/パスワードの制御はコンピュータシステム(72)への要求によって行うことができる。与えられた「機密文書」印刷物に関して管理作業が必要な場合、その作業は「文書」(複数でも可)(43)の有効な配布時のみ行われる。

本方法をコンピュータシステムからの印刷を行うための「認証可能な文書」の原稿作成および、特に、「認証可能な文書」の原稿からの認証された紙コピーの作成に使用するべく実施するために提案される装置は「文書サーバ」(1)もしくは(3)、「機密文書」を作成しなければならないいずれかのコンピュータシステム上に存在する「ドライバ」(82)、および「保管サーバ」(73)からなる。後者(73)は主として「通信モジュール」(84)および「保管マネージャ」(85)を含む。「文書サーバ」(1)はさらに、先に定義された機能モジュールに加えて、「ディレクトリモジュール」(20)を含む。この装置の作用は以下の通りである。

ある組織が「認証可能な文書」(92)を作成したい場合、その組織はアプリケーションマネージャ(34)を介してそのコンピュータシステム(72)上で、作成すべき文書(48)と、本発明によれば、これらの文書の「ルール」(49)の定義を可能にする要素とを定義する。作成すべき文書は直接、アプリケーション(81)によって構築される。ルールは上述のものと同じ作用によってドライバ(82)によって作成される。文書の作成準備が整った時に、文書はコンピュータネットワーク(71)を介して、印刷のための「文書サーバ」(71)と、「保管マネージャ」(85)を介して文書(91)の電子画像を保存する「



保管サーバ」(73)とに送られる。このマネージャ(85)は「ルール」に含まれた要素から各文書を見出すことのできるものでなければならず、また、得られたコピーの各アクセスもしくは記録管理を行ってもよい。伝送はコンピュータシステム(72)からその通信モジュール(83)を介して「文書サーバ」(1)に、また、通信モジュール(18)、(83)および(84)を介して「保管サーバ」(73)に行われる。「文書サーバ」(1)上では、上述の特徴のように、最終文書(92)が、場合によっては作成マネージャ(35)の制御を介して作成される。作成された文書(92)はメールによる通常の伝送手段および従来の紙文書頒布手段を介してその受信先(36)に伝送される。この受信先は発信元(34)によって指定された直接の受信先、もしくはその文書の最初の受信先から(いずれかの権利を得るために)その文書が伝送される外部機関とすることができる。このように同定された受信先(36)がこの文書(92)の認証されたコピーを所望する場合には自身の「文書サーバ」(3)にその文書を提示する一方、ユーザインタフェース(11)に従来のコピーではなく認証されたコピーを要求する(しかしながら、認証されたコピーの獲得が得られることは利用者が認証可能な原稿から認証のない通常のコピーを要求することを妨げない)。また、利用者は全体的な文書の全部もしくは一部のコピーを得るために、認証可能な原稿文書の抜粋のみを提示することもできる。この場合、利用者は認証されたコピーを得たいというその要求のみを発見する一方、全体的な文書の補完的な要素をいつ得るかについては要求の明確な定義を保留する。次いで、文書(92)はこの文書(92)のデジタル化画像(42)を得るためにその「文書サーバ」

(3)の「デジタル化モジュール」(12)によってデジタル化される。分析モジュール(16)は、マーキングの検出後、先に定義されたプロセスに従って「ルール」を分析する。この分析の結果から、文書(43)の実際の画像を得ることなく、「ルール」が利用可能な形式(45)で転写される。「制御モジュール」(15)は最初の文書を作成したコンピュータシステム(72)に関連した「保管サーバ」(73)の電子アドレスを得るために「ディレクトリモジュール」(20)に要求を行う。この要求が失敗した場合、操作は停止され、発信元機関

」(73)は先に定義したものと同一であり、本例では「ドライバ」(82)は使用されない。

利用者(36)は紙形式の「認証可能な文書」(92)から、電子的な認証可能なコピー(94)、あるいは提示された文書に関連する電子取引(95)をも得るために要求を行うことができる。このプロセスは認証された紙コピーの獲得と同一であるが、この場合、「文書サーバ」(3)は、文書(92)の分析および上述のような対応する「ルール」(92)の獲得後、「ディレクトリモジュール」(20)への要求後に「通信モジュール」(18)に対し、関係する「保管サーバ」(73)が、提示された文書(92)の電子画像(91)を利用者(36)によって示されたコンピュータシステム(74)に直接送るようになるための要求を行う。「保管システム」(73)から受信側コンピュータシステム(74)への伝送は各々の通信モジュール(84)および(86)の使用を介して行われる。「保管マネージャ」(85)は原稿文書の発信元のために、作成されたコピー(94)もしくは発生した取引(95)を管理する。受信側のいずれかのコンピュータシステム(74)上に存在する「処理モジュール」(87)はそのシステムにおける認証された電子的コピー(94)の保存および管理ならびに(場合によっては)提示された原稿(92)から発生した取引に対応する要素(95)の生成を可能にする。

本発明は、その特徴に従って、同一の組織内で紙文書の安全な流通を保証するために使用することができる。上述の装置を備えた企業は、他の文書作成もしくは複製装置を排除して、その企業内ではいかなる機密文書も権限のない第三者のためには印刷されないようにすることができる。同様に、その組織内で文書を局所的に複製もしくはファックスすることもできない。文書の置換を伴う「機密文

書」のハッキングはハッカーに危険を冒しかつハッキングの痕跡を残すことを強いる。

本発明が文書作成もしくは複製のための標準となる場合は、価値のある文書(銀行券、チケット等)の同一のコピーを妨ぐこと、および文書作成者が彼らの作品の頒布もしくはコピー毎に報酬を得ることを保証する。

を権限のある者によって登録するため、対応するメッセージがユーザインタフェース(11)のレベルで発せられる。「ディレクトリモジュール」(20)が電子アドレスを返送する際、「制御モジュール」(15)は、文書の認証済みコピーを得るためにその文書の適当な参照を伴った前記アドレスを「通信モジュール」(18)に送る。提示された文書が、利用者が所望のコピーをより明確に定義するための全体的な文書の抜粋に過ぎない(提示された文書とコピーした文書とが相違し得る)場合、「保管サーバ」(73)は最初に、利用者がそのコピー要求(詳細な一覧、著作権のための複製費等)を完遂するのに必要な全ての要素を文書サーバ(3)に返送する。要求が明確に発現された場合、保管サーバ(73)はマネージャ(85)を介して対応する文書(92)の、もしくは後者によって定義される電子画像(91)を探索する。要求されたコピーの作成が著作権料の支払いを伴うものである場合、対応する管理は「保管サーバ」(73)の「保管マネージャ」(85)によって達成される。通信は各々の「通信モジュール」(18)および(84)の使用によってコンピュータネットワーク(71)を介して行われる。「文書サーバ」(3)は文書(91)の電子画像を受信することにより、この「文書サーバ」は実際の文書(46)のデジタル化画像および、作成すべき文書のコピーの特性に適合させることができる「関連したルール」(44)の双方を保存することができる。次いで、「形成モジュール」(17)は文書(46)のデジタル画像および「最終ルール」(44)から最終形式(47)のデジタル化文書を作成する。認証されたコピー(93)がこの要素(47)から、「印刷モジュール」(14)によって、場合によっては「出力管理モジュール」(14)を介して、作成される。

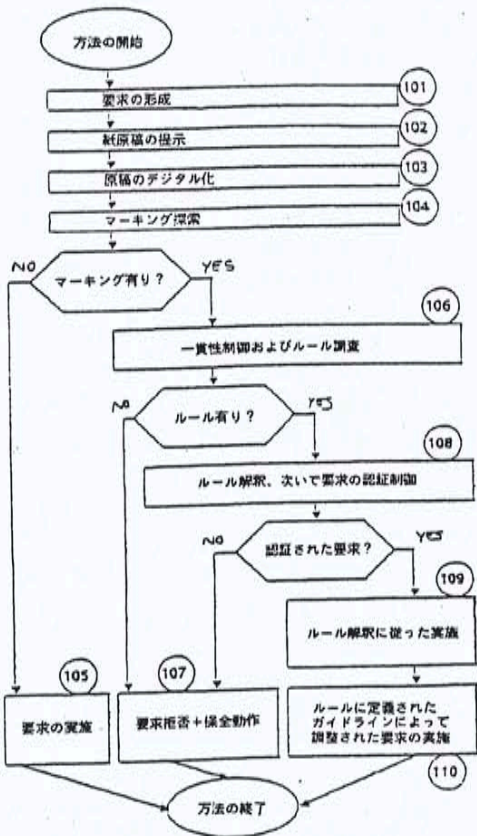
本方法を「認証可能な文書」(92)の原稿からの認証された電子的コピーの作成もしくは認証された(すなわち、取引に使用される文書発信元の管理下における)電子的取引の実施に使用するべく実施するために提案される装置は、「文書サーバ」(3)、および電子的コピーの受信もしくは電子取引の登録をしなければならない任意のコンピュータシステム上の「保管サーバ」(73)および「処理モジュール」(87)を備える。「文書サーバ」(3)および「保管サーバ

権利を公開する文書(管理、会計文書、もしくは取引に関する文書)を印刷したい各企業および対応する権利を登録したい企業のために、発行時に本装置を用いることによって、いかなる複雑な技術をも排除して通常の紙を使用することが可能になる一方、あらゆる改竄の企ては発生した取引に対してその改竄が有効でないために無効化される。したがって、例えば、銀行が適合する装置を備えていれば、発行された小切手を振り替えて、食券を回収すること、社会保障決算に関する投資信託会社からの付加的償還を処理すること、会計担当者もしくは税務担当者が伝票、請求書もしくはあらゆる会計文書を登録することが可能になる。ホチキス留めもしくは製本された厚い文書の場合、利用者は、(発行者によって認証されれば)文書の1ページを提示するだけで、提示された文書を分解することなく全部のコピーを得ることができる。発行者は自身が作成する文書を、また、これらの文書から得られる複製もしくは取引を全体的に管理し続けること、また発行された原稿から作成された任意のコピーに関する著作権を認めることさえも可能である。



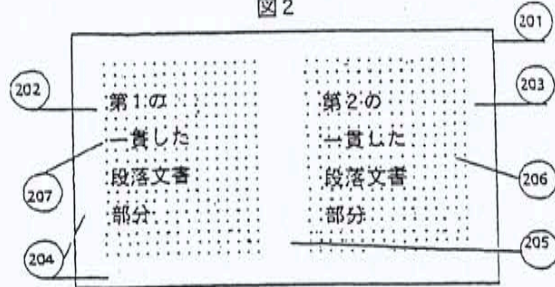
【図1】

図1



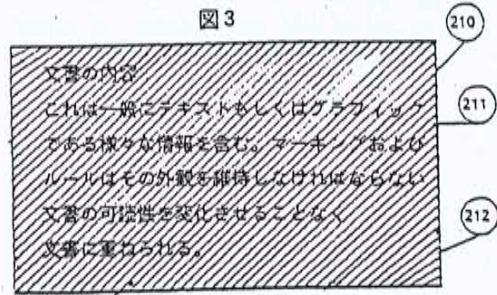
【図2】

図2



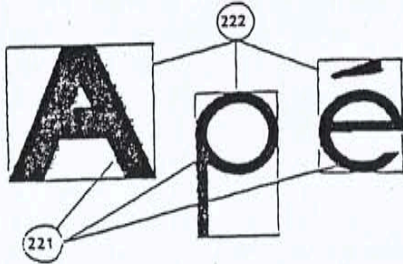
【図3】

図3



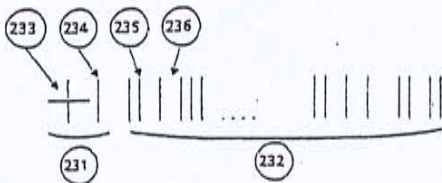
【図4】

図4



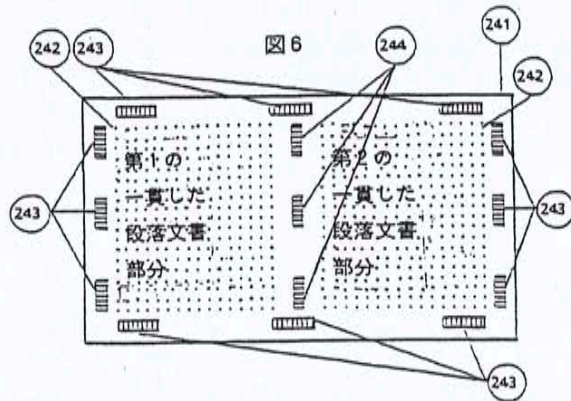
【図5】

図5



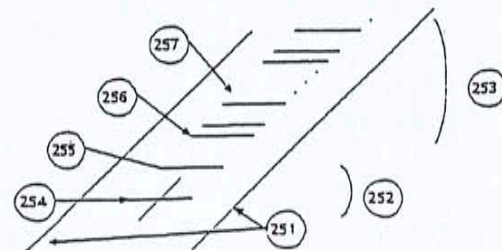
【図6】

図6



【図7】

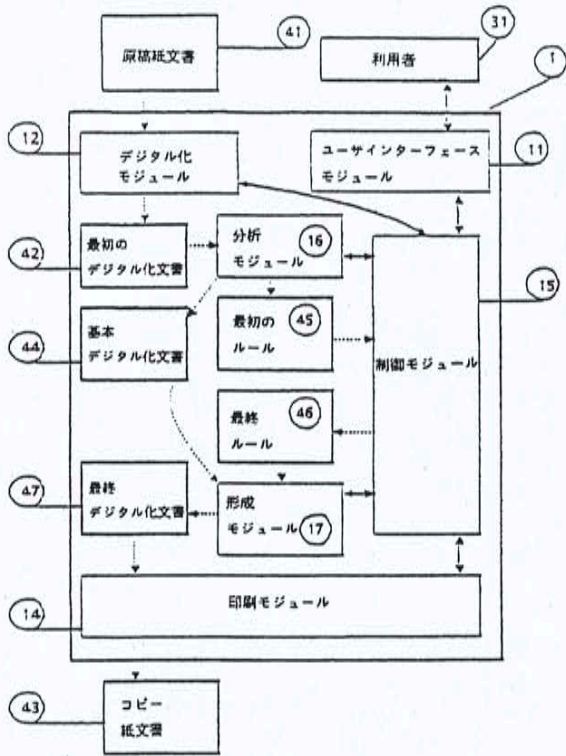
図7





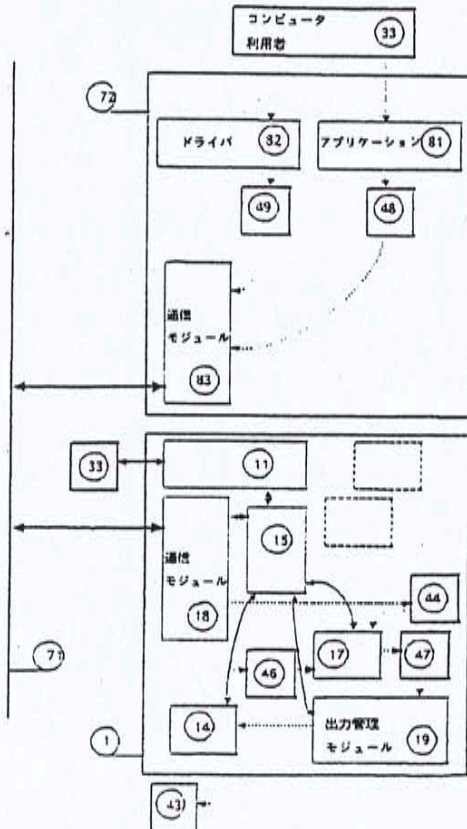
【図8】

図8



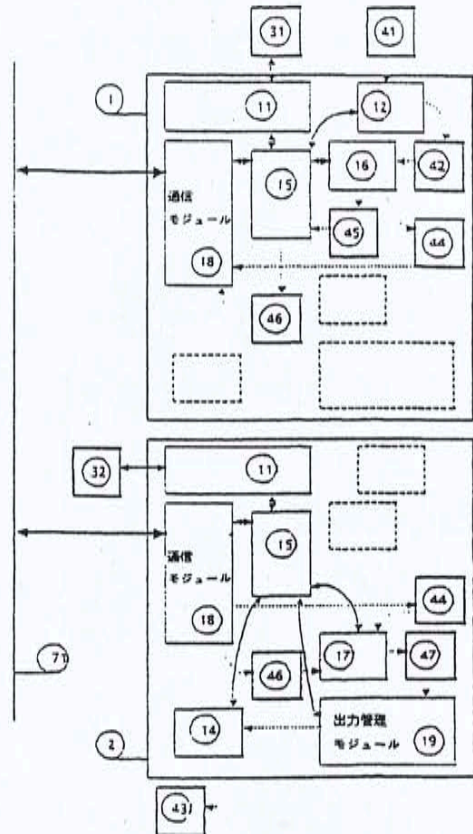
【図10】

図10



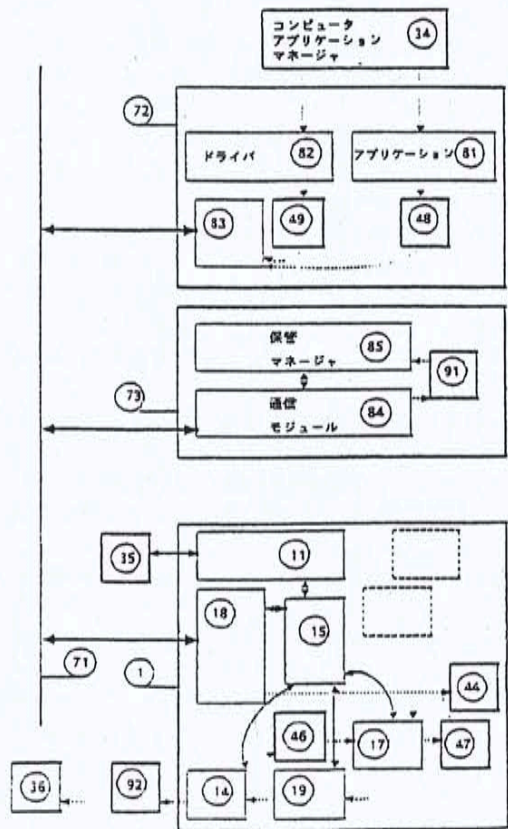
【図9】

図9



【図11】

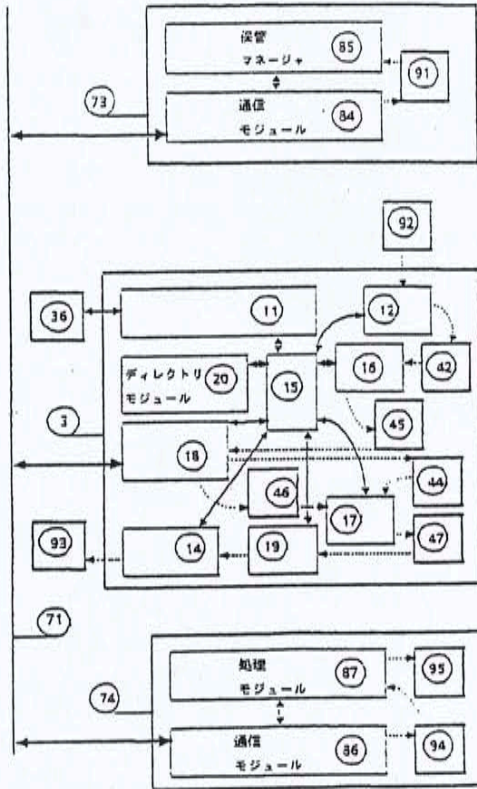
図11





【図12】

図12



(44) 特表平11-509995

—前工程後に文書が「機密文書」と同定された場合、「ルール」を探索および解読するための補完的な分析(106)、異常時には要求の拒絶(107)

—前工程後に文書が「機密文書」と同定された場合、「ルール」に定義された要素と要求および要求者の特徴づける要素に関する要求の認証管理(108)、異常時には要求の拒絶(107)。

—前工程後に、文書が「機密文書」と同定され、要求が認証された場合、要求者によって与えられる補完的要素と組み合わせられた、「ルール」で定義された動作もしくはそれらに由来する動作の実行(109)。

—提示された文書が「通常文書」(105)である場合および、提示された文書が、「ルール」の解釈に由来するガイドラインによれば「機密文書」(110)であって複製が認証される場合、要求された複製の作成を順に実施することを特徴とする方法。

2. 請求項1による方法を実施するための装置であって、以下の機能モジュール

—利用者がその要求および自身を正確に定義することを可能にする「ユーザインタフェースモジュール」(11)。

—提示された文書のコンピュータ操作を可能にするために基本的な黒色および白色の点への分解もしくは場合によってはカラーもしくは赤外線属性の付与を行う「デジタル化モジュール」(12)。

—認証された時に、利用者によって定義された紙コピーを対応する電子手段から構築する「印刷モジュール」(14)。

—コンピュータモジュールである「分析モジュール」(16)、「制御モジュール」(15)および「形成モジュール」(17)であって、分析モジュールはデジタル化された文書からの「マーキング」および「ルール」の検出および解読に適したアルゴリズムを含み、「制御モジュール」は全モジュールの駆動および結合を保障し、「形成モジュール」は、(認証された場合に)原稿文書のデジタル画像から、原稿のルールに

請求の範囲

1. 文書を複製するための方法であって、機密と考えられる文書に予め付加的な特定のグラフィック要素である「マーキング」および「ルール」を付加し、マーキングは「機密文書」と「通常文書」とを区別することを可能にする要素であり、前記「マーキング」は、実際の文書の可読性を妨げないが文書の縮小部分でも検知可能でなければならない全文書の特有のグラフィック性(可視か否か)によって達成され、この「マーキング」は「機密文書」と考えられる任意の文書上に存在し、したがって、任意の「通常文書」に欠けており、ルールは全ての「機密文書」に関する要素であって、その関連する文書の複製に関するルールおよび制限を定義するものであり、この要素は以下「ルール」と称し、複製ルールおよび制限には「ルール」として統合されるべき与えられた文書の参照および同定要素に関する知識が表示や文書のコピーが要求された時に処理装置が達成しなければならない動作を関連づけることができ、この要素は「マーキング」と補完的なものであり(「マーキング」を有していない文書には「ルール」がなく、「マーキング」を有する要素は「ルール」を保有しなければならず)、「ルール」は実際の文書の可読性の改変を最小とするような方法で文書上にエンコードされ、もしも「ルール」が文書の複製を可能にするが、原稿の改変を伴うものである場合は、適当な(既存のもしくはこの目的で特に定義された)言葉を用いて改変ガイドラインを「ルール」に含有させること、および以下の工程

- 実施すべき複製作業の定義要求(101)。
- 原稿文書の提示(102)。
- 原稿文書のデジタル化(103)。
- 文書の「通常性」もしくは「機密性」を決定するための文書の可能な「

マーキング」を検出するためのデジタル化の結果の分析(104)。

(45) 特表平11-509995

含まれた変形ガイドラインを尊重しながら、「マーキング」および「ルール」のない作成すべき文書のデジタル化画像を形成し、このように構築された文書はそれ自体の「マーキング」および「ルール」を備えているものを組み合わせることを特徴とする装置。

3. さらに、文書の複製に要する任意の電子ファイルを2つの同一の「文書サーバ」(1)間で対話および交換させることを可能にする「通信モジュール」(18)および、要求されたコピーがコピーを作成する「文書サーバ」の外部からの要求に由来する場合に作動されるコンピュータモジュールであって、作成されるべき文書を保持し、受信先が受信側「文書サーバ」であることを自ら同定した場合のみ、これを解放する「出力管理モジュール」(19)を含むことを特徴とする請求項2記載の装置。

4. 機密文書を印刷しなければならない任意のコンピュータシステム(72)に付加された「ドライバ」(82)をさらに含み、前記ドライバは所望の紙文書の構築に必要な全ファイルおよび特徴を「文書サーバ」(1)の「通信モジュール」(18)に送られるために提供されていることを特徴とする請求項3記載の装置。

5. さらに、「認証可能な文書」(92)の作成中に前記「認証可能な文書」からの認証されたコピーの作成のための要求が発現された時に復元用にその電子的同等物(91)を保存する「保管サーバ」(73)と、任意の「文書サーバ」(3)から任意の「保管サーバ」(73)へのアクセスを管理する「ディレクトリモジュール」(20)とを含むことを特徴とする請求項4記載の装置。

6. さらに、「認証可能な文書」の提示および提示された文書にリンクされた「保管サーバ」(73)への要求に際して「文書サーバ」上で発現された要求の実行中に、認証されたコピーもしくは取引を受信しなければならない任意のコンピュータシステム上に組み込まれた「処理モジュール」(87)を含むことを特徴とする請求項5記載の装置。