

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2015 年 4 月 2 日(02.04.2015)



(10) 国際公開番号
WO 2015/045302 A1

- (51) 国際特許分類:
G06F 21/10 (2013.01) *G06F 21/62* (2013.01)
- (21) 国際出願番号: PCT/JP2014/004670
- (22) 国際出願日: 2014 年 9 月 11 日(11.09.2014)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2013-198689 2013 年 9 月 25 日(25.09.2013) JP
- (71) 出願人: NECソリューションイノベータ株式会社(NEC SOLUTION INNOVATORS, LTD.) [JP/JP];
〒1368627 東京都江東区新木場一丁目 1 8 番 7 号 Tokyo (JP).
- (72) 発明者: 島津 秀雄(SHIMAZU, Hideo); 〒1368627
東京都江東区新木場一丁目 1 8 番 7 号 NEC ソリューションイノベータ株式会社内 Tokyo (JP).
- (74) 代理人: 下坂 直樹(SHIMOSAKA, Naoki); 〒1088001
東京都港区芝五丁目 7 番 1 号日本電気株式会社内 Tokyo (JP).

- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーロパ (AM, AZ, BY, KG, KZ, RU, TJ, TM), ユーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

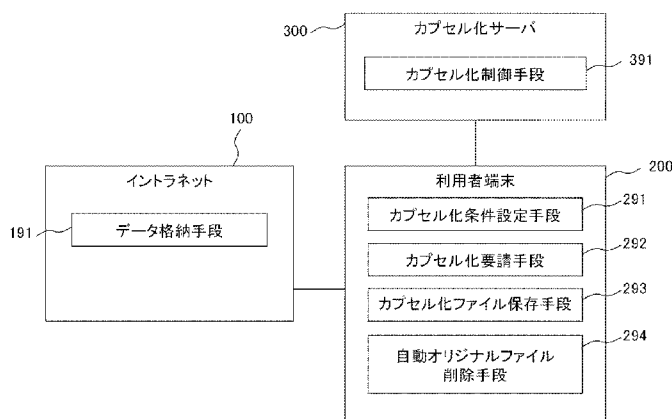
添付公開書類:

— 国際調査報告 (条約第 21 条(3))

(54) Title: FILE MANAGEMENT SYSTEM AND USER TERMINAL USED IN FILE MANAGEMENT SYSTEM

(54) 発明の名称: ファイル管理システムおよびファイル管理システムに用いる利用者端末

[図16]



- 100 Intranet
191 Data storage means
200 User terminal
291 Encapsulation condition setting means
292 Encapsulation request means
293 Encapsulated file storage means
294 Automatic original file deletion means
300 Encapsulation server
391 Encapsulation control means

(57) Abstract: [Problem] The purpose of the invention is to allow one using a terminal that does not have a digital rights management (DRM) system to create an encapsulated file from an original file, by adding access rights thereto and encrypting the same, while ensuring that the original file in the state prior to the aforementioned process does not remain. [Solution] A file management system comprises an intranet having a data storage means, an encapsulation server, and a user terminal which is capable of accessing the intranet and the encapsulation server. The user terminal further comprises an encapsulation request means for sending an original file and access rights information to the encapsulation server and receiving an encapsulated file whereupon the encapsulation is completed. The user terminal further comprises an encapsulated file storage means for storing the encapsulated file in the data storage means, and an automatic original file deletion means for deleting the original file upon the storing of the encapsulated file.

(57) 要約:

[続葉有]



〔課題〕 デジタル権利管理（DRM）を基盤としてもたない端末を用いながら、オリジナルファイルにアクセス権を付加して暗号化したカプセル化ファイルの作成を行い、かつ処理前のオリジナルファイルを残さないようにする。〔解決手段〕ファイル管理システムは、データ格納手段を有するイントラネットと、カプセル化サーバと、イントラネットとカプセル化にアクセスが可能な利用者端末を有する。利用者端末は、カプセル化サーバにオリジナルファイルとアクセス権情報とをカプセル化サーバに送り、カプセル化が完了したカプセル化ファイルを受信するカプセル化要請手段を有する。また利用者端末は、カプセル化ファイルをデータ格納手段に保存するカプセル化ファイル保存手段と、カプセル化ファイルの保存を契機としてオリジナルファイルを削除する自動オリジナルファイル削除手段とを有する。

明 細 書

発明の名称：

ファイル管理システムおよびファイル管理システムに用いる利用者端末 技術分野

[0001] 本発明は、ファイル管理システムおよびファイル管理システムに用いる利用者端末に関する。

背景技術

[0002] 企業では、膨大な量の電子ファイル（以下、ファイルと呼ぶ）が作成され、個人のPC（Personal Computer）やファイルサーバに格納され、流通されている。その中には、機密性の高い情報が多数含まれている。例えば、未発表製品の価格表が記載された表計算ソフトのデータ、人事情報などが記載されたワープロファイル、公表前の広報用資料が記載されたプレゼンテーションファイル、他社との連携に関する機密情報のやりとりが記述された電子メール、等が含まれる。

[0003] しかし、それらは、必ずしも十分に管理されていないのが実態であり、企業の情報漏えいのリスクを増大させている。そこで、最近では、それを解決する方法として、ファイルそのものが「自分で自分の身を守る」仕組みが採用されるようになってきた。この仕組みが、デジタル権利管理（Digital Rights Management, DRM）である。DRMは、元々、映像コンテンツや音楽コンテンツなどの有料コンテンツを小額課金で取引する仕組みとして普及が始まったものだが、これを、企業のファイルの管理に対しても適用している。

[0004] 一般的なDRMを利用する場合、ファイルの作成者が、そのファイルに対するアクセス権を設定する。そしてファイルとアクセス権情報とを一つにまとめて暗号化する。ここでは、この操作を「カプセル化」と呼ぶこととする。また、アクセス権とは、ファイルを利用できる人と、その人がファイルに対して実行可能な操作を規定するものである。具体的には例えば、参照のみ

可能、編集・変更可能、すべての権利を行使可能、などである。

[0005] 利用者がカプセル化されたファイルを利用する場合には、カプセル化サーバが、利用者のアクセス権を検証した上で、カプセル化の解除を行い、利用者にカプセル化が解除されたファイルを返送する。ここでは、この解除操作を「非カプセル化」とも呼ぶこととする。利用者は自身が所有するアクセス権に応じたファイルの操作を実行することが出来る。

[0006] なお、上記の一般的なDRMを利用するためには、利用者端末がそのDRMを実行するためのDRM機能を内蔵している必要がある。内蔵していない場合は、DRMの管理下にあるファイルを利用することが出来ない。

[0007] ところが、近年、クラウド環境の発達により、DRM機能を持たない端末からもDRMで管理されたファイルを利用したいという要求が高まっている。例えば、スマートフォンやタブレットPC、公共のコンピュータなど、DRM機能を持たない端末からも、ファイルのカプセル化および非カプセル化を利用できる方法の確立が望まれている。

[0008] この課題を解決する技術も種々検討されている。ファイルのカプセル化については、例えば特許文献1にその方法が開示されている。この方法では、利用者端末からの要請により、カプセル化サーバがカプセル化を代行する。利用者端末がオリジナルファイルとアクセス権情報をセットにしてカプセル化サーバに送信すると、カプセル化サーバがカプセル化ファイルを生じて返送し、利用者端末はカプセル化ファイルを受取ることができる。特許文献1自体は利用者端末がDRM機能を持たないことを前提としたものではないが、この技術を応用することにより、DRM機能を持たない利用者端末からもカプセル化を行うことが可能である。

[0009] また非カプセル化については、例えば特許文献2にDRM機能を持たない端末を用いて、カプセル化されたファイルを利用する一方法が開示されている。この技術を用いると、DRM機能を持たない端末からもカプセル化ファイルを閲覧することが出来る。そのプロセスは次の通りである。

1) まず利用者は、カプセル化ファイルと、自身のアクセス権情報をカプセ

ル化サーバに送信する。

2) カプセル化サーバは、利用者がアクセス権を有するか確認する。

3) アクセス権が確認された場合は、カプセル化を解除し、中身のファイルを利用者が閲覧可能な形式に変換する。この形式は、閲覧のみが可能であり、コピー、ペースト、印刷、変更、画面キャプチャなどが一切できないものとする。これは利用者が編集等閲覧より上の権限を有していたとしても同様に閲覧のみ可能とする。なお、アクセス権が確認されなかった場合には、要求を却下しカプセル化を解除しない。

[0010] 以上、説明したように特許文献1、特許文献2によればDRM機能を持たない端末を用いてもDRMを用いたファイルのカプセル化、およびカプセル化されたファイルの閲覧を行うことが出来る。

[0011] また特許文献3、特許文献4にも、関連する技術が開示されている。

先行技術文献

特許文献

[0012] 特許文献1：特開2010-117983号公報

特許文献2：特表2013-504136号公報

特許文献3：特表2010-505206号公報

特許文献4：特開2008-123049号公報

発明の概要

発明が解決しようとする課題

[0013] しかしながら、これらの技術にはそれぞれ問題点があった。

[0014] 特許文献1の技術の問題点は、カプセル化ファイルの元となったオリジナルファイルがそのまま利用者端末に残ってしまうことである。オリジナルファイルが残ると不正アクセスがあった場合に情報が盗まれてしまう。オリジナルファイルを利用者が削除すれば問題ないが、怠ったり、忘れたりする危険があった。

[0015] また、特許文献2の技術には、利用者が、ファイルの閲覧以外の操作が出

来ないという問題点があった。企業においては、複数の利用者がファイルを編集したり、属性を変更したりしたいというニーズが数多く存在する。特許文献2の技術ではこのニーズに応えることが出来ない。

[0016] 本発明は上記の問題点に鑑みてなされたものであり、DRM機能を持たない端末を用いて、ファイルのカプセル化、非カプセル化を実行可能にする方法を提供することを目的とする。また、非カプセル化されたファイルに対し閲覧以外の操作を可能とする方法を提供すること、および情報流出リスクを低減する方法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

[0017] 上記の課題を解決するため、本発明のファイル管理システムは、データ格納手段を備えるイントラネットと、オリジナルファイルと前記オリジナルファイルに対するアクセス権情報とをまとめて暗号化してカプセル化ファイルを生成するカプセル化サーバと、前記イントラネットおよび前記カプセル化サーバにアクセス可能な利用者端末と、を有し、前記カプセル化サーバが前記利用者端末から前記オリジナルファイルと前記アクセス権情報とを受け取り前記カプセル化ファイルを生成し前記カプセル化ファイルを前記利用者端末に返送するカプセル化制御手段を有し、前記利用者端末がカプセル化条件を設定するカプセル化条件設定手段と前記カプセル化サーバにカプセル化を要請するカプセル化要請手段と返送された前記カプセル化ファイルを前記データ格納手段に保存するカプセル化ファイル保存手段と前記カプセル化ファイルの保存を契機として前記ファイル格納手段に格納された前記オリジナルファイルを自動的に削除する自動ファイル削除手段と、を有している。

発明の効果

[0018] 本発明の効果は、DRMを基盤としてもたない端末を用いて情報漏えいが防止できることである。これはオリジナルファイルをカプセル化し、オリジナルファイルが自動的に削除されるためである。

図面の簡単な説明

[0019] [図1]本発明第2の実施の形態を示すブロック図である。

[図2]本発明第2の実施の形態に用いるアクセス権の一例である。

[図3]本発明第2の実施の形態に用いる認証情報の一例である。

[図4]本発明第2の実施の形態の動作を示すフローチャートである。

[図5A]本発明第2の実施の形態の処理前の具体例を示すブロック図である。

[図5B]本発明第2の実施の形態の処理後の具体例を示すブロック図である。

[図6]本発明第3の実施の形態の動作を示すフローチャートである。

[図7]本発明第4の実施の形態を示すブロック図である。

[図8]本発明第4の実施の形態の非カプセル化要請部の動作を示すフローチャートである。

[図9]本発明第4の実施の形態の非カプセル化サーバの動作を示すフローチャートである。

[図10]本発明第5の実施の形態を示すブロック図である。

[図11]本発明第6の実施の形態を示すブロック図である。

[図12]本発明第6の実施の形態の動作を示すフローチャートである。

[図13]本発明第7の実施の形態を示すブロック図である。

[図14]本発明第8の実施の形態を示すブロック図である。

[図15]本発明第9の実施の形態を示すブロック図である。

[図16]本発明第1の実施の形態を示すブロック図である。

発明を実施するための形態

[0020] 次に、本発明の実施の形態について図面を参照して詳細に説明する。

[0021] 〔第1の実施形態〕

図16は、本発明第1の実施の形態を示すブロック図である。ファイル管理システムは、イントラネット100とカプセル化サーバ300と、イントラネット100およびカプセル化サーバ300にアクセスが可能な利用者端末200と、を有している。

[0022] イン트라ネット100は、データを格納するデータ格納手段191を有している。

[0023] カプセル化サーバ300は、オリジナルファイルとオリジナルファイルに

対するアクセス権情報とをまとめて暗号化してカプセル化ファイルを生成するカプセル化制御手段391を有している。カプセル化制御手段391は、利用者端末200からオリジナルファイルとアクセス権情報とを受け取り、カプセル化ファイルを生成し生成したカプセル化ファイルを利用者端末200に返送する。ここでアクセス権情報とは、オリジナルファイルについて誰にどのような操作を許容するかを規定する情報である。

[0024] 利用者端末200は、カプセル化条件を設定するカプセル化条件設定手段291と、カプセル化サーバ300にカプセル化を要請するカプセル化要請手段292と、を有する。カプセル化条件設定手段291は、オリジナルファイルに付与するアクセス権情報を設定する。また、利用者端末200は、カプセル化サーバ300から受け取ったカプセル化ファイルをデータ格納手段191に保存するカプセル化ファイル保存手段293を有する。さらに、当該カプセル化ファイルの保存を契機として、データ格納手段191に格納されたオリジナルファイルを自動的に削除する自動オリジナルファイル削除手段294を有している。

[0025] 以上説明したように、本実施の形態によれば、DRMを基盤としてもたない端末を用いて、オリジナルファイルをカプセル化し、元のオリジナルファイルを自動的に削除することができる。このため情報漏えいが防止できる。

[0026] 〔第2の実施形態〕

図1は第2の実施の形態のファイル管理システムを示すブロック図である。本実施の形態では、ファイル管理システムの構成および動作の詳細を示す。

[0027] イン트라ネット100にデータ格納部101とアクセス権情報格納部102とが設けられている。また利用者端末200がイン트라ネット100に接続されている。またカプセル化サーバ300がインターネットやイン트라ネットなどのネットワーク上に配置されている。利用者端末200には利用者ID格納部201、カプセル化条件設定部202、カプセル化要請部203、カプセル化ファイル保存部204、自動オリジナルファイル削除部205

が設けられている。ここでIDとは識別子 (i d e n t i f i e r) の略である。カプセル化サーバ300には利用可能者ID格納部301、カプセル化制御部302が設けられている。

[0028] データ格納部101はイントラネット内のストレージであり、オリジナルファイルやカプセル化ファイルが格納される。

[0029] アクセス権情報格納部102は、オリジナルファイルをカプセル化する時に用いるアクセス権情報を格納する。ここで、アクセス権とは、当該ファイルへアクセスできる利用者と、各利用者が利用できるファイル操作を規定するものである。図2にアクセス権設定リストの一例を示す。利用可能なユーザーがリストの5名であり、それぞれのアクセス権は、Shimazuは全ての操作が可能、Yamadaが参照、編集、削除、カプセル化が可能、Takahashiが参照と編集が可能、KimuraとSuzukiが参照のみ可能となっている。なお、これはあくまで一例であり、本発明の適用はアクセス権の設定方法に限定されるものではない。

[0030] 図1に戻って、カプセル化サーバ300について説明する。カプセル化サーバ300は、外部からの要請により、オリジナルファイルとアクセス権情報を受け取り、カプセル化ファイルを生成して返送する。カプセル化サーバ300は、例えばイントラネットまたはインターネット上の独立したWEBサーバとして動作する。カプセル化要請部203からカプセル化サーバ300へのカプセル化要請は、例えばインターネット上のリクエストとして送信され、カプセル化サーバ300がこれを受付ける形になる。リクエストの形式は、例えばHTTP形式 (H y p e r T e x t T r a n s f e r P r o t o c o l) を用いることができる。

[0031] 利用可能者ID格納部301はカプセル化サーバ300を利用可能な利用者のIDを格納する。またパスワードなどの認証情報も格納する。カプセル化制御部302は、カプセル化の実行に先立って、利用可能者ID格納部301を参照し、利用者に利用資格があるか判定する。なお、利用者の成りすましを防止するため、例えば、図3に示すようなそれぞれの利用者IDに対

してパスワードを設定するなど、認証情報を設定するとよい。なお、ここでは例としてパスワードを挙げたが、認証情報には、必要に応じて任意の方法を用いることができる。

[0032] カプセル化制御部302は、受信したオリジナルファイルとアクセス権情報からカプセル化ファイルを生成し、利用者端末200に返送する。

[0033] 利用者端末200はイントラネットにアクセス可能な端末であり、利用者ID格納部201、カプセル化条件設定部202、カプセル化要請部203、カプセル化ファイル保存部204、自動オリジナルファイル削除部205を有する。利用者端末200は、具体的には、例えばスマートフォンやタブレットPC (Personal Computer) などであり、DRM機能を持っていないものとする。あるいは持っていないが本実施の形態では使用しない。

[0034] 利用者ID格納部201は、カプセル化サーバの利用に必要な利用者IDと、認証に必要なパスワードなどを保持する。

[0035] カプセル化条件設定部202は、利用者がカプセル化するオリジナルファイルを指定し、オリジナルファイルに対するアクセス権を設定する手段である。

[0036] カプセル化要請部203は、設定されたカプセル化条件に従って、カプセル化サーバ300にカプセル化の実行とカプセル化ファイルの返送を要請する手段である。カプセル化要請部203は、オリジナルファイルをデータ格納部101から取り出し、設定されたアクセス権情報とともにカプセル化サーバ300に送信する。またカプセル化要請に先立ち、利用者IDおよび必要な認証情報を送信して認証を確立する機能も有する。

[0037] カプセル化ファイル保存部204は、カプセル化サーバ300から返送されたカプセル化ファイルを、データ格納部101のオリジナルファイルと同じパスに保存する。

[0038] 自動オリジナルファイル削除部205は、カプセル化ファイルの保存が完了するとオリジナルファイルを強制的に削除する。これにより、オリジナル

ファイルがカプセル化ファイルに置き換えられたことになる。

[0039] 次に本実施の形態におけるカプセル化動作について説明する。

[0040] 図4は利用者端末200の動作を示すフローチャートである。なお説明に用いる符号は図1と同じものを用いる。利用者がカプセル化するオリジナルファイル名と、設定するアクセス権情報と、を入力し、カプセル化条件設定部202がこれを受付け(S101)、アクセス権情報格納部102にアクセス権情報を保存する(S102)。次にカプセル化要請部203がデータ格納部101からオリジナルファイルを取り出し、そのパスを記憶する(S103)。次にカプセル化要請部203が利用者ID格納部201から利用者IDと認証情報を取り出しカプセル化サーバ300に送信する(S104)。カプセル化サーバ300の認証が確立しない場合は(S105__NO)、カプセル化を中止する。カプセル化サーバ300の認証が成功したら(S105__YES)、オリジナルファイルとアクセス権情報をセットにしてカプセル化サーバ300に送信する(S106)。カプセル化が完了し、カプセル化サーバ300からカプセル化ファイルが返送されたら、カプセル化要請部203がこれを受信する(S107)。次にカプセル化ファイル保存部204がカプセル化ファイルをデータ格納部101の元のオリジナルファイルと同じパスに保存する(S108)。保存が完了したら自動オリジナルファイル削除部205が、元のオリジナルファイルを削除する(S109)。以上のようにして、オリジナルファイルとカプセル化ファイルとの置き換えが完了する。なおS104からS105の認証は、S101からS103の間の任意のタイミングで行っても問題ない。

[0041] 次に具体的な例を用いて、本実施の形態の概要を説明する。図5(図5A、図5B)は具体例を示すブロック図である。図5A、図5Bでは、符号が1から始まるものをオリジナルファイル、2から始まるものをカプセル化ファイルとする。図5Aは初期状態であり、データ格納部101にはオリジナルファイル1A、カプセル化ファイル2B、2Cが格納されている。ここで、図5A中の矢印で示すように、利用者端末200が、1Aのカプセル化を

、カプセル化サーバ300に要請する。

[0042] カプセル化サーバ300は、カプセル化を実行しカプセル化ファイル2Aを生成する。次いでカプセル化サーバ300は2Aを利用者端末200に返送する。

[0043] 利用者端末200が2Aを受信すると、図5Bの矢印で示すように、データ格納部101に2Aが保存され、元のオリジナルファイル1Aが削除される。以上の動作によって、図5Bでは、データ格納部101には、カプセル化ファイル2だけが保持され、オリジナルファイル1が存在しなくなる。以上説明したように、本実施の形態によれば、データ格納部101に格納されているファイルを全てカプセル化ファイルとすることができる。

[0044] 以上説明したように、本実施の形態によれば、オリジナルファイルを確実に削除し、カプセル化ファイルとして安全に保持することが出来る。

[0045] 〔第3の実施形態〕本実施の形態は、第2の実施の形態と大部分は同じであるが、カプセル化ファイルの保存とオリジナルファイルの削除方法が異なる。図6は本実施の形態、カプセル化要請部203の動作を示すフローチャートである。なお説明に用いる符号は図1と同じものを用いる。

[0046] S201からS207までは第1の実施の形態のS101からS107と同じである。本実施の形態ではカプセル化ファイルを受信すると（S207）、カプセル化ファイルを元のオリジナルファイル1と同じ名前でデータ格納部101に上書き保存する（S208）。このようにすると、カプセル化ファイル2の保存とオリジナルファイル1の置き換えが確実であり、効率も良い。

[0047] 〔第4の実施形態〕本実施の形態は、DRM機能を持たない端末が、カプセル化ファイルのカプセル化を解除してオリジナルの利用を可能とするものである。利用者端末200は、カプセル化ファイルの非カプセル化を非カプセル化サーバ300に要請し、閲覧だけでなく編集等も行えるオリジナルファイルとして受信する。

[0048] 図7は本実施の形態のシステム構成を示すブロック図である。イントラネ

ット１００にデータ格納部１０１とアクセス権情報格納部１０２が設けられている。これらの構成は第２、第３の実施の形態と同様である。また利用者端末２００がイントラネット１００に接続されている。また非カプセル化サーバ４００がインターネットやイントラネットなどのネットワーク上に配置されている。非カプセル化サーバ４００には、利用可能者ＩＤ格納部４０１と非カプセル化制御部４０２が設けられている。

[0049] 非カプセル化サーバ４００は、外部からの要請により、カプセル化ファイルのカプセル化を解除して、オリジナルファイルを生成する。

[0050] 利用可能者ＩＤ格納部４０１は非カプセル化サーバ４００を利用可能な利用者のＩＤおよび認証情報を格納する。非カプセル化制御部４０２が非カプセル化を実行する際には、利用可能者ＩＤ格納部４０１を参照し利用資格があるか判定する。判定には利用者ＩＤだけでなく、任意の認証情報も用いることができる。

[0051] 非カプセル化制御部４０２は、認証の確立した利用者からカプセル化ファイルを受取ると、カプセル化を解除してカプセル化ファイルの中のアクセス権情報を参照する。ここで利用者ＩＤに全てのファイル操作が可能なアクセス権（フルアクセス権と称する）が付与されていることが確認できた場合は、カプセル化ファイルからオリジナルファイルを取り出し、利用者に返送する。

[0052] 利用者端末２００には、利用者ＩＤ格納部２０１、非カプセル化条件設定部２１２、非カプセル化要請部２１３、オリジナルファイル保存部２１４、自動カプセル化ファイル削除部２１５が設けられている。

[0053] 非カプセル化条件設定部２１２は利用者が、非カプセル化するファイルを指定する手段である。

[0054] 非カプセル化要請部２１３は、利用者ＩＤおよび必要な認証情報とデータ格納部１０１に格納されたカプセル化ファイルのコピーを非カプセル化サーバ４００に送り、非カプセル化を要請する。

[0055] オリジナルファイル保存部２１４は、非カプセル化サーバ４００から返送

されたオリジナルファイルを元のカプセル化ファイルと同じパスに保存する。自動カプセル化ファイル削除部215は、オリジナルファイルの保存が完了したら、元のカプセル化ファイルを強制的に削除する。

[0056] 次に本実施の形態の非カプセル化動作について説明する。利用者があるカプセル化ファイルを非カプセル化しようとする場合、利用者は非カプセル化条件設定部212に、非カプセル化するファイル名を指定する。非カプセル化要請部213は指定されたカプセル化ファイルの非カプセル化を、非カプセル化サーバ400に要請する。

[0057] 図8は非カプセル化における利用者端末200の動作を示すフローチャートである。なお説明に用いる各部の符号は図7と同じものを用いる。利用者が非カプセル化するファイルを指定すると、まず非カプセル化条件設定部212がこのファイル名を受付ける(S301)。次に、非カプセル化要請部213が、データ格納部101から指定されたカプセル化ファイルを取り出し、パスを記憶する(S302)。次に利用者IDと必要な認証情報を非カプセル化サーバ400に送信する(S303)。認証が失敗した場合は(S304__NO)、非カプセル化を中止する。認証に成功したら(S304__YES)、カプセル化ファイルを非カプセル化サーバ400に送信する(S305)。非カプセル化サーバ400では、カプセル化ファイルを復号化して、利用者が全ての操作が可能な権限(フルアクセス権)を有しているかを判定する。そして、フルアクセス権を有していれば復号化されたファイルからオリジナルファイルを取り出し、非カプセル化要請部213に返送する。非カプセル化サーバの動作については後述する。次に非カプセル化要請部213は、オリジナルファイルを受信する(S306)。次にオリジナルファイル保存部214が受信したオリジナルファイルを元のカプセル化ファイルと同じパスに保存する(S307)。保存が完了したら自動カプセル化ファイル削除部215が、データ格納部101に格納されている元のカプセル化ファイルを削除する(S308)。以上のようにして、カプセル化ファイル2がオリジナルファイル1に置き換えられ、利用者はオリジナルファイル1

を自由に操作することが出来る。また同名のファイルが2つ存在することによる混乱を避けることが出来る。

[0058] 次に非カプセル化サーバ400の動作について説明する。図9は非カプセル化サーバ400の動作を示すフローチャートである。なお説明に用いる各部の符号は図7と同じものを用いる。まず非カプセル化サーバの正当な利用者か認証するための認証情報を受信する(S401)。次に非カプセル化サーバ400は、利用可能者ID格納部401を参照し、利用者が非カプセル化サーバ400の正当な利用者であるかを調査する(S402)。利用者IDが登録されていなければ(S403__NO)、非カプセル化の要請を拒否して終了する。利用者IDの登録が確認できたら認証OKとし(S403__YES)、認証成功メッセージを送信する(S404)。次に利用者端末からカプセル化ファイルが送信され、非カプセル化サーバ400はこれを受信する(S405)。次に非カプセル化サーバ400は、カプセル化ファイルを復号化する(S406)。次に復号化されたアクセス権情報を参照し、利用者が全ての操作が可能であるフルアクセス権を有しているか調査する(S407)。フルアクセス権がない場合には(S408__NO)、復号化したファイルを再カプセル化し、利用者端末に対し、非カプセル化不可のメッセージを送信して終了する。再カプセル化したカプセル化ファイルは削除するか、非カプセル化要請部213に返送する。利用者がフルアクセス権を有していると判定された場合は(S408__YES)、復号化されたファイルからオリジナルファイルを取り出して、利用者端末に返送する。

[0059] 以上のようにして、利用者はオリジナルファイルを受取ることが出来る。またこれを許されるのが、全ての操作が可能なフルアクセス権を有する利用者だけであるため、利用者の範囲を最低限にとどめることが出来る。また、元のカプセル化ファイルが削除されるため、同名のファイルが2つ存在することによる混乱を避けることができる。

[0060] なお、第2の実施の形態と同様に、受信したオリジナルファイルを、元のカプセル化ファイル2に対し同名で上書き保存すると、ファイルの保存と削

除が同時に出来るため、確実であり、効率が良い。

[0061] 〔第5の実施形態〕図10は、本発明第4の実施の形態を示すブロック図である。本実施の形態ではカプセル化と非カプセル化の両方を実施する仕組みが実装されている。

[0062] イン트라ネット100にデータ格納部101とアクセス権情報格納部102とが設けられている。これらの構成は第2～4の実施の形態と同様である。また利用者端末200がイントラネット100に接続されている。そしてカプセル化制御サーバ500がインターネットやイントラネットなどのネットワーク上に配置されている。カプセル化制御サーバ500には、利用可能者ID格納部501とカプセル化非カプセル化制御部502が設けられている。

[0063] カプセル化制御サーバ500は、外部からの要請に応じて、オリジナルファイルのカプセル化を行い、またカプセル化ファイルの非カプセル化を行う。

[0064] またカプセル化制御サーバ500は、利用可能者ID格納部501を参照し、利用者に利用資格があるか判定する。

[0065] 利用者端末200は、カプセル化制御条件設定部222と、カプセル化制御要請部223と、ファイル保存部224と、自動ファイル削除部225を有する。

[0066] カプセル化制御条件設定部222では、どのファイルの処理を要請するのか、またそれがカプセル化なのか非カプセル化なのかを指定する。またカプセル化においては、どのようなアクセス権を設定するかを指定する。

[0067] カプセル化制御要請部223は、カプセル化制御条件設定部222に指示された条件に従って、オリジナルファイルのカプセル化、またはカプセル化ファイルの非カプセル化を、カプセル化制御サーバ500に要請する。カプセル化制御サーバ500、利用可能者ID格納部501を参照して認証を行い、カプセル化非カプセル化制御部502がカプセル化、または非カプセル化処理を行う。処理が完了して返送されたファイルはファイル保存部224

によってデータ格納部 101 に格納される。そして保存が完了すると、元のオリジナルファイルまたは元のカプセル化ファイルが自動ファイル削除部 225 によって強制的に削除される。

[0068] カプセル化および非カプセル化の動作については、第 2～第 4 の実施の形態と同様であるため、説明を省略する。

[0069] 以上のように、カプセル化と非カプセル化の両方を実行できるようにしておくことには、例えば次の様な利点がある。まず利用者が非カプセル化を行ってオリジナルファイルを利用するとする。そのままでは、オリジナルファイルが残ってしまうので、利用が済んだらオリジナルファイルを再びカプセル化する。本実施の形態では、カプセル化と同時にオリジナルファイルの削除が自動的に行われるため、オリジナルファイルを利用している期間以外は、ファイルはカプセル化されている。したがって情報を安全に保持することが出来る。

[0070] 〔第 6 の実施形態〕前記したように、第 5 の実施の形態を利用すると、利用者はオリジナルファイル 1 を自由に利用できるし、利用している期間以外はファイルをカプセル化して格納することができる。しかしながら、利用者が一つずつファイルをカプセル化するのは面倒であり、これを怠ったり、カプセル化されていないオリジナルファイルを見落とししたりする可能性がある。そこで、本実施の形態では、自動的にオリジナルファイルを見つけ、これをカプセル化し、元のオリジナルファイルを削除する仕組みを提供する。

[0071] 図 11 は本実施の形態のファイル管理システムを示すブロック図である。イントラネット 100 にデータ格納部 101 とアクセス権情報格納部 102 と標準アクセス権情報格納部 103 が設けられている。また利用者端末 200 がイントラネット 100 に接続されている。利用者端末 200 は、利用者 ID 格納部 201 と、自動カプセル化要請部 233 と、自動カプセル化ファイル保存部 234 と、自動オリジナルファイル削除部 235 と、自動ファイル巡回検査部 236 と、巡回制御タイマー 237 と、を有する。またカプセル化制御サーバ 500 がインターネットやイントラネットなどのネットワー

ク上に配置されている。カプセル化制御サーバ500には、利用可能者ID格納部501とカプセル化非カプセル化制御部502が設けられている。なおカプセル化制御サーバ500をカプセル化サーバ300に置き換えた構成とすることもできる。

[0072] 標準アクセス権情報格納部103は、オリジナルファイルをカプセル化する時に用いる標準アクセス権情報を格納する。標準アクセス権は、自動的にカプセル化するファイルのアクセス権として事前に定めたアクセス権である。例えば、「当社の社員は全ての操作が可能」とか「本人はすべての操作が可能、それ以外は参照のみ」などとする。

[0073] 自動ファイル巡回検査部236は、データ格納部101に格納されているファイルを1つずつチェックし、オリジナルファイルを検出したら自動カプセル化要請部233にファイル名を送信する。

[0074] 自動カプセル化要請部233は自動ファイル巡回検査部236からファイル名を受信すると、そのオリジナルファイルのカプセル化を、カプセル化制御サーバ500に要請する。このときデータ格納部101からオリジナルファイルを取り出し、標準アクセス権情報格納部103から標準アクセス権情報を取り出し、カプセル化要請とともにカプセル化制御サーバ500に送信する。なおカプセル化要請に先立って利用者IDを送信し、必要な認証は確立しておく。

[0075] 自動カプセル化ファイル保存部234は、カプセル化制御サーバ500から返送された、カプセル化ファイル2をデータ格納部101の元のオリジナルファイル1と同じパスに保存する。

[0076] 自動オリジナルファイル削除部235はカプセル化ファイル2の保存を契機として、自動的に元のオリジナルファイル1を削除する。なお、自動カプセル化ファイル保存部234がカプセル化ファイル2を元のオリジナルファイルに同名で上書き保存する仕様とした場合は、自動オリジナルファイル削除部235は設けなくても良い。

[0077] 巡回制御タイマー237は、予め設定されたインターバルを用いて、自動

ファイル巡回検査部 236 の起動と停止をと制御する。巡回制御タイマー 237 には、起動インターバルと、起動から終了までの継続インターバルの 2 つを外部から設定しておく。巡回制御タイマー 237 は、現在時刻を記録し、起動インターバルごとに、自動ファイル巡回検査部 236 を起動する。そして前記の継続インターバルの時間間隔が来ると自動ファイル巡回検査部 236 の動作を強制的に中断させる。

[0078] 次に、自動ファイル巡回検査部 236 の動作について説明する。図 12 は自動ファイル巡回検査部 236 の動作を示すフローチャートである。なお説明に用いる各部の符号は図 11 と同じものを用いる。

[0079] まず巡回制御タイマー 237 から起動命令を受信し起動する (S501)。次いでデータ格納部に格納されたファイルを一つずつ検査する (S502)。調べたファイルがオリジナルファイルでない場合は (S503__NO)、次のファイルの検査に進む。オリジナルファイルを検出した場合は (S503__YES)、自動カプセル化要請部 233 にファイル名を送信する (S504)。巡回制御タイマー 237 から停止命令を受信した場合は停止する (S505__YES)。停止命令が無かった場合には (S505__NO)、ファイル検査に戻って次のファイルを検査する。なおここでは、巡回制御タイマー 237 からの停止命令が、S504 (自動カプセル化要請部 233 へのファイル名送信) 後に停止命令を受信する例を示した。しかしながら、停止命令は任意のタイミングで受信され、自動ファイル巡回検査部 236 は任意のタイミングで停止される。

[0080] 自動ファイル巡回検査部 236 は、終了することがなく永遠に動き続けるプログラムの構成をしており、利用者端末 200 がマルチタスクシステムの場合、本来の操作を妨げないように、優先度の低いタスクとして動作させることが望ましい。本実施の形態では、巡回制御タイマー 237 の働きにより、適当なタイミングで動作を一時中断する仕組みとしている。しかしながら、利用者端末 200 が十分強力で自動ファイル巡回検査部 236 がバックグラウンドで動作していても、本来の操作を妨げることがないなら、インター

バルを無限大にして、常に動作させておくことも可能である。

[0081] 以上説明したように、本実施の形態によれば、オリジナルファイル 1 を取りこぼすことなくカプセル化ファイル 2 に置き換えられるため。確実に情報を保護することが出来る。

[0082] 〔第 7 の実施形態〕利用者端末 200 がスマートフォンやタブレット PC などの携帯機器の場合、バックグラウンドのプログラムが増えると電池の消耗が早まるので、利用者から好まれない。本実施の形態では、電池の消耗を心配せずにファイルの自動カプセル化を実行する手段を提供する。

[0083] 図 13 は第 7 の実施の形態を示すブロック図である。利用者端末 200 は、第 6 の実施の形態の構成に加えて、充電状況格納部 239 を備えている。また巡回制御タイマーが、充電状況に依存して巡回を制御する充電状況依存型巡回制御タイマー 238 となっている。

[0084] 充電状況格納部 239 は、利用者端末 200 が充電中であることを常に記録する。そして充電処理が中断された場合は、「充電処理が中止された」というイベントを割り込みイベントとして発生させる。これらは利用者端末 200 の制御回路（図示せず）で実現され、プログラムレベルでは、割り込みイベントとして検知されるのが一般的な実装である。

[0085] 充電状況依存型巡回制御タイマー 238 には、起動する起動インターバルと、起動から終了までの継続インターバルの 2 つを外部から設定しておく。充電状況依存型巡回制御タイマー 238 は、現在時刻を記録し、起動インターバルごとに、充電状況格納部 239 を調べて、充電中であるときのみ自動ファイル巡回検査部 236 を起動する。そして継続インターバルの時間間隔が来るまで動作する。ただし、充電状況格納部 239 から充電処理中止の割り込みイベントを受信すると、自動ファイル巡回検査部 236 の動作は強制的に中断される。

[0086] 以上、説明したように、本実施の形態によれば、充電中のみ自動カプセル化処理を行うため、自動カプセル化による電池の消耗を心配する必要がなくなる。

[0087] 〔第8の実施形態〕図14は本発明第8の実施の形態を示すブロック図である。本実施の形態では、自動カプセル化処理をイントラネット100の中に設けられた個人フォルダについてのみ行う。ここでは自動カプセル化の仕組としては、第7の実施の形態を適用した例を示している。イントラネット100の中に個人フォルダ110が設けられ、個人フォルダ110の中に、データ格納部101、アクセス権情報格納部102、標準アクセス権情報格納部103、が設けられている。イントラネットの規模が大きく、イントラネット内に個人フォルダが設けられ、そのフォルダの管理が利用者に任されているような場合は、このような形態が望ましい。動作については第7の実施の形態と同様である。

[0088] 〔第9の実施形態〕第6から第8の実施の形態では、データ格納部101、アクセス権情報格納部102、標準アクセス権情報格納部103がイントラネット100の中に置かれているものとした。ところが、これらが全て利用者端末200の中に設けられている場合にも、同様の形態が適用できる。なぜならば、この構成は、第1から第7の実施の形態で、利用者端末200がイントラネット100に常時接続している状態と実質的に同じだからである。

[0089] 図15は本実施の形態を示すブロック図である。本実施の形態の利用者端末200は、第7の実施の形態の利用者端末200の構成に加えて、データ格納部251、アクセス権情報格納部252、標準アクセス権情報格納部253が設けられている。動作については第7の実施の形態と同様である。

[0090] 本実施の形態においては、利用者が利用者端末200内に保持しているデータを漏れなくカプセル化できるので、セキュリティが向上する。また図15のように、充電依存型の自動カプセル化処理としておけば、利用者が利用者端末200を充電するたびに、自動カプセル化が実行されるので、非常に便利である。

[0091] なお、本実施の形態の利用者端末200に対するカプセル化、非カプセル化の処理に、他の実施の形態を適用できることは言うまでもない。

[0092] 以上、上述した実施形態を模範的な例として本発明を説明した。しかしながら、本発明は、上記実施形態には限定されない。即ち、本発明は、本発明のスコープ内において、当業者が理解し得る様々な態様を適用することができる。

[0093] この出願は、2013年9月25日に提出された日本出願特願2013-198689を基礎とする優先権を主張し、その開示の全てをここに取り込む。

符号の説明

- [0094]
- 1 オリジナルファイル
 - 2 カプセル化ファイル
 - 100 イン트라ネット
 - 101、251 データ格納部
 - 102、252 アクセス権情報格納部
 - 103、253 標準アクセス権情報格納部
 - 191 データ格納手段
 - 200 利用者端末
 - 201 利用者ID格納部
 - 202 カプセル化条件設定部
 - 203 カプセル化要請部
 - 204 カプセル化ファイル保存部
 - 205 自動オリジナルファイル削除部
 - 212 非カプセル化条件設定部
 - 213 非カプセル化要請部
 - 214 オリジナルファイル保存部
 - 215 自動カプセル化ファイル削除部
 - 222 カプセル化制御条件設定部
 - 223 カプセル化制御要請部
 - 224 ファイル保存部

- 2 2 5 自動ファイル削除部
- 2 3 3 自動カプセル化要請部
- 2 3 4 自動カプセル化ファイル保存部
- 2 3 5 自動オリジナルファイル削除部
- 2 3 6 自動ファイル巡回検査部
- 2 3 7 巡回制御タイマー
- 2 3 8 充電状況依存型巡回制御タイマー
- 2 3 9 充電状況格納部
- 2 9 1 カプセル化条件設定手段
- 2 9 2 カプセル化要請手段
- 2 9 3 カプセル化ファイル保存手段
- 2 9 4 自動オリジナルファイル削除手段
- 3 0 0 カプセル化サーバ
- 3 0 1、4 0 1、5 0 1 利用可能者 I D 格納部
- 3 0 2 カプセル化制御部
- 3 9 1 カプセル化制御手段
- 4 0 0 非カプセル化サーバ
- 4 0 2 非カプセル化制御部
- 5 0 0 カプセル化制御サーバ
- 5 0 2 カプセル化非カプセル化制御部

請求の範囲

- [請求項1] データ格納手段を備えるイントラネットと、オリジナルファイルと前記オリジナルファイルに対するアクセス権情報とをまとめて暗号化してカプセル化ファイルを生成するカプセル化サーバと、前記イントラネットおよび前記カプセル化サーバにアクセス可能な利用者端末と、を有し、前記カプセル化サーバが前記利用者端末から前記オリジナルファイルと前記アクセス権情報とを受け取り前記カプセル化ファイルを生成し前記カプセル化ファイルを前記利用者端末に返送するカプセル化制御手段を有し、前記利用者端末が、カプセル化条件を設定するカプセル化条件設定手段と、前記カプセル化サーバにカプセル化を要請するカプセル化要請手段と、返送された前記カプセル化ファイルを前記データ格納手段に保存するカプセル化ファイル保存手段と、前記カプセル化ファイルの保存を契機として前記ファイル格納手段に格納された前記オリジナルファイルを自動的に削除する自動ファイル削除手段と、を有することを特徴とするファイル管理システム。
- [請求項2] 前記カプセル化サーバが、前記カプセル化サーバの利用資格を有する利用者のID (i d e n t i f i e r) を格納する利用可能者ID格納部と、前記利用可能者ID格納部を参照して前記カプセル化サーバにアクセスした利用者IDが前記カプセル化サーバを利用可能であるか判定する利用資格判定部と、を有することを特徴とする請求項1に記載のファイル管理システム。
- [請求項3] 前記カプセル化ファイル保存部が前記カプセル化ファイルを前記オリジナルファイルと同名で前記オリジナルファイルに上書き保存するカプセル化ファイル上書き保存部を有する、ことを特徴とする請求項1に記載のファイル管理システム。
- [請求項4] 前記利用者端末からアクセスが可能であり前記カプセル化ファイルを非カプセル化して前記オリジナルファイルを取り出す非カプセル化サーバを有し、前記非カプセル化サーバが、前記利用者IDが前記オ

リジナルファイルに対するアクセス権を有している場合に非カプセル化を行う非カプセル化制御手段を有し、前記利用者端末が前記カプセル化ファイルと前記利用者IDとを前記カプセル化解除サーバに送信して非カプセル化を要請する非カプセル化要請手段と、前記オリジナルファイルを受信して前記データ格納手段に保存するオリジナルファイル保存手段と、前記オリジナルファイルの保存を契機として前記データ格納手段に格納された前記カプセル化ファイルを自動的に削除する自動カプセル化ファイル削除手段と、を有していることを特徴とする請求項1乃至請求項3いずれか一項に記載のファイル管理システム。

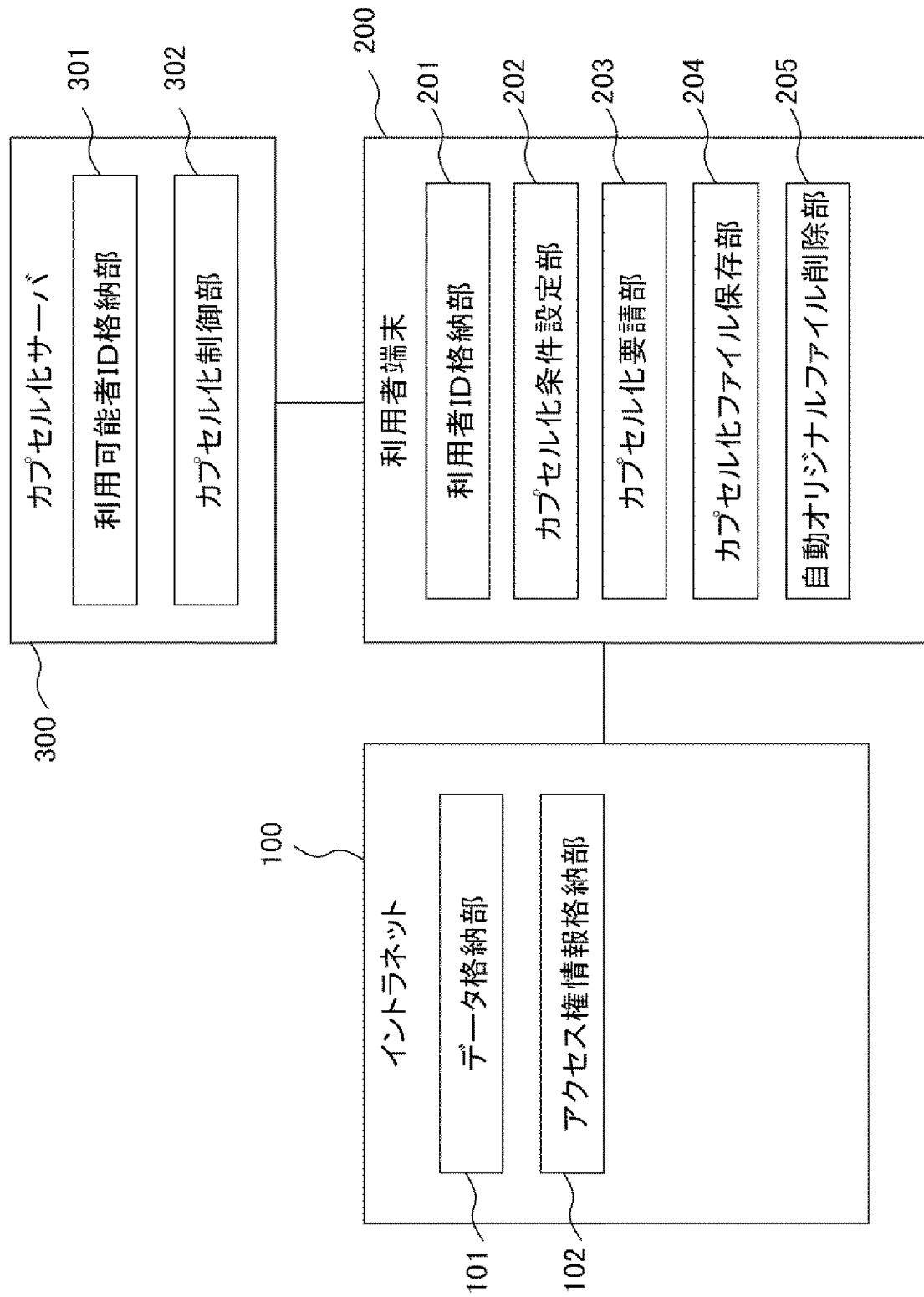
[請求項5] 前記カプセル化解除サーバが、前記カプセル化ファイルを復号化して前記カプセル化ファイル中のアクセス権情報を参照し前記利用者IDが前記カプセル化ファイルに対して全ての操作が可能なアクセス権を有しているか判定するアクセス権判定手段を有していることを特徴とする請求項4に記載のファイル管理システム。

[請求項6] 前記オリジナルファイル保存手段が、前記オリジナルファイルを前記カプセル化ファイルと同名で前記カプセル化ファイルに上書き保存するオリジナルファイル上書き保存手段を有している、ことを特徴とする請求項4または請求項5に記載のファイル管理システム。

[請求項7] 前記イントラネットが標準アクセス権情報が格納された標準アクセス権情報格納手段を有し、前記利用者端末が、前記データ格納手段を巡回しオリジナルファイルの存在を検出する自動ファイル巡回検査手段と、前記自動ファイル巡回検査部が前記オリジナルファイル検出した場合に前記オリジナルファイルと前記標準アクセス権情報格納部から取り出した前記標準アクセス権情報と前記利用者IDとを自動的に前記カプセル化サーバに送信してカプセル化を要請する自動カプセル化要請部を有する、ことを特徴とする請求項1乃至請求項3いずれか一項に記載のファイル管理システム。

- [請求項8] 前記巡回検査部を予め定められた時間間隔で起動および停止する巡回制御タイマーを有することを特徴とする請求項7に記載のファイル管理システム。
- [請求項9] 前記利用者端末が、電池と、前記電池を充電するための受電手段と、前記受電手段の受電状況を格納する受電状況格納手段と、前記受電状況格手段が受電を検知した時に前記自動ファイル巡回検査手段を起動しかつ前記充電状況検査手段が受電の途絶を検知した時に前記自動ファイル巡回検査手段を停止する充電状況依存型巡回制御タイマーと、を有することを特徴とする請求項7に記載のファイル管理システム。
- [請求項10] イン트라ネット内に設けられたファイル格納手段および前記ファイル格納手段に格納されたオリジナルファイルに対するアクセス権情報を格納するアクセス権情報格納手段と、ネットワーク上に配置され利用者から利用者IDとオリジナルファイルとアクセス権情報とカプセル化要請とを受け取り前記オリジナルファイルと前記アクセス権情報とをまとめて暗号化したカプセル化ファイルを生成し利用者に返送するカプセル化サーバと、前記イントラネットに接続する利用者端末と、を有するファイル管理システムに用いる利用者端末であって、前記利用者IDと前記オリジナルファイルと前記アクセス権情報とを前記カプセル化装置に送信してカプセル化ファイルの返送を要請するカプセル化要請手段と、前記カプセル化ファイルを前記ファイル格納手段に保存するカプセル化ファイル保存手段と、前記カプセル化ファイルの保存を契機として前記ファイル格納手段から格納された前記オリジナルファイルを自動的に削除する自動オリジナルファイル削除手段と、を有することを特徴とするファイル管理システムに用いる利用者端末。

[図1]



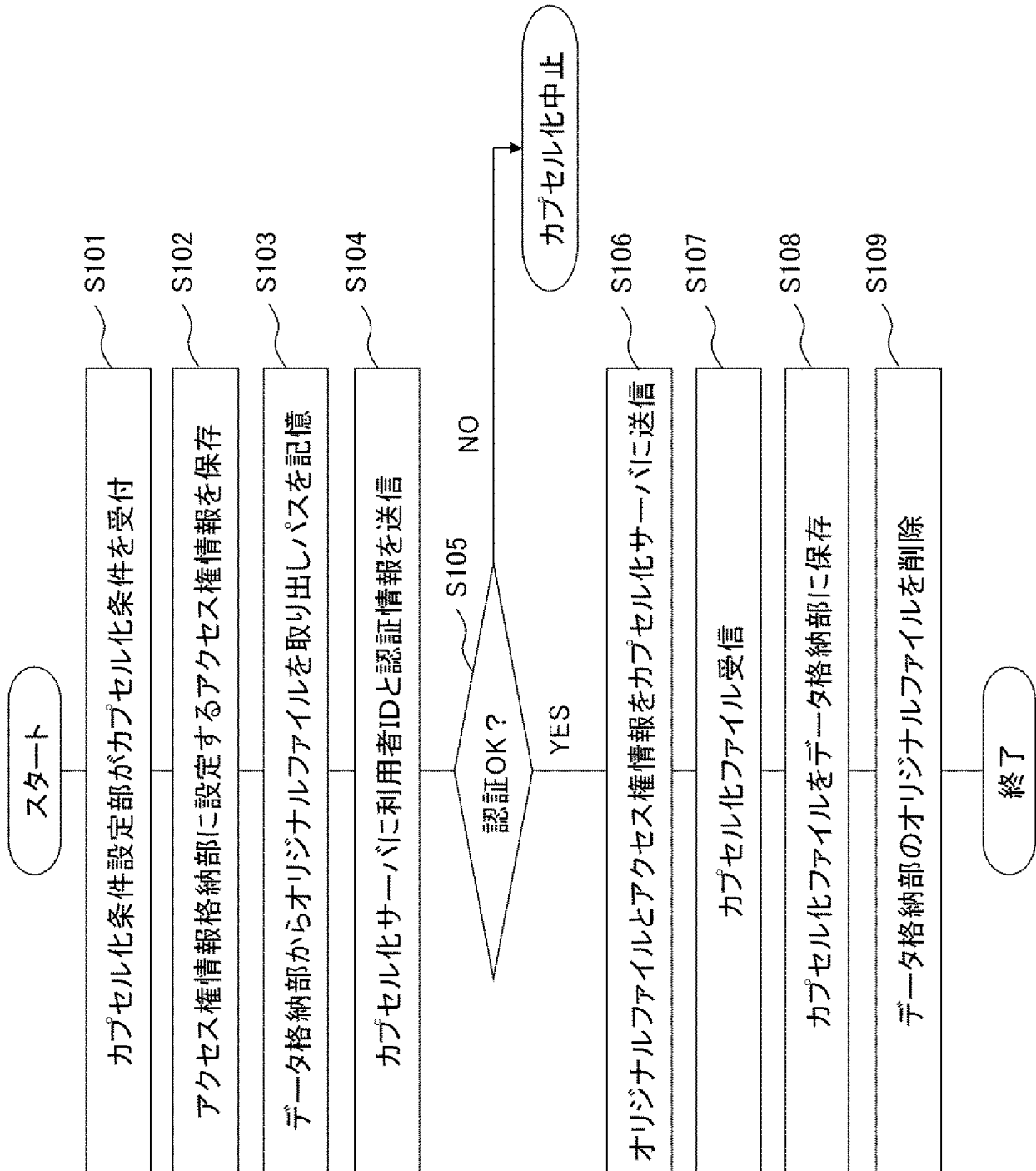
[図2]

利用者ID	アクセス権	パスワード
Shimazu	全ての操作	Pw1
Yamada	参照、編集、削除、カプセル化	Pw2
Takahashi	参照、編集	Pw3
Kimura	参照	Pw4
Suzuki	参照	Pw5

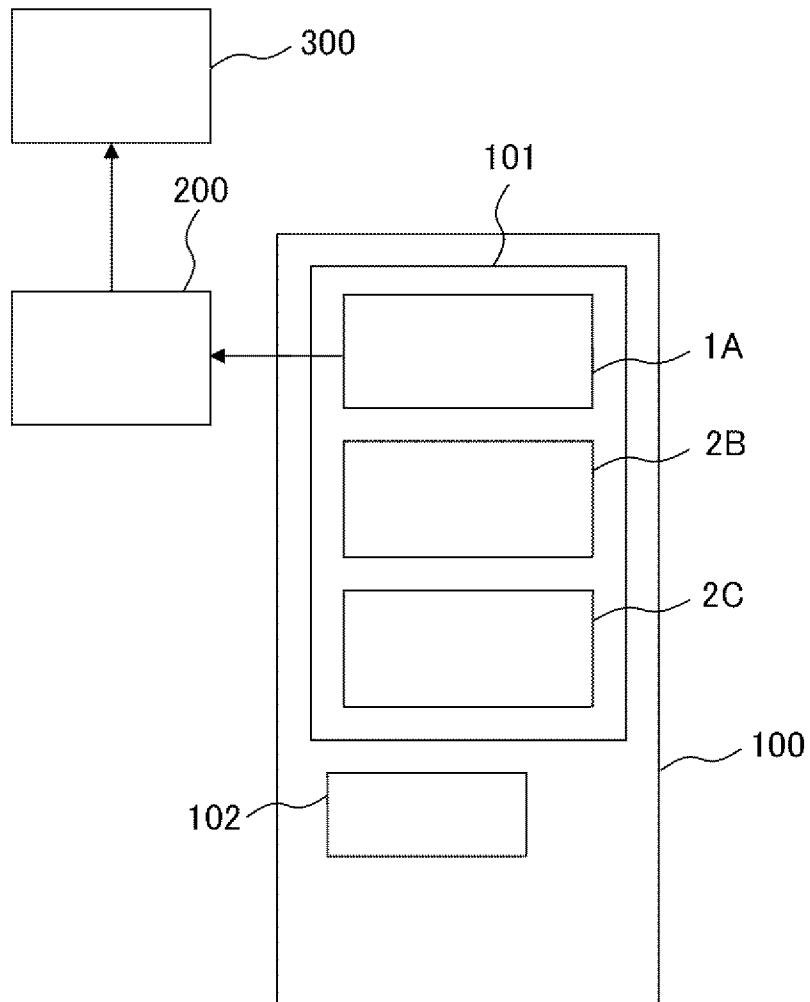
[図3]

利用者ID	パスワード
Shimazu	Pw1
Yamada	Pw2
Takahashi	Pw3
Kimura	Pw4
Suzuki	Pw5

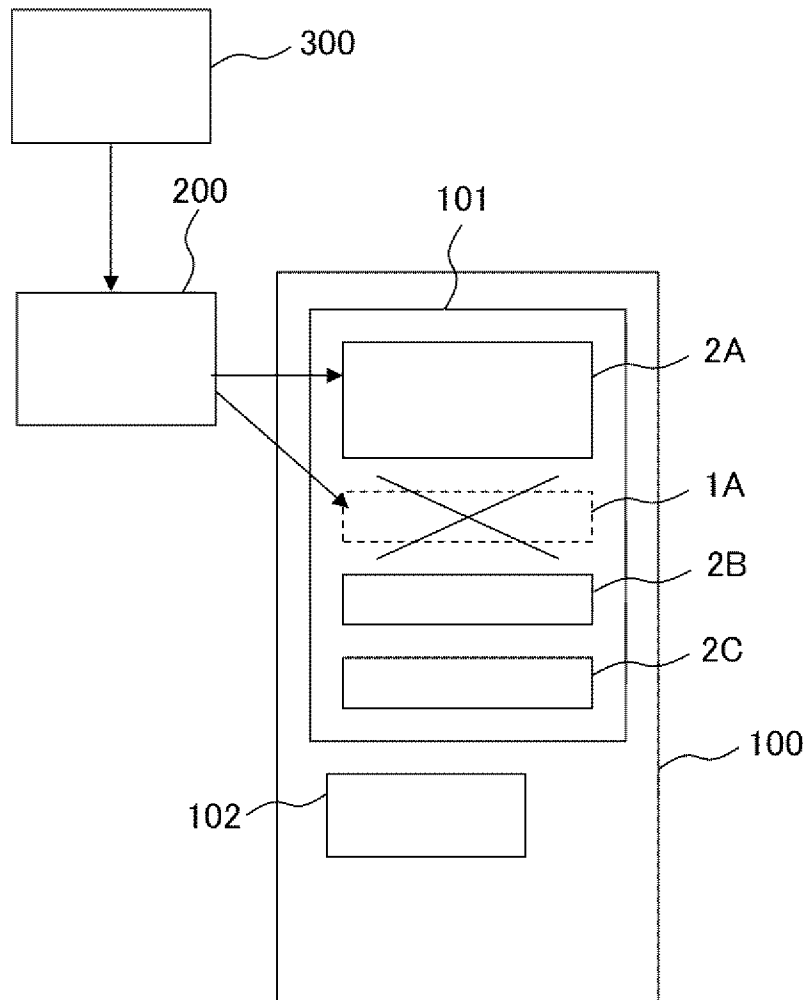
[図4]



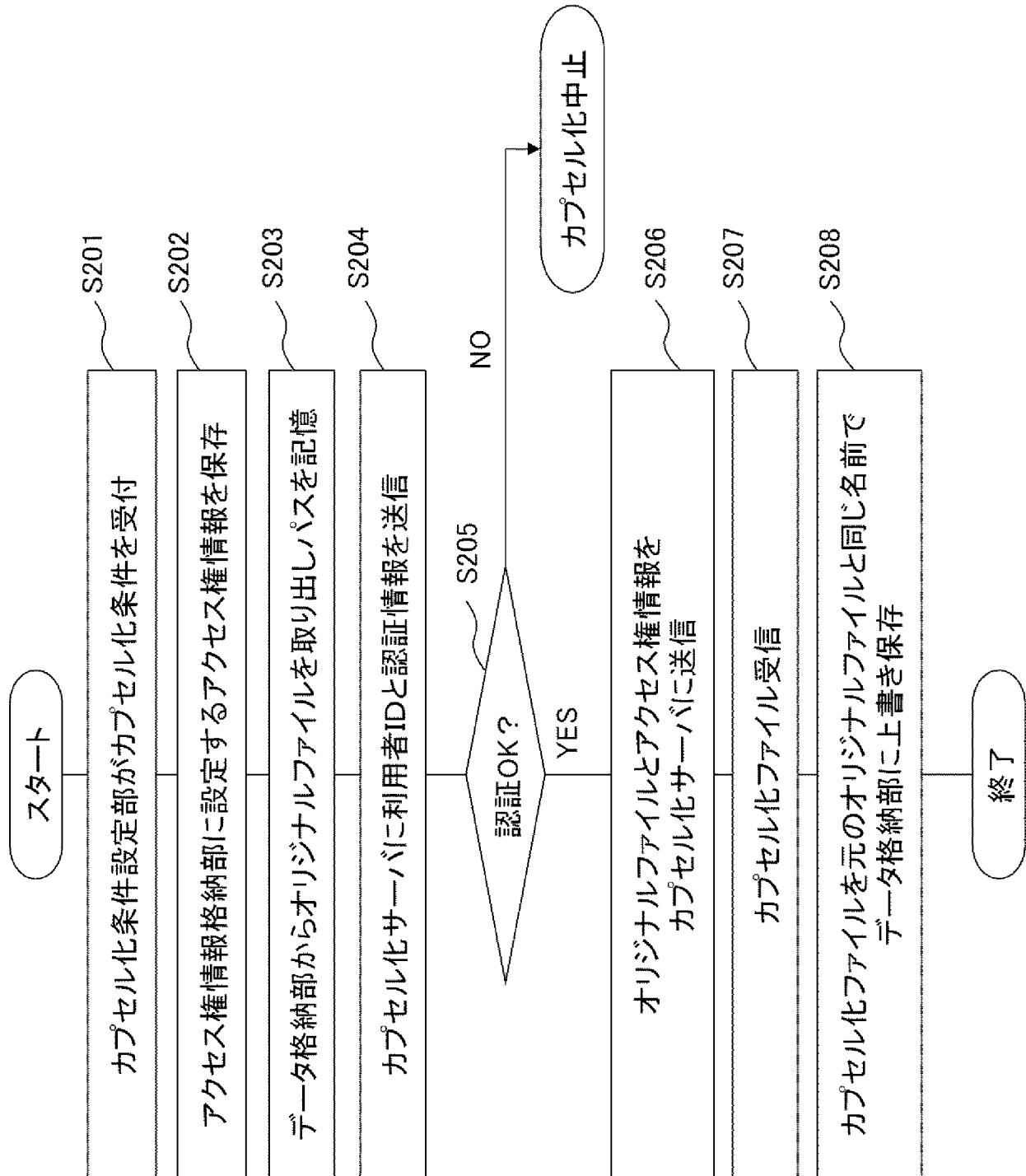
[図5A]



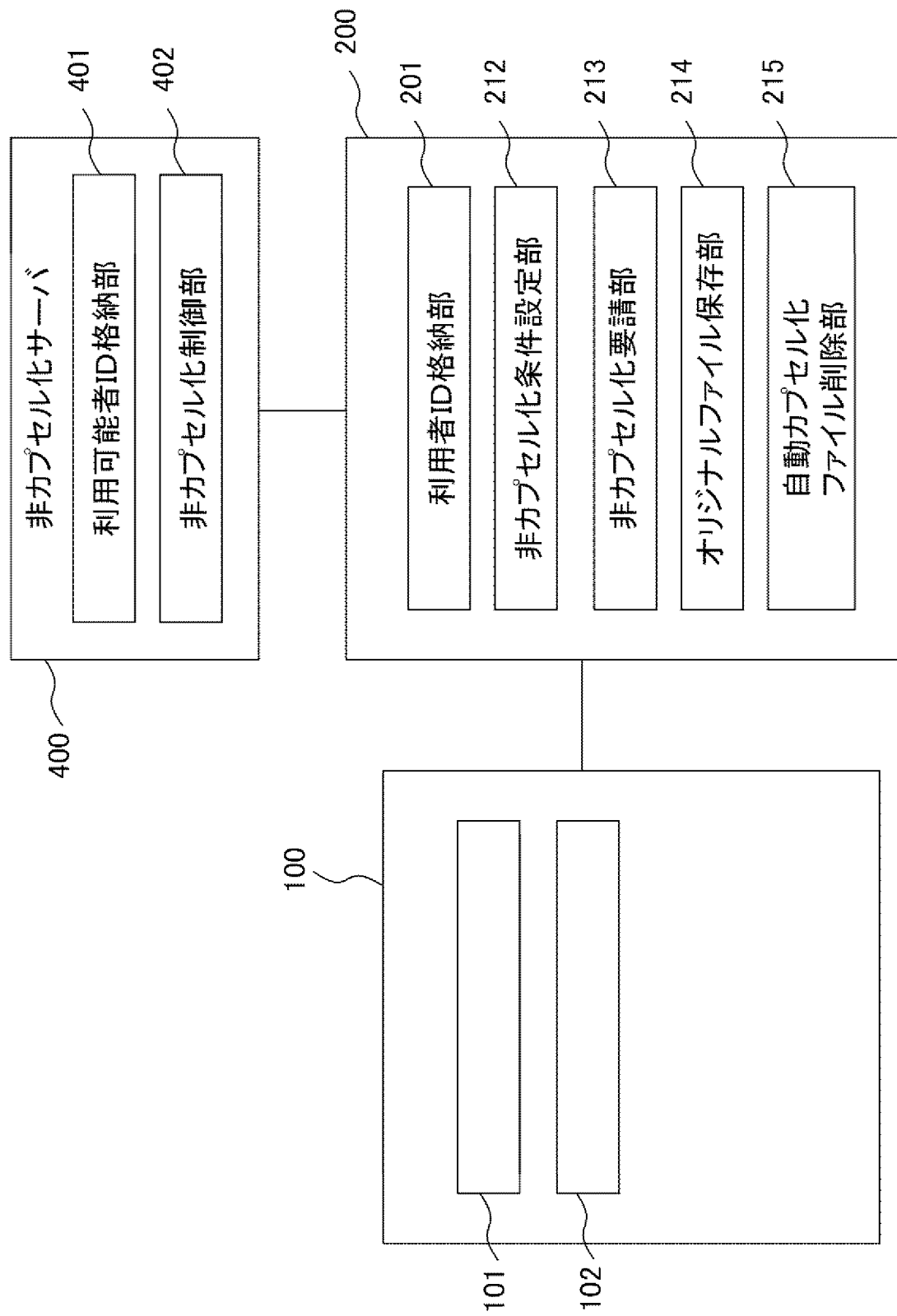
[図5B]



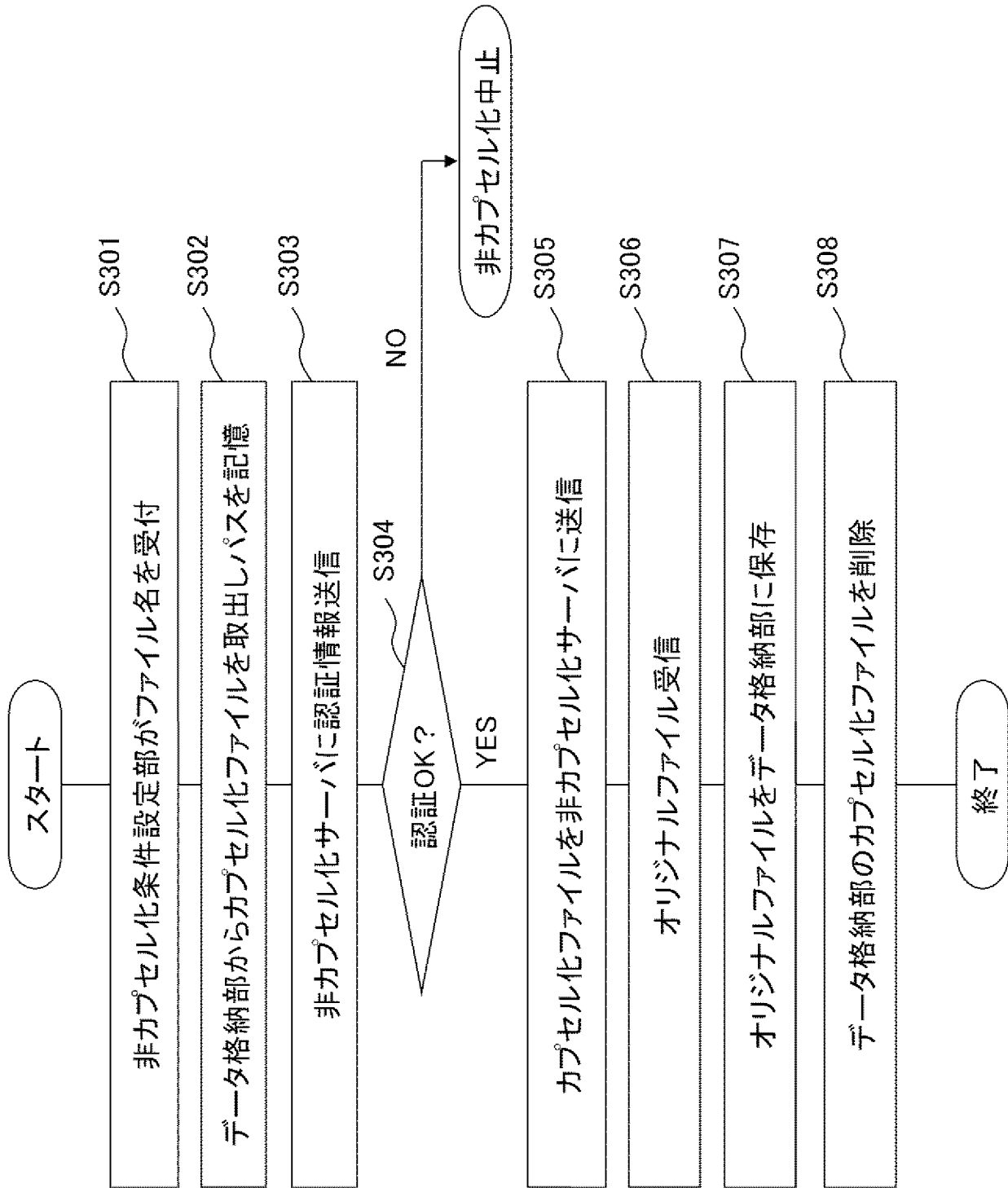
[図6]



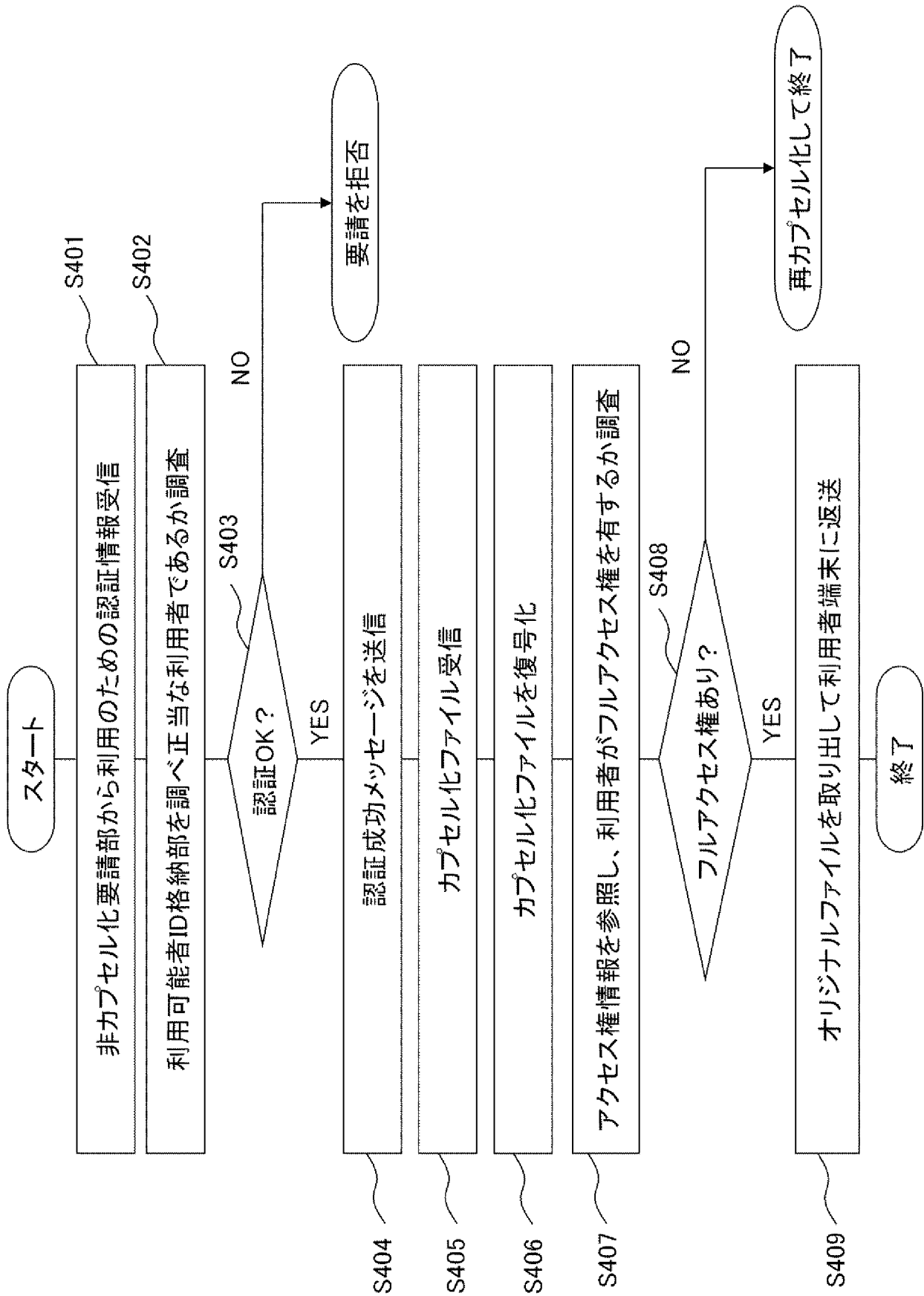
[図7]



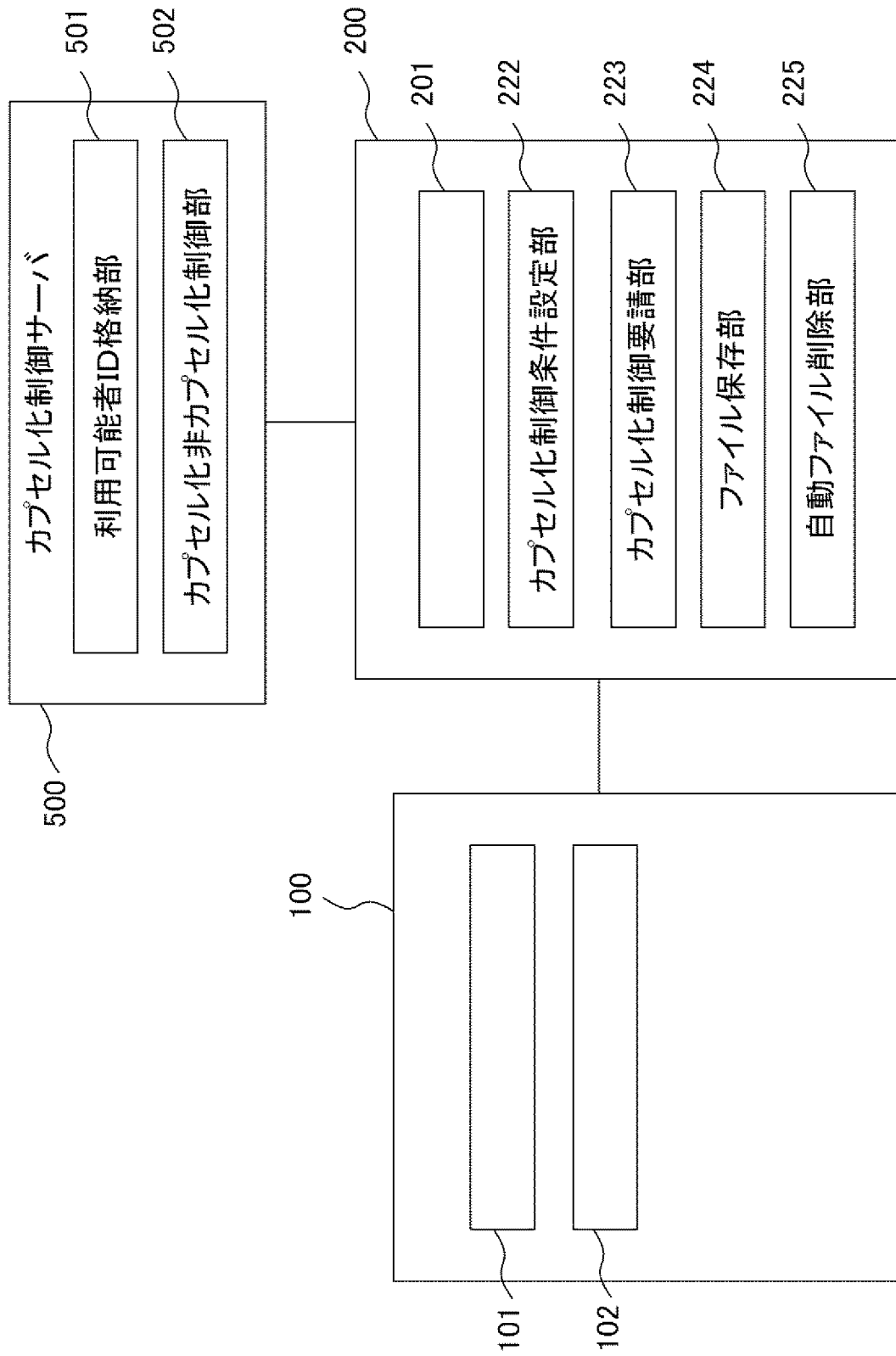
[図8]



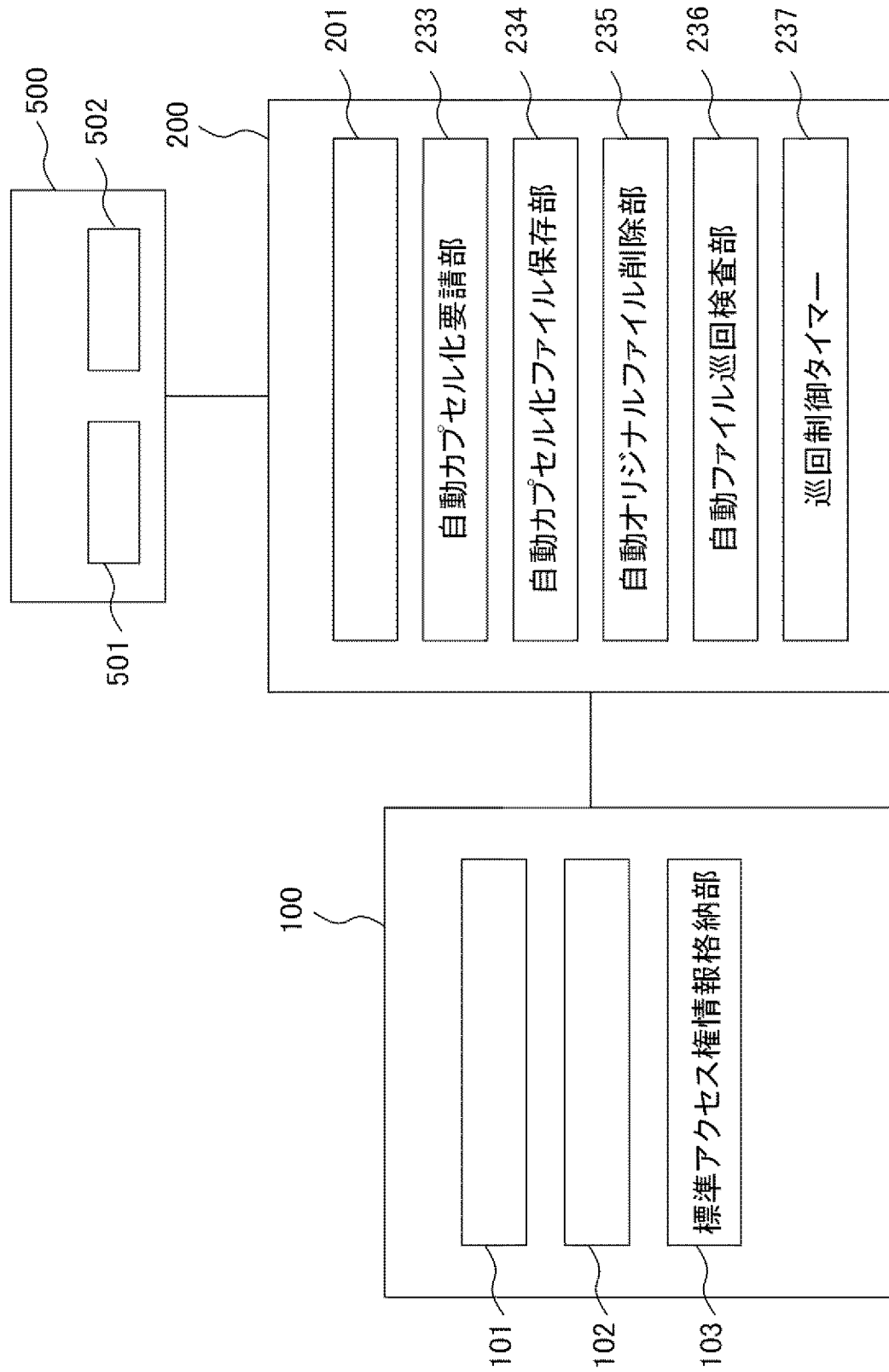
[図9]



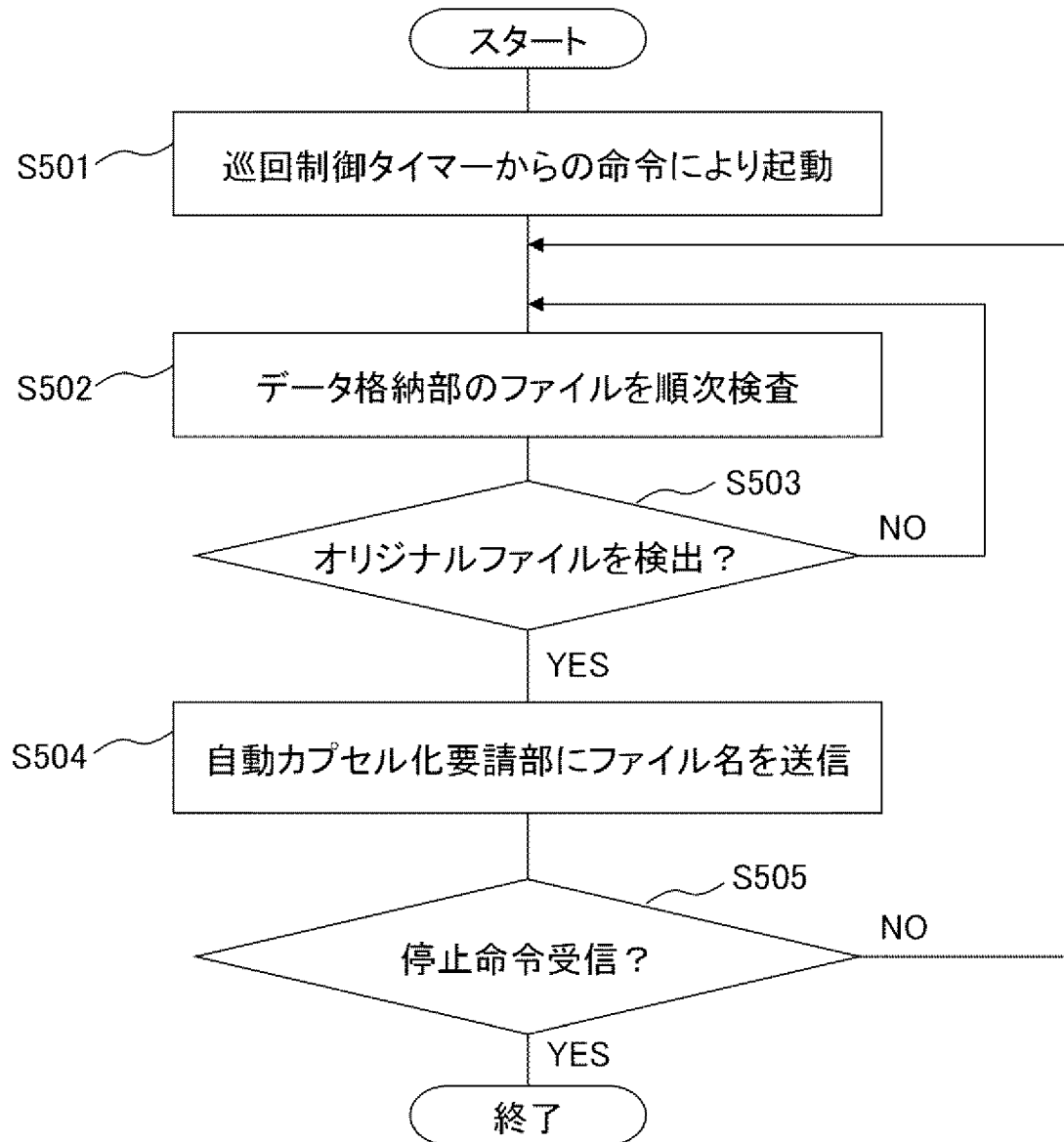
[図10]



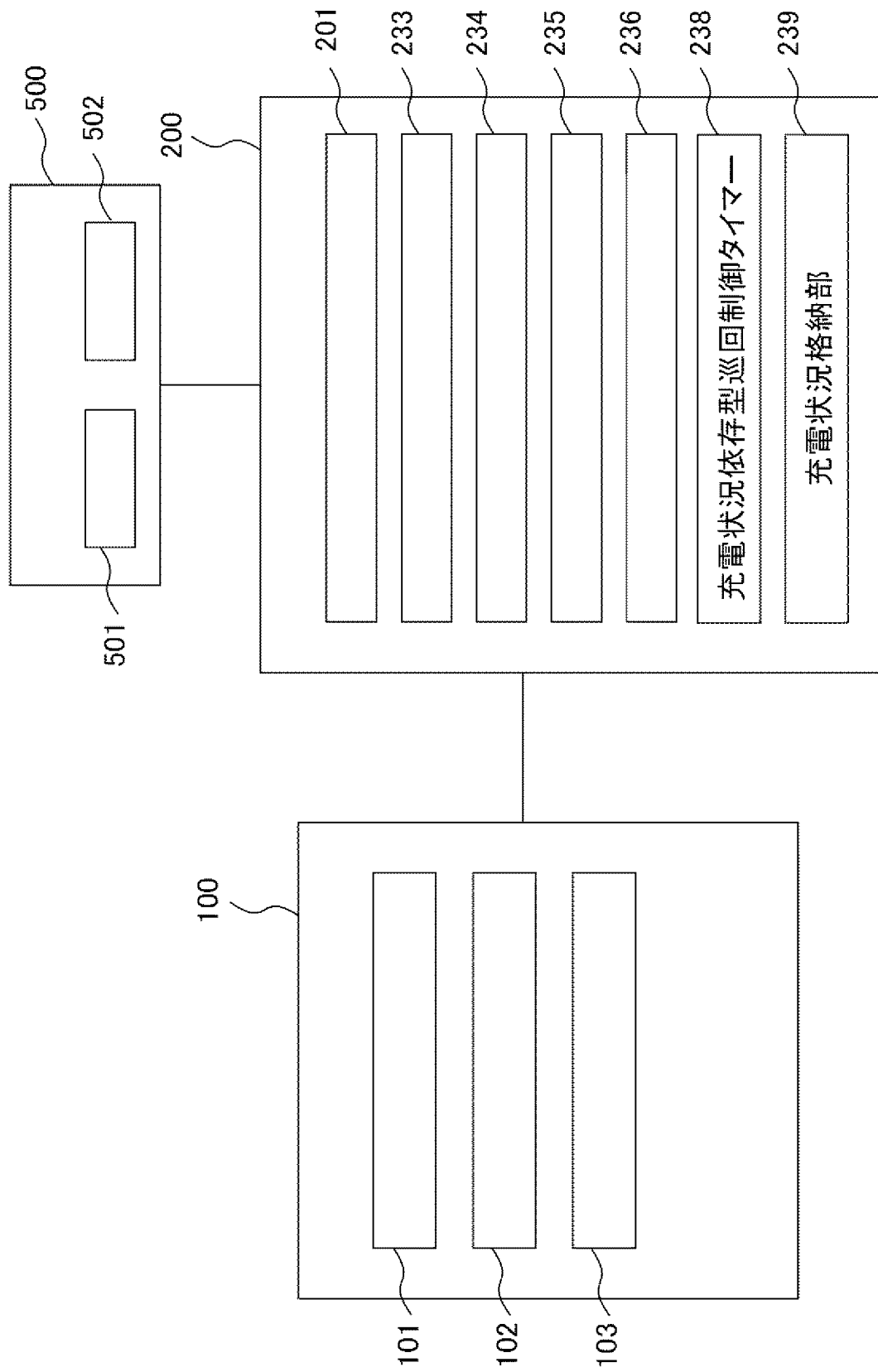
[図11]



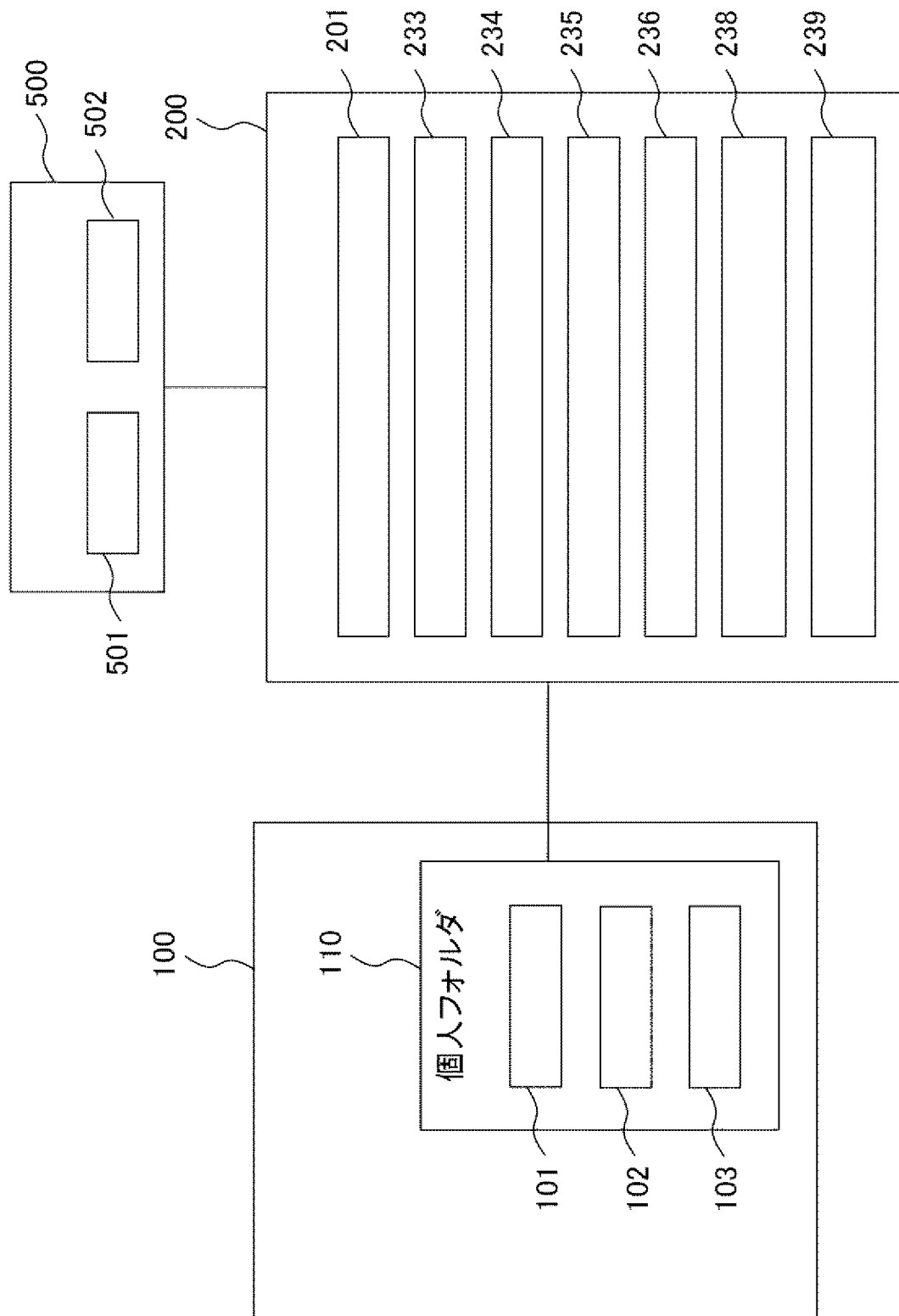
[図12]



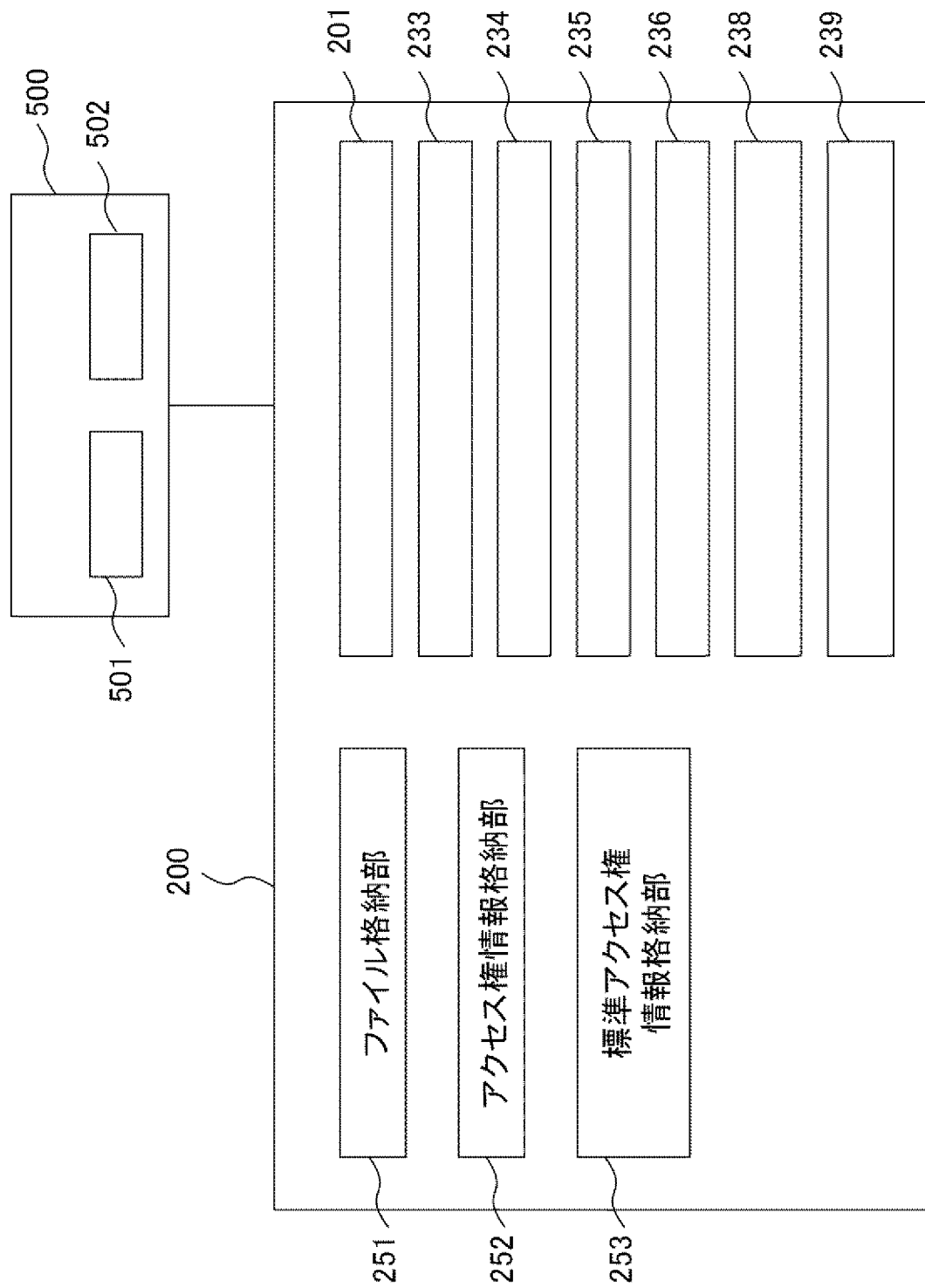
[図13]



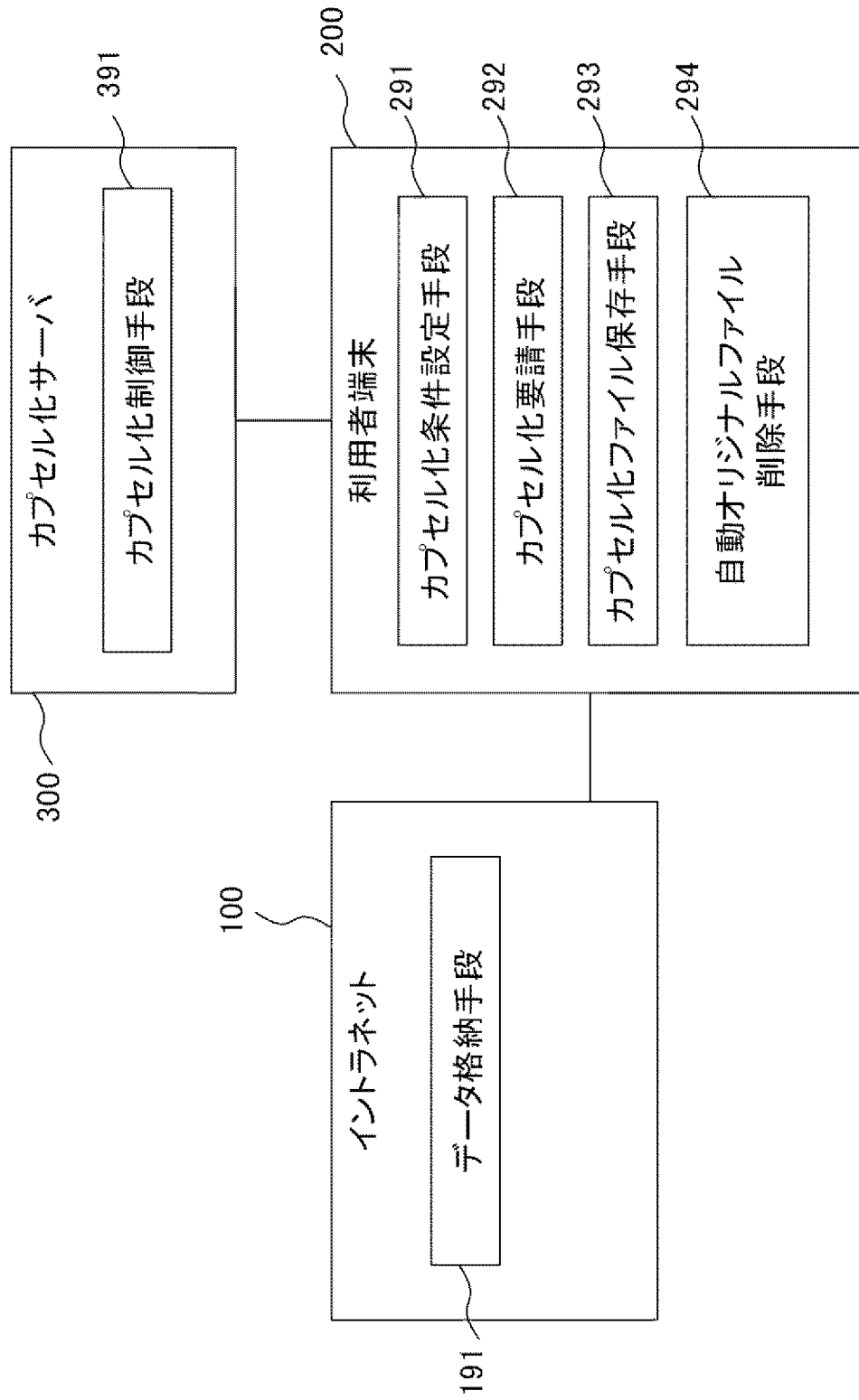
[図14]



[図15]



[図16]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2014/004670

A. CLASSIFICATION OF SUBJECT MATTER

G06F21/10(2013.01)i, G06F21/62(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F21/10, G06F21/62

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2014
Kokai Jitsuyo Shinan Koho	1971-2014	Toroku Jitsuyo Shinan Koho	1994-2014

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 2011-170715 A (NEC System Technologies, Ltd.), 01 September 2011 (01.09.2011), paragraphs [0012] to [0051]; fig. 1 to 3 (Family: none)	1, 2, 10 3-9
Y A	JP 2006-48220 A (Ricoh Co., Ltd.), 16 February 2006 (16.02.2006), paragraphs [0054] to [0060] (Family: none)	1, 2, 10 3-9
A	WO 2011/032001 A1 (SYMANTEC CORP.), 17 March 2011 (17.03.2011), claim 1 & JP 2013-504136 A & US 2011/0061110 A1 & EP 2476054 A & CN 102597947 A	1-10

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
04 December, 2014 (04.12.14)

Date of mailing of the international search report
16 December, 2014 (16.12.14)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. G06F21/10(2013.01)i, G06F21/62(2013.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（I P C））

Int.Cl. G06F21/10, G06F21/62

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 1 4 年
日本国実用新案登録公報	1 9 9 6 - 2 0 1 4 年
日本国登録実用新案公報	1 9 9 4 - 2 0 1 4 年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
Y A	JP 2011-170715 A（N E C システムテクノロジー株式会社） 2011.09.01, [0012]-[0051], 図 1-図 3（ファミリーなし）	1, 2, 10 3-9
Y A	JP 2006-48220 A（株式会社リコー） 2006.02.16, [0054]-[0060] （ファミリーなし）	1, 2, 10 3-9
A	WO 2011/032001 A1（SYMANTEC CORPORATION） 2011.03.17, claim 1 & JP 2013-504136 A & US 2011/0061110 A1 & EP 2476054 A & CN 102597947 A	1-10

☐ C 欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の 1 以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日

0 4 . 1 2 . 2 0 1 4

国際調査報告の発送日

1 6 . 1 2 . 2 0 1 4

国際調査機関の名称及びあて先

日本国特許庁（I S A / J P）
郵便番号 1 0 0 - 8 9 1 5
東京都千代田区霞が関三丁目 4 番 3 号

特許庁審査官（権限のある職員）

宮司 卓佳

5 S

9 5 5 5

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 4 6