(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2010-67012
(P2010-67012A)
(43)公開日　平成22年3月25日(2010.3.25)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/24	(2006.01)	G06F	12/14	560B	5B017
G06F 21/20	(2006.01)	G06F	12/14	520A	5B285
		G06F	15/00	330B	

審査請求 未請求　請求項の数 3　ＯＬ　（全 9 頁）

(21)出願番号　特願2008-232786 (P2008-232786)
(22)出願日　平成20年9月11日 (2008.9.11)

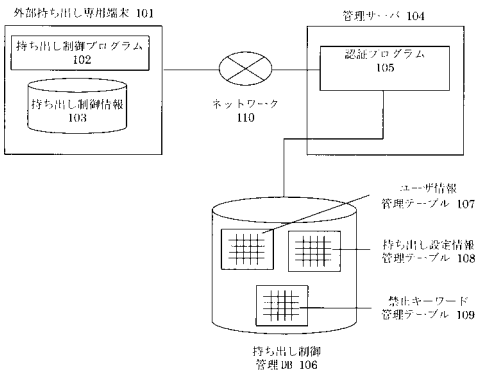
(71)出願人　000233055
日立ソフトウエアエンジニアリング株式会社
東京都品川区東品川四丁目１２番７号
(74)代理人　100096954
弁理士　矢島　保夫
(72)発明者　栗田　裕康
東京都品川区東品川四丁目１２番７号　日立ソフトウエアエンジニアリング株式会社内
(72)発明者　花田　大助
東京都品川区東品川四丁目１２番７号　日立ソフトウエアエンジニアリング株式会社内

Ｆターム(参考)　5B017 AA03　BA06　BB10　CA16

最終頁に続く

(54)【発明の名称】ファイルの持ち出し監視システム

(57)【要約】
【課題】外部へ持ち出しを行う管理された端末から持ち出し操作を行う場合などにおいて、持ち出しが許可されたユーザであっても、組織として持ち出しを禁止する重要な機密情報が含まれるファイルを外部へ持ち出しできないようにする技術を提供することを目的とする。
【解決手段】管理サーバでユーザごとに持ち出しの許可／不許可の設定情報とファイルの持ち出しを禁止するキーワードを設定する。ユーザ端末で管理サーバへアクセスし、ユーザ認証に成功した場合、管理サーバはユーザ端末へそのユーザの持ち出しの許可／不許可の設定情報と禁止キーワードを送信する。ユーザ端末でファイルの持ち出し要求があった場合、持ち出しの許可／不許可の設定情報から持ち出し可否を判定し、許可されている場合、さらに当該ファイルの内容が禁止キーワードを含むかどうかを判定し、禁止キーワードがあればその持ち出しを禁止する。
【選択図】図１



【特許請求の範囲】
【請求項１】
ネットワークに接続されたユーザ端末と管理サーバとを備えるファイルの持ち出し監視システムであって、
前記管理サーバは、
各ユーザごとに、ファイルの持ち出し先ごとの持ち出しの許可／不許可の設定情報を格納した持ち出し設定情報管理テーブルを記憶する手段と、
各ユーザごとの禁止キーワードを格納した禁止キーワード管理テーブルを記憶する手段と、
前記ユーザ端末からのログイン要求に応じてユーザ認証を行う手段と、
ユーザ認証が成功した場合、そのユーザに対応する持ち出し先ごとの持ち出しの許可／不許可の設定情報と禁止キーワードとを送信する手段と
を備え、
前記ユーザ端末は、
前記管理サーバにログイン要求を送信する手段と、
前記管理サーバから送信される、当該ユーザに対応する持ち出し先ごとの持ち出しの許可／不許可の設定情報と禁止キーワードとを受信し、持ち出し制御情報として記憶する手段と、
ユーザから持ち出し先を指定したファイル持ち出し要求があったとき、前記持ち出し制御情報中の当該ユーザに対応する持ち出し先ごとの持ち出しの許可／不許可の設定情報を参照して、当該ファイルの当該持ち出し先への持ち出しが許可されているか判定する手段と、
当該ファイルの当該持ち出し先への持ち出しが許可されていた場合、当該ファイルの内容に前記持ち出し制御情報中の禁止キーワードが含まれていないか判定する手段と、
当該ファイルの内容に前記禁止キーワードが含まれていた場合は、当該ファイルの持ち出しを禁止し、含まれていなかった場合は、当該ファイルの持ち出しを許可する手段と
を備えることを特徴とする持ち出し監視システム。
【請求項２】
請求項１に記載の持ち出し監視システムにおいて、
前記管理サーバの禁止キーワード管理テーブルは、ユーザのグループごとの禁止キーワードを格納したものであり、
前記ユーザ端末の禁止キーワードが含まれていないか判定する手段は、そのユーザが属するグループの禁止キーワードについて前記ファイルの内容に含まれていないかを判定するものである
ことを特徴とする持ち出し監視システム。
【請求項３】
請求項１または２に記載の持ち出し監視システムにおいて、
前記管理サーバの禁止キーワード管理テーブルは、各ユーザまたはグループの持ち出し先ごとの禁止キーワードを格納したものであり、
前記ユーザ端末の禁止キーワードが含まれていないか判定する手段は、指定された持ち出し先の禁止キーワードについて前記ファイルの内容に含まれていないかを判定するものである
ことを特徴とする持ち出し監視システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、外部記録媒体やネットワークドライブへのファイル持ち出しによる情報漏洩を防止する技術に関するものである。
【背景技術】
【０００２】

従来、ユーザ端末からの不正なファイルの持ち出しを防ぐ方法として、ユーザごとに対して外部記録媒体への持ち出しやネットワークドライブへの持ち出しの許可／不許可を設定する方法がある。

【０００３】

例えば、下記の非特許文献１では、管理サーバでユーザごとにリムーバブルメディア、外付けハードディスク、ネットワークドライブ、および印刷といった制御単位でファイルの持ち出しの許可／不許可を設定し、ユーザ端末では、管理サーバから認証を受けるまではファイルの持ち出しを禁止し、ユーザ認証後はユーザごとに設定された持ち出しの許可／不許可に従ってファイルの持ち出しを許可したり禁止したりすることにより、不正なファイルの持ち出しを防ぐようにしている。

【０００４】

本発明に関連する公知技術文献としては、下記特許文献１が挙げられる。該特許文献１のシステムは、正規にログインしていないユーザが不正に電子データを持ち出そうとしたとき、偽のデータを無尽蔵に転送し、転送をいつまでも完了させないようにして、正規にログインしていないユーザに対して牽制するものである。

【特許文献１】特開２００６－３０１７９８

【非特許文献１】日立ソフトウェアエンジニアリング株式会社、持ち出し制御による情報漏洩防止、[平成２０年２月２９日検索]、インターネット[URL：http://hitachisoft.jp/products/hibun/product/ae_if.html]

【発明の開示】

【発明が解決しようとする課題】

【０００５】

一方、上記の従来の技術では、単に持ち出すことをユーザに許可した場合、悪意のあるユーザにより機密性の高い重要なファイルを外部記録媒体へ複製されたり、印刷されたりして、機密情報が外部に漏洩されてしまう脅威がある。また、ユーザが機密性の高い重要なファイルであることを認識せずに、外部記録媒体へ機密性の高い重要なファイルを複製して外部へ持ち出し、ユーザの過失により外部記録媒体を紛失することで、機密情報が外部に漏洩してしまう脅威がある。

【０００６】

本発明の目的は、外部へ持ち出しを行う管理された例えば専用の端末から持ち出し操作を行う場合などにおいて、持ち出しが許可されたユーザであっても、組織として持ち出しを禁止する重要な機密情報が含まれるファイルを外部へ持ち出しできないようにする技術を提供することにある。

【課題を解決するための手段】

【０００７】

上記の目的を達成するために、本発明は、ネットワークに接続されたユーザ端末と管理サーバとを備え、管理サーバは、各ユーザごとに、ファイルの持ち出し先ごとの持ち出しの許可／不許可の設定情報を格納した持ち出し設定情報管理テーブルと、各ユーザごとの禁止キーワードを格納した禁止キーワード管理テーブルとを記憶するようにする。ユーザ端末からのログイン要求があり、ユーザ認証に成功したら、そのユーザに対応する持ち出し先ごとの持ち出しの許可／不許可の設定情報と禁止キーワードとを送信する。ユーザ端末は、管理サーバにログイン要求を送信し、管理サーバから送信される当該ユーザに対応する持ち出し先ごとの持ち出しの許可／不許可の設定情報と禁止キーワードとを受信し、持ち出し制御情報として記憶する。また、ユーザ端末は、ユーザから持ち出し先を指定したファイル持ち出し要求があったとき、前記持ち出し制御情報中の当該ユーザに対応する持ち出し先ごとの持ち出しの許可／不許可の設定情報を参照して、当該ファイルの当該持ち出し先への持ち出しが許可されているか判定し、さらに、当該ファイルの当該持ち出し先への持ち出しが許可されていた場合、当該ファイルの内容に前記持ち出し制御情報中の禁止キーワードが含まれていないか判定し、当該ファイルの内容に前記禁止キーワードが含まれていた場合は、当該ファイルの持ち出しを禁止し、含まれていなかった場合は、当

該ファイルの持ち出しを許可する。なお、管理サーバからユーザ端末への上記設定情報と禁止キーワードの送信は、ユーザログイン時に行ってもよいし、ファイル持ち出し要求があったときに行ってもよい。

【０００８】

前記管理サーバの禁止キーワード管理テーブルは、ユーザのグループごとの禁止キーワードを格納したものとし、前記ユーザ端末の禁止キーワードが含まれていないかの判定では、そのユーザが属するグループの禁止キーワードについて前記ファイルの内容に含まれていないかを判定するようにしてもよい。また、前記管理サーバの禁止キーワード管理テーブルは、各ユーザまたはグループの持ち出し先ごとの禁止キーワードを格納したものとし、前記ユーザ端末の禁止キーワードが含まれていないかの判定では、指定された持ち出し先の禁止キーワードについて前記ファイルの内容に含まれていないかを判定するようにしてもよい。

【０００９】

また、上記ユーザ端末は、外部持ち出し専用の端末とすれば、多数のユーザ端末からのファイル持ち出しを制限し、管理者が専用端末を管理できるので情報漏洩の防止をより強化することができる。

【発明の効果】

【００１０】

以上説明したように、本発明によれば、ユーザごとの持ち出しの許可／不許可の設定だけでなく、ファイルごとに禁止キーワードを用いて持ち出し可否を自動的に判断し制御することができる。ファイルの持ち出しを禁止するキーワードは、管理サーバで一元的に管理者が設定できるため、ユーザのモラルに依存することなく組織のセキュリティを強化することができる。各ユーザごとの持ち出しの許可／不許可の設定情報で許可になっている場合でも、さらに禁止キーワードによるチェックを行うので、重要な機密情報が含まれるファイルを外部持ちだしできないようにすることができる。

【００１１】

また、各ユーザまたはグループごとの禁止キーワードは、持ち出し先ごとに設定できるようにすれば、持ち出し先ごとに持ち出し制限の厳しさを変えることができる。例えば、手で持ち運べる外付けハードディスクなどのメディアについては持ち出し制限を厳しくし、ネットワークドライブのような一般的には持ち運び不可であるメディアについては持ち出し制限を緩くすることなどが可能になる。

【発明を実施するための最良の形態】

【００１２】

以下、本発明を実施する場合の一形態を、図面を参照して具体的に説明する。

【００１３】

図１は、本発明の一実施の形態を示すシステム構成図である。図１において、ネットワーク（１１０）には、外部持ち出し専用端末（１０１）、および管理サーバ（１０４）が接続されている。外部持ち出し専用端末（１０１）には、持ち出し制御プログラム（１０２）がインストールされており、持ち出し制御プログラム（１０２）はファイルの持ち出し可否の判定に必要な持ち出し制御情報（１０３）を持っている。管理サーバ（１０４）には、認証プログラム（１０５）がインストールされており、認証プログラム（１０５）は持ち出し制御管理ＤＢ（１０６）を管理している。

【００１４】

持ち出し制御管理ＤＢ（１０６）は、ユーザ情報管理テーブル（１０７）、持ち出し設定情報管理テーブル（１０８）、および禁止キーワード管理テーブル（１０９）を備える。ユーザ情報管理テーブル（１０７）には、認証プログラム（１０５）を介して管理者が設定したユーザ認証に必要な情報を格納する。持ち出し設定情報管理テーブル（１０８）には、認証プログラム（１０５）を介して管理者が設定したユーザごとのリムーバブルメディア、外付けハードディスク、ネットワークドライブ、および印刷といった持ち出し先単位での持ち出しの許可／不許可の設定情報を格納する。禁止キーワード管理テーブル（

１０９）には、認証プログラム（１０５）を介して管理者が設定したユーザごとのファイルの持ち出しを禁止するキーワードを格納する。具体的には図２で説明するが、ファイルの持ち出しを禁止するキーワードには、ＡＮＤ条件やＯＲ条件を設定できる。例えば、ファイルの持ち出しを禁止するキーワードに「“社外秘”ＡＮＤ“顧客情報”」が設定された場合、持ち出そうとしているファイルの内容に、“社外秘”と“顧客情報”の両方の単語があるとそのファイルの持ち出しが禁止される。また、例えば、ファイルの持ち出しを禁止するキーワードに「“社外秘”ＯＲ“部外秘”」が設定された場合、持ち出そうとしているファイルの内容に、“社外秘”または“部外秘”という何れかの単語があるとそのファイルの持ち出しが禁止される。

【００１５】

ユーザの操作に応じて、持ち出し制御プログラム（１０２）は、認証プログラム（１０５）にアクセスする。認証プログラム（１０５）は、ユーザよりアクセスがあった場合、持ち出し制御管理ＤＢ（１０６）に問い合わせて当該ユーザに対するユーザ認証を行い、ユーザ認証に成功した場合、そのユーザに該当する持ち出しの許可／不許可の設定情報とファイルの持ち出しを禁止するキーワードを持ち出し制御プログラム（１０２）に送信する。持ち出し制御プログラム（１０２）は、送信された情報を暗号化して持ち出し制御情報（１０３）に格納する。

【００１６】

ユーザが外部持ち出し専用端末（１０１）からファイルを外部へ持ち出そうとしたとき、持ち出し制御プログラム（１０２）は、持ち出し制御情報（１０３）に問い合わせを行い、ユーザの持ち出し先への持ち出し可否を判定する。持ち出し先への持ち出しが不許可の場合には、外部へのファイルの持ち出しを禁止する。持ち出し先への持ち出しが許可されている場合には、持ち出し制御プログラム（１０２）は、持ち出そうとしているファイルの内容にファイルの持ち出しを禁止するキーワードと一致する箇所があるかどうかを判定する。持ち出しを禁止するキーワードと一致する箇所がある場合には、外部へのファイルの持ち出しを禁止し、持ち出しを禁止するキーワードと一致する箇所がない場合には、外部へのファイルの持ち出しを許可する。

【００１７】

図２は、持ち出し制御管理ＤＢ（１０６）が保持するテーブルの例を示す図である。図１に示したように、持ち出し制御管理ＤＢ（１０６）は、ユーザ情報管理テーブル（１０７）と持ち出し設定情報管理テーブル（１０８）と禁止キーワード管理テーブル（１０９）の３つのテーブルを保持している。

【００１８】

ユーザ情報管理テーブル（１０７）には、ユーザＩＤ（２０１）とパスワード（２０２）の情報が保管されている。持ち出し設定情報管理テーブル（１０８）には、ユーザＩＤ（２０１）と持ち出しの許可／不許可の設定情報（２０３）の情報が保管されている。禁止キーワード管理テーブル（１０９）には、ユーザＩＤ（２０１）と持ち出しを禁止するキーワード（２０４）の情報が保管されている。

【００１９】

ユーザＩＤ（２０１）には、任意の英数文字列からなるユーザＩＤが格納されている。なお、ユーザＩＤ（２０１）は、各テーブルの主キーであるため、各ユーザが特定できるように一意に保たれている。パスワード（２０２）には、任意の英数文字列からなる各ユーザごとのパスワードが格納される。このパスワードは、ユーザ認証の際に利用される。

【００２０】

持ち出しの許可／不許可の設定情報（２０３）には、リムーバブルメディア、外付けハードディスク、ネットワークドライブ、および印刷といった持ち出し先単位ごとに許可または不許可が格納され、それら以外の情報が格納されることはない。リムーバブルメディアは、ＵＳＢメモリ、フレキシブルディスク、リムーバブルハードディスク、ＣＤ－Ｒ、ＤＶＤ－Ｒ、ＤＶＤ－ＲＡＭなどの各種のリムーバブルなデータメディアを含む。外付けハードディスクは、外部持ち出し専用端末１０１に接続された外付けのハードディスクで

ある。

【００２１】

持ち出しを禁止するキーワード（２０４）には、管理者が設定した各ユーザごとのキーワード（任意の文字列）が格納される。ＡＮＤ条件やＯＲ条件を設定した場合は、例えば「“社外秘”ＡＮＤ“顧客情報”」や「“社外秘”ＯＲ“部外秘”」という形で格納され、キーワードを何も設定しない場合は何も格納されない。

【００２２】

図３は、外部持ち出し専用端末（１０１）と管理サーバ（１０４）との間の処理のフローチャートである。

【００２３】

ユーザが外部持ち出し専用端末（１０１）にある持ち出し制御プログラム（１０２）を起動し、ユーザＩＤとパスワードを入力したとする（ステップ３０１）。持ち出し制御プログラム（１０２）は、入力されたユーザＩＤとパスワードを管理サーバ（１０４）の認証プログラム（１０５）に暗号化して送信する（ステップ３０２）。

【００２４】

管理サーバ（１０４）の認証プログラム（１０５）は、受信したユーザＩＤとパスワードを基に持ち出し制御管理ＤＢ（１０６）に問い合わせ（ステップ３０３）、ユーザ認証を行う（ステップ３０４）。ユーザ認証に失敗した場合、その旨を持ち出し制御プログラム（１０２）に通知し（ステップ３０７）、持ち出し制御プログラム（１０２）が認証失敗ダイアログを表示する（ステップ３０８）。

【００２５】

一方、ユーザ認証に成功した場合、管理サーバ（１０４）の認証プログラム（１０５）は、持ち出し制御管理ＤＢ（１０６）に問い合わせ、そのユーザに該当する持ち出しの許可／不許可の設定情報と持ち出しを禁止するキーワードを外部持ち出し専用端末（１０１）の持ち出し制御プログラム（１０２）へ送信する（ステップ３０５）。

【００２６】

外部持ち出し専用端末（１０１）の持ち出し制御プログラム（１０２）は、認証プログラム（１０５）より送信された持ち出しの許可／不許可の設定情報と持ち出しを禁止するキーワードを持ち出し制御情報（１０３）に暗号化して格納する（ステップ３０６）。

【００２７】

図４は、外部持ち出し専用端末（１０１）でファイルを外部へ持ち出すときの処理のフローチャートである。

【００２８】

ユーザが外部持ち出し専用端末（１０１）からファイルを外部へ持ち出そうとしたとする（ステップ４０１）。これは、ファイルを指定し、当該ファイルをリムーバブルメディア、外付けハードディスク、またはネットワークドライブに書き込んだり（コピー・移動など）、あるいは印刷を指示した場合である。

【００２９】

外部持ち出し専用端末（１０１）の持ち出し制御プログラム（１０２）は、持ち出し制御情報（１０３）に問い合わせを行い、当該ユーザの持ち出し先（ユーザにより指示された持ち出し先）への持ち出し可否を判定する（ステップ４０２）。持ち出し先への持ち出しが不許可の場合、持ち出し制御プログラム（１０２）は当該持ち出し先へのファイルの書き込み・印刷を抑止する（ステップ４０５）。これによりファイルを外部へ持ち出すことができない。

【００３０】

また、ステップ４０２で持ち出し先への持ち出しが許可の場合、持ち出し制御プログラム（１０２）は、持ち出し制御情報（１０３）に問い合わせを行い、持ち出そうとしているファイルの内容にファイルの持ち出しを禁止するキーワードと一致する箇所があるかどうかを判定する（ステップ４０３）。持ち出そうとしているファイルの内容に、持ち出しを禁止するキーワードと一致する箇所がある場合、持ち出し制御プログラム（１０２）は

、外部へのファイルの書き込み・印刷を抑止する（ステップ４０５）。これによりファイルを外部へ持ち出すことができない。なお、図２で説明したが、持ち出しを禁止するキーワードがＡＮＤやＯＲの条件を含む場合、ステップ４０３の判定では、それらのＡＮＤやＯＲの条件に沿ってＹＥＳ／ＮＯを判定するものである。

【００３１】

また、ステップ４０３で、持ち出そうとしているファイルの内容に、ファイルの持ち出しを禁止するキーワードと一致する箇所がない場合、持ち出し制御プログラム（１０２）は、外部へのファイルの書き込みを許可する（ステップ４０４）。これによりファイルを外部へ持ち出すことができる。

【００３２】

なお、上記実施形態では、ステップ４０３で当該ファイルの内容を読み出すことができることを前提としているが（例えば当該ファイルの内容を読み出すことができるアプリケーションがインストールされていることなど）、もし当該ファイルの内容を読み出すことができない場合は、当該ファイルの持ち出しは禁止するものとする。

【００３３】

上記実施形態では、各ユーザごとに持ち出しの許可／不許可の設定情報と持ち出しを禁止するキーワードとを用意しているが、これらはユーザごとではなくグループ単位で設定するようにしてもよい。この場合、持ち出し設定情報管理テーブル１０８はユーザごとの設定情報とし、禁止キーワード管理テーブル１０９はユーザのグループ単位で設定することとしてもよい。これにより、ユーザごとの持ち出しの許可／不許可は各ユーザの権限に応じて設定でき、一方、グループ単位で重要な禁止キーワードを含む文書は絶対に外部への持ち出しことが禁止されるようにできる。

【００３４】

さらに、禁止キーワード管理テーブル１０９において、持ち出し先単位で禁止キーワードを設定できるようにしてもよい。これにより、例えばＵｓｅｒ１の持ち出しについて、外付けハードディスクでは第１のキーワードを禁止キーワードとして登録し、リムーバブルメディアでは別の第２のキーワードを禁止キーワードとして登録する、というようなことが可能になる。一般的に、外付けハードディスクやリムーバブルメディアなど容易に手で持ち運び可能な持ち出し先については持ち出し制限を厳しくし、ネットワークドライブのような手で持ち運びできないような持ち出し先については持ち出し制限を比較的緩くしても良いと考えられる。したがって、各ユーザ（あるいはグループ）ごとに且つ各持ち出し先単位で禁止キーワードを設定できるようにすることで、持ち出し先別に持ち出し制限を変えて管理することが可能になる。

【図面の簡単な説明】

【００３５】

【図１】本発明の一実施形態のシステム構成図である。

【図２】持ち出し制御管理ＤＢの保持するテーブル図である。

【図３】外部持ち出し専用端末と管理サーバ間の処理のフローチャートである。

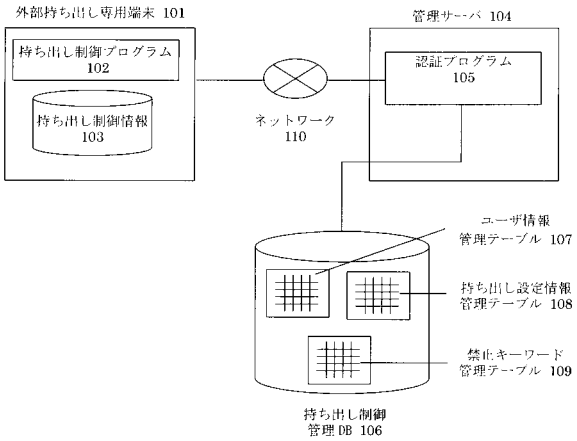
【図４】外部持ち出し専用端末でファイルを外部に持ち出すときの処理のフローチャートである。

【符号の説明】

【００３６】

１０１…外部持ち出し専用端末、１０２…持ち出し制御プログラム、１０３…持ち出し制御情報、１０４…管理サーバ、１０５…認証プログラム、１０６…持ち出し制御管理ＤＢ、１０７…ユーザ情報管理テーブル、１０８…持ち出し設定情報管理テーブル、１０９…禁止キーワード管理テーブル、１１０…ネットワーク。

【図１】



【図２】

201 / 202 ユーザ情報管理テーブル 107

ユーザ ID	パスワード
User1	********
User2	********
User3	********
:	:
UserN	********

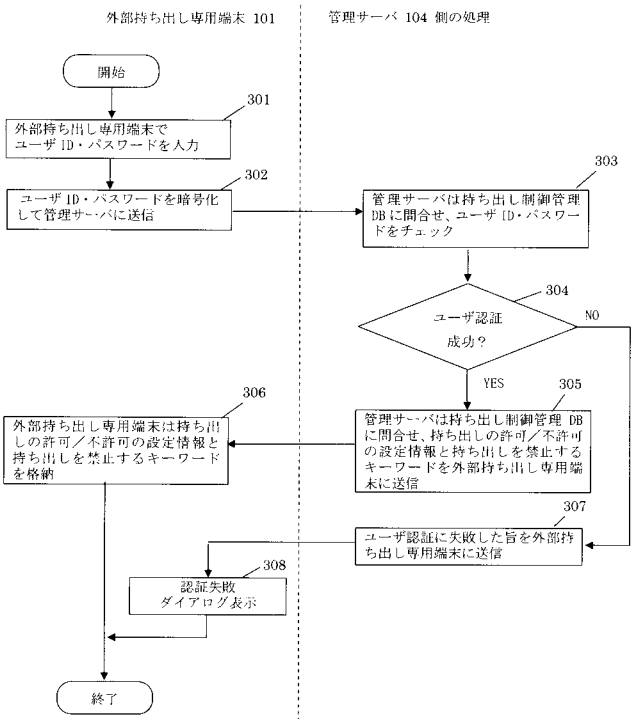
201 / 203 持ち出し設定情報管理テーブル 108

ユーザ ID	持ち出しの許可／不許可の設定情報			
	外付けハードディスク	リムーバブルメディア	ネットワークドライブ	印刷
User1	許可	許可	許可	許可
User2	不許可	不許可	不許可	許可
User3	許可	許可	許可	許可
:	:	:	:	:
UserN	不許可	不許可	許可	不許可

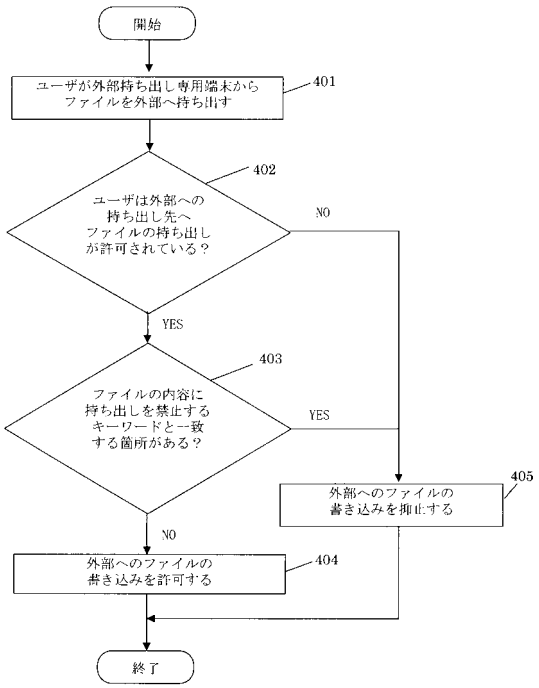
201 / 204 禁止キーワード管理テーブル 109

ユーザ ID	持ち出しを禁止するキーワード
User1	(“社外秘” AND “顧客情報”) OR “部外秘”
User2	“社外秘” AND “顧客情報”
User3	
:	:
UserN	“社外秘” OR “部外秘”

【図３】



【図４】



フロントページの続き

Ｆターム(参考) 5B285 AA04 BA07 CA02 CA03 CA32 CB01