(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5704517号
(P5704517)
(45)発行日　平成27年4月22日(2015.4.22)　(24)登録日　平成27年3月6日(2015.3.6)

(51)Int.Cl.　F I
G06F 21/62 (2013.01)　G06F 21/62 318
G06F 21/62 390

請求項の数 6　(全 16 頁)

(21)出願番号　特願2011-549873(P2011-549873)
(86)(22)出願日　平成22年12月6日(2010.12.6)
(86)国際出願番号　PCT/JP2010/071837
(87)国際公開番号　WO2011/086787
(87)国際公開日　平成23年7月21日(2011.7.21)
審査請求日　平成25年11月15日(2013.11.15)
(31)優先権主張番号　特願2010-5187(P2010-5187)
(32)優先日　平成22年1月13日(2010.1.13)
(33)優先権主張国　日本国(JP)

(73)特許権者　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100079108
弁理士　稲葉　良幸
(74)代理人　100109346
弁理士　大貫　敏史
(74)代理人　100117189
弁理士　江口　昭彦
(74)代理人　100134120
弁理士　内藤　和彦
(74)代理人　100109586
弁理士　土屋　徹雄

最終頁に続く

(54)【発明の名称】機密情報漏洩防止システム、機密情報漏洩防止方法及び機密情報漏洩防止プログラム

(57)【特許請求の範囲】
【請求項１】
アプリケーションプログラムによりネットワークアクセスサービス提供手段を介して送信されるネットワークアクセス要求と、アプリケーションプログラムにより直接送信されるネットワークアクセス要求とを、当該アプリケーションプログラムに割り当てられているセキュリティレベルに基づいて制御する機密情報漏洩防止システムであって、
前記ネットワークアクセスサービス提供手段が前記アプリケーションプログラムにより呼び出されたか否かを監視する第１監視手段と、
前記ネットワークアクセス要求がネットワークへ送信されるか否かを監視する第２監視手段と、
前記第１監視手段により前記ネットワークアクセスサービス提供手段の呼び出しが検出された場合、当該検出された呼び出しに係るネットワークアクセス要求を、当該サービス提供手段を呼び出したアプリケーションプログラムに割り当てられているセキュリティレベルに基づいて制御する第１アクセス制御手段と、
前記第２監視手段により前記ネットワークアクセス要求の送信が検出された場合、当該検出されたネットワークアクセス要求に対して前記第１アクセス制御手段が既にアクセス制御を行ったか否かを判断し、判断結果が否である場合は、当該ネットワークアクセス要求を、当該ネットワークアクセス要求を送信したアプリケーションプログラムに割り当てられているセキュリティレベルに基づいて制御する第２アクセス制御手段と、
を備えることを特徴とする機密情報漏洩防止システム。

【請求項２】
前記第２アクセス制御手段は、
前記第２監視手段により前記ネットワークアクセス要求の送信が検出された場合、当該検出されたネットワークアクセス要求に対して前記第１アクセス制御手段が既にアクセス制御を行ったか否かの問い合わせを当該第１アクセス制御に問い合わせることを特徴とする請求項１に記載の機密情報漏洩防止システム。
【請求項３】
前記第１アクセス制御手段又は前記第２アクセス制御手段の制御対象となるアプリケーションのアプリケーション情報、もしくは、前記第２アクセス制御手段の制御対象とならないネットワークアクセスサービス提供手段の情報を定義した参照情報を記憶する記憶手段を備え、
前記第２アクセス制御手段は、
前記第２監視手段により前記ネットワークアクセス要求の送信が検出された場合、前記記憶手段に記憶された参照情報を参照することにより、前記検出されたネットワークアクセス要求に対して前記第１アクセス制御手段が既にアクセス制御を行ったか否かを判断することを特徴とする請求項１に記載の機密情報漏洩防止システム。
【請求項４】
アプリケーションプログラムよりネットワークアクセスサービス提供プログラムを介して送信されるネットワークアクセス要求と、アプリケーションプログラムにより直接送信されるネットワークアクセス要求とを、当該アプリケーションプログラムに割り当てられているセキュリティレベルに基づいて制御する機密情報漏洩防止システムにおける機密情報漏洩防止方法であって、
前記ネットワークアクセスサービス提供プログラムが前記アプリケーションにより呼び出されたか否かを監視する第１監視ステップと、
前記ネットワークアクセス要求がネットワークへ送信されるか否かを監視する第２監視ステップと、
前記第１監視ステップにより前記ネットワークアクセスサービス提供プログラムの呼び出しが検出された場合、当該検出された呼び出しに係るネットワークアクセス要求を、当該サービス提供プログラムを呼び出したアプリケーションプログラムに割り当てられているセキュリティレベルに基づいて制御する第１アクセス制御ステップと、
前記第１監視ステップにより前記ネットワークアクセス要求の送信が検出された場合、当該検出されたネットワークアクセス要求に対して既にアクセス制御が行われたか否かを判断し、判断結果が否である場合は、当該ネットワークアクセス要求を、当該ネットワークアクセス要求を送信したアプリケーションプログラムに割り当てられているセキュリティレベルに基づいて制御する第２アクセス制御ステップと、
を備えることを特徴とする機密情報漏洩防止方法。
【請求項５】
前記第１アクセス制御ステップ又は前記第２アクセス制御ステップの制御対象となるアプリケーションのアプリケーション情報、もしくは、前記第２アクセス制御ステップの制御対象とならないネットワークアクセスサービス提供プログラムの情報を定義した参照情報を記憶する記憶装置を備え、
前記第２アクセス制御ステップは、
前記第２監視ステップにより前記ネットワークアクセス要求の送信が検出された場合、前記記憶装置から前記参照情報を参照することにより、前記検出されたネットワークアクセス要求に対して既にアクセス制御が行われたか否かを判断することを特徴とする請求項４に記載の機密情報漏洩防止方法。
【請求項６】
アプリケーションプログラムによりネットワークアクセスサービス提供プログラムを介して送信されるネットワークアクセス要求と、アプリケーションプログラムにより直接送信されるネットワークアクセス要求とを、当該アプリケーションプログラムに割り当てら

れているセキュリティレベルに基づいてそれぞれ制御するコンピュータに、
前記ネットワークアクセスサービス提供プログラムが前記第１アプリケーションにより呼び出されたか否かを監視する第１監視ステップと、
前記ネットワークアクセス要求がネットワークへ送信されるか否かを監視する第２監視ステップと、
第１監視ステップにより前記サービス提供プログラムの呼び出しが検出された場合、当該検出された呼び出しに係るネットワークアクセス要求を、当該サービス提供プログラムを呼び出した第１アプリケーションプログラムに割り当てられているセキュリティレベルに基づいて制御する第１アクセス制御ステップと、
第２監視ステップにより前記ネットワークアクセス要求の送信が検出された場合、当該検出されたネットワークアクセス要求に対して既にアクセス制御が行われたか否かを判断し、判断結果が否である場合は、当該ネットワークアクセス要求を、当該ネットワークアクセス要求を送信した第２アプリケーションプログラムに割り当てられているセキュリティレベルに基づいて制御する第２アクセス制御ステップと、
を実行させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、機密情報の漏洩を防止するための技術に係り、特に、マルチレベルセキュリティを用いて機密情報の漏洩を防止するための技術に関する。
【背景技術】
【０００２】
機密情報の漏洩防止に関して様々な技術が提案されている。例えば、特許文献１（特開２００４－２２０１２０）には、認証機構が、データベースに蓄積されたユーザ情報とユーザがアクセスしたい情報リソースとの対応情報とを比較することによりユーザを認証する方法が記載されている。
【０００３】
特許文献２（特開２００５－２７５６６９）には、データ送信指令が出された場合に、当該データ送信指令を出したアプリケーションプログラムが監視対象として登録されている場合には、当該データ送信指令を制限するデータ監視方法が記載されている。
【０００４】
特許文献３（特開２００９－１６９８９５）には、機密ファイルのネットワークへの送出を検知すると、機密情報が含まれていることを示す付加情報をパケットに付与してからネットワークへ送出するクライアント端末が記載されている。
【０００５】
特許文献４（特開２００８－０３３５８４）には、クライアント装置にインストールされたＶＭ（セキュリティ仮想マシン）が、ＷＷＷブラウザ等のプログラムとオペレーティングシステム（ＯＳ）との間に自身を介在させ、当該プログラムが発行するファイルアクセスに関するシステムコールの内容をセキュアな内容に改変してからオペレーティングシステムに渡す構成が記載されている。
【先行技術文献】
【特許文献】
【０００６】
【特許文献１】特開２００４－２２０１２０号公報
【特許文献２】特開２００５－２７５６６９号公報
【特許文献３】特開２００９－１６９８９５号公報
【特許文献４】特開２００８－０３３５８４号公報
【発明の概要】
【発明が解決しようとする課題】
【０００７】

ここで、データやアプリケーションおよびユーザやデバイス等にセキュリティレベルを特定するラベルを付与し、この付与されたラベルに基づいてアクセス対象へのアクセスを制限するマルチレベルセキュリティシステム（ＭＬＳ）が知られている。このようなマルチレベルセキュリティシステムは、例えば、予めアプリケーションに「一般」又は「機密」等を示すラベルを付与しておき、アプリケーションがアクセス対象へアクセスする際に、この付与されたラベルに基づいて当該アクセスを制御するものである。

【０００８】

しかしながら、アプリケーションが、ネットワーク上のアクセス対象にアクセス（以下、「ネットワークアクセス」という。）するような場合には、アプリケーションがアクセス対象にアクセスする前に、これをチェックして制御する必要があるところ、以下に述べるような問題がある。

【０００９】

例えば、アプリケーションによるネットワークアクセスについては、当該アクセスが端末装置からネットワークへ送出される直前のタイミングで、これをチェックして制御することが考えられる。かかるチェックは、例えば、ファイアウォール等を利用して実行することが可能である。しかし、アプリケーションの中には、例えばオペレーティングシステム等が提供するネットワークサービス機能を利用してネットワークアクセスを行うものがあるところ、このような場合、ネットワークアクセスは、アプリケーションではなくオペレーティングシステムによって実行される。そのため、ファイアウォールは、アプリケーションではなくオペレーティングシステムによるネットワークアクセスを検出するため、当該ネットワークアクセスがどのアプリケーションに由来するものなのか判断することができず、その結果、アプリケーションのラベルに応じたアクセス制御を行うことは困難である。

【００１０】

一方、ネットワークサービス機能を利用したアプリケーションのネットワークアクセスについては、当該ネットワークサービス機能がアプリケーションによって呼び出されるタイミングで、これをチェックして制御することが考えられる。かかるチェックは、例えば、特許文献４に記載されているようなシステムコールのフックを用いて実行することが可能である。しかしながら、この方法では、監視対象が、フックを設定した特定のアプリケーションに限定されてしまうため、アプリケーションの監視漏れが発生する可能性があるという問題がある。

【００１１】

従って、アプリケーションによるネットワークアクセスの方法にかかわらず、当該アプリケーションによるネットワークアクセスを漏れなく制御することが必要となるところ、上記特許文献１乃至４のいずれも、かかる課題を解決するための有効な仕組みを提供するものではない。

【００１２】

従って、本発明の目的は、アプリケーションによるネットワークアクセスの方法にかかわらず、当該アプリケーションによるネットワークアクセスを、当該アプリケーションのセキュリティレベルに応じて漏れなく制御することができるシステムを提供することにある。

【課題を解決するための手段】

【００１３】

本発明は、アプリケーションプログラムによりネットワークアクセスサービス提供手段を介して送信されるネットワークアクセス要求と、アプリケーションプログラムにより直接送信されるネットワークアクセス要求とを、当該アプリケーションプログラムに割り当てられているセキュリティレベルに基づいて制御する機密情報漏洩防止システムであって、前記ネットワークアクセスサービス提供手段が前記アプリケーションプログラムにより呼び出されたか否かを監視する第１監視手段と、前記ネットワークアクセス要求がネットワークへ送信されるか否かを監視する第２監視手段と、前記第１監視手段により前記ネッ

トワークアクセスサービス提供手段の呼び出しが検出された場合、当該検出された呼び出しに係るネットワークアクセス要求を、当該サービス提供手段を呼び出したアプリケーションプログラムに割り当てられているセキュリティレベルに基づいて制御する第１アクセス制御手段と、前記第２監視手段により前記ネットワークアクセス要求の送信が検出された場合、当該検出されたネットワークアクセス要求に対して前記第１アクセス制御手段が既にアクセス制御を行ったか否かを判断し、判断結果が否である場合は、当該ネットワークアクセス要求を、当該ネットワークアクセス要求を送信したアプリケーションプログラムに割り当てられているセキュリティレベルに基づいて制御する第２アクセス制御手段と、
を有する。

【００１４】

また、本発明は、アプリケーションプログラムよりネットワークアクセスサービス提供プログラムを介して送信されるネットワークアクセス要求と、アプリケーションプログラムにより直接送信されるネットワークアクセス要求とを、当該アプリケーションプログラムに割り当てられているセキュリティレベルに基づいて制御する機密情報漏洩防止システムにおける機密情報漏洩防止方法であって、制御手段が、前記ネットワークアクセスサービス提供プログラムが前記アプリケーションにより呼び出されたか否かを監視する第１監視ステップと、前記ネットワークアクセス要求がネットワークへ送信されるか否かを監視する第２監視ステップと、前記第１監視ステップにより前記ネットワークアクセスサービス提供プログラムの呼び出しが検出された場合、当該検出された呼び出しに係るネットワークアクセス要求を、当該サービス提供プログラムを呼び出したアプリケーションプログラムに割り当てられているセキュリティレベルに基づいて制御する第１アクセス制御ステップと、前記第１監視ステップにより前記ネットワークアクセス要求の送信が検出された場合、当該検出されたネットワークアクセス要求に対して既にアクセス制御が行われたか否かを判断し、判断結果が否である場合は、当該ネットワークアクセス要求を、当該ネットワークアクセス要求を送信したアプリケーションプログラムに割り当てられているセキュリティレベルに基づいて制御する第２アクセス制御ステップと、を有する。

【００１５】

また、本発明は、アプリケーションプログラムによりネットワークアクセスサービス提供プログラムを介して送信されるネットワークアクセス要求と、アプリケーションプログラムにより直接送信されるネットワークアクセス要求とを、当該アプリケーションプログラムに割り当てられているセキュリティレベルに基づいてそれぞれ制御するコンピュータに、前記ネットワークアクセスサービス提供プログラムが前記第１アプリケーションにより呼び出されたか否かを監視する第１監視ステップと、前記ネットワークアクセス要求がネットワークへ送信されるか否かを監視する第２監視ステップと、第１監視ステップにより前記サービス提供プログラムの呼び出しが検出された場合、当該検出された呼び出しに係るネットワークアクセス要求を、当該サービス提供プログラムを呼び出した第１アプリケーションプログラムに割り当てられているセキュリティレベルに基づいて制御する第１アクセス制御ステップと、第２監視ステップにより前記ネットワークアクセス要求の送信が検出された場合、当該検出されたネットワークアクセス要求に対して既にアクセス制御が行われたか否かを判断し、判断結果が否である場合は、当該ネットワークアクセス要求を、当該ネットワークアクセス要求を送信した第２アプリケーションプログラムに割り当てられているセキュリティレベルに基づいて制御する第２アクセス制御ステップと、を実行させるためのプログラムである。本発明のプログラムは、本発明の機密情報漏洩防止方法の各処理をコンピュータに実行させることを特徴とする。本発明のプログラムは、ＣＤ－ＲＯＭ等の光学ディスク、磁気ディスク、半導体メモリなどの各種の記録媒体を通じて、又は通信ネットワークなどを介してダウンロードすることにより、コンピュータにインストール又はロードすることができる。

【００１６】

なお、本明細書等において、手段とは、単に物理的手段を意味するものではなく、その

手段が有する機能をソフトウェアによって実現する場合も含む。また、１つの手段が有する機能が２つ以上の物理的手段により実現されても、２つ以上の手段の機能が１つの物理的手段により実現されてもよい。

【発明の効果】

【００１７】

従って、本発明の目的は、アプリケーションによるネットワークアクセスの方法にかかわらず、当該アプリケーションによるネットワークアクセスを、当該アプリケーションのセキュリティレベルに応じて漏れなく制御することができるシステムを提供することが可能になる。

【図面の簡単な説明】

【００１８】

【図１】機密情報漏洩防止システムの概略構成を示す図である。

【図２】クライント及びサーバのハードウェアの概略を示す図である。

【図３】ラベル割り当て手段が生成したラベル割当リストの一例を示す図である。

【図４】サーバ情報記憶手段のデータ構造の一例を示す図である。

【図５】アクセス制御ルール記憶手段のデータ構造の一例を示す図である。

【図６】機密情報漏洩防止処理の流れの一例を示すフローチャートである。

【発明を実施するための形態】

【００１９】

以下、本発明の実施の形態について図面を参照しつつ詳細に説明する。なお、同一の要素には同一の符号を付し、重複する説明を省略する。また、本実施形態では、本発明に係る機密情報漏洩防止システムを、クライアント内のアプリケーションがネットワークを介してサーバのフォルダにアクセスする構成に適用しているが、本発明はこれに限られず、アクセス主体がネットワーク上のアクセス対象に対して実行する処理に対して適宜適用することができる。

【００２０】

［システム構成］

図１は、本実施形態に係る機密情報漏洩防止システムが適用されるクライアント・サーバシステムの概略構成を示すブロック図である。本システムは、クライアント１００とサーバ２００とを含み、クライアント１００とサーバ２００はネットワークＮを介して相互に接続される。

【００２１】

クライアント１００は、図２に示すように、クライアント１００の処理及び動作を制御する制御手段としてのＣＰＵ３０１、ＲＯＭ３０２やＲＡＭ３０３等のメモリ、各種情報を格納する外部記憶装置（ＨＤＤ）３０４、通信インタフェース３０５、入力インタフェース３０６、ディスプレイ等の出力インタフェース３０７及びこれらを結ぶバス等のハードウェアを備える汎用のコンピュータを適用することができる。ＲＯＭ３０２、ＲＡＭ３０３及び／又は外部記憶装置３０４は、単に記憶装置とも呼ばれる。クライアント１００は、ＣＰＵ３０１がメモリや外部記憶装置３０４に記憶される所定のプログラムを実行することにより、後述するサービス提供手段１０２、ラベル割り当て手段１０３、第１ネットワークアクセス制御手段１０６、第２ネットワークアクセス制御手段１０７などの各種機能実現手段として機能することができる。なお、図１では、１つのクライアント１００を例示しているが、サーバ２００には複数のクライアント１００を接続することができ、クライアント１００の数は設計に応じて適宜設定することができる。

【００２２】

クライアント１００は、アプリケーション１０１と、サービス提供手段１０２と、ラベル割り当て手段１０３と、サーバ情報記憶手段１０４と、アクセス制御ルール記憶手段１０５と、第１ネットワークアクセス制御手段１０６と、第２ネットワークアクセス制御手段１０７と、通信手段１０８と、を備える。

【００２３】

アプリケーション（アプリケーションプログラム）１０１は、外部記憶装置３０４等に格納され、ＣＰＵ３０１によって実行されることにより、ユーザに所定の機能を提供するプログラムである。アプリケーション１０１は、特に限定はないが、例えば、文書作成機能や情報閲覧機能等を有する既存のソフトウェアを適用することができ、本実施形態では、ネットワークアクセスの方法とラベルの内容に応じて以下のように区別される。

【００２４】

アプリケーション１０１は、ネットワークへのアクセス要求をサービス提供手段１０２を介して送信するアプリケーション（第１アプリケーションプログラム）と、ネットワークへのアクセス要求を直接送信するアプリケーション（第２アプリケーションプログラム）とに区別される。前者はサービス提供手段１０２を利用するためサービス利用アプリケーションと呼ばれ、後者はサービス提供手段１０２を利用しないためサービス非利用アプリケーションと呼ばれる。具体的には、サービス利用アプリケーションは、例えばシステムコールによってサービス提供手段１０２を呼び出すと、サービス提供手段１０２が通信ソケットを生成するなどしてネットワークアクセスを実行する。一方、サービス非利用アプリケーションは、通信ソケットを直接生成するなどしてネットワークアクセスを自ら実行する。

【００２５】

また、アプリケーション１０１は、割り当てられたラベルの内容に応じて、一般ラベルが割り当てられたアプリケーション（一般アプリケーション）と、機密ラベルが割り当てられたアプリケーション（機密アプリケーション）とに区別される。

【００２６】

さらに、アプリケーション１０１は、サービス提供手段１０２を利用してネットワークアクセスを行い、かつ、ラベル割り当て手段１０３によって一般ラベルが割り当てられたアプリケーション（サービス利用一般アプリケーション）と、サービス提供手段１０２を利用してネットワークアクセスを行い、かつ、ラベル割り当て手段１０３によって機密ラベルが割り当てられたアプリケーション（サービス利用機密アプリケーション）と、サービス提供手段１０２を利用せずにネットワークアクセスを行い、かつ、ラベル割り当て手段１０３によって一般ラベルが割り当てられたアプリケーション（サービス非利用一般アプリケーション）と、サービス提供手段１０２を利用してネットワークアクセスを行い、かつ、ラベル割り当て手段１０３によって機密ラベルが割り当てられたアプリケーション（サービス非利用機密アプリケーション）と、に区別される。

【００２７】

図１に示すアプリケーションＡ１０１ａは、サービス利用一般アプリケーションに該当し、アプリケーションＢ１０１ｂは、サービス利用機密アプリケーションに該当し、アプリケーションＣ１０１ｃは、サービス非利用一般アプリケーションに該当し、アプリケーションＤ１０１ｄは、サービス非利用機密アプリケーションに該当する。

【００２８】

サービス提供手段１０２は、ネットワークアクセスに関するネットワークサービスをアプリケーション１０１に提供可能に構成されたプログラム（以下、「ネットワークアクセスサービス提供プログラム」又は「サービス提供プログラム」という。）であり、アプリケーション１０１とは独立したプログラムである。アプリケーション１０１が、例えばシステムコールを使ってサービス提供手段１０２を呼び出すと、サービス提供手段１０２は、通信手段１０８を介してネットワークにアクセスし、アクセスした結果をアプリケーション１０１に提供する。

【００２９】

サービス提供手段１０２は、特に限定はないが、例えば、Ｗｅｂ閲覧サービスやネットワークファイル共有サービスなどの機能を提供する既存のプログラムが該当し、ここでは、オペレーティングシステムにより提供される場合について説明する。サービス提供手段１０２は、例えば、アプリケーション１０１から、サーバ２００内のフォルダ２０３へのアクセス要求を受け付けると、サーバアプリケーション２０２へアクセスし、フォルダ２

０３内のデータをサーバアプリケーション２０２から取得し、取得したデータをアプリケーション１０１に提供する。

【００３０】

ラベル割り当て手段１０３は、セキュリティレベルを示す情報（以下、「ラベル」という。）をアプリケーションに対して割り当て可能に構成されている。また、アプリケーションと当該アプリケーションに割り当てたラベルを対応付けたリストを所定の記憶領域に格納可能に構成されている。ラベルには、例えば、セキュリティの低い「一般」とセキュリティの高い「機密」の２種類を付与することができるが、ラベルの内容はこれに限られず、設計に応じて適宜設定することができる。例えば、「機密」、「極秘」、「秘」、「区分外」などのラベルを割り当ててもよい。図３は、アプリケーションを一意的に識別するプロセス番号（ＩＤ）と、アプリケーション名と、アプリケーションに割り当てたラベルの対応関係を示すラベル割り当てリストの一例を示している。

【００３１】

また、ラベル割り当て手段１０３は、第１アクセス制御手段１０６ｂや第２アクセス制御手段１０７ｂから、所定のアプリケーションに割り当てられたラベルについて問合せを受け付けると、当該アプリケーションに割り当てたラベルをラベル割り当てリストから読み出して通知できるように構成されている。また、ラベル割り当て手段１０３により割り当てられたラベルは、機密アプリケーション（101b,101c）から一般アプリケーション（101a,101d）へのクライアント１００内での情報流通を禁止する際にも用いることができる。

【００３２】

サーバ情報記憶手段１０４は、アクセス対象と当該アクセス対象に割り当てられているラベルの情報とを対応付けて記憶する記憶装置であり、データベースとしての機能を有する。サーバ情報記憶手段１０４は、アクセス対象記憶手段とも呼ばれる。アクセス対象には、例えば、データを格納したフォルダを設定することができるが、これに限られず、アクセス先の装置やメールアドレスなど設計に応じて適宜設定することができる。また、アクセス対象に割り当てられるラベルには、「一般」と「機密」の２種類を付与することができるが、これに限られず、設計に応じて適宜設定することができる。図４は、サーバ情報記憶手段１０４のデータ構造の一例を示している。同図に示すように、アクセス対象の一例であるフォルダＡには「一般」、フォルダＢには「機密」が割り当てられている。

【００３３】

アクセス制御ルール記憶手段１０５は、アプリケーションによるネットワークアクセスを制限するための情報（アクセス制御ルール）を記憶する記憶装置である。アクセス制御ルール記憶手段１０５は、特に限定はないが、例えば、アプリケーション毎に各アクセス対象と当該アクセス対象へのアクセス制御の内容を対応付けて格納する。制御の内容は、例えば、アクセスの「許可」「禁止」などが該当するが、アクセスの種類や性質に応じて適宜設定／変更することが可能である。図５は、アクセス制御ルール記憶手段のデータ構造の一例を示している。同図に示すように、機密アプリケーションには、機密フォルダに対して「アクセス許可」が、一般フォルダに対して「読み込み許可」が、それぞれ対応づけて設定されている。一方、一般アプリケーションには、機密フォルダに対して「アクセス禁止」が、一般フォルダに対して「アクセス許可」が、それぞれ対応づけて設定されている。

【００３４】

第１ネットワークアクセス制御手段１０６は、サービス利用アプリケーション（101a、101b）とサービス提供手段１０２との間の通信を監視可能に構成されている第１監視手段（サービス提供手段監視手段）１０６ａと、サービス利用アプリケーション（101a、101b）によるサービス提供手段１０２を介したネットワークアクセスを制御可能に構成されている第１アクセス制御手段１０６ｂと、を有している。

【００３５】

第１監視手段１０６ａは、サービス利用アプリケーション（101a、101b）によるサービ

ス提供手段１０２の呼び出しを監視するものであり、例えば、ＡＰＩ（Application Program Interface）やシステムコールのフックなどの従来技術を用いて実現することができる。

【００３６】

また、第１アクセス制御手段１０６ｂは、第１監視手段１０６ａがサービス利用アプリケーション（101a、101b）によるサービス提供手段１０２の呼び出しをフックすると、フックされた呼び出しからネットワークアクセスを行おうとしているアプリケーション１０１のプロセス番号やアクセス対象を抽出する。そして、プロセス番号に基づいてサービス利用アプリケーション（101a、101b）のラベルをラベル割当手段１０３から取得し、アクセス対象であるフォルダ２０３のラベルをサーバ情報記憶手段１０４から取得する。そして、取得したサービス利用アプリケーション（101a、101b）のラベルとフォルダ２０３のラベルとに基づいて、アクセス制御ルール記憶手段１０５からアクセス制御ルールを参照することにより、サービス利用アプリケーション（101a、101b）のネットワークアクセスを制御する。

【００３７】

また、第１アクセス制御手段１０６ｂは、第２アクセス制御手段１０７ａからアクセス制御済みか否かの問合せを受け付けた場合は、所定の処理に従ってアクセス制御済みか否かを判断し、その結果を第２アクセス制御手段１０７ｂへ送信可能に構成されている。第１アクセス制御手段１０６ｂは、例えば、問合せに含まれるアプリケーションのプロセス番号やポート番号が、監視対象であるサービス提供手段１０２のプロセス番号やポート番号と一致するか否かを判断し、一致する場合はアクセス制御済みである旨を回答し、一致しない場合はアクセス制御済みでない旨を回答する。

【００３８】

第２ネットワークアクセス制御手段１０７は、通信手段１０８を介して実行される全てのネットワーク通信を監視可能に構成されている第２監視手段（ネットワークアクセス監視手段）１０７ａと、ネットワークアクセスがフックされた場合に、当該アプリケーションに対するアクセス制御が第２アクセス制御手段１０７ｂによって既に行われたか否かを判断し、判断結果に応じてネットワークアクセスを制御可能に構成されている第２アクセス制御手段１０７ｂと、を有している。

【００３９】

第２の監視手段１０７ａは、アプリケーション１０１による全てのネットワークアクセスを監視するものであり、例えば、ＴＤＩ（Transport Driver Interface）ドライバや、ＮＤＩＳ（Network Driver Interface Specification）ドライバなどの従来技術を適用して実現することができる。

【００４０】

また、第２アクセス制御手段１０７ｂは、第２監視手段１０７ｂによりアプリケーション１０１によるネットワークアクセスがフックされた場合に、当該アプリケーションに対するアクセス制御が第１アクセス制御手段１０６ｂによって既に行われたか否かを判断する。アクセス制御が既に行われたか否かは、例えば、第２アクセス制御手段１０７ｂが、フックされたアクセスからネットワークアクセスを行おうとしているアプリケーション（101c、101d）、もしくは、サービス提供手段１０２のプロセス番号やネットワークアクセスに用いるポート番号を抽出し、このプロセス番号やポート番号を含む問合せ（アクセス制御済みか否かの問合せ）を第１アクセス制御手段１０６ｂに通知し、第１アクセス制御手段１０６ｂから受信した問合結果に基づいて判断することができる。

【００４１】

なお、アクセス制御済みか否かの判断は、第１アクセス制御手段１０６ｂに問合せを行う方法に限られない。例えば、第１アクセス制御手段１０６ｂ又は第２アクセス制御手段１０７ｂが、アクセス制御を行うべきアプリケーション（（101ａ、101b）又は（101c、101d））のアプリケーション情報（例えば、プロセス番号やポート番号など）を予め定義して参照情報として所定の記憶領域に格納しておき、第２監視手段１０７ａがネットワー

クアクセスをフックすると、第２アクセス制御手段１０７ｂは、当該所定の記憶領域に格納されている参照情報を参照することにより、第１アクセス制御手段１０６ｂによるアクセス制御済みか否かの判断を行うようにしてもよい。また、参照情報は、アクセス制御を行うべきアプリケーションの情報に限られない。例えば、第２アクセス制御手段１０７ｂが制御する必要のないプログラムの情報、すなわち、サービス提供手段１０２の情報（例えば、プロセス番号やポート番号など）を、参照情報として所定の記憶領域に格納してもよい。第２アクセス制御手段１０７ｂは、当該参照情報を参照することにより、第１アクセス制御手段１０６ｂによるアクセス制御済みか否かの判断を行うことができる。

【００４２】

また、第２アクセス制御手段１０７ｂは、判断結果が否（アクセス制御済みでない）の場合、ネットワークアクセスへのアクセス制御を実行する。なお、この場合のネットワークアクセスは、サービス非利用アプリケーション（101c、101d）によるものとなる。具体的には、第２アクセス制御手段１０７ｂは、第２監視手段１０７がフックしたネットワークアクセスからアプリケーション（101c、101d）のプロセス番号やアクセス対象を抽出し、プロセス番号に基づいてアプリケーション（101c、101d）のラベルをラベル割当手段１０３から取得する。また、アクセス対象であるフォルダ２０３のラベルをサーバ情報記憶手段１０４から取得する。そして、取得したアプリケーション（101c、101d）のラベルとフォルダ２０３のラベルとに基づいて、アクセス制御ルール記憶手段１０５からアクセス制御ルールを参照することにより、アプリケーション（101c、101d）に対するアクセス制御を行う。なお、第２アクセス制御手段１０７ｂは、判断結果が是（アクセス制御が既に行われていると）の場合は、当該アプリケーション１０１（101a、101b）によるアクセスをそのまま許可する。

【００４３】

通信手段１０８は、ネットワークＮを介してサーバ２００その他の図示しない装置と通信し、情報を入出力可能に構成されている。例えば、ネットワークインタフェースカード（ＮＩＣ）やＴＣＰ／ＩＰドライバ等の既存の通信モジュールを備えている。

【００４４】

次に、サーバ２００は、通信手段２０１と、サーバアプリケーション２０２と、フォルダ２０３とを備えている。サーバ２００は、サーバ２００の処理及び動作を制御するＣＰＵ、ＲＯＭやＲＡＭ等のメモリ、各種情報を格納する外部記憶装置、通信インタフェース、入出力インタフェース及びこれらを結ぶバス等のハードウェアを備える汎用のサーバ・コンピュータを適用することができる。なお、サーバ・コンピュータのハードウェア構成は、図２にて説明したハードウェア構成と同様であるため、説明を省略する。

【００４５】

通信手段２０１は、ネットワークＮを介してクライアント１００その他の図示しない装置と通信し、情報を入出力可能に構成されている。例えば、ネットワークインタフェースカード（ＮＩＣ）やＴＣＰ／ＩＰドライバ等の既存の通信モジュールを備えている。

【００４６】

サーバアプリケーション２０２は、ネットワークサービスを提供するプログラムであり、外部記憶装置等に格納され、ＣＰＵによって実行される。特に限定はないが、例えば、ＦＴＰやＣＩＦＳなどを実装した既存のプログラムが該当する。

【００４７】

フォルダ２０３は、アクセス対象となるデータを保管するものであり、ディレクトリとも呼ばれる。フォルダ２０３は、割り当てられるラベルによって区別され、本実施形態では、一例として、一般ラベルが割り当てられたフォルダ（一般フォルダ）と、機密ラベルが割り当てられたフォルダ（機密フォルダ）とに区別される。なお、ラベルの内容はこれに限られず、設計に応じて適宜設定することができる。フォルダ２０３とラベルの対応関係は、サーバ情報記憶手段１０４に格納されている（図４）。

【００４８】

次に、ネットワークＮは、クライアント１００とサーバ２００の間で情報を送受信する

ための回線である。ネットワークＮは、例えば、インターネット、専用線、パケット通信網、電話回線、ＬＡＮ、企業内ネットワーク、その他の通信回線、それらの組み合わせ等のいずれであってもよく、有線であるか無線であるかを問わない。

【００４９】

［機密情報漏洩防止処理の流れ］

図５を参照して、本実施形態に係る機密情報漏洩防止処理について説明する。なお、同図に示す各処理ステップは処理内容に矛盾を生じない範囲で任意に順番を変更して又は並列に実行することができる。また、各処理ステップ間に他のステップを追加してもよい。また、便宜上１ステップとして記載されているステップは、複数ステップに分けて実行することができる一方、便宜上複数ステップに分けて記載されているものは、１ステップとして把握することができる。

【００５０】

電源投入などの所定のタイミングで、第２監視手段１０７ｂは、全てのネットワーク通信の監視を開始する（Ｓ１０１）。また、第１監視手段１０６ａは、サービス利用アプリケーション（101a又は101b）とサービス提供手段１０２との間の通信の監視を開始する（Ｓ１０２）。

【００５１】

制御手段（ＣＰＵ）により実行されるアプリケーション１０１は、例えば、ユーザによる操作指示に従って、指定されたネットワーク上のアクセス対象に対するアクセスを開始する（Ｓ１０３）。ここでは、サーバ２００のフォルダ２０３（203a又は203b）がアクセス対象に指定されたものとする。以下、アプリケーション１０１が、サービス利用アプリケーション（101a又は101b）である場合の処理について説明し、次に、サービス非利用アプリケーション（101c又は101d）である場合の処理について説明する。

【００５２】

サービス利用アプリケーション（101a又は101b）は、例えばシステムコールによりサービス提供手段１０２を呼び出す（Ｓ１０４）。

【００５３】

第１監視手段１０６ａは、サービス利用アプリケーション（101a又は101b）がサービス提供手段１０２を呼び出すと、当該呼び出しをフックする（Ｓ１０５；ＹＥＳ）。

【００５４】

第１アクセス制御手段１０６ｂは、第１監視手段１０６ａによりフックされた呼び出しに含まれる情報（例えば、プロセス番号やフォルダ情報）に基づいて、サービス利用アプリケーション（101a又は101b）を特定し、アクセス制御を開始する。

【００５５】

第１アクセス制御手段１０６ｂは、当該サービス利用アプリケーション（101a又は101b）に割り当てられているラベルを、プロセス番号に基づいてラベル割り当て手段１０３から取得し、一方、アクセス先のフォルダ２０３（203a又203b）に割り当てられているラベルを、フォルダ情報に基づいてサーバ情報記憶手段１０４から取得する（Ｓ１０６ｂ）。

【００５６】

第１アクセス制御手段１０６ｂは、ラベル割り当て手段１０３から取得したサービス利用アプリケーション（101a又は101b）に割り当てられているラベルと、サーバ情報記憶手段１０４から取得したアクセス先のフォルダ２０３（203a又203b）に割り当てられているラベルとに基づいて、アクセス制御ルール記憶手段１０５に記憶されているアクセス制御ルールを参照し、サービス利用アプリケーション（101a又は101b）のフォルダ２０３（203a又203b）に対するアクセスを制御する。

【００５７】

例えば、アプリＡからフォルダＢに対するアクセス要求である場合は、一般アプリケーションから機密フォルダへのアクセス要求であるため、アクセス制御ルールにより、当該アクセスは禁止される。一方、アプリＢからフォルダＢに対するアクセス要求である場合は、機密アプリケーションから機密フォルダへのアクセス要求であるため、アクセス制御

ルールにより、当該アクセスは許可される。

【００５８】

サービス提供手段１０２は、第１アクセス制御手段１０６ｂによるアクセス制御に従って、フォルダ２０３へのネットワークアクセスを実行する（Ｓ１０８）。例えば、サービス提供手段１０２は、当該サービス提供手段１０２のポート番号やプロセス番号及びアクセス先のフォルダ情報を含む通信ソケット等を生成して通信手段１０８へ送出する。なお、サービス提供手段１０２は、アクセスが禁止された場合は、ネットワークアクセスを実行せずに処理を終了する。

【００５９】

一方、Ｓ１０３に戻り、アプリケーション１０１が、サービス非利用アプリケーション（101c又は101d）である場合について説明する。サービス非利用アプリケーション（101c又は101d）は、当該サービス非利用アプリケーション（101c又は101d）のポート番号やプロセス番号及びアクセス先のフォルダ情報を含む通信ソケット等を直接生成して、通信手段１０８へ送出することにより、ネットワークアクセスを実行する（Ｓ１０９）。

【００６０】

次に、第２監視手段１０７ａは、サービス提供手段１０２又はサービス非利用アプリケーション（101c又は101d）によるネットワークアクセスをフックする（Ｓ１１０；ＹＥＳ）。

【００６１】

第２アクセス制御手段１０７ｂは、第２監視手段１０７ａによりフックされたアクセスが、第１アクセス制御手段１０６ｂによってアクセス制御が既に行われているか否かを判断する（Ｓ１１１）。例えば、第２アクセス制御手段１０７ｂは、通信ソケットに含まれるポート番号やプロセス番号を含む問い合わせを第１アクセス制御手段１０６ｂに送信する。そして、問合せ結果を受信すると、この問い合わせ結果に基づいて、アクセス制御済みか否かを判断する。なお、参照情報が所定の記憶領域に格納されている場合は、通信ソケットに含まれるポート番号やプロセス番号に基づいて参照情報を参照し、参照結果に基づいて、アクセス制御済みか否かを判断する。

【００６２】

第２アクセス制御手段１０７ｂは、第２監視手段１０７ａによりフックされたアクセスが、第１アクセス制御手段１０６ｂによってアクセス制御が既に行われていると判断した場合は（Ｓ１１２；ＹＥＳ）、フックしたネットワークイベントを実行するなどして通信を許可する（Ｓ１１３）。なお、この場合、フックされたアクセスは、サービス提供手段１０２によるものである。

【００６３】

一方、第２アクセス制御手段１０７ｂは、第２監視手段１０７ａによりフックされたアクセスが、第１アクセス制御手段１０６ｂによってアクセス制御が行われていないと判断した場合は（Ｓ１１２；ＮＯ）、当該アプリケーションのアクセス制御を実行する。なお、この場合のアプリケーション１０１は、サービス非利用アプリケーション（101c又は101d）である。

【００６４】

第２アクセス制御手段１０７ｂは、サービス非利用アプリケーション（101c又は101d）に割り当てられているラベルを、フックしたアクセスから得られるプロセス番号に基づいてラベル割り当て手段１０３から取得し、アクセス先のフォルダ２０３（203a又203b）に割り当てられているラベルを、フックしたアクセスから得られるフォルダ情報に基づいてサーバ情報記憶手段１０４から取得する（Ｓ１１４）。

【００６５】

第２アクセス制御手段１０７ｂは、ラベル割り当て手段１０３から取得したサービス非利用アプリケーション（101c又は101d）に割り当てられているラベルと、サーバ情報記憶手段１０４から取得したアクセス先のフォルダ２０３（203a又203b）に割り当てられているラベルとに基づいて、アクセス制御ルール記憶手段１０５に記憶されているアクセス制

御ルールを参照し、サービス非利用アプリケーション（101c又は101d）のフォルダ２０３（203a又203b）に対するアクセスを制御する（Ｓ１１５）。

【００６６】

例えば、アプリＣからフォルダＡに対するアクセス要求である場合は、機密アプリケーションから一般フォルダへのアクセス要求であるため、アクセス制御ルールにより、読み込みのみが許可される。一方、アプリＤからフォルダＢに対するアクセス要求である場合は、一般アプリケーションから一般フォルダへのアクセス要求であるため、アクセス制御ルールにより、当該アクセスは許可される。

【００６７】

以上より、アプリケーション１０１又はサービス提供手段１０２は、第１アクセス制御手段１０６ｂ又は第２アクセス制御手段１０７ｂによるアクセス制御に従って、サーバ２００のサーバアプリケーション２０２と通信し、サーバアプリケーション２０２からアクセス対象のフォルダ２０３のデータを取得する（Ｓ１１６）。

【００６８】

以上、本実施形態によれば、サービス利用アプリケーション（101a又は101b）によるサービス利用手段を介したネットワークアクセスは、第１ネットワークアクセス制御手段１０６により制御され、サービス非利用アプリケーション（101c又は101d）によるネットワークアクセスは、第２ネットワークアクセス制御手段１０７により制御されることになる。その結果、ネットワークアクセスの方法にかかわらず、アプリケーションからのネットワークアクセスを、当該アプリケーションに付与されたラベルに応じて漏れなく制御することが可能になる。

【００６９】

また、既存システムのクライアントは、そのほとんどがプロプラエタリ・ソフトウェアを実装しているため、オペレーションシステムやアプリケーションを改造することは好ましくないところ、本実施形態によれば、既存のオペレーションシステムやアプリケーションを改造することなく、機密情報漏洩防止を実現することが可能になる。

【００７０】

また、本実施形態によれば、例えばマシン仮想化（VA）等の方法によりマルチセキュリティを実現する場合に比べて、リソース消費量を抑えることができるので、低スペックの装置にも適用することが可能になる。

【００７１】

［その他の実施形態］

なお、本発明は、上記した実施の形態に限定されるものではなく、本発明の要旨を逸脱しない範囲内において、他の様々な形で実施することができる。このため、上記実施形態はあらゆる点で単なる例示にすぎず、限定的に解釈されるものではない。例えば、上述の各処理ステップは処理内容に矛盾を生じない範囲で任意に順番を変更して又は並列に実行することができる。

【００７２】

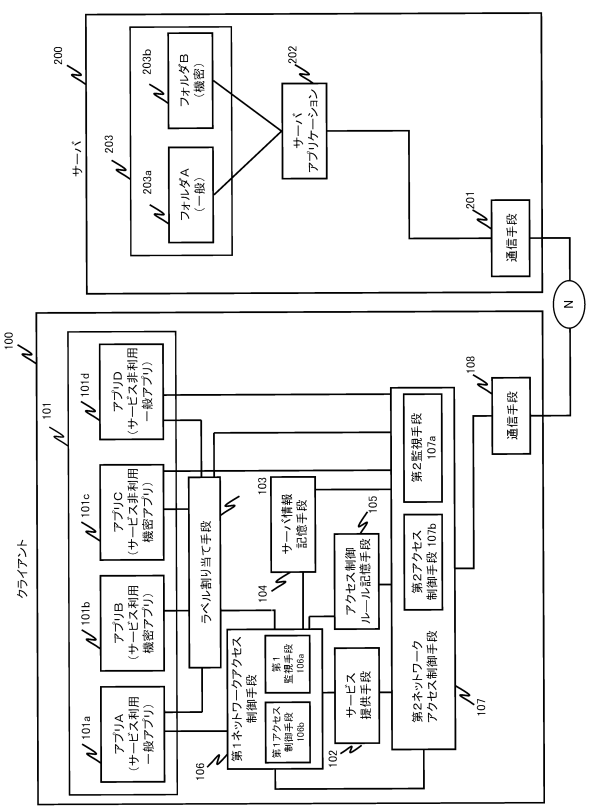
例えば、上記実施形態では、クライアント１００が１つのサービス提供手段１０２を有する場合について説明したが、クライアント１００は、設計に応じて任意の数のサービス提供手段１０２を有することができる。クライアント１００が複数のサービス提供手段１０２を有する場合、第１監視１０６ａは、アプリケーション１０１と各サービス提供手段１０２との間の通信をそれぞれ監視し、第２アクセス制御手段１０６ｂは、監視結果に応じてアクセス制御を行うように構成される。

【００７３】

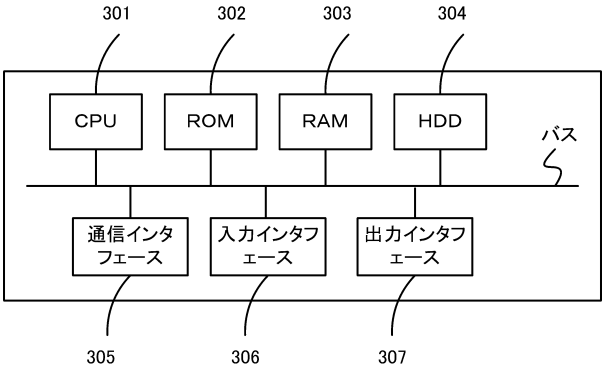
また、例えば、上記実施形態では、アプリケーションによるフォルダに対する読み書きを制御する場合について説明したが、アクセス主体、アクセス内容及びアクセス対象については、任意にこれを設定することができる。例えば、アプリケーションがネットワークを介してメールを送受信する場合には、アプリケーションやメールアドレスに割り当てられたラベルに応じて、メールの送受信を制御するようにしてもよい。

【００７４】
この出願は、２０１０年１月１３日に出願された日本出願特願２０１０－５１８７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。
【００７５】
以上、実施形態を参照して本発明を説明したが、本発明は上記実施形態に限定されるものではない。本発明の構成や詳細には、本発明のスコープ内で当業者が理解し得る様々な変更をすることができる。
【産業上の利用可能性】
【００７６】
本発明に係る機密情報漏洩防止システム、機密情報漏洩防止方法及び機密情報漏洩防止プログラムは、アプリケーションによるネットワークアクセスの方法にかかわらず、当該アプリケーションによるネットワークアクセスを、当該アプリケーションのセキュリティレベルに応じて漏れなく制御することに適している。
【符号の説明】
【００７７】
１００…クライアント、１０１…アプリケーション、１０１ａ…アプリＡ（サービス利用一般アプリ）、１０１ｂ…アプリＢ（サービス利用機密アプリ）、１０１ｃ…アプリＣ（サービス非利用機密アプリ）、１０１ｄ…アプリＤ（サービス非利用一般アプリ）、１０２…サービス提供手段、１０３…ラベル割当手段、１０４…サーバ情報記憶手段、１０５…アクセス制御ルール記憶手段、１０６…第１ネットワークアクセス制御手段、１０６ａ…第１監視手段、１０６ｂ…第１アクセス制御手段、１０７…第２ネットワークアクセス制御手段、１０７ａ…第２監視手段、１０７ｂ…第２アクセス制御手段、１０８…通信手段、２００…サーバ、２０１…通信手段、２０２…サーバアプリケーション、２０３…フォルダ、２０３ａ…フォルダＡ（一般）、２０３ｂ…フォルダ（機密）

【図１】



【図２】



【図３】

103

プロセスID	アプリケーション	ラベル
0001	アプリA	一般
0002	アプリＢ	機密
0003	アプリＣ	機密
0004	アプリＤ	一般
⋮	⋮	⋮

【図４】

104

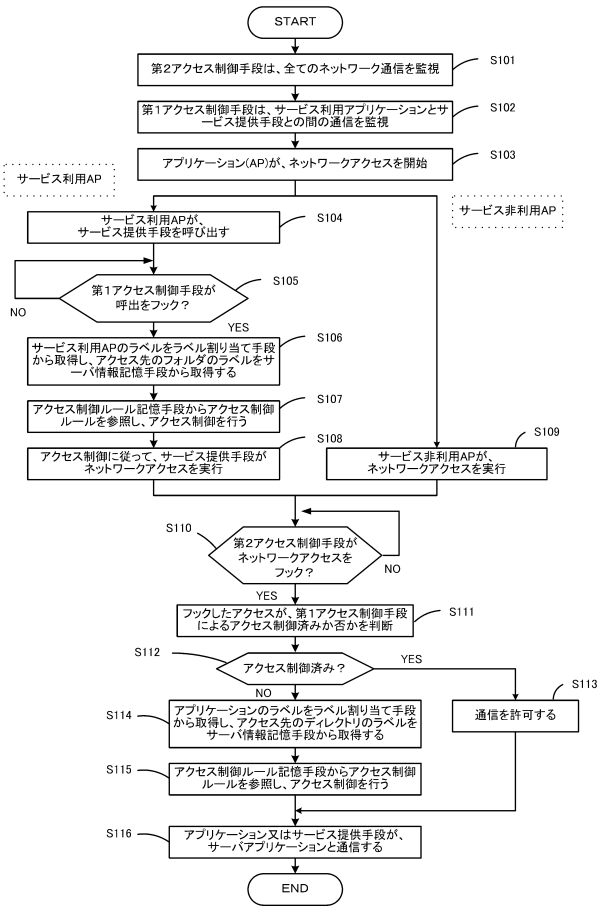
フォルダ	ラベル
フォルダA	一般
フォルダB	機密
⋮	⋮

【図５】

105

	機密フォルダ	一般フォルダ
機密アプリケーション	アクセス許可。	読み込みのみ許可。
一般アプリケーション	アクセス禁止。	アクセス許可。

【図６】



フロントページの続き

(72)発明者　佐々木　貴之
東京都港区芝五丁目７番１号　日本電気株式会社内

審査官　平井　誠

(56)参考文献　特開２００３－１７３２８４（ＪＰ，Ａ）
特開平１１－２７２６１６（ＪＰ，Ａ）
特開２００３－０４４２９７（ＪＰ，Ａ）
特開２００５－２０９１８１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１