

【公報種別】特許法第 17 条の 2 の規定による補正の掲載

【部門区分】第 6 部門第 3 区分

【発行日】平成22年3月11日 (2010.3.11)

【公開番号】特開2007-48310(P2007-48310A)

【公開日】平成19年2月22日 (2007.2.22)

【年通号数】公開・登録公報2007-007

【出願番号】特願2006-268814(P2006-268814)

【国際特許分類】

G 0 6 F 21/22 (2006.01)

G 0 6 F 21/20 (2006.01)

G 0 6 F 21/24 (2006.01)

【F I】

G 0 6 F 9/06 6 6 0 E

G 0 6 F 15/00 3 3 0 D

G 0 6 F 12/14 5 2 0 B

G 0 6 F 12/14 5 5 0 A

G 0 6 F 12/14 5 2 0 A

【手続補正書】

【提出日】平成22年1月26日 (2010.1.26)

【手続補正 1】

【補正対象書類名】特許請求の範囲

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項 1】

コンピュータ上のオペレーティングシステムが管理しているコンピュータリソースに対するアクセスを制御する情報処理装置であって、

前記オペレーティングシステムが管理しているコンピュータリソースを示すリソース情報と、コンピュータリソースを他のコンピュータリソースへ出力するアクセス権限の種類を示すアクセス権限情報と、アクセス権限が有効となる条件とを、前記オペレーティングシステムが管理しているコンピュータリソース毎に管理する管理テーブルを記憶する記憶手段と、

前記コンピュータリソースに対するプロセスからの操作要求を、前記オペレーティングシステムへ渡る前に捕捉する捕捉手段と、

プロセスと第 1 コンピュータリソースとの対応が記憶媒体に既に登録されている状態で、前記捕捉手段で第 2 コンピュータリソースに対する操作要求を捕捉した場合、前記管理テーブルを参照して、前記第 1 コンピュータリソースの第 1 アクセス権限情報と、前記第 2 コンピュータリソースの第 2 アクセス権限情報とをチェックして、そのチェックした両者それぞれのアクセス権限の有無に基づいて、該第 1 コンピュータリソースから該第 2 コンピュータリソースへ出力するアクセス権限が前記プロセスにあるか否かを判定する判定手段と、

前記判定手段の判定の結果、前記アクセス権限があれば前記操作要求をオペレーティングシステムに渡し、その結果を前記プロセスに返す処理手段と、

前記判定手段の判定の結果、前記アクセス権限がなければ前記操作要求によって実行すべき処理を拒否する拒否手段と

を備えることを特徴とする情報処理装置。

【請求項 2】

前記捕捉手段は、前記プロセスがコンピュータリソースを保持する場合には、その捕捉した操作要求に対して該プロセスと前記コンピュータリソースとの対応を記憶媒体に登録する

ことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 3】

前記捕捉手段は、更に、前記オペレーティングシステムからの操作要求を、コンピュータリソースにアクセスする前に捕捉する

ことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 4】

前記アクセス権限情報は、前記オペレーティングシステムで定義されていない拡張したアクセス権限を指定するアクセス権限である

ことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 5】

前記アクセス権限情報は、他媒体への移動権限、他媒体へのコピー権限、印刷権限、共有メモリへの読み込み権限、画面キャプチャ権限、使用プロセスの限定権限のうち少なくとも 1 つを指定する情報を含む

ことを特徴とする請求項 4 に記載の情報処理装置。

【請求項 6】

前記拒否手段は、要求された前記第 2 コンピュータリソースにアクセスせずにアクセス違反のエラー通知を前記プロセスに返す

ことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 7】

当該情報処理装置でのアクセス制御に関する履歴情報を出力する履歴情報出力手段を更に備える

ことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 8】

前記履歴情報出力手段は、前記履歴情報として、前記処理手段による処理内容あるいは前記拒否手段による拒否内容を示すコンピュータリソースのアクセス状況を出力する

ことを特徴とする請求項 7 に記載の情報処理装置。

【請求項 9】

前記履歴情報出力手段は、指定された通知先の端末に履歴情報を通知する

ことを特徴とする請求項 7 または 8 に記載の情報処理装置。

【請求項 10】

前記履歴情報は、ファイル名、ユーザ名、操作名、日時、端末名の少なくとも 1 つを含む

ことを特徴とする請求項 7 または 8 に記載の情報処理装置。

【請求項 11】

前記第 1 コンピュータリソースとして複製権限のないファイルをアプリケーションがオープンしている状態で、該アプリケーションが該ファイルの前記第 2 コンピュータリソースとしての別ファイルを作成する操作要求を捕捉した場合、前記判定手段は、前記アクセス権限がないと判定し、前記拒否手段は、アプリケーションが別ファイルを作成することを拒否することで、前記操作要求によって実行すべき別ファイルの作成を拒否する

ことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 12】

前記第 1 コンピュータリソースとして印刷権限のないファイルをアプリケーションがオープンしている状態で、該アプリケーションが該ファイルを印刷する操作要求を捕捉した場合、前記判定手段は、前記アクセス権限がないと判定し、前記拒否手段は、該アプリケーションのプリンタ選択またはプリンタデバイスのオープンを拒否することで、前記操作要求によって実行すべき印刷を拒否する

ことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 13】

前記第 2 コンピュータリソースとしてアクセス権限のない外部装置へのアクセスを要求する操作要求を捕捉した場合、前記判定手段は、前記アクセス権限がないと判定し、前記拒否手段は、アクセス禁止エラーまたは前記外部装置が存在しないというエラーを前記プロセスに返すことで、前記操作要求によって実行すべきアクセスを拒否する

ことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 1 4】

前記第 1 コンピュータリソースとして複写権限のないファイルをアプリケーションがオープンしている状態で、該アプリケーションが該ファイルの一部または全てを複写 / 埋め込みオブジェクトの形式でデータを前記第 2 コンピュータリソースに登録する操作要求を捕捉した場合、前記判定手段は、前記アクセス権限がないと判定し、前記拒否手段は、前記データの登録に替えて空データを登録することで、前記操作要求によって実行すべきデータの登録を拒否する

ことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 1 5】

前記第 1 コンピュータリソースとして外部出力権限のないファイルをアプリケーションがオープンしている状態で、該アプリケーションが該ファイルを外部出力する操作要求を捕捉した場合、前記判定手段は、前記アクセス権限がないと判定し、前記拒否手段は、該アプリケーションからの接続要求または送信要求をアクセス違反もしくはタイムアウトのエラーで拒否することで、前記操作要求によって実行すべき外部出力を拒否する

ことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 1 6】

ウィンドウを所有しているアプリケーションが画面イメージ取得権限のないファイルを前記第 1 コンピュータリソースとして保持している状態で、該アプリケーションが該ファイルを画面イメージ取得する操作要求を捕捉した場合、前記判定手段は、前記アクセス権限がないと判定し、前記拒否手段は、画面の一部または全体、または該ウィンドウのイメージ取得を拒否することで、前記操作要求によって実行すべき画面イメージ取得を拒否する

ことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 1 7】

前記判定手段は、前記捕捉手段で捕捉した操作要求に対するコンピュータリソース内部に前記アクセス権限情報が記述されている場合、前記コンピュータリソース内部に記述されている前記アクセス権限情報を参照する

ことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 1 8】

前記コンピュータリソースは、Web ページであり、

前記アクセス権限情報は、前記 Web ページ内のタグとして記述されている

ことを特徴とする請求項 1 7 に記載の情報処理装置。

【請求項 1 9】

オペレーティングシステムが管理しているコンピュータリソースに対するアクセスを制御する情報処理方法であって、

保持手段が、前記オペレーティングシステムが管理しているコンピュータリソースを示すリソース情報と、コンピュータリソースを他のコンピュータリソースへ出力するアクセス権限の種類を示すアクセス権限情報と、アクセス権限が有効となる条件とを、前記オペレーティングシステムが管理しているコンピュータリソース毎に管理する管理テーブルを記憶媒体で保持する保持工程と、

捕捉手段が、前記コンピュータリソースに対するプロセスからの操作要求を、前記オペレーティングシステムへ渡る前に捕捉する捕捉工程と、

判定手段が、プロセスと第 1 コンピュータリソースとの対応が記憶媒体に既に登録されている状態で、前記捕捉工程で第 2 コンピュータリソースに対する操作要求を捕捉した場合、前記管理テーブルを参照して、前記第 1 コンピュータリソースの第 1 アクセス権限情報と、前記第 2 コンピュータリソースの第 2 アクセス権限情報とをチェックして、そのチ

チェックした両者それぞれのアクセス権限の有無に基づいて、該第 1 コンピュータリソースから該第 2 コンピュータリソースへ出力するアクセス権限が前記プロセスにあるか否かを判定する判定工程と、

処理手段が、前記判定工程の判定の結果、前記アクセス権限があれば前記操作要求をオペレーティングシステムに渡し、その結果を前記プロセスに返す処理工程と、

拒否手段が、前記判定工程の判定の結果、前記アクセス権限がなければ前記操作要求によって実行すべき処理を拒否する拒否工程と

を備えることを特徴とする情報処理方法。

【請求項 20】

コンピュータ上のオペレーティングシステムが管理しているコンピュータリソースに対するアクセスを制御する情報処理をコンピュータに実行させるためのプログラムであって、前記コンピュータを、

前記オペレーティングシステムが管理しているコンピュータリソースを示すリソース情報と、コンピュータリソースを他のコンピュータリソースへ出力するアクセス権限の種類を示すアクセス権限情報と、アクセス権限が有効となる条件とを、前記オペレーティングシステムが管理しているコンピュータリソース毎に管理する管理テーブルを記憶する記憶手段と、

前記コンピュータリソースに対するプロセスからの操作要求を、前記オペレーティングシステムへ渡す前に捕捉する捕捉手段と、

プロセスと第 1 コンピュータリソースとの対応が記憶媒体に既に登録されている状態で、前記捕捉手段で第 2 コンピュータリソースに対する操作要求を捕捉した場合、前記管理テーブルを参照して、前記第 1 コンピュータリソースの第 1 アクセス権限情報と、前記第 2 コンピュータリソースの第 2 アクセス権限情報とをチェックして、そのチェックした両者それぞれのアクセス権限の有無に基づいて、該第 1 コンピュータリソースから該第 2 コンピュータリソースへ出力するアクセス権限が前記プロセスにあるか否かを判定する判定手段と、

前記判定手段の判定の結果、前記アクセス権限があれば前記操作要求をオペレーティングシステムに渡し、その結果を前記プロセスに返す処理手段と、

前記判定手段の判定の結果、前記アクセス権限がなければ前記操作要求によって実行すべき処理を拒否する拒否手段と

して機能させることを特徴とするプログラム。

【請求項 21】

前記捕捉手段は、前記プロセスがコンピュータリソースを保持する場合には、その捕捉した操作要求に対して該プロセスと前記コンピュータリソースとの対応を記憶媒体に登録する

ことを特徴とする請求項 20 に記載のプログラム。

【請求項 22】

前記捕捉手段は、更に、前記オペレーティングシステムからの操作要求を、コンピュータリソースにアクセスする前に捕捉する

ことを特徴とする請求項 20 に記載のプログラム。

【請求項 23】

前記アクセス権限情報は、前記オペレーティングシステムで定義されていない拡張したアクセス権限を指定するアクセス権限である

ことを特徴とする請求項 20 に記載のプログラム。

【請求項 24】

前記アクセス権限情報は、他媒体への移動権限、他媒体へのコピー権限、印刷権限、共有メモリへの読み込み権限、画面キャプチャ権限、使用プロセスの限定権限のうち少なくとも 1 つを指定する情報を含む

ことを特徴とする請求項 23 に記載のプログラム。

【請求項 25】

前記拒否手段は、要求された前記第 2 コンピュータリソースにアクセスせずにアクセス違反のエラー通知を前記プロセスに返す

ことを特徴とする請求項 20 に記載のプログラム。

【請求項 26】

前記情報処理装置でのアクセス制御に関する履歴情報を出力する履歴情報出力手段を更に備える

ことを特徴とする請求項 20 に記載のプログラム。

【請求項 27】

前記履歴情報出力手段は、前記履歴情報として、前記処理手段による処理内容あるいは前記拒否手段による拒否内容を示すコンピュータリソースのアクセス状況を出力する

ことを特徴とする請求項 26 に記載のプログラム。

【請求項 28】

前記履歴情報出力手段は、指定された通知先の端末に履歴情報を通知する

ことを特徴とする請求項 26 または 27 に記載のプログラム。

【請求項 29】

前記履歴情報は、ファイル名、ユーザ名、操作名、日時、端末名の少なくとも 1 つを含む

ことを特徴とする請求項 26 または 27 に記載のプログラム。

【請求項 30】

前記第 1 コンピュータリソースとして複製権限のないファイルをアプリケーションがオープンしている状態で、該アプリケーションが該ファイルの前記第 2 コンピュータリソースとしての別ファイルを作成する操作要求を捕捉した場合、前記判定手段は、前記アクセス権限がないと判定し、前記拒否手段は、アプリケーションが別ファイルを作成することを拒否することで、前記操作要求によって実行すべき別ファイルの作成を拒否する

ことを特徴とする請求項 20 に記載のプログラム。

【請求項 31】

前記第 1 コンピュータリソースとして印刷権限のないファイルをアプリケーションがオープンしている状態で、該アプリケーションが該ファイルを印刷する操作要求を捕捉した場合、前記判定手段は、前記アクセス権限がないと判定し、前記拒否手段は、該アプリケーションのプリンタ選択またはプリンタデバイスのオープンを拒否することで、前記操作要求によって実行すべき印刷を拒否する

ことを特徴とする請求項 20 に記載のプログラム。

【請求項 32】

前記第 2 コンピュータリソースとしてアクセス権限のない外部装置へのアクセスを要求する操作要求を捕捉した場合、前記判定手段は、前記アクセス権限がないと判定し、前記拒否手段は、アクセス禁止エラーまたは前記外部装置が存在しないというエラーを前記プロセスに返すことで、前記操作要求によって実行すべきアクセスを拒否する

ことを特徴とする請求項 20 に記載のプログラム。

【請求項 33】

前記第 1 コンピュータリソースとして複写権限のないファイルをアプリケーションがオープンしている状態で、該アプリケーションが該ファイルの一部または全てを複写 / 埋め込みオブジェクトの形式でデータを前記第 2 コンピュータリソースに登録する操作要求を捕捉した場合、前記判定手段は、前記アクセス権限がないと判定し、前記拒否手段は、前記データの登録に替えて空データを登録することで、前記操作要求によって実行すべきデータの登録を拒否する

ことを特徴とする請求項 20 に記載のプログラム。

【請求項 34】

前記第 1 コンピュータリソースとして外部出力権限のないファイルをアプリケーションがオープンしている状態で、該アプリケーションが該ファイルを外部出力する操作要求を捕捉した場合、前記判定手段は、前記アクセス権限がないと判定し、前記拒否手段は、該アプリケーションからの接続要求または送信要求をアクセス違反もしくはタイムアウトのエ

ラーで拒否することで、前記操作要求によって実行すべき外部出力を拒否することを特徴とする請求項 20 に記載のプログラム。

【請求項 35】

ウィンドウを所有しているアプリケーションが画面イメージ取得権限のないファイルを前記第 1 コンピュータリソースとして保持している状態で、該アプリケーションが該ファイルを画面イメージ取得する操作要求を捕捉した場合、前記判定手段は、前記アクセス権限がないと判定し、前記拒否手段は、画面の一部または全体、または該ウィンドウのイメージ取得を拒否することで、前記操作要求によって実行すべき画面イメージ取得を拒否することを特徴とする請求項 20 に記載のプログラム。

【請求項 36】

前記判定手段は、前記捕捉手段で捕捉した操作要求に対するコンピュータリソース内部に前記アクセス権限情報が記述されている場合、前記コンピュータリソース内部に記述されている前記アクセス権限情報を参照する

ことを特徴とする請求項 20 に記載のプログラム。

【請求項 37】

前記コンピュータリソースは、Web ページであり、

前記アクセス権限情報は、前記 Web ページ内のタグとして記述されている

ことを特徴とする請求項 36 に記載のプログラム。