(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5226199号
(P5226199)

(45)発行日　平成25年7月3日(2013.7.3)　(24)登録日　平成25年3月22日(2013.3.22)

(51)Int.Cl.		F I		
G06F 21/62	(2013.01)	G06F	21/24	163C
G06F 21/55	(2013.01)	G06F	21/00	155C
G06F 21/44	(2013.01)	G06F	21/20	144A

請求項の数 31　(全 48 頁)

(21)出願番号	特願2006-268814 (P2006-268814)
(22)出願日	平成18年9月29日 (2006.9.29)
(62)分割の表示	特願2001-322437 (P2001-322437)の分割
原出願日	平成13年10月19日 (2001.10.19)
(65)公開番号	特開2007-48310 (P2007-48310A)
(43)公開日	平成19年2月22日 (2007.2.22)
審査請求日	平成18年10月27日 (2006.10.27)
審判番号	不服2011-5804 (P2011-5804/J1)
審判請求日	平成23年3月15日 (2011.3.15)
(31)優先権主張番号	特願2000-352113 (P2000-352113)
(32)優先日	平成12年11月20日 (2000.11.20)
(33)優先権主張国	日本国(JP)
(31)優先権主張番号	特願2001-161403 (P2001-161403)
(32)優先日	平成13年4月23日 (2001.4.23)
(33)優先権主張国	日本国(JP)

(73)特許権者　500083226
ハミングヘッズ株式会社
東京都中央区月島１丁目２番１３号
(74)代理人　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(74)代理人　100130409
弁理士　下山　治

最終頁に続く

(54)【発明の名称】情報処理装置及びその方法、プログラム

(57)【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、前記コンピュータリソースにアクセスするために指定されたアプリケーションからの操作要求を、前記アプリケーションと前記オペレーティングシステムとの間に介在するリソース管理プログラムが、前記アプリケーションが発行する前記コンピュータリソースに対する操作要求を監視して、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、

前記捕捉手段が捕捉した前記アプリケーションからの第１の操作要求によって前記アプリケーションが第１コンピュータリソースを保持する場合、前記リソース管理プログラムが、前記アプリケーションと前記第１コンピュータリソースとの対応関係を示す情報として、前記アプリケーションが前記第１コンピュータリソースを保持しているという情報を記憶媒体に登録する登録手段と、

前記アプリケーションと前記第１コンピュータリソースとの対応関係を示す情報が前記

登録手段によって前記記憶媒体に既に登録されている状態で、前記捕捉手段が、前記第１コンピュータリソースに対する前記アプリケーションからの更なる第２の操作要求であって前記第１コンピュータリソースから第２コンピュータリソースへ出力する操作要求を捕捉した場合、前記リソース管理プログラムが、前記管理テーブルで管理されるコンピュータリソース毎のレコードの内、前記第１コンピュータリソースのレコードのアクセス権限情報をチェックして、前記第１コンピュータリソースから前記第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アプリケーション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、前記リソース管理プログラムが、前記第２の操作要求をオペレーティングシステムに渡し、その結果を前記アプリケーションに返す処理手段と、

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、前記リソース管理プログラムが、前記第２の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、

前記拒否手段は、

前記アクセス権限がなく、かつ、前記アプリケーションが発行した前記第２の操作要求の結果としてエラーを返すことができる場合は、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アプリケーションに返すことで、前記第２の操作要求によって実行すべき処理を拒否し、

前記アクセス権限がなく、かつ、前記アプリケーションが発行した前記第２の操作要求の結果としてエラーを返すことができない場合は、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、前記第２の操作要求を、前記リソース管理プログラムが予め用意したダミーのリソースへの操作要求に代えて、前記第２の操作要求を処理することで、前記第２の操作要求によって実行すべき処理を拒否する

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、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３】

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４】

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、画面キャプチャー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３に記載の情報処理装置。

【請求項５】

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６】

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５に記載の情報処理装置。

【請求項７】

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５または６に記載の情報処理装置。

【請求項８】

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５または６に記載の情報処理装置。

【請求項９】
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、前記第２の操作要求として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、前記第２の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１０】
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、前記第２の操作要求として該アプリケーションが該ファイルを前記第２コンピュータリソースとしてのプリンタへ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、前記第２の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１１】
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、前記第２の操作要求として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、前記第２の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１２】
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、前記第２の操作要求として該アプリケーションが該ファイルを前記第２コンピュータリソースとしての外部装置へ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、前記第２の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１３】
ウイ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、前記第２の操作要求として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、または該ウインドウのイメージ取得を拒否することで、前記第２の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１４】
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１５】
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１４に記載の情報処理装置。
【請求項１６】

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、前記コンピュータリソースにアクセスするために指定されたアプリケーションからの操作要求を、前記アプリケーションと前記オペレーティングシステムとの間に介在するリソース管理プログラムが、前記アプリケーションが発行する前記コンピュータリソースに対する操作要求を監視して、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、
登録手段が、前記捕捉工程が捕捉した前記アプリケーションからの第１の操作要求によって前記アプリケーションが第１コンピュータリソースを保持する場合、前記リソース管理プログラムが、前記アプリケーションと前記第１コンピュータリソースとの対応関係を示す情報として、前記アプリケーションが前記第１コンピュータリソースを保持しているという情報を記憶媒体に登録する登録工程と、
判定手段が、前記アプリケーションと前記第１コンピュータリソースとの対応関係を示す情報が前記登録工程によって前記記憶媒体に既に登録されている状態で、前記捕捉工程が、前記第１コンピュータリソースに対する前記アプリケーションからの更なる第２の操作要求であって前記第１コンピュータリソースから第２コンピュータリソースへ出力する操作要求を捕捉した場合、前記リソース管理プログラムが、前記管理テーブルで管理されるコンピュータリソース毎のレコードの内、前記第１コンピュータリソースのレコードのアクセス権限情報をチェックして、前記第１コンピュータリソースから前記第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アプリケーション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、前記リソース管理プログラムが、前記第２の操作要求をオペレーティングシステムに渡し、その結果を前記アプリケーションに返す処理工程と、
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、前記リソース管理プログラムが、前記第２の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、
前記拒否工程は、
前記アクセス権限がなく、かつ、前記アプリケーションが発行した前記第２の操作要求の結果としてエラーを返すことができる場合は、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アプリケーションに返すことで、前記第２の操作要求によって実行すべき処理を拒否し、
前記アクセス権限がなく、かつ、前記アプリケーションが発行した前記第２の操作要求の結果としてエラーを返すことができない場合は、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、前記第２の操作要求を、前記リソース管理プログラムが予め用意したダミーのリソースへの操作要求に代えて、前記第２の操作要求を処理することで、前記第２の操作要求によって実行すべき処理を拒否する
ことを特徴とする情報処理方法。
【請求項１７】
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、前記コンピュータリソースにアクセスするために指定されたアプリケーションからの操作要求を、前記アプリケーションと前記オペレーティングシステムとの間に介在するリソース管理プログラムが、前記アプリケーションが発行する前記コンピュータリソースに対する操作要求を監視して、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、
前記捕捉手段が捕捉した前記アプリケーションからの第１の操作要求によって前記アプリケーションが第１コンピュータリソースを保持する場合、前記リソース管理プログラムが、前記アプリケーションと前記第１コンピュータリソースとの対応関係を示す情報として、前記アプリケーションが前記第１コンピュータリソースを保持しているという情報を記憶媒体に登録する登録手段と、
前記アプリケーションと前記第１コンピュータリソースとの対応関係を示す情報が前記登録手段によって前記記憶媒体に既に登録されている状態で、前記捕捉手段が、前記第１コンピュータリソースに対する前記アプリケーションからの更なる第２の操作要求であって前記第１コンピュータリソースから第２コンピュータリソースへ出力する操作要求を捕捉した場合、前記リソース管理プログラムが、前記管理テーブルで管理されるコンピュータリソース毎のレコードの内、前記第１コンピュータリソースのレコードのアクセス権限情報をチェックして、前記第１コンピュータリソースから前記第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アプリケーション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、前記リソース管理プログラムが、前記第２の操作要求をオペレーティングシステムに渡し、その結果を前記アプリケーションに返す処理手段と、
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、前記リソース管理プログラムが、前記第２の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、
前記拒否手段は、
前記アクセス権限がなく、かつ、前記アプリケーションが発行した前記第２の操作要求の結果としてエラーを返すことができる場合は、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アプリケーションに返すことで、前記第２の操作要求によって実行すべき処理を拒否し、
前記アクセス権限がなく、かつ、前記アプリケーションが発行した前記第２の操作要求の結果としてエラーを返すことができない場合は、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、前記第２の操作要求を、前記リソース管理プログラムが予め用意したダミーのリソースへの操作要求に代えて、前記第２の操作要求を処理することで、前記第２の操作要求によって実行すべき処理を拒否する
ことを特徴とするプログラム。
【請求項１８】
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１７に記載のプログラム。
【請求項１９】
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１７に記載のプログラム。
【請求項２０】
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、画面キャプチャー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１９に記載のプログラム。
【請求項２１】

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１７に記載のプログラム。
【請求項２２】
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２１に記載のプログラム。
【請求項２３】
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２１または２２に記載のプログラム。
【請求項２４】
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２１または２２に記載のプログラム。
【請求項２５】
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、前記第２の操作要求として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、前記第２の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１７に記載のプログラム。
【請求項２６】
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、前記第２の操作要求として該アプリケーションが該ファイルを前記第２コンピュータリソースとしてのプリンタへ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、前記第２の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１７に記載のプログラム。
【請求項２７】
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、前記第２の操作要求として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、前記第２の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１７に記載のプログラム。
【請求項２８】
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、前記第２の操作要求として該アプリケーションが該ファイルを前記第２コンピュータリソースとしての外部装置へ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、前記第２の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１７に記載のプログラム。
【請求項２９】
ウイ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、前記第２の操作要求として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

たは該ウインドウのイメージ取得を拒否することで、前記第２の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１７に記載のプログラム。
【請求項３０】
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１７に記載のプログラム。
【請求項３１】
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３０に記載のプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
　本発明は、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方法及び装置、プログラムに関するものである。
【背景技術】
【０００２】
　従来において、パーソナルコンピュータ等のコンピュータにおけるファイルや記憶装置等のリソースにアプリケーションプログラムを介してユーザがアクセスする場合に、アクセス権限のないユーザに情報が解読または盗聴されるのを防ぐために、オペレーティングシステム（以下、ＯＳ）内にアクセス権限のチェック機能を設ける方法、あるいは専用のアクセス管理ツールを付加してアクセス権限のチェックを行なう方法が知られている。
【０００３】
　例えば、Ｗｉｎｄｏｗｓ（米国マイクロソフト社の登録商標）に代表される汎用のＯＳにおいては、ファイルの読み取り、書き込み、実行をアクセス権限のないユーザに対しては許可しない機能が備わっている。また、ファイルの削除、アクセス権限の変更、所有権の変更についての権限を設定可能にした汎用ＯＳもある。
【０００４】
　また、アクセス管理ツールとして、例えば、特許文献１に開示されているように、ファイルの参照と共に複写の可否を登録し、その可否によって参照、複写を制限するものが知られている。詳しくは、表示領域に読み出し制限の属性を付加し、表示画面のキャプチャーを防止するものが知られている。
【特許文献１】特開平７－８４８５２号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
　アクセス権限のないユーザに対して情報の持ち出しを全面的に禁止するためには、図９に示すように、メールへの添付、印刷、ファイル移動／ファイルコピー、クリップボードへのコピー、フロッピー（登録商標）ディスクへの別名保存、オブジェクトの貼り付け、画面のキャプチャーなどの機能を制限する必要がある。さらに、ネットワークを通じた情報の持ち出しを制限する必要がある。
【０００６】
　しかしながら、上記従来技術にあっては、ファイル移動／ファイルコピー及び画面のキャプチャー以外の操作（例えばクリップボードへのコピー）に対して制限することができないという問題がある。もしも、クリップボードへのコピーなどの操作を制限しようとする場合には、ＯＳまたはアプリケーション自体に変更を加えることが必要になり、汎用的な応用ができないという問題がある。

【０００７】
本発明の目的は、ＯＳやプロセス（ＯＳの元に稼動しているプログラムであり、アプリケーションやデーモンなど）を変更することなく、ファイルや画面以外のコンピュータリソースを含めてアクセス権限のないユーザに対するリソースの操作を制限し、しかも既存環境における禁止または制限事項を拡張することができるコンピュータリソースの制御が可能な情報処理装置及びその方法を提供することにある。
【課題を解決するための手段】
【０００８】
上記の目的を達成するための本発明による情報処理方法は以下の構成を備える。即ち、
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方法であって、
前記コンピュータリソースに対するプロセスまたは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捕捉工程と、
前記捕捉工程で捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する判定工程と、
前記判定工程の判定の結果、アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返す処理工程と、
前記判定工程の判定の結果、アクセス権限がなければ当該操作要求を拒否する拒否工程と
を備える。
【０００９】
また、好ましくは、前記捕捉工程は、更に、前記コンピュータリソースに対するプロセス及び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。
【００１０】
また、好ましくは、前記判定工程は、特定のコンピュータリソースを指定するリソース指定情報、アクセス権限が有効となる条件情報、既存環境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情報を含むアクセス権限管理テーブルを参照して、アクセス権限があるか否かを判定する。
【００１１】
また、好ましくは、前記判定工程は、コンピュータリソース内部に記述された、既存環境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情報を参照して、アクセス権限があるか否かを判定する。
【００１２】
また、好ましくは、前記判定工程は、アクセス権限が獲得できたか否かをもって、アクセス権限があるか否かを判定する。
【００１３】
また、好ましくは、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、画面キャプチャー権限、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。
【００１４】
また、好ましくは、前記拒否工程は、要求された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要求元プロセスに返す。
【００１５】
また、好ましくは、前記拒否工程は、要求されたコンピュータリソースにアクセスせずにアクセス成功の通知を要求元プロセスに返す。
【００１６】
また、好ましくは、ダミーのコンピュータリソースへの操作要求に変換してオペレーティングシステムに渡し、その結果を要求元プロセスに返す。
【００１７】

後述するプロテクション化電子情報とは、対象の電子情報に対する操作を制御する制限プログラムと、電子情報に対して印刷禁止や複製禁止といった制限する操作の内容を定義した制限属性を、対象の電子情報に付加し、実行可能形式にしたものである。

【００１８】

対象の電子情報に対して制限プログラムと制限属性を付加することで元の電子情報を変換する処理をプロテクション化と呼び、プロテクション化した電子情報をプロテクション化電子情報と呼ぶことにする。また、プロテクション化を実現するプログラムをプロテクション化プログラムと呼ぶことにする。

【００１９】

また、制限プログラムは、プロテクション化電子情報を元の電子情報として利用可能にするための展開ルーチン部と、電子情報へのアクセスを制御するための制限ルーチン部からなる。

【００２０】

さらに、制限属性は、電子情報に対して制限する操作と条件の組を１組以上保持し、必要に応じて、電子情報にアクセスするためのアプリケーション等のプログラムを特定する情報を保持する。

【００２１】

ここで、アプリケーションとは、電子情報にアクセスするために使用されるプログラムを指し、例えば、文書ファイルにアクセスするためのワープロソフトや、画像や動画を再生または編集するプログラムなどがそれに相当する。

【００２２】

アプリケーションはユーザが必ずしも操作するものとは限らず、一般的にＯＳもしくはプラットフォームの機能を利用して電子情報にアクセスするプログラムを、総称してここではアプリケーションと呼ぶことにする。

【００２３】

また、ＯＳ（オペレーティングシステム）にはマイクロソフト社のＷｉｎｄｏｗｓ（登録商標）やアップル社のＭａｃＯＳ、さらに一般的にＵＮＩＸ（登録商標）と呼ばれるものがあり、携帯端末機などでもＯＳは稼動している。さらに、ここでいうプラットフォームとは、ＯＳのことを指すこともあるが、より広く、Ｗｅｂ情報を閲覧するブラウザソフトなども、電子情報を扱う汎用的な環境を提供し、その上で実行可能な形式のプログラムを実行することができるコンピュータ上の基本プログラムという意味で、プラットフォームに含めることにする。

【発明の効果】

【００２４】

本発明によれば、基本的には、ファイル、ネットワーク、記憶装置、表示画面、外部装置等のＯＳが管理しているコンピュータリソースに対するプロセスまたはＯＳ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。次に、その捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する。判定の結果、アクセス権限があれば当該操作要求通りにＯＳに渡し、その結果を要求元プロセスに返し、アクセス権限がなければ当該操作要求を拒否するようにする。そのため、ＯＳやプロセス（ＯＳの元に稼動しているプログラムであり、アプリケーションやデーモンなど）を変更することなく、ファイルや画面以外のコンピュータリソースを含めてアクセス権限のないユーザに対するリソースの操作を制限することができる。

【００２５】

また、リソース管理プログラムを既存の環境に組み込むだけで、上述したような各種の不正アクセスを制限することができ、既存のアクセス権限の範囲を拡張することが可能になる。

【００２６】

また、リソース制御プログラムを既存の環境に組み込むだけで、各種の不正アクセスを制限することができ、従来のアクセス権限の範囲を拡張することが可能になる。

【００２７】
さらに、アクセス違反に対応する機能を有していないアプリケーションに対しても対応することができるなどの効果が得られる。
【００２８】
さらに、急速に進展しているｅビジネスに本発明による権限制限システムを応用すれば、不正アクセスの防止、各種有料コンテンツの配信による課金に効力を発揮する。急激な高齢化社会の到来と伴{共}に在宅就労も重要な課題になってきた。
【００２９】
本Ｈ．Ｈシステムの導入によって、安全に企業のドキュメント、データ、情報が家庭内で取り出せて、家庭内作業と成果をＷｅｂサイト、企業に送ることも可能になる。
【００３０】
また、電子情報に制限プログラム及び制限属性を付加することでプロテクション化し、プロテクション化電子情報を利用することで電子情報への操作を制限することができる。
【００３１】
また、制限プログラムは、電子情報を受け取る側のコンピュータ上で実行可能な形式にすることにより、受け取り側の既存の環境にあらかじめ制限プログラム等を組み込む必要がなく、上述したような各種の不正アクセスを制限することができ、既存のアクセス権限の範囲を拡張することが可能になる。
【００３２】
さらに、アクセス違反に対応する機能を有していないアプリケーションに対しても対応することができるなどの効果が得られる。
【００３３】
例えば、著作権が適用される場合など利用範囲を制限したい電子情報を提供するにあたって、プロテクション化した電子情報を提供することにより、受け取った側での利用範囲を制限できるといった効果が得られる。
【発明を実施するための最良の形態】
【００３４】
＜第１実施形態＞
以下、本発明の実施の形態を図面により詳細に説明する。
【００３５】
図１Ａ、図１Ｂは本発明を実施する環境の一実施の形態を示すハードウェア構成図である。
【００３６】
図１Ａに示す構成は、スタンドアロン構成におけるコンピュータ１０１のハード構成を示すものであり、ハードディスクドライブ（ＨＤＤ）１０１１を備えたパーソナルコンピュータ（ＰＣ）１０１２、ディスプレイ１０１３、プリンタ１０１４、外部にリソースデータを出力することが可能な外部装置１０１５で構成されている。
【００３７】
パーソナルコンピュータ１０１２には、汎用のＯＳとアプリケーションが組み込まれており、さらに本発明に係るリソース管理プログラムが組み込まれている。
【００３８】
図１Ｂは、ネットワーク１０２を利用する場合の構成を示すものであり、図１Ａに示したのと同様な構成のコンピュータ１０１ａ～１０１ｃがネットワーク１０２を介して相互に接続されている。
【００３９】
このような構成において、一般的に、アプリケーションがＯＳの管理するリソースにアクセスするには、ＯＳが提供するＡＰＩ（Ａｐｐｌｉｃａｔｉｏｎ Ｐｒｏｇｒａｍ Ｉｎｔｅｒｆａｃｅ）を利用する。このＡＰＩの利用方法はＯＳにより確定しており、ＡＰＩを利用する実行コード部を判別することができる。本発明では、リソースへのアクセスに必要なすべてのＡＰＩを監視する監視ルーチンを設け、アプリケーションがＡＰＩを利用

する前に、その実行コード部を変更するか、ＡＰＩ処理の入り口を監視ルーチンと置き換えることで、ＡＰＩ利用時に監視ルーチンが利用されるようにする。監視ルーチンは、アプリケーションが求めるＡＰＩを処理するか、もしくはＡＰＩの処理をせずに不正命令としてアプリケーションに結果を返す。本発明のリソース管理プログラムによって拡張したアクセス権限の管理は、ＯＳの管理とは別に本プログラムが管理し、アクセス権限の種類別に監視ルーチンを設ける。この方法により、リソースを不正に利用するアプリケーションから、そのアクセスを制限する。

【００４０】

図２は、本発明に係るリソース管理プログラム２０３の構成及びＡＰＩ監視／制御の概念を示す図であり、リソース管理プログラム２０３はＡＰＩ監視コントローラ（ＡＰＩ監視ＣＴＲＬ）２０３１、ＡＰＬ（アプリケーション）監視コントローラ（ＡＰＬ監視ＣＴＲＬ）２０３２、アクセス制御コントローラ（アクセス制御ＣＴＲＬ）２０３３、ＯＳ監視コントローラ（ＯＳ監視ＣＴＲＬ）２０３４から構成されている。

このリソース管理プログラム２０３は、リソースアクセス要求を出すアプリケーション２０２１や画面キャプチャーなどのＯＳ機能操作２０２２を備える一般的なアプリケーションからなるユーザ環境２０２と汎用ＯＳ２０１との間に位置し、汎用ＯＳ２０１およびユーザ環境２０２が提供するリソースに対する要求を監視するようになっている。

【００４１】

なお、汎用ＯＳ２０１は、ＯＳが管理するリソース２０１１と、ＯＳがアプリケーション２０２１に提供しているＡＰＩ群２０１２を備える。

【００４２】

本発明に係るリソース管理プログラム２０３におけるＡＰＩ監視ＣＴＲＬ２０３１は、アクセス制御を行なうのに必要な全てのＡＰＩを監視するモジュールである。また、ＡＰＬ監視ＣＴＲＬ２０３２は、アプリケーション２０２１が保持しているリソースを記憶するモジュールである。アクセス制御ＣＴＲＬ２０３３はリソース２０１１のアクセスが許可されているかを判断するモジュールであり、アクセス権限管理テーブル２０３５を備える。また、ＯＳ監視ＣＴＲＬ２０３４は、汎用ＯＳ２０１の機能によってリソースへアクセスする操作を監視するモジュールである。

【００４３】

アクセス権限管理テーブル２０３５は、図３に示すように、リソース指定情報２０３５１、条件２０３５２、ｎ個のアクセス権限情報２０３５３～２０３５ｎをリソース毎に登録可能に構成されている。

【００４４】

リソース指定情報２０３５１は、汎用ＯＳ２０１が管理しているリソース２０１１のうち、特定のものを指定するための情報であり、例えば、ファイルの場合はファイル名やファイルＩＤなどの情報が登録される。通信データの場合は、ホスト名、ポート番号、ＩＰアドレスなどが登録され、メモリの場合は、そのオブジェクトを示すオブジェクト名、アドレスなどが登録される。また、外部装置の場合は、そのデバイスドライバを示すデバイス名などが登録される。

【００４５】

条件２０３５２は、アクセス権限が有効となる条件またはその組み合わせをしめすものであり、例えばユーザ名／ＩＤ、グループ名／ＩＤ、時刻、使用アプリケーションなどが登録される。

【００４６】

アクセス権限情報２０３５３～２０３５ｎは、既存環境で定義されていない拡張したアクセス権限のうち、指定したリソースに付加した権限を示すものであり、例えば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（Ｗｉｎｄｏｗｓではクリップボードなど）、画面キャプチャー権限、使用アプリケーションの限定（特定アプリケーション以外での使用禁止やメール添付の禁止）などが登録される。

【００４７】

なお、一般的に、リソースへのアクセスは複数のＡＰＩによって行われることがあり、その場合はリソース指定情報はＯＳが管理するＩＤ（ハンドルなど）に変換されることがある。その場合、リソース管理プログラム２０３の内部においては、リソース指定情報とそのＩＤは同一視するようにしている。

【００４８】

このような構成に係るリソース管理プログラム２０３の処理について、図２の（１）～（９）（図中の丸数字１～９に対応）で示す情報伝達手順に従って説明する。

【００４９】

（１）アプリケーション２０２１が発行したＡＰＩによってリソースへのアクセス要求があれば、ＡＰＩ監視ＣＴＲＬ２０３１がその要求を捕捉し、アクセス制御ＣＴＲＬ２０３３に伝える。

【００５０】

（２）アクセス制御ＣＴＲＬ２０３３は、アクセス権限チェックを行なう際、必要に応じて、アプリケーション２０２１が保持しているリソースの情報をＡＰＬ監視ＣＴＲＬ２０３２から取得する。

【００５１】

（３）アクセスを拒否する条件として２通りあるが、第１の条件Ａ（アクセス拒否Ａ）では、上記（１）のアクセス要求に対して、アクセス権限管理テーブル２０３５を参照してそのリソースへのアクセス権限チェックを行なう。チェックの結果、権限がない場合、アプリケーション２０２１が発行したＡＰＩの処理を行なわずに、結果としてアクセス違反のエラーを返す。

【００５２】

（４）第２の条件Ｂ（アクセス拒否Ｂ）では、（１）のアクセス要求に対して、アクセス権限管理テーブル２０３５を参照してそのリソースへのアクセス権限チェックを行なう。チェックの結果、権限がなく、かつ、アプリケーション２０２１が発行したＡＰＩ{処理}の結果としてエラーを返すことができない場合、アプリケーション２０２１が要求したリソースへの処理を行なわずに、リソース管理プログラム２０３が予め用意したダミーのリソースへのアクセス要求に代えて、ＡＰＩの処理を行なう。

【００５３】

その結果、アプリケーション２０２１は要求に成功したように動作するが、実際には要求したリソースにアクセスできない。

【００５４】

（５）アクセス要求（１）に対してアクセス権限チェックを行った結果、権限がある場合、ＡＰＩ監視ＣＴＲＬ２０３１がそのアクセス要求を捕捉し、アプリケーション２０２１が発行したＡＰＩの処理をそのまま汎用ＯＳ２０１に伝え、その結果をアプリケーション２０２１に返す。

【００５５】

（６）上記（５）の処理によって、ＡＰＩが成功し、かつ、そのＡＰＩによってアプリケーション２０２１がリソースを保持する場合は、ＡＰＬ監視ＣＴＲＬ２０３２に伝える。ＡＰＬ監視ＣＴＲＬ２０３２はアプリケーション２０２１と保持しているリソースの対応を登録する。

【００５６】

アプリケーション２０２１がリソースの解放要求ＡＰＩを発行し、かつそのＡＰＩが成功した場合も、ＡＰＬ監視ＣＴＲＬ２０３２に伝える。ＡＰＬ監視ＣＴＲＬ２０３２はアプリケーション２０２１と保持していたリソースの対応を抹消する。

【００５７】

（７）ＯＳ標準機能の操作によって、リソースへのアクセス要求があれば、ＯＳ監視ＣＴＲＬ２０３４がそのアクセス要求を捕捉し、アクセス制御ＣＴＲＬ２０３３に伝える。

【００５８】

（８）アクセス要求（７）に対して、アクセス権限管理テーブル２０３５を参照してそ

のリソースへのアクセス権限チェックを行なう。チェックの結果、権限がない場合、（７）の操作を無視する。

【００５９】

（９）アクセス要求（７）に対して、アクセス権限管理テーブル２０３５を参照してそのリソースへのアクセス権限チェックを行なう。チェックの結果、権限がある場合、（７）の操作を汎用ＯＳ２０１に伝える。

【００６０】

図４は、目的とするリソースに対するアクセス権限がある場合に、そのリソースを解放するまでのアプリケーション２０２１、リソース管理プログラム２０３、汎用ＯＳ２０１のやり取りを示したＡＰＩの監視及び制御の第１の基本型（１）のシーケンス図である。

【００６１】

この第１の基本型（１）では、アプリケーション２０２１が発行したＡＰＩによって目的のリソースへのアクセス要求があった場合（ステップ４０１）、リソース管理プログラム２０３はアプリケーション２０２１がそのリソースへのアクセス権限があるかをチェックする（ステップ４０２）。チェックの結果、アクセス権限がある場合（ステップ４０３）、汎用ＯＳ２０１にアプリケーション２０２１が発行したＡＰＩをそのまま伝える。汎用ＯＳ２０１は、ＯＳ本来のＡＰＩ処理を行なう（ステップ４０４）。

【００６２】

リソース管理プログラム２０３は、ＡＰＩ処理が成功した場合、アプリケーション２０２１がそのリソースを保持しているという情報を登録する（ステップ４０５）。そして、汎用ＯＳ２０１からのＡＰＩ結果をそのままアプリケーション２０２１に返す（ステップ４０６）。これにより、リソースへのアクセス完了となる（ステップ４０７）。

【００６３】

この後、アプリケーション２０２１から保持しているリソースの解放要求が発行された場合（ステップ４０８）、リソース管理プログラム２０３はその解放要求を汎用ＯＳ２０１に伝える。汎用ＯＳ２０１は、ＯＳ本来のＡＰＩ処理を行なう（ステップ４０９）。リソース管理プログラム２０３は、ＡＰＩ処理が成功した場合、アプリケーション２０２１がそのリソースを保持しているという情報を解除する（ステップ４１０）。そして、汎用ＯＳ２０１からのＡＰＩ結果をそのままアプリケーション２０２１へ返す（ステップ４１１）。これにより、保持しているリソースの解放完了となる（ステップ４１２）。

【００６４】

図５は、目的とするリソースに対するアクセス権限がなかった場合に、そのアクセスが拒否されるまでのアプリケーション２０２１、リソース管理プログラム２０３、汎用ＯＳ２０１のやり取りを示したＡＰＩの監視及び制御の第２の基本型（２）のシーケンス図である。

【００６５】

この第２の基本型（２）では、アプリケーション２０２１が発行したＡＰＩによって目的のリソースへのアクセス要求があった場合（ステップ５０１）、リソース管理プログラム２０３はアプリケーション２０２１がそのリソースへのアクセス権限があるかをチェックする（ステップ５０２）。チェックの結果、アクセス権限がなかった場合（ステップ５０３）、アクセス違反エラーをアプリケーション２０２１に返す（ステップ５０４）。これにより、リソースへのアクセス処理終了となる（ステップ５０５）。

【００６６】

また、アクセス違反エラーに対応していないアプリケーション２０２１が発行したＡＰＩによって目的のリソースへのアクセス要求があった場合（ステップ５０６）、リソース管理プログラム２０３はアプリケーション２０２１がそのリソースへのアクセス権限があるかをチェックする（ステップ５０７）。チェックの結果、アクセス権限がなく、かつ、アプリケーション２０２１がアクセス違反エラーに対応していない場合（ステップ５０８）、リソース管理プログラム２０３が予め用意したダミーのリソースへのアクセス要求に置き換え、汎用ＯＳ２０１に渡す（ステップ５０９）。

【００６７】
汎用ＯＳ２０１は、ＯＳ本来のＡＰＩ処理を行なう（ステップ５１０）。リソース管理プログラム２０３は、汎用ＯＳ２０１からのＡＰＩ処理結果をそのままアプリケーション２０２１へ返す（ステップ５１１）。この結果、目的のリソースへのアクセス処理終了となるが、ダミーリソースのため、実質的には何も行われない（ステップ５１２）。
【００６８】
本発明は、以上のようにしてアクセス権限のないリソースへのアクセスを制限するものであるが、汎用のＯＳであるＷｉｎｄｏｗｓとＵＮＩＸの場合のＡＰＩを例に挙げて説明する。
【００６９】
まず、ファイルへの複製処理を禁止する例について説明する。
【００７０】
ファイルへの複製処理については、従来、読み込み許可ファイルはファイルのコピーが可能であり、その結果オリジナの複製が複数存在したり、別媒体に転写して持ち出すことが可能であった。本発明では、ファイルコピーを実現するＡＰＩを監視／制御することにより、権限のないファイルのコピーを禁止する。その場合に、Ｗｉｎｄｏｗｓにおいて監視／制御するＡＰＩとして次のものがある。なお、以下で例示するＡＰＩの機能については、各種の文献で公開されているので、その詳細な説明は省略する。
【００７１】
（１）ファイルオープン／作成ＡＰＩ
ＣｒｅａｔｅＦｉｌｅＡ
ＣｒｅａｔｅＦｉｌｅＷ
ＯｐｅｎＦｉｌｅ
＿ｌｏｐｅｎ
＿ｌｃｒｅａｔ
ＧｅｔＯｐｅｎＦｉｌｅＮａｍｅＡ
ＧｅｔＯｐｅｎＦｉｌｅＮａｍｅＷ
ＧｅｔＳａｖｅＦｉｌｅＮａｍｅＡ
ＧｅｔＳａｖｅＦｉｌｅＮａｍｅＷ
（２）ファイルクローズＡＰＩ
ＣｌｏｓｅＨａｎｄｌｅ
＿ｌｃｌｏｓｅ
（３）ファイルコピー／移動ＡＰＩ
ＣｏｐｙＦｉｌｅＡ
ＣｏｐｙＦｉｌｅＷ
ＭｏｖｅＦｉｌｅＡ
ＭｏｖｅＦｉｌｅＷ
ＭｏｖｅＦｉｌｅＥｘＡ
ＭｏｖｅＦｉｌｅＥｘＷ
ＤｅｌｅｔｅＦｉｌｅＡ
ＤｅｌｅｔｅＦｉｌｅＷ
ＤｒａｇＱｕｅｒｙＦｉｌｅＡ
ＤｒａｇＱｕｅｒｙＦｉｌｅＷ
ＵＮＩＸの場合、監視／制御するＡＰＩとしては次のものがある。
【００７２】
（１）ファイルオープン／作成ＡＰＩ
ｏｐｅｎ
ｃｒｅａｔ
（２）ファイルクローズＡＰＩ
ｃｌｏｓｅ

（３）ファイルコピー／移動ＡＰＩ
ｒｅｎａｍｅ
このようなＡＰＩの監視によってファイルへの複製処理を禁止する場合、具体的な方法として３つの方法がある。
【００７３】
＜方法１＞（ファイルオープン中に複製処理を行なうことが判明している場合）
アプリケーションが、複製権限のないファイルをオープンし保持している間（ファイルをクローズするまでの期間）、そのアプリケーションが別のファイルを作成することを拒否する。
【００７４】
＜方法２＞（ファイルクローズ後に複製処理を行なう可能性はあるが、複数ファイルを扱わないことが判明している場合）
アプリケーションが、複製権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するか、複製権限のあるファイルをオープンするまで、そのアプリケーションが別のファイルを作成することを拒否する。
【００７５】
＜方法３＞（ファイルクローズ後に複製処理を行なう可能性があり、複数ファイルを扱う可能性がある場合）
アプリケーションが、複製権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するまで、そのアプリケーションが別のファイルを作成することを拒否する。
【００７６】
なお、いずれの方法であっても、別に作成されるファイルによって複製が残ることがないと判明している場合（一時ファイルなどの作成）は拒否しない。
【００７７】
次に、特定ファイルまたは全ての印刷を禁止する例について説明する。
【００７８】
従来、印刷機能を実装したアプリケーションによって、ファイルの内容を印刷し、外部に持ち出すことは可能であった。本発明では、印刷を実現するＡＰＩを監視／制御することにより、印刷権限のないファイルの印刷を禁止する。また、ＦＡＸなどその他の外部装置についても、それぞれの外部装置の選択や制御を実現するＡＰＩを監視／制御することにより、同様に禁止する。その場合に、Ｗｉｎｄｏｗｓ及びＵＮＩＸにおいて監視／制御するＡＰＩとして次のものがある。
【００７９】
Ｗｉｎｄｏｗｓの場合
（１）デバイスオープンＡＰＩ
ＣｒｅａｔｅＤＣＡ
ＣｒｅａｔｅＤＣＷ
（２）デバイスクローズＡＰＩ
ＲｅｌｅａｓｅＤＣ
ＣｌｏｓｅＰｒｉｎｔｅｒ
（３）プリンタ選択／ＡＰＬ処理ＡＰＩ
ＯｐｅｎＰｒｉｎｔｅｒＡ
ＯｐｅｎＰｒｉｎｔｅｒＷ
ＧｅｔＰｒｉｎｔｅｒＡ
ＧｅｔＰｒｉｎｔｅｒＷ
ＳｅｔＰｒｉｎｔｅｒＡ
ＳｅｔＰｒｉｎｔｅｒＷ
ＳｅｎｄＭｅｓｓａｇｅＡ
ＳｅｎｄＭｅｓｓａｇｅＷ

ＰｏｓｔＭｅｓｓａｇｅＡ
ＰｏｓｔＭｅｓｓａｇｅＷ
ＵＮＩＸの場合
（１）デバイスオープンＡＰＩ
ｏｐｅｎ
（２）デバイス制御ＡＰＩ
ｉｏｃｔｒｌ
（３）デバイスクローズＡＰＩ
ｃｌｏｓｅ
このようなＡＰＩの監視によって印刷処理を禁止する場合、具体的な方法として３つの方法がある。

【００８０】
＜方法１＞（ファイルオープン中に印刷処理可能なことが判明している場合）
アプリケーションが、印刷権限のないファイルをオープンし保持している間（ファイルをクローズするまでの期間）、そのアプリケーションのプリンタ選択、およびプリンタデバイスのオープンを拒否する。

【００８１】
＜方法２＞（ファイルクローズ後に印刷処理を行なう可能性はあるが、複数ファイルを扱わないことが判明している場合）
アプリケーションが、印刷権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するか、印刷権限のあるファイルをオープンするまで、そのアプリケーションのプリンタ選択、およびプリンタデバイスのオープンを拒否する。

【００８２】
＜方法３＞（ファイルクローズ後に印刷処理を行なう可能性があり、複数ファイルを扱う可能性がある場合）
アプリケーションが、印刷権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するまで、そのアプリケーションのプリンタ選択、およびプリンタデバイスのオープンを拒否する。

【００８３】
次に、外部装置の利用を禁止する例について説明する。

【００８４】
従来、ＯＳに装備されている機能や外部装置そのものに権限を付加することは、一般的にはできなかった。本発明では、監視／制御すべきＡＰＩを限定できる機能の指定や、外部装置利用の指定をすることにより、その利用を禁止する。その場合に、Ｗｉｎｄｏｗｓ及びＵＮＩＸにおいて監視／制御するＡＰＩとして次のものがある。

【００８５】
Ｗｉｎｄｏｗｓの場合
（１）デバイスオープンＡＰＩ
ＣｒｅａｔｅＦｉｌｅＡ
ＣｒｅａｔｅＦｉｌｅＷ
ＯｐｅｎＦｉｌｅ
＿ｌｏｐｅｎ
＿ｌｃｒｅａｔ
（２）デバイスクローズＡＰＩ
ＣｌｏｓｅＨａｎｄｌｅ
＿ｌｃｌｏｓｅ
ＵＮＩＸの場合
（１）デバイスオープンＡＰＩ
ｏｐｅｎ
（２）デバイス制御ＡＰＩ

ｉｏｃｔｒｌ
（３）デバイスクローズＡＰＩ
ｃｌｏｓｅ
例えば、このようなＡＰＩの監視によって印刷を禁止する場合、具体的な方法として次の方法がある。
【００８６】
＜方法＞
アクセス権限管理テーブル２０３５にて、特定の条件のもとに特定外部装置の使用を禁止されている場合、その外部装置の利用を以下の方法で拒否する。その外部装置のデバイス名をもってデバイスオープンＡＰＩ要求があった場合、アクセス禁止エラー、もしくは外部装置が存在しないというエラーを返すことで要求を拒否する。
【００８７】
次に、ファイル内の一部のデータまたは全ての複写を禁止する例について説明する。
【００８８】
従来、アプリケーションによってファイルを画面表示した結果、その内容のすべてまたは一部をＯＳの機能によって複写することまたはオブジェクトという単位で別ファイルに埋め込むことが可能であった。
【００８９】
本発明では、転写や埋め込み機能を実現するＡＰＩ（クリップボードのＡＰＩ、ＯＬＥのＡＰＩなど）を監視／制御することで、複写権限のないデータの流用を禁止する。
【００９０】
その場合に、Ｗｉｎｄｏｗｓにおいて監視／制御するＡＰＩとして次のものがある。
【００９１】
Ｗｉｎｄｏｗｓの場合
（１）複写／埋め込みＡＰＩ
ＯｐｅｎＣｌｉｐｂｏａｒｄ
ＳｅｔＣｌｉｐｂｏａｒｄＤａｔａ
ＧｅｔＣｌｉｐｂｏａｒｄＤａｔａ
ＧｅｔＯｐｅｎＣｌｉｐｂｏａｒｄＷｉｎｄｏｗ
ＯｌｅＣｒｅａｔｅ
ＯｌｅＣｒｅａｔｅＥｘ
ＯｌｅＣｒｅａｔｅＦｒｏｍＦｉｌｅ
ＯｌｅＣｒｅａｔｅＦｒｏｍＦｉｌｅＥｘ
ＯｌｅＣｒｅａｔｅＦｒｏｍＤａｔａ
ＯｌｅＣｒｅａｔｅＦｒｏｍＤａｔａＥｘ
ＯｌｅＣｒｅａｔｅＬｉｎｋ
ＯｌｅＣｒｅａｔｅＬｉｎｋＥｘ
ＯｌｅＣｒｅａｔｅＬｉｎｋＦｒｏｍＤａｔａ
ＯｌｅＣｒｅａｔｅＬｉｎｋＦｒｏｍＤａｔａＥｘ
ＯｌｅＣｒｅａｔｅＬｉｎｋＴｏＦｉｌｅ
ＯｌｅＣｒｅａｔｅＬｉｎｋＴｏＦｉｌｅＥｘ
ＣｌｏｓｅＣｌｉｐｂｏａｒｄ
このようなＡＰＩの監視によって複写処理を禁止する場合、具体的な方法として４つの方法がある。
【００９２】
＜方法１＞（ファイルオープン中に複写処理可能なことが判明している場合）
アプリケーションが、複写権限のないファイルをオープンし保持している間（ファイルをクローズするまでの期間）、そのアプリケーションが複写／埋め込みオブジェクトの形式でデータを登録する際に、拒否もしくは空データを登録する。
【００９３】

＜方法２＞（ファイルクローズ後に複写処理を行なう可能性はあるが、複数ファイルを扱わないことが判明している場合）
アプリケーションが、複写権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するか、複写権限のあるファイルをオープンするまで、そのアプリケーションが複写／埋め込みオブジェクトの形式でデータを登録する際に、拒否もしくは空データを登録する。

【００９４】
＜方法３＞（ファイルクローズ後に複写処理を行なう可能性があり、複数ファイルを扱う可能性がある場合）
アプリケーションが、複写権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するまで、そのアプリケーションが複写／埋め込みオブジェクトの形式でデータを登録する際に、拒否もしくは空データを登録する。

【００９５】
＜方法４＞（複写権限のないファイルを埋め込みオブジェクトとして取り込む場合）
複写権限のないファイルを取り込む処理を行なう際に、オブジェクトの登録もしくはそのオブジェクトの取得ＡＰＩにおいて、アクセス違反のエラーを返すか、空データを登録あるいは取得することで、処理要求を拒否する。

【００９６】
次に、ネットワークを介してファイルが外部へ流出することを禁止する例について説明する。

【００９７】
従来、ファイルコピー以外に、ＦＴＰプログラムのように、ネットワークを介してファイルを外部へ転送することは可能であった。本発明では、ネットワークリソースにアクセスするＡＰＩを監視／制御することで、外部出力権限のないファイルを使用中のアプリケーションから、外部へのファイル内容の出力を禁止する。その場合に、Ｗｉｎｄｏｗｓ及びＵＮＩＸにおいて監視／制御するＡＰＩとして次のものがある。

【００９８】
Ｗｉｎｄｏｗｓの場合
ＷＳＡＳｔａｒｔｕｐ
ａｃｃｅｐｔ
ｂｉｎｄ
ｃｏｎｎｅｃｔ
ｇｅｔｈｏｓｔｂｙｎａｍｅ
ｇｅｔｈｏｓｔｂｙａｄｄｒ
ｇｅｔｐｒｏｔｏｂｙｎａｍｅ
ｇｅｔｐｒｏｔｏｂｙｎｕｍｂｅｒ
ｇｅｔｓｅｒｖｂｙｎａｍｅ
ｇｅｔｓｅｒｖｂｙｐｏｒｔ
ｇｅｔｐｅｅｒｎａｍｅ
ｇｅｔｓｏｃｋｎａｍｅ
ｇｅｔｈｏｓｔｎａｍｅ
ｇｅｔｓｏｃｋｏｐｔ
ｓｅｔｓｏｃｋｏｐｔ
ｒｅｃｖ
ｒｅｃｖｆｒｏｍ
ｓｏｃｋｅｔ
ｓｅｌｅｃｔ
ｓｅｎｄ
ｓｅｎｄｔｏ
ＷＳＡＳｅｎｄ

ＷＳＡＳｅｎｄＴｏ
ＷＳＡＡｓｙｎｃＳｅｌｅｃｔ
ＷＳＡＡｓｙｎｃＧｅｔＨｏｓｔＢｙＡｄｄｒ
ＷＳＡＡｓｙｎｃＧｅｔＨｏｓｔＢｙＮａｍｅ
ＷＳＡＡｓｙｎｃＧｅｔＰｒｏｔｏＢｙＮｕｍｂｅｒ
ＷＳＡＡｓｙｎｃＧｅｔＰｒｏｔｏＢｙＮａｍｅ
ＷＳＡＡｓｙｎｃＧｅｔＳｅｒｖＢｙＰｏｒｔ
ＷＳＡＡｓｙｎｃＧｅｔＳｅｒｖＢｙＮａｍｅ
ＷＳＡＣａｎｃｅｌＡｓｙｎｃＲｅｑｕｅｓｔ
ＷＳＡＳｅｔＢｌｏｃｋｉｎｇＨｏｏｋ
ＷＳＡＵｎｈｏｏｋＢｌｏｃｋｉｎｇＨｏｏｋ
ＷＳＡＣｌｅａｎｕｐ
ｃｌｏｓｅｓｏｃｋｅｔ
ｓｈｕｔｄｏｗｎ

ＵＮＩＸの場合

ａｃｃｅｐｔ
ｂｉｎｄ
ｃｏｎｎｅｃｔ
ｇｅｔｈｏｓｔｂｙｎａｍｅ
ｇｅｔｈｏｓｔｂｙａｄｄｒ
ｇｅｔｐｒｏｔｏｂｙｎａｍｅ
ｇｅｔｐｒｏｔｏｂｙｎｕｍｂｅｒ
ｇｅｔｓｅｒｖｂｙｎａｍｅ
ｇｅｔｓｅｒｖｂｙｐｏｒｔ
ｇｅｔｐｅｅｒｎａｍｅ
ｇｅｔｓｏｃｋｎａｍｅ
ｇｅｔｈｏｓｔｎａｍｅ
ｇｅｔｓｏｃｋｏｐｔ
ｓｅｔｓｏｃｋｏｐｔ
ｒｅｃｖ
ｒｅｃｖｆｒｏｍ
ｓｏｃｋｅｔ
ｓｅｌｅｃｔ
ｓｅｎｄ
ｓｅｎｄｔｏ
ｃｌｏｓｅｓｏｃｋｅｔ
ｓｈｕｔｄｏｗｎ

このようなＡＰＩの監視によって使用中のアプリケーションから外部へのデータ出力を禁止する場合、具体的な方法として３つの方法がある。

【００９９】

＜方法１＞（ファイルオープン中に出力処理可能なことが判明している場合）

アプリケーションが、外部出力権限のないファイルをオープンし保持している間（ファイルをクローズするまでの期間）、そのアプリケーションからの接続要求や送信要求を、アクセス違反もしくはタイムアウトなどのエラーで拒否する。

【０１００】

＜方法２＞（ファイルクローズ後に出力処理を行なう可能性はあるが、複数ファイルを扱わないことが判明している場合）

アプリケーションが、出力権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するか、出力権限のあるファイルをオープンするまで、そのアプリケーションの接続要求や送信要求を、アクセス違反もしくはタイムアウトなどのエラーで拒

否する。
【０１０１】
＜方法３＞（ファイルクローズ後に出力処理を行なう可能性があり、複数ファイルを扱う可能性がある場合）
アプリケーションが、出力権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するまで、そのアプリケーションの接続要求や送信要求を、アクセス違反もしくはタイムアウトなどのエラーで拒否する。
【０１０２】
ただし、その通信によってデータ出力されないことが判明している場合は、拒否しない。
【０１０３】
次に、ファイルの内容のイメージを取得することを禁止する例について説明する。
【０１０４】
ＯＳの機能として画面全体や一部、またはウインドウ単位の画面をイメージデータとして取得することが、一般的には可能であり、従来、そのイメージデータを流用、持ち出しすることができた。本発明では、画面内のイメージデータ取得ＡＰＩを監視／制御することで、イメージデータ取得を禁止する。
【０１０５】
その場合に、Ｗｉｎｄｏｗｓにおいて監視／制御するＡＰＩとして次のものがある。
【０１０６】
（１）デバイスオープンＡＰＩ
ＧｅｔＷｉｎｄｏｗＤＣ
ＷｉｎｄｏｗＦｒｏｍＤＣ
ＧｅｔＤＣ
ＧｅｔＤＣＥＸ
ＧｅｔＤｅｓｋｔｏｐＷｉｎｄｏｗ
ＧｅｔＤｅｖｉｃｅＣａｐｓ
ＣｒｅａｔｅＤＣＡ
ＣｒｅａｔｅＤＣＷ
（２）イメージ取得ＡＰＩ
ＢｉｔＢｌｔ
ＳｔｒｅｔｃｈＢｌｔ
（３）デバイスクローズＡＰＩ
ＤｅｌｅｔｅＤＣ
ＲｅｌｅａｓｅＤＣ
このようなＡＰＩの監視によって画面イメージを取得することを禁止する場合、具体的な方法として３つの方法がある。
【０１０７】
＜方法１＞（画面全体のキャプチャーを拒否する場合）
現在画面上に表示されているウイ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保持している場合、画面全体のイメージ取得を拒否する。画面全体のイメージ取得処理の有無は、画面全体を管理しているウインドウ（Ｗｉｎｄｏｗｓの場合はデスクトップウインドウ）の状態を監視することで行なう。ＷｉｎｄｏｗｓにおけるＤｉｒｅｃｔＤｒａｗなど、画面全体のイメージを取得するＡＰＩが存在すれば、同様に拒否する。
【０１０８】
さらに、ディスプレイデバイスからＶＲＡＭイメージを取得するアプリケーションに対しては、それを拒否する。
【０１０９】
＜方法２＞（ウインドウの画面イメージ取得を拒否する場合）

現在画面上に表示されているウイ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保持している場合、そのウインドウのイメージ取得を拒否する。ウインドウが画面上に表示されているかは、ウインドウの状態を監視することで行なう。

【０１１０】

また、画面イメージ取得の拒否は、そのウインドウに関連付けられたデバイスコンテキストからのイメージコピーを拒否することで行なう。

【０１１１】

＜方法３＞（画面の一部のイメージ取得を拒否する場合）

画面イメージを取得する領域が判断できる場合は、＜方法１＞における条件を、取得領域が対象となるウインドウと重なる時とし、以降は＜方法１＞と同様にして画面の一部のイメージ取得を拒否する。また、領域が判断できない時は、＜方法１＞と同様にして画面全体のイメージ取得を拒否する。

【０１１２】

次に、ファイル種別毎に利用アプリケーションを限定する例について説明する。

【０１１３】

従来、アプリケーション利用に制限がないため、参照以外の目的でファイルにアクセス可能であった。本発明では、ファイルごとに利用アプリケーションを限定できる。その場合に、Ｗｉｎｄｏｗｓにおいて監視／制御するＡＰＩとして次のものがある。

【０１１４】

（１）ファイルオープンＡＰＩ
　　ＣｒｅａｔｅＦｉｌｅＡ
　　ＣｒｅａｔｅＦｉｌｅＷ
　　ＯｐｅｎＦｉｌｅ
　　＿ｌｏｐｅｎ
　　＿ｌｃｒｅａｔ
（２）ファイルクローズＡＰＩ
　　ＣｌｏｓｅＨａｎｄｌｅ
　　＿ｌｃｌｏｓｅ
（３）プロセス管理ＡＰＩ
　　ＷｉｎＥｘｅｃ
　　ＣｒｅａｔｅＰｒｏｃｅｓｓＡ
　　ＣｒｅａｔｅＰｒｏｃｅｓｓＷ
　　ＥｘｉｔＰｒｏｃｅｓｓ
ＵＮＩＸの場合
（１）ファイルオープンＡＰＩ
　　ｏｐｅｎ
（２）ファイルクローズＡＰＩ
　　ｃｌｏｓｅ

このようなＡＰＩの監視によって利用アプリケーションを限定する場合、具体的な方法として次の方法がある。

＜方法＞

アプリケーションがファイルをオープンする際、そのファイルの権限をチェックし、許可されたアプリケーションでない場合はアクセス違反エラーを返すことで、オープン要求を拒否する。

【０１１５】

次に、ＯＳに装備されている特定の機能の利用を禁止する例について説明する。

【０１１６】

従来、ＯＳに装備されている機能に権限を付加することは、一般的にはできなかった。本発明では、監視／制御すべきＡＰＩを限定する機能を指定することで、その利用を禁止

することができる。例えば、ファイルのタイムスタンプやシステム日時の変更を禁止するなどである。その場合に、Ｗｉｎｄｏｗｓにおいて監視／制御するＡＰＩとして次のものがある。

【０１１７】

（１）ファイルのタイムスタンプ変更ＡＰＩ

ＳｅｔＦｉｌｅＴｉｍｅ

（２）システム日時の変更ＡＰＩ

ＳｅｔＳｙｓｔｅｍＴｉｍｅ

ＳｅｔＳｙｓｔｅｍＴｉｍｅＡｄｊｕｓｔｍｅｎｔ

このようなＡＰＩの監視によってＯＳにおける特定の機能の利用を禁止する場合、具体的な方法として次の方法がある。

【０１１８】

＜方法＞

特定の条件下で禁止されているＡＰＩが発行された際に、アクセス違反エラーを返すか、実際の処理を行なわずにダミー処理を施し、正常リターンすることで、禁止されているＡＰＩ（ＯＳ機能）を拒否する。

【０１１９】

次に、プロセス内メモリの参照または変更を禁止する例について説明する。

【０１２０】

従来、アプリケーションが明示的に拒否しない限り、プロセス内メモリの参照／変更を禁止することができなかった。本発明では、プロセス内メモリの参照／変更ＡＰＩを監視／制御することで、他のアプリケーションからの参照／変更を禁止することができる。

【０１２１】

その場合に、Ｗｉｎｄｏｗｓにおいて監視／制御するＡＰＩとして次のものがある。

【０１２２】

（１）プロセス管理ＡＰＩ

ＯｐｅｎＰｒｏｃｅｓｓ

ＣｒｅａｔｅＰｒｏｃｅｓｓ

ＣｌｏｓｅＨａｎｄｌｅ

（２）メモリ操作ＡＰＩ

ＲｅａｄＰｒｏｃｅｓｓＭｅｍｏｒｙ

ＷｒｉｔｅＰｒｏｃｅｓｓＭｅｍｏｒｙ

ＲｅａｄＰｒｏｃｅｓｓＭｅｍｏｒｙＶｌｍ

ＷｒｉｔｅＰｒｏｃｅｓｓＭｅｍｏｒｙＶｌｍ

このようなＡＰＩの監視によってプロセス内メモリの参照または変更を禁止する印刷を禁止する場合、具体的な方法として次の方法がある。

【０１２３】

＜方法＞

アクセスが禁止されているアプリケーションのプロセス内メモリにおいて、メモリ操作ＡＰＩが要求された際に、アクセス違反エラーを返す。

【０１２４】

次に、ブラウザに表示したＷｅｂページの印刷や保存や外部装置への出力を禁止する例について説明する。

【０１２５】

従来、閲覧や再生のみを許可したＷｅｂページでも、実際にはブラウザソフトによって印刷や保存が可能であった。ＷｅｂページをロードするためのネットワークリソースにアクセスするＡＰＩを監視し、ブラウザが行なう印刷や保存を監視／制御することにより、印刷や保存や外部装置への出力操作を禁止することができる。その場合に、監視／制御するＡＰＩとして次のようなものがある。

【０１２６】

Ｗｉｎｄｏｗｓの場合
（１）通信ＡＰＩ
ＷＳＡＳｔａｒｔｕｐ
ａｃｃｅｐｔ
ｂｉｎｄ
ｃｏｎｎｅｃｔ
ｇｅｔｈｏｓｔｂｙｎａｍｅ
ｇｅｔｈｏｓｔｂｙａｄｄｒ
ｇｅｔｐｒｏｔｏｂｙｎａｍｅ
ｇｅｔｐｒｏｔｏｂｙｎｕｍｂｅｒ
ｇｅｔｓｅｒｖｂｙｎａｍｅ
ｇｅｔｓｅｒｖｂｙｐｏｒｔ
ｇｅｔｐｅｅｒｎａｍｅ
ｇｅｔｓｏｃｋｎａｍｅ
ｇｅｔｈｏｓｔｎａｍｅ
ｇｅｔｓｏｃｋｏｐｔ
ｓｅｔｓｏｃｋｏｐｔ
ｒｅｃｖ
ｒｅｃｖｆｒｏｍ
ｓｏｃｋｅｔ
ｓｅｌｅｃｔ
ｓｅｎｄ
ｓｅｎｄｔｏ
ＷＳＡＳｅｎｄ
ＷＳＡＳｅｎｄＴｏ
ＷＳＡＡｓｙｎｃＳｅｌｅｃｔ
ＷＳＡＡｓｙｎｃＧｅｔＨｏｓｔＢｙＡｄｄｒ
ＷＳＡＡｓｙｎｃＧｅｔＨｏｓｔＢｙＮａｍｅ
ＷＳＡＡｓｙｎｃＧｅｔＰｒｏｔｏＢｙＮｕｍｂｅｒ
ＷＳＡＡｓｙｎｃＧｅｔＰｒｏｔｏＢｙＮａｍｅ
ＷＳＡＡｓｙｎｃＧｅｔＳｅｒｖＢｙＰｏｒｔ
ＷＳＡＡｓｙｎｃＧｅｔＳｅｒｖＢｙＮａｍｅ
ＷＳＡＣａｎｃｅｌＡｓｙｎｃＲｅｑｕｅｓｔ
ＷＳＡＳｅｔＢｌｏｃｋｉｎｇＨｏｏｋ
ＷＳＡＵｎｈｏｏｋＢｌｏｃｋｉｎｇＨｏｏｋ
ＷＳＡＣｌｅａｎｕｐ
ｃｌｏｓｅｓｏｃｋｅｔ
ｓｈｕｔｄｏｗｎ
（２）その他、前述のファイル、印刷、外部装置への操作を禁止する場合のＡＰＩ
ＵＮＩＸの場合
（１）
ａｃｃｅｐｔ
ｂｉｎｄ
ｃｏｎｎｅｃｔ
ｇｅｔｈｏｓｔｂｙｎａｍｅ
ｇｅｔｈｏｓｔｂｙａｄｄｒ
ｇｅｔｐｒｏｔｏｂｙｎａｍｅ
ｇｅｔｐｒｏｔｏｂｙｎｕｍｂｅｒ
ｇｅｔｓｅｒｖｂｙｎａｍｅ
ｇｅｔｓｅｒｖｂｙｐｏｒｔ

ｇｅｔｐｅｅｒｎａｍｅ
ｇｅｔｓｏｃｋｎａｍｅ
ｇｅｔｈｏｓｔｎａｍｅ
ｇｅｔｓｏｃｋｏｐｔ
ｓｅｔｓｏｃｋｏｐｔ
ｒｅｃｖ
ｒｅｃｖｆｒｏｍ
ｓｏｃｋｅｔ
ｓｅｌｅｃｔ
ｓｅｎｄ
ｓｅｎｄｔｏ
ｃｌｏｓｅｓｏｃｋｅｔ
ｓｈｕｔｄｏｗｎ

（２）その他、前述のファイル、印刷、外部装置への操作を禁止する場合のＡＰＩ

このような通信ＡＰＩを監視し、印刷や保存や外部装置への出力を禁止する方法として、次の方法がある。

【０１２７】

まず、Ｗｅｂページ内に記述された禁止指定を読み取る。具体的には、ｈｔｔｐプロトコルまたは同等のプロトコルのデータを監視し、その中のＷｅｂページデータ部分に印刷や保存の禁止指定タグが含まれていれば、そのＷｅｂページは印刷や保存が禁止されていると判断する。または、権限の獲得を利用者に求め、獲得できなかった場合に印刷や保存が禁止されていると判断する。しかし、獲得できた場合には、印刷や保存が禁止されていないものと判断する。すなわち、アクセス権限が獲得できたか否かをもって、アクセス権限があるか否かを判定する。

【０１２８】

印刷や保存や外部装置への出力が禁止されているページを表示しているブラウザが、印刷や保存を行なおうとした場合、前述した印刷やファイルの保存や外部装置への出力を禁止する方法を用いて、それを禁止する。

【０１２９】

ここで説明したＷｅｂページの例は、そのしくみの類似性により、容易にディジタルテレビジョンのコンテンツにおいても利用できるものである。

【０１３０】

次に、リソース管理プログラムを応用した例を示しておく。

【０１３１】

図６は、リソース管理プログラム２０３が管理しているリソースのアクセス状況を履歴管理プログラム６０１に転送し、履歴管理データベース（ＤＢ）６０２に格納しておき、必要に応じて、図８に示すようなアクセス監視履歴として画面表示する構成を示したものである。通報プログラム６０３は、不正なアクセスがあった場合にシステム管理者の端末に対し、図７Ｂで示すような内容の不正アクセス通知画面を送信し、表示させるものである。

【０１３２】

なお、一般ユーザが不正アクセスを行なった場合には、図７Ａで示すような画面表示が行われる。

【０１３３】

なお、上記の説明においては、アクセス権限管理テーブル２０３５を参照してアクセス権限の有無を判定するようにしているが、コンピュータリソース内部に記述された、既存環境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情報を参照し、アクセス権限があるか否かを判定するようにすることもできる。

【０１３４】

また、上記の説明において用いたネットワークリソースとは、通信媒体、デバイス、ア

クセスポイント、ディジタルテレビジョンのチャンネル、通信データまたはコンテンツなど、ＯＳが管理しているリソースのうちネットワークに関するものである。

【０１３５】

以上のように、第１実施形態においては、リソース管理プログラム２０３によって、基本的には、ファイル、ネットワーク、記憶装置、表示画面、外部装置等のＯＳが管理しているコンピュータリソースに対するプロセスまたはＯＳ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し、その捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する。判定の結果、アクセス権限があれば当該操作要求通りにＯＳに渡し、その結果を要求元プロセスに返す。一方、アクセス権限がなければ当該操作要求を拒否するようにする。これにより、ＯＳやプロセス（ＯＳの元に稼動しているプログラムであり、アプリケーションやデーモンなど）を変更することなく、ファイルや画面以外のコンピュータリソースを含めてアクセス権限のないユーザに対するリソースの操作を制限することができる。

【０１３６】

また、リソース管理プログラム２０３を既存の環境に組み込むだけで、上述したような各種の不正アクセスを制限することができ、既存のアクセス権限の範囲を拡張することが可能になる。

【０１３７】

さらに、要求元のアプリケーションがアクセス違反に対応する機能を有していない場合であっても、ダミーのコンピュータリソースへの操作要求に変換してＯＳに渡すようにしたため、アクセス違反に対応する機能を有していないアプリケーションに対しても対応することができる。

【０１３８】

なお、リソース管理プログラム２０３は、ＣＤ－ＲＯＭ等のディスク型ストレージ、半導体メモリ及び通信ネットワークなどの各種の媒体を通じてコンピュータにインストールまたはロードすることができる。また、プログラム製品単体として、コンピュータユーザに提供することができる。

【０１３９】

また、第１実施形態で例示したＡＰＩについては、その一例を示しただけであって、ＯＳのバージョンアップなどによって追加された場合でも容易に対応できることは言うまでもない。

【０１４０】

＜第２実施形態＞

図１０は本発明による第２実施形態のシステム構成を示す図である。

【０１４１】

図１０において、１１は、先に説明したセキュリティ環境における本発明のコンピュータアーキテクチャの構造を有するサーバを示している。本構成は、第１実施形態のリソース管理プログラム２０３によって実現されるハミングヘッズセキュリティ管理システム（Ｈ．Ｈシステム）の全体構成を示すもので、本発明によるコンピュータアーキテクチャのＨｉｅｒａｒｃｈｙを示している。

【０１４２】

２０１はＯＳであり、先に説明したようにＷｉｎｄｏｗｓでも、ＭＡＣでもＯＳはどれでもよい。本ＨＨシステムは、ＯＳに依存しないのが特徴である。１８のＡＰＩ１（Ａｐｐｌｉｃａｔｉｏｎ　Ｐｒｏｇｒａｍ　Ｉｎｔｅｒｆａｃｅ　１）は、ＯＳ２０１の中に位置していて、ＯＳ２０１とのインターフェースの役割を果たす。これは、図２のＯＳ２０１がアプリケーションに提供しているＡＰＩ群２０１２に対応する。また、リソース管理プログラム２０３に対応するＳＣＭ１９からの要求に応じて、ＯＳ２０１に指示をおくる。

【０１４３】

この場合の指示とは、クライアントへの情報の提供の方法に関するものであって、情報

を一切拒否したり、閲覧のみ可としたり、コピー、メール、転送等の許可を行なう。

【０１４４】

１９のＳＣＭ（Ｓｅｃｕｒｉｔｙ Ｃｏｎｔｒｏｌ Ｍａｎａｇｅｍｅｎｔ）は、図２のリソース管理プログラム２０３に対応し、本発明の主旨であるＨ．Ｈ（ハミングヘッズ）セキュリティモジュールを示す。これは、ＯＳ２０１、ＡＰＬ２１（アプリケーション・ソフトウエア）の処理を監視し、何らかの条件で、ＡＰＬ２１によるリソースへのアクセスの許可、不許可を決める。１２はアクセス権限管理テーブルであり、図２のアクセス権限管理テーブル２０３５を拡張したものである。特に、このアクセス権限管理テーブル１２では、本システムにどのような形でクライアントがアクセス可能か、を判断する。また、クライアントがアクセスした場合、アクセス権限管理テーブル１２の中に人の名、電話番号、あるいはＩＤ番号を保持し、それらでアクセスしたクライアントの位置付けと重みを判断する。

【０１４５】

尚、ここで説明するクライアントとは、サーバ１１に対する１つの端末あるいは、その端末を使用する複数ユーザそれぞれあるいはそれらの一部あるいはすべてを示すものである。

【０１４６】

特に、クライアントの要求をそのまま受け入れるか、条件をつけて許可するかは、アクセス権限管理テーブル１２に格納されているクライアントの個人データによって判断する。尚、情報の提供を要求通りクライアントに提供できないが、課金することによって提供できることもある。この場合は、クライアントの個人データに課金の有無に応じてクライアントの要求をそのまま受け入れるか、条件をつけて許可するかの設定を行なっておく。

【０１４７】

２０のＡＰＩ２（Ａｐｐｌｉｃａｔｉｏｎ Ｐｒｏｇｒａｍ Ｉｎｔｅｒｆａｃｅ ２）は、ＡＰＬ２１とＳＣＭ１９間のＡＰＩとして機能し、クライアントのアクセスを監視していて、アクセスがあればＯＳ２０１にわたす。また、ＯＳ２０１のコントロール下にある外部装置の監視も行なう。ＯＳ２０１の要求する全てのリソースが対象になる。また、ＡＰＩ２（２０）は、図６の履歴管理プログラムの機能を有し、必要に応じて履歴ファイル１４に、クライアントからのアクセス、要求の履歴を記憶する。

【０１４８】

２１のＡＰＬは、各種のアプリケーションプログラムであって、例えばマイクロソフト社のＯｆｆｉｃｅ２０００、Ｗｏｒｄ、Ｅｘｃｅｌ、Ｐｏｗｅｒ Ｐｏｉｎｔなどの類である。クライアントは文章、図、あるいは静止画、動画、音声、音楽等の情報の利用・再生をＯＳのコントロール下で行なう。１３はＡＰＬ２１で作成されたファイルであり、例えば、各種のアプリケーションソフト、クライアントの作成したファイル群である。

【０１４９】

２２は、例えば、ＳＣＭ１９を搭載したサーバ１１と、外部装置とを接続するインターフェース（Ｉ／Ｆ）であり、本例では、通信ネットワーク１５、ドライバソフト１６を介して外部装置（クライアント２８、ユーザの画面２３、プリンタ２４、Ｆａｘ／コピー機２５）に接続している。

【０１５０】

又、他のクライアントは通信ネットワーク１５を介して、２３、２４、２５、２８等の外部装置を用いて情報の提供を受けることが出来る。

【０１５１】

２６は公衆網通信インターフェースであり、２７は外部装置接続用のＵＳＢ、ＲＳ２３２Ｃ、ＩＥＥＥ１３９４等のシリアル、パラレルのコネクターと接続する通信ラインである。２９は外部装置との接続線であって、ドライバソフト１６は、外部装置２３、２４、２５、２８かサーバ１１に内蔵されているのが一般的である。

【０１５２】

図１１は、図１０に示した構成において、ＯＳ２０１、外部装置２３、２４、２５、２

８、ファイル１３とＳＣＭ１９との関係を示した模式図である。
ファイル１３には、クライアントによって作られた創作物、サーバ１１が提供するＨ．Ｈサイト（ハミングヘッズサイト）、サーバ１１から提供される各種の情報が格納されている。この情報とは、文章、図、絵、音声、静止画、動画等を含む。
【０１５３】
ＳＣＭ１９はＯＳ２０１とＡＰＬ２１の中間に位置して情報の抽出、使用について、クライアントの動きを監視している。ＯＳ２０１のコントロール下で外部装置２３、２４、２５、２８への情報の出力についてクライアントの権限をチェックして、制限をくわえる。制限とは、先に説明したように情報のコピー、電子メールによる転送の許諾権を与えるものである。
【０１５４】
アクセス権限管理テーブル１２には、クライアントの権限情報を格納していて、要求に応じてその都度、照合して外部装置への出力に制限をくわえる。クライアントはあらかじめ個人の情報を登録しておく必要がある。企業、法人、政府機関、自治体等であれば、部長、課長、一般職というように職位によって権限を制限したり、与えたりしてもよい。
【０１５５】
又、外部の一般人がクライアントとしてアクセス要求する場合もある。その時には、外部に出せる情報であれば無料のものと有料のものとを層別してＳＣＭ１９が管理しておけばよい。
【０１５６】
＜第３実施形態＞
実施形態１、２では、リソース管理プログラム２０３が事前にサーバやクライアントに搭載された環境で、本発明のセキュリティ環境を提供するものであった。しかしながら、このリソース管理プログラム２０３が事前に搭載されていないサーバやクライアントでは、本発明のセキュリティ環境を実現することができない。そこで、第３実施形態では、リソース管理プログラム２０３が事前に搭載されていないサーバやクライアントに対し、本発明のセキュリティ環境を実現するための構成について説明する。
【０１５７】
図１２は第３実施形態を示すシステム構成図である。
【０１５８】
図１２に示す構成は、プロテクション化電子情報を提供する情報処理装置３１０と電子情報を受け取り利用するための情報処理装置３１１とプロテクション化電子情報を受け取り側へ送信することが可能な通信回線３１２からなるシステム構成を示すものである。
【０１５９】
提供側の情報処理装置３１０は、ハードディスクドライブ（ＨＤＤ）３１０３を備えたコンピュータ（ＰＣ）３１００、外部にプロテクション化電子情報を出力することが可能な外部装置（例えば、フロッピー（登録商標）ディスクドライブ（ＦＤＤ））３１０２で構成され、提供対象の電子情報３１０１を保持している。また、通信回線３１２と接続する外部インターフェース（Ｉ／Ｆ）３１０４を有している。
【０１６０】
尚、ＰＣ３１００は、パーソナルコンピュータやワークステーション等の汎用コンピュータであり、汎用コンピュータが標準的に装備する不図示のキーボードやマウス、ディスプレイ等を有している。
【０１６１】
一方、受け取り側の情報処理装置３１１は、ハードディスクドライブ（ＨＤＤ）３１１２を備えたコンピュータ（ＰＣ）３１１０、外部からプロテクション化電子情報を読み込むことが可能な外部装置（例えば、フロッピー（登録商標）ディスクドライブ（ＦＤＤ））３１１３、ディスプレイ３１１６、プリンタやＦＡＸ、コピー機等の出力部３１１５、キーボードやマウス等の入力部３１１４で構成され、外部インターフェース（Ｉ／Ｆ）３１１７を介して受け取ったプロテクション化電子情報３１１１を保持している。また、通

信回線３１２と接続する外部インターフェース（Ｉ／Ｆ）３１１７を有している。
【０１６２】
このようにして、提供側の情報処理装置３１０と受け取り側の情報処理装置３１１は、通信回線３１２を利用してプロテクション化電子情報を含む各種電子情報の受け渡しが可能となっている。
【０１６３】
ＰＣ３１００には、汎用のＯＳまたはプラットフォームが組み込まれており、さらに第３実施形態に係るプロテクション化プログラムが組み込まれている。
【０１６４】
ＰＣ３１１０には、汎用のＯＳと受け取った電子情報にアクセスするためのアプリケーションが組み込まれている。
【０１６５】
提供側では、提供する電子情報３１０１をプロテクション化プログラムによってプロテクション化し、プロテクション化電子情報を作成する。作成したプロテクション化電子情報を外部装置３１０２もしくは通信網３１２を介して受け取り側に渡し、受け取り側の情報処理装置３１１では、外部装置３１１３もしくは通信回線３１２を介してプロテクション化電子情報を受け取る。そして、受け取ったプロテクション化電子情報を実行することで、目的の電子情報を利用可能となるが、その電子情報に対するプロテクション化によって利用範囲は制限される。例えば、印刷操作の禁止や利用ユーザの限定などである。尚、この制限は、第１実施形態のリソース管理プログラム２０３によって実現されるものである。
【０１６６】
このように、第３実施形態では、受け取り側に制限操作を定義したプロテクション化電子情報を渡すことによって、提供側は受け取り側の利用範囲を限定した形で電子情報を提供することが可能となる。
【０１６７】
図１３Ａは、プロテクション化電子情報の構成を示す図であり、プロテクション化電子情報３２０は制限プログラム３２１、制限属性３２２、制限対象の元電子情報３２３から構成される。また、図１３Ｂに示すように、制限プログラム３２１は展開ルーチン部３２１０と制限ルーチン部３２１１から構成される。尚、この制限ルーチン部３２１１は、第１実施形態のリソース管理プログラム２０３に対応する。
【０１６８】
さらに、図１３Ｃに示すように、制限属性３２２は対象アプリケーション情報３２２０、制限操作情報３２２１１～３２２１Ｎ、それに対応する制限条件情報３２２２１～３２２２Ｎから構成される。尚、制限操作情報と制限条件情報の組は必要に応じて複数保持することがあり、図ではＮ組の制限操作情報と制限条件情報の組を保持している状態を示している。
【０１６９】
制限操作情報としては、アプリケーション、ＯＳまたはプラットフォームに実装されている機能のうち、制限したい機能を指定する。例えば、印刷、編集、表示、画面のイメージ取得、外部装置への保存などである。
【０１７０】
制限条件としては、操作を制限するための条件を指定する。例えば、利用可能な時間の指定、利用可能なコンピュータの指定、利用可能なユーザやグループの指定、課金条件などである。
【０１７１】
無条件に特定の操作を制限する場合は、制限条件を省略する。
【０１７２】
また、対象アプリケーションが自明であるような場合には、対象アプリケーション情報３２２０は省略されることもある。例えば、Ｗｉｎｄｏｗｓでは対象ファイルの拡張子に

よってアプリケーションが特定されることがあり、これは対象アプリケーションが自明なケースである。

【０１７３】

逆に、対象アプリケーションを明示することで、電子情報にアクセスするアプリケーションを限定することが可能となる。

【０１７４】

制限ルーチン部３２１１は、対象の電子情報に対する操作を監視及び制御するプログラムコード（第１実施形態のリソース管理プログラム２０３）が実装されており、その内容および実現方法については、第１実施形態で説明した通りである。

【０１７５】

図１４は第３実施形態におけるプロテクション化電子情報の提供手順を示すフローチャートである。

【０１７６】

ステップＳ３０で、対象となる電子情報３２３を読み込み、メモリやハードディスクなどの記憶媒体に記憶する。

【０１７７】

この時、電子情報３２３を暗号化した状態で記憶する場合もある。この場合は、プロテクション化した状態では元の電子情報を読み取ることは困難となり、よりセキュリティが向上する。

【０１７８】

ステップＳ３１で、電子情報３２３に対して制限する操作およびその条件が定義された制限属性３２２を、ステップＳ３０で記憶した電子情報３２３に付加する。また、必要であれば制限属性３２２に電子情報３２３を利用するためのアプリケーション情報を含めることもある。アプリケーション情報を含めた場合は、そのアプリケーションを使用してのみ電子情報にアクセス可能となる。

【０１７９】

ステップＳ３２で、電子情報３２３へのアクセス制御を実行する制限プログラム３２１を、Ｓ３０で記憶した電子情報３２３に付加する。これによって、プロテクション化電子情報３２０が生成される。制限プログラム３２１の内容は、対象の電子情報３２３に対して指定した制限内容が制御可能であるプログラムコードが実装されていれば十分であるので、対象の電子情報３２３や制限属性３２２によって異なるものになっても良い。

【０１８０】

また、制限プログラム３２１は、プロテクション化電子情報３２０を受け取る側のＯＳやプラットフォームで実行可能である必要があるため、受け取る側の利用環境に応じた実行可能な形式のプログラムコードにする。

【０１８１】

ステップＳ３３で、プロテクション化電子情報３２０を出力する。ここで、プロテクション化電子情報３２０は、ステップＳ３０で記憶した電子情報３２３にステップＳ３１およびステップＳ３２によって制限属性３２２および制限プログラム３２１が付加されたものであり、プロテクション化電子情報３２０を利用する環境において実行可能な形式にする。

【０１８２】

図１５は第３実施形態のプロテクション化電子情報の利用手順を示すフローチャートである。

【０１８３】

プロテクション化電子情報３２０は、利用環境において実行可能な形式になっているが、プロテクション化電子情報３２０を実行した際の処理は、制限プログラム３２１中の展開ルーチン部３２１０にあるプログラムコードによって行われる。このフロー図は、展開ルーチン部の流れを説明するものである。

【０１８４】

なお、制限プログラム３２１には、展開ルーチン部３２１０の他に制限ルーチン部３２１１が含まれているが、制限ルーチン部３２１１はアプリケーションからのアクセスを制御するプログラムコード（第１実施形態のリソース管理プログラム２０３）からなっており、その詳細については、第１実施形態で説明した通りである。

【０１８５】

ステップＳ４０１で、プロテクション化電子情報３２０を起動する。起動方法は利用環境によって異なるが、例えばＯＳが実行ファイルとして起動する場合や、ＷｅｂブラウザがプラグインやＪＡＶＡアプレットとして起動する場合がある。

【０１８６】

ステップＳ４０２で、制限プログラム３２１中に含まれる制限ルーチン部３２１１をコンピュータ内のＲＡＭにロードし起動する。

【０１８７】

ステップＳ４０３は、プロテクション化電子情報３２０に含まれている制限属性３２２を取得する。制限属性３２２に起動するアプリケーション情報３２２０が含まれている場合は、そのアプリケーション情報３２２０を取得し起動すべきアプリケーションを特定する。制限属性３２２に起動するアプリケーション情報が含まれていない場合は、起動すべきアプリケーションを自動判断によって特定する。

【０１８８】

自動判断の方法は、例えば電子情報３２３のタイプや拡張子からＯＳにて定義されているアプリケーションを取得する方法や、利用環境に応じてアプリケーションを特定する方法がある。

【０１８９】

また、制限属性３２２に含まれている制限操作および制限条件を取得し、ステップＳ４０２によって起動した制限ルーチン部３２１１に渡す。

【０１９０】

ステップＳ４０４で、ステップＳ４０３によって特定したアプリケーションを起動する。

【０１９１】

ステップＳ４０５で、ステップＳ４０３によるアプリケーションの起動が成功したか失敗したかを判断する。アプリケーションの起動が成功した場合は（ステップＳ４０３でＹｅｓ）、ステップＳ４０７に進む。そして、ステップＳ４０７以降では、ステップＳ４０２によって起動した制限ルーチン部３２１１が、その仕組みにより、アプリケーションのアクセスに対する監視を開始し、これ以降のアプリケーションの操作に対して制御が可能となる。

【０１９２】

ステップＳ４０３によるアプリケーションの起動が失敗した場合は（ステップＳ４０４でＮｏ）、プロテクション化電子情報３２０の実行を終了する。

【０１９３】

尚、プロテクション化電子情報３２０の実行を終了する際に、ステップＳ４１３において、ステップＳ４０２にて起動した制限ルーチン部３２１１を終了させる場合もある。

【０１９４】

この制限ルーチン部３２１１を終了させない時は、以降のプロテクション化電子情報３２０の起動時に、同一の制限ルーチン部３２１１を起動させる場合、その起動が速くなるという利点がある。ステップＳ４０３によるアプリケーションの起動が失敗した場合にステップＳ４１３を実行するか否かは、利用環境に応じて選択すれば良い。

【０１９５】

一方、アプリケーションの起動が成功した場合、ステップＳ４０７で、プロテクション化電子情報３２０に含まれる元の電子情報３２３を抜き出し、アプリケーションがアクセス可能な状態に復元する。例えば、アプリケーションがファイルの形式でアクセスするのであれば、ファイル形式に出力する。元の電子情報と同じ形式の情報に復元することで、

アプリケーションからのアクセスが可能となる。
【０１９６】
なお、図１４のステップＳ３０において電子情報３２３を暗号化している場合は、ステップＳ４０７にて、その電子情報３２３の復号も行なう。
【０１９７】
ステップＳ４０８で、ステップＳ４０７で復元した電子情報をステップＳ４０４で起動したアプリケーションに渡す。
【０１９８】
ステップＳ４０９で、アプリケーションが電子情報３２３に対して通常のアクセスを行なっている状態となる。ただし、制限ルーチン部３２１１によってアクセスは制御されているため、制限属性３２２で定義された制限の範囲でのみ電子情報３２３が利用できる。すなわち、プロテクション化によって禁止された操作を試みた場合、制限ルーチン部３２１１によって拒否される。また、課金によって操作が許可される場合もある。
【０１９９】
ステップＳ４１０で、アプリケーションが電子情報３２０を解放する。一般的にアプリケーションは、電子情報３２０の使用が終了すると、その使用しなくなった電子情報を解放する。ファイル形式の電子情報の場合は、解放のことをクローズとも呼ぶ。
【０２００】
ステップＳ４１１で、ステップＳ４１０でアプリケーションが電子情報３２０を解放したことをトリガーにして、ステップＳ４０７にて復元した電子情報３２０を抹消する。
【０２０１】
ステップＳ４１２で、アプリケーションを終了する。
【０２０２】
ステップＳ４１３で、ステップＳ４１２のアプリケーション終了をトリガーにして、ステップＳ４０２で起動した制限ルーチン部３２１１を終了およびコンピュータ上から解放する。
【０２０３】
ステップＳ４１１およびステップＳ４１３は、プロテクション化電子情報３２０を起動し、元の電子情報をアプリケーションが利用している間に解放および抹消する処理であるが、これらの処理は省略することもできる。省略した場合も、目的の電子情報に対する操作の制限は可能であるが、これらの処理を行なうことで、元の電子情報の痕跡を残さないという利点がある。また、コンピュータ上のリソースを節約できるという利点もある。
【０２０４】
次に、第３実施形態の具体例について説明する。
【０２０５】
図１６はファイル形式の電子情報を提供する場合の具体例を示す図である。ここでは、電子情報として、ワープロソフトで利用する文書ファイルを例に挙げている。
【０２０６】
文書ファイルを提供する側（３５０）では、制限付きで提供したい文書ファイル（３５０１）に対して、プロテクション化を行ない（３５０２）、プロテクション化文書ファイル（３５０３）を作成し、このプロテクション化文書ファイル（３５０３）を利用者側に提供することで、文書ファイルに対する利用者側での操作を制限する。
【０２０７】
提供手段としては、電子メールソフトやＦＴＰソフトといったファイルを転送するためのソフトを利用して提供する方法（３５１）、フロッピー（登録商標）ディスクやＣＤ－Ｒ／ＲＷといった、記録可能かつ取り外し可能な媒体にコピーし提供する方法（３５２）、ＬＡＮや公衆回線などのネットワークを用いたリモートファイルシステムを利用して提供する方法（３５３）などがある。
【０２０８】
いずれの方法も、プロテクション化文書ファイル３５０３はファイル形式のまま利用者

側に提供される。提供されたプロテクション化文書ファイル３５０３は利用者側のコンピュータで実行可能な形式をしており、実行することで、電子情報にアクセスするためのワープロソフトが実行され、すでに述べた方法によって、ワープロソフトで対象の電子情報が利用可能となる。しかも、利用中は制限ルーチン部によってワープロソフトのアクセスが制御されており、禁止された操作は拒否される。

【０２０９】

例えば、閲覧のみ許可するために、印刷、編集または文書の転写を禁止する場合、ワープロソフトが禁止したい機能を備えたものであれば、制限ルーチン部にこれらの制御プログラムコードを含め、制限操作として印刷、編集、転写機能を指定することで実現可能となる。

【０２１０】

また、利用時間や利用者、利用場所を限定する場合には、制限条件として、それらの条件を指定することで制限可能となる。

【０２１１】

さらに、課金情報を制限条件に指定することで、利用者が文書ファイルを閲覧する際に、課金することも可能となる。

【０２１２】

この例は、著作権の対象となる文書ファイルや、特定の人にのみ提供する場合に有効となる例である。

【０２１３】

図１７はファイル形式以外の電子情報を提供する場合の具体例を示す図である。ここでは、電子情報として、画像、音楽、動画等のマルチメディア情報を例に挙げている。

【０２１４】

マルチメディア情報を提供する側（３６０）では、制限付きで提供したいマルチメディア情報（３６０１）に対して、プロテクション化を行ない（（３６０２）、プロテクション化マルチメディア情報（３６０３）を作成し、このプロテクション化マルチメディア情報（３６０３）を利用者側に提供することで、マルチメディア情報に対する利用者側での操作を制限する。

【０２１５】

提供手段としては、Ｗｅｂシステムを利用して提供する方法（３６１）、携帯電話などの携帯端末機を用いたサービスを利用して提供する方法（３６２）などがある。

【０２１６】

いずれの方法も、プロテクション化マルチメディア情報３６０３は通信網を介して通信データとして利用者側に提供される。提供されたプロテクション化マルチメディア情報３６０３は利用者側のコンピュータで稼動しているＷｅｂブラウザソフトや、携帯端末機のＯＳ上で実行可能な形式をしており、プロテクション化マルチメディア情報３６０３を実行することで、マルチメディア情報にアクセスするためのマルチメディアソフトが実行され、すでに述べた方法によって、対象の電子情報が利用可能となる。しかも、利用中は制限ルーチン部によってマルチメディアソフトのアクセスが制御されており、禁止された操作は拒否される。

【０２１７】

ここで、Ｗｅｂブラウザや携帯端末機上で実行可能な形式としては、ＪＡＶＡアプレットの形式や特定のプラグインにて実行される形式などがある。すなわち、プロテクション化電子情報３６０３の形式は、利用者側のプラットフォームで実行可能な形式であり、対象のアプリケーションが起動できるものであれば良い。

【０２１８】

なお、実行可能な形式がファイル形式であれば、プロテクション化文書ファイル３５０３で説明した方法と同じ方法にて実現される。

【０２１９】

例えば、閲覧のみ許可するために、印刷、編集またはマルチメディアの転写を禁止する

場合、マルチメディアソフトが禁止したい機能を備えたものであれば、制限ルーチン部にこれらの制御プログラムコードを含め、制限操作として印刷、編集、転写機能を指定することで実現可能となる。

【０２２０】

また、利用時間や利用者、利用場所を限定する場合には、制限条件として、それらの条件を指定することで制限可能となる。

【０２２１】

さらに、課金情報を制限条件に指定することで、利用者がマルチメディア情報を利用する際に、課金することも可能となる。

【０２２２】

この例は、ライブ情報などをリアルタイムで提供する場合のようにファイル形式で提供が困難なマルチメディア情報や、Ｗｅｂシステムを利用した不特定多数に対する提供において課金するような場合に有効となる例である。

【０２２３】

以上説明したように、第３実施形態によれば、プロテクション化電子情報を作成することで、事前にセキュリティが確保されていない環境においても、必要に応じて、所望のセキュリティを確保した環境を提供することができる。

【０２２４】

以上の第３実施形態で例示したプロテクション化電子情報ついては、その一例を示しただけであって、電子情報の利用環境に合わせた実行可能な形式であれば良く、ＯＳやプラットフォームがバージョンアップなどによって変更された場合でも容易に対応でき、さらに制限プログラムの機能の範囲において、制限する操作を拡張できることは言うまでもない。

【０２２５】

また、対象となる電子情報も、例に示したもの以外に適用可能な電子情報は多くあり、プロテクション化可能な電子情報であれば同様に制限をかけることが可能であることは言うまでもない。

【０２２６】

なお、本発明におけるプロテクション化プログラムは、ＣＤ－ＲＯＭ等のディスク型ストレージ、半導体メモリ及び通信ネットワークなどの各種の媒体を通じてコンピュータにインストールまたはロードすることができる。また、プログラム製品単体として、コンピュータユーザに提供することができる。

【０２２７】

＜第４実施形態＞

第４実施形態は、第１～第３実施形態の適用例について説明する。特に、第４実施形態では、イントーネット等の広域な通信環境に第１～第３実施形態を適用した例である。図１８は第４実施形態を示すシステム構成図である。

通信ネットワーク１５は公衆網であり、インターネットＩＰ、電話網ＰＳＴＮ、ＸＤＳＬ網、デジタル網ＩＳＤＮ、Ｂ－ＩＳＤＮ、ＡＴＭ、モバイル網、衛星網等を使用している。

３１は公式のＷｅｂサイトであり、例えば、ＮＴＴドコモ社のiモードサイトがある。３２はモバイル無線網のアンテナであり、第４実施形態では、iモードサイトに接続している。もちろんＰＨＳ、他のＰＤＣ（Ｐｅｒｓｏｎａｌ　Ｄｅｇｉｔａｌ　Ｃｅｌｌａｒ）も使用できる。特に、ＩＭＴ２０００は高速なので動画の伝送に優れている。

【０２２８】

３３は第２実施形態で説明したサーバ（以下、Ｈ．Ｈサーバ）を有するＨ．Ｈサイトであり、各種情報提供を行う。このＨ．Ｈサイト３３は、先に説明したようにセキュリティを万全にしたシステムであり、クライアントの権限によって制限を設けるものである。Ｈ．Ｈサイトは、第２実施形態で説明したＳＣＭ１９をインプリメントしたソフトを搭載したサーバを使用している。

【０２２９】
３４はデータベースのサイトであり、各種のビジネス、研究等に必要な情報が格納してあって、Ｈ．Ｈサイト３３を介して使用できる。３５はＷｅｂキャストであり、デジタル放送をＨ．Ｈサイトを通して利用できる。３６は銀行、クレジット会社等の金融機関のサイトであり、Ｈ．Ｈサイト３３を使用して課金された場合、使用料の徴収をおこなう。
【０２３０】
３７はＷｅｂ上に設けられたモールであり、Ｈ．Ｈサイト３３を通してショッピングができる。購入の支払いは金融機関のサイト３６よりおこなう。
【０２３１】
Ｗｅｂ上で商品を買ったり、デジタル放送を見たり聞いたりして、課金が発生したときにはＨ．Ｈサイト３３を介しているので、利用者であるクライアント、それにサービスの提供者はセキュリティが万全であるから安心して使用できる。
【０２３２】
３８はＨ．Ｈサイト３３の利用者のための端末機器をコンビニ、街角、広場に設置した例である。図示してないがプリンタ、コピー機等も接続している。３９は学校、研究機関を、４０は工場、オフィスを示し、それぞれＨ．Ｈサイト３３の利用者のための端末機器が設定されている。
【０２３３】
４１は一般家庭でのＨ．Ｈサイト３３の利用者のための端末機器の設置例であり、４５は、ホームサーバを示す。近年、在宅で仕事をする人がふえてきた。通信回線の発展の恩恵によるものであって、企業内のデータ、情報を活用する場合、本発明によるセキュリティの効果が発揮する。４６はホームルータである。
【０２３４】
４２は携帯情報端末機器であり、モバイル機器ともいう。携帯情報端末機器４２の普及は顕著で、特にｉモードの発展は急速にたちあがった。ＣＨＴＭＬのブラウザに電子メールを送信することが可能で、これをもってＨ．Ｈサイト３３にもアクセスできるから利便性はよい。さらに、ＰａｌｍＯＳに見られるようにＰＤＡ（携帯情報端末機器）の使い勝手もよい。プリンタ、インターネットカメラ、デジタルカメラを搭載したり接続することもできる。
【０２３５】
４３はクライアント（ユーザ）である。図１８では、モバイラーとしてクライアント４３は場所を問わず、何処ででも仕事ができる。当然Ｈ．Ｈサイト３３を利用することで、そのセキュリティである権限制限機能が発揮されるから、図示してない企業のイントラネットも容易に使用できる。
【０２３６】
４４は車載移動体であり、モバイルインターネットによって同様にＨ．Ｈサイト３３からのサービスを受けることができる。
【０２３７】
尚、第４実施形態では、Ｈ．Ｈサイト３３にＨ．Ｈサーバを構成した例を説明したが、Ｗｅｂサイト３１上にこのサーバを構成しても良い。また、第３実施形態によるプロテクション化電子情報を作成するためのプロテクション化プログラムを適用する場合は、例えば、Ｈ．Ｈサイト３３やＷｅｂサイト３１上に構成し、必要に応じて、利用者が利用することになる。
【０２３８】
＜第５実施形態＞
第５実施形態は、第１～第３実施形態の別の適用例について説明する。特に、第５実施形態では、企業内のイントラネットに第１～第３実施形態を適用した例である。
【０２３９】
図１９は第５実施形態を示すシステム構成図である。
【０２４０】

尚、図１９において、第４実施形態と同じ構成要素については、同じ参照番号を付加し、その詳細については省略する。

【０２４１】

通信ネットワーク１５より回線２６を介してルータ５１に接続されている。５２はＷＷＷサーバであり、５３はファイアウォールである。ファイアウォール（Ｆ／Ｗ）５３のには、Ｈ．Ｈサーバ５５に接続されている。６７はＷＷＷサーバとＦ／Ｗ５３を接続する接続線であり、６６はＦ／Ｗ５３とＨ．Ｈサーバ５５を接続する接続線である。

【０２４２】

５６はＨ．Ｈサーバ５５とＬＡＮ５４で接続されている企業のデータベースである。このデータベース５６には、顧客のリスト、営業情報、工場であれば生産、製造の技術情報、設計開発の情報等企業活動に必要な各種のデータ、および情報が格納されていてクライアントである企業の社員は先に説明したような、権限に応じて制限付きで利用できる。これらの情報は、職能階層に応じて利用できる情報とできない情報がある。場合によっては代表権のある役員しか開示できない情報もあって、Ｈ．Ｈサーバ５５によって適切な制限下の元で管理することが可能である。

【０２４３】

企業内ＬＡＮ５４を介して接続される５７、５８、５８ｍｎは、企業内のクライアントＰＣ、サーバである。５９は多機能電話機、６０はプリンタ、ＦＡＸ/コピー機である。６１は携帯情報端末機器（例えば、ＰＤＡ）、６２は携帯電話機、６３はモバイルノートＰＣを示す。これらの機器は社内、構内モバイル機器として用いる。６５は構内移動車載端末を示す。６４は企業内、構内モバイル端末機器用のアンテナを示す。

【０２４４】

本イントラネットは、企業だけでなく法人、研究機関、教育機関でも使用できるのをはじめ、企業外からもアクセスできる。外からの使用の場合はセキュリティを確保しつつ内部の情報を提供するということが可能になる。ゆえに、本発明によるシステムはきわめて有効である。

【０２４５】

尚、第５実施形態では、イントラネット内にＨ．Ｈサーバ５５を構成した例を説明したが、Ｈ．Ｈサーバ５５が実現するセキュリティ機能を企業ＬＡＮ５４上のクライアントに構成しても良い。また、第３実施形態によるプロテクション化電子情報を作成するためのプロテクション化プログラムを適用する場合は、例えば、Ｈ．Ｈサーバ５５上に構成し、必要に応じて、利用者が利用することになる。

【０２４６】

＜第６実施形態＞

第６実施形態は、第１～第３実施形態のさらに別の適用例について説明する。特に、第６実施形態では、ＳＯＨＯ等のエンドユーザ環境に第１～第３実施形態を適用した例である。

【０２４７】

図２０は第６実施形態を示すシステム構成図である。

【０２４８】

尚、図２０において、第４実施形態と同じ構成要素については、同じ参照番号を付加し、その詳細については省略する。

【０２４９】

先に説明したようにＩＴの普及によって、家庭で就労する人が増えてきた。我が国でもすでに６百万人を超えたと言われている。少子高齢化と共にこの傾向は増加の一途にあるといえる。

【０２５０】

図２０において、エンドユーザがいる家４１は、ホームルータ７２を介して公衆回線２６に接続される。ホームルータ７２はホームＬＡＮ７３に接続されている。ホームＬＡＮ７３は有線ＬＡＮだけではなく、ブルートース、ＩｒＤＡを使用した無線ＬＡＮでもよい

。７４はＰＣまたはホームサーバ、７５は大画面付きの多機能電話機、７６はＴＶ、７７は音響ＡＶ機器、７８は携帯情報端末機器を示す。７１はアンテナで公衆無線網との接続を行なう。４１は家、家庭を示す。

【０２５１】

在宅就労は各種の企業情報、機密情報を扱うのでセキュリティの確保は最重要課題である。第６実施形態では、公式Ｗｅｂサイト３１からＨ．Ｈサイト３３を通して情報の授受を行なうから安全である。又、仕事だけでなく娯楽としてのコンテンツをネットワークから配信を受ける環境になってきた。Ｗｅｂキャスト３５からＴＶや音楽の配信を受けて、ＴＶ端末７６、ＡＶ機器７７、携帯情報端末機器７８で閲覧、鑑賞を行なうことができ、生活を豊かにすることができる。

【０２５２】

有料娯楽コンテンツの提供をネットワーク上のサイトから受けた場合、料金の支払いが生ずる。この場合、Ｈ．Ｈサイト３３を利用することで、例えば、クレジットカード番号を入力して金融機関のサイト３６から利用料の自動引き落としが可能になる。この場合、なりすましを防止するために個人認証が必要になる。個人認証の方法は各種提案されているが、ＩＤ番号、電話番号のほかに機密度の高い場合は公開鍵を使用するのもよい。なお、ホームサーバ７４をＨ．Ｈサーバを搭載して安全を確保してもよい。組織に属して家庭で就労する場合、ホームサーバ７４は企業から提供されたものを使用して家庭就労するという、条件を設けるのも一つのホームワーキングの方法である。

【０２５３】

また、第３実施形態によるプロテクション化電子情報を作成するためのプロテクション化プログラムを適用する場合は、例えば、Ｈ．Ｈサイト３３やＷｅｂサイト３１上に構成し、必要に応じて、利用者が利用することになる。

【０２５４】

次に、第６実施形態におけるセキュリティ確保についての流れ、ユーザ、クライアントに制限と課金を課す流れについて説明する。

【０２５５】

図２１は第６実施形態を実現するためのフローチャートである。

【０２５６】

尚、図２１では、便宜上、Ｈ．Ｈサイト３３と、そのＨ．Ｈサーバの管理下にあるＨ．Ｈサイト３３にアクセスするクライアント間の処理として説明するが、通信ネットワーク１５上のＨ．Ｈサーバとクライアント間の処理で図２１の処理が実現されても良い。ステップＳ８１で、クライアントが情報を得るためにＨ．Ｈサイト３３にアクセスする。ステップＳ８２で、Ｈ．Ｈサイト３３で、アクセスしてきたクライアントの個人情報を検索、照合する。

【０２５７】

ステップＳ８３で、クライアントからの情報の特定を行なう。ここでいう特定とは、機密度の程度と、アクセスしてきたクライアントの職位の階層によって権限の制限を受けるのが特徴である。クライアント、ユーザは組織に所属しているものであれば、職位の階層は自動判別できる。一般からのアクセスも可能であるから提供できる情報と出来ないものを区別する。また、無料で提供できる企業のカタログ類とか宣伝類のほかに有料で頒布できる情報もある。有料でも価値の高いものは、課金の程度を変えて頒布するのを特徴とすれば、本Ｈ．Ｈサイト３３はビジネスとして成立する。

【０２５８】

ステップＳ８４で、Ｈ．Ｈサイト３３にアクセスしてきたクライアントからの要求にこたえられるか否かを判定する。

【０２５９】

ステップ８４で、判定の結果、そのクライアントに情報を提供しても良い場合、ステップＳ８５で、ＯＫの返事、表示を出す。次に、ステップＳ８６で、例えば、クライアントが要求情報のコピーと電子メールでの他人への転送を要求する。ステップＳ８７で、クラ

イアントの職責、権限をＨ．Ｈサイト３３によって判定する。先に説明したが、本発明では個人の権限によって情報の利用を制限するものである。

【０２６０】

判定の結果、クライアントの要求を了承する場合、ステップＳ８８で、コピーもメール転送もＯＫである旨をクライアントの画面に表示する。尚、この要求が了承される場合とは、例えば、クライアントが高位な権限をもっているか、要求情報の機密性の低いものであったと判断される。

【０２６１】

ステップＳ８９で、クライアントがどんな情報、ドキュメントをいつ、コピーしたか、メール転送したかの履歴がＨ．Ｈサーバ３３に記録される。

【０２６２】

ステップＳ９０で、Ｈ．Ｈサーバ３３での履歴の管理が終了し、要求情報の提供する条件が満たされるので、クライアントへ要求情報を提供する。

【０２６３】

一方、ステップＳ８４の判定の結果、そのクライアントに情報を提供できない場合、ステップＳ９１で、クライアントへ要求が拒否される旨を通知する。ステップＳ９２で、クライアントは、ＩＤ番号として、電話番号、保険証の番号、免許証、年金番号等を入力する。このようなＩＤ番号を入力する必要があるクライアントとは、Ｈ．Ｈサイト３３に初めてアクセスしてきたクライアントや、Ｈ．Ｈサイト３３を利用しない一般のクライアントが想定される。

【０２６４】

そして、ステップＳ９３で、Ｈ．Ｈサイト３３は、入力されたＩＤ番号に基づいて、以降の処理の実行の可否を判定する。実行を拒否する場合、処理を終了する。一方、実行を許可する場合、ステップＳ８５に進む。

【０２６５】

お金を払えば提供を許可する情報であれば、課金の金額をクライアントに知らせる。金額は情報、ドキュメントの機密度、重要度によって価値は変わり、金額も異なる。

【０２６６】

つまり、ステップＳ９３は、課金を情報公開の条件としない情報であったり、有料の場合はクライアントが必要としない情報であったり、課金金額によってはクライアントが必要とする情報であったりする場合を想定して構成されている。このようにして、入手の許可が可能であれば、ステップＳ８５へ進み、許可できなければ、処理を終了する。

【０２６７】

一方、ステップ８７の判定の結果、クライアントの要求が了承できない場合、ステップＳ９４に進む。ステップＳ９４では、欲しい情報、ドキュメントのコピー、電子メール転送がＳ８７の判定によって不可と判定されているが、クライアントの画面で閲覧することを許可し、そのような表示をクライアントの画面に出力する。このため、閲覧用情報がクライアントに送られるが、Ｈ．Ｈサイト３３によってその情報がコントロールされているため、クライアントの画面に情報が表示されていても、その情報のコピーと電子メール{で}の転送はできない。

【０２６８】

ステップＳ９５で、Ｈ．Ｈサイト３３に先に説明したような履歴を管理する。ステップＳ９６で、クライアントの画面に要求のあった情報が表示される。ここで、クライアントによっては、どうしてもコピー、電子メールでの転送をしたい情報もある。そこで、クライアントは、ここであらためてサイト、サーバに許可の要求をだすことが可能である。つまり、ステップＳ９７で、課金による情報の提供を申請する。ここのステップではクライアントの職責、階層は、Ｈ．Ｈサイト３３に認知されているから金額の程度によって、許可できる場合もある。

【０２６９】

課金すれば提供できるとＨ．Ｈサイト３３が判断した場合、金額を提示する。課金して

も提供できないとＨ．Ｈサイト３３が判断すれば、ステップＳ９８で、この処理はクライアントへの操作拒否の通知画面表示のみで終了する。また、情報、ドキュメントの程度に応じて表示時間に制限を加えてもよい。所定時間内の表示を行って、より長時間見たい場合は課金制度を導入するのも一方法である。

【０２７０】

この場合、ステップＳ９９、ステップＳ１００で、Ｈ．Ｈサイト３３からより長時間の表示と課金の有無をクライアント、ユーザに問い合わせる。Ｈ．Ｈサーバ３３とクライアントが了解すれば、ステップＳ１０１で画面表示を長時間行なう。

【０２７１】

Ｈ．Ｈサーバ３３の課金とクライアントの了解が得られない場合は、所定時間のみの表示でこの処理は終了する。

【０２７２】

以上説明したように、第１実施形態ではアクセス権限をＯＳやそのプロセスを変更しないでクライアントに対して制限して不正行為を防止する例を説明した。また、第２実施形態では、Ｈ．Ｈサーバのシステム構成を説明した。また、第３実施形態では、第１実施形態で実現されるセキュリティ環境を、任意の利用者に提供する構成を説明した。

【０２７３】

第４実施形態では、通信ネットワーク、特にインターネットを中心にして社会環境で発揮するＨ．Ｈサイトのシステム構成を説明した。

【０２７４】

第５実施形態では、企業内、工場、学校、研究機関、団体等のイントラネットに本Ｈ．Ｈサーバの応用について説明した。さらに、第６実施形態では、ホームオフイス、在宅就労における本Ｈ．Ｈサイトの応用について説明した。

【０２７５】

なお、図２１のフローチャートは、Ｈ．Ｈサーバ、サイトを介して情報、ドキュメントの閲覧、コピー、電子メール転送について説明してあるが、図１８で説明したＷｅｂキャストからのデジタル放送の配信、各種無料有料コンテンツからの配信による課金システムにも適用することが可能である。

【０２７６】

尚、本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体を、システムあるいは装置に配給し、そのシステムあるいは装置のコンピュータ（またはＣＰＵやＭＰＵ）が記憶媒体に格納されたプログラムコードを読み出し実行することによっても、達成されることは言うまでもない。

【０２７７】

この場合、記憶媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。

【０２７８】

プログラムコードを供給するための媒体としては、例えば、フロッピー（登録商標）ディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＣＤ－Ｒ／ＲＷ、ＤＶＤ－ＲＯＭ／ＲＡＭ、磁気テープ、不揮発性のメモリカード、ＲＯＭなどを用いることができる。

【０２７９】

また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼動しているＯＳやプラットフォームなどが実際の処理の一部または全部を行ない、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【０２８０】

さらに、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機

能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵなどが実際の処理の一部または全部を行ない、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【０２８１】

本発明を上記媒体に適用する場合、その記憶媒体には、先に説明したフローチャートに対応するプログラムコードが格納されることになる。

【図面の簡単な説明】

【０２８２】

【図１Ａ】本発明の実施環境の第１実施形態を示すハードウェア構成図である。

【図１Ｂ】本発明の実施環境の第１実施形態を示すハードウェア構成図である。

【図２】本発明の第１実施形態におけるリソース管理プログラムの機能構成及びＯＳとアプリケーションとの関係を示す図である。

【図３】本発明の第１実施形態におけるアクセス権限管理テーブルのデータ構成例を示す図である。

【図４】本発明の第１実施形態におけるＡＰＩの監視／制御の第１の基本型を示すシーケンス図である。

【図５】本発明の第１実施形態におけるＡＰＩの監視／制御の第２の基本型を示すシーケンス図である。

【図６】本発明の第１実施形態におけるアクセス履歴を記録する機能を示すブロック構成図である。

【図７Ａ】本発明の第１実施形態における不正アクセスを示す画面例を示す図である。

【図７Ｂ】本発明の第１実施形態における不正アクセスを通知する画面例を示す図である。

【図８】本発明の第１実施形態におけるアクセス監視履歴の表示画面の例を示す図である。

【図９】アクセス制限対象となるリソースへの実際のアクセス方法の例を示す図である。

【図１０】本発明の第２実施形態のＨ．Ｈサーバの構成を示す図である。

【図１１】本発明の第２実施形態のＳＣＭとＯＳ、ファイル、外部装置との関係を示す図である。

【図１２】本発明の第３実施形態を示すハードウェア構成図である。

【図１３Ａ】本発明の第３実施形態におけるプロテクション化電子情報の構成を示す図である。

【図１３Ｂ】本発明の第３実施形態における制限プログラムの構成を示す図である。

【図１３Ｃ】本発明の第３実施形態における制限属性をの構成を示す図である。

【図１４】本発明の第３実施形態におけるプロテクション化電子情報の提供手順を示すフローチャートである。

【図１５】本発明の第３実施形態におけるプロテクション化電子情報の利用手順を示すフローチャートである。

【図１６】本発明の第３実施形態におけるファイル形式の電子情報を提供する場合の具体例を示す図である。

【図１７】本発明の第３実施形態におけるマルチメディア情報を提供する場合の具体例を示す図である。

【図１８】本発明の第４実施形態を示すシステム構成図である。

【図１９】本発明の第５実施形態を示すシステム構成図である。

【図２０】本発明の第６実施形態を示すシステム構成図である。

【図２１】ユーザ、クライアントへの制限と課金のプロセスを示すフローチャートである。

【符号の説明】

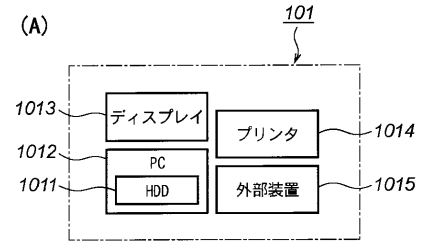
【０２８３】

１０１　コンピュータ
１０２　ネットワーク
２０１　汎用ＯＳ
２０３　リソース管理プログラム
６０１　履歴管理プログラム
６０２　履歴ＤＢ
６０３　通報プログラム
２０３１　ＡＰＩ監視コントローラ
２０３２　ＡＰＬ監視コントローラ
２０３３　アクセス制御コントローラ
２０３４　ＯＳ監視コントローラ
２０３５　アクセス権限管理テーブル
１１　Ｈ．Ｈサーバ
１２　アクセス権限管理テーブル
１３　ファイル
１４　履歴ファイル
１５　通信ネットワーク
１６　外部装置ドライバソフト
１７　汎用ＯＳ
１８　ＡＰＩ１（Ａｐｐｌｉｃａｔｉｏｎ　Ｐｒｏｇｒａｍ　Ｉｎｔｅｒｆａｃｅ　１）
１９　ＳＣＭ（Ｓｅｃｕｒｉｔｙ　Ｃｏｎｔｒｏｌ　Ｍａｎｅｇｅｍｅｎｔ）
２０　ＡＰＩ２（Ａｐｐｌｉｃａｔｉｏｎ　Ｐｒｏｇｒａｍ　Ｉｎｔｅｒｆａｃｅ　２）
２１　ＡＰＬ（Ａｐｐｌｉｃａｔｉｏｎ　Ｐｒｏｇｒａｍ　Ｌｏｇｉｃ）
２２　外部装置インターフェース
２３　画面端末装置、ＴＶ、ＰＤＡ、大画面付多機能電話機
２４　プリンタ
２５　Fax/コピー機
２６　公衆網通信インターフェース
２７　通信ライン
２８　クライアント
３１　公式Ｗｅｂサイト
３２　無線基地局
３３　Ｈ．Ｈサイト
３４　データベースサイト
３５　Ｗｅｂキャスト
３６　金融機関
３７　Ｗｅｂモール
３８　コンビニ、街角ターミナル
３９　学校、研究機関
４０　企業、工場、オフィス
４１　家庭、在宅就業
４２、７８　携帯情報端末機器、携帯電話機、ＰＤＡ
４３　ユーザ、クライアント
４４　車載移動端末機器
４５、７４　ホームサーバ
４６、７２　ホームルータ
５１　ルータ
５２　Ｗｅｂサーバ

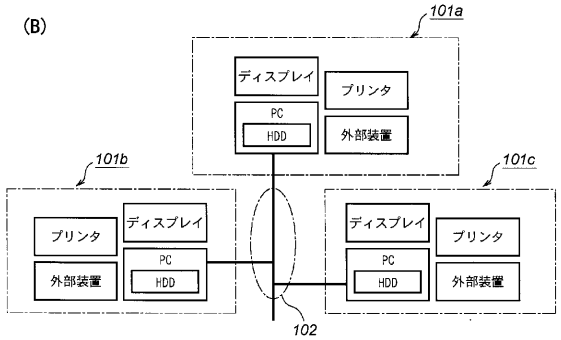
５３　ファイアウォール
５４　ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）
５５　Ｈ．Ｈサーバ
５６　データベース
５７、５８、５８ｍｎ　ＰＣ、サーバ
５９、７５　多機能電話機
６０　Ｆａｘ、プリンタ、コピー機
６１　携帯情報端末機器
６２　携帯電話機
６３　ノートＰＣ
６４　構内無線アンテナ
６５　構内移動車載端末機器
６６、６７　接続線
７１　ホーム無線アンテナ
７６　ＴＶ
７７　音響機器
３１０　電子情報を提供する側の情報処理装置
３１１　電子情報を受け取る側の情報処理装置
３１２　通信ネットワーク
３１００、３１１０　コンピュータ
３１０１　電子情報
３１０２、３１１３　取り外し可能ディスクドライブ
３１０３、３１１２　ハードディスクドライブ
３１０４、３１１７　外部インターフェース
３１１１　プロテクション化電子情報
３１１４　入力部
３１１５　出力部
３１１６　ディスプレイ
３２０　プロテクション化電子情報
３２１　制限プログラム
３２２　制限属性情報
３２３　元電子情報
３２１０　展開ルーチン部
３２１１　制限ルーチン部
３２２０　対象アプリケーション情報
３２２１１　制限操作情報１
３２２１Ｎ　制限操作情報Ｎ
３２２２１　制限条件情報1
３２２２Ｎ　制限条件情報Ｎ
３５０、３６０　電子情報提供側
３５０１　一般的な文書ファイル
３５０２、３６０２　プロテクション化の処理
３５０３　プロテクション化文書ファイル
３５１　メールやＦＴＰ等による情報提供方法
３５２　ＦＤ等の記憶媒体を利用した情報提供方法
３５３　ネットワークにて共有
３５４、３６３　電子情報利用者側
３６０１　画像、音楽、動画等のマルチメディア情報ファイル
３６０３　プロテクション化マルチメディア情報
３６１　Ｗｅｂページにて公開

３６２　携帯用端末へのサービス

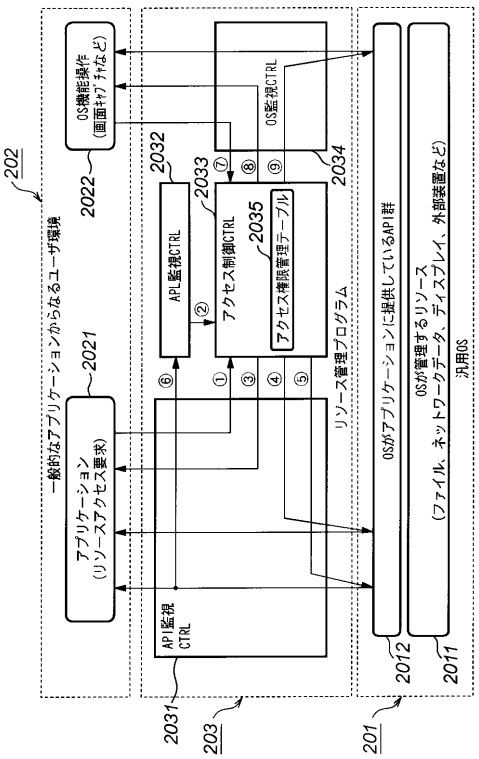
【図１Ａ】



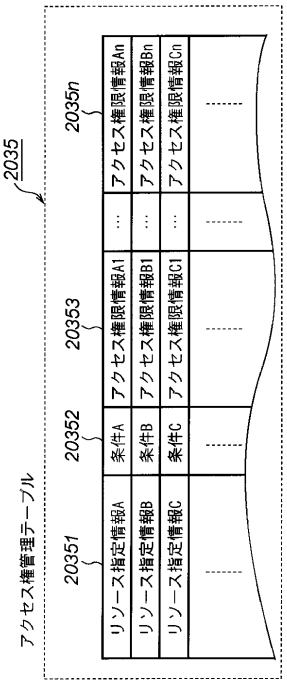
【図１Ｂ】



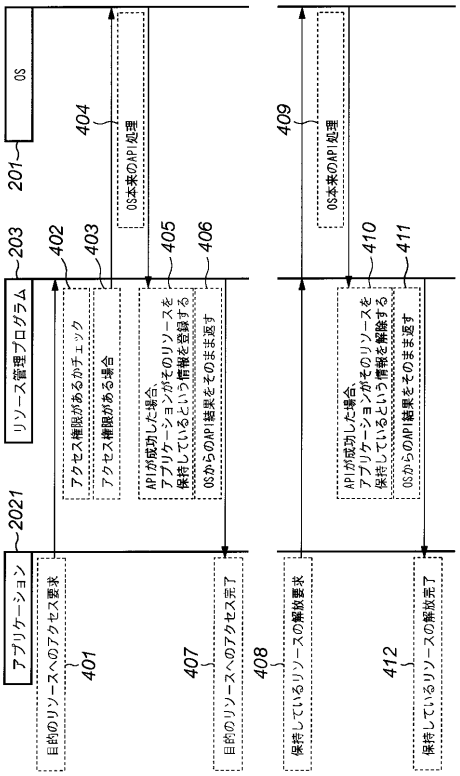
【図２】



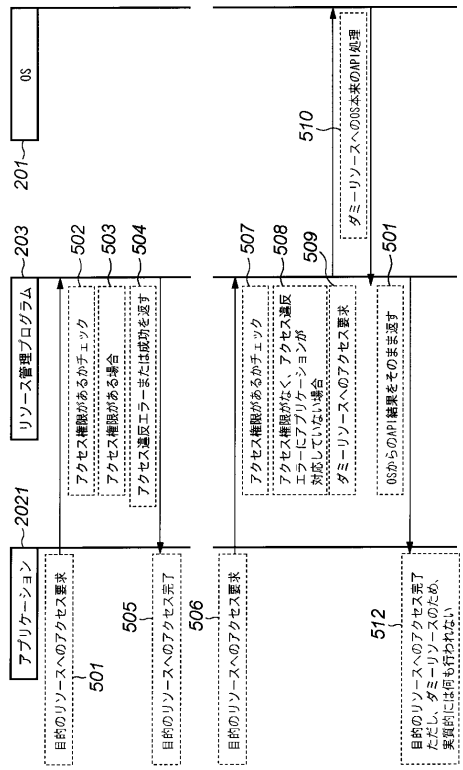
【図３】



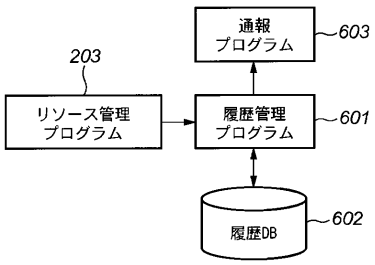
【図４】



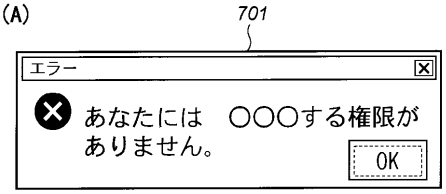
【図５】



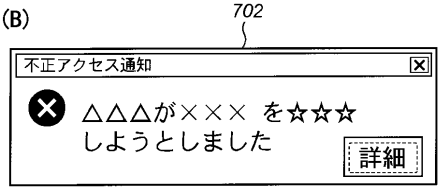
【図６】



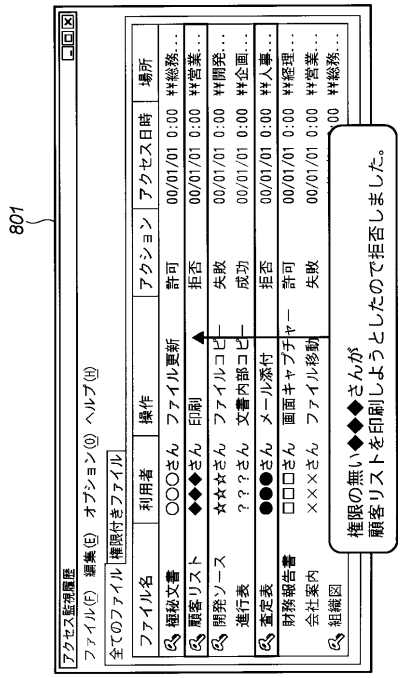
【図７Ａ】



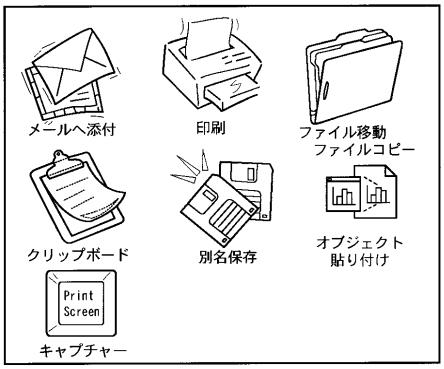
【図７Ｂ】



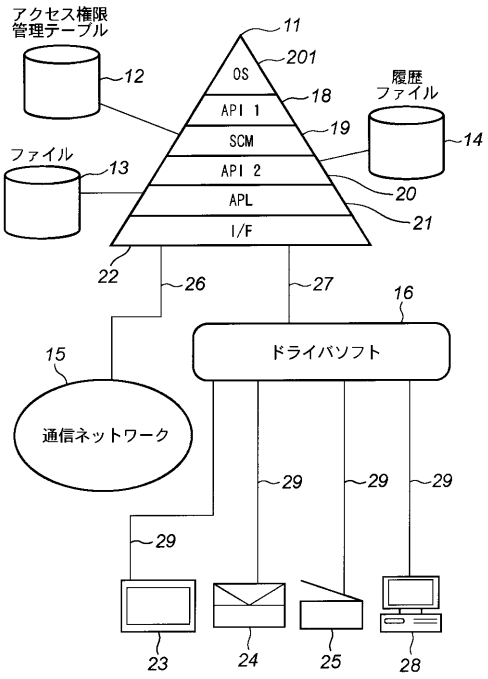
【図８】


801
アクセス監視履歴
ファイル(F) 編集(E) オプション(O) ヘルプ(H)
全てのファイル 権限付きファイル
ファイル名 利用者 操作 アクション アクセス日時 場所
極秘文書 ○○○さん ファイル更新 許可 00/01/01 0:00 ¥¥総務...
顧客リスト ◆◆◆さん 印刷 拒否 00/01/01 0:00 ¥¥営業...
開発ソース ☆☆☆さん ファイルコピー 失敗 00/01/01 0:00 ¥¥開発...
進行表 ？？？さん 文書内部コピー 成功 00/01/01 0:00 ¥¥企画...
査定表 ●●●さん メール添付 拒否 00/01/01 0:00 ¥¥人事...
財務報告書 □□□さん 画面キャプチャー 許可 00/01/01 0:00 ¥¥経理...
会社案内 ×××さん ファイル移動 失敗 00/01/01 0:00 ¥¥営業...
組織図 00 ¥¥総務...
権限の無い◆◆◆さんが
顧客リストを印刷しようとしたので拒否しました。

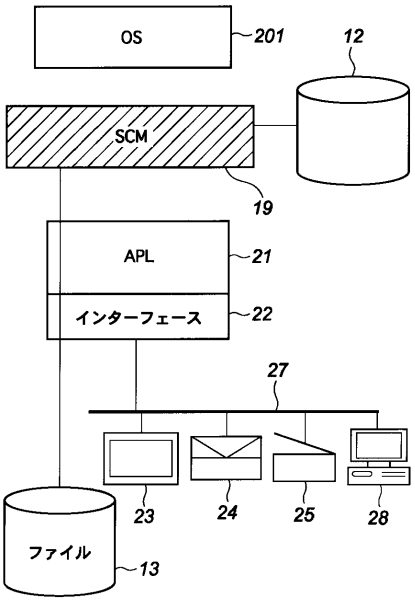
【図９】


メールへ添付
印刷
ファイル移動
ファイルコピー
クリップボード
別名保存
オブジェクト
貼り付け
Print Screen
キャプチャー

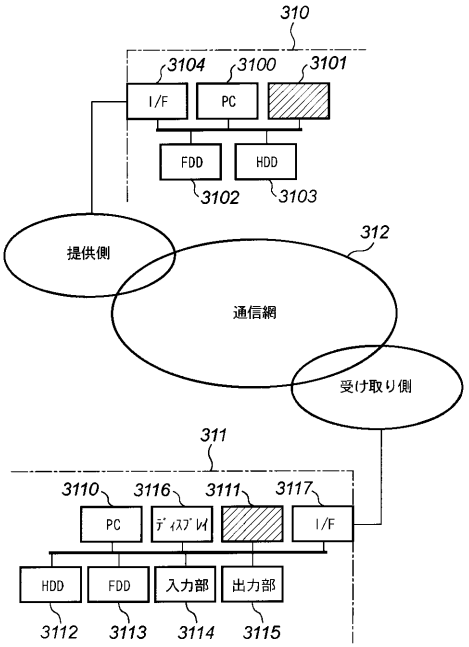
【図１０】


アクセス権限
管理テーブル
12
11
OS
201
API 1
18
SCM
19
API 2
APL
20
I/F
21
履歴
ファイル
14
ファイル
13
22
26
27
16
ドライバソフト
15
通信ネットワーク
29
29
29
29
23
24
25
28

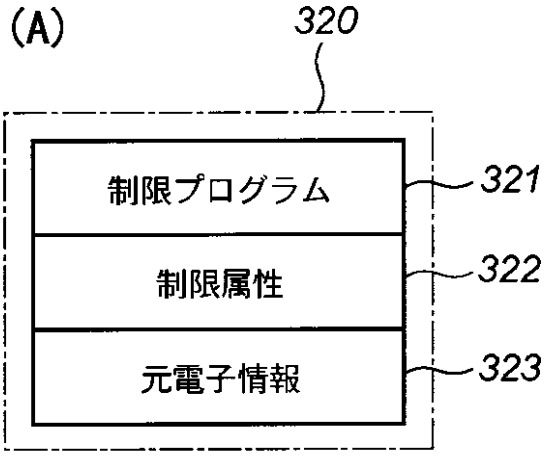
【図１１】


OS
201
12
SCM
19
APL
21
インターフェース
22
27
23
24
25
28
ファイル
13

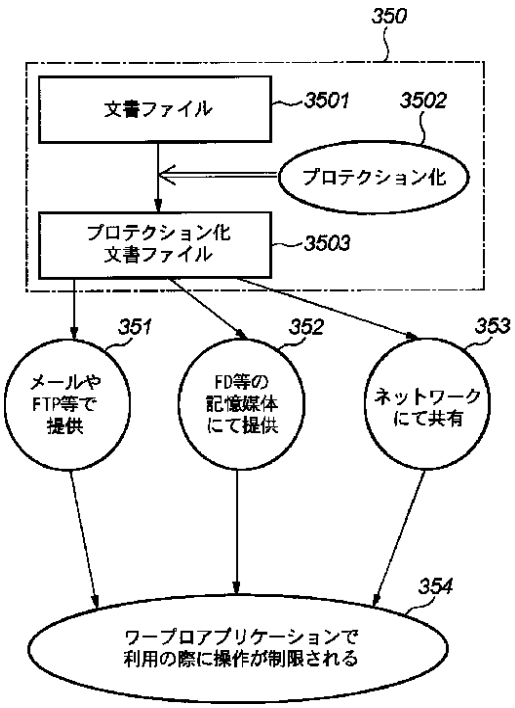
【図１２】



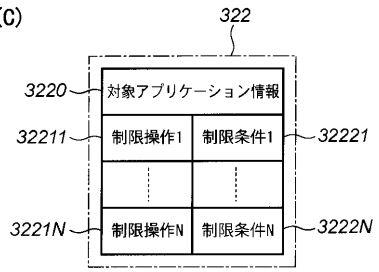
【図１３Ａ】



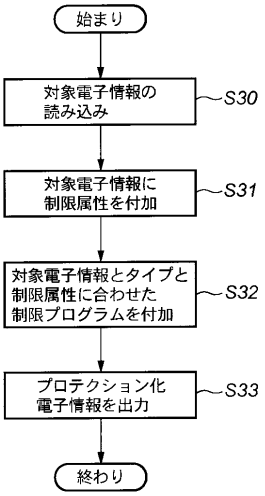
【図１３Ｂ】



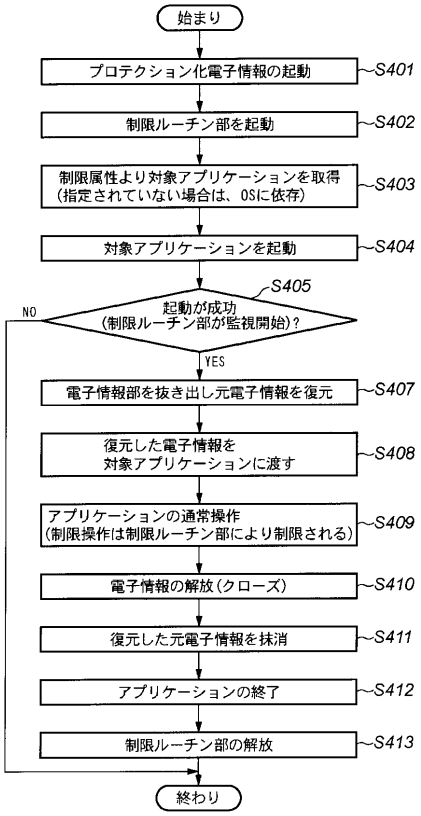
【図１３Ｃ】



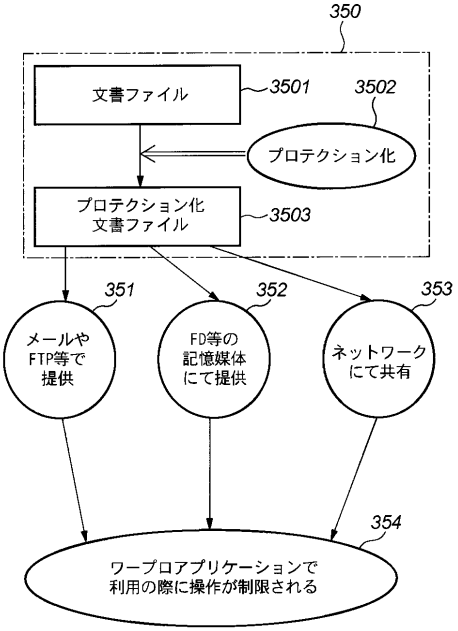
【図１４】



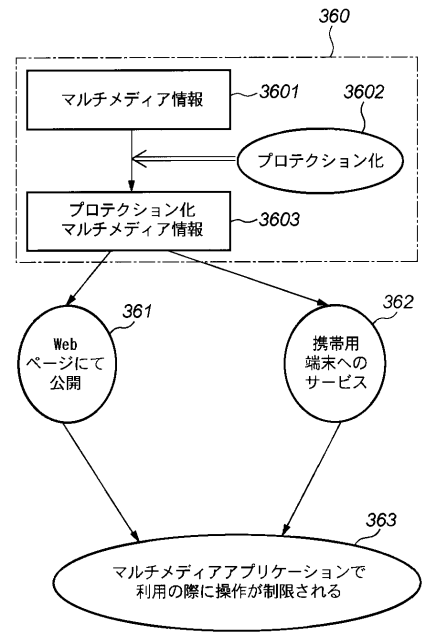
【図１５】



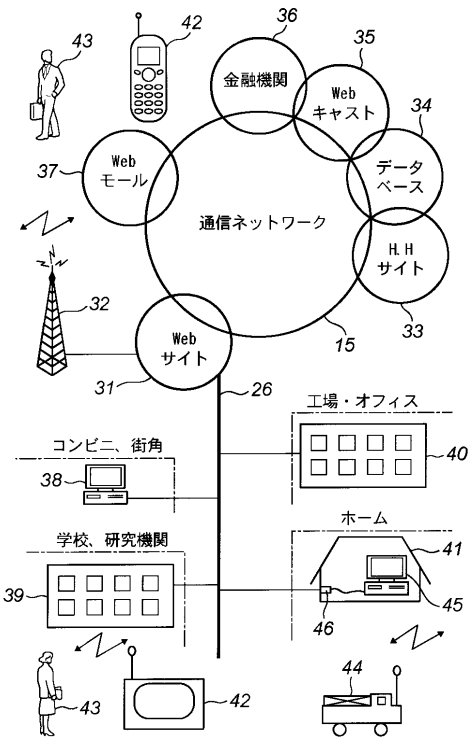
【図１６】



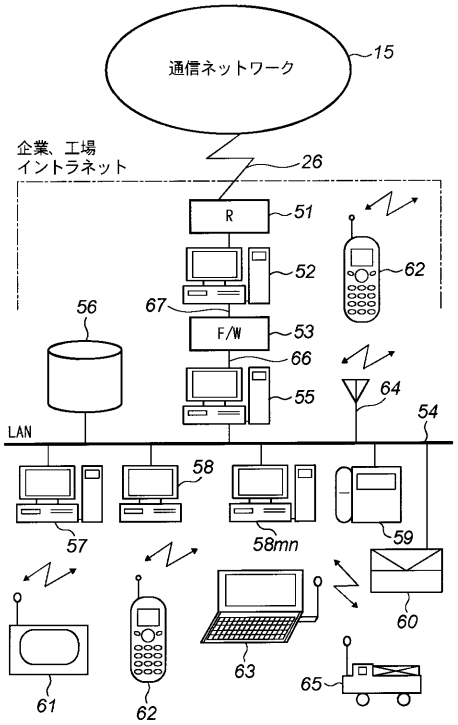
【図１７】



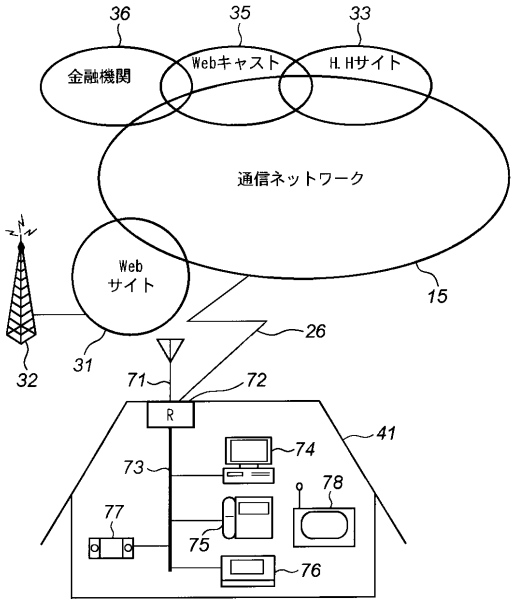
【図１８】



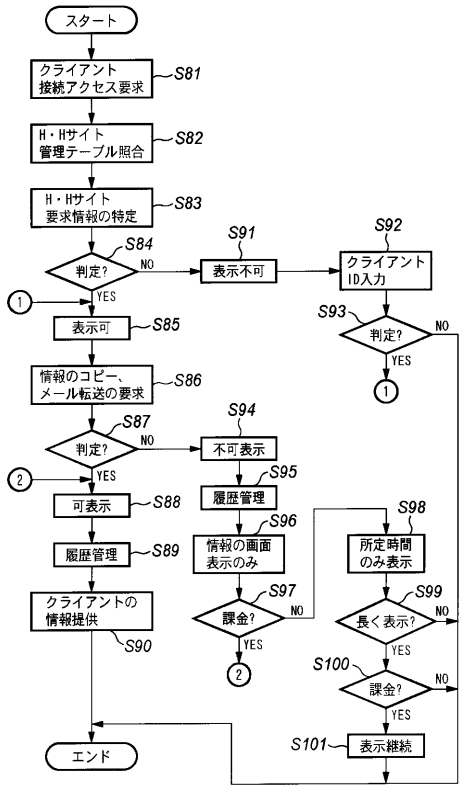
【図１９】


通信ネットワーク
15
企業、工場
イントラネット
26
R
51
52
62
56
67
F/W
53
66
55
64
54
LAN
58
57
58mn
59
60
61
62
63
65

【図２０】


36
35
33
金融機関
Webキャスト
H.Hサイト
通信ネットワーク
Web
サイト
15
26
31
32
71
72
R
41
74
73
78
77
75
76

【図２１】


スタート
クライアント
接続アクセス要求
S81
H・Hサイト
管理テーブル照合
S82
H・Hサイト
要求情報の特定
S83
判定?
S84
NO
YES
表示不可
S91
クライアント
ID入力
S92
判定?
S93
NO
YES
表示可
S85
情報のコピー、
メール転送の要求
S86
判定?
S87
NO
YES
不可表示
S94
履歴管理
S95
可表示
S88
履歴管理
S89
情報の画面
表示のみ
S96
課金?
S97
NO
YES
所定時間
のみ表示
S98
長く表示?
S99
NO
YES
課金?
S100
NO
YES
表示継続
S101
クライアントの
情報提供
S90
エンド

フロントページの続き

(31)優先権主張番号　特願2001-190445(P2001-190445)
(32)優先日　平成13年5月22日(2001.5.22)
(33)優先権主張国　日本国(JP)

(72)発明者　大江　尚之
東京都中央区月島一丁目２番１３号　ハミングヘッズ株式会社内
(72)発明者　志摩　貴浩
東京都中央区月島一丁目２番１３号　ハミングヘッズ株式会社内

合議体
審判長　酒井　伸芳
審判官　石井　茂和
審判官　原　秀人

(56)参考文献　特開平０８－０８７４４０（ＪＰ，Ａ）
特開平０８－３１４７８６（ＪＰ，Ａ）
特開平１１－２９６３３６（ＪＰ，Ａ）
特開平０９－０６２６２７（ＪＰ，Ａ）
特開平０５－１３４９３０（ＪＰ，Ａ）
特開平１０－１７７５２４（ＪＰ，Ａ）
特開２０００－０２９８４５（ＪＰ，Ａ）
Ｄｏｒｉｎ　Ｍｉｌｌｅｒ“ＵＮＩＸとＭＶＳのセキュリティ”，ＵＮＩＸ　ＭＡＧＡＺＩＮＥ，株式会社アスキー，１９９７年4月1日発行，第１２巻，第4号，ｐ．１１５－１１９