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

特許第5429744号
(P5429744)

(45)発行日　平成26年2月26日(2014.2.26)　(24)登録日　平成25年12月13日(2013.12.13)

(51)Int.Cl.　　F I
G06F 21/62 (2013.01)　　G06F 21/24 165C
G06F 12/00 (2006.01)　　G06F 12/00 537A

請求項の数 6　(全 14 頁)

(21)出願番号　特願2009-190257(P2009-190257)
(22)出願日　平成21年8月19日(2009.8.19)
(65)公開番号　特開2011-43912(P2011-43912A)
(43)公開日　平成23年3月3日(2011.3.3)
審査請求日　平成24年8月14日(2012.8.14)

(73)特許権者　504133110
国立大学法人電気通信大学
東京都調布市調布ケ丘一丁目５番地１
(74)代理人　100082131
弁理士　稲本　義雄
(74)代理人　100121131
弁理士　西川　孝
(72)発明者　原　大輔
東京都調布市調布ヶ丘一丁目５番地１　国立大学法人電気通信大学内
(72)発明者　中山　泰一
東京都調布市調布ヶ丘一丁目５番地１　国立大学法人電気通信大学内

審査官　平井　誠

最終頁に続く

(54)【発明の名称】情報処理装置および方法、並びにプログラム

(57)【特許請求の範囲】
【請求項１】
複数のユーザそれぞれにより所有されるリソースへアクセスするプロセスが、所定の実行権限で動作する情報処理装置において、
前記ユーザを特定するユーザ特定情報と、前記ユーザにより所有される前記リソースへアクセスするための位置情報とを対応付けて記憶する記憶手段と、
前記リソースへのアクセスが前記位置情報を含んでリクエストされたとき、前記リクエストに含まれる位置情報に基づいて、前記記憶手段で対応付けられた前記ユーザ特定情報を取得し、取得した前記ユーザ特定情報により特定される前記ユーザに、前記プロセスの実行権限を変更する変更手段と、
前記変更手段によって変更された前記プロセスの実行権限で、前記位置情報に基づいて前記リソースを取得する取得手段と、
前記取得手段によって取得された前記リソースを、前記リクエストに対するレスポンスとして送信する処理を制御する送信制御手段と
を備え、
前記取得手段によって取得される前記リソースが、前記変更手段によって変更された前記プロセスの実行権限をさらに変更する動的なリソースである場合、
前記取得手段は、前記プロセスの実行権限のさらなる変更を無効にする処理を行い、
前記送信制御手段は、前記取得手段によって取得された前記リソースの送信を行わせないで、エラーを表すレスポンスの送信を行わせる

情報処理装置。
【請求項２】
前記プロセスは、前記情報処理装置の管理者の実行権限で起動し、
前記変更手段は、前記送信制御手段によって前記レスポンスが送信された後、前記プロセスの実行権限を前記管理者に戻す
請求項１に記載の情報処理装置。
【請求項３】
前記変更手段は、再度、前記リソースへのアクセスがリクエストされたときに、前記プロセスの実行権限を管理者に戻す
請求項１に記載の情報処理装置。
【請求項４】
前記記憶手段は、前記ユーザ特定情報および前記ユーザの属するグループを特定するグループ特定情報と、前記位置情報とを対応付けて予め記憶する
請求項１に記載の情報処理装置。
【請求項５】
複数のユーザそれぞれにより所有されるリソースへアクセスするプロセスが、所定の実行権限で動作し、前記ユーザを特定するユーザ特定情報と、前記ユーザにより所有される前記リソースへアクセスするための位置情報とを対応付けて記憶する記憶手段を備える情報処理装置の情報処理方法において、
前記リソースへのアクセスが前記位置情報を含んでリクエストされたとき、前記リクエストに含まれる位置情報に基づいて、前記記憶手段で対応付けられた前記ユーザ特定情報を取得し、取得した前記ユーザ特定情報により特定される前記ユーザに、前記プロセスの実行権限を変更する変更ステップと、
前記変更ステップの処理によって変更された前記プロセスの実行権限で、前記位置情報に基づいて前記リソースを取得する取得ステップと、
前記取得ステップの処理によって取得された前記リソースを、前記リクエストに対するレスポンスとして送信する処理を制御する送信制御ステップと、
前記取得ステップの処理によって取得される前記リソースが、前記変更ステップの処理によって変更された前記プロセスの実行権限をさらに変更する動的なリソースである場合、
前記プロセスの実行権限のさらなる変更を無効にする処理を行う処理ステップと、
前記取得ステップの処理によって取得された前記リソースの送信を行わせないで、エラーを表すレスポンスの送信を行わせるエラー送信制御ステップと
を含む情報処理方法。
【請求項６】
複数のユーザそれぞれにより所有されるリソースへアクセスするプロセスが、所定の実行権限で動作し、前記ユーザを特定するユーザ特定情報と、前記ユーザにより所有される前記リソースへアクセスするための位置情報とを対応付けて記憶する記憶手段を備える情報処理装置の処理をコンピュータに実行させるプログラムにおいて、
前記リソースへのアクセスが前記位置情報を含んでリクエストされたとき、前記リクエストに含まれる位置情報に基づいて、前記記憶手段で対応付けられた前記ユーザ特定情報を取得し、取得した前記ユーザ特定情報により特定される前記ユーザに、前記プロセスの実行権限を変更する変更ステップと、
前記変更ステップの処理によって変更された前記プロセスの実行権限で、前記位置情報に基づいて前記リソースを取得する取得ステップと、
前記取得ステップの処理によって取得された前記リソースを、前記リクエストに対するレスポンスとして送信する処理を制御する送信制御ステップと、
前記取得ステップの処理によって取得される前記リソースが、前記変更ステップの処理によって変更された前記プロセスの実行権限をさらに変更する動的なリソースである場合、

前記プロセスの実行権限のさらなる変更を無効にする処理を行う処理ステップと、
前記取得ステップの処理によって取得された前記リソースの送信を行わせないで、エラーを表すレスポンスの送信を行わせるエラー送信制御ステップと
を含む処理をコンピュータに実行させるプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、情報処理装置および方法、並びにプログラムに関し、特に、ファイルのセキュリティを高めることができるようにする情報処理装置および方法、並びにプログラムに関する。

【背景技術】

【０００２】

UNIX（登録商標）およびUNIX系OS（Operating System）には、プロセスの実行権限を変更するシステムコールとして、実ユーザID（Identification）や実グループIDを設定（変更）するsetuid(), setgid()等のシステムコールがある。また、同様に、実効ユーザIDや実効グループIDを設定（変更）するseteuid(), setegid()等のシステムコールがある。

【０００３】

UNIXおよびUNIX系OSにおけるプロセスのうち、ユーザ毎に異なる実行権限で動作するものは、通常、管理者権限（root権限）で生成された後、上述したシステムコールを実行することで、実ユーザIDまたは実効ユーザID（実グループIDまたは実効グループID）が各ユーザ（一般ユーザ）に変更されて、動作する。例えば、シェルのプロセスは、ログインしたユーザによって、異なる実行権限で動作する。

【０００４】

なお、root権限で動作するプロセスが、実ユーザIDや実グループIDを変更するsetuid(), setgid()等のシステムコールを実行して、その実行権限が一般ユーザに遷移すると、これ以降、実行権限はrootに戻ることができない。

【０００５】

一方、root権限で動作するプロセスが、seteuid(), setegid()等のシステムコールを実行した場合、実ユーザID（実グループID）は変更されず、実効ユーザID（実効グループID）のみ変更されるため、実行権限はrootに戻ることができる。

【０００６】

ところで、Apache（Apache HTTP（HyperText Transfer Protocol） Server）等のウェブサーバ（ウェブサーバソフトウェア）におけるプロセスは、伝統的に一律専用の一般ユーザ（専用ユーザ）の実行権限で動作する。

【０００７】

このようなウェブサーバについて、例えば、図１に示されるように、同一の計算機（ウェブサーバ１１）に、それぞれのアカウントを持つ複数のユーザＡ，Ｂ，Ｃがウェブサイトを開設する場合、ユーザＡ，Ｂ，Ｃは、各自のディレクトリ配下に、各自がその所有者であるリソース（ファイルf_A，f_B，f_C）を配置する。そして、インターネット等のネットワークを介したパーソナルコンピュータ１２－１，１２－２等からのリソースへのアクセスのリクエストがあった場合、専用ユーザの実行権限で動作するプロセスP_1，P_2，P_3，P_4が、ファイルf_A，f_B，f_Cに対して読み出しや書込みなどのアクセスができるように、各ファイルについて、UNIXにおけるパーミッションモデル“owner/group/other”の“other”に、読み出し、書込み、実行等のアクセス権を付与する必要があった。

【０００８】

このように、“other”にアクセス権を付与した場合、ウェブサーバ１１を共用するユーザの中の悪意のあるユーザによって、ファイルを盗視されたり、改竄される恐れがある。例えば、悪意のあるユーザＢが、ウェブサーバ１１にログインして、「cp」（ファイル・ディレクトリのコピー）や「rm」（ファイル・ディレクトリの削除）等のコマンドを実

行することで、ファイルを盗視したり、改竄することができてしまう（図中、太点線矢印）。また、ユーザＢが、自身のウェブサイト（ファイルf_B）にスクリプトを含むようにし、そのスクリプトに「cp」や「rm」等のコマンドを実行させることで、ファイルを盗視したり、改竄することができてしまう（図中、太線矢印）。

【０００９】

なお、１つのプロセスの内部で、機能モジュール別にセキュリティ権限を設定することで、機能モジュール毎のファイルへのアクセスを制御するようにする手法がある（特許文献１参照）。

【先行技術文献】

【特許文献】

【００１０】

【特許文献１】特開２００６－３３１１３７号

【発明の概要】

【発明が解決しようとする課題】

【００１１】

しかしながら、特許文献１の手法では、リクエストに応じたプロセスの中の所定の機能モジュールが、ファイルの所有者に関わらず、そのファイルへアクセスできてしまい、ファイルが盗視されたり、改竄されるのを防ぐことができない。

【００１２】

本発明は、このような状況に鑑みてなされたものであり、他のユーザによってファイルが盗視・改竄されないようにするものである。

【課題を解決するための手段】

【００１３】

本発明の一側面の情報処理装置は、複数のユーザそれぞれにより所有されるリソースへアクセスするプロセスが、所定の実行権限で動作する情報処理装置であって、前記ユーザを特定するユーザ特定情報と、前記ユーザにより所有される前記リソースへアクセスするための位置情報とを対応付けて記憶する記憶手段と、前記リソースへのアクセスが前記位置情報を含んでリクエストされたとき、前記リクエストに含まれる位置情報に基づいて、前記記憶手段で対応付けられた前記ユーザ特定情報を取得し、取得した前記ユーザ特定情報により特定される前記ユーザに、前記プロセスの実行権限を変更する変更手段と、前記変更手段によって変更された前記プロセスの実行権限で、前記位置情報に基づいて前記リソースを取得する取得手段と、前記取得手段によって取得された前記リソースを、前記リクエストに対するレスポンスとして送信する処理を制御する送信制御手段とを備え、前記取得手段によって取得される前記リソースが、前記変更手段によって変更された前記プロセスの実行権限をさらに変更する動的なリソースである場合、前記取得手段は、前記プロセスの実行権限のさらなる変更を無効にする処理を行い、前記送信制御手段は、前記取得手段によって取得された前記リソースの送信を行わせないで、エラーを表すレスポンスの送信を行わせる。

【００１５】

前記プロセスは、前記情報処理装置の管理者の実行権限で起動させ、前記変更手段には、前記送信制御手段によって前記レスポンスが送信された後、前記プロセスの実行権限を前記管理者に戻させることができる。

【００１６】

前記変更手段には、再度、前記リソースへのアクセスがリクエストされたときに、前記プロセスの実行権限を管理者に戻させることができる。

【００１７】

前記記憶手段には、前記ユーザ特定情報および前記ユーザの属するグループを特定するグループ特定情報と、前記位置情報とを対応付けて予め記憶させることができる。

【００１８】

本発明の一側面の情報処理方法は、複数のユーザそれぞれにより所有されるリソースへ

アクセスするプロセスが、所定の実行権限で動作し、前記ユーザを特定するユーザ特定情報と、前記ユーザにより所有される前記リソースへアクセスするための位置情報とを対応付けて記憶する記憶手段を備える情報処理装置の情報処理方法であって、前記リソースへのアクセスが前記位置情報を含んでリクエストされたとき、前記リクエストに含まれる位置情報に基づいて、前記記憶手段で対応付けられた前記ユーザ特定情報を取得し、取得した前記ユーザ特定情報により特定される前記ユーザに、前記プロセスの実行権限を変更する変更ステップと、前記変更ステップの処理によって変更された前記プロセスの実行権限で、前記位置情報に基づいて前記リソースを取得する取得ステップと、前記取得ステップの処理によって取得された前記リソースを、前記リクエストに対するレスポンスとして送信する処理を制御する送信制御ステップと、前記取得ステップの処理によって取得される前記リソースが、前記変更ステップの処理によって変更された前記プロセスの実行権限をさらに変更する動的なリソースである場合、前記プロセスの実行権限のさらなる変更を無効にする処理を行う処理ステップと、前記取得ステップの処理によって取得された前記リソースの送信を行わせないで、エラーを表すレスポンスの送信を行わせるエラー送信制御ステップとを含む。

【００１９】

本発明の一側面のプログラムは、複数のユーザそれぞれにより所有されるリソースへアクセスするプロセスが、所定の実行権限で動作し、前記ユーザを特定するユーザ特定情報と、前記ユーザにより所有される前記リソースへアクセスするための位置情報とを対応付けて記憶する記憶手段を備える情報処理装置の処理をコンピュータに実行させるプログラムであって、前記リソースへのアクセスが前記位置情報を含んでリクエストされたとき、前記リクエストに含まれる位置情報に基づいて、前記記憶手段で対応付けられた前記ユーザ特定情報を取得し、取得した前記ユーザ特定情報により特定される前記ユーザに、前記プロセスの実行権限を変更する変更ステップと、前記変更ステップの処理によって変更された前記プロセスの実行権限で、前記位置情報に基づいて前記リソースを取得する取得ステップと、前記取得ステップの処理によって取得された前記リソースを、前記リクエストに対するレスポンスとして送信する処理を制御する送信制御ステップと、前記取得ステップの処理によって取得される前記リソースが、前記変更ステップの処理によって変更された前記プロセスの実行権限をさらに変更する動的なリソースである場合、前記プロセスの実行権限のさらなる変更を無効にする処理を行う処理ステップと、前記取得ステップの処理によって取得された前記リソースの送信を行わせないで、エラーを表すレスポンスの送信を行わせるエラー送信制御ステップとを含む処理をコンピュータに実行させる。

【００２０】

本発明の一側面においては、ユーザを特定するユーザ特定情報と、ユーザにより所有されるリソースへアクセスするための位置情報とが対応付けて記憶され、リソースへのアクセスが位置情報を含んでリクエストされたとき、リクエストに含まれる位置情報に基づいて、対応付けられたユーザ特定情報が取得され、取得したユーザ特定情報により特定されるユーザに、プロセスの実行権限が変更され、変更されたプロセスの実行権限で、位置情報に基づいてリソースが取得され、取得されたリソースを、リクエストに対するレスポンスとして送信する処理が制御され、取得されるリソースが、変更されたプロセスの実行権限をさらに変更する動的なリソースである場合、プロセスの実行権限のさらなる変更を無効にする処理が行われ、取得されたリソースの送信が行われないで、エラーを表すレスポンスの送信が行われる。

【発明の効果】

【００２１】

本発明の一側面によれば、他のユーザによってファイルが盗視・改竄されないようにすることが可能となる。

【図面の簡単な説明】

【００２２】

【図１】従来のウェブサーバについて説明する図である。

【図２】本発明の一実施の形態である情報処理装置としてのウェブサーバを含むネットワークシステムの構成例を示すブロック図である。
【図３】図２のウェブサーバのハードウェア構成例を示すブロック図である。
【図４】図２のウェブサーバの機能構成例を示すブロック図である。
【図５】プロセス実行権限変更処理について説明するフローチャートである。
【図６】実行権限情報について説明する図である。
【発明を実施するための形態】
【００２３】
以下、本発明の実施の形態について図を参照して説明する。
【００２４】
［ウェブサーバを含むネットワークシステムの構成例］
図２は、本発明の一実施の形態である情報処理装置としてのウェブサーバを含むネットワークシステムの構成例を示している。
【００２５】
図２において、ウェブサーバ１１１、およびパーソナルコンピュータ１１２－１乃至１１２－３は、インターネット１１３を介して相互に接続されている。ウェブサーバ１１１と、パーソナルコンピュータ１１２－１乃至１１２－３とは、HTTPに則り、相互に通信を行う。なお、以下において、パーソナルコンピュータ１１２－１乃至１１２－３のそれぞれについて、特に区別する必要がない場合は、単に、パーソナルコンピュータ１１２ということとする。
【００２６】
ウェブサーバ１１１は、パーソナルコンピュータ１１２からのリクエストに基づいて、そのリクエストに応じたHTML（HyperText Markup Language）や画像などのオブジェクトを、リクエストに対するレスポンスとして、パーソナルコンピュータ１１２に送信する。なお、ウェブサーバ１１１には、複数のウェブサイトが複数のユーザによって開設されている。
【００２７】
パーソナルコンピュータ１１２は、ユーザの操作に基づいて、ウェブサーバ１１１に対してリクエストを送信し、そのリクエストに応じたレスポンスであるHTMLや画像などのオブジェクトを、それぞれにおいて起動されるウェブブラウザに表示させる。
【００２８】
なお、図２においては、パーソナルコンピュータ１１２は、パーソナルコンピュータ１１２－１乃至１１２－３の３個であるものとしたが、実際には、本実施の形態は、より多くのパーソナルコンピュータ１１２を含むネットワークシステムに対して適用されるものとする。
【００２９】
また、図２においては、ウェブサーバ１１１とパーソナルコンピュータ１１２とは、インターネット１１３を介して接続されるものとしたが、イントラネットやローカルエリアネットワーク等、他のネットワークを介して接続されるようにしてもよい。
【００３０】
［ウェブサーバのハードウェア構成例］
次に、図３を参照して、ウェブサーバ１１１のハードウェア構成例について説明する。
【００３１】
図３に示されるように、CPU（Central Processing Unit）２０１、ROM（Read Only Memory）２０２、RAM（Random Access Memory）２０３及び入出力インタフェース２０５がバス２０４に接続されている。また、入力部２０６、出力部２０７、記録部２０８、通信部２０９及びドライブ２１０が入出力インタフェース２０５に接続されている。また、ドライブ２１０にはリムーバブルメディア２１１が接続されている。
【００３２】
CPU２０１は、ROM２０２、または記録部２０８に記録されているプログラムにしたがっ

て各種の処理を実行する。RAM２０３には、CPU２０１が実行するプログラムやデータなどが適宜記録される。これらのCPU２０１、ROM２０２、およびRAM２０３は、バス２０４により相互に接続されている。

【００３３】

入出力インタフェース２０５は、バス２０４を介して、CPU２０１に接続されている。入力部２０６は、キーボード、マウス、マイクロフォンなどで構成され、出力部２０７はディスプレイ、スピーカなどで構成されている。CPU２０１は、入力部２０６から入力される指令に対応して各種の処理を実行する。そして、CPU２０１は、実行処理の結果を出力部２０７に出力する。

【００３４】

記録部２０８は、例えばハードディスクからなり、CPU２０１が実行するプログラムや各種のデータを記録する。通信部２０９は、インターネット１１３（図２参照）やローカルエリアネットワークなどのネットワークを介して、パーソナルコンピュータ１１２を含む外部の装置と通信する。

【００３５】

また、ウェブサーバ１１１は、通信部２０９を介してプログラムを取得し、記録部２０８に記録してもよい。

【００３６】

ドライブ２１０は、磁気ディスク、光ディスク、光磁気ディスク、或いは半導体メモリなどのリムーバブルメディア２１１が装着されたとき、それらを駆動し、そこに記録されているプログラムやデータなどを取得する。取得されたプログラムやデータは、必要に応じて記録部２０８に転送され、記録される。

【００３７】

［ウェブサーバの機能構成例］

次に、図４を参照して、ウェブサーバ１１１の具体的な機能構成例について説明する。

【００３８】

図４のウェブサーバ１１１は、ネットワークI/F（Interface）３１１、リクエスト受信制御部３１２、実行権限情報取得部３１３、実行権限管理部３１４、プロセス実行権限変更部３１５、コンテンツ取得部３１６、コンテンツ記録部３１７、およびレスポンス送信制御部３１８から構成される。特に、リクエスト受信制御部３１２、実行権限情報取得部３１３、プロセス実行権限変更部３１５、コンテンツ取得部３１６、およびレスポンス送信制御部３１８は、ウェブサーバとしてのプログラムを実行するCPU２０１により実現される機能である。

【００３９】

ネットワークI/F３１１は、図３の通信部２０９に対応し、インターネット１１３を介して、パーソナルコンピュータ１１２と通信する。ネットワークI/F３１１は、パーソナルコンピュータ１１２からのリクエストを受信し、そのリクエストに応じたオブジェクトとしてのリソースを、リクエストに対するレスポンスとして、パーソナルコンピュータ１１２に送信する。

【００４０】

リクエスト受信制御部３１２は、パーソナルコンピュータ１１２からのリクエストをネットワークI/F３１１を介して取得する。リクエスト受信制御部３１２は、取得したリクエストに含まれる情報を、実行権限情報取得部３１３に供給する。

【００４１】

実行権限情報取得部３１３は、リクエスト受信制御部３１２からの情報に基づいて、ウェブサーバ１１１において起動するプロセスの実行権限を管理するための情報である実行権限情報を、実行権限管理部３１４から取得し、取得した実行権限情報をプロセス実行権限変更部３１５に供給する。

【００４２】

実行権限管理部３１４は、図３のRAM２０３または記録部２０８に対応し、ユーザによ

り予め設定された実行権限情報を記憶し、実行権限情報取得部３１３からの要求に応じた実行権限情報を、適宜、実行権限情報取得部３１３に供給する。実行権限管理部３１４には、後で図６を用いて詳述するように、ユーザを特定するユーザ特定情報（ユーザIDおよびグループID）とユーザにより所有されるリソースへアクセスするための位置情報（ドメイン名）とが対応付けられて記憶（登録）されている。実行権限管理部３１４は、本発明の記憶手段に相当する。

【００４３】

プロセス実行権限変更部３１５は、実行権限情報取得部３１３から供給された実行権限情報に基づいて、ウェブサーバ１１１において起動しているプロセスの実行権限を変更する。なお、実行権限情報取得部３１３及びプロセス実行権限変更部３１５は、本発明の変更手段に相当する。

【００４４】

コンテンツ取得部３１６は、プロセス実行権限変更部３１５によって変更された実行権限で、パーソナルコンピュータ１１２からのリクエストに応じて、コンテンツ記録部３１７から、ウェブサーバ１１１が保管しているリソースとしてのコンテンツファイルを取得する。コンテンツ取得部３１６は、取得したコンテンツファイルを、レスポンス送信制御部３１８に供給する。コンテンツ取得部３１６は、本発明の取得手段に相当する。

【００４５】

また、コンテンツ取得部３１６は、コンテンツ判定部３３１を備えており、コンテンツ判定部３３１は、コンテンツ記録部３１７から取得したコンテンツファイルが、プロセスの実行権限をさらに変更する動的なコンテンツファイルであるか否かを判定する。コンテンツ判定部３３１は、本発明の判定手段に相当する。

【００４６】

コンテンツ記録部３１７は、図３の記録部２０８に対応し、種々のコンテンツファイルを記録している。より具体的には、コンテンツ記録部３１７は、ウェブサーバ１１１内にそれぞれのウェブサイトを開設した複数のユーザ毎のディレクトリ配下にコンテンツファイルを配置するように記録している。コンテンツファイルは、そのファイル毎に定義された許可情報によって、ユーザに対するアクセス権が設定されている。

【００４７】

レスポンス送信制御部３１８は、コンテンツ取得部３１６からのコンテンツファイルを、パーソナルコンピュータ１１２からのリクエストに対するレスポンスとして、ネットワークI/F３１１に送信させる制御を行う。なお、レスポンス送信制御部３１８は、本発明の送信制御手段に相当する。

【００４８】

［ウェブサーバによるプロセス実行権限変更処理］

次に、図５のフローチャートを参照して、ウェブサーバ１１１によるプロセス実行権限変更処理について説明する。

【００４９】

なお、前提として、ウェブサーバ１１１におけるプロセスは、root権限で起動するものとする。

【００５０】

ステップＳ１１において、ネットワークI/F３１１は、パーソナルコンピュータ１１２から送信されてくる、コンテンツファイル（リソース）へのアクセスのリクエストを受信する。パーソナルコンピュータ１１２から送信されてくるリクエストには、コンテンツファイルの所在を特定するためのURL（Uniform Resource Locator）や、パーソナルコンピュータ１１２において起動されるウェブブラウザを介して入力されたログイン名およびパスワード等が含まれる。なお、URLまたはこれに含まれるドメイン名（ホスト名）は、本発明の位置情報に対応する。リクエスト受信制御部３１２は、ネットワークI/F３１１によって受信されたリクエストを取得し、そのリクエストに含まれるURLを、実行権限情報取得部３１３に供給する。例えば、リクエスト受信制御部３１２は、リクエストに含まれ

るURLである“http://aaa.com/main.html”を、実行権限情報取得部３１３に供給する。このとき、リクエスト受信制御部３１２は、リクエストにログイン名およびパスワードが含まれる場合、それらに基づいて、パーソナルコンピュータ１１２の使用者を認証する。

【００５１】

ステップＳ１２において、実行権限情報取得部３１３は、パーソナルコンピュータ１１２からのリクエストに含まれるURLのドメイン名（ホスト名）（例えば、“aaa.com”）が、実行権限管理部３１４が記憶している実行権限情報に登録（記憶）されているか否かを判定する。

【００５２】

ここで、図６を参照して、実行権限情報取得部３１３が記憶している実行権限情報の例について説明する。

【００５３】

図６においては、実行権限情報として、ドメイン名と、ユーザIDおよびグループIDとが対応付けられている。より具体的には、ドメイン名“aaa.com”と、ユーザID“1234”およびグループID“111”とが対応付けられており、ドメイン名“bbb.net”と、ユーザID“2345”およびグループID“222”とが対応付けられており、ドメイン名“zzz.jp”と、ユーザID“9999”およびグループID“999”とが対応付けられている。

【００５４】

図６の実行権限情報において、ドメイン名は、ウェブサーバ１１１においてコンテンツファイル（リソース）が記録（保管）されている位置（場所）を示しており、ユーザIDおよびグループIDは、そのコンテンツファイルの所有者（ユーザ）およびその所有者が属するグループを特定する情報である。ユーザIDおよびグループIDは、本発明のユーザ特定情報及びグループ特定情報にそれぞれ対応する。

【００５５】

なお、実行権限情報は、各ユーザによってウェブサイトが開設され、コンテンツファイルが作成されたときに追加登録されてもよいし、ユーザによって任意のタイミングで追加登録されてもよい。

【００５６】

図５のフローチャートに戻り、ステップＳ１２において、リクエストに含まれるURLのドメイン名が実行権限情報に登録されていないと判定された場合、実行権限情報取得部３１３は、その旨を表す情報をコンテンツ取得部３１６に供給し、処理は、後述するステップＳ２０に進む。

【００５７】

一方、ステップＳ１２において、リクエストに含まれるドメイン名が実行権限情報に登録されていると判定された場合、ステップＳ１３において、実行権限情報取得部３１３は、リクエストに含まれるURLのドメイン名（例えば、“aaa.com”）に対応するユーザID（例えば、“1234”）およびグループID（例えば、“111”）を取得し、リクエストに含まれるURLとともに、プロセス実行権限変更部３１５に供給する。

【００５８】

ステップＳ１４において、プロセス実行権限変更部３１５は、実行権限情報取得部３１３からのユーザIDおよびグループIDに基づいて、プロセスの実行権限を変更する。より具体的には、例えば、プロセス実行権限変更部３１５は、seteuid(1234), setegid(111)のシステムコールを実行し、実効ユーザIDおよび実効グループIDを変更することで、プロセスの実行権限を、rootから、リクエストされているファイル（main.html）の所有者（以下、ユーザＡともいう）に変更し、リクエストに含まれるURL“http://aaa.com/main.html”をコンテンツ取得部３１６に供給する。

【００５９】

ステップＳ１５において、コンテンツ取得部３１６は、プロセス実行権限変更部３１５によって変更された実行権限で、パーソナルコンピュータ１１２からのリクエストに含まれるURLのドメイン名（ホスト名）に基づいて、コンテンツ記録部３１７から、コンテン

ツファイルを取得する。より具体的には、例えば、コンテンツ取得部３１６は、プロセス実行権限変更部３１５からのURLのドメイン名（ホスト名）“http://aaa.com/main.html”に基づいて、コンテンツ記録部３１７から、コンテンツファイルmain.htmlを取得する。

【００６０】

ここで、コンテンツファイルは、ファイルパーミッションという、ファイル毎に定義された、読み出し、書込み、実行等のアクセスについての許可情報によって、所定のユーザやグループに対するアクセス権が設定されている。この場合、コンテンツファイルmain.htmlについては、ファイルパーミッションによって、その所有者であるユーザＡのみに対して、読み出し、書込み、実行が可能であるように設定されている。このとき、プロセスの実行権限はユーザＡにあるので、コンテンツ取得部３１６は、コンテンツファイルmain.htmlを取得することができる。

【００６１】

ステップＳ１６において、コンテンツ判定部３３１は、コンテンツ取得部３１６が取得したコンテンツファイルが、プロセスの実行権限をさらに変更する動的なコンテンツファイルであるか否かを判定する。より具体的には、コンテンツ判定部３３１は、取得されたコンテンツファイルが、CGI（Common Gateway Interface）等を利用した、スクリプトを含むコンテンツファイルであるか否かを判定する。このようなスクリプトを含むコンテンツファイルを動的なコンテンツファイルという。

【００６２】

ステップＳ１６において、取得したコンテンツファイルが、動的なコンテンツファイルであると判定された場合、ステップＳ１７において、コンテンツ判定部３３１は、そのコンテンツファイルが、実ユーザIDや実グループIDを変更するsetuid(), setgid()系のシステムコールを実行するか否かを判定する。

【００６３】

ステップＳ１７において、動的なコンテンツファイルが、setuid(), setgid()系のシステムコールを実行しないと判定されたか、または、ステップＳ１６において、取得したコンテンツファイルが、動的なコンテンツファイルでないと判定された場合、コンテンツ取得部３１６は、取得したコンテンツファイルをレスポンス送信制御部３１８に供給し、処理はステップＳ１８に進む。

【００６４】

ステップＳ１８において、レスポンス送信制御部３１８は、コンテンツ取得部３１６からのコンテンツファイルを、パーソナルコンピュータ１１２からのリクエストに対するレスポンスとして、ネットワークI/F３１１に送信させる制御を行う。また、レスポンス送信制御部３１８は、レスポンスを送信した旨を表す情報を、プロセス実行権限変更部３１５に供給する。

【００６５】

これにより、パーソナルコンピュータ１１２のウェブブラウザには、リクエストに応じたHTMLや画像などのオブジェクトが表示される。

【００６６】

一方、ステップＳ１７において、動的なコンテンツファイルが、setuid(), setgid()系のシステムコールを実行すると判定された場合、ステップＳ１９において、コンテンツ判定部３３１は、setuid(), setgid()系のシステムコールを無効にする。

【００６７】

ステップＳ１９の処理の後、または、ステップＳ１２において、リクエストに含まれるURLのドメイン名が実行権限情報に登録されていないと判定された場合、ステップＳ２０において、コンテンツ取得部３１６は、エラーが発生したことを示すエラーレスポンスを表示させるためのコンテンツファイルを、コンテンツ記録部３１７から取得し、レスポンス送信制御部３１８に供給する。レスポンス送信制御部３１８は、コンテンツ取得部３１６からのコンテンツファイルを、ネットワークI/F３１１に送信させるとともに、レスポ

ンスを送信した旨を表す情報を、プロセス実行権限変更部３１５に供給する。このとき、レスポンス送信制御部３１８は、ステップＳ１５でコンテンツ取得部３１６によりコンテンツファイルmain.htmlが取得された場合には、ネットワークI/F３１１に対して、その取得されたコンテンツファイルmain.htmlを送信させる制御を行わず、エラーが発生したことを示すエラーレスポンスを表示させるためのコンテンツファイルのみを送信させる制御を行う。

【００６８】

これにより、パーソナルコンピュータ１１２のウェブブラウザには、「Sorry, Not Found.」や、「要求されたページは見つかりません」等のコメントを含むエラーレスポンスが表示される。

【００６９】

ステップＳ２１において、プロセス実行権限変更部３１５は、レスポンス送信制御部３１８からの情報に基づいて、実行権限をrootに戻す。より具体的には、プロセス実行権限変更部３１５は、seteuid(0), setegid(0)のシステムコールを実行し、実効ユーザIDおよび実効グループIDを変更することで、プロセスの実行権限を、ユーザＡからrootに変更する。

【００７０】

なお、ステップＳ２１の処理は、ステップＳ１２において、リクエストに含まれるドメイン名が実行権限情報に登録されていないと判定された場合には、プロセスの実行権限は変更されていないので、実行されない。

【００７１】

以上の処理によれば、ウェブサーバにおいて、リソースへのアクセスのリクエストに応じて、プロセスの実行権限をリソースの所有者に変更し、その実行権限の下で、リクエストに含まれるURLで指定されるリソースのみへアクセスできる。したがって、アクセスの対象となるリソースの所有者以外のユーザ権限では、そのリソースへはアクセスできないので、他のユーザによってファイルが盗視されたり、改竄されるのを防ぐことができる。

【００７２】

また、CGI等を利用した、スクリプトを含むコンテンツファイルにおいては、setuid(), setgid()系のシステムコールを実行することができ、悪意のあるユーザに実行権限を取られてしまう可能性があるが、以上の処理によれば、setuid(), setgid()系のシステムコールを実行できるのは、ウェブサーバ１１１のプログラムのみであるので、悪意のあるユーザに実行権限を取られてしまう可能性を低減することができる。

【００７３】

なお、以上においては、レスポンスが送信された後に、プロセスの実行権限をrootに戻すようにしたが、ウェブブラウザから、再度、コンテンツファイルへのアクセスのリクエストを受信して（ステップＳ１１）から、一般ユーザに実行権限が変更される（ステップＳ１４）までの間に、プロセスの実行権限をrootに戻すようにしてもよい。

【００７４】

上述した一連の処理は、ハードウェアにより実行させることもできるし、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、例えば、UNIXおよびUNIX系OSで起動する、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、プログラム記録媒体からインストールされる。

【００７５】

なお、本明細書において、プログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【００７６】

また、本明細書において、システムとは、複数の装置により構成される装置全体を表す

ものである。

【００７７】

なお、本発明の実施の形態は、上述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において種々の変更が可能である。

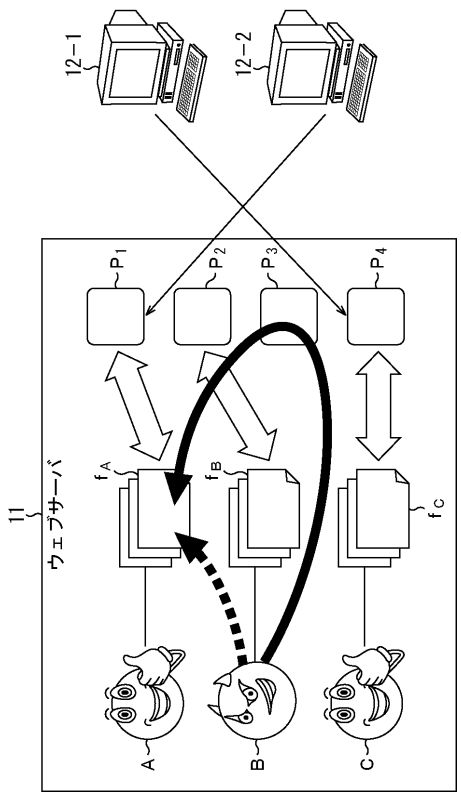
【符号の説明】

【００７８】

１１１　ウェブサーバ，　２０１　CPU，　２０３　RAM，　２０８　記録部，　２０９　通信部，　３１１　ネットワークI/F，　３１２　リクエスト受信制御部，　３１３　実行権限情報取得部，　３１４　実行権限管理部，　３１５　プロセス実行権限変更部，　３１６　コンテンツ取得部，　３１７　コンテンツ記録部，　３１８　レスポンス送信制御部，　３３１　コンテンツ判定部

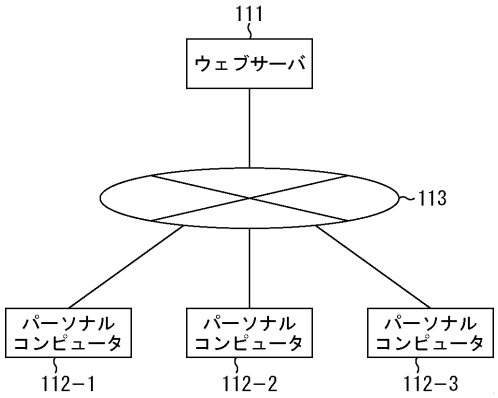
【図１】

図1

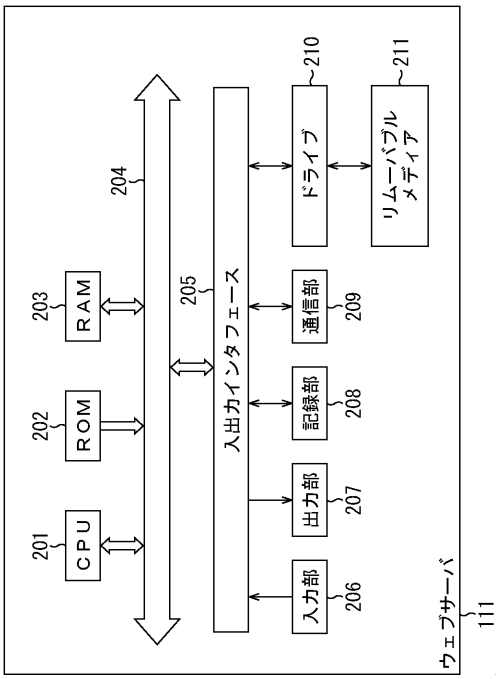


【図２】

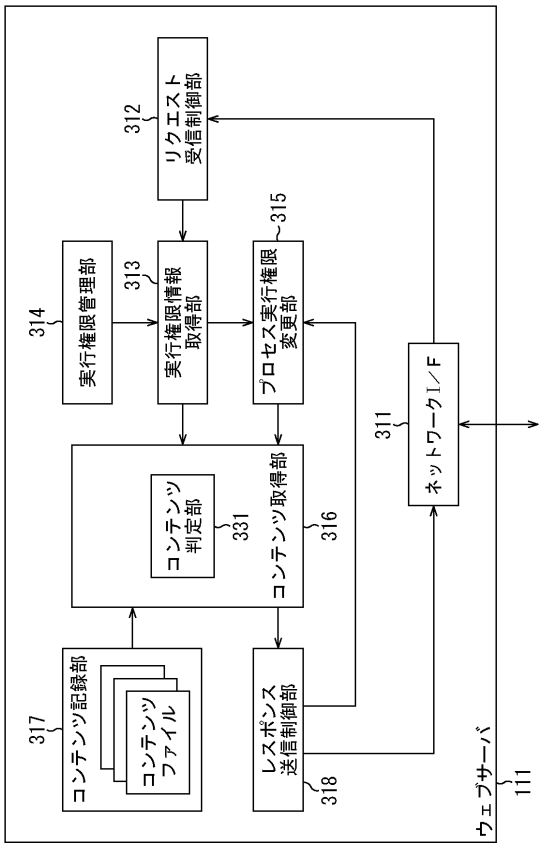
図2



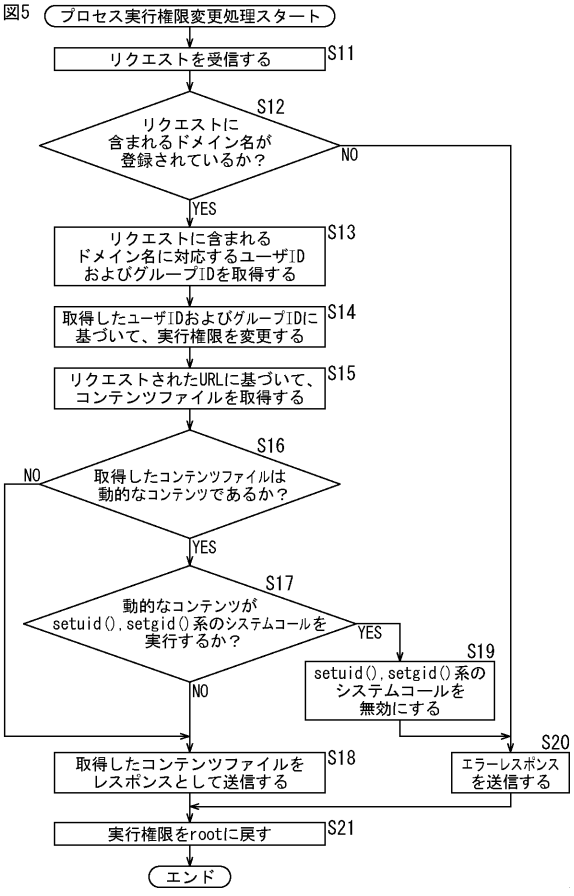
【図３】
図3



【図４】
図4



【図５】
図5



【図６】
図6

ドメイン名	ユーザID	グループID
aaa.com	1234	111
bbb.net	2345	222
・・・	・・・	・・・
zzz.jp	9999	999

フロントページの続き

(56)参考文献 原 大輔 DAISUKE HARA, Ｈａｒａｃｈｅ：ファイル所有者の権限で動作するWWWサーバ Harache: A WWW Server Running with the Authority of the File Owner, 情報処理学会論文誌 第４６巻 第１２号 IPSJ Journal, 日本, 社団法人情報処理学会 Information Processing Society of Japan, ２００５年１２月 5日, 第46巻, P.3127-3137
ジョリツ ウィリアム フレデリック William Frederick Jolitz, ３８６ＢＳＤ カーネル ソースコードの秘密 初版 Source Code Secrets The Basic Kernel, 株式会社アスキー ASCII Corporation, １９９８年１２月３１日, 第1版, P.372-374
原 大輔 Daisuke HARA, Ｈｕｓｓａ：スケーラブルかつセキュアなサーバアーキテクチャ, ＦＩＴ２００９ 第８回情報科学技術フォーラム 講演論文集 第１分冊 査読付き論文・一般論文 モデル・アルゴリズム・プログラミング ソフトウェア ハードウェア・アーキテクチャ Forum on Information Technology 2009, ２００９年 8月２０日, P.81-84
原 大輔 Daisuke HARA, ファイル所有者のユーザ権限で動作するＨＴＴＰサーバの設計と実現, 第６６回（平成１６年）全国大会講演論文集（１） アーキテクチャ ソフトウェア科学・工学, ２００４年 3月 9日, P.1-101～1-102

(58)調査した分野(Int.Cl., ＤＢ名)
Ｇ０６Ｆ ２１