(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2007-280096
(P2007-280096A)
(43)公開日　平成19年10月25日(2007.10.25)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 11/34	(2006.01)	G06F	11/34	A	5B017
G06F 21/24	(2006.01)	G06F	12/14	560B	5B042
G06F 12/00	(2006.01)	G06F	12/00	531J	5B082
		G06F	12/00	537A	

審査請求 未請求　請求項の数 10　ＯＬ　（全 18 頁）

(21)出願番号　特願2006-106172 (P2006-106172)
(22)出願日　平成18年4月7日 (2006.4.7)

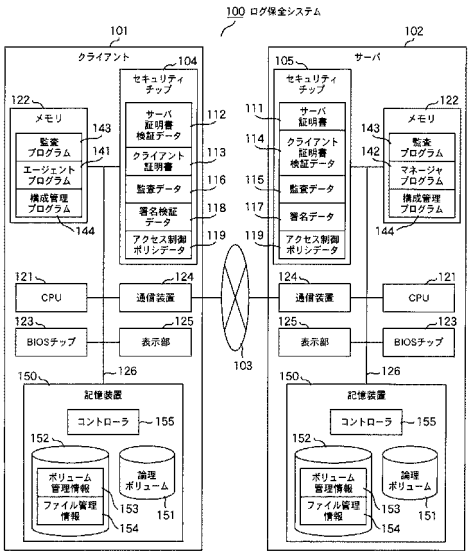
(71)出願人　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　110000350
ポレール特許業務法人
(72)発明者　甲斐　賢
神奈川県川崎市麻生区王禅寺１０９９番地
株式会社日立製作所システム開発研究所内
(72)発明者　荒井　正人
神奈川県川崎市麻生区王禅寺１０９９番地
株式会社日立製作所システム開発研究所内

最終頁に続く

(54)【発明の名称】ログ保全方法、プログラムおよびシステム

(57)【要約】
【課題】クライアントで取得し保存したログファイルの更新を防止すると共に、そのログファイルの書き込み領域を安全かつ効率的に再利用する。
【解決手段】エージェントプログラム１４１はログファイルを記憶装置１５０に保存する。記憶装置１５０は、ボリューム管理情報１５３に従って記憶装置１５０へのアクセスを制御することで、ログファイルの更新を防止する。マネージャプログラム１４２は、エージェントプログラム１４１と通信し、ログファイルの回収を行う。回収が完了した後は、マネージャプログラム１４２がログ削除メッセージを、セキュリティチップ１０５を使って署名し、エージェントプログラム１４１がセキュリティチップ１０４を使って署名を検証し、正しいログ削除要求であることを確認し、ログファイルを保護していたボリューム管理情報１５３を書き換え、保護を解除する。
【選択図】図１

図 1



【特許請求の範囲】
【請求項１】
クライアントが該クライアントで実行されたユーザ操作やデータアクセスの履歴をログファイルに記録し、サーバがネットワークを介して前記ログファイルを回収して保存するログ保全方法において、
前記クライアントは、
前記ログファイルの書き込み要求に対し、その記憶装置上の前記ログファイルの書き込み領域の属性が書き込み可能であれば、前記ログファイルを当該書き込み領域に記録するとともに、当該書き込み領域の属性を書き込み禁止に更新し、
書き込まれた前記ログファイルを読み出して前記サーバへ送信し、
前記サーバは、
前記ログファイルを受信して自身の記憶装置に書き込み、
前記ログファイルの削除を指示するメッセージを前記クライアントへ送信し、
前記クライアントは、前記メッセージを受信し、前記書き込み領域の属性を書き込み可能に更新することを特徴とするログ保全方法。
【請求項２】
前記クライアントの前記記憶装置は、前記書き込み領域の属性を保持し、前記ログファイル書き込みのためのＩ／Ｏ要求に応答し、前記記憶装置自身が当該書き込み領域の属性を書き込み不可に更新して、前記ログファイルを当該書き込み領域に記録することを特徴とする請求項１記載のログ保全方法。
【請求項３】
前記サーバは、前記メッセージをメッセージ発行ごとに異なる内容とし、前記メッセージを受信した前記クライアントは、前記メッセージが正当な場合に前記書き込み領域の属性を書き込み可能に更新することを特徴とする請求項１記載のログ保全方法。
【請求項４】
クライアントが該クライアントで実行されたユーザ操作やデータアクセスの履歴をログファイルに記録し、サーバがネットワークを介して前記ログファイルを回収して保存するログ保全方法において、
前記クライアントは、
改ざんがないことを確認された許可プログラムが記憶装置上のログ書き込み領域への前記ログファイルの書き込みを要求するものであれば、前記ログファイルを当該書き込み領域に記録し、
書き込まれた前記ログファイルを読み出して前記サーバへ送信し、
前記サーバは、
前記ログファイルを受信して自身の記憶装置に書き込み、
前記ログファイルの削除を指示するメッセージを前記クライアントへ送信し、
前記クライアントは、前記メッセージを受信し、前記ログ書き込み領域上の前記ログファルを削除することを特徴とするログ保全方法。
【請求項５】
前記クライアントのセキュリティチップは、前記許可プログラムの識別子と保護対象の前記ログ書き込み領域に関する情報とを保持し、前記ログファイルが記録された前記ログ書き込み領域に関する情報を保持することを特徴とする請求項４記載のログ保全方法。
【請求項６】
前記サーバは、前記メッセージをメッセージ発行ごとに異なる内容とし、前記メッセージを受信した前記クライアントは、前記メッセージが正当な場合に前記ログファイルを削除することを特徴とする請求項４記載のログ保全方法。
【請求項７】
計算機内で実行されたユーザ操作やデータアクセスの履歴をログファイルに記録するクライアントと、ネットワークを介して前記ログファイルを回収して保存するサーバとを有するログ保全システムにおいて、

前記クライアントは、前記ログファイルの書き込み要求に対し、その記憶装置上の前記ログファイルの書き込み領域の属性が書き込み可能であれば、前記ログファイルを当該書き込み領域に記録するとともに、当該書き込み領域の属性を書き込み禁止に更新する手段と、
書き込まれた前記ログファイルを読み出して前記サーバへ送信する手段と、
前記サーバから前記ログファイルの削除を指示するメッセージを受信し、前記書き込み領域の属性を書き込み可能に更新する手段とを有し、
前記サーバは、
前記ログファイルを受信して自身の記憶装置に書き込む手段と、
前記メッセージを前記クライアントへ送信する手段とを有することを特徴とするログ保全システム。

【請求項８】
計算機内で実行されたユーザ操作やデータアクセスの履歴をログファイルに記録するクライアントと、ネットワークを介して前記ログファイルを回収して保存するサーバとを有するログ保全システムにおいて、
前記クライアントは、改ざんがないことを確認された許可プログラムが記憶装置上のログ書き込み領域への前記ログファイルの書き込みを要求するものであれば、前記ログファイルを当該書き込み領域に記録する手段と、
書き込まれた前記ログファイルを読み出して前記サーバへ送信する手段と、
前記サーバから前記ログファイルの削除を指示するメッセージを受信し、前記ログ書き込み領域上の前記ログファイルを削除する手段とを有し、
前記サーバは、前記ログファイルを受信して自身の記憶装置に書き込む手段と、
前記メッセージを前記クライアントへ送信する手段とを有することを特徴とするログ保全システム。

【請求項９】
クライアント側のコンピュータに該クライアントで実行されたユーザ操作やデータアクセスの履歴をログファイルに記録し、サーバ側のコンピュータにネットワークを介して前記ログファイルを回収して保存する手順を実行させるためのプログラムであって、
前記クライアントに、
前記ログファイルの書き込み要求に対し、その記憶装置上の前記ログファイルの書き込み領域の属性が書き込み可能であれば、前記ログファイルを当該書き込み領域に記録するとともに、当該書き込み領域の属性を書き込み禁止に更新し、
書き込まれた前記ログファイルを読み出して前記サーバへ送信し、
前記サーバから前記ログファイルの削除を指示するメッセージを受信し、前記書き込み領域の属性を書き込み可能に更新する手順を実行させ、
前記サーバに、
前記ログファイルを受信して自身の記憶装置に書き込み、
前記メッセージを前記クライアントへ送信する手順を実行させるためのプログラム。

【請求項１０】
クライアント側のコンピュータに該クライアントで実行されたユーザ操作やデータアクセスの履歴をログファイルに記録し、サーバ側のコンピュータにネットワークを介して前記ログファイルを回収して保存する手順を実行させるためのプログラムであって、
前記クライアントに、改ざんがないことを確認された許可プログラムが記憶装置上のログ書き込み領域への前記ログファイルの書き込みを要求するものであれば、前記ログファイルを当該書き込み領域に記録し、
書き込まれた前記ログファイルを読み出して前記サーバへ送信し、
前記サーバから前記ログファイルの削除を指示するメッセージを受信し、前記ログ書き込み領域上の前記ログファイルを削除する手順を実行させ、
前記サーバに、前記ログファイルを受信して自身の記憶装置に書き込み、
前記メッセージを前記クライアントへ送信する手順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、クライアントで取得したログをサーバで回収するログ保全技術に関する。
【背景技術】
【０００２】
個人情報保護法の完全施行や日本版ＳＯＸ法（Ｓａｒｂａｎｅｓ－Ｏｘｌｅｙ法、企業改革法）の制定予定を受け、セキュリティ対策の一つとして、クライアントＰＣにおける操作ログやデータアクセスログなどを取得し保管することが求められるようになってきた。クライアントで上記ログを取得することにより、もし個人情報の漏えいが発覚したときには、個人情報を漏えいした可能性の高いクライアントの絞り込みや、例えば電子メール、USBフラッシュメモリ、印刷などの漏えい経路を追跡することができる。また上記ログを取得することにより、決められたセキュリティポリシ以外の操作をクライアントで行っていないことを外部監査人に証明するといった法令遵守の点でも有用である。
【０００３】
クライアントで取得したログはクライアントで保管することも可能であるが、ログを保全しなければならない点と、クライアントの場合リソースが限られていることが多い点からすると、上記ログをサーバで回収することが望ましい。しかし、クライアントは可搬であることも多く、クライアントを利用するときに必ずしもサーバと接続されているとは限らない。そのため、クライアントで取得したログをサーバで回収するまでにクライアントにローカルで保管するときの保全が必要となる。とくに一度書き込んだログを勝手に更新されないことが必要となる。
【０００４】
このような一度書き込んだデータの更新を防止するために、近年はＷＯＲＭ（Ｗｒｉｔｅ　Ｏｎｃｅ　Ｒｅａｄ　Ｍａｎｙ）という技術が知られている。ＷＯＲＭとは、一度記録したデータは更新を行うことができず、参照のみ行える、データの性質である。以下、ＷＯＲＭの性質を持つデータを、ＷＯＲＭデータと呼ぶ。特許文献１によれば、２つのＷＯＲＭ記憶装置においてリモートコピーを行う時、対象となるデータがＷＯＲＭデータであるか否かを意識してリモートコピーを行う方法が開示されている。この方法を利用すれば、クライアントでログをローカルにＷＯＲＭデータとして書き出すことによって、クライアントで保管する間のログの改ざんを防止でき、さらにサーバへのリモートコピー後もＷＯＲＭ属性が継承されることにより、サーバにコピーしたログの改ざん防止まで実現することができる。このようなＷＯＲＭ属性の設定は、管理端末から手動で行うものである。
【０００５】
【特許文献１】特開２００５－３３９１９１号公報
【発明の開示】
【発明が解決しようとする課題】
【０００６】
しかしながら、特許文献１による方法では、クライアントで取得したログをサーバで回収した後のことまで考慮されていなかった。つまり、ログをサーバに回収した後にはクライアントにログを残し続ける必要はなく、もしログを残し続けた場合にはクライアントのＷＯＲＭ記憶装置を圧迫してしまう。またＷＯＲＭ属性を解除するには、管理端末から手動で解除を行う必要があり、手間がかかると共に操作ミスがあった場合にログの改ざんにつながるおそれがある。
【０００７】
以上のように、従来技術においては、クライアントで取得したログを保全してサーバで

回収したとしても、クライアントのリソースを圧迫することになり、また管理端末の操作ミスが原因で起こるログ改ざんを防止することができなかった。

【０００８】

そこで、本発明の目的は、クライアントで取得したログをサーバで回収する場合に、クライアント側のログ記憶領域を効率的かつ安全に再利用することが可能な、ログ保全技術を提供することにある。

【課題を解決するための手段】

【０００９】

本発明は、クライアント側のユーザ操作やデータアクセスを監視し、記録したログファイルを、ネットワークを介してサーバに回収してサーバで保存するクライアント・サーバ型システムにおいて、クライアントは、ローカルに記録するログファイルの更新を防止し、サーバにログファイルを回収した後に、ローカルに記録したログファイルを削除する。サーバは、クライアントから回収したログファイルを自身の記憶装置に書き込んだ後に、クライアントにログファイルの削除を要求する。

【発明の効果】

【００１０】

本発明によれば、クライアントのログファイル書き込み領域を安全かつ効率的に再利用できる。

【発明を実施するための最良の形態】

【００１１】

以下、本発明の実施形態について、適宜、図面を参照しながら詳しく説明する。

【実施例１】

【００１２】

図１は、本発明の実施形態に係るログ保全システムの全体構成を示した図である。図１に示すように、ログ保全システム１００は、クライアント１０１、サーバ１０２を含んで構成され、クライアント１０１とサーバ１０２はネットワーク１０３を介して接続される。ネットワーク１０３は通信を可能とする回線であれば形態を問わず、ＴＣＰ／ＩＰネットワーク、ＩＳＤＮ回線、無線ＬＡＮ通信などのいずれであっても良い。なお、ログ保全システム１００は、例えば、企業内情報システムにおけるクライアント統合管理システムや、コールセンタにおけるオペレータ端末管理システムなどに適用される。

【００１３】

図１はまた、クライアント１０１のブロック構成も示している。クライアント１０１は、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）１２１と、半導体メモリのＲＡＭなどのメモリ１２２と、電源をオフにしても記憶されたデータが保存される記憶装置１５０と、ネットワーク１０３と通信を行う通信装置１２４と、クライアント１０１の電源がオンになった直後の起動処理を行うＢＩＯＳ（Ｂａｓｉｃ Ｉｎｐｕｔ／Ｏｕｔｐｕｔ Ｓｙｓｔｅｍ）チップ１２３と、ＬＣＤ（Ｌｉｑｕｉｄ Ｃｒｙｓｔａｌ Ｄｉｓｐｌａｙ）などの表示部１２５と、ＴＣＧ（Ｔｒｕｓｔｅｄ Ｃｏｍｐｕｔｉｎｇ Ｇｒｏｕｐ）の提唱するＴＰＭ（Ｔｒｕｓｔｅｄ Ｐｌａｔｆｏｒｍ Ｍｏｄｕｌｅ）チップなど、耐タンパ性を備えた記憶領域を有し、チップごとに固有のＩＤが記録されているセキュリティチップ１０４などを含み、さらに、これらの機構がバス１２６を介して相互に接続されて構成される。ここで、ＢＩＯＳチップ１２３には、バス１２６に接続された機器（内蔵機器や周辺機器）を検出し、これらの機器を制御するプログラム群（ＢＩＯＳ）が格納されている。

【００１４】

さらに記憶装置１５０は、コントローラ１５５により記憶装置１５０の動作が制御される。また記憶装置１５０内の記憶領域は、１つ以上の論理ボリュームに分割される。論理ボリューム１５１は、複数の論理ボリュームのうちの一つである。論理ボリュームへのアクセスを管理するボリューム管理情報１５３は、記憶装置１５０内の記憶領域１５２に記録される。本実施形態では、ボリューム管理情報１５３は、記憶装置１５０内の記憶領域

１５２に記録するとしたが、コントローラ１５５のフラッシュメモリ等、記憶領域１５２以外に記録しても良い。

【００１５】

コントローラ１５５は、ボリューム管理情報１５３を用いて論理ボリュームへのＩ／Ｏ要求を制御する。また、ファイル管理情報１５４は、後述する構成管理プログラム１４４によってアクセスされる情報である。

【００１６】

さらにセキュリティチップ１０４は、後述するサーバ証明書１１１を検証するためのサーバ証明書検証データ１１２と、サーバ１０２にクライアント１０１を識別・認証してもらうためのクライアント証明書１１３と、後述するエージェントプログラム１４１と後述する構成管理プログラム１４４のプログラムファイルのハッシュ値や、バス１２６に接続された機器情報などの監査データ１１６と、後述する署名データ１１７で署名されたメッセージを検証するための署名検証データ１１８と、記憶装置１５０へのファイルアクセスを制御するためのポリシ（又はポリシー）をあらわすアクセス制御ポリシデータ１１９を保持する。これらのデータは、セキュリティチップ１０４の耐タンパ性により、所定の手順以外によるアクセスから保護される。なお、アクセス制御ポリシデータ１１９は、実施例１では使用しない。

【００１７】

以上のように構成されたクライアント１０１では、監査プログラム１４３、エージェントプログラム１４１、構成管理プログラム１４４がメモリ１２２にロードされ、ＣＰＵ１２１が上記したプログラム群を実行する。

【００１８】

監査プログラム１４３は、エージェントプログラム１４１と構成管理プログラム１４４が改ざんされていないことを確認するプログラムである。

【００１９】

エージェントプログラム１４１は、クライアント１０１でのユーザ操作やデータアクセスを監視し、監視結果をログとして記憶装置１５０に記録すると共に、記録されたログをサーバ１０２に送信するプログラムである。またエージェントプログラム１４１は、ログを記憶装置１５０に書き出すときには、ＷＯＲＭ属性のついたボリュームに書き出すようにプログラムされている。

【００２０】

構成管理プログラム１４４は、記憶装置１５０へのファイルアクセスを監視すると共に、ファイル管理情報１５４を管理するプログラムである。構成管理プログラム１４４は、クライアント１０１に搭載されるファイルシステムの一部を構成する。

【００２１】

さらに図１はまた、サーバ１０２のブロック構成も示している。詳細な説明を省略するが、サーバ１０２もクライアント１０１とほぼ同様の構成となる。ただし、相違点として、クライアント１０１で取得したログを回収するためのマネージャプログラム１４２の機能を備える。またセキュリティチップ１０５は、クライアント１０１にサーバ１０２を識別・認証してもらうためのサーバ証明書１１１と、クライアント証明書１１３を検証するためのクライアント証明書検証データ１１４と、マネージャプログラム１４２や構成管理プログラム１４４のプログラムファイルのハッシュ値や、バス１２６に接続された機器情報のような監査データ１１５と、マネージャプログラム１４２からエージェントプログラム１４１に送るメッセージを署名するための署名データ１１７とを保持する。

【００２２】

サーバ１０２では、監査プログラム１４３、マネージャプログラム１４２、構成管理プログラム１４４がメモリ１２２にロードされ、ＣＰＵ１２１が上記したプログラム群を実行する。

【００２３】

図２は、クライアント１０１の記憶装置１５０に格納されるボリューム管理情報１５３

とファイル管理情報１５４の一例を示した図である。なお、サーバ１０２の記憶装置１５０においても同様のボリューム管理情報１５３とファイル管理情報１５４を記憶し、管理するものとなる。

【００２４】

ボリューム管理情報１５３は、ボリューム管理テーブル２０１と、ＷＯＲＭが設定されたボリュームに対応するボリューム毎に用意されたＷＯＲＭ属性２０５とを記憶する。

【００２５】

ボリューム管理テーブル２０１は、ボリューム番号２０２と、容量２０３と、Ｉ／Ｏ制御種別２０４とを記憶し、管理する。ボリューム番号２０２は、論理ボリュームの番号を示す。容量２０３は、論理ボリュームの記憶容量を示す。Ｉ／Ｏ制御種別２０４には、通常またはＷＯＲＭのいずれかの属性が構成管理プログラム１４４によって設定される。Ｉ／Ｏ制御種別２０４に通常が設定されたボリュームについては、全てのセクタに対する参照、更新が共に可能である。一方、Ｉ／Ｏ制御種別２０４にＷＯＲＭが設定されたボリュームについては、後述するＷＯＲＭ属性２０５に設定された条件に基づいて、全てのセクタあるいは一部の特定のセクタに対する更新が制限される。

【００２６】

ＷＯＲＭ属性２０５には、設定された更新禁止領域を示す情報が０個以上含まれる。ＷＯＲＭ属性２０５は、更新禁止領域の開始番地２０６と終了番地２０７の組と、ライトフラグ２０８のＯＮまたはＯＦＦによって構成されており、これらの情報は構成管理プログラム１４４によって設定される。開始番地２０６と終了番地２０７は、各々開始セクタ番号と終了セクタ番号を示す。ライトフラグ２０８は、更新禁止領域に対し、1回の更新または書き込みができるか否かを示す。ＯＮは、更新禁止領域に対し、１回の更新または書き込みができることを示し、ＯＦＦは、書き込みおよび更新ができないことを示す。初期状態ではＯＮに設定されている。

【００２７】

ファイル管理情報１５４は、ファイルを書き込んだセクタの情報として、ボリューム番号２１６、パス名２１１と、パス名２１１で指定されるファイルの開始番地２１２と終了番地２１３の組と、記憶装置ＩＤ２１４を記憶し、管理する。記憶装置ＩＤ２１４には、ファイルがどこで新規作成されたかを示す属性情報として、セキュリティチップ１０４の固有ＩＤを記録し、サーバ１０２の記憶装置にコピーする時には、記憶装置ＩＤ２１４が継承されるものである。フラグメント情報２１５は、ファイルが複数のセクタに分断して書き込まれる場合の管理情報を記憶する。図２の例では、各ログファイルの記憶領域は、各更新禁止領域に対応している。

【００２８】

本実施形態では、サーバ１０２が保持するボリューム管理情報１５３およびファイル管理情報１５４は、クライアント１０１が保持するボリューム管理情報１５３およびファイル管理情報１５４と同様の構成をとるとしたが、クライアント１０１とまったく同じ構成である必要はない。

【００２９】

つぎに図３から図５を使って、ログ保全システム１００において、クライアント１０１が行うログ取得、およびサーバ１０２が行うログ回収の処理の流れを説明する。

【００３０】

図３は、クライアント１０１の電源投入時における処理の一例を示すフローチャートである。

【００３１】

クライアント１０１の電源が投入されると、ステップ３０１において、ＢＩＯＳチップ１２３からＢＩＯＳが起動する。つぎにステップ３０２において、ＢＩＯＳは、セキュリティチップ１０４の保持する監査データ１１６を使って、バス１２６に接続された記憶装置１５０があらかじめ決められた正当な機器であるかどうかをチェックする。もし正当な機器でないならば、ステップ３１１において、表示部１２５にアラートを出し、ステップ

３１２において、クライアント１０１の電源をＯＦＦにする。

【００３２】

ステップ３０２において、記憶装置１５０が正当な機器であることを確認すると、ステップ３０３において、ＢＩＯＳは、ＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ）を起動する。ＯＳが起動を完了すると、ステップ３０４において、監査プログラム１４３がセキュリティチップ１０４の監査データ１１６を使って、エージェントプログラム１４１と構成管理プログラム１４４のプログラムファイルが改ざんされていないことを確認する。例えば、セキュリティチップ１０４は、監査データ１１６に記録されたプログラムファイルのハッシュ値と、ステップ３０４の処理を実行する時のエージェントプログラム１４１等のプログラムファイルのハッシュ値とを比較し、両者のハッシュ値が一致していれば正しいプログラムであると判定し、監査プログラム１４３に通知する。もし、正しいプログラムでないと判定すると、監査プログラム１４３は、ステップ３１１と同様に表示部１２５にアラートを出し、ステップ３１２と同様にクライアント１０１の電源をＯＦＦにする。

【００３３】

ステップ３０４でエージェントプログラム１４１等が正しいと判定すると、ステップ３０５において、監査プログラム１４３は、構成管理プログラム１４４を起動する。以降、クライアント１０１で発生する記憶装置１５０へのアクセスについては全て構成管理プログラム１４４が監視する。つづいてステップ３０６において、エージェントプログラム１４１を起動する。以降、クライアント１０１で発生するユーザの操作やデータアクセスなどについては全てエージェントプログラム１４１が監視する。ステップ３０７において、エージェントプログラム１４１は、監視した結果をログとして記憶装置１５０に書き込むが、ステップ３０７についてはさらに図４を使って詳細に説明する。

【００３４】

ステップ３０８において、構成管理プログラム１４４は、記憶装置１５０の記憶領域が一杯であるかどうかを判定する。判定は例えば、書き込み可能領域が所定の値より小さければ一杯であると判定する。もし記憶装置１５０が一杯であれば、ステップ３１１と同様に、表示部１２５にアラートを表示し、ステップ３１２と同様に、クライアント１０１の電源をＯＦＦにする。あるいは、ステップ３１２において、サーバ１０２にアラートを表示部１２５に表示してもよい。

【００３５】

ステップ３０９において、エージェントプログラム１４１は、マネージャプログラム１４２との通信路を確立することを試みる。通信路の確立は、まずエージェントプログラム１４１がセキュリティチップ１０４のクライアント証明書１１３を、通信装置１２４を介してサーバ１０２に送信する。サーバ１０２のマネージャプログラム１４２は、受け取ったクライアント証明書１１３を、セキュリティチップ１０５のクライアント証明書検証データ１１４を使って検証する。検証に成功すると、マネージャプログラム１４２は、サーバ証明書１１１を、通信装置１２４を介してクライアント１０１に送信する。エージェントプログラム１４１は、受け取ったサーバ証明書１１１を、サーバ証明書検証データ１１２を使って検証する。検証に成功すると、通信路を暗号化するための鍵を交換することなどを行い、クライアント１０１とサーバ１０２の間の通信路を確立する。以上の処理が全て成功すると、つづいてステップ３１０において、クライアント１０１の記憶装置１５０からログの回収を行うが、ステップ３１０については図５を使って詳細に説明する。またステップ３０９において、通信路の確立に失敗すると、ふたたびステップ３０７に戻る。

【００３６】

以上の処理により、クライアント１０１の電源投入時の処理が完了する。あとは電源をＯＦＦにするまで、ステップ３０７からステップ３１０までの処理を繰り返す。

【００３７】

なおサーバ１０２の電源投入時についても、図３に示したフローチャートとほぼ同様のものとなるが、サーバ１０２に特有の処理として、ステップ３０４においては、監査プログラム１４３は、マネージャプログラム１４２と構成管理プログラム１４４があらかじめ

決められた正当なプログラムであることを判定する。またステップ３０６においては、マネージャプログラム１４２を起動するものとなる。さらに、ステップ３０９およびステップ３１０においては、マネージャプログラム１４２がエージェントプログラム１４１からのログを回収するものとなるが、ログ回収のサーバ１０２における処理については、図５を使って詳細に説明する。

【００３８】

つづいて図４を使って、ステップ３０７で説明した、記憶装置１５０への書き込み処理について詳細に説明する。実施例１においては、ログファイルの更新を防ぐために、記憶装置１５０のＷＯＲＭ機能を利用した実施形態をとる。

【００３９】

ステップ４０１において、構成管理プログラム１４４は、記憶装置１５０へのファイルアクセスを監視し、書き込みを検出する。ステップ４０２において、構成管理プログラム１４４は、ファイル管理情報１５４を参照し、ボリューム番号２１６とパス名２１１の組で指定されるファイル単位の書き込み要求を、開始番地２１２と終了番地２１３の組で指定されるセクタ単位のＩ／Ｏ要求に変換する。もし、ファイル管理情報１５４にないファイル書き込み要求ならば、当該ファイル書き込み要求に関するファイル管理情報を新たなエントリとしてファイル管理情報１５４に追加する。構成管理プログラム１４４が所属するファイルシステムは、記憶装置１５０に対してＩ／Ｏ要求を発行する。

【００４０】

ステップ４０３において、コントローラ１５５は、記憶装置１５０へのＩ／Ｏ要求を受け付ける。つぎにステップ４０４において、コントローラ１５５はボリューム管理情報１５３のボリューム管理テーブル２０１を参照し、書き出し先のボリュームのＩ／Ｏ制御種別２０４を調べる。Ｉ／Ｏ制御種別がＷＯＲＭならば、ステップ４０５において、ボリューム管理情報１５３のＷＯＲＭ属性２０５を参照し、書き込み先セクタが所属する更新禁止領域のライトフラグ２０８を判定する。もしライトフラグがＯＮならば、ステップ４０６において、ステップ４０１で書き込み要求のあったファイルに対応した新たなセクタ領域を確保し、ＷＯＲＭ属性２０５の更新禁止領域の新たなエントリを追加する。さらにライトフラグ２０８をＯＦＦにする。その後、ステップ４０７において、ステップ４０１で書き込み要求のあったファイルを、論理ボリューム１５１に書き込む。

【００４１】

もしステップ４０４において、書き出し先ボリュームのＩ／Ｏ制御種別２０４が通常ならば、ステップ４０７で示したように、ファイルを論理ボリューム１５１に書き込む。

【００４２】

また、もしステップ４０５において、ライトフラグ２０８がＯＦＦならば、ステップ４０９において、セクタ領域への更新を禁止する。さらにステップ４１０において、表示部１２５にアラートを通知する。

【００４３】

以上のコントローラ１５５の処理が完了すると、構成管理プログラム１４４に制御が戻り、ステップ４０８において、構成管理プログラム１４４は、ファイル管理情報１５４のエントリを更新する。すなわち当該ファイルのエントリがあれば、書き込んだ領域に対応して開始番地２１２と終了番地２１３を記録する。当該ファイルのエントリがなければ、ボリューム番号２１６から記憶装置ＩＤ２１４に至るまでのファイル管理情報を記録する。なお、記憶装置ＩＤ２１４には、セキュリティチップ１０４の保持する固有のＩＤを記録する。

【００４４】

なおサーバ１０２における記憶１５０へのファイル書き込みについても、図４に示すフローチャートと同様の処理を行う。これにより、ログファイルの更新を防ぐことができる。

【００４５】

図５は、ステップ３１０で示した、サーバ１０２によるログファイルの回収の流れの詳

細を示すフローチャートである。

【００４６】

ステップ５０１において、エージェントプログラム１４１は、記憶装置１５０に書かれたログファイルを読み出し、ステップ３０９で確立した通信路を経由して、サーバ１０２にそのログファイルと、ログファイルに対応するファイル管理情報１５４の記憶装置ＩＤ２１４とを送信する。

【００４７】

ステップ５０２において、マネージャプログラム１４２は、ログファイルと記憶装置ＩＤ２１４とを受信する。続くステップ３０７において、このログファイルをサーバ１０２の記憶装置１５０に保存する。ここで、マネージャプログラム１４２は、Ｉ／Ｏ制御種別２０４がＷＯＲＭであるボリュームに対してログを書き込むよう、プログラムされているものである。ここで、記憶装置１５０に保存するときの詳細なフローチャートは、図４に示した処理とほぼ同様であるが、ステップ４０８においてステップ５０２で受信した記憶装置ＩＤ２１４をファイル管理情報１５４に記録する点のみが異なるものとなる。記憶装置１５０への保存が完了すると、つぎにステップ５０３において、ログの保存が完了したためにクライアント１０１側のログファイルを削除しても構わない旨のログ削除メッセージを生成する。この時、ログ削除メッセージは、メッセージを出すごとに異なるものとなるように構成する。例えば、書き込んだログのファイルのハッシュ値を含めて、ログ削除メッセージを構成する。ログ削除メッセージを毎回変更する理由は、リプレイの攻撃によりログ領域が不正に削除されるのを防ぐためである。ステップ５０４において、マネージャプログラム１４２は、ログ削除メッセージに署名データ１１７を使って署名を施す。ステップ５０５において、クライアント１０１に署名のついたログ削除メッセージを送信する。

【００４８】

ステップ５０６において、エージェントプログラム１４１は、ログ削除メッセージを受信する。ステップ５０７において、ログ削除メッセージを、署名検証データ１１８を使って検証し、正当なサーバから送られてきたメッセージであるかどうかを判定する。もし正当なサーバからのメッセージであれば、ステップ５０８において、構成管理プログラム１４４に命じて、該当するファイルが占有していたボリューム管理情報１５３の更新禁止領域のＷＯＲＭ属性２０５のライトフラグ２０８をＯＮにし、該当する論理ボリューム１５１のセクタ領域を削除する。なお、論理ボリューム１５１のセクタ領域の削除については、パス名などのファイル管理情報１５４を削除するだけでも良い。あるいは論理ボリューム１５１の該当領域を所定の文字で上書きしてから、パス名などのファイル管理情報１５４を削除するものであっても良い。さらには論理ボリューム１５１の該当領域を所定の文字で上書きし、ファイルサイズを０にしてから、パス名などのファイル管理情報１５４は残しておくものであっても良い。

【００４９】

ステップ５０７において、もし正当なサーバからのメッセージでないならば、エージェントプログラム１４１は、マネージャプログラム１４２に対して、サーバ１０２の記憶装置１５５に書き込んだログを削除する要求を出す。ステップ５０９において、マネージャプログラム１４２は、ログを削除する。さらにステップ５１０において、エージェントプログラム１４１は、ログの回収が失敗したメッセージを表示部１２５にアラートとして出す。

【００５０】

以上のログの回収処理が完了することにより、クライアント１０２の記憶装置１５０のログ記憶領域を再利用することができるようになり、ログの保全性を確保するとともに記憶装置１５０の圧迫を防止することができる。

【００５１】

図６は、クライアント１０１のログファイルをサーバ１０２に回収するまでの状態遷移をあらわした図である。まずそれぞれの状態について説明する。

【００５２】
状態６０１は、まだクライアント１０１でログが何もない状態である。状態６０７は、クライアント１０１の記憶装置１５０にサイズが０のファイルを作成した状態である。状態６０６は、クライアント１０１の記憶装置１５０にログファイルを書き込み中の状態である。状態６０２は、クライアント１０１の記憶装置１５０にログが書き込まれた状態である。状態６０３は、クライアント１０１からサーバ１０２にログをコピー中の状態である。状態６０４は、クライント１０１からサーバ１０２へのログのコピーが完了した状態である。状態６０８は、クライアント１０１の記憶装置１５０に書き込んだファイルの内容を削除した状態である。状態６０５は、クライアント１０１の記憶装置１５０のＷＯＲＭ保護領域が再利用可能になった状態である。

【００５３】
次に同じ図６を使って、状態の遷移について説明する。状態６０１から状態６０７への遷移は、ログファイルの新規作成６１８により行われる。状態６０７から状態６０６への遷移は、ログファイルの書き込み開始６１０により行われる。状態６０６から状態６０２への遷移は、ログファイルの書き込み完了６１１により行われる。状態６０２から状態６０３への遷移は、ログ回収開始６１２により行われる。また、状態６０３から状態６０２への遷移は、ログ回収の前提として必要となる通信路の通信失敗６１３などのエラー時に行われる。状態６０３から状態６０４への遷移は、ログ回収終了６１４により行われる。また、状態６０４から状態６０３への遷移は、ログ回収の前提として必要となる通信路の通信失敗６１５などのエラー時に行われる。状態６０４から状態６０８への遷移は、クライアント１０１に記録されたログの削除成功６１６により行われる。また、状態６０４から状態６０２への遷移は、ログの削除失敗６１７などのエラー時に行われる。状態６０８から状態６０５への遷移は、クライアント１０１に記録されたログファイルのパス削除６１９により行われる。

【００５４】
以上の状態遷移図により、一度クライアント１０１に書き込まれたログを確実にサーバ１０２で回収すると共に、クライアント１０１の記憶装置１５０を効率良く再利用することができることを示している。

【００５５】
図７は、ログ保全システム１００を導入した場合のクライアント１０１のライフサイクルの一例を説明する図である。

【００５６】
クライアント１０１に対しては、まずフェーズ７０１において、セキュリティチップ１０４に、サーバ証明書検証データ１１２と、クライアント証明書１１３と、署名検証データ１１８を所定の手順を踏んで書き込む。このとき、クライアント証明書１１３は、信頼可能な認証局から発行してもらうものである。

【００５７】
フェーズ７０２において、フェーズ７０１で発行してもらったクライアント証明書１１３を検証するためのクライアント証明書検証データ１１４を、サーバ１０２のセキュリティチップ１０５に所定の手順を踏んで書き込む。サーバ１０２は、管理対象となるクライアント１０１の台数分のクライアント証明書検証データ１１４を保持する。

【００５８】
フェーズ７０３において、クライアント１０１に、監査プログラム１４３、エージェントプログラム１４１、構成管理プログラム１４４のプログラムをインストールする。

【００５９】
フェーズ７０４において、クライアント１０１のセキュリティチップ１０４に、エージェントプログラム１４１と構成管理プログラム１４４のプログラムファイルのハッシュ値と、バス１２６で接続された機器の構成情報など、監査データ１１６を所定の手順を踏んで書き込む。

【００６０】

以上のフェーズが完了すると、フェーズ７０５において、ユーザによるクライアント１０１の利用を開始する。

【００６１】

フェーズ７０５において、もしエージェントプログラム１４１や構成管理プログラム１４４にセキュリティホールが発見されるなど、プログラムの更新の必要がある場合には、フェーズ７０６において、各種プログラムの再インストールを行い、つづいてフェーズ７０４と同様に、監査データ１１６を所定の手順を踏んで更新する。

【００６２】

またフェーズ７０５において、もし記憶装置１５０が故障した場合や、空き容量が所定の値以下になった場合には、フェーズ７０７で記憶装置１５０を交換し、つづいてフェーズ７０４と同様に、監査データ１１６を所定の手順を踏んで更新する。

【００６３】

本実施形態においては、フェーズ７０５はユーザにクライアント１０１が渡された時点をあらわすものであり、その他のフェーズはすべて、例えばシステム管理者あるいは保守員にクライアント１０１が渡された時点をあらわすものである。

【実施例２】

【００６４】

以上説明してきた実施例１の実施形態においては、ログファイルの更新を防止するために、記憶装置１５０の有するＷＯＲＭ機能を利用することで実現した。実施例２の実施形態においては、記憶装置１５０はＷＯＲＭ機能を持たず、代替手段として、構成管理プログラム１４４がアクセス制御ポリシデータ１１９の通りに記憶装置１５０へのアクセスを制御してログファイルの更新を防止する方法について説明する。なお、実施例２の実施形態においては、ＷＯＲＭ属性２０５とファイル管理情報１５４を使用しない。

【００６５】

図８は、アクセス制御ポリシデータ１１９の詳細を説明した図である。アクセス制御ポリシデータ１１９は、許可プログラムテーブル８００と、保護対象フォルダテーブル８１０と、アクセス制御テーブル８２０とを記憶する。

【００６６】

アクセス制御テーブル８２０は、構成管理プログラム１４４が記憶装置１５０へのアクセスを制御するためのポリシが記述されたものである。すなわち、記憶装置１５０へのアクセス対象となるファイルが、ボリューム番号８２１とファイルパス名８２２の組で指定されるファイルへのアクセスであった場合、許可プログラム識別子８２３で識別されるプログラムからのアクセスだけを許可し、それ以外のプログラムからのアクセスを禁止する。ボリューム番号８２１は、ファイル実体が格納されるボリュームの番号である。

【００６７】

許可プログラムテーブル８００は、アクセス制御テーブル８２０の許可プログラム識別子８２３で識別されるプログラムを指定する。プログラムは、ボリューム番号８０１とプログラムパス名８０２の組によって一意に識別される、あるいは、たとえばプログラムファイルのハッシュ値といったプログラム特徴値８０３によって一意に識別される、あるいは、両方によって一意に識別されるものである。ボリューム番号８０１は、プログラムの実体が格納されるボリュームの番号である。

【００６８】

保護対象フォルダテーブル８１０は、アクセス制御テーブル８２０で保護対象となるファイルの領域を指定するものである。ボリューム番号８１１とパス名８１２の組で指定されるフォルダ中のファイルが該当する場合に、アクセス制御テーブル８２０にあるポリシで保護される対象ファイルとなる。

【００６９】

なお保護対象フォルダテーブル８１０およびアクセス制御テーブル８２０のエントリをフォルダ名やファイルパス名で指定する代わりに、セクタの開始番地と終了番地など、記憶領域のアドレス範囲で設定してもよい。

【００７０】
図９は、実施例２における構成管理プログラム１４４の動作を示すフローチャートである。ステップ９０１においては、構成管理プログラム１４４は、記憶装置１５０への書き込みを監視する。ステップ９０２においては、セキュリティチップ１０４にあるアクセス制御ポリシデータ１１９を読み込み、照合を開始する。なお、アクセス制御ポリシデータ１１９は、一度読み込んだ後は、構成管理プログラム１４４がメモリ１２２に保持するものであっても良い。
【００７１】
ステップ９０３においては、書き込み対象となるファイルが、保護対象フォルダテーブル８１０で指定されるフォルダ以下にあるかどうかを判定する。もし、そのフォルダ以下にないならば、ステップ４０２の変換をした後、記憶装置１５０に対してＩ／Ｏ要求を発行する。ステップ９０７において、コントローラ１５５が、記憶装置１５０へのＩ／Ｏ要求を受け付け、ステップ９０８において、論理ボリューム１５１にファイルを書き込む。
【００７２】
ステップ９０３において、保護対象とするフォルダ以下にあるならば、つづくステップ９０４において、許可プログラムテーブル８００との照合を行い、書き込みを許可されたプログラムからの書き込み要求であるかどうかを判定する。もし、書き込みを許可されたプログラム以外からの要求ならば、ステップ９１０において、書き込みを禁止し、つづくステップ９１１において、表示部１２５にアラートを出しユーザに通知する。
【００７３】
ステップ９０４において、書き込みを許可されたプログラムからの書き込み要求ならば、つづくステップ９０５において、書き込み対象となるファイルがアクセス制御テーブル８２０にあるかどうかを判定する。許可プログラムからの書き込み要求であることを確認するために、構成管理プログラム１４４からセキュリティチップ１０５へ当該許可プログラムのプログラム特徴値を送信し、セキュリティチップ１０５がプログラム特徴値８０３と照合して許可プログラムからの要求と認証してもよい。もしアクセス制御テーブル８２０にないならば、ステップ９０９において、アクセス制御テーブル８２０に書き込み要求を許可するようなエントリを追加し、ステップ４０２の変換とＩ／Ｏ要求の発行を経由した後、ステップ９０７およびステップ９０８と同様にファイル書き込みを行う。
【００７４】
ステップ９０５において、アクセス制御テーブル８２０にあるならば、つづくステップ９０６において、許可プログラム識別子８２３が一致しているかどうかを判定する。もし一致しているならば、ステップ４０２の変換とＩ／Ｏ要求の発行を経由した後、ステップ９０７およびステップ９０８と同様にファイル書き込みを行う。もし、一致していないならば、ステップ９１０およびステップ９１１と同様に書き込みを禁止する。
【００７５】
以上の処理により、構成管理プログラム１４４は、ログファイルの追記を行うエージェントプログラム１４１が書き込んだログファイルに対し、エージェントプログラム１４１以外のプログラムからのアクセスを禁止することによって、ログファイルの不正な更新を防止することができる。
【００７６】
また、実施例２における、サーバ１０２からのログ削除メッセージを受けたクライアント１０１における処理については、図５に示したものとほぼ同様である。ただし、ステップ５０８において、エージェントプログラム１４１は、構成管理プログラム１４４に命じ、アクセス制御ポリシデータ１１９のアクセス制御テーブル８２０から、サーバ１０２にコピーが完了したログファイルを保護していたエントリを削除する。これは当該ログファイルをその記憶領域から削除するのと等価である。
【００７７】
さらに、第２の実施例における、クライアント１０１のライフサイクルについては、図７に示したのとほぼ同様であるが、ステップ７０４において、アクセス制御ポリシデータ

１１９を所定の手順を踏んでセキュリティチップ１０４に書き込むものとなる。

【００７８】

以上説明してきた実施例２により、記憶装置１５０に書き込まれたログファイルの不正な更新を防止すると共に、サーバ１０２にログファイルが書き込まれた後はクライアント１０１の記憶装置１５０を再利用することを、記憶装置１５０のＷＯＲＭ機能を利用せずに、構成管理プログラム１４４のアクセス制御機能により実現することができる。

【００７９】

以上述べたログ保全システムは、クライアント・サーバ型のシステム全般に適用することができる。クライアントＰＣ以外にも、携帯電話やＰＤＡといった可搬機器にも適用することができる。

【図面の簡単な説明】

【００８０】

【図１】実施形態のログ保全システムの構成を示した図である。

【図２】ボリューム管理情報とファイル管理情報の例を示した図である。

【図３】クライアントの電源投入時の処理例を示すフローチャートである。

【図４】記憶装置への書き込み処理のフローチャートである。

【図５】サーバによるログ回収の処理例を示すフローチャートである。

【図６】実施形態のログ回収の状態遷移を示した図である。

【図７】実施形態のログ保全システム導入後のクライアントのライフサイクルを示した図である。

【図８】実施例２のアクセス制御ポリシデータの構成を示した図である。

【図９】実施例２の記憶装置への書き込み処理のフローチャートである。

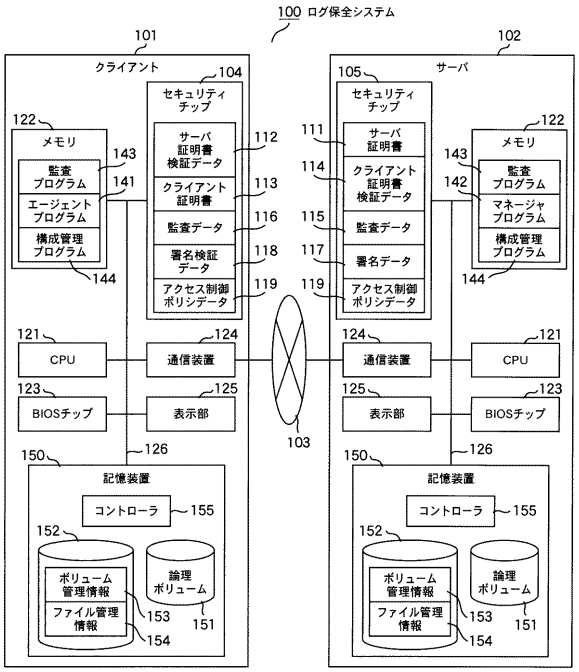
【符号の説明】

【００８１】

１００：ログ保全システム、１０１：クライアント、１０２：サーバ、１０４：セキュリティチップ、１０５：セキュリティチップ、１１９：アクセス制御ポリシデータ、１４１：エージェントプログラム、１４２：マネージャプログラム、１４３：監査プログラム、１４４：構成管理プログラム、１５０：記憶装置、１５３：ボリューム管理情報、１５４：ファイル管理情報、１５５：コントローラ。

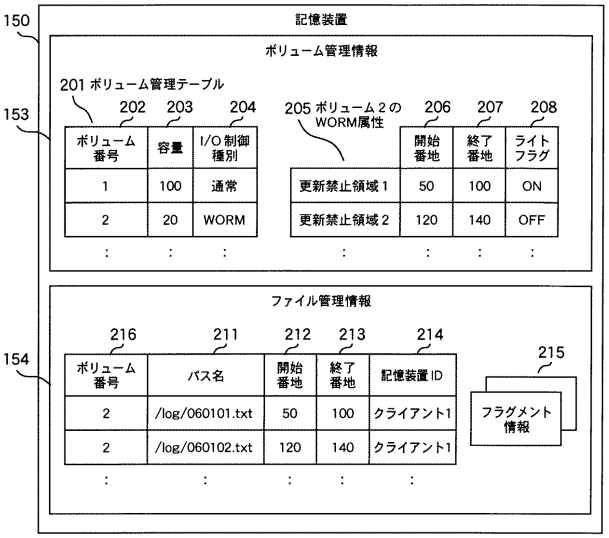
【図１】

図 1



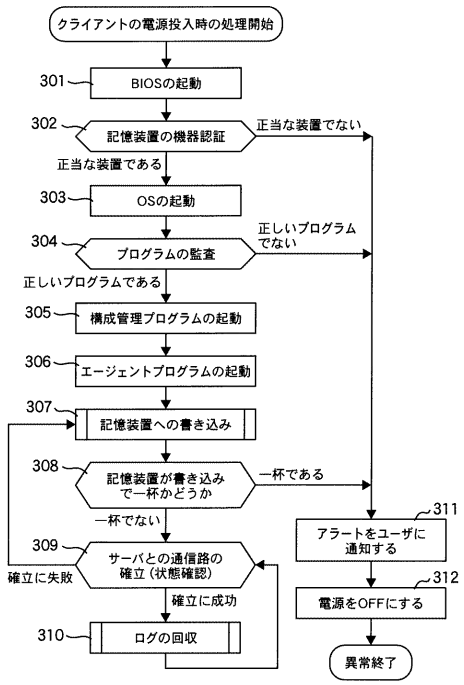
【図２】

図 2



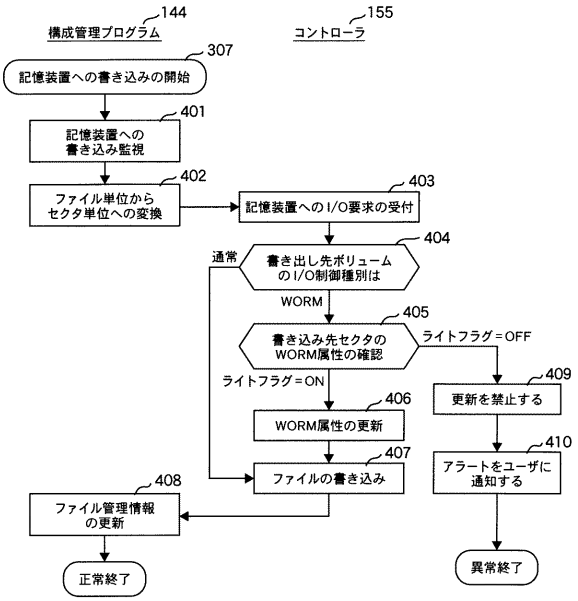
【図３】

図 3



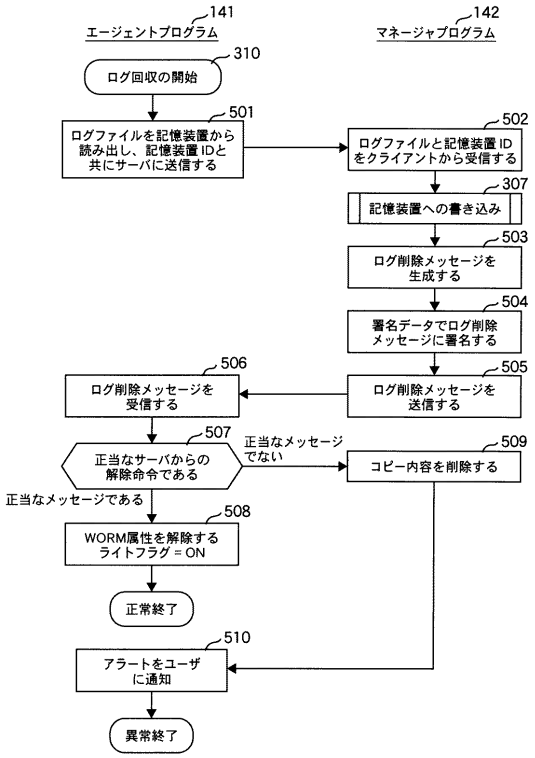
【図４】

図 4



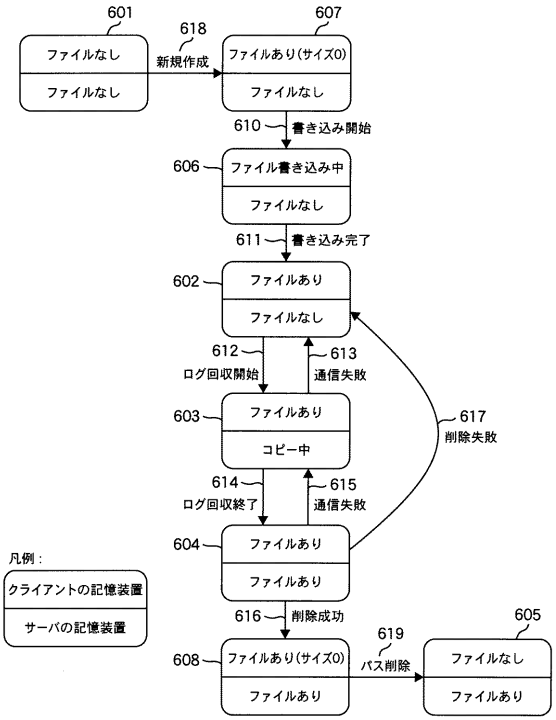
【図５】

図 5



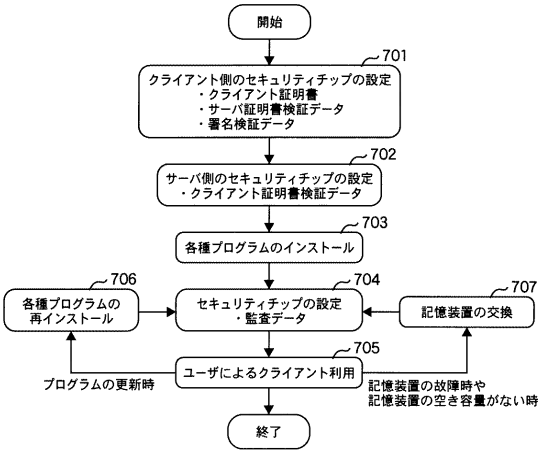
【図６】

図 6



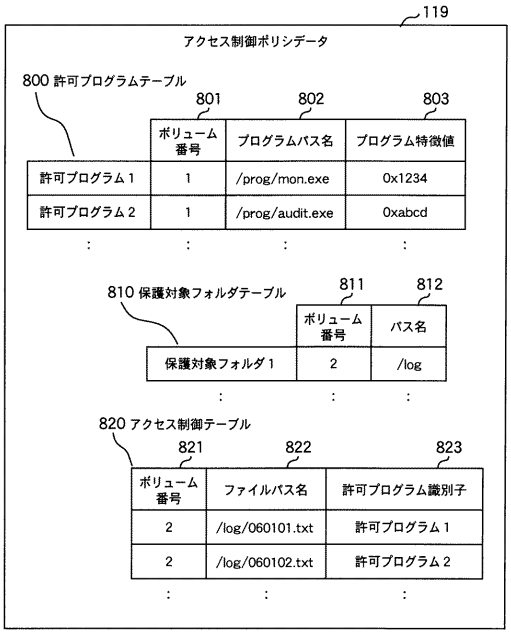
【図７】

図 7



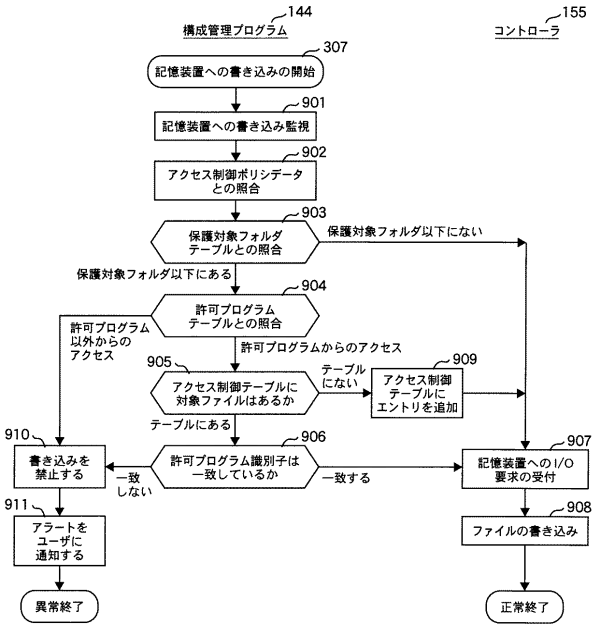
【図８】

図 8



【図９】

図 9


144
構成管理プログラム
155
コントローラ
307
記憶装置への書き込みの開始
901
記憶装置への書き込み監視
902
アクセス制御ポリシデータとの照合
903
保護対象フォルダテーブルとの照合
保護対象フォルダ以下にない
保護対象フォルダ以下にある
904
許可プログラムテーブルとの照合
許可プログラム以外からのアクセス
許可プログラムからのアクセス
905
アクセス制御テーブルに対象ファイルはあるか
テーブルにない
909
アクセス制御テーブルにエントリを追加
テーブルにある
906
許可プログラム識別子は一致しているか
一致しない
一致する
910
書き込みを禁止する
911
アラートをユーザに通知する
異常終了
907
記憶装置へのI/O要求の受付
908
ファイルの書き込み
正常終了

フロントページの続き

(72)発明者　森田　　光
神奈川県川崎市幸区鹿島田８９０番地　　株式会社日立製作所情報・通信グループ内
(72)発明者　佐藤　直人
神奈川県川崎市麻生区王禅寺１０９９番地　　株式会社日立製作所システム開発研究所内

Ｆターム(参考) 5B017 AA07 BA06 CA16
5B042 GA12 GC10 HH30 MA01 MA09 MA16 MC22 MC37
5B082 DD04 DD08 EA11