(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4912084号
(P4912084)
(45)発行日　平成24年4月4日(2012.4.4)　(24)登録日　平成24年1月27日(2012.1.27)

(51)Int.Cl.　F I
G06F 11/34 (2006.01)　G06F 11/34　C

請求項の数 2　(全 12 頁)

(21)出願番号　特願2006-226088(P2006-226088)
(22)出願日　平成18年8月23日(2006.8.23)
(65)公開番号　特開2008-52390(P2008-52390A)
(43)公開日　平成20年3月6日(2008.3.6)
審査請求日　平成21年1月20日(2009.1.20)

(73)特許権者　000233055
株式会社日立ソリューションズ
東京都品川区東品川四丁目１２番７号
(74)代理人　100088720
弁理士　小川　眞一
(72)発明者　西出　隆志
東京都品川区東品川４丁目１２番７号　日立ソフトウエアエンジニアリング株式会社内
(72)発明者　橋本　浩昌
東京都品川区東品川４丁目１２番７号　日立ソフトウエアエンジニアリング株式会社内

最終頁に続く

(54)【発明の名称】監査用ログ記録制御方法および情報漏洩監視プログラム

(57)【特許請求の範囲】
【請求項１】
クライアントコンピュータにおける任意のアプリケーションによる各種リソースへの入出力操作を監視し、監視結果を監査用のログ情報として記憶手段に記録し、その記録したログ情報をクライアントコンピュータにおける各種の操作を監査するログサーバに送信する情報漏洩監視手段を備えた監査用ログ記録制御方法であって、
前記情報漏洩監視手段が、
前記記憶手段に記録したログ情報が記録可能な容量の上限に達したか、または当該記憶手段の残容量が予め設定された下限を下回ったかを検出し、その検出結果に基づいて前記記憶手段に記録したログ情報をログサーバに送信する第１のステップと、
ログサーバへの送信が成功した場合には、前記アプリケーションの入出力操作に起因する新たなログ情報を前記記憶手段に記録すると共に、送信したログ情報を前記記憶手段から削除し、ログサーバへの送信が不成功の場合には、前記情報漏洩監視手段を実装したクライアントコンピュータの機能の一部または全部を制限した縮退動作のうち管理サーバから予め受信しておいたクライアント別の監査用ログ記録制御情報に従い選択された縮退動作に移行させる第２のステップと、
前記記録手段に記録したログ情報を前記ログサーバに送信することにより前記記憶手段に記憶したログ情報が記録可能な容量の上限を下回った場合、または記憶手段の残容量が予め設定された下限を上回った場合には、縮退動作から通常動作に復帰させる第３のステップとを前記アプリケーションの入出力操作に起因するログ情報の記録時に実行すること

を特徴とし、前記第２のステップにおいて、ログサーバへの送信が不成功の場合、過去のログに新規のログを前記記憶手段に上書きするログラップ書き込み、過去のログに新規ログを制限なしに書き込む上限なし書き込み、ログ情報が記録可能な容量の上限に達したあるいは記憶手段の残容量が予め設定された下限を下回った場合には、過去のログに新規のログを上書きすることなく前記縮退動作に移行させる上限あり書き込みのログ記録形態を前記管理サーバに設定した前記クライアント別の監査用ログ記録制御情報によって設定可能に構成されていることを特徴とする監査用ログ記録制御方法。

【請求項２】

クライアントコンピュータにおける任意のアプリケーションによる各種リソースへの入出力操作を監視し、監視結果を監査用のログ情報として記憶手段に記録し、その記録したログ情報をクライアントコンピュータにおける各種の操作を監査するログサーバに送信する情報漏洩監視プログラムであって、

前記記憶手段に記録したログ情報が記録可能な容量の上限に達したか、または当該記憶手段の残容量が予め設定された下限を下回ったかを検出し、その検出結果に基づいて前記記憶手段に記録したログ情報をログサーバに送信する第１のステップと、

ログサーバへの送信が成功した場合には、前記アプリケーションの入出力操作に起因する新たなログ情報を前記記憶手段に記録すると共に、送信したログ情報を前記記憶手段から削除し、ログサーバへの送信が不成功の場合には、前記情報漏洩監視手段を実装したクライアントコンピュータの機能の一部または全部を制限した縮退動作のうち管理サーバから予め受信しておいたクライアント別の監査用ログ記録制御情報に従い選択された縮退動作に移行させる第２のステップと、

前記記録手段に記録したログ情報を前記ログサーバに送信することにより前記記憶手段に記憶したログ情報が記録可能な容量の上限を下回った場合、または記憶手段の残容量が予め設定された下限を上回った場合には、縮退動作から通常動作に復帰させる第３のステップとを前記アプリケーションの入出力操作に起因するログ情報の記録時にコンピュータに実行させることを特徴とし、前記第２のステップにおいて、ログサーバへの送信が不成功の場合、過去のログに新規のログを前記記憶手段に上書きするログラップ書き込み、過去のログに新規ログを制限なしに書き込む上限なし書き込み、ログ情報が記録可能な容量の上限に達したあるいは記憶手段の残容量が予め設定された下限を下回った場合には、過去のログに新規のログを上書きすることなく前記縮退動作に移行させる上限あり書き込みのログ記録形態を前記管理サーバに設定した前記クライアント別の監査用ログ記録制御情報によって設定可能に構成されていることを特徴とする情報漏洩監視プログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、クライアントコンピュータにおける任意のアプリケーションによる各種リソースへの入出力操作を監視し、監視結果を監査用のログ情報として記憶手段に記録し、その記録したログ情報をクライアントコンピュータにおける各種の操作を監査するログサーバに送信する監査用ログ記録制御方法および情報漏洩監視プログラムに関するものである。

【背景技術】

【０００２】

企業や各種の団体に設置されたコンピュータシステムにおいては、組織内の機密情報が外部に漏洩しないように機密データの外部記憶装置への書き込み禁止、印刷の禁止など各種の情報漏洩監視手段が導入されている。この情報漏洩手段には、組織内の各構成員が使用するクライアントコンピュータにおける任意のアプリケーションによる各種リソースへの入出力操作を監視し、監視結果を監査用のログ情報として記憶手段に記録し、その記録したログ情報を監査用のログサーバに送信して解析することにより、クライアントコンピュータにおいて情報漏洩の原因となるような不正な操作が行われていないかを定期的に調

べるためのログ記録手段を付加したものがある。
この場合、クライアントコンピュータにおけるログ情報を記録する場合、通常、クライアントコンピュータのハードディスク内に記録するが、ハードディスクの記憶容量は無限大ではないため、ログ情報の記録量が所定量を超えてしまうと、監査サーバに対して未送信のログ情報の記憶領域に新たなログ情報が上書きされてしまい、ログサーバに送信すべきログ情報の一部が喪失してしまうことが起こり、クライアントコンピュータにおける全ての挙動を解析できなくなることがある。
【０００３】
このようなログ情報の喪失を防止する技術として、下記の特許文献１に開示されたものがある。
【特許文献１】特開平５－２９８１５７
【０００４】
この特許文献１に記載のものは、障害調査用ログ出力の際に、ログ情報の解析処理をログ出力処理の前に行い、不用なログ出力を減らし、ログ容量の満杯による過去に出力されたログへの上書きの可能性を軽減させる仕組みを開示したものである。
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかしながら、上記特許文献１に記載の技術では、情報漏洩監視手段を実装した情報処理システムで収集されるような監査ログを想定していない。監査ログは情報処理システムで過去の挙動を記録し、ユーザによる不正利用を抑止するために収集されるもので管理者によっては全ての監査用のログ情報の確実な収集が望ましいと考えている。そのような場合、上記特許文献１の技術ではログ喪失の可能性が軽減されるだけで確実に収集されることにはならない。
また、情報漏洩監視手段を実装した情報処理システムでは監査用のログ情報は、通常、クライアントコンピュータ自身で収集し、ログを一括管理するログサーバへと収集されるが、クライアントコンピュータがログサーバとのネットワークから長時間にわたって遮断された状況になった場合、監査用ログ情報が長時間にわたって収集されず、クライアントコンピュータのログ情報を確実に収集し、不正な挙動を監査できなくなるといった事態が生じ、情報漏洩監視機能としての信頼性が低下するという問題がある。
【０００６】
本発明の目的は、クライアントコンピュータ内に記録された監査用のログ情報の全てをログサーバに収集する確実性を向上させ、情報漏洩監視機能としての信頼性の低下を防止することができるログ記録制御方法および情報漏洩監視プログラムを提供することにある。
【課題を解決するための手段】
【０００７】
上記目的を達成するために、本発明に係るログ記録制御方法は、クライアントコンピュータにおける任意のアプリケーションによる各種リソースへの入出力操作を監視し、監視結果を監査用のログ情報として記憶手段に記録し、その記録したログ情報をクライアントコンピュータにおける各種の操作を監査するログサーバに送信する情報漏洩監視手段を備えた監査用ログ記録制御方法であって、
前記情報漏洩監視手段が、
前記記憶手段に記録したログ情報が記録可能な容量の上限に達したか、または当該記憶手段の残容量が予め設定された下限を下回ったかを検出し、その検出結果に基づいて前記記憶手段に記録したログ情報をログサーバに送信する第１のステップと、ログサーバへの送信が成功した場合には、前記アプリケーションの入出力操作に起因する新たなログ情報を前記記憶手段に記録すると共に、送信したログ情報を前記記憶手段から削除し、ログサーバへの送信が不成功の場合には、当該監視手段を実装したクライアントコンピュータの機能の一部または全部を制限した縮退動作に移行させる第２のステップと、前記記録手段

に記録したログ情報を前記ログサーバに送信することにより前記記憶手段に記憶したログ情報が記録可能な容量の上限を下回った場合、または記憶手段の残容量が予め設定された下限を上回った場合には、縮退動作から通常動作に復帰させる第３のステップとを前記アプリケーションの入出力操作に起因するログ情報の記録時に実行することを特徴とする。

また、前記第１のステップにおいて、縮退動作に移行させるか否かを管理サーバによる設定情報によって決定することを特徴とする。

【０００８】

本発明に係る情報漏洩監視プログラムは、クライアントコンピュータにおける任意のアプリケーションによる各種リソースへの入出力操作を監視し、監視結果を監査用のログ情報として記憶手段に記録し、その記録したログ情報をクライアントコンピュータにおける各種の操作を監査するログサーバに送信する情報漏洩監視プログラムであって、

前記記憶手段に記録したログ情報が記録可能な容量の上限に達したか、または当該記憶手段の残容量が予め設定された下限を下回ったかを検出し、その検出結果に基づいて前記記憶手段に記録したログ情報をログサーバに送信する第１のステップと、ログサーバへの送信が成功した場合には、前記アプリケーションの入出力操作に起因する新たなログ情報を前記記憶手段に記録すると共に、送信したログ情報を前記記憶手段から削除し、ログサーバへの送信が不成功の場合には、当該監視手段を実装したクライアントコンピュータの機能の一部または全部を制限した縮退動作に移行させる第２のステップと、前記記録手段に記録したログ情報を前記ログサーバに送信することにより前記記憶手段に記憶したログ情報が記録可能な容量の上限を下回った場合、または記憶手段の残容量が予め設定された下限を上回った場合には、縮退動作から通常動作に復帰させる第３のステップとを前記アプリケーションの入出力操作に起因するログ情報の記録時にコンピュータに実行させることを特徴とする。

また、前記第１のステップにおいて、縮退動作に移行させるか否かを管理サーバによる設定情報によって決定するステップを備えることを特徴とする。

【発明の効果】

【０００９】

本発明によれば、例えば、組織内の情報処理システムにＬＡＮ等のネットワークで接続されたクライアントコンピュータを比較的長期の出張などで組織外へ持ち出して使用した場合、あるいは不正にネットワークから切り離して使用した場合に、アプリケーションの入出力操作に起因するログ情報の記録時に、既に記録したログ情報が記憶手段に記録可能な容量の上限に達していた場合、または当該記憶手段の残容量が予め設定された下限を下回っていた場合、記憶手段に記録したログ情報をログサーバに送信することを試みるが、ログサーバへの送信が不成功となり、クライアントコンピュータの機能の一部または全部を制限した縮退動作に移行させる。このため、クライアントコンピュータではアプリケーションの入出力操作が不可能になり、ユーザに対してログサーバへのログ情報の送信が強制される。

これにより、クライアントコンピュータにおいては、ログ情報が上書きされて一部が喪失することも生じなくなり、ログサーバではクライアントコンピュータに記録されたログ情報を時系列で確実に収集することが可能になる。

また、ユーザに対しては、ネットワークから不正に、あるいは長期にわたって切り離す行為が無駄であることを知らしめることができ、ネットワークから切り離して不正行為を行うことに対する抑止力を与えることができる。

【発明を実施するための最良の形態】

【００１０】

以下、本発明を実施する場合の一形態について図面を参照して具体的に説明する。

図１は、本発明に係る監査用ログ記録制御方法を適用した情報処理システムの実施の形態を示すシステム構成図であり、クライアントコンピュータ１と、クライアント認証及び監査用ログ記録制御情報のクライアントコンピュータ１への配信、クライアントインストール媒体の作成などを行う管理サーバ２と、クライアントコンピュータ１のハードディス

ク１４に記録されたログを収集して収集済み監査用ログＤＢ３１に記録した後、解析するログサーバ３とで構成されている。

クライアントコンピュータ１には、任意のアプリケーション１１、情報漏洩監視プログラム１２、ＯＳ（オペレーティングシステム）１３がハードディスク１４に記憶されている。

【００１１】

情報漏洩監視プログラム１２は、図２に示すように、任意のアプリケーション１１による印刷要求、メール送信要求、外部媒体データ書き出し要求などの各種リソースへの入出力操作を捕捉し、管理サーバ２からの設定情報によって許可されている入出力要求（あるいは操作）であれば許可し、捕捉した入出力要求をＯＳ１３に渡し、許可されていない入出力要求であれば、捕捉した入出力要求を破棄し、外部媒体などへの不正なデータ書き出しによる情報漏洩を防止するものである。この情報漏洩監視プログラム１２は、ログサーバ３で不正な操作が行われていないかを監査するための監査用のログ情報をリソースへの入出力時にハードディスク１４に記録し、ログサーバ３に送信する機能も備えている。

このような機能を備えた情報漏洩監視プログラム１２は、図３に示すように、管理サーバ２で管理者によって作成されたインストール媒体２２によってクライアントコンピュータ１にインストールされるものである。

【００１２】

インストール媒体２２に記録された情報漏洩監視プログラム１２には、管理サーバ２の監査用ログ記録制御情報ＤＢ２１に登録されたクライアントコンピュータ別の監査用ログ記録制御情報（以下、制御情報と略記）が初期情報として設定され、この制御情報に基づいて記録するログ情報の上限、記録したログ情報の送信時間周期等が制御される。

【００１３】

図４は、管理サーバ２の監査用ログ記録制御情報ＤＢ２１に登録されたクライアントコンピュータ別の監査用ログ記録制御情報の例を示すものであり、クライアントコンピュータＩＤ別に、ログ容量上限、ディスク残量下限、定期的ログ送信設定、縮退動作フラグ、縮退動作詳細設定、クライアント設定フラグといった項目で構成されている。

ログ容量上限とは、クライアントコンピュータ１のハードディスク１４に記録する監査用のログ情報の上限を制御するものである。なお、ログ容量上限＝０ＭＢとは、ログ容量記録容量に制限がないことを意味する。社員が出張等により自身のクライアントコンピュータ１を外部に持ち出す必要が生じた場合、管理者が管理サーバ２からログ容量上限＝０ＭＢとした監査用ログ記録制御情報を送信し、この制御情報によってログ容量上限値を変更して持ち出すことにより、出張先でのログが無制限に記録される。

ディスク残量下限とは、ハードディスク１４に記録したログ情報をログサーバ３に送信して吐き出す場合の指標となるディスク残量の下限値である。例えば、ディスク残量下限＝２０ＭＢとは、残量が２０ＭＢ以下になったらログ情報をログサーバ３に送信する必要があることを意味する。

【００１４】

定期的ログ送信設定とは、ログサーバ３に対してログ情報を定期的に送信する時間周期を表すものである。この場合、定期的ログ送信設定＝６０ｓｅｃとは、６０秒間隔でログ情報を送信することを意味する。また、定期的ログ送信設定＝０ｓｅｃとは、ログ情報を定期的に送信するのではなく、予め定めたイベント、例えば管理サーバ２にログインした直後に送信することを意味する。

定期的制御情報受信設定とは、監査用ログ記録制御情報を管理サーバ２から定期的に受信する設定であるか否かを表すものである。

縮退動作フラグとは、記録したログ情報がログ容量上限を上回った場合、またはハードディスク１４の残量がディスク残量下限を下回った場合に、クライアントコンピュータ１の機能の一部または全部を制限した縮退動作に移行させるかを定めるものであり、ＯＮは縮退動作に移行させ、ＯＦＦは移行させないことを意味する。

【００１５】

縮退動作詳細設定とは、縮退動作の内容を規定するものであり、全操作禁止、印刷のみ許可といった一部機能の制限または全機能の制限内容が設定される。

クライアント設定フラグとは、監査用ログ記録制御情報ＤＢ２１に登録されたクライアントコンピュータ別の監査用ログ記録制御情報が管理者によって変更された場合に、その変更が各クライアントコンピュータに反映されたかを示す識別情報であり、クライアントコンピュータ１が管理サーバ２と送受信することにより、管理者によって変更された監査用ログ記録制御情報が反映された場合には、当該フラグは済み、そうでない場合には未済となる。

例えば、監査用ログ記録制御情報ＤＢ２１に登録されたクライアントコンピュータ別の監査用ログ記録制御情報のうち、クライアントコンピュータＩＤ１に相当する部分を変更した場合、クライアント設定フラグは未済となる。そして、クライアントコンピュータＩＤ１へ変更後の設定が当該ＩＤ１のクライアントコンピュータに配信されたとき、クライアント設定フラグは済みとなる。管理者はこの監査用ログ記録制御情ＤＢ２１のクライアント設定フラグを見ることで対応するクライアントコンピュータの監査用ログ記録制御情報のクライアントコンピュータに反映された否かを判別することができる。

【００１６】

本実施形態では、次の３種類の監査用ログ記録形態をクライアントコンピュータ１に対して設定できる。

（１）ログラップ書き込み

監査用ログ記録制御情報によって０ＭＢ以上のログ容量の上限が設定されており、ハードディスク１４に記録したログ容量が設定された上限に達したが、ログサーバ３に送信できない状況では過去のログに新規のログを上書きする。

上書きを許可する形態としては、クライアントコンピュータ１で扱う情報の機密性が低く、監査ログの重要性が低い場合、あるいはログサーバ３の不具合によりログ情報を収集できなくなった場合などに使用される。情報漏洩の原因を確実に解析する上ではログラップ設定をＯＦＦにしておくことが望ましい。

（２）ログ上限無し書込み

ログ容量の上限が監査用ログ記録制御情報によって無制限（０ＭＢ）に設定されており、過去のログが上書きされることなく制限なしに追加ログとして書込む。

（３）ログ上限あり縮退動作

ログ容量の上限が監査用ログ記録制御情報によって設定されており、ログ容量が上限に達したあるいはディスク残容量が下限を下回ったがログサーバ３に送信できない状況では過去のログに新規のログを上書きすることはなく、その時点で監査用ログ記録制御情報が定める縮退動作に移行させる。そして、ログサーバ３と通信可能状態となり、ログ送信ができ、ログ容量が減ってログ書込みが再度可能になれば縮退動作から通常状態へ復帰させる。この場合、ログ容量が上限に（あるいはディスク残容量が下限に）近づいているときユーザに注意を促す表示を行うことも可能である。

図４の制御情報の例においては、ログラップ書き込みはＩＤ４のクライアントコンピュータとなり、ログ上限無し書込み設定はＩＤ２のクライアントコンピュータ、ログ上限あり縮退設定はＩＤ１，ＩＤ３のクライアントコンピュータとなる。

【００１７】

図５は、クライアントコンピュータ１に実装された情報漏洩監視プログラム１２が管理サーバ２から監査用ログ記録制御情報を受信する場合の手順を示すフローチャートであり、クライアントコンピュータ１が起動されると（ステップ５０１）、情報漏洩監視プログラム１２はステップ５０２～５１１の処理を実行する。

すなわち、管理サーバ２と通信し（ステップ５０３）、管理サーバ２側で監査用ログ記録制御情報が変更されていることが管理サーバ２からの通知情報によって判定し（ステップ５０４）、変更されていた場合には管理サーバ２から最新の監査用ログ記録制御情報を受信し（ステップ５０５）、ハードディスク１４内に記憶されている監査用ログ記録制御情報を最新の情報に更新する（ステップ５０６）。なお、この監査用ログ記録制御情報は

クライアントコンピュータ１のユーザによって改変不可能に記憶される。
監査用ログ記録制御情報が変更されていなかった場合、ステップ５０８に進む。
クライアントコンピュータ１の監査用ログ記録制御情報が更新されると、管理サーバ２の監査用ログ記録制御情報ＤＢ２１内の当該クライアントコンピュータに対応するクライアント設定フラグは設定済みとなる（ステップ５０７）。
次に、監査用ログ記録制御情報を管理サーバ２から定期的に受信する設定であるかを判定し（ステップ５０８）、そうであった場合、設定時間だけスリープし（ステップ５０９）、設定時間を過ぎた段階でステップ５０３以降の処理を繰り返す。
しかし、定期的に受信する設定でなかった場合には、ステップ５１０に移り、ステップ５０２～５０９の繰り返しループを抜ける。
以上の処理により、管理サーバ２で設定された監査用ログ記録制御情報が定期的にクライアントコンピュータ１に反映される。

【００１８】

図６は、監査用ログ記録制御情報によって０ＭＢ以上のログ容量の上限が設定されており、ハードディスク１４に記録したログ容量が設定された上限に達したが、ログサーバ３に送信できない状況では過去のログに新規のログを上書きする形態であるログラップ書き込み時の処理を示すフローチャートであり、アプリケーション１１によりリソースに対して何らかの入出力要求が発生した場合、情報漏洩監視プログラム１２はそのログの記録を試みる（ステップ６０１）。このとき、ハードディスク１４内のログの記録領域が満杯でなければログを書き込み、その書き込みに成功した場合は処理を終了する。
しかし、ログ記憶領域が満杯であった場合、ログサーバ３へハードディスク１４内に記録したログ情報の送信する（ステップ６０４）。そして、ログ送信が成功した場合には、新規のログを書き込み、その書き込みに成功した場合には（ステップ６０６）、処理を終了する。
しかし、ログ送信に失敗した場合には、過去のログ情報を消去して新規のログ情報を上書きする（ステップ６０７）。

【００１９】

図７は、ログ容量の上限が監査用ログ記録制御情報によって無制限（０ＭＢ）に設定されており、過去のログが上書きされることなく制限なしに追加ログとして書込む形態であるログ上限無し書込み時における情報漏洩監視プログラム１２の処理を示すフローチャートである。
ログ容量の上限が監査用ログ記録制御情報によって無制限（０ＭＢ）に設定されていた場合、情報漏洩監視プログラム１２は、現在のログ記録容量に関係なく追加のログ情報を書き込む（ステップ７０１）。

【００２０】

図８は、ログ上限あり縮退動作を行う場合の情報漏洩監視プログラム１２の処理を示すフローチャートである。
ログ容量の上限が監査用ログ記録制御情報によって設定されていた場合に、アプリケーション１１によりリソースに対して何らかの入出力要求が発生した場合、情報漏洩監視プログラム１２はそのログの記録を試みる（ステップ８０１）。このとき、ハードディスク１４内のログ情報の記録済み容量がログ容量上限値で設定されている容量を上回っていた場合、あるいはディスク残量が下限を下回っていた場合（ステップ８０２）、ログサーバ３へハードディスク１４内に記録したログ情報の送信する（ステップ８０６）。そして、ログ送信が成功した場合には（ステップ８０７）、送信済みログ情報を消去し（ステップ７０８）、新規のログを書き込み（ステップ８０９）、処理を終了する。

【００２１】

しかし、ログ送信に失敗した場合には、ユーザに対して、監査用ログ記録制御情報によって設定されている縮退動作になることを通知し（ステップ８１０）、設定された縮退動作に移行させる（ステップ８１２）。
その後、監査用ログ記録制御情報の定期的ログ送信設定で設定された時間周期のログ送

信タイミングになったか、またはユーザによるログ送信指示操作が行われたかを判定し、ログ送信タイミングになった場合、あるいはログ送信指示操作が行われた場合には記録しておいたログ情報をログサーバ３に送信し、ログ情報の記録済み容量がログ容量上限値で設定されている容量を下回った場合、あるいはディスク残量が下限を上回った場合には、縮退動作から通常動作状態に復帰させる（ステップ８１３）。

【００２２】

一方、リソースに対して何らかの入出力要求が発生した場合に、ハードディスク１４内のログ情報の記録済み容量がログ容量上限値で設定されている容量を上回っていなかった場合、あるいはディスク残量が下限を下回っていなかった場合（ステップ８０２）、入出力要求に伴う新規のログ情報を書き込み（ステップ８０３）、ログ容量上限値に近い、またはディスク残量の下限に近いかどうかを判定し（ステップ８０４）、Ｙｅｓであればその旨の通知メッセージを表示し（ステップ８０５）、Ｎｏであれば処理を終了する。

なお、ログ容量上限値に近い、またはディスク残量の下限に近いかどうかは、図４では示していないが、ログ容量上限値及びディスク残量の下限値の付加情報として設定された値を基づき判定するものである。

【００２３】

以上のように本実施の形態においては、組織内の情報処理システムにＬＡＮ等のネットワークで接続されたクライアントコンピュータを比較的長期の出張などで組織外へ持ち出して使用する場合、ログ上限無し書込み設定をクライアントコンピュータへ設定することで、監査用ログ情報の全てをクライアントコンピュータ１のハードディスク１４内に記録し、組織内のネットワークに再接続した際に、記録されたログ情報をログサーバで確実に収集し、解析することが可能になる。

また、通常は社内ネットワークに接続されているべきであるクライアントコンピュータに対してはログ上限あり縮退設定を行っておくことで、不正にネットワークから切り離す、あるいは不正に持ち出すという脅威に対していずれは縮退動作となり、ユーザの操作が制限されることから不正を行おうとするユーザに対する抑止力を与え、情報漏洩を防止するのに貢献することができる。

また、通常はユーザがそのクライアントコンピュータ上で直接に操作を行うことが少なく監査ログがそれ程重要でないログサーバなどではログラップ設定としておけば、ログサーバの故障やネットワーク障害などでログサーバへログ送信ができない状況が続いたときでも監査用ログ情報がログサーバのハードディスクを圧迫することなく、また縮退動作になることもないためログサーバを安定稼動させることができる。

【図面の簡単な説明】

【００２４】

【図１】本発明適用した情報処理システムの実施形態を示すシステム構成図である。

【図２】クライアントコンピュータに実装される情報漏洩監視プログラムの機能説明図である。

【図３】クライアントコンピュータに実装される情報漏洩監視プログラムが管理サーバによって作成されたインストール媒体でクライアントコンピュータにインストールされるものであることを示す説明図である。

【図４】管理サーバの監査用ログ記録制御情報ＤＢに登録される監査用ログ記録制御情報の例を示す図である。

【図５】クライアントコンピュータに実装された情報漏洩監視プログラムが管理サーバから監査用ログ記録制御情報を定期的に受信する情報漏洩監視プログラムの処理を示すフローチャートである。

【図６】ハードディスクに記録したログ容量が設定された上限に達したが、ログサーバに送信できない状況では過去のログに新規のログを上書きする形態であるログラップ書き込み時における情報漏洩監視プログラムの処理を示すフローチャートである。

【図７】ログ容量の上限が監査用ログ記録制御情報によって無制限（０ＭＢ）に設定されており、過去のログが上書きされることなく制限なしに追加ログとして書込む形態である

ログ上限無し書込み時における情報漏洩監視プログラムの処理を示すフローチャートである。

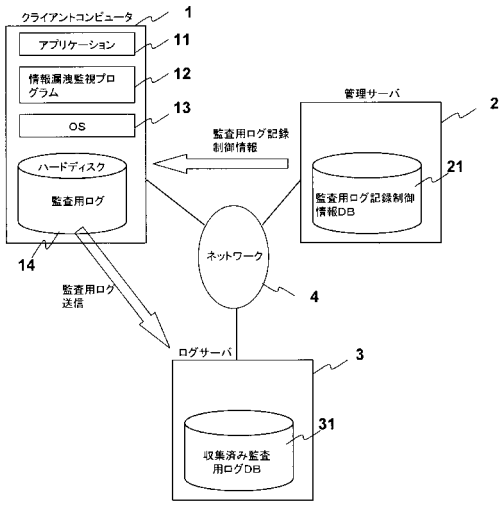
【図８】ログ上限あり縮退動作を行う場合の情報漏洩監視プログラムの処理を示すフローチャートである。

【符号の説明】

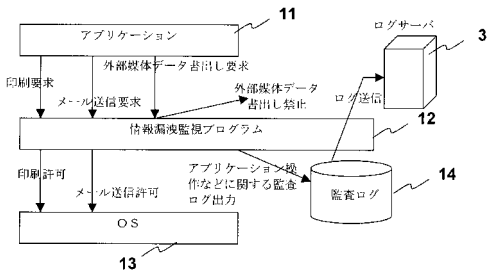
【００２５】

１　クライアントコンピュータ
２　管理サーバ
３　ログサーバ
４　ネットワーク
１１　アプリケーション
１２　情報漏洩監視プログラム
１３　ＯＳ
１４　ハードディスク
２１　監査用ログ記録制御情報ＤＢ
３１　収集済み監査用ログＤＢ

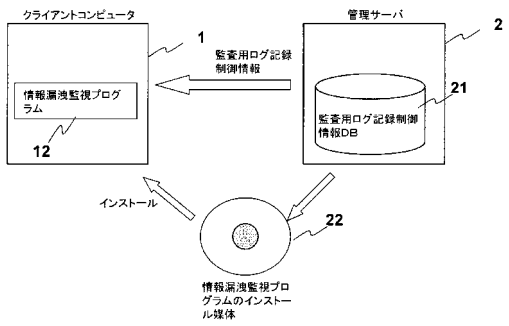
【図１】



【図２】



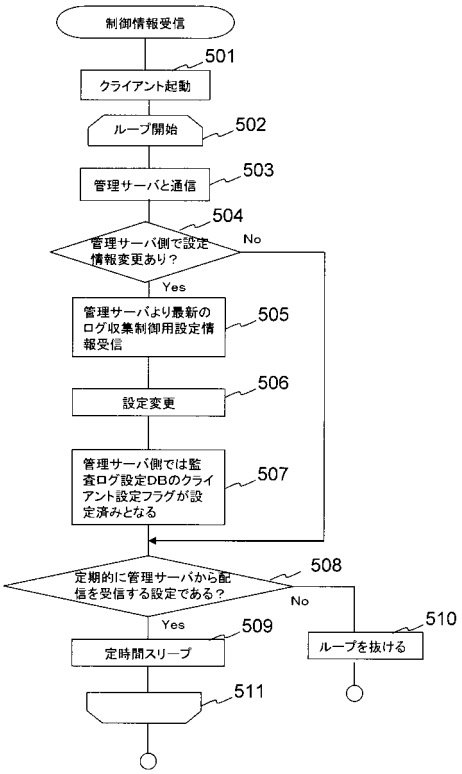
【図３】



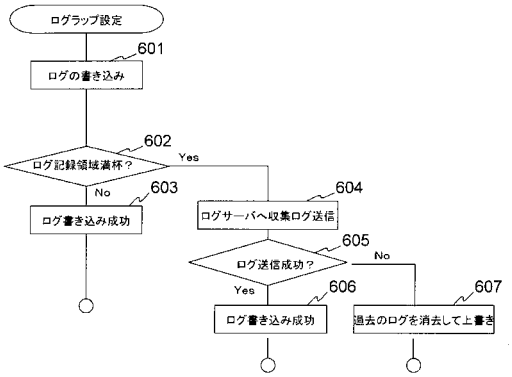
【図４】

クライアントコンピュータID	ログ容量上限	ディスク残容量下限	定期的ログ送信設定	定期的制御情報受信設定	緊退動作フラグ	緊退動作詳細設定	クライアント設定フラグ
ID1	1MB	20MB	0sec	あり	ON	全操作禁止	済み
ID2	0MB	−	60sec	あり	−	−	未済
ID3	5MB	20MB	3600sec	あり	ON	印刷のみ許可	済み
ID4	0.5MB	−	7200sec	なし	OFF	−	済み

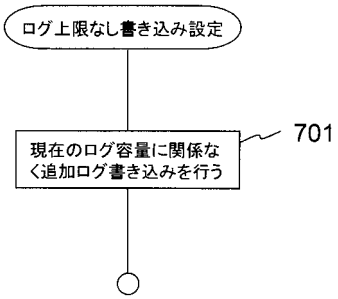
【図５】



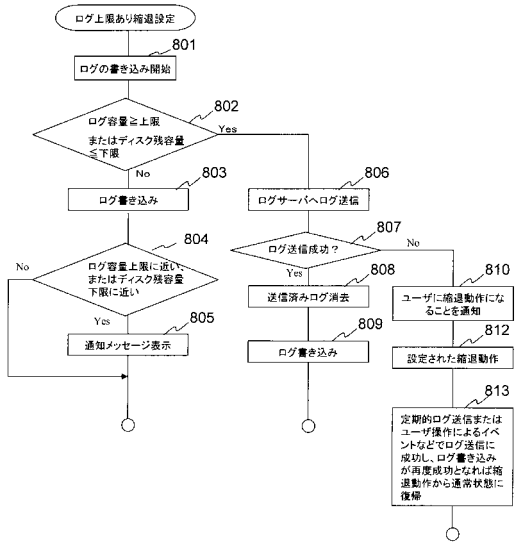
【図６】



【図７】



【図８】


ログ上限あり縮退設定
801
ログの書き込み開始
802
ログ容量≧上限
またはディスク残容量
≦下限
Yes
No
803
ログ書き込み
804
No
ログ容量上限に近い
またはディスク残容量
下限に近い
Yes
805
通知メッセージ表示
806
ログサーバへログ送信
807
ログ送信成功？
No
Yes
808
送信済みログ消去
809
ログ書き込み
810
ユーザに縮退動作になることを通知
812
設定された縮退動作
813
定期的ログ送信またはユーザ操作によるイベントなどでログ送信に成功し、ログ書き込みが再度成功となれば縮退動作から通常状態に復帰

フロントページの続き

(72)発明者　南城　勝将
東京都品川区東品川４丁目１２番７号　日立ソフトウエアエンジニアリング株式会社内

審査官　和田　財太

(56)参考文献　特開２００１－３５０６５２（ＪＰ，Ａ）
特開２００５－２９３４２６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　１１／３４
Ｇ０６Ｆ　２１／２０