(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2005-149267
(P2005-149267A)
(43)公開日　平成17年6月9日(2005.6.9)

(51)Int.Cl.[7]	F I	テーマコード（参考）
G06F 1/00	G06F 1/00 370E	

審査請求 未請求　請求項の数 10　ＯＬ　（全 12 頁）

(21)出願番号　特願2003-387671 (P2003-387671)
(22)出願日　平成15年11月18日 (2003.11.18)

(71)出願人　397067853
株式会社インテリジェントウェイブ
東京都江東区木場５丁目１２番８号
(74)代理人　100117592
弁理士　土生　哲也
(72)発明者　青木　修
東京都江東区木場５丁目１２番８号　株式会社インテリジェントウェイブ内
(72)発明者　河野　裕晃
東京都江東区木場５丁目１２番８号　株式会社インテリジェントウェイブ内

(54)【発明の名称】証拠画面保存プログラム、証拠画面保存方法及び証拠画面保存システム

(57)【要約】
【課題】　コンピュータに対して行われた不正操作の発生時点において、速やかに証拠画面を保存することが可能な証拠画面保存プログラムを提供する。
【解決手段】　コンピュータがオペレーションを受け付けると、ルール等を参照して不正操作であるか否かの判定を行う。不正操作と判定されると、ＶＲＡＭやデバイスコンテキストより当該オペレーションにより画面に表示される表示データを取得して、日時等を付した証拠資料として証拠データ格納部に格納する。かかる証拠データや不正の通知は、ネットワークを通じて管理者に送信してもよい。不正操作に対しては、オペレーションの中止やネットワークの切断等の停止処理が行われる。
【選択図】　図５

【特許請求の範囲】
【請求項１】
コンピュータに対して行われた不正操作の証拠画面を保存するための証拠画面保存プログラムであって、前記コンピュータに、
前記コンピュータが受け付けたオペレーションが不正操作であるかを判定するステップと、
前記オペレーションが不正操作であると判定されると、前記オペレーションにより前記コンピュータの画面に表示される表示データを取得するステップと、
前記表示データに前記オペレーションを特定する情報を付した証拠データを証拠データ格納部に格納するステップと、
を実行させるための証拠画面保存プログラム。
【請求項２】
前記コンピュータに、前記オペレーションが不正操作であると判定されると、前記コンピュータにかかるキーストローク、ネットワーク、アプリケーション又はオペレーションシステムの少なくとも一つのログを記録するステップを実行させること
を特徴とする請求項１記載の証拠画面保存プログラム。
【請求項３】
コンピュータに対して行われた不正操作の証拠画面を保存するための証拠画面保存プログラムであって、前記コンピュータに、
前記コンピュータが受け付けたオペレーションが不正操作であるかを判定するステップと、
前記オペレーションが不正操作であると判定されると、前記オペレーションにより前記コンピュータの画面に表示される表示データを取得するステップと、
前記表示データに前記オペレーションを特定する情報を付した証拠データを、ネットワークを通じて管理サーバに送信するステップと、
を実行させるための証拠画面保存プログラム。
【請求項４】
前記コンピュータに、前記オペレーションが不正操作であると判定されると、前記コンピュータにかかるキーストローク、ネットワーク、アプリケーション又はオペレーションシステムの少なくとも一つのログを前記管理サーバに送信するステップを実行させること
を特徴とする請求項３記載の証拠画面保存プログラム
【請求項５】
前記表示データを取得するステップにおいては、仮想化されたディスプレイ領域に前記オペレーションによって書き出されたデータを表示データとして取得すること
を特徴とする請求項１乃至４いずれかに記載の証拠画面保存プログラム。
【請求項６】
前記表示データを取得するステップにおいては、前記コンピュータの画面表示を行うためのバッファに前記オペレーションによって書き出されたデータを表示データとして取得すること
を特徴とする請求項１乃至４いずれかに記載の証拠画面保存プログラム。
【請求項７】
コンピュータに対して行われた不正操作の証拠画面を保存するための証拠画面保存方法であって、
前記コンピュータが、前記コンピュータが受け付けたオペレーションが不正操作であるかを判定するステップと、
前記コンピュータが、前記オペレーションが不正操作であると判定されると、前記オペレーションにより前記コンピュータの画面に表示される表示データを取得するステップと、
前記コンピュータが、前記表示データに前記オペレーションを特定する情報を付した証拠データを証拠データ格納部に格納するステップと、
を有することを特徴とする証拠画面保存方法。

【請求項８】
コンピュータに対して行われた不正操作の証拠画面を保存するための証拠画面保存方法であって、
前記コンピュータが、前記コンピュータが受け付けたオペレーションが不正操作であるかを判定するステップと、
前記コンピュータが、前記オペレーションが不正操作であると判定されると、前記オペレーションにより前記コンピュータの画面に表示される表示データを取得するステップと、
前記コンピュータが、前記表示データに前記オペレーションを特定する情報を付した証拠データを、ネットワークを通じて管理サーバに送信するステップと、
前記管理サーバが、前記証拠データを証拠データ格納部に格納するステップと、
を有することを特徴とする証拠画面保存方法。
【請求項９】
コンピュータに対して行われた不正操作の証拠画面を保存するための証拠画面保存システムであって、
前記コンピュータが受け付けたオペレーションが不正操作であるかを判定する不正操作判定手段と、
前記不正操作判定手段においてオペレーションが不正操作であると判定されると、前記オペレーションにより前記コンピュータの画面に表示される表示データを取得する表示データ取得手段と、
前記表示データ取得手段の取得した表示データに前記オペレーションを特定する情報が付された証拠データを格納する証拠データ格納手段と、
を備えることを特徴とする証拠画面保存システム。
【請求項１０】
前記不正操作判定手段においてオペレーションが不正操作であると判定されると、前記コンピュータにかかるキーストローク、ネットワーク、アプリケーション又はオペレーションシステムの少なくとも一つのログを記録するログ記録手段を備えること
を特徴とする請求項９記載の証拠画面保存システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、コンピュータに対して行われた不正操作の証拠画面を保存するための証拠画面保存プログラム、証拠画面保存方法及び証拠画面保存システムに関するものである。
【背景技術】
【０００２】
特に企業等がコンピュータで重要情報を取り扱う場合、コンピュータをインターネット等のネットワークに接続して使用する場合であれば、外部からの不正なデータの侵入を防止するとともに、コンピュータの不正操作による内部からのデータ流出や漏洩を防止することが必要になる。また、コンピュータをネットワークに接続せずにスタンドアローンで用いる場合も、コンピュータ内のデータの不正なコピーやデータを消去、破壊する操作など、不正操作を防止することが必要になる。
【０００３】
このような不正操作を防止するために、一つにはコンピュータやネットワークの操作履歴をログとして記録し、トラブルが生じた場合にはログを参照して不正の発生源を特定することが一般的に行われている。また、不正操作を速やかに検出してトラブルの発生を未然に防止するために、不正操作のパターンをルールとして登録し、コンピュータの実行するオペレーションをかかるルールと対比して不正操作を判定する方法も用いられるようになっている。
【０００４】
上記の方法により不正が検出された場合、不正を停止させるための方法として、実行中のオペレーションの中断、管理者への報告や操作者への警告などの処理が実行される。例

えば、ネットワークにおける不正操作を監視する場合であれば、通信を切断するとともに、管理者に通知レポートを、操作者に警告レポートを送信する方法が開示されている（特許文献１参照）。また、コンピュータに対する操作を監視する場合であれば、モニタに警告メッセージを出す方法が開示されている（特許文献２参照）。

【０００５】

【特許文献１】特開２００２－２３２４５１号公報　段落番号０００５

【特許文献２】特開２００２－２５８９７２号公報　段落番号００３４

【発明の開示】

【発明が解決しようとする課題】

【０００６】

前記特許文献記載の方法のように、不正操作そのものを停止させることは重要であるが、例えば不正操作を行った者に対して法的措置をとる場合においては、不正操作の証拠を保存することが重要である。また、法的措置にまでは至らなくても、社内において業務時間中に社員が娯楽用のＷｅｂサイトを閲覧していることに注意を与える場合など、閲覧を行った記録が保存されていることが好ましい。

【０００７】

このような証拠資料は、ログを記録することによっても可能であるが、不正が発生した場合には該当するログの特定を行わなければならない。また、アクセスしたファイルが変更されていたり、ファイルが削除されてしまった場合には、不正が行われていた時点での操作状況を再現することができないという問題を有しており、不正が発生した時点において即座に確実な証拠を保存することが好ましい。

【０００８】

本発明は、このような課題に対応してなされたものであり、コンピュータに対して行われた不正操作の発生時点において、速やかに証拠画面を保存することが可能な証拠画面保存プログラム、証拠画面保存方法及び証拠画面保存システムを提供することを目的とするものである。

【課題を解決するための手段】

【０００９】

上記の課題を解決する第一の発明は、コンピュータに対して行われた不正操作の証拠画面を保存するための証拠画面保存プログラムであって、前記コンピュータに、前記コンピュータが受け付けたオペレーションが不正操作であるかを判定するステップと、前記オペレーションが不正操作であると判定されると、前記オペレーションにより前記コンピュータの画面に表示される表示データを取得するステップと、前記表示データに前記オペレーションを特定する情報を付した証拠データを証拠データ格納部に格納するステップと、を実行させるための証拠画面保存プログラムである。前記コンピュータに、前記オペレーションが不正操作であると判定されると、前記コンピュータにかかるキーストローク、ネットワーク、アプリケーション又はオペレーションシステムの少なくとも一つのログを記録するステップを実行させることを特徴とすることもできる。

【００１０】

第一の発明においては、不正操作と判定されたオペレーションによりコンピュータの画面に表示される表示データを保存することにより、不正操作が行われた証拠を速やかに保存することができる。コンピュータの操作履歴は常時ログとして記録してもよいが、不正操作であると判定された後のログを記録することにより、画面の表示データと併せて不正操作が行われた証拠を効果的に保存することができる。

【００１１】

尚、本発明において不正操作の判定には、予め登録されたルールベースによる判定の他、ユーザの操作傾向を分析したユーザプロファイルによる判定などどのような判定方法を用いてもよい。また、保存する表示データのファイル形式は、画面表示を再現できるものであればよく、特定の形式に限定されるものではない。オペレーションを特定するための情報には、オペレーションを行ったユーザのユーザＩＤ、オペレーションが行われた時刻

等が用いられる。

【００１２】

上記の課題を解決する第二の発明は、コンピュータに対して行われた不正操作の証拠画面を保存するための証拠画面保存プログラムであって、前記コンピュータに、前記コンピュータが受け付けたオペレーションが不正操作であるかを判定するステップと、前記オペレーションが不正操作であると判定されると、前記オペレーションにより前記コンピュータの画面に表示される表示データを取得するステップと、前記表示データに前記オペレーションを特定する情報を付した証拠データを、ネットワークを通じて管理サーバに送信するステップと、を実行させるための証拠画面保存プログラムである。前記コンピュータに、前記オペレーションが不正操作であると判定されると、前記コンピュータにかかるキーストローク、ネットワーク、アプリケーション又はオペレーションシステムの少なくとも一つのログを前記管理サーバに送信するステップを実行させることを特徴としてもよい。

【００１３】

第二の発明においては、第一の発明と同様に取得した表示データを管理サーバに送信して、管理サーバで不正操作を集中監視することにより、不正操作が行われた証拠を保存するとともに、管理者による速やかな対応を行うことができる。ログを記録して証拠性を高めることができることや、不正操作の判定方法、表示データのファイル形式、オペレーションを特定する情報に関する要件については、第一の発明と同様である。

【００１４】

また、第一の発明及び第二の発明は、前記表示データを取得するステップにおいては、仮想化されたディスプレイ領域に前記オペレーションによって書き出されたデータを表示データとして取得することを特徴とすることもできる。

【００１５】

本発明においては、証拠として不正操作によって画面に表示される表示データを特定することが必要になるが、画面に表示される表示データは、デバイスコンテキスト等の仮想化されたディスプレイ領域に書き出されたデータより特定することができる。

【００１６】

さらに、第一の発明及び第二の発明は、前記表示データを取得するステップにおいては、前記コンピュータの画面表示の行うためのバッファに前記オペレーションによって書き出されたデータを表示データとして取得することを特徴とすることもできる。

【００１７】

不正操作によって画面に表示される表示データを特定するためには、コンピュータの画面表示用のビデオボードに設けられたＶＲＡＭ等の画面表示を行うためのバッファに書き出されたデータを取得することとしてもよい。

【００１８】

第一の発明及び第二の発明は、上記の証拠画面保存プログラムの実行により行うことができる証拠画面保存方法として把握することもできる。また、上記の証拠画面保存プログラムを用いた証拠画面保存システムとして構成することもできる。

【００１９】

つまり、第一の発明に対応する証拠画面保存方法は、コンピュータに対して行われた不正操作の証拠画面を保存するための証拠画面保存方法であって、前記コンピュータが、前記コンピュータが受け付けたオペレーションが不正操作であるかを判定するステップと、前記コンピュータが、前記オペレーションが不正操作であると判定されると、前記オペレーションにより前記コンピュータの画面に表示される表示データを取得するステップと、前記コンピュータが、前記表示データに前記オペレーションを特定する情報を付した証拠データを証拠データ格納部に格納するステップと、を有することを特徴とする証拠画面保存方法である。

【００２０】

また、第二の発明に対応する証拠画面保存方法は、コンピュータに対して行われた不正操作の証拠画面を保存するための証拠画面保存方法であって、前記コンピュータが、前記

コンピュータが受け付けたオペレーションが不正操作であるかを判定するステップと、前記コンピュータが、前記オペレーションが不正操作であると判定されると、前記オペレーションにより前記コンピュータの画面に表示される表示データを取得するステップと、前記コンピュータが、前記表示データに前記オペレーションを特定する情報を付した証拠データを、ネットワークを通じて管理サーバに送信するステップと、前記管理サーバが、前記証拠データを証拠データ格納部に格納するステップと、を有することを特徴とする証拠画面保存方法である。

【００２１】

さらに、第一の発明及び第二の発明に対応する証拠画面保存システムは、コンピュータに対して行われた不正操作の証拠画面を保存するための証拠画面保存システムであって、前記コンピュータが受け付けたオペレーションが不正操作であるかを判定する不正操作判定手段と、前記不正操作判定手段においてオペレーションが不正操作であると判定されると、前記オペレーションにより前記コンピュータの画面に表示される表示データを取得する表示データ取得手段と、前記表示データ取得手段の取得した表示データに前記オペレーションを特定する情報が付された証拠データを格納する証拠データ格納手段と、を備えることを特徴とする証拠画面保存システムである。前記不正操作判定手段においてオペレーションが不正操作であると判定されると、前記コンピュータにかかるキーストローク、ネットワーク、アプリケーション又はオペレーションシステムの少なくとも一つのログを記録するログ記録手段を備えることを特徴とすることもできる。

【発明の効果】

【００２２】

本発明により、コンピュータに対して行われた不正操作の発生時点において、速やかに証拠資料として画面に表示されたデータを保存することができるので、法的措置が必要な場合等においても不正操作の事実を容易に証明することが可能になる。その結果、コンピュータの利用者に対しても抑止効果が働き、不正操作の発生を予防する効果も期待することができる。

【発明を実施するための最良の形態】

【００２３】

本発明を実施するための最良の形態について、図面を用いて以下に詳細に説明する。尚、以下の説明は本発明の実施形態の一例であって、本発明はかかる実施形態に限定されるものではない。

【００２４】

図１は、本発明にかかる証拠画面保存システムをネットワークに接続された端末の監視に用いる例の全体構成を示す図である。図２は、本発明にかかる証拠画面保存システムをネットワークに接続された端末の監視に用いる例におけるネットワーク上の監視位置を示す図である。図３は、本発明にかかる証拠画面保存システムをネットワークに接続された端末の監視に用いる例の機能の概要を示す図である。図４は、本発明にかかる証拠画面保存プログラムを用いた不正監視システムの構成を示すブロック図である。図５は、本発明にかかる証拠画面保存プログラムによる処理の概要を示す図である。図６は、本発明にかかる証拠画面保存プログラムにより取得された証拠データを格納するテーブルの一例を示す図である。図７は、本発明にかかる証拠画面保存プログラムの処理手順を示すフローチャートである。

【００２５】

本発明にかかる証拠画面保存システムはコンピュータに対して行った不正操作の証拠画面を保存するものであるが、スタンドアローンで使用されているコンピュータに用いるものであってもよいし、ネットワークに接続されたコンピュータの監視に用いることとしてもよい。前者の場合は、証拠画面に関するデータはユーザが使用するコンピュータに保存されるが、後者の場合は、ネットワーク全体の不正を監視する不正監視サーバにまとめて保存することとしてもよい。

【００２６】

図１は、後者のネットワークに接続されたコンピュータの監視に用いる例を示したものである。図１において、複数のユーザ端末はＬＡＮ等の社内ネットワークで接続され、社内ネットワークはインターネットと接続されている。不正監視サーバはネットワーク上を流れるデータを監視して、インターネットとの間での不正な情報の送受信などの行為を監視している。

【００２７】

図１の例においては、本発明にかかる証拠画面保存システムは、２つの部分において不正操作を監視している。一つはユーザ端末上で実行されるオペレーションを監視し、不正操作であると判定されると、不正操作時点の操作画面をキャプチャーして、当該ユーザ端末又は不正監視サーバに格納する。もう一つは、不正監視サーバがネットワークを流れるデータを監視し、不正操作に該当するデータを検出すると、当該データを送受信するユーザ端末を特定して、当該データによりユーザ端末に表示される操作画面をキャプチャーして、当該ユーザ端末又は不正監視サーバに格納する。

【００２８】

尚、不正監視サーバがネットワーク上でデータを監視する位置については、図２の例に示したように、ユーザ端末内において実行されるデータの監視の他に、ネットワークのセグメント単位で送受信されるデータの監視、メールサーバにおけるデータの監視、ゲートウェイにおけるデータの監視など、様々な位置に配置することができる。

【００２９】

図３は、本発明にかかる証拠画面保存システムをネットワークに接続されたコンピュータの監視に用いる場合について、ユーザ端末と不正監視サーバのそれぞれの機能の一例を示したものである。ユーザ端末では本発明にかかる証拠画面保存プログラムが実行され、不正操作を検出すると、ディスプレイに警告メッセージを表示するとともに、警告音を発生させる。併せて、不正操作により表示された画面をキャプチャーして、発生時刻等の情報とともに画面の表示データを、端末の識別情報を付した証拠データとして不正監視サーバに送信する。

【００３０】

不正監視サーバでは、端末の識別情報や発生時刻等の情報をキーに分類された証拠データが格納される。証拠データの他に、不正発生後の操作についての各種ログをユーザ端末から取得して格納することとしてもよい。不正監視サーバにおいてもディスプレイに警告メッセージを表示するとともに、警告音を発生させて、管理者に不正操作の発生を速やかに通知することとしてもよい。

【００３１】

図４を用いて、本発明にかかる証拠画面保存プログラムを用いた不正監視システムの構成について説明する。ユーザ端末１０には、ＣＰＵ１１、ＲＡＭ１２、ＲＯＭ１３、ＨＤＤ１４及びビデオボード１５を備えられている。ＨＤＤ１４には、本発明にかかる証拠画面保存プログラムを含めた不正操作を監視するための不正監視プログラム１４１が格納されていて、不正操作を判定するためのルールを格納する不正ルール格納部１４２、不正操作が行われた場合の証拠画面に関するデータを格納する証拠データ格納部１４３が備えられている。ビデオボード１５には、ディスプレイ１７に表示するための画面内容を書き込むバッファであるＶＲＡＭ１６が備えられている。尚、不正監視プログラム１４１を格納するＨＤＤ１４については、フラッシュメモリなどプログラムを格納することができるその他の記憶媒体を用いるものであってもよい。

【００３２】

ＨＤＤ１４に格納された不正監視プログラム１４１による監視を実行するためには、ＲＯＭ１３に記憶された入力制御や出力制御などのハードウェア制御のための基本的な各種プログラムを起動し、ＲＡＭ１２を不正監視プログラム１４１のワークエリアとして機能させながら、ＣＰＵ１１が演算処理を行う。不正操作の判定は、ユーザ端末１０が受け付けたオペレーションを不正ルール格納部１４２に格納されたルールと対比する演算処理により行われ、不正操作であると判定されると当該オペレーションによりディスプレイ１７

に表示される画面のキャプチャーを行う。

【００３３】

ここでキャプチャーすべき画面の表示データは、ＣＰＵ１１及びＲＡＭ１２における演算処理において、デバイスコンテキスト等の仮想化されたディスプレイ領域に書き出されたデータを取得することにより、特定することができる。又は、ディスプレイ１７に表示を行うためのバッファであるＶＲＡＭ１６に当該オペレーションによって書き出されたデータを取得して、特定することもできる。

【００３４】

キャプチャーされた画面の表示データは、オペレーションを行ったユーザのＩＤやオペレーションを受け付けた時刻など、当該オペレーションを識別するためのデータを付与して、証拠データ格納部１４３に格納される。図６は、このように取得された証拠データを格納するテーブルの一例を示すものであるが、対象となるオペレーション毎に設けられたレコードに、オペレーションの受付日時やユーザＩＤとともに、ディスプレイに表示された表示データのファイル名が記録されている。かかる画面ファイル自体も、証拠データ格納部１４３に格納されるが、ファイルの形式はどのような形式であってもよい。

【００３５】

また、不正が発生した後は、不正操作を行った直接のオペレーション以外にも、当該コンピュータに対して行われた操作、例えばキーストローク、ネットワーク、アプリケーション又はオペレーションシステムなどのログを記録することとしてもよい。かかるログは、当該ユーザの操作履歴を証明し、証拠画面と併せて不正操作が行われたことを立証することに用いることができるため、不正の発生の如何に関わらず常時ログをとることとしてもよいが、ログを記録するハードウェアのリソースを考慮すると、不正の発生後からログを記録するよう構成することが好ましい。

【００３６】

尚、ユーザ端末１０に設けられる不正ルール格納部１４２は、ユーザ端末１０を含むネットワークを監視する不正監視サーバ２０に不正ルール格納部２１として設けられていてもよい。一般に、不正を判定するルールをユーザ単位で設定する場合には、ユーザ端末１０に設けられる不正ルール格納部１４２を用いることが好ましく、同一のネットワークに属する複数の端末に共通ルールを適用するときは、不正監視サーバ２０に設けられる不正ルール格納部２１を用いることが好ましい。

【００３７】

また、取得した証拠データはユーザ端末１０内の証拠データ格納部１４３に格納してもよいが、証拠データを削除されるリスクを軽減するためには、管理者の管理下にある不正監視サーバ２０に設けられる証拠データ格納部２２を用いることが好ましい。

【００３８】

図５は、本発明にかかる証拠画面保存プログラムによる処理の概要を示している。尚、以下に説明する各部は物理的に分離されているものではなく、図４で示したように各々を実行する不正監視プログラム１４１の一部のプログラムとしてＨＤＤ１４に格納されており、順次読み出されてＲＡＭ１２をワークエリアとして機能させながら、ＣＰＵ１１により演算処理が実行されるものであってもよい。

【００３９】

まず、ユーザ端末がオペレーションを受け付けると、不正判定部において当該オペレーションが不正操作であるか否かの判定を行う。かかる判定は、一般的な不正のパターンから作成された不正ルール格納部に格納されたルールと対比して行うことができるが、ルールベースによる判定に限定されるものではなく、ユーザの操作パターンから作成されたユーザプロファイル等と対比して、特異な行動か否かから不正操作を判定することとしてもよい。

【００４０】

当該オペレーションが不正操作であると判定されると、表示データ取得部において当該オペレーションによりユーザ端末のディスプレイに表示される表示データを取得する。取

得する表示データは、ＶＲＡＭ又はデバイスコンテキストに書き出されたデータから特定する。表示データは画像ファイルとして保存され、オペレーションの受付日時やユーザＩＤなど当該オペレーションを特定するための情報を付して、証拠データ格納部に格納される。また、かかる証拠データは、ネットワークを通じて管理用のサーバ等に送信して保存することとしてもよい。さらに、不正操作を中止させるために、停止処理実行部において警告メッセージの表示、警告音の発生、オペレーションの中止処理、ネットワークの切断などの処理を実行することとしてもよい。

【００４１】

警告メッセージの表示や警告音の発生は、ユーザ端末側において行ってもよいし、管理用のサーバ側において行うこととしてもよい。ユーザ端末側で行う場合については、不正を検出しない場合においても、特定の時間、ランダム、起動時など様々な設定を行ってダミーの警告メッセージや警告音を発して監視が行われていることを明らかにすることにより、ユーザに対する抑止効果を高めることもできる。この場合は、実際に画面のキャプチャーまで行うこととしてもよい。

【００４２】

図７のフローチャートを用いて、本発明にかかる証拠画面保存プログラムの処理手順について説明する。まず、不正操作であるか否かを判定するための、コンピュータが受け付けたデータを取得する（Ｓ０１）。次に、不正ルールデータベースに格納されたルールを参照し（Ｓ０２）、取得したデータと対比して不正ルールに該当するか否かを判定する（Ｓ０３）。不正ルールに該当しなければ、不正操作の判定処理は終了する。

【００４３】

不正ルールに該当する場合には、ユーザが操作するコンピュータに警告音又は警告メッセージを発生させるか否かの設定を確認する（Ｓ０４）。発生の設定がされている場合には、警告音又は警告メッセージを発生させる（Ｓ０５）。続いて、デバイスコンテキストから不正判定を行った操作により表示される表示データを取得する（Ｓ０６）。表示データは、日付等の不正操作を特定するための情報が付されて（Ｓ０７）、証拠資料としてデータベース等に格納される（Ｓ０８）。さらに、表示データを管理サーバに送信するか否かの設定を確認し（Ｓ０９）、送信の設定がされている場合には管理サーバにも送信される（Ｓ１０）。

【図面の簡単な説明】

【００４４】

【図１】本発明にかかる証拠画面保存システムをネットワークに接続された端末の監視に用いる例の全体構成を示す図である。

【図２】本発明にかかる証拠画面保存システムをネットワークに接続された端末の監視に用いる例におけるネットワーク上の監視位置を示す図である。

【図３】本発明にかかる証拠画面保存システムをネットワークに接続された端末の監視に用いる例の機能の概要を示す図である。

【図４】本発明にかかる証拠画面保存プログラムを用いた不正監視システムの構成を示すブロック図である。

【図５】本発明にかかる証拠画面保存プログラムによる処理の概要を示す図である。

【図６】本発明にかかる証拠画面保存プログラムにより取得された証拠データを格納するテーブルの一例を示す図である。

【図７】本発明にかかる証拠画面保存プログラムの処理手順を示すフローチャートである。

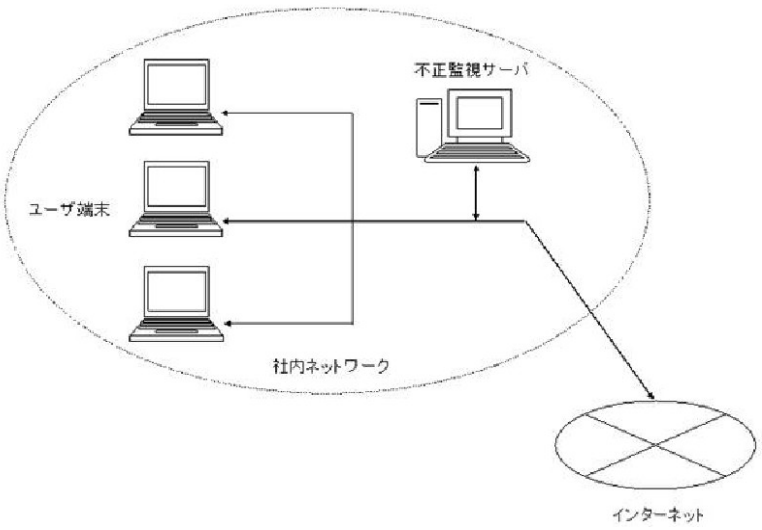
【符号の説明】

【００４５】

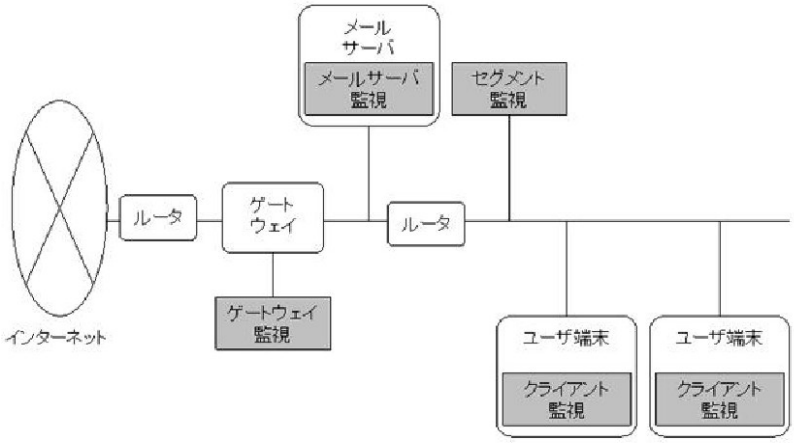
１０　ユーザ端末
１１　ＣＰＵ
１２　ＲＡＭ
１３　ＲＯＭ

１４　　ＨＤＤ
１４１　不正監視プログラム
１４２　不正ルール格納部
１４３　証拠データ格納部
１５　　ビデオボード
１６　　ＶＲＡＭ
１７　　ディスプレイ
２０　　不正監視サーバ
２１　　不正ルール格納部
２２　　証拠データ格納部

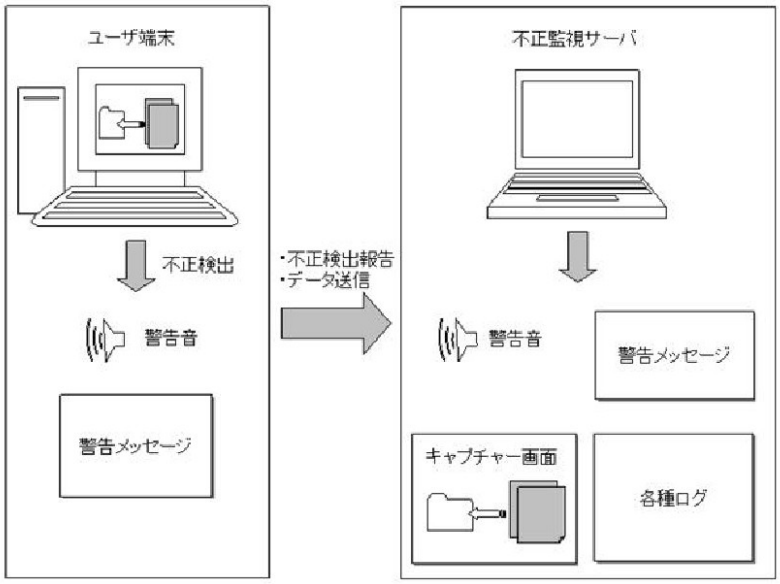
【図１】



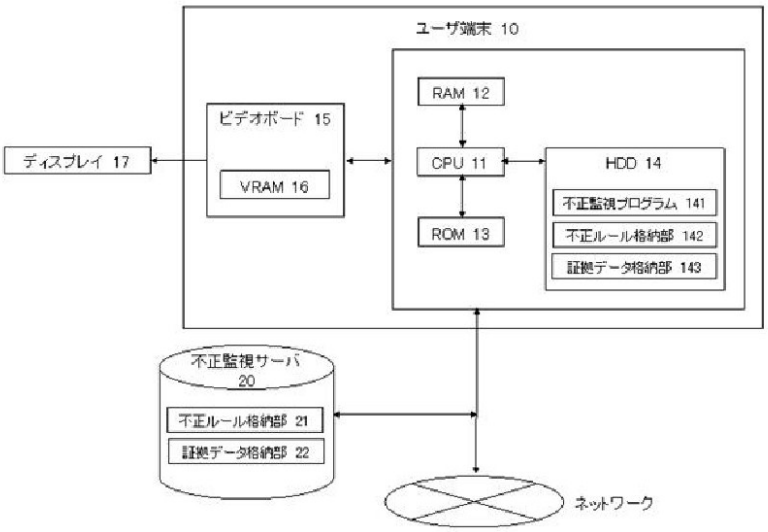
【図２】


メール
サーバ
メールサーバ
監視
セグメント
監視
ルータ
ゲート
ウェイ
ルータ
インターネット
ゲートウェイ
監視
ユーザ端末
クライアント
監視
ユーザ端末
クライアント
監視

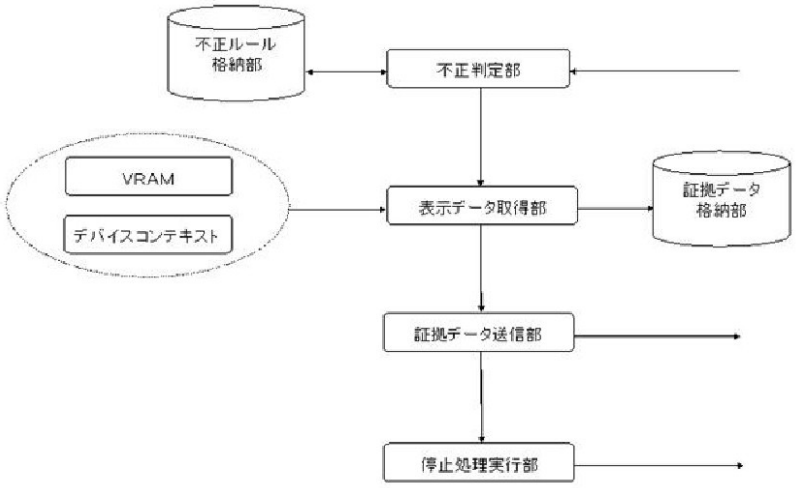
【図３】


ユーザ端末
不正検出
警告音
警告メッセージ
・不正検出報告
・データ送信
不正監視サーバ
警告音
警告メッセージ
キャプチャー画面
各種ログ

【図４】


ユーザ端末 10
RAM 12
ビデオボード 15
ディスプレイ 17
VRAM 16
CPU 11
HDD 14
不正監視プログラム 141
不正ルール格納部 142
証拠データ格納部 143
ROM 13
不正監視サーバ
20
不正ルール格納部 21
証拠データ格納部 22
ネットワーク

【図５】



【図６】

年月日	時間	不正の種類	ユーザID	画面ファイル	通知済
2003.10.23	10:20	不正コピー	10001	001.gif	1
2003.10.23	12:32	ファイル更新	10002	002.gif	0
2003.10.24	22:52	不正ログイン	10001	003.gif	1
・ ・ ・					

【図７】