

明 細 書

発明の名称：

端末装置、ファイル分析装置、ファイル分析システム、ファイル分析方法
およびプログラム

技術分野

[0001] 本発明は、端末装置、ファイル分析装置、ファイル分析システム、ファイル分析方法およびプログラムに関する。

本願は、2018年9月26日に日本に出願された特願2018-180718号に基づき優先権を主張し、その内容をここに援用する。

背景技術

[0002] 分析対象となるシステムにおいて発生するログを取得して分析するログ分析システムが知られている（例えば、特許文献1参照。）。当該ログとして、例えば、セキュリティに関するログがある。

このようなログ分析システムでは、セキュリティ用のセンサが、分析対象となるシステムにおいて発生するログを監視して検出する。このような監視は、常時行われる。また、当該ログ分析システムでは、分析対象となるシステムが、センサによって検出されたログをネットワークを介してログ分析装置に伝送する。また、当該ログ分析システムでは、ログ分析装置が、分析対象となるシステムから伝送されたログを分析する。

[0003] しかしながら、このようなログ分析システムを動作させるためには、センサによって検出されたログをログ分析装置に伝送するための設定が必要であった。当該設定としては、例えば、センサの環境を整えるための設定、および、ネットワークの環境を整えるための設定を含む。

このため、ログ分析システムを動作させるために、このような環境の設定を行う作業に時間および負担がかかる場合があった。また、ログ分析システムを動作させるために、センサの環境およびネットワークの環境を変更する必要があるが、分析対象となるシステムを有する組織等によっては、このよ

うな変更の許可を得ることが難しい場合があった。

先行技術文献

特許文献

[0004] 特許文献1：特許第5640166号公報

発明の概要

発明が解決しようとする課題

[0005] 上記のように、従来では、ログ分析システムを動作可能な状態にするための初期的な負担が大きかった。

[0006] 本発明の実施形態は、このような事情に鑑み、簡易にログの分析を行うことができる端末装置、ファイル分析装置、ファイル分析システム、ファイル分析方法およびプログラムを提供する。

課題を解決するための手段

[0007] 本発明の一態様に係る端末装置は、ログを常時監視し常時監視された前記ログを出力するセキュリティセンサから出力された複数の前記ログのうちの一部の前記ログを取得し、取得された前記ログを含むファイルを生成するファイル生成部と、前記ファイル生成部によって生成された前記ファイルを、1回の分析対象となる1個または複数個の前記ファイルに含まれる前記ログの情報が許容されるデータ量の上限値以下であるという条件が満たされる場合にファイル分析を行うファイル分析装置に送信するファイル送信部と、前記ファイル分析装置から送られる前記ファイルの分析結果の通知を受ける通知制御部と、前記1回の分析対象となる1個または複数個の前記ファイルに含められる予定の前記ログの情報が許容されるデータ量の前記上限値以下であるという条件が満たされるか否かを判定するファイル条件判定部と、前記ファイル条件判定部によって前記条件が満たされないと判定された場合、前記ファイルに含められる前記ログのデータ量を削減するログ削減部と、を備え、前記ファイル条件判定部によって前記条件が満たされないと判定された場合、前記ログ削減部によって前記ファイルに含められる前記ログのデータ

量を削減して、前記条件が満たされるようにされた前記ログの情報をを用いて、前記ファイル生成部が前記ファイルを生成し、前記ファイル送信部が前記ファイルを前記ファイル分析装置に送信する、端末装置である。

[0008] 本発明の一態様に係る端末装置において、前記ログ削減部は、前記ログが発生した日時が含まれるべき期間であって当該期間に含まれる前記ログの情報について前記条件が満たされる当該期間が表示されるようにし、前記ログ削減部は、表示された前記期間がユーザの操作によって変更されたときに、前記条件が満たされない場合には、前記条件が満たされるように前記期間を変更し、前記ファイル生成部は、前記条件が満たされる前記期間に含まれる前記ログの情報をを用いて前記ファイルを生成する、構成であってもよい。

本発明の一態様に係る端末装置において、前記ユーザの操作によって1個または2個以上のセンサが指定され、前記ファイルに含められる予定の前記ログの情報には、指定された前記センサによって検出された前記ログの情報が含められる、構成であってもよい。

本発明の一態様に係る端末装置において、前記ファイルの分析のサービスに関する契約の内容と、前記サービスの利用状況とに基づいて、前記ファイルの分析の要求が可能であるか否かを判定する分析要求可否判定部を備える、構成であってもよい。

[0009] 本発明の一態様に係るファイル分析装置は、ログを常時監視し常時監視された前記ログを出力するセキュリティセンサから出力された複数の前記ログのうちの一部の前記ログを含むファイルであって端末装置から送信された1回の分析対象となる1個または複数個の前記ファイルを受信する受信部と、前記受信部によって受信された前記ファイルについて、前記1回の分析対象となる1個または複数個の前記ファイルに含まれる前記ログの情報が許容されるデータ量の上限値以下であるという検査条件が満たされるか否かを判定するファイル検査部と、前記ファイル検査部によって前記検査条件が満たされると判定された前記1回の分析対象となる1個または複数個の前記ファイルに含まれる前記ログの情報について分析を行うファイル分析部と、前記フ

ファイル分析部によって行われた前記ファイルの分析の結果の通知を前記端末装置に送る通知部と、を備える。

本発明の一態様に係るファイル分析装置において、前記ファイル分析部によって行われる前記分析に関する課金情報を管理する管理部を備え、前記課金情報は、前記分析の回数に応じた金額の情報を含み、前記分析の回数に応じた金額の情報は、前記分析の回数に応じた有料の金額の情報、または、前記分析の回数が所定の回数以下では無料であることを示す情報である、構成であってもよい。

[0010] 本発明の一態様に係るファイル分析システムは、端末装置と、ファイル分析装置と、を備えたファイル分析システムであって、前記端末装置は、ログを常時監視し常時監視された前記ログを出力するセキュリティセンサから出力された複数の前記ログのうちの一部の前記ログを取得し、取得された前記ログを含むファイルを生成するファイル生成部と、前記ファイル生成部によって生成された前記ファイルを前記ファイル分析装置に送信するファイル送信部と、前記ファイル分析装置から送られる前記ファイルの分析結果の通知を受ける通知制御部と、1回の分析対象となる1個または複数個の前記ファイルに含められる予定の前記ログの情報が許容されるデータ量の上限值以下であるという条件が満たされるか否かを判定するファイル条件判定部と、前記ファイル条件判定部によって前記条件が満たされないと判定された場合、前記ファイルに含められる前記ログのデータ量を削減するログ削減部と、を備え、前記ファイル条件判定部によって前記条件が満たされないと判定された場合、前記ログ削減部によって前記ファイルに含められる前記ログのデータ量を削減して、前記条件が満たされるようにされた前記ログの情報をを用いて、前記ファイル生成部が前記ファイルを生成し、前記ファイル送信部が前記ファイルを前記ファイル分析装置に送信し、前記ファイル分析装置は、前記端末装置から送信された前記ファイルを受信する受信部と、前記受信部によって受信された前記ファイルについて所定の検査条件が満たされるか否かを判定するファイル検査部と、前記ファイル検査部によって前記検査条件が

満たされると判定された前記ファイルについて分析を行うファイル分析部と、前記ファイル分析部によって行われた前記ファイルの分析の結果の通知を前記端末装置に送る通知部と、を備える。

[0011] 本発明の一態様に係るファイル分析方法は、端末装置が、ログを常時監視し常時監視された前記ログを出力するセキュリティセンサから出力された複数の前記ログのうちの一部の前記ログを取得し、1回の分析対象となる1個または複数個のファイルに含められる予定の前記ログの情報が許容されるデータ量の上限值以下であるという条件が満たされるか否かを判定し、前記条件が満たされないと判定された場合、前記ファイルに含められる前記ログのデータ量を削減して、前記条件が満たされるようにされた前記ログの情報をを用いて、前記ファイルを生成し、前記ファイルをファイル分析装置に送信し、前記ファイル分析装置が、前記端末装置から送信された前記ファイルを受信し、受信された前記ファイルについて所定の検査条件が満たされるか否かを判定し、前記検査条件が満たされると判定された前記ファイルについて分析を行い、前記ファイルの分析の結果の通知を前記端末装置に送り、前記端末装置が、前記ファイル分析装置から送られる前記ファイルの分析結果の通知を受ける。

[0012] 本発明の一態様に係るプログラムは、ログを常時監視し常時監視された前記ログを出力するセキュリティセンサから出力された複数の前記ログのうちの一部の前記ログを取得する機能と、1回の分析対象となる1個または複数個のファイルに含められる予定の前記ログの情報が許容されるデータ量の上限值以下であるという条件が満たされるか否かを判定する機能と、前記条件が満たされないと判定された場合、前記ファイルに含められる前記ログのデータ量を削減して、前記条件が満たされるようにされた前記ログの情報をを用いて、前記ファイルを生成する機能と、生成された前記ファイルを、前記1回の分析対象となる1個または複数個の前記ファイルに含まれる前記ログの情報が許容されるデータ量の前記上限値以下であるという前記条件が満たされる場合にファイル分析を行うファイル分析装置に送信する機能と、前記フ

ファイル分析装置から送られる前記ファイルの分析結果の通知を受ける機能と、をコンピュータに実現させるためのプログラムである。

発明の効果

[0013] 上記したファイル分析システム、ファイル分析装置、端末装置、ファイル分析方法およびプログラムによれば、簡易にログの分析を行うことができる。

図面の簡単な説明

[0014] [図1]本発明の一実施形態に係るファイル分析システムの概略的な構成例を示す図である。

[図2]本発明の一実施形態に係る端末装置の概略的な構成例を示す図である。

[図3]本発明の一実施形態に係るファイルの概略的な構成例を示す図である。

[図4]本発明の一実施形態に係るファイル分析結果を表す情報の一例を示す図である。

[図5]本発明の一実施形態に係るファイル分析結果を表す情報の他の一例を示す図である。

[図6]本発明の一実施形態に係るファイル分析が可能なログの範囲を表す情報の一例を示す図である。

[図7]本発明の一実施形態に係る契約情報の一例を示す図である。

[図8]本発明の一実施形態に係る端末装置において行われる処理の手順の一例を示す図である。

[図9]本発明の一実施形態に係る端末装置において行われる処理の手順の一例を示す図である。

[図10]本発明の一実施形態に係る端末装置において行われる処理の手順の一例を示す図である。

[図11]本発明の一実施形態に係る端末装置において行われる処理の手順の一例を示す図である。

[図12]本発明の一実施形態に係るファイル分析装置において行われる処理の手順の一例を示す図である。

[図13]本発明の一実施形態に係るファイル分析装置において行われる処理の手順の一例を示す図である。

[図14]本発明の一実施形態に係るファイル分析装置において行われる処理の手順の一例を示す図である。

[図15]本発明の一実施形態に係る情報処理装置のハードウェア構成の一例を示す図である。

発明を実施するための形態

[0015] 本発明の実施形態について図面を参照して詳細に説明する。

[0016] [ファイル分析システム]

図1は、本発明の一実施形態に係るファイル分析システム1の概略的な構成例を示す図である。なお、図1に示される機能ブロックの構成は、一例であり、他の構成が用いられてもよい。

ファイル分析システム1は、分析部11と、複数の端末部21～23と、ネットワーク31を備える。

それぞれの端末部21～23と分析部11とは、ネットワーク31を介して通信可能に接続される。

[0017] ここで、それぞれの端末部21～23は、それぞれ異なる管理主体により管理されている。当該管理主体は、例えば、会社または学校などの組織であってもよく、あるいは、個人であってもよい。当該管理主体が組織である場合には、当該組織に属する者が端末部21～23を管理する。また、当該管理主体が個人である場合には、当該個人に相当する者が端末部21～23を管理する。本実施形態では、それぞれの端末部21～23を管理する者をユーザと呼ぶ場合もある。

なお、複数の端末部21～23のうちの2個以上の端末部が、同じ管理主体によって管理されてもよい。当該2個以上の端末部は、複数の端末部21～23のうちの一部であってもよく、あるいは、全部であってもよい。

[0018] 端末部21～23の数は、1以上の任意の数であってもよい。

本実施形態では、説明の便宜上、複数の端末部21～23の構成および動

作は、それぞれの端末部 2 1 ～ 2 3 の管理主体が異なり得る点を除いて、同様である。このため、本実施形態では、1 個の端末部 2 1 を代表させて説明する。

なお、それぞれの端末部 2 1 ～ 2 3 の構成あるいは動作が異なる態様が用いられてもよい。

[0019] 本実施形態では、分析部 1 1 は、複数の端末部 2 1 ～ 2 3 のそれぞれに対して、それぞれの端末部 2 1 ～ 2 3 の管理主体が異なり得る点を除いて、同様な動作を行う。

なお、分析部 1 1 は、複数の端末部 2 1 ～ 2 3 のそれぞれに対して、異なる動作を行う構成が用いられてもよい。

[0020] 本実施形態では、分析部 1 1 は、複数の端末部 2 1 ～ 2 3 に対して共通になっている。なお、ファイル分析システム 1 は、複数の分析部 1 1 を備えてもよい。この場合、複数の分析部 1 1 が、複数の端末部 2 1 ～ 2 3 を分担して、動作を行う。

ここで、分析部 1 1 は、例えば、装置あるいはシステムであると捉えられてもよい。また、端末部 2 1 は、例えば、装置あるいはシステムであると捉えられてもよい。

[0021] ネットワーク 3 1 は、任意のネットワークであってもよい。ネットワーク 3 1 は、例えば、インターネットであってもよく、あるいは、専用のネットワークであってもよい。

なお、それぞれの端末部 2 1 ～ 2 3 と分析部 1 1 との通信は、例えば、有線の通信であってもよく、無線の通信であってもよく、あるいは、有線の通信と無線の通信との両方を組み合わせて含んでもよい。

[0022] [端末部の概要]

端末部 2 1 を代表させて説明する。

端末部 2 1 は、ログ検出装置 5 1 と、ログ管理装置 5 2 と、端末装置 5 3 を備える。ログ管理装置 5 2 は、記憶部 1 5 1 を備える。

図 1 の例では、ログ検出装置 5 1 とログ管理装置 5 2 と端末装置 5 3 のそ

れぞれがネットワーク 31 と接続される構成を示すが、これに限られない。

[0023] ログ検出装置 51 は、所定のログを検出する。本実施形態では、ログ検出装置 51 は、常時、所定の対象を監視して、当該対象のログを検出する。本実施形態では、当該ログは、セキュリティに関するログ（セキュリティログ）であり、例えば、ネットワーク 31 を介する通信を対象としたログである。

ログ検出装置 51 は、例えば、所定のログを検出するセンサを用いて構成されてもよい。本実施形態では、ログ検出装置 51 は、端末装置 53 によって行われる通信に関するログを検出する。ログ検出装置 51 は、検出されたログを出力する。本実施形態では、ログ検出装置 51 は、検出されたログをログ管理装置 52 に送信する。

なお、本実施形態では、ログ検出装置 51 は、検出されたログを記憶しない。他の例として、ログ検出装置 51 は、検出されたログを記憶する記憶部を備えてもよい。

[0024] ログ管理装置 52 は、ログ検出装置 51 により検出されたログを記憶部 151 に記憶して管理する。

ここで、ログ管理装置 52 は、ログ検出装置 51 により検出されたログを、所定のまとまりごとに、記憶部 151 に記憶してもよい。当該所定のまとまりは、例えば、ログの検出時刻が所定の期間に含まれる当該ログのまとまりであってもよい。当該所定のまとまりは、例えば、ファイルとして生成されてもよい。当該所定の期間は、例えば、1 日単位の期間であってもよい。

ログ管理装置 52 は、例えば、ログを記憶して管理するログ管理サーバ装置を用いて構成されてもよい。

ログ検出装置 51 あるいはログ管理装置 52 は、例えば、コンピュータシステムのログを記録するための通信プロトコルであるシスログ（syslog）を使用してもよい。

[0025] 端末装置 53 は、例えば、ユーザによって操作される情報処理装置を用いて構成される。当該情報処理装置は、例えば、コンピュータである。当該コ

ンピュータは、例えば、デスクトップ型のコンピュータ、ノート型のコンピュータ、携帯電話のコンピュータ、あるいは、スマートフォンのコンピュータなどであってもよい。

端末装置 5 3 は、ログ管理装置 5 2 の記憶部 1 5 1 に記憶されたログに基づいて、ログ管理装置 5 2 の記憶部 1 5 1 に記憶されたログの少なくとも一部を含む所定のファイルを生成する。端末装置 5 3 は、生成されたファイルをネットワーク 3 1 を介して分析部 1 1 に送信する。

また、端末装置 5 3 は、分析部 1 1 から送信された電子メールをネットワーク 3 1 を介して受信する。

また、端末装置 5 3 は、分析部 1 1 により提供される Web ページの情報を取得する。

[0026] [ファイル分析部の概要]

分析部 1 1 は、ファイル分析装置 4 1 と、Web サーバ装置 4 2 と、メールサーバ装置 4 3 を備える。

図 1 の例では、ファイル分析装置 4 1 と、Web サーバ装置 4 2 と、メールサーバ装置 4 3 のそれぞれがネットワーク 3 1 と接続される構成を示すが、これに限られない。

[0027] ファイル分析装置 4 1 は、記憶部 1 1 1 と、通信部 1 1 2 と、ファイル検査部 1 1 3 と、ファイル分析部 1 1 4 と、通知部 1 1 5 と、管理部 1 1 6 を備える。

通信部 1 1 2 は、受信部 1 2 1 を備える。

ファイル検査部 1 1 3 は、復号部 1 3 1 と、解凍部 1 3 2 を備える。

なお、本実施形態では、「圧縮」と「解凍」という語を使用して説明するが、例えば、「解凍」の代わりに「伸張」などの語が使用されてもよい。

[0028] ファイル分析装置 4 1 において行われる動作の概要を示す。

記憶部 1 1 1 は、各種の情報を記憶する。

通信部 1 1 2 は、情報の通信を行う。本実施形態では、通信部 1 1 2 は、ネットワーク 3 1 を介した通信を行う。

受信部 1 2 1 は、端末装置 5 3 からネットワーク 3 1 を介して分析部 1 1 に送信されたファイルを受信する。受信部 1 2 1 は、受信されたファイルをファイル検査部 1 1 3 に出力する。本実施形態では、端末装置 5 3 は、当該ファイルをファイル分析装置 4 1 に宛てて送信する。

- [0029] ファイル検査部 1 1 3 は、受信部 1 2 1 から出力されたファイルを入力する。ファイル検査部 1 1 3 は、入力されたファイルについて、所定の条件（説明の便宜上、「検査条件」ともいう。）が満たされるか否かを判定する検査を行う。ファイル検査部 1 1 3 は、入力されたファイルについて、検査条件が満たされると判定した場合には、当該ファイルをファイル分析部 1 1 4 に出力する。一方、ファイル検査部 1 1 3 は、入力されたファイルについて、検査条件が満たされないと判定した場合には、所定の情報（説明の便宜上、「検査エラー情報」ともいう。）を通知部 1 1 5 に出力する。

本実施形態では、記憶部 1 1 1 は、検査条件を特定する情報を記憶する。ファイル検査部 1 1 3 は、当該情報に基づいて、検査条件を取得する。

- [0030] ここで、本実施形態では、端末装置 5 3 からファイル分析装置 4 1 に送信されるファイルは、当該ファイルの情報が圧縮された後に、圧縮後のファイルが暗号化された状態である。

ファイル検査部 1 1 3 では、入力されたファイルは暗号化された状態であり、復号部 1 3 1 が当該ファイルを復号する。また、ファイル検査部 1 1 3 では、復号されたファイルの情報は圧縮されており、解凍部 1 3 2 が、当該情報を解凍する。これにより、圧縮および暗号化されたファイルが、圧縮および暗号化される前のファイル（説明の便宜上、「元のファイル」ともいう。）に変換される。ファイル検査部 1 1 3 は、これにより得られた元のファイルについて、所定の検査を行う。ファイル検査部 1 1 3 は、検査条件が満たされると判定した場合には、このような元のファイルをファイル分析部 1 1 4 に出力する。

- [0031] 検査条件としては、任意の条件が用いられてもよい。

検査条件としては、例えば、1 回の分析対象のファイルに含まれるログの

データ量が所定の上限値以下であるという条件、または、1回の分析対象のファイルのサイズが所定の上限値以下であるという条件、あるいは、これら両方の条件を含んでもよい。

検査条件としては、例えば、分析対象のファイルがコンピュータウィルスに侵されていないという条件を含んでもよい。なお、分析対象のファイルがコンピュータウィルスに侵されているか否かは、例えば、アンチウィルスソフトウェアを用いて判定されてもよい。検査条件としては、例えば、分析対象のファイルが所定のフォーマットのファイルであるという条件を含んでもよい。

検査条件としては、例えば、分析対象のファイルが所定の情報を含むという条件を含んでもよい。当該所定の情報は、例えば、正当な端末装置53から送信されたファイルであることを示す情報であってもよい。

[0032] ファイル分析部114は、ファイル検査部113から出力されたファイルを入力する。ファイル分析部114は、入力されたファイルについて、所定の条件（説明の便宜上、「分析条件」ともいう。）に基づいて、分析を行う。ファイル分析部114は、入力されたファイルについて、分析を行った結果に関する所定の情報（説明の便宜上、「分析結果情報」ともいう。）を通知部115に出力する。

本実施形態では、記憶部111は、分析条件を特定する情報を記憶する。ファイル分析部114は、当該情報に基づいて、分析条件を取得する。

[0033] 分析条件としては、任意の条件が用いられてもよい。

分析条件としては、例えば、分析対象のファイルに含まれるログについて、問題があるか否かを判定するための条件が用いられてもよい。当該問題は、例えば、コンピュータウィルスであってもよく、あるいは、他の事象であってもよい。

分析条件としては、例えば、「ログに含まれる送信元を識別する情報、ログに含まれる送信先を識別する情報、あるいは、ログに含まれる他の情報が、所定の情報に一致する場合には、問題があると判定する条件」が用いられ

てもよい。分析条件としては、例えば、問題があると判定すべきログの条件がリスト化されたブラックリストに記述された当該条件が用いられてもよい。また、問題があると判定すべき条件は、例えば、「ルール」と呼ばれてもよい。

なお、分析対象のファイルに複数の種類のログが含まれ得る場合には、例えば、ファイル分析部 114 は、それぞれのログの種類を判定する。この場合、それぞれのログの情報は、当該ログの種類を特定する情報を含む。他の例として、このようなログの種類は、ファイル分析部 114 の代わりに、ファイル検査部 113 によって判定されてもよい。

[0034] 通知部 115 は、ファイル検査部 113 から検査エラー情報が入力された場合、当該検査エラー情報に基づく所定の情報を端末装置 53 に通知する。当該所定の情報としては、端末装置 53 に検査のエラーに関する情報を通知するための情報が用いられ、任意の情報が用いられてもよい。

また、通知部 115 は、ファイル分析部 114 から分析結果情報が入力された場合、当該分析結果情報に基づく所定の情報を端末装置 53 に通知する。当該所定の情報としては、端末装置 53 に分析結果に関する情報を通知するための情報が用いられ、任意の情報が用いられてもよい。

[0035] ここで、通知部 115 から端末装置 53 に情報を通知する手法としては、任意の手法が用いられてもよい。

本実施形態では、端末装置 53 に通知すべき情報が発生した場合、通知部 115 は、端末装置 53 に宛てた電子メールを作成し、作成された電子メールをメールサーバ装置 43 に送信する。この場合、通知部 115 は、端末装置 53 からアクセスすることが可能なアクセス先の情報を当該電子メールに含める。当該情報は、例えば、URL (Uniform Resource Locator) であってもよい。

通知部 115 は、電子メールに含めたアクセス先の情報に該当する Web ページを生成し、生成された Web ページの情報を Web サーバ装置 42 に送信する。通知部 115 は、当該 Web ページに、端末装置 53 に通知する

情報を含める。

- [0036] メールサーバ装置 4 3 は、通知部 1 1 5 から送信された電子メールを受信する。メールサーバ装置 4 3 は、受信された電子メールを、当該電子メールの宛先に送信する。本実施形態では、端末装置 5 3 が宛先となっている電子メールが、メールサーバ装置 4 3 からネットワーク 3 1 を介して端末装置 5 3 に送信される。

Webサーバ装置 4 2 は、通知部 1 1 5 から送信されたWebページの情報を受信する。Webサーバ装置 4 2 は、受信された情報に基づいて、当該Webページを閲覧可能に提供する。本実施形態では、Webサーバ装置 4 2 は、端末装置 5 3 からのアクセスに応じて、当該Webページを端末装置 5 3 に閲覧可能に提供する。

- [0037] 管理部 1 1 6 は、端末装置 5 3 について、各種の管理を行う。

本実施形態では、分析部 1 1 において、端末装置 5 3 の情報が未知である場合と、端末装置 5 3 の情報が既知である場合があり得る。

本実施形態では、端末装置 5 3 の管理主体と、分析部 1 1 によってファイル分析のサービスを提供する管理主体との間で、当該サービスに関する契約が締結されている場合に、当該契約に関して端末装置 5 3 の情報が分析部 1 1 に設定される。当該情報は、例えば、記憶部 1 1 1 に記憶されてもよい。当該情報は、例えば、端末装置 5 3 を特定する情報を含んでもよい。当該情報は、端末装置 5 3 の電子メールのアドレスを含んでもよい。

一方、本実施形態では、このような契約が締結されていない場合に、分析部 1 1 において、端末装置 5 3 の情報が未知である。

- [0038] ここで、契約に関して設定される端末装置 5 3 の情報としては、例えば、サービスを受けることが可能なファイル分析の範囲を特定する情報、あるいは、サービスを受けるために必要な料金に関する情報（説明の便宜上、「課金情報」ともいう。）などであってもよい。

サービスを受けることが可能なファイル分析の範囲は、例えば、データ量、回数、期間などのうちの 1 以上を用いて設定されてもよい。サービスを受

けることが可能なファイル分析の範囲は、例えば、所定の期間において分析対象とするすべてのログのデータ量の総和に対する上限値、１回の分析対象とするログのデータ量に対する上限値、所定の期間においてファイル分析のサービスを受けることが可能な回数の上限值などのうちの１以上を用いて特定されてもよい。

[0039] 一例として、サービスは、固定額で課金されてもよい。

他の例として、サービスは、従量的に課金されてもよい。この場合、管理部１１６は、端末装置５３に対して提供したサービスについて、課金する料金を決定するための情報を記憶部１１１に記憶して管理する。当該情報は、例えば、所定の期間においてファイル分析のサービスを受けたログのデータ量の総和、所定の期間においてファイル分析のサービスを受けた回数などのうちの１以上の情報であってもよい。例えば、ファイル分析を利用したデータ量または回数に応じた金額の課金が行われてもよい。また、例えば、ファイル分析を利用した所定のデータ量までは無料とするサービス、または、ファイル分析を利用した所定の回数までは無料とするサービスが行われてもよい。

また、管理部１１６は、端末装置５３について現時点で課金されている料金を特定する情報を記憶部１１１に記憶して管理してもよい。

[0040] 具体例として、管理部１１６は、ファイル分析部１１４によって行われるファイル分析に関する課金情報を管理する。当該課金情報は、ファイル分析の回数に応じた金額の情報を含む。ファイル分析の回数に応じた金額の情報は、例えば、ファイル分析の回数に応じた有料の金額の情報、または、ファイル分析の回数が所定の回数以下では無料であることを示す情報である。

なお、ここでは、ファイル分析の回数に応じた課金について具体例を示したが、ファイル分析のデータ量に応じた課金などについても同様である。

[0041] [端末装置の詳細]

図２は、本発明の一実施形態に係る端末装置５３の概略的な構成例を示す図である。なお、図２に示される機能ブロックの構成は、一例であり、他の

構成が用いられてもよい。 端末装置 5 3 は、入力部 2 1 1 と、出力部 2 1 2 と、操作部 2 1 3 と、表示部 2 1 4 と、通信部 2 1 5 と、記憶部 2 1 6 と、制御部 2 1 7 を備える。

制御部 2 1 7 は、ログ取得部 2 3 1 と、ファイル条件取得部 2 3 2 と、ファイル条件判定部 2 3 3 と、ログ削減部 2 3 4 と、ファイル生成部 2 3 5 と、圧縮部 2 3 6 と、暗号化部 2 3 7 と、通知制御部 2 3 8 と、分析要求可否判定部 2 3 9 を備える。

[0042] 入力部 2 1 1 は、外部の装置から出力される情報を入力する。

出力部 2 1 2 は、外部の装置に情報を出力する。

ここで、外部の装置は、任意の装置であってもよい。当該外部の装置は、例えば、持ち運びが可能な記録媒体であってもよい。当該外部の装置は、例えば、印刷装置であってもよい。

操作部 2 1 3 は、ユーザにより行われる操作に対応する情報を入力する。操作部 2 1 3 は、例えば、キーボード、あるいは、マウスなどを含んでもよい。

表示部 2 1 4 は、画面を有し、情報を当該画面に出力する。これにより、当該情報が当該画面に表示される。

[0043] 通信部 2 1 5 は、ネットワーク 3 1 を介した通信を行う。本実施形態では、端末装置 5 3 は、通信部 2 1 5 によって、ネットワーク 3 1 と通信可能に接続される。

なお、端末装置 5 3 は、ログ検出装置 5 1 を経由して、ネットワーク 3 1 と接続されてもよい。この場合、通信部 2 1 5 は、送信対象の信号を、ログ検出装置 5 1 を経由して、ネットワーク 3 1 に出力する。この場合、ログ検出装置 5 1 は、通信部 2 1 5 から出力された信号を入力し、入力された信号をネットワーク 3 1 に出力する。また、この場合、通信部 2 1 5 は、ネットワーク 3 1 から、ログ検出装置 5 1 を経由して、信号を入力する。この場合、ログ検出装置 5 1 は、ネットワーク 3 1 から信号を入力し、入力された信号を通信部 2 1 5 に出力する。

[0044] 記憶部 2 1 6 は、各種の情報を記憶する。

制御部 2 1 7 は、端末装置 5 3 における各種の制御を行う。

[0045] ログ取得部 2 3 1 は、ログを取得する。本実施形態では、ログ取得部 2 3 1 は、ログ管理装置 5 2 に記憶されたログのなかから、所定のログを取得する。

ファイル条件取得部 2 3 2 は、ファイルの条件（説明の便宜上、「ファイル条件」ともいう。）を取得する。

本実施形態では、記憶部 2 1 6 は、ファイル条件を特定する情報を記憶する。ファイル条件取得部 2 3 2 は、当該情報に基づいて、ファイル条件を取得する。

ファイル条件判定部 2 3 3 は、ファイル条件取得部 2 3 2 により取得されたファイル条件に基づいて、判定の対象となるファイルについて、当該ファイル条件が満たされるか否かを判定する。

[0046] ここで、本実施形態では、ファイル条件は、少なくとも、1 回の分析対象となるファイルに含まれるログの情報について、許容されるデータ量の上限値の条件を含む。

なお、1 回の分析対象となるファイルが 1 個である場合には、許容されるデータ量の上限値は、1 個のファイルに含まれるログの情報について許容されるデータ量の上限値となる。

また、1 回の分析対象となるファイルが複数である所定個数である場合には、許容されるデータ量の上限値は、当該所定個数のファイルに含まれるログの情報の総和について許容されるデータ量の上限値となる。

[0047] ログ削減部 2 3 4 は、分析対象として不要なログ（説明の便宜上、「不要ログ」ともいう。）を削減する処理（説明の便宜上、「不要ログ削減処理」ともいう。）を行う機能と、分析対象とするログの範囲（説明の便宜上、「ログ範囲」ともいう。）を制限することで分析対象とするログを削減する処理（説明の便宜上、「ログ範囲削減処理」ともいう。）を行う機能を有する。これにより、ログ削減部 2 3 4 は、分析対象とするログのデータ量を削減

する。なお、本実施形態では、ファイルに含められるログのデータ量が大きくなると、当該ファイルのサイズが大きくなる、または、当該ファイルの数が多くなる。

本実施形態では、ログ削減部 234 は、分析対象とするファイルが生成されるときには、常時、不要ログ削減処理を行う。

また、本実施形態では、ログ削減部 234 は、1 回の分析対象となるファイルに含められる予定のログの情報について、そのデータ量が許容されるデータ量の上限値を超えた場合に、ログ範囲削減処理を行う。

[0048] なお、他の構成例として、ログ削減部 234 は、1 回の分析対象となるファイルに含められる予定のログの情報について、そのデータ量が許容されるデータ量の上限値以下である場合には、不要ログ削減処理を行わなくてもよい。そして、ログ削減部 234 は、1 回の分析対象となるファイルに含められる予定のログの情報について、そのデータ量が許容されるデータ量の上限値を超えた場合に、不要ログ削減処理を行ってもよい。この場合、ログ削減部 234 は、不要ログ削減処理の後においても、1 回の分析対象となるファイルに含められる予定のログの情報について、そのデータ量が許容されるデータ量の上限値を超えた場合に、ログ範囲削減処理を行う。

[0049] ファイル生成部 235 は、1 回の分析対象となるファイルに含められる予定のログの情報をを用いて、当該情報が含められたファイルを生成する。当該情報は、例えば、ログ削減部 234 によって削減されていない場合と、ログ削減部 234 によって削減された場合がある。

なお、一例として、ファイル生成部 235 は、ログ管理装置 52 の記憶部 151 に記憶された所定期間ごとのログのまとまり（例えば、ファイルにされたまとまり）を、ファイル生成部 235 によって生成されたファイルとして、利用してもよい。この際、ファイル生成部 235 は、ログ管理装置 52 の記憶部 151 に記憶された所定期間ごとのログのまとまり（例えば、ファイルにされたまとまり）について、フォーマット等を変更してもよい。

他の例として、ファイル生成部 235 は、ログ管理装置 52 の記憶部 15

1に記憶された所定期間ごとのログのまとまり（例えば、ファイルにされたまとまり）から一部のログが削減されたログのまとまりを用いてファイルを生成してもよい。

[0050] 圧縮部236は、ファイル生成部235によって生成されたファイルを圧縮する。

暗号化部237は、圧縮部236によって圧縮されたファイルを暗号化する。

制御部217では、暗号化部237によって暗号化されたファイルを、通信部215によって、ネットワーク31を介して、ファイル分析装置41に送信する。

[0051] ここで、端末装置53における暗号化部237によって暗号化された情報は、ファイル分析装置41における復号部131によって行われる復号によって、元の情報に戻される。

また、端末装置53における圧縮部236によって圧縮された情報は、ファイル分析装置41における解凍部132によって行われる解凍によって、元の情報に戻される。

[0052] 通知制御部238は、ファイル分析装置41の通知部115によって行われる通知の内容を受信するための処理を行う。

本実施形態では、通知制御部238は、メールサーバ装置43からネットワーク31を介して端末装置53に宛てて送信される電子メールを、通信部215によって、受信する。また、通知制御部238は、受信された電子メールに記述されているアクセス先のWebページにアクセスし、Webサーバ装置42によって提供される当該Webページの情報を取得する。このアクセスは、例えば、ユーザによって行われる操作部213の操作に応じて行われてもよい。

[0053] 分析要求可否判定部239は、所定の条件（説明の便宜上、「分析要求条件」という。）に基づいて、端末装置53からファイル分析装置41に対してファイル分析の要求を行うことが可能か否かを判定する。当該分析要求条

件としては、任意の条件が用いられてもよく、例えば、データ量、回数、期間などのうちの１以上に関する条件が用いられてもよい。

[0054] ここで、本実施形態では、分析要求可否判定部２３９は、端末装置５３の管理主体と、分析部１１によってファイル分析のサービスを提供する管理主体との間で、当該サービスに関する契約が締結されている場合に、このような判定を行う。分析要求可否判定部２３９は、当該契約の内容と、端末装置５３における当該サービスの利用状況に基づいて、端末装置５３からファイル分析装置４１に対してファイル分析の要求を行うことが可能か否かを判定する。

例えば、記憶部２１６は、契約が締結された端末装置５３を特定する情報、当該契約の内容を特定する情報、および端末装置５３におけるサービスの利用状況を特定する情報を記憶する。端末装置５３を特定する情報は、例えば、端末装置５３の電子メールのアドレスを含んでもよい。

分析部１１によってファイル分析のサービスを提供する管理主体から見ると、当該サービスに関する契約が締結された端末装置５３の管理主体は、顧客となる。複数の端末部２１～２３の管理主体は、それぞれ、異なる顧客となり得る。

[0055] [ファイル]

図３は、本発明の一実施形態に係るファイル１０１１の概略的な構成例を示す図である。

ファイル１０１１は、ヘッダと、複数のログ情報を含む。

ログ情報は、例えば、発生等の日時、シグネチャ、送信元を識別する情報、送信先を識別する情報、エラーコードなどのうちの１以上の情報を含んでもよい。送信元を識別する情報および送信先を識別する情報としては、例えば、ＩＰ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）アドレスが用いられてもよい。これらの情報は、例えば、ヘッダに含まれてもよい。

また、ヘッダは、例えば、端末装置５３の電子メールのアドレスを含んでもよい。

[0056] なお、図3の例では、ファイル1011に複数のログ情報が区分されて含まれる構成例を示したが、他の例として、ファイル1011に1個のまとまりのログ情報が含まれると捉えられてもよい。

また、複数のファイル1011が1回の分析対象のまとまりとなる場合には、例えば、それぞれのファイル1011のヘッダに、このようなまとまりであることを特定する情報が含まれてもよい。

[0057] 図4は、本発明の一実施形態に係るファイル分析結果を表す情報の一例を示す図である。

図4には、Webサーバ装置42により提供されるWebページに基づいて、端末装置53の表示部214によって画面に表示される表示内容2011の一例を示してある。

図4の例では、表示内容2011において、「ファイル分析の結果」として、「問題は検出されませんでした。」という文字情報が表示されている。つまり、ファイル分析の結果として、問題が検出されなかった場合を示してある。なお、このような場合の表示内容2011は、他の内容であってもよい。

[0058] 図5は、本発明の一実施形態に係るファイル分析結果を表す情報の他の一例を示す図である。

図5には、Webサーバ装置42により提供されるWebページに基づいて、端末装置53の表示部214によって画面に表示される表示内容2111の一例を示してある。図5の例では、表示内容2111において、「ファイル分析の結果」として、「以下の問題が検出されました。・・・」という文字情報が表示されている。つまり、ファイル分析の結果として、問題が検出された場合を示してある。この場合、このような表示の内容は、警告（アラート）と捉えられてもよい。なお、このような場合の表示内容2111は、他の内容であってもよい。

なお、ファイル分析の結果における「問題」は、例えば、「インシデント」あるいは「異常」などと呼ばれてもよい。

[0059] [分析対象とするログの削減：不要ログ削減処理]

ログ削減部 234 は、ログ取得部 231 によって取得されたログのうちで、不要なログを削減することで、分析対象とするログを削減する。

本実施形態では、端末装置 53 において、分析対象とされることが不要なログを特定する情報が記憶部 216 に記憶されている。

[0060] ここで、分析対象とされることが不要なログは、任意に定められてもよい。

一例として、分析対象とされることが不要なログは、分析対象とされることが不要な 1 以上のログを特定する情報を含むリストを用いて定められてもよい。当該リストは、ホワイトリストと呼ばれてもよい。ログ削減部 234 は、当該リストの内容に基づいて、ログ取得部 231 によって取得されたログのうちで、分析対象とされることが不要なログを分析対象から削減する。

[0061] [分析対象とするログの削減：ログ範囲削減処理]

本実施形態では、ファイル条件には、少なくとも、1 回の分析の対象とすることができるログのデータ量の上限値が含まれている。

本実施形態では、端末装置 53 において、ファイル条件判定部 233 は、1 回の分析の対象の候補となっているログを判定対象のログとして、当該ログのデータ量の総和が所定の上限値以下であるか否かを判定する。

この結果、当該ログのデータ量の総和が所定の上限値を超える場合には、ログ削減部 234 は、1 回の分析の対象の候補となっているログの一部を当該候補から削除することによって、1 回の分析の対象の候補となっているログを削減する。

[0062] なお、本実施形態では、ログ削減部 234 は、分析の対象の候補となっているログの一部を当該候補から削除するが、当該ログの一部自体はログ管理装置 52 の記憶部 151 に記憶されたままとする。

また、本実施形態では、不要ログ削減処理とログ範囲削減処理との両方が行われる場合を示すが、不要ログ削減処理とログ範囲削減処理とのうちの任意の一方が他方とは独立に行われてもよい。

[0063] 図6は、本発明の一実施形態に係るファイル分析が可能なログの範囲を表す情報の一例を示す図である。

図6には、1回の分析の対象とすることができるログの範囲を提示するために、端末装置53の表示部214によって画面に表示される表示内容2211の一例を示してある。図6の例では、期間が「2018/7/10 13:00~2018/7/12 15:45」であり、センサが「センサA」であれば、ファイル分析が可能であることを示している。

[0064] ここで、期間は、ログが発生した日時が含まれるべき期間を示している。図6に示される「2018/7/10 13:00~2018/7/12 15:45」は、2018年7月10日の13時00分から2018年7月12日の15時45分までの期間を表している。

図6の例では、期間は、ひとまとまりの連続した期間であるが、離散した2以上のまとまりの期間が用いられてもよい。

通常、ある期間の範囲から、期間の範囲が短くされると、ログのデータ量の総和も減少する。

[0065] センサは、ログを検出したセンサを示している。図6に示される「センサA」は、例えば、ログ検出装置51のセンサを示している。

なお、センサとしては、例えば、1個のセンサが指定されてもよく、あるいは、2個以上のセンサが指定されてもよい。通常、ある個数のセンサから、センサの個数が減少させられると、ログのデータ量の総和も減少する。

[0066] 本実施形態では、端末装置53において、ファイル条件取得部232、ファイル条件判定部233およびログ削減部234は、ユーザからの明示の指示が無くても自動的にそれぞれの処理を実行する。これにより、端末装置53では、ファイル分析の対象となるファイルが生成される前に、自動的に、分析の対象とするログの削減が行われる。そして、図6に示される表示内容2211が、ユーザに対して表示される。つまり、データ量の点で分析対象とすることが可能なログの範囲が、推奨されるログの範囲として、ユーザに提示される。

[0067] ここで、端末装置 5 3 では、例えば、初期的に表示するログの範囲の条件が設定されている。当該条件は、任意の条件であってもよい。当該条件を特定する情報が記憶部 2 1 6 に記憶されている。

例えば、当該条件は、開始から終了までの期間に関して、終了時点が定められていてもよい。一例として、当該終了時点は、初期的にログの範囲を表示する処理が行われる時点（つまり、現時点）に設定される規則、あるいは、その時点よりも所定時間だけ前の時点に設定される規則に基づいて設定されてもよい。この場合、ログ削減部 2 3 4 は、設定された終了時点におけるログを最新のログとして、当該ログから古い方（開始時点）へ遡って所定のデータ量のログを分析対象として抽出することが可能である。

また、例えば、当該条件は、センサに関して、1 以上の所定のセンサが定められていてもよい。一例として、当該所定のセンサは、あらかじめ定められた「センサ A」に設定されるという規則に基づいて設定されてもよい。

[0068] また、端末装置 5 3 は、ユーザによって行われる操作部 2 1 3 の操作に応じて、制御部 2 1 7 によって、ログの範囲の一部または全部を変更してもよい。

この場合、制御部 2 1 7 では、ユーザの操作によって変更された後のログの範囲が 1 回の分析の対象とすることができるログの範囲にあるとファイル条件判定部 2 3 3 によって判定された場合には、ユーザによる変更を承認する。

[0069] 一方、制御部 2 1 7 では、ユーザの操作によって変更された後のログの範囲が 1 回の分析の対象とすることができるログの範囲を超えるとファイル条件判定部 2 3 3 によって判定された場合には、ログ削減部 2 3 4 によってログを削減する。この際、ログ削減部 2 3 4 は、例えば、ユーザの操作によって変更された箇所については変更しない。つまり、ユーザによる変更を優先させる。そして、制御部 2 1 7 では、ログの削減が行われた結果として得られたログの範囲を表示部 2 1 4 の画面に表示する。

なお、ユーザの操作によって変更された箇所について変更しないとファイ

ル条件が満たされない場合には、制御部 2 1 7 では、エラーを示す情報を表示部 2 1 4 の画面に表示してもよい。

[0070] このような構成により、例えば、ユーザは、1 回の分析の対象とすることができるログの範囲を把握していなくても、端末装置 5 3 によって適切なログの範囲が提示されて、このようなログの範囲を利用することができる。

また、例えば、ユーザは、当該ユーザの希望に応じて、端末装置 5 3 によって提示されたログの範囲を不可能なログの範囲へ変更した場合においても、端末装置 5 3 によって再びログの範囲が調整されて新たなログの範囲が提示されるため、非常に便利である。

[0071] 図 6 に示される表示内容 2 2 1 1 には、「アップロード」を示す所定のボタン 2 2 2 1 が含まれている。

ユーザは、端末装置 5 3 の操作部 2 1 3 を操作することで、画面において当該ボタン 2 2 2 1 を押下（例えば、マウスでクリックなど）することが可能である。当該ボタン 2 2 2 1 が押下されると、その時点で表示されているログの範囲が採用されて、当該範囲にあるログが含まれるファイルが生成され、生成されたファイルが端末装置 5 3 からネットワーク 3 1 を介してファイル分析装置 4 1 に送信される。

[0072] なお、本実施形態では、ログの範囲を決定するためのパラメータとして、「期間」と「センサ」が用いられるが、他のパラメータが用いられてもよい。

[0073] [契約の内容]

図 7 は、本発明の一実施形態に係る契約情報 3 0 1 1 の一例を示す図である。

図 7 の例では、契約情報 3 0 1 1 は、顧客の識別情報と、契約の内容と、が対応付けられている。契約の内容は、例えば、回数、容量、期間などである。

なお、図 7 の例では、契約情報 3 0 1 1 は、顧客の契約の内容とともに、契約の内容に関して利用の状況も含んでいる。他の例として、顧客の契約の

内容と、契約の内容に関する利用の状況とが、別々に管理されてもよい。

[0074] 顧客の識別情報は、例えば、番号の情報であってもよい。本実施形態では、顧客の識別情報によって、それぞれの顧客の端末装置 53 が識別される。図 7 の例では、識別情報として、「001」、「002」、「003」などの情報が用いられている。

[0075] 回数は、それぞれの顧客の端末装置 53 について、ファイル分析のサービスを受けることが可能な最大の回数を表す。図 7 の例では、回数として、「2/10」などの情報が用いられている。例えば、「2/10」は、最大の回数が 10 であり、そのうち 2 回が既に行われたことを表している。

容量は、それぞれの顧客の端末装置 53 について、ファイル分析のサービスを受けることが可能なデータ量の総容量を表す。図 7 の例では、容量として、「300/1000」などの情報が用いられている。例えば、「300/1000」は、最大の容量が 1000 G バイトであり、そのうち 300 G バイトのサービスが既に行われたことを表している。期間は、それぞれの顧客の端末装置 53 について、ファイル分析のサービスを受けることが可能な期間を表す。図 7 の例では、期間として、「2018/1/1~2018/12/31」などの情報が用いられている。例えば、「2018/1/1~2018/12/31」は、2018 年 1 月 1 日から 2018 年 12 月 31 日までが有効な期間であることを表している。

[0076] 本実施形態では、ファイル分析装置 41 において、管理部 116 は、契約情報 3011 を管理する。例えば、契約情報 3011 は、記憶部 111 に記憶される。

また、本実施形態では、端末装置 53 において、契約情報 3011 のうち当該端末装置 53 の顧客に該当する部分の情報を記憶部 216 に記憶する。つまり、ファイル分析装置 41 では複数の顧客に関する情報を管理するが、それぞれの顧客の端末装置 53 では当該顧客に関する情報を管理する。

[0077] [端末装置からファイル分析装置へのアクセス]

端末装置 53 からファイル分析装置 41 にアクセスする手法としては、特

に限定はない。

一例として、端末装置 5 3 は、分析部 1 1 によってファイル分析のサービスを提供する管理主体によって閲覧可能にされている Web ページにアクセスする。当該 Web ページは、例えば、Web サーバ装置 4 2 によって提供されてもよい。

端末装置 5 3 は、例えば、ユーザによって行われる操作部 2 1 3 の操作に応じて、当該 Web ページにアクセスしてもよい。

また、端末装置 5 3 は、例えば、ファイル分析のサービスを受けるための契約を締結している場合に、ファイル分析装置 4 1 からアクセスされてもよい。この場合、ファイル分析装置 4 1 では、端末装置 5 3 を特定する情報が記憶部 1 1 1 に記憶されており、管理部 1 1 6 が当該情報に基づいて端末装置 5 3 にアクセスする。

[0078] ファイル分析のサービスにおいて、端末装置 5 3 とファイル分析装置 4 1 とは、オンデマンドで処理を実行してもよい。例えば、端末装置 5 3 から発せられる要求に応じて、ファイル分析装置 4 1 によって当該要求を満たすための処理を実行してもよい。

[0079] [ファイル分析のための専用のツール]

端末装置 5 3 において、ファイル分析のサービスを受けるための専用のツール（説明の便宜上、「専用ツール」ともいう。）を備えてもよい。当該専用ツールは、ソフトウェアであってもよい。当該ソフトウェアは、プログラムであってもよい。

端末装置 5 3 において、当該ソフトウェアは、例えば、記憶部 2 1 6 に記憶されている。そして、端末装置 5 3 において、当該ソフトウェアの内容に基づいて処理を行う。

[0080] 専用ツールは、例えば、分析部 1 1 によってファイル分析のサービスを提供する管理主体によって、端末装置 5 3 の管理主体に配布される。当該専用ツールは、例えば、記録媒体に格納されて配布されてもよく、あるいは、ファイル分析装置 4 1 などから端末装置 5 3 に対してネットワーク 3 1 を介し

て送信（ダウンロード）されてもよい。端末装置 5 3 では、例えば、当該専用ツールであるプログラムをインストールして利用可能にする。

専用ツールは、例えば、無料で配布されてもよく、あるいは、有料で配布されてもよい。

また、専用ツールは、例えば、ファイル分析のサービスを受けるための契約をした者に配布されてもよく、あるいは、このような契約をしなくても、任意の者に配布されてもよい。

[0081] 端末装置 5 3 において、専用ツールを備える場合には、当該専用ツールの機能によって、ファイル分析装置 4 1 にアクセスしてもよい。当該アクセスの先は、所定の Web ページであってもよい。

また、端末装置 5 3 において、専用ツールを備える場合には、ファイル分析装置 4 1 から端末装置 5 3 への通信は、電子メールを用いた通信、あるいは、Web プッシュ通知を用いた通信であってもよい。

[0082] 図 2 の例では、端末装置 5 3 におけるファイル条件取得部 2 3 2 の機能とファイル条件判定部 2 3 3 の機能は、例えば、専用ツールによって実現される機能に含まれてもよい。この場合、例えば、専用ツールが端末装置 5 3 に備えられていない状態では、端末装置 5 3 においてファイル条件取得部 2 3 2 の機能とファイル条件判定部 2 3 3 の機能が備えられていなくてもよい。

この場合、端末装置 5 3 では、例えば、これらの機能と同様な処理を行うときには、ユーザによって行われる操作部 2 1 3 の操作に応じて当該処理を行う。つまり、ユーザの手動の操作によって、これらの機能と同様な処理を行う。

[0083] 同様に、図 2 の例では、端末装置 5 3 におけるログ削減部 2 3 4 の機能は、例えば、専用ツールによって実現される機能に含まれてもよい。この場合、例えば、専用ツールが端末装置 5 3 に備えられていない状態では、端末装置 5 3 においてログ削減部 2 3 4 の機能が備えられていなくてもよい。

この場合、端末装置 5 3 では、例えば、当該機能と同様な処理を行うときには、ユーザによって行われる操作部 2 1 3 の操作に応じて当該処理を行う

。つまり、ユーザの手動の操作によって、当該機能と同様な処理を行う。

[0084] また、同様に、図2の例では、端末装置53における圧縮部236の機能、暗号化部237の機能、分析要求可否判定部239、およびファイル生成部235の機能のうちの1以上は、例えば、専用ツールによって実現される機能に含まれてもよい。この場合、例えば、専用ツールが端末装置53に備えられていない状態では、端末装置53において該当する機能が備えられていなくてもよい。

この場合、端末装置53では、例えば、当該機能と同様な処理を行うときには、ユーザによって行われる操作部213の操作に応じて当該処理を行う。つまり、ユーザの手動の操作によって、当該機能と同様な処理を行う。

[0085] また、専用ツールは、他の機能を実現してもよい。

ここで、専用ツールが、所定の機能を実現するために参照する情報を記憶部216などに記憶して管理する場合には、例えば、ファイル分析装置41などからの要求によって当該情報が自動的に更新されてもよい。当該情報は、例えば、ホワイトリストの情報であってもよい。端末装置53における当該情報は、例えば、定期的に、あるいは、当該情報の元となる情報に変化があったときに、自動的に更新されてもよい。これにより、当該情報は、端末装置53とファイル分析装置41との間で共有されて同じ情報に保たれ、最新の情報に維持される。当該情報の更新は、例えば、専用ツールによって行われてもよい。

[0086] 専用ツールは、圧縮部236の機能として、独自のフォーマットで圧縮を行う機能を備えてもよい。この場合、ファイル分析装置41では、解凍部132の機能として、当該フォーマットに適合したフォーマットで解凍を行う機能を備える。ファイル分析システム1では、このような独自のフォーマットが用いられることで、セキュリティリスクを低減することができる。

一例として、専用ツールは、独自のフォーマットでファイルを圧縮するとき、圧縮後のファイルが解凍されなくても読み出すことが可能なヘッダなどに、所定の情報を書き込んでもよい。この場合、ファイル分析装置41で

は、ファイル検査部 1 1 3 によって、圧縮後のファイルに含まれる当該所定の情報があらかじめ定められた情報であると判定された場合には、当該圧縮後のファイルが安全であるとみなす。当該所定の情報は、任意の情報であってもよく、例えば、専用ツールによって圧縮されたことを示す情報である。

[0087] 同様に、専用ツールは、暗号化部 2 3 7 の機能として、独自のフォーマットで暗号化を行う機能を備えてもよい。この場合、ファイル分析装置 4 1 では、復号部 1 3 1 の機能として、当該フォーマットに適合したフォーマットで復号を行う機能を備える。ファイル分析システム 1 では、このような独自のフォーマットが用いられることで、セキュリティリスクを低減することができる。

[0088] 同様に、専用ツールは、ファイル生成部 2 3 5 の機能として、独自のフォーマットでファイルを生成する機能を備えてもよい。この場合、ファイル分析装置 4 1 では、ファイル検査部 1 1 3 は、このような独自のフォーマットが用いられているか否かを検査する。この場合、ファイル分析装置 4 1 では、このような独自のフォーマットが用いられることで、セキュリティリスクを低減することができる。

[0089] 専用ツールとしては、例えば、ファイル条件の判定を行う機能を備えるツール、ログの削減を行う機能を備えるツール、圧縮を行う機能を備えるツール、暗号化を行う機能を備えるツールなどのように、複数の異なる機能のツールが別々に備えられてもよく、あるいは、これらのうちの 2 以上がまとめられたツールが備えられてもよい。

また、専用ツールとしては、圧縮と解凍の両方の機能を有するツールが備えられてもよい。また、専用ツールとしては、暗号化と復号の両方の機能を有するツールが備えられてもよい。

[0090] ファイル分析システム 1 では、端末装置 5 3 において専用ツールによって分析対象のファイルが生成されることで、例えば、端末装置 5 3 からファイル分析装置 4 1 に送信される当該ファイルが所定の検査条件を満たす状態を確保することが容易となる。つまり、ユーザによって行われる任意の操作に

応じてファイルが生成される場合と比べて、専用に設けられた専用ツールによってファイルが生成される場合の方が、所定の検査条件に適合させやすい。つまり、専用ツールによって所定の検査条件が満たされるファイルを生成する構成としておくことで、ファイル分析装置41におけるファイル検査部113によるファイル検査を省略すること、あるいは、当該ファイル検査に要する負担を低減することが可能である。これにより、ファイル分析装置41におけるファイル検査部113によるファイルの検査を簡易化することが可能である。

[0091] ここで、専用ツールによって図6に示される表示内容2211を用いた制御を行う一例を示す。

端末装置53において、表示部214の画面に、専用ツールによる枠が表示されているとする。このとき、ユーザによって行われる操作部213の操作に応じて、分析対象の情報のアイコンが当該枠にドラッグアンドドロップされる。当該アイコンは、例えば、セキュリティセンサのログファイルを表すアイコンであってもよい。

すると、専用ツールは、分析対象のログを読み取り、ホワイトリストに基づいて当該ログから分析に必要な行（不要ログ）を削除する。そして、専用ツールは、必要に応じて、分析対象となるログが所定のサイズに収まってサイズオーバーにならないように、最新の日時のログから過去に遡ってログを切り出す。この際、専用ツールは、ログの日時の範囲を算出して表示部214の画面に表示する。ユーザは、この表示内容（図6の例では、表示内容2211）を確認し、アップロードのボタン2221を押下する操作を行う。これに応じて、専用ツールは、分析対象のログを含むファイルを独自のフォーマットで圧縮してファイル分析装置41に送信する。ファイル分析装置41は、受信されたファイルについて検査、分析を行い、通知を行う。

このようにして、専用ツールを用いて、ユーザによる簡単な操作で、サイズが制限されたファイルをファイル分析装置41に送信することが可能である。

専用ツールは、例えば、ブラウザ上でファイルをアップロードまたは加工して使用する形態でもよい。

[0092] 〔ファイル分析システムにおいて行われる処理〕

図 8 は、本発明の一実施形態に係る端末装置 5 3 において行われる処理の手順の一例を示す図である。

図 8 の例では、端末装置 5 3 は、ユーザによって行われる手動の操作に基づいて、ファイル分析のサービスを利用する場合を示す。

本例では、ファイル条件取得部 2 3 2、ファイル条件判定部 2 3 3 およびログ削減部 2 3 4 の機能がオフ（無効）になっている場合あるいは当該機能が端末装置 5 3 に備えられていない場合を示す。

[0093] （ステップ S 1）

端末装置 5 3 では、操作部 2 1 3 が、ユーザによって行われる操作の内容を受け付けて取得する。そして、ステップ S 2 の処理へ移行する。本例では、当該操作は、ファイル分析のサービスを利用するための操作である。

[0094] （ステップ S 2）

端末装置 5 3 では、ファイル生成部 2 3 5 が、取得された操作の内容に基づいて、ファイル分析の対象とするファイルを生成する。そして、ステップ S 3 の処理へ移行する。

ここで、端末装置 5 3 では、生成されたファイルについて、圧縮部 2 3 6 による圧縮、および暗号化部 2 3 7 による暗号化のうち的一方または両方を行ってもよい。

[0095] （ステップ S 3）

端末装置 5 3 では、制御部 2 1 7 が通信部 2 1 5 によって、生成されたファイルをネットワーク 3 1 を介してファイル分析装置 4 1 に送信する。そして、ステップ S 4 の処理へ移行する。

これにより、ファイル分析装置 4 1 では、端末装置 5 3 から受信されたファイルについて検査、分析の処理を行い、端末装置 5 3 に対して通知を行う。

なお、端末装置５３では、例えば、ユーザによる所定の操作を操作部２１３によって受け付けたことに応じて、ファイルの送信を行ってもよい。

[0096] （ステップＳ４）

端末装置５３では、通知制御部２３８が、ファイル分析装置４１からの通知を受信する。その後、端末装置５３では、通知制御部２３８が、表示部２１４の画面に、受信された通知の内容を表示する。そして、本フローの処理を終了する。これにより、ユーザは、当該通知の内容を把握することができ、つまり、ファイル分析の結果を把握することができる。

[0097] 図９は、本発明の一実施形態に係る端末装置５３において行われる処理の手順の一例を示す図である。

図９の例では、端末装置５３は、所定の規則（説明の便宜上、「ファイル生成規則」ともいう。）に基づいて、ファイル分析のサービスを利用する場合を示す。ファイル生成規則は、例えば、記憶部２１６に記憶されている。ファイル生成規則は、ファイルを生成するための規則であり、例えば、ファイルを生成するタイミング、ファイルに含めるログの範囲などのうちの１以上の規則が含まれてもよい。

本例では、ファイル条件取得部２３２、ファイル条件判定部２３３およびログ削減部２３４の機能がオフ（無効）になっている場合あるいは当該機能が端末装置５３に備えられていない場合を示す。

[0098] （ステップＳ２１）

端末装置５３では、ファイル生成部２３５が、ファイル生成規則を読み出して取得する。そして、ステップＳ２２の処理へ移行する。

[0099] （ステップＳ２２）

端末装置５３では、ファイル生成部２３５が、取得されたファイル生成規則の内容に基づいて、ファイル分析の対象とするファイルを生成する。そして、ステップＳ２３の処理へ移行する。

ここで、端末装置５３では、生成されたファイルについて、圧縮部２３６による圧縮、および暗号化部２３７による暗号化のうち的一方または両方を

行ってもよい。

[0100] (ステップS 2 3)

端末装置 5 3 では、制御部 2 1 7 が通信部 2 1 5 によって、生成されたファイルをネットワーク 3 1 を介してファイル分析装置 4 1 に送信する。そして、ステップ S 2 4 の処理へ移行する。

これにより、ファイル分析装置 4 1 では、端末装置 5 3 から受信されたファイルについて検査、分析の処理を行い、端末装置 5 3 に対して通知を行う。

[0101] (ステップS 2 4)

端末装置 5 3 では、通知制御部 2 3 8 が、ファイル分析装置 4 1 からの通知を受信する。そして、端末装置 5 3 では、通知制御部 2 3 8 が、表示部 2 1 4 の画面に、受信された通知の内容を表示する。そして、本フローの処理を終了する。これにより、ユーザは、当該通知の内容を把握することができ、つまり、ファイル分析の結果を把握することができる。

[0102] 図 1 0 は、本発明の一実施形態に係る端末装置 5 3 において行われる処理の手順の一例を示す図である。

図 1 0 の例では、端末装置 5 3 は、所定のファイル条件に適合するファイルを生成する。なお、ファイル生成の前後の処理としては、任意の処理が用いられてもよい。

本例では、ファイル条件取得部 2 3 2、ファイル条件判定部 2 3 3 およびログ削減部 2 3 4 の機能が端末装置 5 3 に備えられていてオン（有効）になっている場合を示す。

[0103] (ステップS 4 1)

端末装置 5 3 では、ファイル生成部 2 3 5 が、ログ取得部 2 3 1 によって取得されたログに基づいて、ファイルを生成する。そして、ステップ S 4 2 の処理へ移行する。本例では、当該ファイルは、ファイル条件に適合するか否かを判定するために仮に生成されたファイルである。

[0104] (ステップS 4 2)

端末装置 53 では、ファイル条件取得部 232 が、ファイル条件を取得する。そして、ステップ S43 の処理へ移行する。

[0105] (ステップ S43)

端末装置 53 では、ファイル条件判定部 233 が、生成されたファイルがファイル条件を満たすか否かを判定する。

この結果、端末装置 53 では、ファイル条件判定部 233 が、生成されたファイルがファイル条件を満たすと判定した場合には（ステップ S43：YES）、本フローの処理を終了する。この場合、生成されたファイルが分析対象の候補として確定され、それに対応するログの範囲がユーザに提示される（例えば、図 6 の例）。そのログの範囲がユーザによって承認されると、当該ファイルが分析対象として確定される。

一方、端末装置 53 では、ファイル条件判定部 233 が、生成されたファイルがファイル条件を満たさないと判定した場合には（ステップ S43：NO）、ステップ S44 の処理へ移行する。

[0106] (ステップ S44)

端末装置 53 では、ログ削減部 234 が、ファイルに含まれるログを削減する。そして、ステップ S41 の処理に移行する。

なお、本例では、ログの削減の後に、再び、生成されるファイルがファイル条件を満たすか否かを判定する処理を行う場合を示すが、生成されるファイルがファイル条件を満たすようにログの削減が行われる構成ではステップ S44 の処理の後に本フローの処理を終了してもよい。

[0107] 図 11 は、本発明の一実施形態に係る端末装置 53 において行われる処理の手順の一例を示す図である。

図 11 の例では、端末装置 53 は、ファイルの分析要求が可能であるか否かを判定する。なお、本フローの処理は、端末装置 53 においてファイル分析のサービスを受けるための処理が行われるときに、任意のタイミングで行われてもよい。

本例では、分析要求可否判定部 239 が端末装置 53 に備えられていてオ

ン（有効）である場合を示す。なお、分析要求可否判定部２３９がオフ（無効）である場合あるいは端末装置５３に備えられていない場合には、本フローの処理は行われない。

[0108] （ステップＳ６１）

端末装置５３では、分析要求可否判定部２３９が、ファイルの分析要求が可能であるか否かを判定する。この場合、分析要求可否判定部２３９は、例えば、契約情報３０１１と同様な情報に基づいてファイルの分析要求が可能であるか否かを判定してもよい。当該情報は、例えば、記憶部２１６に記憶されて、分析要求可否判定部２３９によって管理されてもよい。

この結果、端末装置５３では、分析要求可否判定部２３９が、ファイルの分析要求が可能であると判定した場合には（ステップＳ６１：ＹＥＳ）、本フローの処理を終了する。一方、端末装置５３では、分析要求可否判定部２３９が、ファイルの分析要求が可能ではないと判定した場合には（ステップＳ６１：ＮＯ）、ステップＳ６２の処理へ移行する。

[0109] （ステップＳ６２）

端末装置５３では、分析要求可否判定部２３９が、ファイル分析のサービスを受けるための処理を中止させる。この場合、分析要求可否判定部２３９は、その旨を表示部２１４の画面に表示させてもよい。そして、本フローの処理を終了する。

なお、端末装置５３では、その後に、再び、ファイル分析のサービスを受けるための処理が行われてもよい。

[0110] 図１２は、本発明の一実施形態に係るファイル分析装置４１において行われる処理の手順の一例を示す図である。

[0111] （ステップＳ１０１）

ファイル分析装置４１では、受信部１２１によって、端末装置５３から送信された分析対象のファイルを受信する。そして、ステップＳ１０２の処理へ移行する。

[0112] （ステップＳ１０２）

ファイル分析装置４１では、ファイル検査部１１３が、受信されたファイルについて、所定の検査条件が満たされるか否かを判定する。

この結果、ファイル分析装置４１では、ファイル検査部１１３が、受信されたファイルについて、所定の検査条件が満たされると判定した場合には（ステップＳ１０２：ＹＥＳ）、ステップＳ１０３の処理へ移行する。

一方、ファイル分析装置４１では、ファイル検査部１１３が、受信されたファイルについて、所定の検査条件が満たされないと判定した場合には（ステップＳ１０２：ＮＯ）、ステップＳ１０４の処理へ移行する。

[0113] （ステップＳ１０３）

ファイル分析装置４１では、ファイル分析部１１４が、検査後のファイルについて、分析条件に基づいて、分析を行う。そして、ステップＳ１０４の処理へ移行する。

[0114] （ステップＳ１０４）

ファイル分析装置４１では、通知部１１５が、端末装置５３に対して通知を行う。

ここで、通知部１１５は、ファイル検査部１１３によってファイルが検査条件を満たさないと判定された場合には、その旨の情報を端末装置５３に対して通知する。

また、通知部１１５は、ファイル分析部１１４によってファイルに問題が無いと判定された場合には、その旨の情報を端末装置５３に対して通知する。

また、通知部１１５は、ファイル分析部１１４によってファイルに問題があると判定された場合には、その旨の情報を端末装置５３に対して通知する。

[0115] ＜変形例＞

図１３を参照して、変形例を説明する。

図１３は、本発明の一実施形態に係るファイル分析装置４１において行われる処理の手順の一例を示す図である。

本例では、ファイル分析装置 4 1 において、ファイル分析部 1 1 4 が、ファイルがファイル条件を満たすか否かを判定する機能と、ファイルに含まれるログを削減する機能を備える場合を示す。

本例では、記憶部 1 1 1 に、ファイル条件を特定する情報が記憶されている。

本例では、端末装置 5 3 において、ファイル条件取得部 2 3 2、ファイル条件判定部 2 3 3 およびログ削減部 2 3 4 の機能がオフ（無効）になっている場合あるいは当該機能が端末装置 5 3 に備えられていない場合に特に有効である。なお、本フローの処理は、端末装置 5 3 において、ファイル条件取得部 2 3 2、ファイル条件判定部 2 3 3 およびログ削減部 2 3 4 の機能が備えられていてオン（有効）である場合に適用されてもよい。

本例では、検査条件の内容は、ファイル条件の内容を含まないとする。なお、検査条件の内容が、ファイル条件の内容の一部を含んでもよい。

[0116] （ステップ S 1 2 1）

ファイル分析装置 4 1 では、受信部 1 2 1 によって、端末装置 5 3 から送信された分析対象のファイルを受信する。そして、ステップ S 1 2 2 の処理へ移行する。

[0117] （ステップ S 1 2 2）

ファイル分析装置 4 1 では、ファイル検査部 1 1 3 が、受信されたファイルについて、所定の検査条件が満たされるか否かを判定する。

この結果、ファイル分析装置 4 1 では、ファイル検査部 1 1 3 が、受信されたファイルについて、所定の検査条件が満たされると判定した場合には（ステップ S 1 2 2：YES）、ステップ S 1 2 3 の処理へ移行する。

一方、ファイル分析装置 4 1 では、ファイル検査部 1 1 3 が、受信されたファイルについて、所定の検査条件が満たされないと判定した場合には（ステップ S 1 2 2：NO）、ステップ S 1 2 6 の処理へ移行する。

[0118] （ステップ S 1 2 3）

ファイル分析装置 4 1 では、ファイル分析部 1 1 4 が、ファイル条件を取

得する。その後、ファイル分析装置 4 1 では、ファイル分析部 1 1 4 が、検査後のファイルについて、ファイル条件が満たされるか否かを判定する。

この結果、ファイル分析装置 4 1 では、ファイル分析部 1 1 4 が、検査後のファイルについて、ファイル条件が満たされると判定した場合には（ステップ S 1 2 3 : YES）、ステップ S 1 2 5 の処理へ移行する。この場合、当該ファイルが分析対象となる。

一方、ファイル分析装置 4 1 では、ファイル分析部 1 1 4 が、検査後のファイルについて、ファイル条件が満たされないと判定した場合には（ステップ S 1 2 3 : NO）、ステップ S 1 2 4 の処理へ移行する。

[0119] （ステップ S 1 2 4）

ファイル分析装置 4 1 では、ファイル分析部 1 1 4 が、検査後のファイルに含まれるログを削減する。そして、ステップ S 1 2 5 の処理に移行する。この場合、削減後のログを含むファイルが分析対象となる。

なお、本例では、ファイル分析部 1 1 4 は、削減後のログが含まれるファイルがファイル条件を満たすようにログの削減を行う。

[0120] （ステップ S 1 2 5）

ファイル分析装置 4 1 では、ファイル分析部 1 1 4 が、分析対象となるファイルについて、分析条件に基づいて、分析を行う。そして、ステップ S 1 2 6 の処理へ移行する。

[0121] （ステップ S 1 2 6）

ファイル分析装置 4 1 では、通知部 1 1 5 が、端末装置 5 3 に対して通知を行う。

ここで、通知部 1 1 5 は、ファイル検査部 1 1 3 によってファイルが検査条件を満たさないと判定された場合には、その旨の情報を端末装置 5 3 に対して通知する。

また、通知部 1 1 5 は、ファイル分析部 1 1 4 によってファイルに問題が無いと判定された場合には、その旨の情報を端末装置 5 3 に対して通知する。

また、通知部 115 は、ファイル分析部 114 によってファイルに問題があると判定された場合には、その旨の情報を端末装置 53 に対して通知する。

また、通知部 115 は、ファイル分析部 114 によってログの削減が行われた場合には、その旨の情報を端末装置 53 に対して通知する。当該情報は、例えば、削減されたログを特定する情報と、削減されなかったログを特定する情報のうちの一方または両方を含んでもよい。これにより、端末装置 53 のユーザは、ファイル分析装置 41 において分析対象のログの削減が行われた場合には、そのことを把握することができる。

[0122] ここで、ファイル分析装置 41 におけるファイル条件の判定処理およびログの削減処理については、例えば、端末装置 53 におけるファイル条件の判定処理およびログの削減処理と同様なものであってもよい。つまり、本例では、端末装置 53 においてファイル条件の判定処理およびログの削減処理が行われなくても、ファイル分析装置 41 においてファイル条件の判定処理およびログの削減処理が行われる。

なお、ファイル分析装置 41 において用いられるファイル条件と、端末装置 53 において用いられるファイル条件が存在する場合には、例えば、これらのファイル条件は、同じであってもよく、あるいは、一部または全部が異なってもよい。

[0123] また、本例では、ファイル分析装置 41 において、ファイル分析部 114 がファイル条件の判定処理およびログの削減処理を行う場合を示したが、他の例として、ファイル分析部 114 の代わりにファイル検査部 113 がファイル条件の判定処理およびログの削減処理を行ってもよい。この場合、検査条件の内容がファイル条件の内容の一部または全部を含んでもよい。検査条件の内容がファイル条件の内容の全部を含む場合には、検査条件の判定だけ行われてもよく、ファイル条件の判定は不要である。

[0124] <変形例>

図 14 を参照して、変形例を説明する。

図１４は、本発明の一実施形態に係るファイル分析装置４１において行われる処理の手順の一例を示す図である。

本例では、ファイル分析装置４１が、所定のタイミング（説明の便宜上、「分析推奨タイミング」ともいう。）で、端末装置５３に対してファイル分析のサービスを利用することを推奨する。分析推奨タイミングは、任意のタイミングであってもよく、例えば、定期的なタイミングであってもよい。

本例では、分析推奨タイミングを特定する情報が、記憶部１１１に記憶されている。

[0125] （ステップＳ１４１）

ファイル分析装置４１では、管理部１１６が、分析推奨タイミングになったか否かを判定する。この場合、管理部１１６は、例えば、ファイル分析装置４１の内部または外部に備えられた時計機能（図示せず）の情報を参照してもよい。

この結果、ファイル分析装置４１では、管理部１１６が、分析推奨タイミングになったと判定した場合には（ステップＳ１４１：ＹＥＳ）、ステップＳ１４２の処理へ移行する。

一方、ファイル分析装置４１では、管理部１１６が、分析推奨タイミングになっていないと判定した場合には（ステップＳ１４１：ＮＯ）、本フローの処理を終了する。

[0126] （ステップＳ１４２）

ファイル分析装置４１では、管理部１１６が、通知部１１５によって、端末装置５３に対して、分析推奨タイミングになったことを示す情報を通知する。そして、本フローの処理を終了する。

なお、本フローの処理は、例えば、一定の時間間隔ごとに行われてもよい。

また、通知部１１５によって端末装置５３に対して通知を行う手法としては、任意の手法が用いられてもよい。

[0127] ここで、端末装置５３では、ファイル分析装置４１から分析推奨タイミン

グであることを推奨（通知）された場合に、一例として、その旨を表す情報を表示部214の画面に表示してもよい。この場合、ユーザは、分析推奨タイミングであることを把握することができる。

また、端末装置53では、ファイル分析装置41から分析推奨タイミングであることを推奨（通知）された場合に、他の例として、ユーザの操作が無くても、自動的に、ファイル分析のサービスを受けるための処理（例えば、図9に示されるフローの処理）を行ってもよい。

[0128] 図15は、本発明の一実施形態に係る情報処理装置4001のハードウェア構成の一例を示す図である。

本実施形態における端末装置53あるいはファイル分析装置41などとして、図15に示されるようなハードウェア構成を有する情報処理装置4001が使用されてもよい。

[0129] 図15の例では、情報処理装置4001は、プロセッサ4011と、操作部4012と、表示部4013と、記憶装置4014と、メモリ4015と、入出力インターフェイス4016と、ネットワークインターフェイス4017と、これらを接続するバス4021を備える。

[0130] プロセッサ4011は、CPU（Central Processing Unit）などから構成されており、プログラムを実行することで、当該プログラムに規定された処理を実行する。

操作部4012は、キーボード、マウスなどのうちの1以上の入力装置を備え、ユーザ（人）により行われる操作を受け付ける。

表示部4013は、画面を有しており、情報を当該画面に表示出力する。

[0131] 記憶装置4014は、不揮発性の記憶部であり、例えば、ハードディスクなどから構成されており、情報を記憶する。

メモリ4015は、揮発性の記憶部であり、RAM（Random Access Memory）などから構成されており、情報を一時的に記憶する。RAMとしては、例えば、DRAM（Dynamic Random Access Memory）が用いられてもよい。

記憶装置４０１４あるいはメモリ４０１５は、例えば、プロセッサ４０１１により実行されるプログラムの情報を記憶してもよい。

[0132] 入出力インターフェイス４０１６は、外部の記録媒体などと接続するインターフェイスである。

ネットワークインターフェイス４０１７は、外部のネットワークと接続するインターフェイスである。

[0133] ここで、情報処理装置４００１は、プロセッサ４０１１として、１個のプロセッサを備えてもよく、または、２個以上のプロセッサを備えてもよい。一例として、情報処理装置４００１は、複数個のＣＰＵを備えて、それぞれのＣＰＵによりそれぞれの処理を実行するとともに、これら複数個のＣＰＵにより連携して全体の処理を実現してもよい。

[0134] [実施形態のまとめ]

以上のように、本実施形態に係るファイル分析システム１では、端末装置５３は、分析対象とするログが含まれるファイルをファイル分析装置４１に送信することで、当該ログについてファイル分析装置４１によって分析された結果の通知を受けることができる。このため、本実施形態に係るファイル分析システム１では、ログを分析するシステムを動作可能な状態にするための初期的な設定が行われなくても、簡易にログの分析を行うことができ、ログ分析のサービスを簡易に実現することができる。

[0135] 例えば、端末装置５３のユーザは、センサの設定およびネットワークの設定が行われなくても、セキュリティセンサのログが含まれるファイルを端末装置５３からファイル分析装置４１に送ることで、監視機能の分析精度の評価あるいは確認を行うことができる。

通常、セキュリティセンサでは常にログを監視することが行われるが、本実施形態に係るファイル分析システム１では、端末装置５３からファイル分析装置４１に、分析が希望されるログが含まれるファイルが送信されればよく、ファイル分析のサービスを簡易に試用することが可能である。

[0136] また、本実施形態に係るファイル分析システム１では、例えば、端末装置

５３では、セキュリティリスクが高まった期間に限って、ファイル分析のサービスを受けることも可能である。

例えば、端末装置５３では、大規模な新型ウィルスが発生したときに、そのときから過去の所定期間のログを対象としてファイル分析のサービスを受けることが可能である。当該所定期間は、例えば、過去２週間などの期間であってもよい。また、端末装置５３において、サービスを受けるための契機としては、例えば、ユーザによって行われる操作に応じてサービスを受けてもよく、あらかじめ設定された新型ウィルスの発生時に関する規則に基づいてサービスを受けてもよく、あるいは、ファイル分析装置４１からの要求に応じてサービスを受けてもよい。

[0137] 本実施形態に係るファイル分析システム１では、端末装置５３において、ログ削減部２３４によってログの削減が行われることで、端末装置５３からファイル分析装置４１に送信されるファイルに含まれるログのデータ量が削減される。これにより、本実施形態に係るファイル分析システム１では、例えば、ファイル分析が行われることが不要なログが端末装置５３において除かれるため、ファイル分析のサービスの効率化を図ることができる。また、本実施形態に係るファイル分析システム１では、例えば、分析対象となるファイルに含まれるログのデータ量に上限値の条件がある場合には、当該条件が満たされるように端末装置５３において当該ログが削減されるため、ファイル分析のサービスを円滑に進めることが可能である。

[0138] 通常、セキュリティセンサでは、ログファイルのデータサイズが大きいことから、当該ログファイルの分析に多大な時間がかかること、あるいは、分析の容量制限の条件が満たされないことが発生し易いが、本実施形態に係るファイル分析システム１では、このような問題を解消することができる。本実施形態に係るファイル分析システム１では、例えば、分析対象とすることが可能なログのデータ量を制限することで、ファイル分析のサービスにかかる負荷を小さくして、ファイル分析のサービスにかかる料金を低価格に抑えることが可能である。

[0139] また、本実施形態に係るファイル分析システム１では、例えば、端末装置５３において、ファイル分析のサービスを受けるための専用ツールが使用されることで、端末装置５３のユーザによって行われる操作を簡易化することが可能である。また、専用ツールが使用されることで、例えば、セキュリティ性を高めることが可能である。

また、本実施形態に係るファイル分析システム１では、端末装置５３とファイル分析装置４１との間でオンデマンドの通信が用いられることで、例えば、低コスト化を図ることが可能である。

[0140] [ログの種類]

本実施形態では、ファイル分析の対象とするログとして、セキュリティセンサのログが用いられる場合を示した。セキュリティセンサのログとしては、例えば、FW (FireWall)、NGFW (New Generation FireWall)、IPS (Intrusion prevention system)、IDS (Intrusion Detection System)、UTM (Unified Threat Management)、WAF (Web Application Firewall) などのログがある。

[0141] 一例として、ログを検出する装置は、コンピュータネットワークにおいて不正な侵入を防止する侵入防止システム (IPS) の装置であってもよい。例えば、当該装置は、不正に関係する可能性があるログを検出してもよい。

他の例として、ログを検出する装置は、通過させてはいけない通信を阻止するファイアウォール (FW) の装置であってもよい。例えば、当該装置は、不正に関係する可能性があるログと、不正に関係しないログとの両方を検出してもよい。

なお、一般に、IPSとファイアウォールとを比較すると、ファイアウォールでは通過した信号についてのログもあるためデータ量が多大になり易く、IPSの方が、問題のある可能性があるログの密度が高いといえる。

[0142] ファイル分析の対象とするログとして、他のログを用いることも可能であ

る。他のログとしては、例えば、認証ログ、エラーログ、端末スキャンログ、通信ログ、プログラム稼働ログ、アプリケーション動作ログなどがある。

認証ログとしては、例えば、Active Directory、BIND (Berkeley Internet Name Domain)、DNS (Domain Name System) などのログがある。

エラーログとしては、例えば、WinEvtなどのログがある。

端末スキャンログとしては、アンチウィルス、EDR (Endpoint Detection and Response) などのログがある。

通信ログとしては、Proxy、mail、Fileアクセス、データベース (DB: DataBase) アクセスなどのログがある。

プログラム稼働ログとしては、例えば、bootログ、dmesgなどのログがある。

アプリケーション動作ログとしては、例えば、イベントログ、固有ログなどのログがある。

[0143] 本実施形態では、ファイル分析の対象としてログが用いられる場合を示したが、ファイル分析の対象としてログ以外の情報を用いることも可能である。

ログ以外の情報としては、例えば、オペレーティングシステム (OS: Operating System) の設定の情報がある。

OSの設定の情報としては、例えば、レジストリの情報などがある。

また、例えば、Webの閲覧の履歴、操作の履歴、あるいは、ログインの履歴などが用いられてもよい。

[0144] 本実施形態では、1個のログ検出装置51によって1種類のログを検出する場合を示したが、2個以上のログ検出装置が備えられて、2種類以上のログを検出する構成が用いられてもよい。

なお、ログ検出装置は、例えば、端末装置53の外部に備えられてもよく、あるいは、端末装置53の内部の機能として備えられてもよい。

[0145] ログ管理装置52は、複数のログ検出装置によって検出されたログの情報

を記憶部 151 に記憶して管理してもよい。

例えば、複数の異なる種類のログの情報が時間順に混じった形で記憶等されてもよい。各ログには、例えば、当該各ログを検出したセンサを識別する情報が付加されている。当該各ログは、当該情報に基づいて、区別されることが可能である。これにより、複数の異なる種類のログの情報が混じった情報から、所定の種類のログの情報が抽出されることが可能である。

[0146] 端末装置 53 において、分析対象とするファイルには、例えば、1 種類のログが含まれてもよく、あるいは、2 種類以上のログが含まれてもよい。

ファイル分析装置 41 において、ファイル検査部 113 によるファイルの検査は、例えば、ログの種類ごとに行われてもよく、あるいは、2 以上のログの種類についてまとめて行われてもよい。

ファイル分析装置 41 において、ファイル分析部 114 によるファイルの分析は、例えば、ログの種類ごとに行われてもよく、あるいは、2 以上のログの種類についてまとめて行われてもよい。

[0147] <構成例>

一構成例として、端末装置（本実施形態では、端末装置 53）において、ログを常時監視し常時監視されたログを出力するセキュリティセンサ（本実施形態では、ログ検出装置 51 のセンサ）から出力された複数のログのうちの一部のログを取得し、取得されたログを含むファイルを生成するファイル生成部（本実施形態では、ファイル生成部 235）と、ファイル生成部によって生成されたファイルをファイル分析装置（本実施形態では、ファイル分析装置 41）に送信するファイル送信部（本実施形態では、通信部 215）と、ファイル分析装置から送られるファイルの分析結果の通知を受ける通知制御部（本実施形態では、通知制御部 238）と、を備える。

一構成例として、端末装置において、分析対象とされることが不要である不要ログ（不要なログ）を特定する情報に基づいて、不要ログをファイルに含められるログから削減することで、ファイルに含められるログのデータ量を削減する不要ログ削減部（本実施形態では、ログ削減部 234 が有する機

能)を備える。

一構成例として、端末装置において、ファイルに含められるログの範囲を削減することで、ファイルに含められるログのデータ量を所定の上限值以下とするログ範囲削減部(本実施形態では、ログ削減部234が有する機能)を備える。

一構成例として、端末装置において、ファイルの分析の要求が可能であるかを判定する分析要求可否判定部(本実施形態では、分析要求可否判定部239)を備える。

[0148] 一構成例として、ファイル分析装置(本実施形態では、ファイル分析装置41)において、端末装置(本実施形態では、端末装置53)から送信されたファイルを受信する受信部(本実施形態では、受信部121)と、受信部によって受信されたファイルについて分析を行うファイル分析部(本実施形態では、ファイル分析部114)と、ファイル分析部によって行われたファイルの分析の結果の通知を端末装置に送る通知部(本実施形態では、通知部115)と、を備え、ファイルは、ログを常時監視し常時監視されたログを出力するセキュリティセンサ(本実施形態では、ログ検出装置51のセンサ)から出力された複数のログのうちの一部のログを含む。

一構成例として、ファイル分析装置において、ファイル分析部によって行われる分析に関する課金情報を管理する管理部(本実施形態では、管理部116)を備える。課金情報は、分析の回数に応じた金額の情報を含む。分析の回数に応じた金額の情報は、分析の回数に応じた有料の金額の情報、または、分析の回数が所定の回数以下では無料であることを示す情報である。

[0149] なお、本発明は、端末装置あるいはファイル分析装置などの装置、ファイル分析システムなどのシステム、ファイル分析方法などの方法、プログラム、プログラムを記録した記録媒体など、様々な態様で実施されてもよい。記録媒体としては、例えば、一時的記録媒体であってもよい。

[0150] 以上のように、実施形態に係る各装置(例えば、端末装置53、ファイル分析装置41など)の機能を実現するためのプログラムをコンピュータ読み

取り可能な記録媒体（記憶媒体）に記録（記憶）して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することにより、処理を行うことができる。

なお、ここでいう「コンピュータシステム」とは、オペレーティングシステムあるいは周辺機器等のハードウェアを含むものであってもよい。

また、「コンピュータ読み取り可能な記録媒体」とは、フレキシブルディスク、光磁気ディスク、ROM（Read Only Memory）、フラッシュメモリ等の書き込み可能な不揮発性メモリ、DVD（Digital Versatile Disc）等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。

さらに、「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークあるいは電話回線等の通信回線を介してプログラムが送信された場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリ（例えば、DRAM）のように、一定時間プログラムを保持しているものも含む。

また、上記のプログラムは、このプログラムを記憶装置等に格納したコンピュータシステムから、伝送媒体を介して、あるいは、伝送媒体中の伝送波により他のコンピュータシステムに伝送されてもよい。ここで、プログラムを伝送する「伝送媒体」は、インターネット等のネットワーク（通信網）あるいは電話回線等の通信回線（通信線）のように情報を伝送する機能を有する媒体のことをいう。

また、上記のプログラムは、前述した機能の一部を実現するためのものであってもよい。さらに、上記のプログラムは、前述した機能をコンピュータシステムに既に記録されているプログラムとの組み合わせで実現できるもの、いわゆる差分ファイル（差分プログラム）であってもよい。

[0151] なお、本発明を実施の形態を用いて説明したが、本発明の技術的範囲は上記実施の形態には限定されない。本発明の精神及び範囲から逸脱することなく様々に変更したり代替態様を採用したりすることが可能なことは、当業者

に明らかである。

符号の説明

- [0152] 1…ファイル分析システム
- 1 1…分析部
 - 2 1～2 3…端末部
 - 3 1…ネットワーク
 - 4 1…ファイル分析装置
 - 4 2…We bサーバ装置
 - 4 3…メールサーバ装置
 - 5 1…ログ検出装置
 - 5 2…ログ管理装置
 - 5 3…端末装置
 - 1 1 1、1 5 1、2 1 6…記憶部
 - 1 1 2、2 1 5…通信部
 - 1 1 3…ファイル検査部
 - 1 1 4…ファイル分析部
 - 1 1 5…通知部
 - 1 1 6…管理部
 - 1 2 1…受信部
 - 1 3 1…復号部
 - 1 3 2…解凍部
 - 2 1 1…入力部
 - 2 1 2…出力部
 - 2 1 3、4 0 1 2…操作部
 - 2 1 4、4 0 1 3…表示部
 - 2 1 7…制御部
 - 2 3 1…ログ取得部
 - 2 3 2…ファイル条件取得部

2 3 3 …ファイル条件判定部
2 3 4 …ログ削減部
2 3 5 …ファイル生成部
2 3 6 …圧縮部
2 3 7 …暗号化部
2 3 8 …通知制御部
2 3 9 …分析要求可否判定部
1 0 1 1 …ファイル
2 0 1 1、2 1 1 1、2 2 1 1 …表示内容
2 2 2 1 …ボタン
3 0 1 1 …契約情報
4 0 0 1 …情報処理装置
4 0 1 1 …プロセッサ
4 0 1 4 …記憶装置
4 0 1 5 …メモリ
4 0 1 6 …入出力インターフェイス
4 0 1 7 …ネットワークインターフェイス
4 0 2 1 …バス

請求の範囲

- [請求項1] ログを常時監視し常時監視された前記ログを出力するセキュリティセンサから出力された複数の前記ログのうちの一部の前記ログを取得し、取得された前記ログを含むファイルを生成するファイル生成部と、
- 、
- 前記ファイル生成部によって生成された前記ファイルを、1回の分析対象となる1個または複数個の前記ファイルに含まれる前記ログの情報が許容されるデータ量の上限値以下であるという条件が満たされる場合にファイル分析を行うファイル分析装置に送信するファイル送信部と、
- 前記ファイル分析装置から送られる前記ファイルの分析結果の通知を受ける通知制御部と、
- 前記1回の分析対象となる1個または複数個の前記ファイルに含まれる予定の前記ログの情報が許容されるデータ量の前記上限値以下であるという条件が満たされるか否かを判定するファイル条件判定部と、
- 前記ファイル条件判定部によって前記条件が満たされないと判定された場合、前記ファイルに含まれる前記ログのデータ量を削減するログ削減部と、
- を備え、
- 前記ファイル条件判定部によって前記条件が満たされないと判定された場合、前記ログ削減部によって前記ファイルに含まれる前記ログのデータ量を削減して、前記条件が満たされるようにされた前記ログの情報をを用いて、前記ファイル生成部が前記ファイルを生成し、前記ファイル送信部が前記ファイルを前記ファイル分析装置に送信する
- 、
- 端末装置。
- [請求項2] 前記ログ削減部は、前記ログが発生した日時が含まれるべき期間で

あって当該期間に含まれる前記ログの情報について前記条件が満たされる当該期間が表示されるようにし、前記ログ削減部は、表示された前記期間がユーザの操作によって変更されたときに、前記条件が満たされない場合には、前記条件が満たされるように前記期間を変更し、

前記ファイル生成部は、前記条件が満たされる前記期間に含まれる前記ログの情報を用いて前記ファイルを生成する、

請求項 1 に記載の端末装置。

[請求項3] 前記ユーザの操作によって 1 個または 2 個以上のセンサが指定され、

前記ファイルに含められる予定の前記ログの情報には、指定された前記センサによって検出された前記ログの情報が含められる、

請求項 2 に記載の端末装置。

[請求項4] 前記ファイルの分析のサービスに関する契約の内容と、前記サービスの利用状況とに基づいて、前記ファイルの分析の要求が可能であるか否かを判定する分析要求可否判定部を備える、

請求項 1 から請求項 3 のいずれか 1 項に記載の端末装置。

[請求項5] ログを常時監視し常時監視された前記ログを出力するセキュリティセンサから出力された複数の前記ログのうちの一部の前記ログを含むファイルであって端末装置から送信された 1 回の分析対象となる 1 個または複数個の前記ファイルを受信する受信部と、

前記受信部によって受信された前記ファイルについて、前記 1 回の分析対象となる 1 個または複数個の前記ファイルに含まれる前記ログの情報が許容されるデータ量の上限値以下であるという検査条件が満たされるか否かを判定するファイル検査部と、

前記ファイル検査部によって前記検査条件が満たされると判定された前記 1 回の分析対象となる 1 個または複数個の前記ファイルに含まれる前記ログの情報について分析を行うファイル分析部と、

前記ファイル分析部によって行われた前記ファイルの分析の結果の通知を前記端末装置に送る通知部と、

を備える、

ファイル分析装置。

[請求項6]

前記ファイル分析部によって行われる前記分析に関する課金情報を管理する管理部を備え、

前記課金情報は、前記分析の回数に応じた金額の情報を含み、

前記分析の回数に応じた金額の情報は、前記分析の回数に応じた有料の金額の情報、または、前記分析の回数が所定の回数以下では無料であることを示す情報である、

請求項5に記載のファイル分析装置。

[請求項7]

端末装置と、ファイル分析装置と、を備えたファイル分析システムであって、

前記端末装置は、

ログを常時監視し常時監視された前記ログを出力するセキュリティセンサから出力された複数の前記ログのうちの一部の前記ログを取得し、取得された前記ログを含むファイルを生成するファイル生成部と、

前記ファイル生成部によって生成された前記ファイルを前記ファイル分析装置に送信するファイル送信部と、

前記ファイル分析装置から送られる前記ファイルの分析結果の通知を受ける通知制御部と、

1回の分析対象となる1個または複数個の前記ファイルに含められる予定の前記ログの情報が許容されるデータ量の上限値以下であるという条件が満たされるか否かを判定するファイル条件判定部と、

前記ファイル条件判定部によって前記条件が満たされないと判定された場合、前記ファイルに含められる前記ログのデータ量を削減するログ削減部と、

を備え、

前記ファイル条件判定部によって前記条件が満たされないと判定された場合、前記ログ削減部によって前記ファイルに含められる前記ログのデータ量を削減して、前記条件が満たされるようにされた前記ログの情報をを用いて、前記ファイル生成部が前記ファイルを生成し、前記ファイル送信部が前記ファイルを前記ファイル分析装置に送信し、

前記ファイル分析装置は、

前記端末装置から送信された前記ファイルを受信する受信部と、

前記受信部によって受信された前記ファイルについて所定の検査条件が満たされるか否かを判定するファイル検査部と、

前記ファイル検査部によって前記検査条件が満たされると判定された前記ファイルについて分析を行うファイル分析部と、

前記ファイル分析部によって行われた前記ファイルの分析の結果の通知を前記端末装置に送る通知部と、

を備える、

ファイル分析システム。

[請求項8]

端末装置が、ログを常時監視し常時監視された前記ログを出力するセキュリティセンサから出力された複数の前記ログのうちの一部の前記ログを取得し、1回の分析対象となる1個または複数個のファイルに含められる予定の前記ログの情報が許容されるデータ量の上限値以下であるという条件が満たされるか否かを判定し、前記条件が満たされないと判定された場合、前記ファイルに含められる前記ログのデータ量を削減して、前記条件が満たされるようにされた前記ログの情報をを用いて、前記ファイルを生成し、前記ファイルをファイル分析装置に送信し、

前記ファイル分析装置が、前記端末装置から送信された前記ファイルを受信し、受信された前記ファイルについて所定の検査条件が満たされるか否かを判定し、前記検査条件が満たされると判定された前記

ファイルについて分析を行い、前記ファイルの分析の結果の通知を前記端末装置に送り、

前記端末装置が、前記ファイル分析装置から送られる前記ファイルの分析結果の通知を受ける、

ファイル分析方法。

[請求項9]

ログを常時監視し常時監視された前記ログを出力するセキュリティセンサから出力された複数の前記ログのうちの一部の前記ログを取得する機能と、

1回の分析対象となる1個または複数個のファイルに含められる予定の前記ログの情報が許容されるデータ量の上限值以下であるという条件が満たされるか否かを判定する機能と、

前記条件が満たされないと判定された場合、前記ファイルに含められる前記ログのデータ量を削減して、前記条件が満たされるようにされた前記ログの情報をを用いて、前記ファイルを生成する機能と、

生成された前記ファイルを、前記1回の分析対象となる1個または複数個の前記ファイルに含まれる前記ログの情報が許容されるデータ量の前記上限値以下であるという前記条件が満たされる場合にファイル分析を行うファイル分析装置に送信する機能と、

前記ファイル分析装置から送られる前記ファイルの分析結果の通知を受ける機能と、

をコンピュータに実現させるためのプログラム。