

明 細 書

発明の名称：

分析装置、端末装置、分析システム、分析方法およびプログラム

技術分野

[0001] 本発明は、分析装置、端末装置、分析システム、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２０１８－１８０９１４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] 例えば、複数の異なる顧客の組織について、セキュリティログの分析を分析装置によって行う分析システムが知られている。

このような分析システムでは、セキュリティログの自動分析に用いられるルールとして、悪性のログの特徴を検出するルールなどが作成されて用いられる。また、このようなルールとして、複数の異なる顧客の組織に共通のルールが用いられることも多い。

[0003] しかしながら、このような共通のルールでは、例えば、特定の組織における悪性ではない装置の名称が偶然に悪性のサーバの名称と一致する場合などに、当該特定の組織のログについて判定の誤り（説明の便宜上、「誤検知」ともいう。）が発生し得る。つまり、悪性ではない当該装置が悪性と判定される誤検知が発生し得る。

このようなとき、例えば、誤検知が発生する当該特定の組織に向けてカスタムのルールを作成することが必要な場合があった。

[0004] なお、特許文献１には、クライアントコンピュータを管理するための集中管理サーバを構内ネットワーク内に備えたコンピュータシステムにおけるウェブアクセス監視方法が開示されている（特許文献１参照。）。当該ウェブアクセス監視方法では、集中管理サーバは、業務上または教育上で不要もしくはは不当なウェブアクセスに対する警告条件および警告時の処理形態を含む

監視ルールを設定する。

先行技術文献

特許文献

[0005] 特許文献1：国際公開第2007／069338号

発明の概要

発明が解決しようとする課題

[0006] しかしながら、複数の異なる顧客の組織のうちの特定の組織に誤検知が発生したときに、従来のようにカスタムのルールが作成される対処だけでは、効率的でない場合があった。

[0007] 本発明の実施形態は、このような事情に鑑み、複数の異なる顧客の組織のうちの特定の組織に誤検知が発生した場合に、効率的に対処することが可能な分析装置、端末装置、分析システム、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

[0008] 本発明の一態様は、第1端末装置に関する対象情報を取得する取得部と、前記取得部によって取得された前記対象情報が第1条件を満たすか否かを判定する分析実行部と、前記分析実行部によって前記対象情報が前記第1条件を満たすことを判定した場合、第1情報を前記第1端末装置に通知する通知部と、前記通知部によって通知された前記第1情報に対して前記第1端末装置から第2情報を受け付ける情報受付部と、前記第1情報に対して前記第1端末装置から前記第2情報が受け付けられた場合に、前記第1端末装置に対する前記第1情報の通知を抑制する通知抑制部と、を備え、前記通知抑制部は、前記第1端末装置について、前記第1条件による前記第1情報の通知を所定の期間停止させ、前記所定の期間が経過した後に前記第1条件による前記第1情報の通知を再開させる、分析装置である。

本発明の一態様は、第1端末装置に関する対象情報を取得する取得部と、前記取得部によって取得された前記対象情報が第1条件を満たすか否かを判

定する分析実行部と、前記分析実行部によって前記対象情報が前記第 1 条件を満たすことを判定した場合、第 1 情報を前記第 1 端末装置に通知する通知部と、前記通知部によって通知された前記第 1 情報に対して前記第 1 端末装置から第 2 情報を受け付ける情報受付部と、前記第 1 情報に対して前記第 1 端末装置から前記第 2 情報が受け付けられた場合に、前記第 1 端末装置に対する前記第 1 情報の通知を抑制する通知抑制部と、前記第 1 条件による前記第 1 情報の通知の状況を管理する管理部と、を備え、前記状況は、少なくとも、抑止されているという状況を含み、前記第 1 情報は、前記通知の状況を用いて検索されることが可能である、分析装置である。

本発明の一態様は、第 1 端末装置に関する対象情報を取得する取得部と、前記取得部によって取得された前記対象情報が第 1 条件を満たすか否かを判定する分析実行部と、前記分析実行部によって前記対象情報が前記第 1 条件を満たすことを判定した場合、第 1 情報を前記第 1 端末装置に通知する通知部と、前記通知部によって通知された前記第 1 情報に対して前記第 1 端末装置から第 2 情報を受け付ける情報受付部と、前記第 1 情報に対して前記第 1 端末装置から前記第 2 情報が受け付けられた場合に、前記第 1 端末装置に対する前記第 1 情報の通知を抑制する通知抑制部と、を備え、前記通知抑制部は、前記第 1 端末装置に対する前記第 1 情報の通知を抑制することを特定する第 2 条件に基づいて、前記第 1 端末装置に対する前記第 1 情報の通知を抑制する、分析装置である。

本発明の一態様は、第 1 端末装置に関する対象情報を取得する取得部と、前記取得部によって取得された前記対象情報が第 1 条件を満たすか否かを判定する分析実行部と、前記分析実行部によって前記対象情報が前記第 1 条件を満たすことを判定した場合、第 1 情報を前記第 1 端末装置に通知する通知部と、前記通知部によって通知された前記第 1 情報に対して前記第 1 端末装置から第 2 情報を受け付ける情報受付部と、前記第 1 情報に対して前記第 1 端末装置から前記第 2 情報が受け付けられた場合に、前記第 1 端末装置に対する前記第 1 情報の通知を抑制する通知抑制部と、を備え、前記対象情報は

、セキュリティに関するログである、分析装置である。

本発明の一態様に係る分析装置において、前記第 1 条件は、問題を検知するルールであり、前記第 1 情報は、前記問題に対応するアラートの情報であり、前記第 2 情報は、前記アラートについて誤りがあることを指示する情報である。

本発明の一態様に係る分析装置において、前記第 1 条件を変更する変更部を備える。本発明の一態様は、セキュリティに関するログを対象情報とし、端末装置に関する前記対象情報を検出して前記対象情報を分析装置に送信する検出装置を有する前記端末装置に関する前記対象情報が前記分析装置によって第 1 条件を満たすことが判定された場合に前記分析装置から通知される前記セキュリティに関する第 1 情報の通知を受信する通知受信制御部と、前記通知受信制御部によって受信された前記第 1 情報に対して前記セキュリティに関する所定の指示を受け付ける指示受付部と、前記第 1 情報に対して前記指示が受け付けられた場合に、前記端末装置に対する前記セキュリティに関する前記第 1 情報の通知を抑制する指示を含む第 2 情報を前記分析装置に送信する指示送信制御部と、を備える、前記端末装置である。

本発明の一態様に係る端末装置において、前記第 1 条件は、問題を検知するルールであり、前記第 1 情報は、前記問題に対応するアラートの情報であり、前記第 2 情報は、前記アラートについて誤りがあることを指示する情報である。

[0009] 本発明の一態様は、第 1 端末装置と、分析装置と、を備える分析システムであって、前記分析装置は、前記第 1 端末装置に関する対象情報を取得する取得部と、前記取得部によって取得された前記対象情報が第 1 条件を満たすか否かを判定する分析実行部と、前記分析実行部によって前記対象情報が前記第 1 条件を満たすことを判定した場合、第 1 情報を前記第 1 端末装置に通知する通知部と、前記通知部によって通知された前記第 1 情報に対して前記第 1 端末装置から第 2 情報を受け付ける情報受付部と、前記第 1 情報に対して前記第 1 端末装置から前記第 2 情報が受け付けられた場合に、前記第 1 端

末装置に対する前記第 1 情報の通知を抑制する通知抑制部と、を備え、前記第 1 端末装置は、前記分析装置から通知される前記第 1 情報の通知を受信する通知受信制御部と、前記通知受信制御部によって受信された前記第 1 情報に対して所定の指示を受け付ける指示受付部と、前記第 1 情報に対して前記指示が受け付けられた場合に、前記第 2 情報を前記分析装置に送信する指示送信制御部と、を備え、前記通知抑制部は、前記第 1 端末装置について、前記第 1 条件による前記第 1 情報の通知を所定の期間停止させ、前記所定の期間が経過した後に前記第 1 条件による前記第 1 情報の通知を再開させる、分析システムである。

本発明の一態様は、第 1 端末装置と、分析装置と、を備える分析システムであって、前記分析装置は、前記第 1 端末装置に関する対象情報を取得する取得部と、前記取得部によって取得された前記対象情報が第 1 条件を満たすか否かを判定する分析実行部と、前記分析実行部によって前記対象情報が前記第 1 条件を満たすことを判定した場合、第 1 情報を前記第 1 端末装置に通知する通知部と、前記通知部によって通知された前記第 1 情報に対して前記第 1 端末装置から第 2 情報を受け付ける情報受付部と、前記第 1 情報に対して前記第 1 端末装置から前記第 2 情報が受け付けられた場合に、前記第 1 端末装置に対する前記第 1 情報の通知を抑制する通知抑制部と、前記第 1 条件による前記第 1 情報の通知の状況を管理する管理部と、を備え、前記第 1 端末装置は、前記分析装置から通知される前記第 1 情報の通知を受信する通知受信制御部と、前記通知受信制御部によって受信された前記第 1 情報に対して所定の指示を受け付ける指示受付部と、前記第 1 情報に対して前記指示が受け付けられた場合に、前記第 2 情報を前記分析装置に送信する指示送信制御部と、を備え、前記状況は、少なくとも、抑止されているという状況を含み、前記第 1 情報は、前記通知の状況を用いて検索されることが可能である、分析システムである。

本発明の一態様は、第 1 端末装置と、分析装置と、を備える分析システムであって、前記分析装置は、前記第 1 端末装置に関する対象情報を取得する

取得部と、前記取得部によって取得された前記対象情報が第1条件を満たすか否かを判定する分析実行部と、前記分析実行部によって前記対象情報が前記第1条件を満たすことを判定した場合、第1情報を前記第1端末装置に通知する通知部と、前記通知部によって通知された前記第1情報に対して前記第1端末装置から第2情報を受け付ける情報受付部と、前記第1情報に対して前記第1端末装置から前記第2情報が受け付けられた場合に、前記第1端末装置に対する前記第1情報の通知を抑制する通知抑制部と、を備え、前記第1端末装置は、前記分析装置から通知される前記第1情報の通知を受信する通知受信制御部と、前記通知受信制御部によって受信された前記第1情報に対して所定の指示を受け付ける指示受付部と、前記第1情報に対して前記指示が受け付けられた場合に、前記第2情報を前記分析装置に送信する指示送信制御部と、を備え、前記通知抑制部は、前記第1端末装置に対する前記第1情報の通知を抑制することを特定する第2条件に基づいて、前記第1端末装置に対する前記第1情報の通知を抑制する、分析システムである。

本発明の一態様は、第1端末装置と、分析装置と、を備える分析システムであって、前記分析装置は、前記第1端末装置に関する対象情報を取得する取得部と、前記取得部によって取得された前記対象情報が第1条件を満たすか否かを判定する分析実行部と、前記分析実行部によって前記対象情報が前記第1条件を満たすことを判定した場合、第1情報を前記第1端末装置に通知する通知部と、前記通知部によって通知された前記第1情報に対して前記第1端末装置から第2情報を受け付ける情報受付部と、前記第1情報に対して前記第1端末装置から前記第2情報が受け付けられた場合に、前記第1端末装置に対する前記第1情報の通知を抑制する通知抑制部と、を備え、前記第1端末装置は、前記分析装置から通知される前記第1情報の通知を受信する通知受信制御部と、前記通知受信制御部によって受信された前記第1情報に対して所定の指示を受け付ける指示受付部と、前記第1情報に対して前記指示が受け付けられた場合に、前記第2情報を前記分析装置に送信する指示送信制御部と、を備え、前記対象情報は、セキュリティに関するログである

、分析システムである。

本発明の一態様に係る分析システムにおいて、前記第 1 条件は、問題を検知するルールであり、前記第 1 情報は、前記問題に対応するアラートの情報であり、前記第 2 情報は、前記アラートについて誤りがあることを指示する情報である。

本発明の一態様に係る分析システムにおいて、前記分析装置は、前記第 1 条件を変更する変更部を備える。

[0010] 本発明の一態様は、第 1 端末装置と、分析装置と、を備える分析システムにおける分析方法であって、前記分析装置は、前記第 1 端末装置に関する対象情報を取得し、取得された前記対象情報が第 1 条件を満たすか否かを判定し、前記対象情報が前記第 1 条件を満たすことを判定した場合、第 1 情報を前記第 1 端末装置に通知し、前記第 1 端末装置は、前記分析装置から通知される前記第 1 情報の通知を受信し、受信された前記第 1 情報に対して所定の指示が受け付けられた場合に、第 2 情報を前記分析装置に送信し、前記分析装置は、前記第 1 端末装置から第 2 情報が受け付けられた場合に、前記第 1 端末装置に対する前記第 1 情報の通知を抑制し、前記分析装置は、前記通知の抑制として、前記第 1 端末装置について、前記第 1 条件による前記第 1 情報の通知を所定の期間停止させ、前記所定の期間が経過した後に前記第 1 条件による前記第 1 情報の通知を再開させる、分析方法である。

本発明の一態様は、第 1 端末装置と、分析装置と、を備える分析システムにおける分析方法であって、前記分析装置は、前記第 1 端末装置に関する対象情報を取得し、取得された前記対象情報が第 1 条件を満たすか否かを判定し、前記対象情報が前記第 1 条件を満たすことを判定した場合、第 1 情報を前記第 1 端末装置に通知し、前記第 1 端末装置は、前記分析装置から通知される前記第 1 情報の通知を受信し、受信された前記第 1 情報に対して所定の指示が受け付けられた場合に、第 2 情報を前記分析装置に送信し、前記分析装置は、前記第 1 端末装置から第 2 情報が受け付けられた場合に、前記第 1 端末装置に対する前記第 1 情報の通知を抑制し、前記分析装置は、前記第 1

条件による前記第 1 情報の通知の状況を管理し、前記状況は、少なくとも、抑止されているという状況を含み、前記第 1 情報は、前記通知の状況を用いて検索されることが可能である、分析方法である。

本発明の一態様は、第 1 端末装置と、分析装置と、を備える分析システムにおける分析方法であって、前記分析装置は、前記第 1 端末装置に関する対象情報を取得し、取得された前記対象情報が第 1 条件を満たすか否かを判定し、前記対象情報が前記第 1 条件を満たすことを判定した場合、第 1 情報を前記第 1 端末装置に通知し、前記第 1 端末装置は、前記分析装置から通知される前記第 1 情報の通知を受信し、受信された前記第 1 情報に対して所定の指示が受け付けられた場合に、第 2 情報を前記分析装置に送信し、前記分析装置は、前記第 1 端末装置から第 2 情報が受け付けられた場合に、前記第 1 端末装置に対する前記第 1 情報の通知を抑制し、前記分析装置は、前記通知の抑制として、前記第 1 端末装置に対する前記第 1 情報の通知を抑制することを特定する第 2 条件に基づいて、前記第 1 端末装置に対する前記第 1 情報の通知を抑制する、分析方法である。

本発明の一態様は、第 1 端末装置と、分析装置と、を備える分析システムにおける分析方法であって、前記分析装置は、前記第 1 端末装置に関する対象情報を取得し、取得された前記対象情報が第 1 条件を満たすか否かを判定し、前記対象情報が前記第 1 条件を満たすことを判定した場合、第 1 情報を前記第 1 端末装置に通知し、前記第 1 端末装置は、前記分析装置から通知される前記第 1 情報の通知を受信し、受信された前記第 1 情報に対して所定の指示が受け付けられた場合に、第 2 情報を前記分析装置に送信し、前記分析装置は、前記第 1 端末装置から第 2 情報が受け付けられた場合に、前記第 1 端末装置に対する前記第 1 情報の通知を抑制し、前記対象情報は、セキュリティに関するログである、分析方法である。

本発明の一態様に係る分析方法において、前記第 1 条件は、問題を検知するルールであり、前記第 1 情報は、前記問題に対応するアラートの情報であり、前記第 2 情報は、前記アラートについて誤りがあることを指示する情報

である。

本発明の一態様に係る分析方法において、前記分析装置は、前記第 1 条件を変更する。

[0011] 本発明の一態様は、分析装置を構成するコンピュータに、第 1 端末装置に関する対象情報を取得する機能と、取得された前記対象情報が第 1 条件を満たすか否かを判定する機能と、前記対象情報が前記第 1 条件を満たすことを判定した場合、第 1 情報を前記第 1 端末装置に通知する機能と、通知された前記第 1 情報に対して前記第 1 端末装置から第 2 情報を受け付ける機能と、前記第 1 情報に対して前記第 1 端末装置から前記第 2 情報が受け付けられた場合に、前記第 1 端末装置に対する前記第 1 情報の通知を抑制する機能と、を実現させるためのプログラムであって、前記通知を抑制する機能は、前記第 1 端末装置について、前記第 1 条件による前記第 1 情報の通知を所定の期間停止させ、前記所定の期間が経過した後に前記第 1 条件による前記第 1 情報の通知を再開させる、プログラムである。 本発明の一態様は、分析装置を構成するコンピュータに、第 1 端末装置に関する対象情報を取得する機能と、取得された前記対象情報が第 1 条件を満たすか否かを判定する機能と、前記対象情報が前記第 1 条件を満たすことを判定した場合、第 1 情報を前記第 1 端末装置に通知する機能と、通知された前記第 1 情報に対して前記第 1 端末装置から第 2 情報を受け付ける機能と、前記第 1 情報に対して前記第 1 端末装置から前記第 2 情報が受け付けられた場合に、前記第 1 端末装置に対する前記第 1 情報の通知を抑制する機能と、前記第 1 条件による前記第 1 情報の通知の状況を管理する機能と、を実現させるためのプログラムであって、前記状況は、少なくとも、抑止されているという状況を含み、前記第 1 情報は、前記通知の状況を用いて検索されることが可能である、プログラムである。

本発明の一態様は、分析装置を構成するコンピュータに、第 1 端末装置に関する対象情報を取得する機能と、取得された前記対象情報が第 1 条件を満たすか否かを判定する機能と、前記対象情報が前記第 1 条件を満たすことを

判定した場合、第 1 情報を前記第 1 端末装置に通知する機能と、通知された前記第 1 情報に対して前記第 1 端末装置から第 2 情報を受け付ける機能と、前記第 1 情報に対して前記第 1 端末装置から前記第 2 情報が受け付けられた場合に、前記第 1 端末装置に対する前記第 1 情報の通知を抑制する機能と、を実現させるためのプログラムであって、前記通知を抑制する機能は、前記第 1 端末装置に対する前記第 1 情報の通知を抑制することを特定する第 2 条件に基づいて、前記第 1 端末装置に対する前記第 1 情報の通知を抑制する、プログラムである。

本発明の一態様は、分析装置を構成するコンピュータに、第 1 端末装置に関する対象情報を取得する機能と、取得された前記対象情報が第 1 条件を満たすか否かを判定する機能と、前記対象情報が前記第 1 条件を満たすことを判定した場合、第 1 情報を前記第 1 端末装置に通知する機能と、通知された前記第 1 情報に対して前記第 1 端末装置から第 2 情報を受け付ける機能と、前記第 1 情報に対して前記第 1 端末装置から前記第 2 情報が受け付けられた場合に、前記第 1 端末装置に対する前記第 1 情報の通知を抑制する機能と、を実現させるためのプログラムであって、前記対象情報は、セキュリティに関するログである、プログラムである。

本発明の一態様に係るプログラムにおいて、前記第 1 条件は、問題を検知するルールであり、前記第 1 情報は、前記問題に対応するアラートの情報であり、前記第 2 情報は、前記アラートについて誤りがあることを指示する情報である。

本発明の一態様に係るプログラムにおいて、さらに、前記第 1 条件を変更する機能を実現させるためのプログラムである。

本発明の一態様は、セキュリティに関するログを対象情報とし端末装置に関する前記対象情報を検出して前記対象情報を分析装置に送信する検出装置を有する前記端末装置を構成するコンピュータに、前記端末装置に関する前記対象情報が前記分析装置によって第 1 条件を満たすことが判定された場合に前記分析装置から通知される前記セキュリティに関する第 1 情報の通知を

受信する機能と、受信された前記第 1 情報に対して前記セキュリティに関する所定の指示を受け付ける機能と、前記第 1 情報に対して前記指示が受け付けられた場合に、前記端末装置に対する前記セキュリティに関する前記第 1 情報の通知を抑制する指示を含む第 2 情報を前記分析装置に送信する機能と、を実現させるためのプログラム。

本発明の一態様に係るプログラムにおいて、前記第 1 条件は、問題を検知するルールであり、前記第 1 情報は、前記問題に対応するアラートの情報であり、前記第 2 情報は、前記アラートについて誤りがあることを指示する情報である。

発明の効果

[0012] 上記した分析装置、端末装置、分析システム、分析方法およびプログラムによれば、複数の異なる顧客の組織のうちの特定の組織に誤検知が発生した場合に、効率的に対処することが可能である。

図面の簡単な説明

[0013] [図1]本発明の一実施形態に係る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アラート一覧の表示内容の一例を示す図である。

[図4]本発明の一実施形態に係るアラート詳細の表示内容の一例を示す図である。

[図5]本発明の一実施形態に係るアラート検索の表示内容の一例を示す図である。

[図6]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7]本発明の一実施形態に係る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8]本発明の一実施形態に係る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9]本発明の一実施形態に係る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10]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

[0014] 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。

[0015] [分析システム]

図1は、本発明の一実施形態に係る分析システム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。

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。

[0016] 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。

[0017] 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21～23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２１を代表させて説明する。

なお、それぞれの端末部２１～２３の構成あるいは動作が異なる態様が用いられてもよい。

[0018] 本実施形態では、分析部１１は、複数の端末部２１～２３のそれぞれに対して、それぞれの端末部２１～２３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１１は、複数の端末部２１～２３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。

[0019] 本実施形態では、分析部１１は、複数の端末部２１～２３に対して共通になっている。なお、分析システム１は、複数の分析部１１を備えてもよい。この場合、複数の分析部１１が、複数の端末部２１～２３を分担して、動作を行う。

ここで、分析部１１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２１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。

[0020] ネットワーク３１は、任意のネットワークであってもよい。ネットワーク３１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２１～２３と分析部１１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。

[0021] [端末部の概要]

端末部２１を代表させて説明する。

端末部２１は、ログ検出装置５１と、端末装置５２を備える。

図１の例では、ログ検出装置５１と端末装置５２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。

[0022] ログ検出装置５１は、検出の対象となる情報（説明の便宜上、「対象情報

」ともいう。)を検出する。本実施形態では、当該対象情報は、所定のログである。本実施形態では、ログ検出装置 5 1 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 3 1 を介する通信を対象としたログである。

ログ検出装置 5 1 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 5 1 は、端末装置 5 2 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 5 1 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 5 1 は、検出されたログを分析部 1 1 に送信する。当該ログの送信は、例えば、所定のログのまとまりごとに行われてもよい。当該まとまりは、所定の期間ごとのまとまりであってもよい。当該所定の期間は、例えば、1 日などであってもよい。

なお、本実施形態では、ログ検出装置 5 1 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 5 1 は、検出されたログを記憶する記憶部を備えてもよい。

[0023] 端末装置 5 2 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 2 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 2 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。また、端末装置 5 2 は、ネットワーク 3 1 を介して分析部 1 1 に情報を送信する。本実施形態では、端末装置 5 2 は、例えば、分析部 1 1 によって行われた分析の結果について、誤った検知（誤検知）に関する情報を分析部 1 1 に送信する。

[0024] [分析部の概要]

分析部 11 は、分析装置 41 と、Webサーバ装置 42 と、メールサーバ装置 43 を備える。

図 1 の例では、分析装置 41 と、Webサーバ装置 42 と、メールサーバ装置 43 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。

[0025] 分析装置 41 は、記憶部 111 と、取得部 112 と、分析実行部 113 と、通知部 114 と、誤検知制御部 115 と、管理部 116 を備える。

取得部 112 は、受信部 131 を備える。

管理部 116 は、検索処理部 151 を備える。

[0026] 分析装置 41 において行われる動作の概要を示す。

記憶部 111 は、各種の情報を記憶する。

取得部 112 は、受信部 131 によって、ログ検出装置 51 からネットワーク 31 を介して分析部 11 に送信されたログを受信する。そして、取得部 112 は、受信されたログを取得する。本実施形態では、取得部 112 は、様々なログを取得することで、様々なログを収集する。取得部 112 は、受信されたログを分析実行部 113 に出力する。本実施形態では、ログ検出装置 51 は、当該ログを分析装置 41 に宛てて送信する。

[0027] ここで、ログ検出装置 51 は、ログの情報を圧縮して、圧縮されたログの情報を分析装置 41 に送信してもよい。この場合、分析装置 41 では、分析実行部 113 は、受信された当該情報を解凍して、元のログの情報を取得する。なお、「解凍」の代わりに「伸張」などと呼ばれてもよい。

また、ログ検出装置 51 は、送信対象の情報を暗号化して、暗号化された情報を分析装置 41 に送信してもよい。この場合、分析装置 41 では、分析実行部 113 は、受信された当該情報を復号して、元の情報を取得する。

[0028] 分析実行部 113 は、取得部 112 から出力されたログを入力する。分析実行部 113 は、入力されたログについて、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。分析実行部 113 は、入力されたログについて、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114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。

分析実行部113は、当該情報に基づいて、分析条件を取得する。

[0029] 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のうちの1以上が、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。

[0030] また、問題があると判定すべき条件は、例えば、「ルール」と呼ばれてもよく、本実施形態では、説明の便宜上、「検知ルール」と呼んで説明する。検知ルールは、例えば、ログに基づいて問題を検知する条件であると捉えられてもよい。つまり、あるログについて、ある検知ルールに該当する状況が発生したと判定された場合に、当該検知ルールに対応付けられた問題が発生したと判定することが行われる。検知ルールは、1以上作成され、本実施形態では、複数の異なる検知ルールが作成されて使用される。

この場合、それぞれの検知ルールには、当該検知ルールに該当するか否かを判定するための規則を特定する情報が含まれる。また、それぞれの検知ルールには、当該検知ルールに該当した場合に発生したとされる問題を特定する情報が対応付けられる。なお、ある検知ルールに該当した場合に発生したとされる問題を特定する情報についても当該検知ルールに含まれる、と捉えられてもよい。

また、それぞれの問題には、当該問題が発生した場合に通知されるべきアラートの内容が対応付けられる。

[0031] これにより、本実施形態では、検知ルールと、問題と、アラート（アラートの内容）とが、対応付けられる。本実施形態では、このような対応付けの情報は、例えば、記憶部 1 1 1 に記憶されて、管理部 1 1 6 によって管理される。

なお、問題とアラートの内容とは、例えば、共通の情報として構成されてもよい。つまり、アラートの内容において問題を提示する場合には、アラートの内容によって問題も通知することが可能である。

[0032] また、本実施形態では、説明の便宜上、それぞれの検知ルールは、初期的には、すべての端末装置 5 2 に共通な検知ルールとして作成される場合を示す。他の例として、初期的に、検知ルールごとに、当該検知ルールが適用される 1 以上の端末装置 5 2 が設定されてもよい。このような設定の内容も当該検知ルールに含まれると捉えられてもよい。

検知ルールの具体例としては、「受信信号について、当該受信信号の送信元の装置の識別情報が所定の識別情報と一致する場合に、不審な送信元からの情報通信であるという問題が発生したとする検知ルール」、「送信信号について、当該送信信号の送信先の装置の識別情報が所定の識別情報と一致する場合に、不審な送信先への情報通信であるという問題が発生したとする検知ルール」などが用いられてもよい。

[0033] ここで、本実施形態では、検知ルールが満たされたときに、当該検知ルールに対応するアラートの通知が行われる場合と、当該検知ルールに対応するアラートの通知が行われない場合がある。本実施形態では、それぞれの検知ルールごとに、当該検知ルールが満たされたときにアラートの通知を行うか否かを規定する規則（本実施形態では、説明の便宜上、「アラートルール」ともいう。）が用いられる。

本実施形態では、検知ルールに対してアラートルールが対応付けられている。アラートルールでは、当該アラートルールに対応付けられた検知ルールが満たされたときにアラートの通知を行うべき端末装置 5 2 を特定する情報、あるいは、当該アラートルールに対応付けられた検知ルールが満たされた

ときにアラートの通知を行わない端末装置 5 2 を特定する情報が含まれる。アラートルールでは、例えば、初期的には、当該アラートルールに対応付けられた検知ルールが満たされたときにすべての端末装置 5 2 に対してアラートの通知を行うべきことが設定される。

[0034] なお、他の例として、アラートルールは、それぞれの端末装置 5 2 ごとに設けられてもよい。この場合、それぞれの端末装置 5 2 のアラートルールでは、当該端末装置 5 2 に対してアラートの通知を行うべき検知ルールを特定する情報、あるいは、当該端末装置 5 2 に対してアラートの通知を行わない検知ルールを特定する情報が含まれる。

[0035] ここで、本実施形態では、検知ルールとアラートルールとが組み合わせられることで、例えば、端末装置 5 2 について、所定の問題を検知してアラートを通知する場合と、所定の問題を検知するがアラートを通知しない場合とが識別される。

アラートを通知しない態様としては、例えば、アラートの通知を所定に期間停止する態様が含まれてもよく、あるいは、アラートの通知を永久的に停止する態様が含まれてもよい。

他の例として、検知ルールとアラートルールとが一体化されたルールが用いられてもよい。

[0036] 本実施形態では、分析実行部 1 1 3 は、ある検知ルールが満たされた場合に、当該検知ルールに対応するアラートルールに基づいて、アラートの通知を行うべき場合には分析結果情報を通知部 1 1 4 に出力し、アラートの通知を行わない場合には分析結果情報を通知部 1 1 4 に出力しない。

なお、本実施形態では、アラートの通知を行うか否かを分析実行部 1 1 3 によって制御する場合を示すが、他の例として、分析実行部 1 1 3 から通知部 1 1 4 へは分析結果情報を出力するが、通知部 1 1 4 がアラートルールの内容に基づいてアラートの通知を行うか否かを制御する構成が用いられてもよい。

[0037] なお、分析対象のログに複数の種類のログが含まれ得る場合には、例えば

、分析実行部 113 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。

[0038] また、例えば、ログ検出装置 51 のセンサが、ログの検出結果とともにアラートの情報を分析装置 41 に送信する構成が用いられてもよい。

この場合、分析装置 41 において、分析実行部 113 は、例えば、ログの検出結果に付されたアラートの情報が正しいか否かを判定する。この場合、例えば、ログの検出結果に付されたアラートの情報が正しいか否かを判定する条件が分析条件として用いられる。

一般に、ログ検出装置 51 のセンサでは、アラートを通知する当該センサから通知される当該アラートの精度は高くない場合も多い。当該アラートは、例えば、シグネチャの名称を含んでもよい。

[0039] 本実施形態では、検知ルールには、問題があるログであることを判定するための条件とともに、アラートの名称（説明の便宜上、「アラート名称」ともいう。）、重要度などのうちの 1 以上が対応付けられて保持されてもよい。当該アラートは、例えば、発生する問題に対応する。

アラート名称は、アラートの名称を表す。アラート名称は、例えば、アラートの種別ごとに、あらかじめ定められている。

それぞれのアラートには、当該アラートの内容の種別ごとを識別する情報が付加されてもよい。

重要度は、アラートの重要度を表す。重要度は、任意の段階で表されてもよい。本実施形態では、重要度は、3 個の段階で表される。

[0040] 通知部 114 は、分析実行部 113 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 52 に通知する。当該所定の情報としては、端末装置 52 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。

[0041] ここで、通知部 114 から端末装置 52 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 52 に通知すべき情報が発生した場合、通知部

114は、端末装置52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114は、端末装置52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114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114は、当該Webページに、端末装置52に通知する情報を含める。

[0042] メールサーバ装置43は、通知部114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43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52が宛先となっている電子メールが、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52に送信される。

Webサーバ装置42は、通知部114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42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42は、端末装置52からのアクセスに応じて、当該Webページを端末装置52に閲覧可能に提供する。

[0043] 誤検知制御部115は、分析実行部113によって行われた分析の結果について、誤検知に関する制御を行う。

誤検知制御部115は、例えば、それぞれのアラートについて端末装置52から誤検知であることの通知を受ける処理、それぞれのアラートについて端末装置52から誤検知であることの通知を受けた場合に通知元である当該端末装置52について当該アラートに該当する検知ルールによるアラートの通知を停止する処理、当該通知元に対する当該検知ルールによるアラートの通知を再開する処理などを行う。

本実施形態では、誤検知制御部115は、当該検知ルールに対応するアラ

ートルールの内容を書き換えることで、当該アラートの通知を停止すること、あるいは、当該アラートの通知を再開することを制御する。

[0044] 管理部 1 1 6 は、端末装置 5 2 について、各種の管理を行う。

管理部 1 1 6 では、例えば、検索処理部 1 5 1 が、情報を検索する処理を行う。検索処理部 1 5 1 は、端末装置 5 2 において行われる検索を端末装置 5 2 の代わりに実行する処理、あるいは、端末装置 5 2 において行われる検索を補助する処理を行ってもよい。検索処理部 1 5 1 は、例えば、記憶部 1 1 1 に記憶された情報を用いて、検索の処理を行う。

また、管理部 1 1 6 は、例えば、記憶部 1 1 1 に記憶される検知ルールなどを書き換えて変更する。このような書き換えには、例えば、新たな登録、上書き、および消去が含まれてもよい。

[0045] 本実施形態では、分析部 1 1 において、端末装置 5 2 の情報が既知である場合を示す。

本実施形態では、端末装置 5 2 の管理主体と、分析部 1 1 によって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 2 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 2 を特定する情報を含んでもよい。当該情報は、端末装置 5 2 の電子メールのアドレスを含んでもよい。

[0046] ここで、契約に関して設定される端末装置 5 2 の情報としては、例えば、サービスを受けることが可能な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。

管理部 1 1 6 は、端末装置 5 2 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 1 1 1 に記憶して管理してもよい。

なお、分析部 1 1 によって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５２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。

[0047] [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５２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５２は、入力部２１１と、出力部２１２と、操作部２１３と、表示部２１４と、通信部２１５と、記憶部２１６と、制御部２１７を備える。

制御部２１７は、通知受信制御部２３１と、指示送信制御部２３２と、検索制御部２３３を備える。

[0048] 入力部２１１は、外部の装置から出力される情報を入力する。

出力部２１２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２１３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２１３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２１４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。

通信部２１５は、ネットワーク３１を介した通信を行う。

記憶部２１６は、各種の情報を記憶する。

制御部２１７は、端末装置５２における各種の制御を行う。

[0049] 通知受信制御部２３１は、分析装置４１の通知部１１４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、通知受信制御部２３１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５２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、通知受信制御部 231 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。

[0050] 通知受信制御部 231 は、取得された電子メールの情報あるいは取得された Web ページの情報を表示部 214 の画面に表示する。

ログの分析結果の通知の内容は、例えば、ログの分析結果として問題が発生したことを判定したことを通知する情報を含む。このような通知は、アラート（警告）の通知となる。

なお、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。

[0051] 指示送信制御部 232 は、ユーザにより行われる操作部 213 の操作に応じた指示を、通信部 215 によって、分析装置 41 に送信する。

本実施形態では、表示部 214 の画面に表示される Web ページにおいて、ユーザは所定の指示を行うための操作を行うことが可能である。

本実施形態では、このような指示として、ログの分析結果において問題が発生したことが判定された検知について、誤った検知（誤検知）であることを通知する指示が用いられる。

[0052] 検索制御部 233 は、分析結果の通知の内容について、各種の検索の処理を行う。

検索制御部 233 は、例えば、分析装置 41 の検索処理部 151 によって行われた検索の処理の結果を受信して提示等してもよい。また、検索制御部 233 は、例えば、分析装置 41 の検索処理部 151 によって補助されて、検索の処理を行ってもよい。また、検索制御部 233 は、例えば、分析装置 41 とは独立して、検索の処理を行ってもよい。

[0053] [アラート一覧]

図 3 は、本発明の一実施形態に係るアラート一覧の表示内容 2011 の一

例を示す図である。

表示内容 2011 は、アラートの一覧を示す。表示内容 2011 は、端末装置 52 において、表示部 214 の画面に表示される。表示内容 2011 は、例えば、端末装置 52 ごとに異なり得る。図 3 の例では、アラートの一覧は、過去に行われたアラートの一覧である。

[0054] 表示内容 2011 は、例えば、分析装置 41 から端末装置 52 に提供された情報に基づいている。

一例として、表示内容 2011 は、分析装置 41 の側で生成されて、分析装置 41 から端末装置 52 に提供されてもよい。他の例として、表示内容 2011 は、分析装置 41 から端末装置 52 に提供された情報が記憶部 216 に記憶された後に、端末装置 52 において記憶部 216 に記憶された情報に基づいて生成されてもよい。なお、表示内容 2011 は、他の情報を含んでもよい。

[0055] 図 3 の例では、日時と、アラート名称と、重要度と、状況と、が対応付けられて表示されている。なお、重要度あるいは状況などのうちの 1 以上に応じて、情報の表示の色が切り替えられてもよい。

[0056] 日時は、アラートが発生した日時を表す。図 3 の例では、例えば、「2018/1/2」は、2018 年 1 月 2 日を表し、他も同様である。

アラート名称としては、図 3 の例では、「不審な送信」、「不審な受信」などがある。なお、これらのアラート名称は、説明の便宜上の例示であり、アラート名称としては任意の名称が用いられてもよい。

重要度としては、図 3 の例では、大きい方から小さい方へ向かって、大、中、小の 3 段階の重要度がある。

状況は、アラートが取り扱われている状況を表す。本実施形態では、状況としては、「未対応」、「調査中」、「対応済」、「保留」、「対応中」、「抑止」などの状況が用いられている。なお、状況としては、任意の状況が用いられてもよい。

[0057] 「未対応」は、アラートが未だに対応されていないことを表す。

「調査中」は、アラートについて調査が行われている最中であることを表す。

「対応済」は、アラートについて対応が済まされていることを表す。つまり、アラートについて問題が解消したことを表す。

「保留」は、アラートについて対応が保留にされていることを表す。

「対応中」は、アラートについて対応が行われている最中であることを表す。

「抑止」は、アラートについて、当該アラートの通知が抑止されていることを表す。本実施形態では、アラートについて、端末装置 5 2 において誤検知が指摘された場合に、分析装置 4 1 において「抑止」の状況が設定される。このような設定は、例えば、アラートルールに対して行われる。

なお、アラートの状況を表す各語は、任意の他の語を用いて表されてもよい。

[0058] ここで、アラートの日時、アラート名称、重要度は、例えば、分析装置 4 1 の分析実行部 1 1 3 により判定されて、これらの情報を含む分析結果情報が分析実行部 1 1 3 から通知部 1 1 4 に出力される。通知部 1 1 4 は、当該分析結果情報に基づいて、端末装置 5 2 に通知する内容にアラートの日時、アラート名称、重要度を含める。

また、アラートの状況は、例えば、端末装置 5 2 においてユーザによって行われる操作部 2 1 3 の操作に応じて設定される。設定されたアラートの状況は、端末装置 5 2 から分析装置 4 1 の通知部 1 1 4 に通知され、管理部 1 1 6 によって管理される。管理部 1 1 6 は、例えば、通知部 1 1 4 によって端末装置 5 2 から受信された情報に基づいて、アラートと状況とを対応付ける情報を記憶部 1 1 1 に記憶して管理する。

[0059] ここで、本実施形態では、アラート一覧において、「抑止」の状況にあるアラートの情報も表示される場合を示したが、他の例として、「抑止」の状況にあるアラートの情報は表示されない態様が用いられてもよい。

[0060] 図 4 は、本発明の一実施形態に係るアラート詳細の表示内容 2 1 1 1 の一

例を示す図である。

表示内容 2 1 1 1 は、アラートの詳細を示す。表示内容 2 1 1 1 は、端末装置 5 2 において、表示部 2 1 4 の画面に表示される。表示内容 2 1 1 1 は、例えば、端末装置 5 2 ごとに異なり得る。

[0061] 表示内容 2 1 1 1 は、例えば、分析装置 4 1 から端末装置 5 2 に提供された情報に基づいている。

一例として、表示内容 2 1 1 1 は、分析装置 4 1 の側で生成されて、分析装置 4 1 から端末装置 5 2 に提供されてもよい。他の例として、表示内容 2 1 1 1 は、分析装置 4 1 から端末装置 5 2 に提供された情報が記憶部 2 1 6 に記憶された後に、端末装置 5 2 において記憶部 2 1 6 に記憶された情報を用いて生成されてもよい。なお、表示内容 2 1 1 1 は、他の情報を含んでもよい。

[0062] アラートの詳細は、例えば、アラートの一覧のなかでユーザにより 1 個のアラートが指示された場合に指示されたアラートについてアラートの詳細が示される。

図 4 の例では、属性領域 2 1 2 1 の枠と、対応状況領域 2 1 2 2 の枠と、内容領域 2 1 2 3 の枠が、1 画面で表示されている。なお、これらの領域の名称、配置などは、任意であってもよい。

[0063] アラート詳細の画面では、1 個のアラートについての情報が表示される。

属性領域 2 1 2 1 には、表示対象となる 1 個のアラートの属性が示される。図 4 の例では、属性領域 2 1 2 1 には、日時、アラート名称、重要度、状況が示されている。なお、重要度あるいは状況などのうちの 1 以上に応じて、情報の表示の色が切り替えられてもよい。

対応状況領域 2 1 2 2 には、複数の対応状況のなかから任意の対応状況を選択することが可能な情報が示される。

内容領域 2 1 2 3 には、アラートあるいはアラートを発生させたログなどについて、詳しい情報が示される。

[0064] 図 4 の例では、選択可能な対応状況としては、「未対応」、「調査中」、

「対応済」、「保留」、「対応中」、「誤検知」、「対象外」がある。それぞれの対応状況に、選択された状態と選択されていない状態とで切り替えられるボタンが表示されている。当該ボタンは、例えば、ユーザにより行われる操作部 2 1 3 の操作に応じて、選択された状態である黒色の状態と、選択されていない状態である白色の状態とで切り替えられる。当該ボタンは、例えば、ラジオボタンであってもよい。

[0065] ここで、「未対応」、「調査中」、「対応済」、「保留」、「対応中」については、図 3 を参照して説明したのと同じである。

「誤検知」は、表示されているアラートについて、誤った検知であることを端末装置 5 2 から分析装置 4 1 に通知するための指示を受け付ける項目である。

「対象外」は、表示されているアラートについて、検知の対象外であることを端末装置 5 2 から分析装置 4 1 に通知するための指示を受け付ける項目である。

なお、本実施形態では、「誤検知」が選択されたアラートには分析装置 4 1 において自動的に「抑止」の状況が設定される。このため、本実施形態では、ユーザは「抑止」の状況を選択することはできない。他の例として、端末装置 5 2 において、ユーザが「抑止」の状況を選択することができる構成が用いられてもよい。

また、本実施形態では、「対象外」が選択されたアラートには分析装置 4 1 において自動的に「抑止」の状況が設定される。

本実施形態では、「誤検知」と「対象外」とは類似するところもあるが、別のものとして設けられている。なお、「対象外」は設けられなくてもよい。

[0066] 図 4 に示される表示内容 2 1 1 1 において、ユーザは、操作部 2 1 3 を操作することで、選択することが可能な対応状況のなかから、表示されているアラートに適した対応状況を選択する。

なお、本実施形態では、対応状況領域 2 1 2 2 において、初期のデフォルト

トでは、「未対応」が選択されているが、他の対応状況が選択されていてもよい。

対応状況領域 2 1 2 2 には、決定のボタン 2 1 3 1 も表示される。ユーザによって行われる操作部 2 1 3 の操作に基づいて、当該ボタン 2 1 3 1 が押下されると、選択されている対応状況を特定する情報が、指示送信制御部 2 3 2 によって端末装置 5 2 から分析装置 4 1 に送信される。

[0067] この場合、端末装置 5 2 では、アラートを特定する情報と、当該アラートについてユーザによって選択された対応状況を特定する情報を分析装置 4 1 に送信する。

分析装置 4 1 では、通知部 1 1 4 が端末装置 5 2 から送信された情報を受信し、管理部 1 1 6 が受信された情報を管理する。

[0068] <「誤検知」の選択>

分析装置 4 1 では、端末装置 5 2 から受信された情報が「誤検知」を示す場合には、誤検知制御部 1 1 5 が当該誤検知に係るアラートを発生させる検知ルールによるアラートの通知を一定期間停止させる。当該一定期間は、任意の期間であってもよく、例えば、1 か月などであってもよい。

本実施形態では、分析装置 4 1 において、このようなアラートの通知の停止は、ユーザによって「誤検知」が選択された端末装置 5 2 に対して行われ、他の端末装置に対しては行われない。つまり、同じ検知ルールであっても、当該検知ルールが誤検知となる端末装置 5 2 のみについて、当該検知ルールによるアラートの通知が停止させられる。

[0069] 本実施形態では、それぞれの顧客ごと、それぞれのアラートごとに、「誤検知」の選択が可能である。例えば、ある検知ルールについて、特定の顧客の組織のみで誤検知となる場合に、当該特定の顧客の組織のみについて誤検知とすることができる。当該特定の顧客の組織では、あるアラートに対して一度「誤検知」が選択されると、一定期間、同じ検知ルールに基づくアラートが通知されることを防止することができる。

[0070] なお、本実施形態では、このようなアラートの通知の停止は一時的に行わ

れるが、他の例として、このようなアラートの通知の停止が永久的に行われてもよく、つまり、該当する端末装置 5 2 について当該検知ルールが永久的に無効にされてもよい。検知ルールを無効にする手法としては、任意であってもよい。検知ルールを無効にする手法としては、例えば、管理部 1 1 6 が、端末装置 5 2 ごとに、それぞれの検知ルールが有効であるかあるいは無効であるかを表す情報を管理してもよい。本実施形態では、当該情報として、例えば、アラートルールの情報が用いられる。

[0071] 分析装置 4 1 において、誤検知制御部 1 1 5 は、記憶部 1 1 1 に記憶される検知ルールによるアラートの通知について、端末装置 5 2 ごとに、有効であるか無効であるかを特定する情報を記憶部 1 1 1 に記憶する。当該情報は、本実施形態では、アラートルールに含まれ、例えば、フラグの情報であってもよい。また、分析装置 4 1 において、誤検知制御部 1 1 5 は、一定期間無効であって停止させられているアラートの通知について、当該期間を特定する情報を記憶部 1 1 1 に記憶されたアラートルールに記憶する。

なお、本実施形態では、アラートの通知が無効である状態を「抑止」の状態とも呼んでいる。

[0072] 分析装置 4 1 において、誤検知制御部 1 1 5 は、記憶部 1 1 1 に記憶される情報に基づいて、一定期間無効であって停止させられるアラートの通知について、当該期間が経過したか否かを判定する。誤検知制御部 1 1 5 は、このような判定を、例えば、一定の時間間隔で行う。

そして、分析装置 4 1 において、誤検知制御部 1 1 5 は、無効の停止期間が経過したアラートの通知があると判定した場合には、当該アラートの通知を再び有効にして、適用が停止させられていた端末装置 5 2 に当該アラートの通知を再び適用する。

[0073] ここで、誤検知が指摘された検知ルールに対応するアラートの通知が再開されたときに適用される当該検知ルールとしては、例えば、アラートの通知が停止させられる前と同じ検知ルールが用いられる。

他の例として、誤検知が指摘された検知ルールに対応するアラートの通知

が再開されたときに適用される当該検知ルールとしては、アラートの通知が停止させられる前の検知ルールに対して改善されるように変更された検知ルールが用いられてもよい。このような検知ルールの変更は、例えば、分析装置 4 1 の側において、アナリストなどの人の思考に基づいて手動で行われてもよく、あるいは、機械学習 (Machine Learning) などの AI (Artificial Intelligence) を用いて行われてもよく、あるいは、あらかじめ定められた変更の規則に基づいて分析装置 4 1 において自動的に行われてもよい。例えば、誤検知制御部 1 1 5 は、端末装置 5 2 において「誤検知」が選択された場合に、その旨を所定の人へ通知してもよい。このような通知は、任意の手法によって行われてもよく、例えば、画面表示、音声出力、紙面に印刷、電子メールの送信などのうちの 1 以上の手法が用いられてもよい。

[0074] AI として機械学習が用いられる場合、例えば、ロジスティック回帰、ベイジアンフィルター、SVM (Support Vector Machine) と Deep Learning、などの技術が使用されてもよい。

分析装置 4 1 あるいは他の装置に、検知ルールの変更に関する処理を行う機能部 (本実施形態では、説明の便宜上、「ルール処理部」ともいう。) が備えられてもよい。

例えば、ルール処理部は、誤検知と判定された検知ルールと、アナリストによる当該検知ルールの変更結果と、が大量に取得されたデータに基づいて、当該データと顧客情報とを組み合わせ、AI で学習させた結果を取得する。そして、ルール処理部は、このような学習の結果を用いて、アナリストと同様な検知ルールの変更処理を自動的行ってもよい。

例えば、AI が変更した検知ルールをアナリストが確認してもよい。

例えば、ルール処理部は、AI によって、アナリストにより新たに作成または変更された検知ルールを確認してもよい。

[0075] なお、誤検知の一例として、分析装置 4 1 では検知ルールに基づいて端末装置 5 2 に対する攻撃を正しく検知しているが、当該攻撃が狙う対象のツー

ルが端末装置 5 2 などの顧客環境において使用されていない場合がある。つまり、顧客環境において使用されていないツールの脆弱性をつく攻撃が当該顧客環境にある端末装置 5 2 に来る場合がある。この場合、分析装置 4 1 では、例えば、発生したアラートについて、自動的に、「誤検知」の選択を確定させてもよい。ここで、顧客環境には、端末装置 5 2 が含まれるとともに、サーバ装置などのように、端末装置 5 2 以外の装置も含まれる。

または、分析装置 4 1 は、検知ルールに基づいて端末装置 5 2 に対する攻撃を正しく検知しているが、当該攻撃が狙う対象のツールが端末装置 5 2 などの顧客環境において使用されていない場合には、アラートの情報を端末装置 5 2 に通知するときに、「誤検知」の選択を推奨する旨、および「誤検知」の選択を推奨する理由を端末装置 5 2 に通知してもよい。この場合、端末装置 5 2 では、ユーザが、このような通知の内容を見て、「誤検知」を選択するか否かを決定する。

ここで、分析装置 4 1 において検知ルールに基づいて攻撃を正しく検知しているが、当該攻撃が狙う対象のツールが端末装置 5 2 などの顧客環境において使用されていない場合として、例えば、顧客環境において、SQL サーバが使用されていないときに、SQL インジェクションの攻撃がされて、ログ検出装置 5 1 から分析装置 4 1 に SQL インジェクションアラートが送られてきた場合がある。

[0076] <「対象外」の選択>

分析装置 4 1 では、端末装置 5 2 から受信された情報が「対象外」を示す場合には、誤検知制御部 1 1 5 が当該対象外に係るアラートを発生させる検知ルールによるアラートの通知を停止させる。

本実施形態では、分析装置 4 1 において、このようなアラートの通知の停止は、「対象外」が選択された端末装置 5 2 に対して行われ、他の端末装置に対しては行われない。つまり、同じ検知ルールであっても、当該検知ルールによるアラートの通知が対象外となる端末装置 5 2 について、当該アラートの通知が停止させられる。

分析装置 4 1 において、誤検知制御部 1 1 5 は、記憶部 1 1 1 に記憶される検知ルールについて、端末装置 5 2 ごとに、対象外であるか否かを特定する情報を記憶部 1 1 1 に記憶してもよい。当該情報としては、例えば、アラートルールの情報が用いられてもよい。

[0077] なお、分析装置 4 1 において検知ルールに基づいて攻撃を正しく検知しているが、当該攻撃が狙う対象のツールが端末装置 5 2 などの顧客環境において使用されていない場合、分析装置 4 1 では、例えば、発生したアラートについて、自動的に、「対象外」の選択を確定させてもよい。

または、分析装置 4 1 は、アラートの情報を端末装置 5 2 に通知するとき、「対象外」を推奨する旨、および「対象外」を推奨する理由を端末装置 5 2 に通知してもよい。この場合、端末装置 5 2 では、ユーザが、このような通知の内容を見て、「対象外」を選択するか否かを決定する。

[0078] また、分析装置 4 1 において検知ルールに基づいて攻撃を正しく検知しているが、当該攻撃が狙う対象のツールが端末装置 5 2 などの顧客環境において使用されていない場合に、端末装置 5 2 において、ユーザによって「誤検知」が選択されたときには、分析装置 4 1 では、例えば、発生したアラートについて、自動的に、「対象外」の選択を確定させてもよい。このような構成では、分析装置 4 1 では、管理部 1 1 6 が、端末装置 5 2 において当該ツールが使用されているか否かを特定する情報を記憶部 1 1 1 に記憶して管理する。そして、分析装置 4 1 では、アラートが発生した端末装置 5 2 について、ツールが使用されているか否かを特定する情報と、当該アラートを発生させた検知ルールとに基づいて、ユーザによる「誤検知」の指定を「対象外」に変更するか否かを判定し、所定の場合には、変更を行う。

なお、他の例として、あるアラートについて、端末装置 5 2 のユーザによって「誤検知」が指定されたが「対象外」に該当する可能性があるとして分析装置 4 1 またはアナリストなどの人によって判定（判断）された場合には、分析装置 4 1 によってユーザに対して「誤検知」を「対象外」に変更するか否かを確認した後に、当該ユーザの許可があったことに応じて変更を行う、構

成が用いられてもよい。

[0079] なお、本実施形態では、「誤検知」と「対象外」が設けられているが、例えば、「誤検知」と「対象外」とが、いずれも、検知ルールによるアラートの通知を停止させるものであってもよい。例えば、「誤検知」と「対象外」とでアラートの通知を停止させる期間が異なる点のみが異なってもよい。一例として、「誤検知」によるアラートの通知の停止期間が有限の値（例えば、１か月など）で、「対象外」によるアラートの通知の停止期間が永久的であってもよい。

[0080] ここで、本実施形態では、アラート詳細において、「抑止」の状況にあるログについてのアラートの情報も表示される場合を示したが、他の例として、「抑止」の状況にあるアラートの情報は表示されない態様が用いられてもよい。

[0081] 図５は、本発明の一実施形態に係るアラート検索の表示内容２２１１の一例を示す図である。

表示内容２２１１は、アラートの検索を行う画面の内容である。表示内容２２１１は、端末装置５２において、表示部２１４の画面に表示される。表示内容２２１１は、例えば、端末装置５２ごとに異なり得る。

[0082] 表示内容２２１１は、例えば、分析装置４１から端末装置５２に提供された情報に基づいている。

一例として、表示内容２２１１は、分析装置４１の側で生成されて、分析装置４１から端末装置５２に提供されてもよい。他の例として、表示内容２２１１は、分析装置４１から端末装置５２に提供された情報が記憶部２１６に記憶された後に、端末装置５２において記憶部２１６に記憶された情報に基づいて生成されてもよい。なお、表示内容２２１１は、他の情報を含んでもよい。

[0083] 図５の例では、検索の条件として、日時の範囲、重要度の範囲、センサの種類別、対応状況の範囲を選択することが可能である。

[0084] 日時の範囲は、開始時点と終了時点で特定される。開始時点および終了時

点は、それぞれ、例えば、年月日で指定される。図5の例では、「2018年4月1日～2018年5月1日」の範囲が指定されている。

重要度は、大きい方から小さい方へ向かって、大、中、小の3段階で指定される。複数の異なる重要度が指定されてもよい。

センサの種別は、個別のセンサの名称などを用いて指定される。複数の異なるセンサが指定されてもよい。

対応状況は、複数の項目のうちから指定される。2以上の異なる項目が指定されてもよい。図5の例では、対応状況として、「未対応」、「調査中」、「対応済」、「保留」、「対応中」、「誤検知」、「抑止」、「対象外」がある。

[0085] 端末装置52において、ユーザにより行われる操作部213の操作に応じて、アラート検索の画面において検索の条件が設定される。

表示内容2211には、検索のボタン2221も表示される。ユーザによって行われる操作部213の操作に基づいて、当該ボタン2221が押下されると、選択されている検索条件を特定する情報が、端末装置52から分析装置41に送信される。

本実施形態では、端末装置52では、検索制御部233がアラートの検索について全体的な制御を行う。

[0086] 分析装置41では、端末装置52から送信された検索条件を特定する情報を受信する。分析装置41において、管理部116は、検索処理部151によって、受信された情報によって特定される検索条件に基づいて、記憶部111に記憶されたアラートに関する情報を参照して、当該検索条件に合ったアラートを検索する。そして、管理部116は、検索処理部151によって検索の結果を示す情報を生成し、通知部114によって当該情報を端末装置52に通知する。本実施形態では、アラートの検索時に、管理部116は、検索処理部151によって、アラートルールの内容を参照して、「抑止」の状況あるいは「対象外」の状況などを判定してもよい。

[0087] [端末装置と分析装置との通信]

本実施形態では、ログ分析のサービスにおいて、端末装置 5 2 と分析装置 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 2 から発せられる要求に応じて、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。

[0088] [専用ツール]

本実施形態では、端末装置 5 2 において、専用のツール（説明の便宜上、「専用ツール」ともいう。）が用いられてもよい。つまり、端末装置 5 2 が備える機能の一部または全部が、専用ツールを用いて構成されてもよい。専用ツールは、例えば、プログラムなどのソフトウェアであってもよい。

例えば、端末装置 5 2 において、通知受信制御部 2 3 1、指示送信制御部 2 3 2、検索制御部 2 3 3 のうちの 1 以上の機能が、専用ツールの機能として構成されてもよい。専用ツールは、例えば、分析部 1 1 の管理主体などによって、有償または無償で、配布されてもよい。管理ツールは、例えば、端末装置 5 2 にインストールされて機能を発揮する。

[0089] [分析システムにおいて行われる処理]

図 6 は、本発明の一実施形態に係る端末装置 5 2 において行われる処理の手順の一例を示す図である。

図 6 の例では、端末装置 5 2 において、アラートの通知を受けた場合に、対応状況が選択される。

[0090] (ステップ S 1)

端末装置 5 2 において、通知受信制御部 2 3 1 は、分析装置 4 1 から送信されるアラートの通知を受信する。そして、ステップ S 2 の処理へ移行する。

[0091] (ステップ S 2)

端末装置 5 2 において、通知受信制御部 2 3 1 は、受信されたアラートの通知を表示する。本例では、端末装置 5 2 において、アラート一覧の表示内容 2 0 1 1 が表示された後に、ユーザの操作によって、アラート詳細の表示内容 2 1 1 1 が表示されたとする。そして、ステップ S 3 の処理へ移行する。

。

[0092] (ステップS3)

端末装置52において、指示送信制御部232は、ユーザによって対応状況を選択する操作があったか否かを判定する。図4の例では、当該操作は、対応状況が指定された状態での決定のボタン2131の押下である。

この結果、端末装置52において、指示送信制御部232は、ユーザによって対応状況を選択する操作があったと判定した場合には(ステップS3: YES)、ステップS4の処理へ移行する。

一方、端末装置52において、指示送信制御部232は、ユーザによって対応状況を選択する操作がなかったと判定した場合には(ステップS3: NO)、本フローの処理を終了する。

[0093] (ステップS4)

端末装置52において、指示送信制御部232は、ユーザによって行われた操作によって受け付けられた対応状況の選択の指示を特定する情報を分析装置41に送信する。そして、本フローの処理を終了する。

[0094] 図7は、本発明の一実施形態に係る分析装置41において行われる処理の手順の一例を示す図である。

図7の例では、分析装置41において、ログの分析を行う。

[0095] (ステップS21)

分析装置41において、取得部112が、受信部131によって、ログ検出装置51から送信されたログを受信して、取得する。本実施形態では、このようなログの受信は、常時行われる。そして、ステップS22の処理へ移行する。

[0096] (ステップS22)

分析装置41において、分析実行部113が、受信されたログについて、分析条件に基づいて分析を行う。分析実行部113は、例えば、所定の検知ルールに適合するログについて、問題があるログとして判定する。そして、ステップS23の処理へ移行する。

[0097] (ステップS 2 3)

分析装置 4 1 において、通知部 1 1 4 は、分析実行部 1 1 3 によって行われた分析の結果の情報を端末装置 5 2 に通知する。そして、本フローの処理を終了する。

なお、本実施形態では、アラートルールに基づいて、通知が必要なアラートは通知部 1 1 4 から端末装置 5 2 に通知され、通知が不要なアラートは通知部 1 1 4 から端末装置 5 2 に通知されない。

[0098] 図 8 は、本発明の一実施形態に係る分析装置 4 1 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、分析装置 4 1 において、「誤検知」の選択に関する処理を行う。なお、本実施形態では、「対象外」の選択に関する処理についても、「誤検知」の選択に関する処理と同様であってもよい。

[0099] (ステップS 4 1)

分析装置 4 1 において、管理部 1 1 6 が、端末装置 5 2 においてアラートについて「誤検知」が選択されたことの通知を受信する。そして、ステップ S 4 2 の処理へ移行する。

[0100] (ステップS 4 2)

分析装置 4 1 において、誤検知制御部 1 1 5 は、「誤検知」が選択された端末装置 5 2 である通知元について、「誤検知」が選択されたアラートを発生する検知ルールによるアラートの通知を停止させる。本例では、当該アラートの停止期間が設定されているとする。そして、ステップ S 4 3 の処理へ移行する。

本実施形態では、例えば、多数の端末装置 5 2 に共通な検知ルールのうち、「誤検知」が選択された端末装置 5 2 について当該検知ルールによるアラートの通知が停止させられる。

[0101] (ステップS 4 3)

分析装置 4 1 において、誤検知制御部 1 1 5 は、停止中のアラートの通知について、停止期間が経過したか否かを判定する。

この結果、分析装置４１において、誤検知制御部１１５は、停止中のアラートの通知について、停止期間が経過したことを判定した場合（ステップＳ４３：ＹＥＳ）、ステップＳ４４の処理へ移行する。

一方、分析装置４１において、誤検知制御部１１５は、停止中のアラートの通知について、停止期間が経過していないことを判定した場合（ステップＳ４３：ＮＯ）、ステップＳ４３の処理を繰り返して行う。

[0102] （ステップＳ４４）

分析装置４１において、誤検知制御部１１５は、停止中のアラートの通知について、停止期間が経過したことを判定した場合、該当する端末装置５２について当該アラートの通知を再開させる。そして、本フローの処理を終了する。

[0103] 図９は、本発明の一実施形態に係る分析装置４１において行われる処理の手順の一例を示す図である。

図９の例では、分析装置４１において、検知ルールの変更に関する処理を行う。

本実施形態では、分析装置４１において、アナリストなどによる指示に応じて、管理部１１６が記憶部１１１に記憶された検知ルールを変更し得る場合を示す。なお、他の例として、分析装置４１の記憶部１１１に記憶された検知ルールの変更が、分析装置４１とは別の装置からのアクセスによって行われる構成が用いられてもよい。

[0104] （ステップＳ６１）

分析装置４１において、管理部１１６が、端末装置５２から「誤検知」の選択の通知が受信されたアラートについて、該当する検知ルールの変更を行う指示を受け付けたか否かを判定する。本例では、当該指示は、例えば、アナリストなどの人によって分析装置４１に与えられる指示であってもよく、あるいは、分析装置４１などの装置によって自動的に与えられる指示であってもよい。

この結果、分析装置４１において、管理部１１６は、当該検知ルールの変

更を行う指示を受け付けたことを判定した場合（ステップS 6 1：YES）、ステップS 6 2の処理へ移行する。

一方、分析装置4 1において、管理部1 1 6は、当該検知ルールの変更を行う指示を受け付けていないと判定した場合（ステップS 6 1：NO）、本フローの処理を終了する。

[0105] （ステップS 6 2）

分析装置4 1において、管理部1 1 6は、受け付けられた指示にしたがって、該当する検知ルールを変更する。そして、本フローの処理を終了する。

[0106] ここで、本実施形態では、ある端末装置5 2において「誤検知」が指摘されたアラートを発生させる検知ルールが、当該端末装置5 2と他の端末装置を含む複数の端末装置について共通に変更されてもよい。当該複数の端末装置は、例えば、変更前の当該検知ルールが適用されたすべての端末装置であってもよく、一部の端末装置であってもよい。

なお、他の例として、ある端末装置5 2において「誤検知」が指摘されたアラートを発生させる検知ルールが、当該端末装置5 2のみについて変更されてもよい。

[0107] [アラートと検知ルールと状況]

本実施形態では、アラートと検知ルールとが1対1に対応しているとして説明した。そして、検知ルールとアラートとアラートルールとが、1対1対1で対応するとして説明した。この場合、アラートとアラートルールとの対応と、当該アラートと検知ルールとの対応に基づいて、当該検知ルールと通知の有効／無効の状況（アラートルールの内容）との対応が特定される。同様に、検知ルールとアラートルールとの対応と、当該検知ルールとアラートとの対応に基づいて、当該アラートと通知の有効／無効の状況（アラートルールの内容）との対応が特定される。本実施形態に係る分析システム1では、検知ルールとアラートとアラートルールとの対応が管理されることで、当該検知ルールに対応するアラートの通知の有効／無効の状況を管理している。

[0108] 他の例として、複数の異なる検知ルールと１つのアラートとが対応付けられてもよい。この場合、分析システム１では、アラートに対して選択された状況を管理するために、当該アラートと当該状況との対応を特定する情報を管理する。それぞれのアラートは、例えば、それぞれのアラートに付される識別情報に基づいて識別される。あるアラートについて「誤検知」が選択された場合には、例えば、そのときに当該アラートを発生させた検知ルールについてアラートの通知を「抑止」の状態とすることが行われてもよい。つまり、当該アラートを発生させる検知ルールは複数存在し得るが、例えば、そのなかで、そのときに当該アラートを発生させた１個の検知ルールを「抑止」の状態とすることが行われてもよい。なお、「対象外」についても、「誤検知」の場合と同様であってもよい。

[0109] [情報処理装置のハードウェア構成の一例]

図１０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５２あるいは分析装置４１などとして、図１０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。

[0110] 図１０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。

[0111] 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。

[0112] 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。

[0113] 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。

[0114] 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。

[0115] [実施形態のまとめ]

以上のように、本実施形態に係る分析システム 1 では、複数の異なる顧客の組織のうちの特定の組織に誤検知が発生した場合に、効率的に対処することが可能である。本実施形態に係る分析システム 1 では、端末装置 52 のユーザは、簡易な操作によって、誤検知が継続されることを抑止することができる。

例えば、検知ルール設計者は、ユーザから与えられる誤検知に関するフィードバックの情報を得ることができる。そして、検知ルール設計者は、例えば、検知ルールによるアラートの通知の抑止の期間中に、当該検知ルールの見直しを行うことができる。例えば、検知ルール設計者は、フィードバックされた情報に基づいて、手動で改善された検知ルールを生成してもよい。例えば、検知ルール設計者は、フィードバックされた情報を機械学習

器に機械学習させることで、改善された検知ルールを機械学習器によって生成してもよい。これにより、例えば、誤検知が削減される。

本実施形態に係る分析システム 1 では、それぞれの顧客ごとに、必ずしもカスタムルールが作成されなくてもよくなる。なお、本実施形態に係る分析システム 1 においても、それぞれの顧客ごとに、カスタムルールが作成されてもよい。

[0116] また、本実施形態に係る分析システム 1 では、抑止されたアラートを検索することができる。これにより、本実施形態に係る分析システム 1 では、無駄な通知を抑止することができた件数、頻度、傾向などを把握することが可能である。

例えば、抑止されたアラートの回数によって、無駄なアラートの通知を防ぐことができた回数を確認することができる。

例えば、抑止されたアラートが全くない場合、あるいは、1か月に1件以下などのように少ない場合には、当該アラートの発生の原因となる攻撃通信が減ったこと、あるいは検知ルールの改善などによって、「誤検知」のアラートが減ったことを確認することができる。

[0117] 本実施形態では、複数の顧客のそれぞれについて、顧客の装置のログを監視するシステムにおいて、次のような構成とする。

すなわち、システムでは、顧客のログを取得し、当該顧客のログが所定の条件を満たすか否かを判定する。システムでは、当該顧客のログが当該所定の条件を満たすと判定された場合に、当該顧客に対して所定の情報を送信する。当該所定の情報は、当該顧客から所定の指示を受け付けることが可能である。そして、システムでは、当該顧客から当該所定の指示が受け付けられた場合に、当該顧客について当該所定の情報の通知を無効（抑止の状況）にする。なお、システムとしては、分析システム 1 ばかりでなく、監視システムなどと呼ばれてもよい。

[0118] <構成例>

一構成例として、分析装置（本実施形態では、分析装置 4 1）において、

第1 端末装置（本実施形態では、端末装置 5 2）に関する対象情報（本実施形態では、ログ）を取得する取得部（本実施形態では、取得部 1 1 2 の機能）と、取得部によって取得された対象情報が第1 条件（本実施形態では、検知ルール）を満たすか否かを判定する分析実行部（本実施形態では、分析実行部 1 1 3 の機能）と、分析実行部によって対象情報が第1 条件を満たすことを判定した場合、第1 情報（本実施形態では、アラートの情報）を第1 端末装置に通知する通知部（本実施形態では、通知部 1 1 4 の機能）と、通知部によって通知された第1 情報に対して第1 端末装置から第2 情報（本実施形態では、「誤検知」の情報、あるいは、「対象外」の情報）を受け付ける情報受付部（本実施形態では、通知部 1 1 4 の機能）と、第1 情報に対して第1 端末装置から第2 情報が受け付けられた場合に、第1 端末装置に対する第1 情報の通知を抑制する通知抑制部（本実施形態では、誤検知制御部 1 1 5 の機能）と、を備える。

[0119] 一構成例として、分析装置において、第1 条件は、問題を検知するルールであり、第1 情報は、当該問題に対応するアラートの情報であり、第2 情報は、当該アラートについて誤りがあることを指示する情報である。

一構成例として、分析装置において、通知抑制部は、第1 端末装置について、第1 条件による第1 情報の通知を所定の期間停止させ、当該所定の期間が経過した後に第1 条件（本実施形態では、停止前と同じであってもよく、あるいは、変更されていてもよい。）による第1 情報の通知を再開させる。

一構成例として、分析装置において、第1 条件を変更する変更部（本実施形態では、管理部 1 1 6）を備える。

一構成例として、分析装置において、第1 条件による第1 情報の通知の状況を管理する管理部（本実施形態では、管理部 1 1 6）を備え、状況は、少なくとも、抑止されているという状況を含み、第1 情報は、通知の状況を用いて検索されることが可能である。

一構成例として、分析装置において、通知抑制部は、第1 端末装置に対する第1 情報の通知を抑制することを特定する第2 条件（本実施形態では、ア

ラートルール)に基づいて、第1端末装置に対する第1情報の通知を抑制する。

一構成例として、分析装置において、対象情報は、セキュリティに関するログである。

[0120] 一構成例として、端末装置（本実施形態では、端末装置52）において、当該端末装置に関する対象情報が分析装置によって第1条件を満たすことが判定された場合に分析装置から通知される第1情報の通知を受信する通知受信制御部（本実施形態では、通知受信制御部231の機能）と、通知受信制御部によって受信された第1情報に対して所定の指示（本実施形態では、「誤検知」の選択の指示、あるいは、「対象外」の選択の指示）を受け付ける指示受付部（本実施形態では、操作部213の機能および指示送信制御部232の機能）と、第1情報に対して当該指示が受け付けられた場合に、端末装置に対する第1情報の通知を抑制する指示を含む第2情報を分析装置に送信する指示送信制御部（本実施形態では、指示送信制御部232の機能）と、を備える。

[0121] なお、本発明は、端末装置あるいは分析装置などの装置、分析システムなどのシステム、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。

[0122] [ログの種類]

本実施形態では、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。

[0123] 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。

[0124] 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。

[0125] 本実施形態では、分析の対象としてログが用いられる場合を示したが、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。

[0126] 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52の外部に備えられてもよく、あるいは、端末装置52の内部の機能として備えられてもよい。

[0127] 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。

[0128] 分析装置41において、分析実行部113によるログの分析は、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。

[0129] 以上のように、実施形態に係る各装置（例えば、端末装置52、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。

[0130] 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

[0131] 1…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…分析装置

4 2…Web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 …端末装置

1 1 1、2 1 6 …記憶部

1 1 2 …取得部

1 1 3 …分析実行部

1 1 4 …通知部

1 1 5 …誤検知制御部

1 1 6 …管理部

1 3 1 …受信部

1 5 1 …検索処理部

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 5 …通信部

2 1 7 …制御部

2 3 1 …通知受信制御部

2 3 2 …指示送信制御部

2 3 3 …検索制御部

2 0 1 1、2 1 1 1、2 2 1 1 …表示内容

2 1 2 1 …属性領域

2 1 2 2 …対応状況領域

2 1 2 3 …内容領域

2 1 3 1、2 2 2 1 …ボタン

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

請求の範囲

[請求項1]

第1 端末装置に関する対象情報を取得する取得部と、
 前記取得部によって取得された前記対象情報が第1 条件を満たすか否かを判定する分析実行部と、
 前記分析実行部によって前記対象情報が前記第1 条件を満たすことを判定した場合、第1 情報を前記第1 端末装置に通知する通知部と、
 前記通知部によって通知された前記第1 情報に対して前記第1 端末装置から第2 情報を受け付ける情報受付部と、
 前記第1 情報に対して前記第1 端末装置から前記第2 情報が受け付けられた場合に、前記第1 端末装置に対する前記第1 情報の通知を抑制する通知抑制部と、
 を備え、
 前記通知抑制部は、前記第1 端末装置について、前記第1 条件による前記第1 情報の通知を所定の期間停止させ、前記所定の期間が経過した後に前記第1 条件による前記第1 情報の通知を再開させる、
 分析装置。

[請求項2]

第1 端末装置に関する対象情報を取得する取得部と、
 前記取得部によって取得された前記対象情報が第1 条件を満たすか否かを判定する分析実行部と、
 前記分析実行部によって前記対象情報が前記第1 条件を満たすことを判定した場合、第1 情報を前記第1 端末装置に通知する通知部と、
 前記通知部によって通知された前記第1 情報に対して前記第1 端末装置から第2 情報を受け付ける情報受付部と、
 前記第1 情報に対して前記第1 端末装置から前記第2 情報が受け付けられた場合に、前記第1 端末装置に対する前記第1 情報の通知を抑制する通知抑制部と、
 前記第1 条件による前記第1 情報の通知の状況を管理する管理部と、
 、

を備え、
 前記状況は、少なくとも、抑止されているという状況を含み、
 前記第 1 情報は、前記通知の状況を用いて検索されることが可能である、
 分析装置。

[請求項3]

第 1 端末装置に関する対象情報を取得する取得部と、
 前記取得部によって取得された前記対象情報が第 1 条件を満たすか否かを判定する分析実行部と、
 前記分析実行部によって前記対象情報が前記第 1 条件を満たすことを判定した場合、第 1 情報を前記第 1 端末装置に通知する通知部と、
 前記通知部によって通知された前記第 1 情報に対して前記第 1 端末装置から第 2 情報を受け付ける情報受付部と、
 前記第 1 情報に対して前記第 1 端末装置から前記第 2 情報が受け付けられた場合に、前記第 1 端末装置に対する前記第 1 情報の通知を抑制する通知抑制部と、
 を備え、
 前記通知抑制部は、前記第 1 端末装置に対する前記第 1 情報の通知を抑制することを特定する第 2 条件に基づいて、前記第 1 端末装置に対する前記第 1 情報の通知を抑制する、
 分析装置。

[請求項4]

第 1 端末装置に関する対象情報を取得する取得部と、
 前記取得部によって取得された前記対象情報が第 1 条件を満たすか否かを判定する分析実行部と、
 前記分析実行部によって前記対象情報が前記第 1 条件を満たすことを判定した場合、第 1 情報を前記第 1 端末装置に通知する通知部と、
 前記通知部によって通知された前記第 1 情報に対して前記第 1 端末装置から第 2 情報を受け付ける情報受付部と、
 前記第 1 情報に対して前記第 1 端末装置から前記第 2 情報が受け付

けられた場合に、前記第 1 端末装置に対する前記第 1 情報の通知を抑制する通知抑制部と、

を備え、

前記対象情報は、セキュリティに関するログである、

分析装置。

[請求項5]

前記第 1 条件は、問題を検知するルールであり、

前記第 1 情報は、前記問題に対応するアラートの情報であり、

前記第 2 情報は、前記アラートについて誤りがあることを指示する情報である、

請求項 1 から請求項 4 のいずれか 1 項に記載の分析装置。

[請求項6]

前記第 1 条件を変更する変更部を備える、

請求項 1 から請求項 5 のいずれか 1 項に記載の分析装置。

[請求項7]

セキュリティに関するログを対象情報とし端末装置に関する前記対象情報を検出して前記対象情報を分析装置に送信する検出装置を有する前記端末装置に関する前記対象情報が前記分析装置によって第 1 条件を満たすことが判定された場合に前記分析装置から通知される前記セキュリティに関する第 1 情報の通知を受信する通知受信制御部と、

前記通知受信制御部によって受信された前記第 1 情報に対して前記セキュリティに関する所定の指示を受け付ける指示受付部と、

前記第 1 情報に対して前記指示が受け付けられた場合に、前記端末装置に対する前記セキュリティに関する前記第 1 情報の通知を抑制する指示を含む第 2 情報を前記分析装置に送信する指示送信制御部と、

を備える前記端末装置。

[請求項8]

前記第 1 条件は、問題を検知するルールであり、

前記第 1 情報は、前記問題に対応するアラートの情報であり、

前記第 2 情報は、前記アラートについて誤りがあることを指示する情報である、

請求項 7 に記載の端末装置。

[請求項9]

第1端末装置と、分析装置と、を備える分析システムであって、
 前記分析装置は、前記第1端末装置に関する対象情報を取得する取得部と、
 前記取得部によって取得された前記対象情報が第1条件を満たすか否かを判定する分析実行部と、
 前記分析実行部によって前記対象情報が前記第1条件を満たすことを判定した場合、第1情報を前記第1端末装置に通知する通知部と、
 前記通知部によって通知された前記第1情報に対して前記第1端末装置から第2情報を受け付ける情報受付部と、
 前記第1情報に対して前記第1端末装置から前記第2情報が受け付けられた場合に、前記第1端末装置に対する前記第1情報の通知を抑制する通知抑制部と、
 を備え、
 前記第1端末装置は、前記分析装置から通知される前記第1情報の通知を受信する通知受信制御部と、
 前記通知受信制御部によって受信された前記第1情報に対して所定の指示を受け付ける指示受付部と、
 前記第1情報に対して前記指示が受け付けられた場合に、前記第2情報を前記分析装置に送信する指示送信制御部と、
 を備え、
 前記通知抑制部は、前記第1端末装置について、前記第1条件による前記第1情報の通知を所定の期間停止させ、前記所定の期間が経過した後に前記第1条件による前記第1情報の通知を再開させる、
 分析システム。

[請求項10]

第1端末装置と、分析装置と、を備える分析システムであって、
 前記分析装置は、前記第1端末装置に関する対象情報を取得する取得部と、
 前記取得部によって取得された前記対象情報が第1条件を満たすか

否かを判定する分析実行部と、

前記分析実行部によって前記対象情報が前記第 1 条件を満たすことを判定した場合、第 1 情報を前記第 1 端末装置に通知する通知部と、

前記通知部によって通知された前記第 1 情報に対して前記第 1 端末装置から第 2 情報を受け付ける情報受付部と、

前記第 1 情報に対して前記第 1 端末装置から前記第 2 情報が受け付けられた場合に、前記第 1 端末装置に対する前記第 1 情報の通知を抑制する通知抑制部と、

前記第 1 条件による前記第 1 情報の通知の状況を管理する管理部と、

を備え、

前記第 1 端末装置は、前記分析装置から通知される前記第 1 情報の通知を受信する通知受信制御部と、

前記通知受信制御部によって受信された前記第 1 情報に対して所定の指示を受け付ける指示受付部と、

前記第 1 情報に対して前記指示が受け付けられた場合に、前記第 2 情報を前記分析装置に送信する指示送信制御部と、

を備え、

前記状況は、少なくとも、抑止されているという状況を含み、

前記第 1 情報は、前記通知の状況を用いて検索されることが可能である、

分析システム。

[請求項11]

第 1 端末装置と、分析装置と、を備える分析システムであって、

前記分析装置は、前記第 1 端末装置に関する対象情報を取得する取得部と、

前記取得部によって取得された前記対象情報が第 1 条件を満たすか否かを判定する分析実行部と、

前記分析実行部によって前記対象情報が前記第 1 条件を満たすこと

を判定した場合、第 1 情報を前記第 1 端末装置に通知する通知部と、
前記通知部によって通知された前記第 1 情報に対して前記第 1 端末装置から第 2 情報を受け付ける情報受付部と、

前記第 1 情報に対して前記第 1 端末装置から前記第 2 情報が受け付けられた場合に、前記第 1 端末装置に対する前記第 1 情報の通知を抑制する通知抑制部と、

を備え、

前記第 1 端末装置は、前記分析装置から通知される前記第 1 情報の通知を受信する通知受信制御部と、

前記通知受信制御部によって受信された前記第 1 情報に対して所定の指示を受け付ける指示受付部と、

前記第 1 情報に対して前記指示が受け付けられた場合に、前記第 2 情報を前記分析装置に送信する指示送信制御部と、

を備え、

前記通知抑制部は、前記第 1 端末装置に対する前記第 1 情報の通知を抑制することを特定する第 2 条件に基づいて、前記第 1 端末装置に対する前記第 1 情報の通知を抑制する、

分析システム。

[請求項12]

第 1 端末装置と、分析装置と、を備える分析システムであって、

前記分析装置は、前記第 1 端末装置に関する対象情報を取得する取得部と、

前記取得部によって取得された前記対象情報が第 1 条件を満たすか否かを判定する分析実行部と、

前記分析実行部によって前記対象情報が前記第 1 条件を満たすことを判定した場合、第 1 情報を前記第 1 端末装置に通知する通知部と、

前記通知部によって通知された前記第 1 情報に対して前記第 1 端末装置から第 2 情報を受け付ける情報受付部と、

前記第 1 情報に対して前記第 1 端末装置から前記第 2 情報が受け付

けられた場合に、前記第 1 端末装置に対する前記第 1 情報の通知を抑制する通知抑制部と、

を備え、

前記第 1 端末装置は、前記分析装置から通知される前記第 1 情報の通知を受信する通知受信制御部と、

前記通知受信制御部によって受信された前記第 1 情報に対して所定の指示を受け付ける指示受付部と、

前記第 1 情報に対して前記指示が受け付けられた場合に、前記第 2 情報を前記分析装置に送信する指示送信制御部と、

を備え、

前記対象情報は、セキュリティに関するログである、
分析システム。

[請求項13]

前記第 1 条件は、問題を検知するルールであり、

前記第 1 情報は、前記問題に対応するアラートの情報であり、

前記第 2 情報は、前記アラートについて誤りがあることを指示する情報である、

請求項 9 から請求項 12 のいずれか 1 項に記載の分析システム。

[請求項14]

前記分析装置は、前記第 1 条件を変更する変更部を備える、

請求項 9 から請求項 13 のいずれか 1 項に記載の分析システム。

[請求項15]

第 1 端末装置と、分析装置と、を備える分析システムにおける分析方法であって、

前記分析装置は、前記第 1 端末装置に関する対象情報を取得し、取得された前記対象情報が第 1 条件を満たすか否かを判定し、前記対象情報が前記第 1 条件を満たすことを判定した場合、第 1 情報を前記第 1 端末装置に通知し、

前記第 1 端末装置は、前記分析装置から通知される前記第 1 情報の通知を受信し、受信された前記第 1 情報に対して所定の指示が受け付けられた場合に、第 2 情報を前記分析装置に送信し、

前記分析装置は、前記第 1 端末装置から第 2 情報が受け付けられた場合に、前記第 1 端末装置に対する前記第 1 情報の通知を抑制し、

前記分析装置は、前記通知の抑制として、前記第 1 端末装置について、前記第 1 条件による前記第 1 情報の通知を所定の期間停止させ、前記所定の期間が経過した後に前記第 1 条件による前記第 1 情報の通知を再開させる、

分析方法。

[請求項16]

第 1 端末装置と、分析装置と、を備える分析システムにおける分析方法であって、

前記分析装置は、前記第 1 端末装置に関する対象情報を取得し、取得された前記対象情報が第 1 条件を満たすか否かを判定し、前記対象情報が前記第 1 条件を満たすことを判定した場合、第 1 情報を前記第 1 端末装置に通知し、

前記第 1 端末装置は、前記分析装置から通知される前記第 1 情報の通知を受信し、受信された前記第 1 情報に対して所定の指示が受け付けられた場合に、第 2 情報を前記分析装置に送信し、

前記分析装置は、前記第 1 端末装置から第 2 情報が受け付けられた場合に、前記第 1 端末装置に対する前記第 1 情報の通知を抑制し、

前記分析装置は、前記第 1 条件による前記第 1 情報の通知の状況を管理し、

前記状況は、少なくとも、抑止されているという状況を含み、

前記第 1 情報は、前記通知の状況を用いて検索されることが可能である、

分析方法。

[請求項17]

第 1 端末装置と、分析装置と、を備える分析システムにおける分析方法であって、

前記分析装置は、前記第 1 端末装置に関する対象情報を取得し、取得された前記対象情報が第 1 条件を満たすか否かを判定し、前記対象

情報が前記第 1 条件を満たすことを判定した場合、第 1 情報を前記第 1 端末装置に通知し、

前記第 1 端末装置は、前記分析装置から通知される前記第 1 情報の通知を受信し、受信された前記第 1 情報に対して所定の指示が受け付けられた場合に、第 2 情報を前記分析装置に送信し、

前記分析装置は、前記第 1 端末装置から第 2 情報が受け付けられた場合に、前記第 1 端末装置に対する前記第 1 情報の通知を抑制し、

前記分析装置は、前記通知の抑制として、前記第 1 端末装置に対する前記第 1 情報の通知を抑制することを特定する第 2 条件に基づいて、前記第 1 端末装置に対する前記第 1 情報の通知を抑制する、

分析方法。

[請求項18]

第 1 端末装置と、分析装置と、を備える分析システムにおける分析方法であって、

前記分析装置は、前記第 1 端末装置に関する対象情報を取得し、取得された前記対象情報が第 1 条件を満たすか否かを判定し、前記対象情報が前記第 1 条件を満たすことを判定した場合、第 1 情報を前記第 1 端末装置に通知し、

前記第 1 端末装置は、前記分析装置から通知される前記第 1 情報の通知を受信し、受信された前記第 1 情報に対して所定の指示が受け付けられた場合に、第 2 情報を前記分析装置に送信し、

前記分析装置は、前記第 1 端末装置から第 2 情報が受け付けられた場合に、前記第 1 端末装置に対する前記第 1 情報の通知を抑制し、

前記対象情報は、セキュリティに関するログである、
分析方法。

[請求項19]

前記第 1 条件は、問題を検知するルールであり、

前記第 1 情報は、前記問題に対応するアラートの情報であり、

前記第 2 情報は、前記アラートについて誤りがあることを指示する情報である、

- 請求項 15 から請求項 18 のいずれか 1 項に記載の分析方法。
- [請求項20] 前記分析装置は、前記第 1 条件を変更する、
請求項 15 から請求項 19 のいずれか 1 項に記載の分析方法。
- [請求項21] 分析装置を構成するコンピュータに、
第 1 端末装置に関する対象情報を取得する機能と、
取得された前記対象情報が第 1 条件を満たすか否かを判定する機能と、
前記対象情報が前記第 1 条件を満たすことを判定した場合、第 1 情報を前記第 1 端末装置に通知する機能と、
通知された前記第 1 情報に対して前記第 1 端末装置から第 2 情報を受け付ける機能と、 前記第 1 情報に対して前記第 1 端末装置から前記第 2 情報が受け付けられた場合に、前記第 1 端末装置に対する前記第 1 情報の通知を抑制する機能と、
を実現させるためのプログラムであって、
前記通知を抑制する機能は、前記第 1 端末装置について、前記第 1 条件による前記第 1 情報の通知を所定の期間停止させ、前記所定の期間が経過した後に前記第 1 条件による前記第 1 情報の通知を再開させる、
プログラム。
- [請求項22] 分析装置を構成するコンピュータに、
第 1 端末装置に関する対象情報を取得する機能と、
取得された前記対象情報が第 1 条件を満たすか否かを判定する機能と、
前記対象情報が前記第 1 条件を満たすことを判定した場合、第 1 情報を前記第 1 端末装置に通知する機能と、
通知された前記第 1 情報に対して前記第 1 端末装置から第 2 情報を受け付ける機能と、 前記第 1 情報に対して前記第 1 端末装置から前記第 2 情報が受け付けられた場合に、前記第 1 端末装置に対する前記

第 1 情報の通知を抑制する機能と、

前記第 1 条件による前記第 1 情報の通知の状況を管理する機能と、
を実現させるためのプログラムであって、

前記状況は、少なくとも、抑止されているという状況を含み、

前記第 1 情報は、前記通知の状況を用いて検索されることが可能である、

プログラム。

[請求項23]

分析装置を構成するコンピュータに、

第 1 端末装置に関する対象情報を取得する機能と、

取得された前記対象情報が第 1 条件を満たすか否かを判定する機能と、

前記対象情報が前記第 1 条件を満たすことを判定した場合、第 1 情報を前記第 1 端末装置に通知する機能と、

通知された前記第 1 情報に対して前記第 1 端末装置から第 2 情報を受け付ける機能と、 前記第 1 情報に対して前記第 1 端末装置から前記第 2 情報が受け付けられた場合に、前記第 1 端末装置に対する前記第 1 情報の通知を抑制する機能と、

を実現させるためのプログラムであって、

前記通知を抑制する機能は、前記第 1 端末装置に対する前記第 1 情報の通知を抑制することを特定する第 2 条件に基づいて、前記第 1 端末装置に対する前記第 1 情報の通知を抑制する、

プログラム。

[請求項24]

分析装置を構成するコンピュータに、

第 1 端末装置に関する対象情報を取得する機能と、

取得された前記対象情報が第 1 条件を満たすか否かを判定する機能と、

前記対象情報が前記第 1 条件を満たすことを判定した場合、第 1 情報を前記第 1 端末装置に通知する機能と、

通知された前記第 1 情報に対して前記第 1 端末装置から第 2 情報を受け付ける機能と、
前記第 1 情報に対して前記第 1 端末装置から前記第 2 情報が受け付けられた場合に、前記第 1 端末装置に対する前記第 1 情報の通知を抑制する機能と、

を実現させるためのプログラムであって、
前記対象情報は、セキュリティに関するログである、
プログラム。

[請求項25] 前記第 1 条件は、問題を検知するルールであり、
前記第 1 情報は、前記問題に対応するアラートの情報であり、
前記第 2 情報は、前記アラートについて誤りがあることを指示する情報である、

請求項 2 1 から請求項 2 4 のいずれか 1 項に記載のプログラム。

[請求項26] さらに、前記第 1 条件を変更する機能を実現させるためのプログラムである、

請求項 2 1 から請求項 2 5 のいずれか 1 項に記載のプログラム。

[請求項27] セキュリティに関するログを対象情報とし端末装置に関する前記対象情報を検出して前記対象情報を分析装置に送信する検出装置を有する前記端末装置を構成するコンピュータに、

前記端末装置に関する前記対象情報が前記分析装置によって第 1 条件を満たすことが判定された場合に前記分析装置から通知される前記セキュリティに関する第 1 情報の通知を受信する機能と、

受信された前記第 1 情報に対して前記セキュリティに関する所定の指示を受け付ける機能と、

前記第 1 情報に対して前記指示が受け付けられた場合に、前記端末装置に対する前記セキュリティに関する前記第 1 情報の通知を抑制する指示を含む第 2 情報を前記分析装置に送信する機能と、

を実現させるためのプログラム。

[請求項28] 前記第 1 条件は、問題を検知するルールであり、

前記第 1 情報は、前記問題に対応するアラートの情報であり、
前記第 2 情報は、前記アラートについて誤りがあることを指示する
情報である、
請求項 27 に記載のプログラム。