明　細　書

発明の名称 ： ログ分析システム

技術分野

[0001] 本発明は、対象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に関する。

本願は、２０１４年３月３１日に、日本に出願された特願２０１４－０７４６０７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] インターネット等の情報通信ネットワーク（以下、単にネットワークと記す）を利用して、様々な情報システムにおいて大量のデータの通信や処理が行われている。一方、ネットワーク上で稼働しているサーバや各種の端末装置等の機器に対する不正なアクセスやサーバ等からの不正な情報流出等の問題が生じ得る。

[0003] 例えば、データ通信に関しては、不正な通信による被害を抑えるために、通信ログを後で検査するのではなく、通信をリアルタイムで監視することが望ましい。そのような従来技術として、例えば、特許文献１は、各種監視装置からのセキュリティ・イベントを収集し、記憶し、記憶されたセキュリティ・イベントのサブセットを、イベント・ストリームとしてマネージャに供給し、イベント・ストリームにおける１以上の未知のイベント・パターンをマネージャによって発見する技術を開示している。

[0004] また従来、ネットワーク上のサーバにおける通信を監視して、不正なアクセスやデータの送受信を検出し、対応処理することが行われている。複数のサーバを監視対象として、その通信をセンターで監視することも行われている。

先行技術文献

特許文献

[0005] 特許文献1：特表２００７－５３６６４６号公報

発明の概要

発明が解決しようとする課題

[0006] 上記のネットワーク上の情報通信の監視等のように、大量のログを分析して特定の性質を有する処理（例えば問題のある通信）を抽出する情報処理では、通常、分析対象として取得されるログのデータ量は膨大である。その一方で、抽出すべき特定の性質を有する処理またはその可能性のある処理に関するログはごくわずかに過ぎない。そのため、分析対象のログを適切に絞り込んで効率良く分析するためには、システム内における処理対象のデータの伝達を高速に行うことが望ましい。

[0007] 本発明の目的は、ログの分析において、処理対象のデータを、信頼度を落とすことなく高速に伝達する手段を提供することにある。

課題を解決するための手段

[0008] 上記の目的を達成するため、本発明の実施態様に係るログ分析システムは、監視対象システムにおいて検知される検知ログを分析する。このログ分析システムは、監視対象システムにおいて行われる検知対象処理を検知し、この検知対象処理の検知ログを取得する取得装置と、この取得装置により取得された検知ログを処理する処理装置と、を備える。そして、処理装置は、検知ログに対する処理を順次行う複数の処理ブロックを含み、先頭の処理ブロックから順に後段の処理ブロックへ検知ログを送りながら処理を行う。処理装置の最後の処理ブロックは、検知ログを受け取ったことを、処理装置の最初の処理ブロックに通知する。処理装置の最初の処理ブロックは、処理を行った検知ログのうち、処理装置の最後の処理ブロックからの通知において最後の処理ブロックに到達したことが確認できない検知ログを、後段の処理ブロックへ再送する。

[0009] 上記のログ分析システムにおいて、処理装置の最初の処理ブロックは、一つの検知ログについて予め定められた回数送信を繰り返した後に、処理装置の最後の処理ブロックからの通知において検知ログが最後の処理ブロックに到達したことが確認できない場合、検知ログの送信を停止してもよい。

上記のログ分析システムにおいて、処理装置の最初の処理ブロックは、検知ログに対して再送される検知ログか否かを識別可能な情報を付加して、この検知ログを後段の処理ブロックに送ってもよい。

上記のログ分析システムにおいて、処理装置の最初の処理ブロックは、検知ログに対して何回目の伝達かを示す情報を付加して、この検知ログを後段の処理ブロックに送ってもよい。

[0010] 本発明の実施態様は、コンピュータを制御して上述した装置の各機能を実現するプログラムとして実現されてもよい。このプログラムは、磁気ディスクや光ディスク、半導体メモリ、その他の記録媒体に格納して配布したり、ネットワークを介して配信したりすることにより、提供してもよい。

発明の効果

[0011] 本発明によれば、ログの分析において、処理対象のデータを、信頼度を落とすことなく高速に伝達することが可能となる。

図面の簡単な説明

[0012] [図1]本実施形態のセキュリティ監視システムの構成例を示す図である。

[図2]図１に示す監視サブシステムを構成する収集ユニットの機能構成例を示す図である。

[図3]コンポーネント化された処理単位ブロックにより構成される図２に示す収集ユニットの構成例を示す図である。

[図4]図１に示す監視サブシステムを構成する検出ユニットの機能構成例を示す図である。

[図5]コンポーネント化された処理単位ブロックにより構成される図４に示す検出ユニットの構成例を示す図である。

[図6]図１に示す監視サブシステムを構成する分析ユニットの機能構成例を示す図である。

[図7]本実施形態における相関分析の概念を示す図である。

[図8A]本実施形態における増分分析の概念を示す図であって、ある分析時における相関分析の対象となった検出事象候補の構成例を示す図である。

[図8B]本実施形態における増分分析の概念を示す図であって、次の分析時における同じ検出事象候補の構成例を示す図である。

[図9]コンポーネント化された処理単位ブロックを含む個別分析処理部、イベント集積処理部、相関分析処理部および増分分析処理部により構成される図６に示す分析ユニットの構成例を示す図である。

[図10]図１に示す監視サブシステムの手動分析ユニットの機能構成例を示す図である。

[図11]本実施形態における通信ログファイルの伝達方式を説明する図である。

[図12]本実施形態による通信ログファイルの伝達の一例を示す図である。

[図13]本実施形態による通信ログファイルの伝達の他の例を示す図である。

[図14]本実施形態による通信ログファイルの伝達のさらに他の例を示す図である。

[図15]図１に示す端末装置の機能構成例を示す図である。

[図16]本実施形態における分析用画面の構成例を示す図である。

[図17]本実施形態の監視サブシステムの各サーバや端末装置を構成するのに好適なハードウェア構成例を示す図である。

発明を実施するための形態

[0013] 以下、添付図面を参照して、本発明の実施形態について詳細に説明する。

以下では、検査対象のシステムから検知対象処理のログ（検知ログ）を取得して分析する本実施形態のログ分析システムを、検知対象処理としてネットワーク上の通信を監視し、検知ログとして通信ログを取得し分析するセキュリティ監視システムに適用した場合を例として説明する。ネットワークに接続されたサーバ等の情報処理装置では、ネットワークを介して様々な通信が行われる。本実施形態のセキュリティ監視システム（ＳＯＣ（Security Operation Center）システム）は、監視対象装置である情報処理装置の通信を監視し、抽出すべき特定の性質を有する検知対象処理の一例として、外部からの不正なアクセスや内部からの不正な情報流出等のような問題のある通信

を抽出する。

[0014] ＜システム構成例＞

図１は、本実施形態のセキュリティ監視システムの構成例を示す図である。

図１に示すように、本実施形態によるセキュリティ監視システムは、監視対象装置１００における通信を監視して通信ログを取得する取得装置としての検知デバイス１１０、ログ取得エージェント１２１およびログ管理サブシステム１２０を備える。また、本実施形態によるセキュリティ監視システムは、取得された通信ログを処理して問題のある通信を抽出する処理装置としての監視サブシステム２００を備える。さらに、本実施形態によるセキュリティ監視システムは、監視サブシステム２００による処理の結果を出力する出力装置としての端末装置３００を備える。図１に示す構成において、監視対象装置１００に搭載される検知デバイス１１０およびログ取得エージェント１２１と、ログ管理サブシステム１２０、監視サブシステム２００および端末装置３００とを区別するために、監視対象装置１００に搭載される構成要素を対象側システムと呼び、ログ管理サブシステム１２０、監視サブシステム２００および端末装置３００をセンター側システムと呼ぶ場合がある。なお、図１において、監視対象装置１００は１台のみが例示されているが、実際のシステムにおいては、複数の監視対象装置１００における通信を監視対象とする。

[0015] 監視対象装置１００は、本実施形態によるセキュリティ監視システムの監視対象であり、検知デバイス１１０およびログ管理サブシステム１２０により取得されるログを生成する装置である。監視対象装置１００は、具体的には、ＩＤＳ（Intrusion Detection System）やＩＰＳ（Intrusion Prevention System）等のセキュリティ・システム、ファイア・ウォールやウィルス対策ソフト等のソフトウェア等が搭載されて動作しているサーバ等である。

なお、本実施形態では、セキュリティ監視システムとしてのログ分析システムが、ネットワーク通信を監視対象として通信ログを取得する例について

説明する。しかしながら、本実施形態の適用例はこれに限定されない。通信以外の種々の処理において生成される様々なログを取得し検査するために本実施形態のログ分析システムを適用することも可能である。

[0016] 検知デバイス１１０は、センサ１１１と、センサ・マネージャ１１２とで構成される。センサ１１１は、本実施形態によるセキュリティ監視システムの監視対象単位である。センサ１１１は、例えば監視対象装置１００における通信の検知機能を用いて実現され、通信に関するデータをリアルタイムで取得する。センサ・マネージャ１１２は、例えば監視対象装置１００の機能を用いて実現され、センサ１１１を管理する。すなわち、センサ１１１およびセンサ・マネージャ１１２は、上述した、ＩＤＳ／ＩＰＳ、ファイア・ウォール、ウィルス対策ソフト等の種々のセキュリティ・システムの機能として、ソフトウェアやソフトウェアとハードウェアとの組み合わせ等の様々な形態で提供される。実際のシステムにおいては、監視対象として設定された監視対象装置１００の仕様や用途、使用環境などに応じて、様々な種類のセンサ１１１およびセンサ・マネージャ１１２が使用される。

[0017] ログ取得エージェント１２１は、センサ・マネージャ１１２の管理下でセンサ１１１により取得された通信に関するデータを、通信ログとして、リアルタイムでログ管理サブシステム１２０へ送信する。本実施形態では、このログ取得エージェント１２１によりログ管理サブシステム１２０に送られる通信ログを「生ログ」と呼ぶ。ログ取得エージェント１２１は、例えば、コンピュータ・プログラムとして提供され、このログ取得エージェント１２１が監視対象装置１００にインストールされて実行されることにより、生ログをログ管理サブシステム１２０へ送信する機能が実現される。生ログを取得するセンサ１１１およびセンサ・マネージャ１１２として、上述したように様々な種類のものが用いられ得る。そのため、生ログに含まれる情報の内容や形式は、生ログを取得したセンサ１１１およびセンサ・マネージャ１１２の種類に応じて異なる場合がある。

なお、図１に示す構成例では、ログ取得エージェント１２１を対象側シス

テムとして監視対象装置１００に搭載する構成を採用している。しかしながら本実施形態はこのような構成に限定されない。ログ取得エージェント１２１を監視対象装置１００に搭載せずにセンター側システムとして構成しても良い。この場合、ネットワークを介して監視対象装置１００に接続された独立のサーバ等としてログ取得エージェント１２１を構成しても良いし、ログ管理サブシステム１２０の機能の一つとしてログ取得エージェント１２１を実現しても良い。

[0018] ログ管理サブシステム１２０は、ログ取得エージェント１２１から生ログを取得する。したがって、ログ管理サブシステム１２０においては、ログ取得エージェント１２１ごとの生ログが取得される。また、ログ管理サブシステム１２０は、取得した生ログをセンサ１１１ごとの通信ログファイルに分割し、リアルタイムで監視サブシステム２００へ送信する。ログ管理サブシステム１２０は、例えば、コンピュータにより実現される。すなわち、コンピュータの記憶装置に格納されたプログラムをＣＰＵが実行することにより、ログ取得エージェント１２１から取得した生ログを通信ログファイルに分割して監視サブシステム２００へ送信する上記の機能が実現される。

[0019] 監視サブシステム２００は、ログ管理サブシステム１２０から取得した通信ログファイルに対する処理を行う処理ユニットとして、収集ユニット２１０と、検出ユニット２２０と、分析ユニット２３０と、手動分析ユニット２４０とを備える。この監視サブシステム２００は、ログ管理サブシステム１２０から取得した通信ログファイルをこれらの処理ユニット２１０、２２０、２３０、２４０により順次処理し、問題のある通信を抽出する。言い換えると、監視サブシステム２００は、通信ログファイルに示される監視対象装置１００で行われた通信を、問題のある通信と問題のない通信とに仕分ける。

[0020] 監視サブシステム２００における処理ユニット２１０、２２０、２３０、２４０は、各々、複数のサーバ（ハードウェア）により実現することが可能であり、複数のサーバが互いに並列かつ非同期に処理を実行することができ

る。そこで、本実施形態において、監視サブシステム２００における処理ユニット２１０、２２０、２３０、２４０間の通信ログファイルの伝達には、例えばＪＭＳ（Java Message Service）等に基づく非同期通信が用いられる。監視サブシステム２００は、例えば、コンピュータにより実現される。すなわち、コンピュータの記憶装置に格納されたプログラムをＣＰＵが実行することにより、各処理ユニット２１０、２２０、２３０、２４０の機能が実現される。各処理ユニット２１０、２２０、２３０、２４０およびユニット間における通信の詳細については後述する。

[0021] 端末装置３００は、監視サブシステム２００による処理結果を出力する装置である。端末装置３００は、監視対象装置１００における通信を解析する解析者（アナリスト）が使用する装置である。監視サブシステム２００による処理の結果として、監視対象装置１００における通信は、問題のある通信と問題のない通信とに仕分けられる。ここで、問題のある通信には、不正な通信であることが明らかな通信と、不正な通信である可能性のある通信（問題のない通信と特定できない通信）とが含まれる。端末装置３００の使用者である解析者は、端末装置３００に出力された監視サブシステム２００の処理結果に基づき、この不正な通信である可能性のある通信を解析して、不正な通信か否かを判断することができる。

[0022] 端末装置３００は、例えば、コンピュータにより実現される。すなわち、コンピュータの記憶装置に格納されたプログラムをＣＰＵが実行することにより、端末装置３００の各機能が実現される。端末装置３００の具体的な機能と、端末装置３００において出力される情報の内容および出力形式の詳細については後述する。

[0023] ＜収集ユニットの機能＞

図２は、監視サブシステム２００を構成する収集ユニット２１０の機能構成例を示す図である。

第１処理ユニットである収集ユニット２１０は、ログ管理サブシステム１２０から取得した通信ログファイルに対して、その通信ログファイルの元の

通信ログ（生ログ）を取得した検知デバイス１１０の種類ごとに設定された処理を行う。ここで、検知デバイス１１０の種類とは、検知デバイス１１０のセンサ１１１およびセンサ・マネージャ１１２の機能を提供するＩＤＳ／ＩＰＳ、ファイア・ウォール、ウィルス対策ソフト等の製品の種別を意味する。なお、検知デバイス１１０の種類を特定する情報（ＩＤ、製品名等）は、例えば、通信ログファイルに含まれている。

[0024] 図２に示すように、本実施形態の収集ユニット２１０は、取得した通信ログファイルに対する処理として、分析対象ログの抽出処理、通信ログの正規化処理、通信ログの振り分け処理、フィルタリング処理を行う。

[0025] 収集ユニット２１０は、分析対象ログの抽出処理では、ログ管理サブシステム１２０から取得した通信ログファイルに含まれる通信ログのうち、監視サブシステム２００による処理（分析）の対象となる通信ログを抽出する。ログ管理サブシステム１２０から取得した通信ログファイル（生ログ）には、検知デバイス１１０のセンサ１１１が起動した／停止したといった動作のログ等（分析に不要なログ）も含まれている。そこで、収集ユニット２１０は、予め設定された監視サブシステム２００の処理対象（分析対象）となる情報のみを抽出し、他の情報を除去する。

[0026] 収集ユニット２１０は、通信ログの正規化処理では、抽出された分析対象の通信ログを予め定められた規則に基づいて正規化する。具体的には、収集ユニット２１０は、通信ログにおける日時、プロトコル番号、送信元ＩＰアドレス（Internet Protocol Address）、送信元ポート、宛先ＩＰアドレス、宛先ポート等の情報を、共通の形式に整える。例えば、収集ユニット２１０は、日時を記述する基準（西暦か和暦か等）および書式を統一したり、ＩＰアドレスの表記法（記数法）を統一したりする。

[0027] ここで、検知デバイス１１０の種類によっては、取得された通信ログに正規化処理の対象となる情報の一部が含まれない場合がある。このような場合の対応として、収集ユニット２１０は、予め設定されたデフォルト値を代入する、情報が無いことを示す値（Ｎｕｌｌ）を代入する、情報を補完せずに

分析を行う、等の処理を行ってもよい。具体的には、不足している情報の種類に応じて、何れの対応を取るかが定められる。なお、通信ログの書式がその通信ログを取得した検知デバイス１１０の製品仕様に合致しない場合や、取得した通信ログにおける値が異常な場合、収集ユニット２１０は、その取得した通信ログを不正な通信ログであるとして、分析対象から除去し、不正な通信ログを格納するデータベースに保存する。取得した通信ログにおける値が異常な場合とは、例えば、日時の値が未来の日時になっている場合である。

[0028] 通信ログの振り分け処理は、検知デバイス１１０が複数の監視対象装置１００における通信を対象とするデータセンタ方式である場合に、正規化された通信ログを、契約等により定められた監視対象ごとの通信ログに分割する処理である。例えば、ネットワーク上に設けられた検知デバイス１１０によるサービスを、登録された監視対象装置１００が利用する環境で実施すると、一つの検知デバイス１１０が複数の監視対象装置１００の通信を検知することがあり得る。この場合、検知デバイス１１０により取得された通信ログファイルには、複数の監視対象装置１００における通信ログが含まれることとなる。そこで、顧客単位で通信ログの分析を行うため、本実施形態では、収集ユニット２１０は、監視対象装置１００ごとに通信ログを分割する。したがって、データセンタ方式による実施形態を採用せず、監視対象ごとに個別の検知デバイス１１０が設けられている場合は、この通信ログの振り分け処理は不要である。なぜなら、この場合、通信ログは、予め振り分けられた状態となっているからである。

[0029] 通信ログの振り分けは、例えば、ＩＰアドレスの範囲（レンジ）情報に基づいて行われる。具体的に、以下の想定例について説明する。すなわち、検知デバイス１１０の扱うＩＰアドレスが「ｘ．ｘ．ｘ．１」～「ｘ．ｘ．ｘ．３０」（ｘは０～２５５の数値）の範囲である。顧客Ａの監視対象装置１００に割り当てられたＩＰアドレスが「ｘ．ｘ．ｘ．１」～「ｘ．ｘ．ｘ．１０」である。顧客Ｂの監視対象装置１００に割り当てられたＩＰアドレス

が「ｘ．ｘ．ｘ．１１」～「ｘ．ｘ．ｘ．１２」である。顧客Ｃの監視対象装置１００に割り当てられたＩＰアドレスが「ｘ．ｘ．ｘ．１３」～「ｘ．ｘ．ｘ．３０」である。このような想定例の場合、これらの監視対象装置１００ごとのＩＰアドレスの範囲を収集ユニット２１０に予め登録しておくことにより、収集ユニット２１０は、ある通信ログが何れの監視対象装置１００に関する通信ログかを判断し、振り分けることができる。

[0030] 収集ユニット２１０は、フィルタリング処理では、顧客ごとに設定された個別の条件・規則に基づき、上記の振り分け処理で振り分けられた通信ログを分析対象とするか否かを判断する。このフィルタリング処理における判定項目は、送信元ＩＰアドレス、送信元ポート、宛先ＩＰアドレス、宛先ポート等を含む。すなわち、ある通信ログにおいて送信元ＩＰアドレスが特定の値であった場合は、収集ユニット２１０は、その通信ログを分析対象から除外する等のように処理することができる。また、検知日時を判定項目に設定した場合、収集ユニット２１０は、特定の日時以降に行われた通信のみを分析対象に含めるように処理することもできる。

[0031] 以上のようにして、収集ユニット２１０は、ログ管理サブシステム１２０から取得した生ログの通信ログファイルから処理対象の通信ログを抽出して正規化する。そして、収集ユニット２１０は、処理の済んだ通信ログを、後段の検出ユニット２２０へ送る。

[0032] 本実施形態では、上記のような処理を行う実行手段を、小さな処理単位ごとにコンポーネント化して構成する。このコンポーネント化された処理単位のブロック（以下、処理単位ブロック）を組み合わせることにより、様々な検知デバイス１１０に対応する処理を容易に構成することが可能となる。個々の処理単位ブロックが実行する処理の内容（処理単位）は、特に限定されないが、処理単位ブロックの組み替えにより種々の検知デバイス１１０に対応することが可能となるような内容に設定される。

[0033] 図３は、コンポーネント化された処理単位ブロックにより構成される収集ユニット２１０の構成例を示す図である。

図３に示す例では、複数の処理単位ブロック２１１は、初期情報取得ブロック２１１ａ、受信件数取得ブロック２１１ｂ、受信ファイル登録ブロック２１１ｃ、項目編集ブロック２１１ｄ、フォーマット不一致ログ情報登録ブロック２１１ｅ、ログ共通項目編集ブロック２１１ｆ、顧客分割ブロック２１１ｄを含む。初期情報取得ブロック２１１ａは、初期情報を取得する処理を行う処理単位ブロックである。受信件数取得ブロック２１１ｂは、受信件数を取得する処理を行う処理単位ブロックである。受信ファイル登録ブロック２１１ｃは、受信ファイルを登録する処理を行う処理単位ブロックである。項目編集ブロック２１１ｄは、項目を編集する処理を行う処理単位ブロックである。フォーマット不一致ログ情報登録ブロック２１１ｅは、フォーマットが不一致であるログの情報を登録する処理を行う処理単位ブロックである。ログ共通項目編集ブロック２１１ｆは、ログの共通項目を編集する処理を行う処理単位ブロックである。顧客分割ブロック２１１ｄは、顧客を分割する処理を行う処理単位ブロックである。これらの処理単位ブロック２１１が組み合わされて収集ユニット２１０が構成されている。なお、図３には、収集ユニット２１０を構成する処理単位ブロック２１１の一部のみが記載されている。例えば、初期情報取得ブロック２１１ａ、受信件数取得ブロック２１１ｂ、受信ファイル登録ブロック２１１ｃ等の処理単位ブロック２１１が、図２に示した分析対象ログ抽出処理を担う。項目編集ブロック２１１ｄ、フォーマット不一致ログ情報登録ブロック２１１ｅ、ログ共通項目編集ブロック２１１ｆ等の処理単位ブロック２１１が、図２に示した正規化処理を担う。顧客分割ブロック２１１ｇ等の処理単位ブロック２１１が、図２に示した振り分け処理を担う。

[0034] 本実施形態では、検知デバイス１１０の種類（ＩＤＳ／ＩＰＳ、ファイア・ウォール、ウィルス対策ソフト等の製品種別）に応じて、適用される処理単位ブロック２１１の種類や順番を設定する。すなわち、監視対象として設定された監視対象装置１００の検知デバイス１１０の種類ごとに、処理単位ブロック２１１の適用順（シーケンス）が用意される。そして、処理対象の

通信ログファイルの生ログを取得した検知デバイス１１０の種類に応じて、その通信ログファイルを処理するために設定されたシーケンスを適用して、各処理単位ブロック２１１による処理を行う。

[0035] 収集ユニット２１０の各処理単位ブロック２１１により行われる処理の結果は、例えば収集ユニット２１０を構成するコンピュータのメモリに、一時的に保持される。そして、収集ユニット２１０における処理が済んだ通信ログと共にその結果を後段の検出ユニット２２０へ送る。

[0036] ＜検出ユニットの機能＞

図４は、監視サブシステム２００を構成する検出ユニット２２０の機能構成例を示す図である。

第２処理ユニットである検出ユニット２２０は、前段の収集ユニット２１０から取得した通信ログに対する処理として、その通信ログファイルの元の通信ログ（生ログ）を取得した検知デバイス１１０の分類ごとに設定された処理を行う。ここで、検知デバイス１１０の分類とは、検知デバイス１１０のセンサ１１１およびセンサ・マネージャ１１２の機能を提供するセキュリティ装置の種別（ＩＤＳ／ＩＰＳやファイア・ウォール等）を意味する。なお、検知デバイス１１０の分類を特定する情報（ＩＤ、機器名等）は、例えば、通信ログファイルに含まれている。

[0037] 図４に示すように、本実施形態の検出ユニット２２０は、収集ユニット２１０により処理された通信ログに対する処理として、共通情報の付加処理と、ログ集約（イベント化）処理とを行う。

[0038] 検出ユニット２２０は、共通情報の付加処理では、通信ログの分析に用いられる共通情報を付加する。この共通情報は、各通信ログに共通の項目に関する情報である。本実施形態では、共通情報として、攻撃パターン情報（オリジナル・シグネチャＩＤ）、通信方向区分、ルール・アクション、プロトコル番号・名称、国コードの５項目が設定される。

[0039] 攻撃パターン情報は、監視サブシステム２００により各通信ログに付与される、攻撃パターンを特定する情報である。検知デバイス１１０が通信ログ

（生ログ）において何らかの攻撃を検知すると、その通信ログに、検知した攻撃を特定する情報（メーカー・シグネチャ情報）を付加する。しかし、この情報の形式は監視対象装置１００や検知デバイス１１０の種類に応じて様々である。このため、本実施形態では、検出ユニット２２０が、オリジナルの情報（攻撃パターン情報）を通信ログに付加する。

[0040] 通信方向区分は、通信ログにより示される通信が、外部ネットワークから監視対象装置１００により区分される内部ネットワークへ向けて行われた通信か、反対に内部ネットワークから監視対象装置１００を通って外部ネットワークへ向けて行われた通信かを示す情報である。ネットワーク・セキュリティの分野では、通信元が内部ネットワークか外部ネットワークかにより、通信の意味合いや重要度が大きく変わる。具体例として、コンピュータ・ウィルスに感染した情報処理装置が行う通信についての通信ログがあった場合について説明する。この場合において、その通信が外部ネットワークから送られた通信であれば、コンピュータ・ウィルスに感染した情報処理装置は外部ネットワークに存在するので、特に問題はない。一方、その通信が内部ネットワークから送られた通信である場合、監視対象装置１００の保護対象である内部ネットワークにコンピュータ・ウィルスに感染した情報処理装置が存在することになるので対処する必要がある。そこで、本実施形態では検出ユニット２２０が各通信ログにおける通信の方向を示す通信方向区分の情報を付与する。ここで、通信方向区分の情報は、例えば監視対象装置１００のネットワーク・アドレスやプライベート・アドレスを参酌し、送信元ＩＰアドレスおよび宛先ＩＰアドレスが監視対象装置１００の内部ネットワークか外部ネットワークかを判断することにより得られる。

[0041] ルール・アクションは、監視対象装置１００において通信が検知された場合に、検知デバイス１１０により、その通信に応じて行われた動作（アクション）を示す情報である。検知デバイス１１０としてＩＤＳやＩＰＳ等のセキュリティ装置が用いられている場合、それらの装置は、それらの装置が有する機能に基づいて、危険な通信を検知したことを報告したり、その通信を

許可せず止めたりする。そこで、検出ユニット２２０がどのような動作が行われたかを示す情報を付与する。このルール・アクションの情報は、検知デバイス１１０であるセキュリティ装置によっても通信ログに付与される場合がある。しかし、同一の動作であっても、セキュリティ装置の種類によって名称が区々である。このため、監視サブシステム２００（の検出ユニット２２０）が統一された名称を付与する。

[0042] プロトコル番号・名称は、通信ログが示す通信に用いられた通信プロトコルの種類を示す情報である。ＴＣＰやＵＤＰ等、いくつかのプロトコルがあるため、検出ユニット２２０はこれらを識別するための情報を付与する。本実施形態では、通信プロトコルの種類を示す情報を例えばＩＡＮＡ（Internet Assigned Number Authority）の定義に基づいて定める。

[0043] 国コードは、通信ログが示す通信の送信元および宛先の国を示す情報であり、通信ログの送信元ＩＰアドレスおよび宛先ＩＰアドレスに基づいて決定される。この国コードは、主に統計情報として用いられる。この国コードは、送信元や宛先の国が、不正な通信による攻撃の多い国か否か、国内か否か等に応じて通信の危険性が異なると考えられる場合には、通信ログの分析に用いることもできる。

[0044] 以上のように、検出ユニット２２０は、共通情報の付加処理では、通信ログの分析において利用価値の高い情報を、共通の様式による情報として、通信ログに付加する。

[0045] 検出ユニット２２０は、ログ集約（イベント化）処理では、通信ログを必要に応じて集約し、分析単位情報であるイベントを生成する。検知デバイス１１０として用いられるセキュリティ装置の種類に応じて、通信ログの情報粒度は異なる。例えば、検知デバイス１１０がファイア・ウォールである場合は、検知対象の通信が一つ検知されれば、直ちにセンサ１１１によりその通信が検知される。これに対し、検知デバイス１１０がＩＤＳ等である場合は、複数の通信に基づき、所定の判断規則により危険な通信が行われていると判断される場合に、センサ１１１によりその危険であると判断された通信

が検知される。検知デバイス１１０がウィルス対策ソフトである場合は、対象の情報処理装置がコンピュータ・ウィルスに感染してからセンサ１１１によりその感染が検知される。したがって、検知デバイス１１０の種類に応じて、一つの通信ログにおける情報の重みが異なる。そこで、本実施形態では、検出ユニット２２０は、検知デバイス１１０の種類に応じて、複数の通信ログを集積してイベント化し、情報の粒度を揃える。すなわち、検出ユニット２２０は、一つの通信ログの情報量が多い検知デバイス１１０により取得された通信ログに関しては、より少ない数の通信ログで一つのイベントとする。一方で、検出ユニット２２０は、一つの通信ログの情報量が少ない検知デバイス１１０により取得された通信ログに関しては、より多い数の通信ログで一つのイベントとする。

[0046] 一例として、本実施形態では、検知デバイス１１０がファイア・ウォールである場合と、検知デバイス１１０がその他の場合とでイベント化の処理を異ならせる。具体的には、検知デバイス１１０がファイア・ウォールである場合は、上述したように通信ログの情報量が少ない（一つの通信でセンサ１１１によりその通信が検知される）。このため、この場合、検出ユニット２２０は、取得された通信ログを、予め定められた規則にしたがって集約することによりイベントを生成する。ファイア・ウォール以外の検知デバイス１１０により取得された通信ログについては、ファイア・ウォールと比較して通信ログの情報量が多い（複数の通信を経てセンサ１１１により事象（通信等）が検知される）。このため、この場合、検出ユニット２２０は一つのログを一つのイベントとする。

[0047] 検知デバイス１１０がファイア・ウォールである場合のイベントの生成処理は、次のようにして行われる。まず、検出ユニット２２０は、通信ログに含まれる情報および上記の共通情報の付加処理で通信ログに付加された共通情報に基づき、予め定められた集約規則に適合する通信ログを集めてイベントとする。具体的には、例えば、検出ユニット２２０は、判定項目として、通信ログに含まれる顧客ＩＤ、検知日付、送信元ＩＰアドレス、送信元ポー

ト番号、宛先ＩＰアドレスまたは宛先ポート番号と、共通情報である通信方向区分、ルール・アクション、プロトコル番号（名称）とが共通である通信ログを対象とする。検出ユニット２２０は、これらの判定項目が共通である通信ログの数が予め定められた閾値以上となったならば、それらの通信ログを集めて一つのイベントとする。

[0048] 上記の集約規則に基づく判断で不適合となった通信ログに対して、次に、ホスト・スキャン集約による判断が行われる。具体的には、例えば、検出ユニット２２０は、判断項目として、通信ログに含まれる顧客ＩＤ、検知日付、送信元ＩＰアドレス、送信元ポート番号、宛先ポート番号と、共通情報である通信方向区分、ルール・アクション、プロトコル番号（名称）とが共通である通信ログを対象とする。検出ユニット２２０は、これらの判断項目が共通である通信ログのうち、ある宛先ＩＰアドレスを有する通信ログの数が予め定められた閾値以上となったならば、それらの通信ログを集めて一つのイベントとする。

[0049] 上記のホスト・スキャン集約による判断で不適合となった通信ログに対して、次に、ポート・スキャン集約による判断が行われる。具体的には、例えば、検出ユニット２２０は、判断項目として、通信ログに含まれる顧客ＩＤ、検知日付、送信元ＩＰアドレス、送信元ポート番号、宛先ＩＰアドレスと、共通情報である通信方向区分、ルール・アクション、プロトコル番号（名称）とが共通である通信ログを対象とする。検出ユニット２２０は、これらの判断項目が共通である通信ログのうち、ある宛先ポート番号を有する通信ログの数が予め定められた閾値以上となったならば、それらの通信ログを集めて一つのイベントとする。

[0050] 検出ユニット２２０は、上記のポート・スキャン集約による判断で不適合となった通信ログに対しては、通信ログの件数に基づく集積を行い、所定の件数の通信ログを一つのイベントとする。このようにして、検出ユニット２２０は、情報粒度の小さいファイア・ウォールの検知デバイス１１０により取得された通信ログを集約して、その情報粒度を他の検知デバイス１１０に

より取得された通信ログ（＝イベント）の情報粒度に近づける。そして、検出ユニット２２０は、情報粒度の揃ったイベントを、後段の分析ユニット２３０へ送る。

[0051] 本実施形態では、上記のような処理を行う実行手段を、小さな処理単位ごとにコンポーネント化して構成する。このコンポーネント化された処理単位のブロック（以下、処理単位ブロック）を組み合わせることにより、検出ユニット２２０における処理の内容（個々の処理単位の種類や実行順など）を設計することができる。そして、様々な監視対象装置１００に対応する処理を容易に構成することが可能となる。個々の処理単位ブロックが実行する処理の内容（処理単位）は、特に限定されないが、処理単位ブロックの組み替えにより種々の監視対象装置１００に対応することが可能となるような内容に設定される。

[0052] 図５は、コンポーネント化された処理単位ブロックにより構成される検出ユニット２２０の構成例を示す図である。

図５に示す例では、複数の処理単位ブロック２２１は、固有識別情報付加ブロック２２１ａ、通信方向区分付加ブロック２２１ｂ、ルール・アクション付加ブロック２２１ｃ、プロトコル番号・名称付加ブロック２２１ｄ、国コード付加ブロック２２１ｅ、集約規則判断ブロック２２１ｆ、ホスト・スキャン集約ブロック２２１ｇ、ポート・スキャン集約ブロック２２１ｈを含む。固有識別情報付加ブロック２２１ａは、固有識別情報を付加する処理単位ブロックである。通信方向区分付加ブロック２２１ｂは、通信方向区分を付加する処理単位ブロックである。ルール・アクション付加ブロック２２１ｃは、ルール・アクションを付加する処理単位ブロックである。プロトコル番号・名称付加ブロック２２１ｄは、プロトコル番号・名称を付加・BR>キる処理単位ブロックである。国コード付加ブロック２２１ｅは、国コードを付加する処理単位ブロックである。集約規則判断ブロック２２１ｆは、集約規則を判断する処理単位ブロックである。ホスト・スキャン集約ブロック２２１ｇは、ホスト・スキャンを集約する処理単位ブロックである。ポート・ス

キャン集約ブロック２２１ｈは、ポート・スキャンを集約する処理単位ブロックである。これらの処理単位ブロック２２１が組み合わされて検出ユニット２２０が構成されている。なお、図５には、検出ユニット２２０を構成する処理単位ブロック２２１の一部のみが記載されている。例えば、固有識別情報付加ブロック２２１ａ、通信方向区分付加ブロック２２１ｂ、ルール・アクション付加ブロック２２１ｃ、プロトコル番号・名称付加ブロック２２１ｄ、国コード付加ブロック２２１ｅ等の処理単位ブロック２２１が、図４に示した共通情報の付加処理を担う。集約規則判断ブロック２２１ｆ、ホスト・スキャン集約ブロック２２１ｇ、ポート・スキャン集約ブロック２２１ｈ等の処理単位ブロック２２１が、図４に示したログ集約（イベント化）処理を担う。

[0053] 本実施形態では、監視対象装置１００の種類（セキュリティ装置の種別）に応じて、適用される処理単位ブロック２２１の種類や順番を設定する。すなわち、監視対象として設定された監視対象装置１００の種類ごとに、処理単位ブロック２２１の適用順（シーケンス）が用意される。そして、処理対象の通信ログファイルの生ログが取得された監視対象装置１００の種類に応じて、その通信ログファイルを処理するために設定されたシーケンスを適用して、各処理単位ブロック２２１による処理を行う。

[0054] 検出ユニット２２０の各処理単位ブロック２２１により行われる共通情報の付加処理およびログ集約処理の結果は、例えば検出ユニット２２０を構成するコンピュータのメモリに、一時的に保持される。そして、通信ログを集約して得られたイベントと共にその結果を後段の分析ユニット２３０へ送る。

[0055] ＜分析ユニットの機能＞

図６は、監視サブシステム２００を構成する分析ユニット２３０の機能構成例を示す図である。

図６に示す構成例において、第３処理ユニットである分析ユニット２３０は、個別分析処理部２３０ａと、イベント集積処理部２３０ｂと、相関分析

処理部２３０ｃと、増分分析処理部２３０ｄとにより構成される。

[0056] 個別分析処理部２３０ａは、検出ユニット２２０により生成されたイベントに対して、個別に、問題のある通信か否かを判断する。具体的には、個別分析処理部２３０ａは、各イベントを不正な通信に関するリスト（いわゆるブラックリスト）と照合（マッチング）し、該当すれば、そのイベントに示される通信を不正な通信と判断する。ここで、不正な通信のリストは、例えば、問題のある通信に関わるＩＰアドレスを登録している。そして、個別分析処理部２３０ａは、イベントに示される通信の送信元ＩＰアドレスまたは宛先ＩＰアドレスの何れかがリストに登録されたＩＰアドレスと合致すれば、その通信が不正な通信であると判断する。

[0057] また、個別分析処理部２３０ａは、問題のある通信のリストとの照合により問題のある通信であると判断されなかったイベントに関して、イベント間の相関関係に基づく分析を行うか否かを判断する。すなわち、個別分析処理部２３０ａは、イベントを、相関関係に基づく分析を行うイベントと、相関関係に基づく分析を行わないイベントとに分類する分類手段（分類部）として機能する。相関関係に基づく分析の対象とするか否かの判断は、例えば、イベントに含まれる通信ログの情報や、検出ユニット２２０による共通情報の付加処理で通信ログに付加された共通情報（攻撃パターン情報、通信方向種別など）により特定される通信の内容に基づいて行われる。相関関係に基づく分析を行う対象とされたイベントに対しては、次にイベント集積処理部２３０ｂによる集積処理が行われる。一方、相関関係に基づく分析を行わないと判断されたイベントに関しては、分析ユニット２３０は、その後の処理を行わず（すなわち、相関分析や増分分析の対象外として）、そのイベントを手動分析ユニット２４０へ送る。

[0058] イベント集積処理部２３０ｂは、個別分析処理部２３０ａにより相関関係に基づく分析の対象とされたイベントを、予め定められた規則に基づいて集積し、一つまたは複数のイベントからなるイベント列（イベント・チェーン）を生成する。さらに、イベント集積処理部２３０ｂは、予め定められた規

則に基づいてイベント列を集積し、一つまたは複数のイベント列からなり、分析による検出対象となる事象の候補（インシデント・キャンディデート：以下、検出事象候補と呼ぶ）を生成する。すなわち、イベント集積処理部２３０ｂは、イベントを集積して、検出事象候補を生成する集積手段（集積部）として機能する。具体的には、例えば、イベント集積処理部２３０ｂは、外部ネットワークに存在するサーバ等からの不正なアクセスによる攻撃に関しては、同じ攻撃者による攻撃（アクセス）、同じ攻撃手段（アクセス方法）、同じ攻撃対象などが想定される通信を抽出し、抽出した通信を検出事象候補としてまとめる。ここで、同じ攻撃者による攻撃、同じ攻撃手段、同じ攻撃対象などが想定される通信の抽出は、例えば、送信元ＩＰアドレス、通信方向区分、検知日付などの情報に基づいて行われる。

[0059] 検知デバイス１１０とログ管理サブシステム１２０とによる通信ログの取得および監視サブシステム２００の収集ユニット２１０および検出ユニット２２０による処理は随時行われている。このため、イベントは時間の経過と共に次々と生成される。新たに生成されたイベントは、イベント集積処理部２３０ｂにより特定の検出事象候補に含まれる対象イベントに該当すると判断されれば、その検出事象候補に組み込まれることとなる。したがって、新たなイベントが追加された検出事象候補は、その度に相関分析処理部２３０ｃおよび増分分析処理部２３０ｄによる処理の対象となる。

[0060] 相関分析処理部（分析手段、分析部）２３０ｃは、攻撃パターン組み合わせ判定と、件数閾値超過判定とを行うことにより、複数のイベントの組み合わせである検出事象候補が問題のある通信か否かを判断する。

[0061] 攻撃パターン組み合わせ判定では、相関分析処理部２３０ｃは、検出事象候補に含まれる通信ログにおける通信方向、送信元・宛先ＩＰアドレス（レンジ）、送信元・宛先ポート、ルール・アクション、送信元・宛先国コード、セッション・データ等の情報に基づいて特定される通信の種類と、攻撃パターン情報（オリジナル・シグネチャＩＤ）の組み合わせとに基づき、検出事象候補により特定される通信が問題のある通信か否かを判断する。すなわ

ち、相関分析処理部２３０ｃは、検出事象候補により特定される通信の内容が、攻撃パターン情報により特定される攻撃パターンに該当するか否かを判断する。なお、ここでは、相関分析処理部２３０ｃは、この通信により、実際に攻撃（情報の搾取、消失など）が行われた可能性が高いか否かを判断する。

[0062] 件数閾値超過判定では、相関分析処理部２３０ｃは、検出事象候補に含まれる通信ログにおける通信方向、送信元・宛先ＩＰアドレス（レンジ）、送信元・宛先ポート、ルール・アクション、送信元・宛先国コードと件数などの情報に基づき、検出事象候補により特定される通信が問題のある通信か否かを判断する。ここでは、相関分析処理部２３０ｃは、検出事象候補により特定される通信の回数が普段と比較して大幅に増加しているか否かを判断する。

[0063] 図７は、相関分析の概念を示す図である。

分析ユニット２３０のイベント集積処理部２３０ｂは、検出ユニット２２０から取得したイベントのうち、集積処理の対象となったイベントを集積してイベント列を生成し、さらに検出事象候補を生成する。そして、イベント集積処理部２３０ｂは、検出事象候補ごとに、各検出事象候補に含まれるイベント列やイベントの間の相関関係に基づき、上記の攻撃パターン組み合わせ判定および件数閾値超過判定を行う。

[0064] 増分分析処理部２３０ｄは、事象変化の判定と、攻撃手段増加の判定と、攻撃件数増加の判定と、攻撃先増加の判定とを行うことにより、複数のイベントの組み合わせである検出事象候補が問題のある通信か否かを判断する。例えば外部ネットワークに存在するサーバ等からの不正なアクセスによる攻撃に関しては、単発の攻撃ではなく同じ攻撃が繰り返し続いたり、攻撃内容が変わったり攻撃先が増加したりすることがある。そこで、増分分析処理部２３０ｄは、検出事象候補に含まれる通信ログに基づいて問題のある通信であることが疑われる事象の変化の有無を判定する。

[0065] 各判定についてさらに説明すると、例えば、増分分析処理部２３０ｄは、

相関分析処理部２３０ｃによる一定期間分（例えば１日分）の分析結果に基づき、各検出事象候補に対する分析に用いられた分析ルール（攻撃パターン組み合わせ判定や件数閾値超過判定のためのルール）の適用の変化が判断される。

事象変化の判定では、前回の分析時と異なる分析ルールが適用された（事象が変化した）場合に、増分分析処理部２３０ｄは、判定対象の検出事象候補に含まれる通信が問題のある通信であると判断する。

攻撃手段増加の判定では、前回分析時と同一ルールが適用されたが、確認対象の攻撃パターン情報が追加された（確認対象の攻撃手段が増えた）場合に、増分分析処理部２３０ｄは、判定対象の検出事象候補に含まれる通信が問題のある通信であると判断する。

攻撃件数増加の判定では、確認対象の攻撃パターン情報が同一の通信（同一の攻撃手法）や、同一の攻撃元からの通信が継続しており、それらの通信による単位時間当たりのイベント件数が増加している場合に、増分分析処理部２３０ｄは、判定対象の検出事象候補に含まれる通信が問題のある通信であると判断する。

攻撃先増加の判定では、攻撃先や接続先が増えた場合に、増分分析処理部２３０ｄは、判定対象の検出事象候補に含まれる通信が問題のある通信であると判断する。

[0066] 図８Ａおよび８Ｂは、増分分析の概念を示す図である。図８Ａは、ある分析時における相関分析の対象となった一つの検出事象候補の構成例を示す。図８Ｂは、次の分析時における同じ検出事象候補の構成例を示す。

ここで、同じ検出事象候補に関する前回分析時の構成（図８Ａ参照）と今回分析時の構成（図８Ｂ参照）とを比較する。今回分析時の構成では、前回分析時には含まれていなかったイベント列（図８Ｂにおいて網掛けが付されたイベント列）が新たに含まれている。このため、この検出事象候補は、上述した事象変化の判定、攻撃手段増加の判定、攻撃件数増加の判定、攻撃先増加の判定の何れかにおいて問題のある通信と判断される。

[0067] 以上のようにして、各種の判定を行った後、分析ユニット２３０は、各検出事象候補に対する分析結果を、分析対象の検出事象候補に対応付けて、手動分析ユニット２４０に送る。分析ユニット２３０による分析結果は、各検出事象候補が、不正な通信か、問題のある通信（不正な通信である可能性のある通信）か、不正でない通信かを示す。

[0068] 本実施形態では、上記のような処理を行う個別分析処理部２３０ａ、イベント集積処理部２３０ｂ、相関分析処理部２３０ｃおよび増分分析処理部２３０ｄを、小さな処理単位ごとにコンポーネント化して構成する。このコンポーネント化された処理単位のブロック（以下、処理単位ブロック）を組み合わせることにより、各処理部２３０ａ～２３０ｄによる処理の内容（個々の処理単位の種類や実行順など）を設計することができる。そして、それまでにない新たな攻撃手法による攻撃が発見された場合にも、その攻撃において行われる通信であることを判定するために適用される処理に関する処理単位ブロックを追加することにより、その攻撃に容易に対応することが可能となる。

[0069] 図９は、コンポーネント化された処理単位ブロックを含む個別分析処理部２３０ａ、イベント集積処理部２３０ｂ、相関分析処理部２３０ｃおよび増分分析処理部２３０ｄにより構成される分析ユニット２３０の構成例を示す図である。

図９に示す例では、複数の処理単位ブロック２３１は、リスト照合ブロック２３１ａ、イベント集約ブロック２３１ｂ、イベント列集約ブロック２３１ｃ、攻撃パターン組み合わせ判定ブロック２３１ｄ、件数閾値超過判定ブロック２３１ｅ、事象変化判定ブロック２３１ｆ、攻撃手段増加判定ブロック２３１ｇ、件数増加率判定ブロック２３１ｈ、宛先ＩＰアドレス増加判定ブロック２３１ｉを含む。リスト照合ブロック２３１ａは、リストを照合する処理を行う処理単位ブロックである。イベント集約ブロック２３１ｂは、イベントを集約する処理を行う処理単位ブロックである。イベント列集約ブロック２３１ｃは、イベント列を集約する処理を行う処理単位ブロックであ

る。攻撃パターン組み合わせ判定ブロック２３１ｄは、攻撃パターンの組み合わせを判定する処理を行う処理単位ブロックである。件数閾値超過判定ブロック２３１ｅは、件数が閾値を超過しているか判定する処理を行う処理単位ブロックである。事象変化判定ブロック２３１ｆは、事象が変化しているか判定する処理を行う処理単位ブロックである。攻撃手段増加判定ブロック２３１ｇは、攻撃手段が増加しているか判定する処理を行う処理単位ブロックである。件数増加率判定ブロック２３１ｈは、件数の増加率を判定する処理を行う処理単位ブロックである。宛先ＩＰアドレス増加判定ブロック２３１ｉは、宛先ＩＰアドレスが増加しているか判定する処理を行う処理単位ブロックである。これらの処理単位ブロック２３１が組み合わされて分析ユニット２３０の各処理部２３０ａ～２３０ｄが構成されている。なお、図９には、分析ユニット２３０を構成する処理単位ブロック２３１の一部のみが記載されている。例えば、リスト照合ブロック２３１ａ等の処理単位ブロック２３１は、個別分析処理部２３０ａによる問題のある通信のリストとの照合を担う。イベント集約ブロック２３１ｂおよびイベント列集約ブロック２３１ｃ等の処理単位ブロック２３１は、イベント集積処理部２３０ｂによるイベント列および検出事象候補の生成を担う。攻撃パターン組み合わせ判定ブロック２３１ｄおよび件数閾値超過判定ブロック２３１ｅ等の処理単位ブロック２３１は、相関分析処理部２３０ｃによる分析を担う。事象変化判定ブロック２３１ｆ、攻撃手段増加判定ブロック２３１ｇ、件数増加率判定ブロック２３１ｈおよび宛先ＩＰアドレス増加判定ブロック２３１ｉ等の処理単位ブロック２３１は、増分分析処理部２３０ｄによる分析を担う。これらの処理単位ブロック２３１の列が、個別分析処理部２３０ａ、イベント集積処理部２３０ｂ、相関分析処理部２３０ｃおよび増分分析処理部２３０ｄを構成する。複数の個別分析処理部２３０ａ、複数のイベント集積処理部２３０ｂ、複数の相関分析処理部２３０ｃおよび複数の増分分析処理部２３０ｄが用意され、それぞれが並列かつ非同期に処理を実行することができる。

[0070] 分析ユニット２３０の各処理単位ブロック２３１により行われる個別分析

処理、イベント集積処理、相関分析処理および増分分析処理の結果は、例えば分析ユニット２３０を構成するコンピュータのメモリに、一時的に保持される。そして、各種の分析処理が済んだ検出事象候補および個別分析処理で集積対象とされなかったイベントと共にその結果を後段の手動分析ユニット２４０へ送る。

[0071] ＜手動分析ユニットの機能＞

図１０は、監視サブシステム２００の手動分析ユニット２４０の機能構成例を示す図である。

第４処理ユニットである手動分析ユニット２４０は、検出ユニット２２０および分析ユニット２３０による上記の各処理によって得られたイベント、イベント列および検出事象候補の情報と、分析ユニット２３０による分析結果とを記憶装置２４１に格納して管理する。また、手動分析ユニット２４０は、端末装置３００からの要求に応じて、送受信部２４２により、記憶装置２４１に格納しているイベント、イベント列および検出事象候補の情報と、分析ユニット２３０による分析結果とを端末装置３００に送る。さらに、手動分析ユニット２４０は、端末装置３００においてこれらの情報に付与された情報を送受信部２４２により取得し、取得した情報を格納している各情報に付加して管理する。

[0072] ＜監視サブシステムの各処理ユニット間の通信＞

本実施形態によるセキュリティ監視システムは、監視対象装置１００における通信を監視して、問題のある通信をリアルタイムに検出する。すなわち、蓄積された通信ログファイルを解析して問題のある通信が行われていたことを事後的に発見するシステムではない。したがって、通信ログから問題のある通信を検出するための監視サブシステム２００における各処理ユニット間における通信ログファイルの伝達は、できるだけ高速に行われることが望ましい。例えば、ＴＣＰ（Transmission Control Protocol）等のようなコネクション型の通信ではなく、コネクションレス型の通信を行う。上述したように、本実施形態では、ＪＭＳに基づくコネクションレス型の通信を行うこ

ととしている。

[0073] ここで、コネクションレス型の通信により通信ログの伝達を行う場合、コネクション型の通信とは異なり、監視サブシステム２００における各処理ユニット間での個々の通信が正常に行われたか否かを判断しない。したがって、各処理ユニット間の通信において処理対象の通信ログファイルが失われたとしても、その事実を認識することができない。そのため、監視サブシステム２００での処理中に処理対象の通信ログファイルが失われた場合に、その事実を検知する仕組みが必要となる。

[0074] 図１１は、本実施形態における通信ログファイルの伝達方式を説明する図である。

図１１は、監視サブシステム２００を構成する処理ユニット列（収集ユニット２１０、検出ユニット２２０、分析ユニット２３０、手動分析ユニット２４０により構成される列）を示している。本実施形態では、図１１に示す処理ユニット列において、先頭の処理ユニット（収集ユニット２１０）から最後の処理ユニット（手動分析ユニット２４０）まで、正常に通信ログの伝達が行われたことを、先頭の処理ユニットにフィードバックする構成が設けられている。

[0075] すなわち、監視サブシステム２００の最後の処理ユニットである手動分析ユニット２４０は、分析ユニット２３０からイベントや検出事象候補の情報を受け取ると、これらのイベントや検出事象候補を構成する通信ログを取得したことを、先頭の処理ユニットである収集ユニット２１０に通知する（図１１における矢印Ｒ参照）。これにより、処理対象の通信ログファイルが、各処理ユニットを経て最後の処理ユニット（手動分析ユニット２４０）まで失われずに到達したことが、先頭の収集ユニット２１０において認識される。収集ユニット２１０は、ある通信ログファイルを後段の処理ユニットである検出ユニット２２０に送信した後、所定の再送停止条件を満足するまで、例えば一定時間ごとに、その通信ログファイルを再送する。

[0076] 再送停止条件の一例として、前回の送信から一定時間以内に、手動分析ユ

ニット２４０から通信ログファイルを取得したことを示す通知を受け取ったことを条件に設定してもよい。再送停止条件をこのように設定することにより、何らかの原因で処理対象の通信ログファイルが消失し、手動分析ユニット２４０まで到達しなかった場合は、手動分析ユニット２４０から収集ユニット２１０への通知が行われない（再送停止条件を満足しない）。このため、一定時間経過後に、収集ユニット２１０から同一通信ログファイルの再送が行われることとなる。

[0077] 再送停止条件の別の例として、所定回数、同じ通信ログファイルを送信したことを条件に設定もよい。再送停止条件のさらに別の例として、最初の送信から所定時間が経過したことを条件に設定してもよい。再送停止条件をこのように設定することにより、所定回数繰り返して通信ログファイルが正常に伝達されなかった場合、コネクションレス型の通信仕様による消失ではなく、監視サブシステム２００に障害が発生していると判断することができる。そこで、この場合は、通信ログファイルの再送を停止すると共に、監視サブシステム２００に障害が発生していることをシステム・オペレータに報知する。なお、同じ通信ログファイルの送信を行った回数の計数については、例えば、収集ユニット２１０が通信ログファイルの送信時に送信回数を計数し、計数した送信回数を保持しておくことにより実現してもよい。

[0078] 上記のように構成された伝達方式では、処理対象の通信ログファイルが手動分析ユニット２４０に到達しなかった場合、各処理ユニット間での通信ログファイルの伝達における何れかの段階で通信ログファイルが失われたことはわかる。一方で、どこで通信ログファイルが失われたかを識別することはできない。しかし、本実施形態では、通信ログファイルが手動分析ユニット２４０に到達しなければ、その通信ログファイルに対する処理（分析）は完了しない。そのため、上記のように、監視サブシステム２００の処理ユニット列の最後に位置する手動分析ユニット２４０を検査位置とした。

[0079] ここで、上記の伝達方式では、各処理ユニット間での通信ログファイルの伝達のどこで通信ログファイルが失われたとしても、先頭の収集ユニット２

１０から最後の手動分析ユニット２４０へ、改めて通信ログファイルが伝達される。そのため、例えば分析ユニット２３０と手動分析ユニット２４０との間で通信ログファイルが失われた場合、その通信ログファイルに対する検出ユニット２２０および分析ユニット２３０による処理は済んでいるにも関わらず、同じ通信ログファイルが再度伝達されることになる。

[0080] しかし、本実施形態では、通信ログファイルが手動分析ユニット２４０に到達しなければ、各処理ユニットにおける処理結果も、手動分析ユニット２４０の記憶装置２４１には格納されず、通信ログファイルと共に消失する。したがって、各処理ユニットは、再送された通信ログファイルに対して、前回の送信時に処理を行ったか否かに関わらず、処理を行う。

[0081] 図１２は、本実施形態による通信ログファイルの伝達の一例を示す図である。 図１２において、“×”は通信ログファイルが消失したことを示している。“○”は通信ログファイルが手動分析ユニット２４０に到達したことを示している。矢印Ｔａ１は１回目の送信を示す。矢印Ｔａ２は２回目の送信を示す。矢印Ｔａ３は３回目の送信を示す。

図１２に示す例において、ある通信ログファイルが、１回目の送信において、収集ユニット２１０から検出ユニット２２０へ送信され、検出ユニット２２０による処理を経た後、検出ユニット２２０から分析ユニット２３０へ送信され、分析ユニット２３０に到達せずに消失している（矢印Ｔａ１参照）。この場合、手動分析ユニット２４０から通信ログファイルを取得したことを示す通知が収集ユニット２１０に対して行われない。このため、収集ユニット２１０は、通信ログファイルを再送する。すなわち、収集ユニット２１０は、通信ログファイルの２回目の送信を行う。

１回目の送信に係る通信ログファイルに対して行われた検出ユニット２２０の処理の結果は、１回目の送信に係る通信ログファイルと共に消失している。このため、検出ユニット２２０は、再送された通信ログファイルに対して処理を行う。

[0082] 図１２に示す例において、２回目の送信では、通信ログファイルは、分析

ユニット２３０による処理を経て、分析ユニット２３０から手動分析ユニット２４０へ送信されたが、手動分析ユニット２４０に到達せずに消失している（矢印Ｔａ２参照）。この場合も、手動分析ユニット２４０から通信ログファイルを取得したことを示す通知が収集ユニット２１０に対して行われない。このため、収集ユニット２１０は、通信ログファイルを再送する。すなわち、収集ユニット２１０は、通信ログファイルの３回目の送信を行う。

２回目の送信に係る通信ログファイルに対して行われた検出ユニット２２０および分析ユニット２３０の処理の結果は、２回目の送信に係る通信ログファイルと共に消失している。このため、検出ユニット２２０および分析ユニット２３０は、再送された通信ログファイルに対して処理を行う。

[0083] 図１２に示す例において、３回目の送信では、通信ログファイルは、手動分析ユニット２４０まで到達し、記憶装置２４１に格納される（矢印Ｔａ３参照）。そして、手動分析ユニット２４０から収集ユニット２１０へ通信ログファイルが到達したことを示す通知が行われる。これにより、この通信ログファイルの再送は停止される。

[0084] 上記の伝達方式を採用すると、通信ログファイルが消失していなくても再送されてしまうことが起こり得る。具体例としては、途中の処理ユニットによる処理に時間がかかったために、手動分析ユニット２４０から通知が行われる前に収集ユニット２１０における再送のための待ち時間が経過してしまった場合である。この場合、同じ通信ログファイル（検出事象候補）とその処理結果が、手動分析ユニット２４０に複数回到達し、記憶装置２４１に重複して格納される可能性がある。そこで、このような場合は、最後に収集ユニット２１０から送信された通信ログファイルおよびその処理結果を有効なデータとして用いることとする。なお、有効なデータとは、後述する、端末装置３００へ送信されて表示部３３０（図１５参照）に表示される対象となるデータである。

[0085] 図１３は、本実施形態による通信ログファイルの伝達の他の例を示す図である。 図１３において、“×”は通信ログファイルが消失したことを示し

ている。“○”は通信ログファイルが手動分析ユニット２４０に到達したことを示している。矢印Ｔｂ１は１回目の送信を示す。矢印Ｔｂ２は２回目の送信を示す。矢印Ｔｂ３は３回目の送信を示す。図１３に示す例においては、後述のように、３回目の送信に係る通信ログファイルが分析ユニット２３０に到達した後に、２回目の送信に係る通信ログファイルが分析ユニット２３０に到達している。

図１３に示す例において、１回目の送信では、通信ログファイルは、検出ユニット２２０による処理を経た後、分析ユニット２３０に到達せずに消失している（矢印Ｔｂ１参照）。２回目の送信では、通信ログファイルは消失せずに手動分析ユニット２４０に到達している（矢印Ｔｂ２参照）。しかしながら、２回目の送信は途中の処理に時間を要している。このため、手動分析ユニット２４０から収集ユニット２１０へ通知が行われる前に３回目の送信が行われている（矢印Ｔｂ３参照）。さらに、２回目の送信に係る通信ログファイルに対する処理に時間を要している。このため、３回目の送信に係る通信ログファイルが、２回目の送信に係る通信ログファイルよりも先に手動分析ユニット２４０に到達している。この場合、手動分析ユニット２４０に到達した順番に関わらず、３回目（最後）の送信に係る通信ログファイルに対して行われた処理の結果が有効なデータとして扱われる。

なお、上記の場合、手動分析ユニット２４０に到達して記憶装置２４１に格納された、同じ通信ログファイルに関する重複したデータのうち、有効なデータ以外のデータ（図１３に示す例では、２回目の送信に係る通信ログファイルに関するデータ）については、削除しても良いし、記憶装置２４１に格納されたまま放置しても良い。

[0086] 図１４は、本実施形態による通信ログファイルの伝達のさらに他の例を示す図である。 図１４において、“×”は通信ログファイルが消失したことを示している。“○”は通信ログファイルが手動分析ユニット２４０に到達したことを示している。矢印Ｔｃ１は１回目の送信を示す。矢印Ｔｃ２は２回目の送信を示す。矢印Ｔｃ３は３回目の送信を示す。

図１３に示した例のように、前に送信された通信ログファイルが手動分析ユニット２４０に到達する前に通信ログファイルの再送が行われる場合がある。このような場合において、後に送信された通信ログファイルが途中で消失する場合があり得る。図１４に示す例では、２回目の送信に係る通信ログファイルが手動分析ユニット２４０に到達する前に通信ログファイルの再送（３回目の送信）が行われている。しかしながら、３回目の送信に係る通信ログファイルは手動分析ユニット２４０に到達せずに消失している。この場合、手動分析ユニット２４０に到達して記憶装置２４１に格納された通信ログファイルは、２回目の送信に係る通信ログファイルだけである。このため、この２回目の送信に係る通信ログファイルに関するデータが有効なデータとして扱われる。

[0087] なお、上記の各処理ユニットによる動作は、再送された通信ログファイルに対する動作の一例に過ぎず、上記の動作に限定されない。例えば、本実施形態の一例として、各処理ユニットの処理結果が、各処理ユニットを構成するコンピュータのメモリに一時的に保持される場合について上記において説明している。しかしながら、本実施形態はこのよう構成に限定されない。本実施形態の別の例として、各処理ユニットの処理結果を所定のデータベースに格納して管理する構成を採用してもよい。この場合、各処理ユニットを伝送中に通信ログファイルが消失しても、既に行われた処理については、処理結果がデータベースに残る。このような場合、処理ユニットが、再送された通信ログファイルに対して重複して処理を行うと、問題のある通信の検出精度に影響を与えてしまう。そこで、重複した処理結果が残らないようにする必要がある。

一例としては、ある処理ユニットにおいて、再送された通信ログファイルが処理済みの通信ログファイルであった場合、既に存在している処理結果の情報を今回の処理結果の情報に置き換えてもよい。すなわち、その通信ログファイルに関する前回の処理結果を破棄する。また、別の例としては、ある処理ユニットにおいて、再送された通信ログファイルが処理済みの通信ログ

ファイルであった場合、その再送された通信ログファイルに対する処理をスキップして（飛ばして）、後段の処理ユニットへ通信ログファイルを送るようにしても良い。

[0088] １回目の通信と再送とを区別するための情報としては、再送であることを示すフラグ・データ等を付加するようにしても良いし、何回目の送信かを示す情報を付加しても良い。送信回数を示す情報を付加する場合、手動分析ユニット２４０から収集ユニット２１０への通知において送信回数を示す情報も一緒に通知すれば、収集ユニット２１０において同じ通信ログファイルの送信回数を計数しなくても、手動分析ユニット２４０からの通知に基づいて、同じ通信ログファイルを何回送信したかを認識することができる。

[0089] ＜端末装置の機能＞

図１５は、端末装置３００の機能構成例を示す図である。

図１５に示す例において、端末装置３００は、送受信部３１０と、データ処理部３２０とを備える。また、端末装置３００は、液晶ディスプレイ等で実現される表示部３３０と、キーボードやマウス等の入力デバイスで実現される操作部３４０とを備える。

[0090] 送受信部３１０は、監視サブシステム２００の手動分析ユニット２４０との間で通信を行うインターフェイスである。送受信部３１０は、手動分析ユニット２４０から検出ユニット２２０および分析ユニット２３０の処理によって得られたイベント、イベント列および検出事象候補の情報と、分析ユニット２３０による分析結果とを受信する。また、送受信部３１０は、操作部３４０の操作により入力される情報を監視サブシステム２００の手動分析ユニット２４０へ送信する。さらに、送受信部３１０は、監視対象装置１００の通信に対する分析の結果として、問題のある通信が発見された場合に、監視対象装置１００のオペレータが操作する端末装置（図示せず）にその通信の発見を通知する。

[0091] データ処理部３２０は、送受信部３１０により監視サブシステム２００の手動分析ユニット２４０から取得したイベント、イベント列および検出事象

候補の情報と、分析ユニット２３０による分析結果とに基づき分析用画面を生成する。また、データ処理部３２０は、生成した分析用画面を表示部３３０に表示させる。

[0092] 図１６は、分析用画面の構成例を示す図である。

図１６に示す例において、表示部３３０に表示される分析用画面は、検索条件表示領域３３１、検出事象候補表示領域３３２、イベント列表示領域３３３、イベント表示領域３３４、コメント表示領域３３５、重要度表示領域３３６の６個の表示領域により構成される。

[0093] 検索条件表示領域３３１には、検出事象候補表示領域３３２に表示される検出事象候補等の検索条件が表示される。この検索条件は、例えば、初期的に適当な条件が設定されてもよい。また、例えば、この検索条件は、操作部３４０の操作により解析者が所望の検索条件を入力することで設定されてもよい。なお、検索対象となる検出事象候補には、一つのイベント列あるいは一つのイベントのみで構成される検出事象候補も含まれる。また、分析ユニット２３０の個別分析処理部２３０ａにより相関関係に基づく分析を行わないとして取り出された単独のイベントを、一つのイベントからなる検出事象候補として検索対象とすることができる。

[0094] 検出事象候補表示領域３３２には、検索条件表示領域３３１に表示された検索条件で検索された検出事象候補および監視サブシステム２００の分析ユニット２３０によるその処理結果が表示される。

[0095] イベント列表示領域３３３には、検出事象候補表示領域３３２に表示された（すなわち、検索条件表示領域３３１において特定された検索条件で検索された）検出事象候補に含まれるイベント列および監視サブシステム２００の分析ユニット２３０によるその処理結果が表示される。

[0096] イベント表示領域３３４には、検出事象候補表示領域３３２に表示された（すなわち、検索条件表示領域３３１において特定された検索条件で検索された）検出事象候補に含まれるイベントおよび監視サブシステム２００の分析ユニット２３０によるその処理結果が表示される。

[0097] コメント表示領域３３５には、解析者が操作部３４０を操作して入力したコメントが表示される。具体的には、例えば、監視対象装置１００の通信に対する解析者の評価等のコメントが入力される。

重要度表示領域３３６には、検出事象候補表示領域３３２に表示された（すなわち、検索条件表示領域３３１において特定された検索条件で検索された）検出事象候補に対する評価を行うための評価レベルが示される。ここで、評価レベルとは、例えば、直ちに対策を取ることが必要か否か、引き続き同種の通信を検出して評価する必要があるか否か等の、検出事象候補により特定される通信に対する必要な対応等に応じて予め段階分けされた、重要度の値である。この重要度表示領域３３６は、解析者による重要度レベルの選択を受け付ける入力インターフェイスとなっている。解析者は、重要度表示領域３３６に表示された重要度レベルの一つを選択することにより、検索された検出事象候補に対する評価を行う。

[0098] 解析者は、表示部３３０の検索条件表示領域３３１に初期的に表示された検索条件や自身が操作部３４０の操作により入力した検索条件に基づいて検索された検出事象候補、イベント列、イベントに基づき、監視対象装置１００の通信を評価（手動分析）する。そして、問題のある通信が発見されたならば、解析者は、操作部３４０を操作して通信の内容（問題の内容）に応じたコメントおよび重要度を入力し、送受信部３１０を介して監視対象装置１００のオペレータに通知する。

[0099] なお、分析ユニット２３０においてリストとの照合により不正な通信（攻撃や不正な情報流出など）と判断された通信や、分析ユニット２３０における分析により不正な通信であることが確定した通信については、解析者の評価を要さずに監視対象装置１００のオペレータへの通知対象として良い。

[0100] ＜ハードウェア構成例＞

図１７は、本実施形態の監視サブシステム２００の各処理ユニットや端末装置３００を構成するのに適用可能なハードウェア（コンピュータ）構成例を示す図である。

図１７に示すコンピュータは、演算手段であるＣＰＵ（Central Processing Unit）１０ａと、主記憶手段であるメモリ１０ｃを備える。また、図１７に示すコンピュータは、外部デバイスとして、磁気ディスク装置（ＨＤＤ：Hard Disk Drive）１０ｇ、ネットワーク・インターフェイス１０ｆ、ディスプレイ装置を含む表示機構１０ｄ、キーボードやマウス等の入力デバイス１０ｉ等を備える。

[0101] 図１７に示す構成例では、メモリ１０ｃおよび表示機構１０ｄは、システム・コントローラ１０ｂを介してＣＰＵ１０ａに接続されている。また、ネットワーク・インターフェイス１０ｆ、磁気ディスク装置１０ｇおよび入力デバイス１０ｉは、Ｉ／Ｏコントローラ１０ｅを介してシステム・コントローラ１０ｂと接続されている。各構成要素は、システム・バスや入出力バス等の各種のバスによって接続される。

[0102] 図１７は、本実施形態が適用されるのに好適なコンピュータのハードウェア構成を例示するに過ぎない。本実施形態は、監視対象装置１００における通信のログファイルをリアルタイムに取得して処理し、不正な通信や問題のある通信を検出することが可能な情報処理装置に広く適用できる。すなわち、本実施形態を実現するための構成は、図１７に示す構成に限定されない。

[0103] 図１７において、磁気ディスク装置１０ｇにはＯＳのプログラムやアプリケーション・プログラムが格納されている。そして、これらのプログラムがメモリ１０ｃに読み込まれてＣＰＵ１０ａに実行されることにより、本実施形態における監視サブシステム２００の各処理ユニット２１０～２４０や端末装置３００における各種の機能が実現される。

産業上の利用可能性

[0104] 本発明は、ログ分析システムに適用してもよい。

符号の説明

[0105] １００…監視対象装置

１１０…検知デバイス

１１１…センサ

１１２…センサ・マネージャ

１２０…ログ管理サブシステム

１２１…ログ取得エージェント

２００…監視サブシステム

２１０…収集ユニット

２２０…検出ユニット

２３０…分析ユニット

２４０…手動分析ユニット

３００…端末装置

請求の範囲

[請求項1] 監視対象システムにおいて検知される検知ログを分析するログ分析システムにおいて、

前記監視対象システムにおいて行われる検知対象処理を検知し、当該検知対象処理の検知ログを取得する取得装置と、

前記取得装置により取得された前記検知ログを処理する処理装置と、を備え、

前記処理装置は、前記検知ログに対する処理を順次行う複数の処理ブロックを含み、先頭の処理ブロックから順に後段の処理ブロックへ当該検知ログを送りながら処理を行い、

前記処理装置の最後の前記処理ブロックは、前記検知ログを受け取ったことを、当該処理装置の最初の前記処理ブロックに通知し、

前記処理装置の前記最初の処理ブロックは、処理を行った前記検知ログのうち、当該処理装置の前記最後の処理ブロックからの通知において当該最後の処理ブロックに到達したことが確認できない検知ログを、後段の処理ブロックへ再送すること、

を特徴とする、ログ分析システム。

[請求項2] 前記処理装置の前記最初の処理ブロックは、一つの前記検知ログについて予め定められた回数送信を繰り返した後に、当該処理装置の前記最後の処理ブロックからの通知において当該検知ログが当該最後の処理ブロックに到達したことが確認できない場合、当該検知ログの送信を停止することを特徴とする、請求項１に記載のログ分析システム。

[請求項3] 前記処理装置の前記最初の処理ブロックは、前記検知ログに対して再送される検知ログか否かを識別可能な情報を付加して、当該検知ログを後段の処理ブロックに送ること、を特徴とする、請求項１または請求項２に記載のログ分析システム。

[請求項4] 前記処理装置の前記最初の処理ブロックは、前記検知ログに対して

何回目の伝達かを示す情報を付加して、当該検知ログを後段の処理ブロックに送ること、を特徴とする、請求項１または請求項２に記載のログ分析システム。