(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2017-117255
(P2017-117255A)
(43)公開日　平成29年6月29日(2017.6.29)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/55	(2013.01)	G06F	21/55	320	5B042
G06F 11/30	(2006.01)	G06F	11/30	320G	

審査請求 有　請求項の数 5　ＯＬ　（全 27 頁）

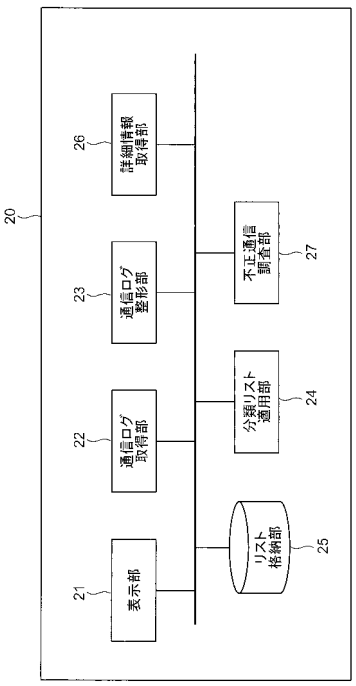
(21)出願番号　特願2015-252933 (P2015-252933)
(22)出願日　平成27年12月25日 (2015.12.25)
(11)特許番号　特許第6007308号 (P6007308)
(45)特許公報発行日　平成28年10月12日 (2016.10.12)

(71)出願人　500072884
株式会社ラック
東京都千代田区平河町２丁目１６番１号
平河町森タワー
(74)代理人　100104880
弁理士　古部　次郎
(74)代理人　100118108
弁理士　久保　洋之
(72)発明者　小笠原　恒雄
東京都千代田区平河町２丁目１６番１号
平河町森タワー

Ｆターム(参考)　5B042 GA39　JJ06　MA08　MA10　MA14
MC09　MC25　MC35

(54)【発明の名称】情報処理装置、情報処理方法及びプログラム

(57)【要約】　（修正有）
【課題】通信ログの分析において、検出された不正通信をもとに別の不正通信の調査を効率良く行う。
【解決手段】通信分析装置２０は、監視対象とするネットワーク上で対象期間内に検知された通信の通信ログを取得する通信ログ取得部２２と、取得された通信ログをもとに不正通信が検出された場合に、取得された通信ログの中から、通信元が不正通信の通信元と同一の通信で、不正通信の発生状況をもとに特定された特定期間内に検知された通信の通信ログを抽出する不正通信調査部２７とを備える。
【選択図】図２



【特許請求の範囲】
【請求項１】
監視対象とするネットワーク上で対象期間内に検知された通信の通信ログを取得する取得手段と、
前記取得手段が取得した通信ログをもとに不正通信が検出された場合に、当該取得手段が取得した当該通信ログの中から、通信元が当該不正通信の通信元と同一の通信で、当該不正通信の発生状況をもとに特定された特定期間内に検知された通信の通信ログを抽出する抽出手段と
を備える情報処理装置。
【請求項２】
前記特定期間は、前記対象期間内に前記通信元にて前記不正通信が最初に発生した時点から最後に発生した時点までの期間をもとに特定されること
を特徴とする請求項１に記載の情報処理装置。
【請求項３】
前記抽出手段は、検出された前記不正通信の通信元が複数存在する場合、当該通信元ごとに、通信元が当該不正通信の通信元と同一の通信で、当該不正通信の発生状況をもとに特定された特定期間内に検知された通信の通信ログを抽出すること
を特徴とする請求項１または２に記載の情報処理装置。
【請求項４】
前記抽出手段は、当該抽出手段が抽出した通信ログをもとに別の不正通信が検出された場合に、前記取得手段が取得した通信ログの中から、通信元が当該別の不正通信の通信元と同一の通信で、当該別の不正通信の発生状況をもとに特定された特定期間内に検知された通信の通信ログを抽出すること
を特徴とする請求項１乃至３のいずれか１項に記載の情報処理装置。
【請求項５】
監視対象とするネットワーク上で対象期間内に検知された通信の通信ログを取得する取得手段と、
前記取得手段が取得した通信ログをもとに不正通信が検出された場合に、当該取得手段が取得した当該通信ログの中から、当該不正通信の通信ログにおけるマルウェアの作成傾向に沿う情報と同じものが含まれる通信ログを抽出する抽出手段と
を備える情報処理装置。
【請求項６】
監視対象とするネットワーク上で対象期間内に検知された通信の通信ログを取得するステップと、
取得された前記通信ログをもとに不正通信が検出された場合に、取得された当該通信ログの中から、通信元が当該不正通信の通信元と同一の通信で、当該不正通信の発生状況をもとに特定された特定期間内に検知された通信の通信ログを抽出するステップと
を含む情報処理方法。
【請求項７】
監視対象とするネットワーク上で対象期間内に検知された通信の通信ログを取得するステップと、
取得された前記通信ログをもとに不正通信が検出された場合に、取得された当該通信ログの中から、当該不正通信の通信ログにおけるマルウェアの作成傾向に沿う情報と同じものが含まれる通信ログを抽出するステップと
を含む情報処理方法。
【請求項８】
コンピュータに、
監視対象とするネットワーク上で対象期間内に検知された通信の通信ログを取得する機能と、
取得された前記通信ログをもとに不正通信が検出された場合に、取得された当該通信ロ

グの中から、通信元が当該不正通信の通信元と同一の通信で、当該不正通信の発生状況をもとに特定された特定期間内に検知された通信の通信ログを抽出する機能と
を実現させるためのプログラム。
【請求項９】
コンピュータに、
監視対象とするネットワーク上で対象期間内に検知された通信の通信ログを取得する機能と、
取得された前記通信ログをもとに不正通信が検出された場合に、取得された当該通信ログの中から、当該不正通信の通信ログにおけるマルウェアの作成傾向に沿う情報と同じものが含まれる通信ログを抽出する機能と
を実現させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理装置、情報処理方法及びプログラムに関する。
【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】
不正な通信による被害を抑えるために、ネットワーク上の情報通信の監視を行う技術として、例えば、特許文献１には、正常な通信のシグネチャのリストを格納したデータベースと、通信データを取得し、通信データのシグネチャが含まれるように、取得した通信データの所定位置から所定長のデータを比較対象データとして抽出する抽出回路と、抽出された比較対象データのうち、通信データのシグネチャ以外のデータをマスクするマスク回路と、マスクされた比較対象データに含まれる通信データのシグネチャをデータベースから検索する検索回路と、データベースに格納された正常な通信のシグネチャに合致しない通信データを検知したときに警告を発する処理実行回路とを備えるボット検出装置が開示されている。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２００９－１６４７１２号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
ネットワーク上の情報通信の監視等のように、大量の通信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通信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又はその可能性のある処理に関する通信ログはごくわずかに過ぎない。そのため、分析対象の通信ログを適切に絞り込んで効率良く分析することは、通信の検査に関わらず、広く情報処理の様々な分野で要請されている。
【０００６】
本発明は、通信ログの分析において、検出された不正通信をもとに別の不正通信の調査を効率良く行うことを目的とする。
【課題を解決するための手段】
【０００７】
かかる目的のもと、本発明は、監視対象とするネットワーク上で対象期間内に検知され

た通信の通信ログを取得する取得手段と、取得手段が取得した通信ログをもとに不正通信が検出された場合に、取得手段が取得した通信ログの中から、通信元が不正通信の通信元と同一の通信で、不正通信の発生状況をもとに特定された特定期間内に検知された通信の通信ログを抽出する抽出手段とを備える、情報処理装置を提供する。

また、特定期間は、対象期間内に通信元にて不正通信が最初に発生した時点から最後に発生した時点までの期間をもとに特定されるもの、であってよい。

さらに、抽出手段は、検出された不正通信の通信元が複数存在する場合、通信元ごとに、通信元が不正通信の通信元と同一の通信で、不正通信の発生状況をもとに特定された特定期間内に検知された通信の通信ログを抽出するもの、であってよい。

そして、抽出手段は、抽出手段が抽出した通信ログをもとに別の不正通信が検出された場合に、取得手段が取得した通信ログの中から、通信元が別の不正通信の通信元と同一の通信で、別の不正通信の発生状況をもとに特定された特定期間内に検知された通信の通信ログを抽出するもの、であってよい。

また、本発明は、監視対象とするネットワーク上で対象期間内に検知された通信の通信ログを取得する取得手段と、取得手段が取得した通信ログをもとに不正通信が検出された場合に、取得手段が取得した通信ログの中から、不正通信の通信ログにおけるマルウェアの作成傾向に沿う情報と同じものが含まれる通信ログを抽出する抽出手段とを備える、情報処理装置も提供する。

さらに、本発明は、監視対象とするネットワーク上で対象期間内に検知された通信の通信ログを取得するステップと、取得された通信ログをもとに不正通信が検出された場合に、取得された通信ログの中から、通信元が不正通信の通信元と同一の通信で、不正通信の発生状況をもとに特定された特定期間内に検知された通信の通信ログを抽出するステップとを含む、情報処理方法を提供する。

そして、本発明は、監視対象とするネットワーク上で対象期間内に検知された通信の通信ログを取得するステップと、取得された通信ログをもとに不正通信が検出された場合に、取得された通信ログの中から、不正通信の通信ログにおけるマルウェアの作成傾向に沿う情報と同じものが含まれる通信ログを抽出するステップとを含む、情報処理方法も提供する。

また、本発明は、コンピュータに、監視対象とするネットワーク上で対象期間内に検知された通信の通信ログを取得する機能と、取得された通信ログをもとに不正通信が検出された場合に、取得された通信ログの中から、通信元が不正通信の通信元と同一の通信で、不正通信の発生状況をもとに特定された特定期間内に検知された通信の通信ログを抽出する機能とを実現させるための、プログラムを提供する。

さらに、本発明は、コンピュータに、監視対象とするネットワーク上で対象期間内に検知された通信の通信ログを取得する機能と、取得された通信ログをもとに不正通信が検出された場合に、取得された通信ログの中から、不正通信の通信ログにおけるマルウェアの作成傾向に沿う情報と同じものが含まれる通信ログを抽出する機能とを実現させるための、プログラムも提供する。

【発明の効果】

【０００８】

本発明によれば、通信ログの分析において、検出された不正通信をもとに別の不正通信の調査を効率良く行うことができる。

【図面の簡単な説明】

【０００９】

【図１】本実施の形態が適用されるコンピュータシステムの全体構成例を示した図である。

【図２】本実施の形態に係る通信分析装置の機能構成例を示したブロック図である。

【図３】通信分析装置を適用するのに好適なコンピュータのハードウェア構成の一例を示した図である。

【図４】通信分析装置を用いて不正通信を検出するための全体的な処理の手順の一例を示

したフローチャートである。
【図５】（ａ）、（ｂ）は、分析対象とする通信ログに分類リストを適用した結果の出力例を示す図である。
【図６】（ａ）、（ｂ）は、分析対象とする通信ログに分類リストを適用した結果の出力例を示す図である。
【図７】該当する通信ログの各分類リストでの発生状況の出力例を示す図である。
【図８】分析処理及び不正通信を特定する処理の手順の一例を示したフローチャートである。
【図９】不正通信の深堀り調査を行う処理の手順の一例を示したフローチャートである。
【図１０】不正通信の発生要因を特定するために表示される通信ログの一例を示す図である。
【図１１】（ａ）、（ｂ）は、元の不正通信をもとに通信ログを絞って分類リストを適用した出力結果の一例について説明するための図である。
【図１２】別の不正通信の調査手順の一例について説明するための図である。
【図１３】別の不正通信の調査を行う処理の手順の一例を示したフローチャートである。
【発明を実施するための形態】
【００１０】
以下、添付図面を参照して、本発明の実施の形態について詳細に説明する。
＜システム構成＞
まず、本実施の形態が適用されるコンピュータシステムについて説明する。図１は、本実施の形態が適用されるコンピュータシステムの全体構成例を示した図である。図示するように、このコンピュータシステムでは、クライアント端末１０ａ、１０ｂ、１０ｃが社内ＬＡＮ（Local Area Network）５０に接続されている。また、通信分析装置２０及び通信データ保存装置３０が、社内ＬＡＮ５０及びインターネット６０の両方に接続されている。さらに、攻撃者サーバ４０がインターネット６０に接続されている。
【００１１】
クライアント端末１０ａ、１０ｂ、１０ｃは、ユーザが使用するコンピュータであり、例えば、パーソナルコンピュータやワークステーション、その他のコンピュータ装置にて実現される。また、本実施の形態において、クライアント端末１０ａ、１０ｂ、１０ｃは、マルウェアに感染することがあるものとする。ここで、マルウェアとは、不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称である。例えば、マルウェアの一つであるボットは、コンピュータに感染した後、Ｃ＆Ｃ（コマンド＆コントロール）サーバと呼ばれる制御用サーバに接続して攻撃者からの指令を待ち、感染したコンピュータ上で指令どおりの処理を実行する。
【００１２】
なお、図１では、クライアント端末１０ａ、１０ｂ、１０ｃを示したが、これらを区別する必要がない場合にはクライアント端末１０と称することもある。また、図１には３台のクライアント端末１０しか示していないが、クライアント端末１０の台数は図示の３台には限定されない。
【００１３】
通信分析装置２０は、社内ＬＡＮ５０とインターネット６０との間のネットワークを監視対象とし、監視対象とするネットワーク上で検知された通信の通信ログ（履歴）を処理（分析）して分析結果を出力する。出力される分析結果は、外部からの不正アクセスや内部からの不正な情報流出等のような不正通信を検出するためのものである。また、分析する対象の通信ログは通信データ保存装置３０に蓄えられており、通信分析装置２０は、例えば解析者（アナリスト）の操作を契機として、通信データ保存装置３０から分析対象とする通信ログを取得して分析を行う。
【００１４】
なお、本実施の形態では、通信分析装置２０が通信データ保存装置３０から通信ログを取得する構成とするが、例えば、通信分析装置２０を社内ＬＡＮ５０とインターネット６

０との間の通信回線上にインラインで設置して、通信分析装置２０にて通信ログを保存するような構成にしても良い。また、通信分析装置２０は、ゲートウェイ等の通信装置の中に設けられても良いし、通信装置とは独立に設けられても良い。本実施の形態では、情報処理装置の一例として、通信分析装置２０が用いられる。

【００１５】

通信データ保存装置３０は、社内ＬＡＮ５０とインターネット６０との間のネットワーク上を流れる通信を通信ログとして保存する。保存される通信ログは、例えば、クライアント端末１０から社内ＬＡＮ５０を介してインターネット６０へアクセスする際に経由するように設置されたプロキシサーバ（不図示）にて生成されるログである。また、例えば、社内ＬＡＮ４０に接続された、ＩＤＳ（Intrusion Detection System）やＩＰＳ（Intrusion Prevention System）等のセキュリティ・システム、ファイアウォール等のソフトウェアが搭載された装置などが生成するログも、通信ログとして保存される。

【００１６】

また、通信データ保存装置３０は、通信ログ以外に、社内ＬＡＮ５０とインターネット６０との間のネットワーク上を流れるパケットデータについても保存している。ここで、通信ログはネットワーク上での通信を記録するものであり、通信ログには、例えば、通信先の情報、通信元の情報、通信が行われた日時等の情報が含まれている。一方で、パケットデータには、例えば、実際にやり取りされたファイルや画像データの中身など、通信ログからは把握できない情報も存在する。

【００１７】

攻撃者サーバ４０は、マルウェアに感染したクライアント端末１０が通信の接続先とするサーバであり、攻撃者が運営しているものである。この攻撃者サーバ４０は、例えばクライアント端末１０がボットに感染した場合には、クライアント端末１０が攻撃者からの指令を待つために接続する接続先の制御用サーバに該当する。また、図１には１台の攻撃者サーバ４０しか示していないが、２台以上の攻撃者サーバ４０が存在する場合もあるものとする。

【００１８】

社内ＬＡＮ５０は、会社内のコンピュータやプリンタを専用回線等で接続し、これらの間でデータを送受信できるようにしたネットワークである。

【００１９】

インターネット６０は、ＴＣＰ／ＩＰ（Transmission Control Protocol／Internet Protocol）を用いて全世界のネットワークを相互に接続した巨大なネットワークである。

【００２０】

そして、本実施の形態において、クライアント端末１０は、マルウェアに感染した場合、攻撃者サーバ４０などの不正なサーバに接続して処理を行う。そこで、本実施の形態に係る通信分析装置２０は、社内ＬＡＮ５０とインターネット６０との間のネットワークを監視対象とし、監視対象であるネットワーク上で検知された通信の通信ログを分析して分析結果を出力する。通信分析装置２０の分析により、監視対象であるネットワーク上で検知された通信は、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ものと、不正な通信である可能性のあるもの（問題のない通信と特定できないもの）とが含まれる。解析者は、通信分析装置２０にて出力された分析結果に基づき、問題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。

【００２１】

＜通信分析装置の機能構成＞

次に、通信分析装置２０の機能構成について説明する。図２は、本実施の形態に係る通信分析装置２０の機能構成例を示したブロック図である。

【００２２】

図示するように、通信分析装置２０は、表示部２１と、通信ログ取得部２２と、通信ログ整形部２３と、分類リスト適用部２４と、リスト格納部２５と、詳細情報取得部２６と

、不正通信調査部２７とを備えている。
【００２３】
表示部２１は、通信分析装置２０での分析結果等の各種情報を画面に表示する。また、表示部２１は、画面に対する解析者からの操作入力を受け付ける。
【００２４】
取得手段の一例としての通信ログ取得部２２は、社内ＬＡＮ５０とインターネット６０との間のネットワークを監視対象とし、監視対象とするネットワーク上で検知された通信の通信ログを通信データ保存装置３０から取得する。ここで、通信ログ取得部２２は、例えば解析者が指定した期間や予め定められた期間を取得の対象期間として、その対象期間内に検知された通信ログを取得する。
【００２５】
通信ログ整形部２３は、通信ログ取得部２２が取得した通信ログについて、分析処理を実行できるように通信ログの形式を整える。また、通信ログ整形部２３は、通信ログに含まれる情報の中で分析に不要な情報の除外や削除を行う。
【００２６】
分類リスト適用部２４は、通信ログ整形部２３にて整形された通信ログに対して分類リストを適用する。そして、分類リスト適用部２４は、分類リストの適用結果を分類リストごとに表示部２１に表示する。また、分類リスト適用部２４は、分類リストごとの適用結果の相関を示す情報を表示部２１に表示する。これらの表示された情報は、解析者が不正通信を特定するために用いられる。分類リストは、問題のある通信を検出するための予め定められた条件（以下、分類条件と称する）が設定されたリストであり、解析者等により予め作成される。分類リストの詳細については後述する。
【００２７】
リスト格納部２５は、複数の分類リストを格納する。
【００２８】
詳細情報取得部２６は、不正通信の可能性がある通信ログに関して、詳細な情報を取得する。ここで、詳細情報取得部２６は、例えば、不正通信の可能性がある通信ログにおける通信先の情報を収集する。また、詳細情報取得部２６は、不正通信の可能性がある通信ログに対応するパケットデータを、通信データ保存装置３０から取得する。これらの通信先の情報やパケットデータの情報は、解析者が不正通信を特定するために用いられる。
さらに、詳細情報取得部２６は、解析者により不正通信が特定された場合に、特定された不正通信の情報を収集し、不正通信の深堀り調査を行う。深堀り調査では、不正通信の通信元の情報や、発生期間、発生要因などに関する情報が収集される。
【００２９】
抽出手段の一例としての不正通信調査部２７は、解析者により特定された不正通信に基づいて、別の不正通信の有無を調査する。
【００３０】
＜通信分析装置のハードウェア構成例＞
次に、本実施の形態に係る通信分析装置２０のハードウェア構成について説明する。図３は、通信分析装置２０を適用するのに好適なコンピュータのハードウェア構成の一例を示した図である。図示するように、通信分析装置２０は、演算手段であるＣＰＵ（Central Processing Unit）２０ａと、主記憶手段であるメモリ２０ｃを備える。また、外部デバイスとして、磁気ディスク装置（ＨＤＤ：Hard Disk Drive）２０ｇ、ネットワークインターフェイス２０ｆ、ディスプレイ装置を含む表示機構２０ｄ、音声機構２０ｈ、キーボードやマウス等の入力デバイス２０ｉ等を備える。
【００３１】
図３に示す構成例では、メモリ２０ｃおよび表示機構２０ｄは、システムコントローラ２０ｂを介してＣＰＵ２０ａに接続されている。また、ネットワークインターフェイス２０ｆ、磁気ディスク装置２０ｇ、音声機構２０ｈおよび入力デバイス２０ｉは、Ｉ／Ｏコントローラ２０ｅを介してシステムコントローラ２０ｂ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。
【００３２】
また、図３において、磁気ディスク装置２０ｇ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２０ｃに読み込まれてＣＰＵ２０ａに実行されることにより、本実施の形態に係る通信分析装置２０の各機能部の機能が実現される。
【００３３】
なお、図３は、本実施の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。本実施の形態は、通信ログを分析することが可能な情報処理装置に広く適用できるものであり、図示の構成においてのみ本実施の形態が実現されるのではない。
【００３４】
＜不正通信を検出する全体手順＞
次に、通信分析装置２０を用いて不正通信を検出するための全体的な処理の手順について説明する。図４は、通信分析装置２０を用いて不正通信を検出するための全体的な処理の手順の一例を示したフローチャートである。
【００３５】
まず、解析者の入力をもとに、通信分析装置２０は、通信ログの分析を行うための事前設定を行う（ステップ１）。次に、通信分析装置２０は、事前設定に基づいて、通信データ保存装置３０から分析対象とする通信ログを取得し、取得した通信ログの整形を行う（ステップ２）。そして、通信分析装置２０は、整形後の通信ログに対して、分類リストを適用して分析処理を実行する（ステップ３）。この分析処理の実行により、分析結果が表示される。
【００３６】
その後、解析者は、表示された分析結果を確認し、不正通信を特定する（ステップ４）。次に、通信分析装置２０は、ステップ４で不正通信と特定された通信ログに絞り、深堀り調査を実行する（ステップ５）。ここでは、不正通信に関する詳細な情報が収集され、不正通信の発生期間や発生要因などが判断される。次に、通信分析装置２０は、ステップ４で特定された不正通信をキーにして、別の不正通信の有無を調査する（ステップ６）。ここで別の不正通信が見つかった場合には、通信分析装置２０は、ステップ５と同様に別の不正通信についても深掘り調査を行う。そして、本処理フローは終了する。
【００３７】
このようにして、通信分析装置２０は、通信データ保存装置３０から取得した通信ログをもとに分析処理を実行し、分析結果を表示する。そして、解析者は、表示された分析結果を確認して不正通信の特定を行う。また、通信分析装置２０は、解析者に特定された不正通信の深堀り調査を実行する。さらに、通信分析装置２０は、解析者に特定された不正通信をキーにして、別の不正通信の有無を調査する。
以下では、図４に示す各ステップについて、より具体的に説明を行う。
【００３８】
＜ステップ１：事前設定＞
図４のステップ１に示す事前設定について詳細に説明する。この事前設定では、解析者の入力により、分析対象とする通信ログの種類やログ形式の指定、分析処理で用いられる分類リストの指定などが行われる。
【００３９】
具体的には、解析者の入力をもとに、通信分析装置２０は、分析対象とする通信ログの種類として、例えば、プロキシログ（プロキシサーバの通信ログ）、ファイアウォールの通信ログなど、どの種類の通信ログを分析対象とするかを指定する。また、通信分析装置２０は、分析対象とする通信ログのログ形式として、例えば、日時を記述する基準（西暦か和暦か等）や書式の指定、ＩＰアドレスの表記法（記数法）の指定を行う。
さらに、分析処理で用いられる分類リストには、適用可能な通信ログの種類がそのリス

トごとに決まっている。そのため、分析対象とする通信ログの種類に合わせて解析者が指定することにより、通信分析装置２０は、複数の分類リストの中から、分析処理で用いる分類リストを指定する。

【００４０】

また、事前設定としてほかに、通信分析装置２０は、例えば、分析の対象とする期間、即ち、発生した日時がいつからいつまでの通信ログを分析の対象とするかを指定したり（以下、ここで分析対象として設定された期間を全分析期間と称する）、後述するホワイトリストの使用有無を指定したりする。

【００４１】

＜ステップ２：通信ログの整形＞

図４のステップ２に示す通信ログの整形について詳細に説明する。通信ログの整形処理に際し、まず、通信ログ取得部２２は、全分析期間内に発生した通信ログのうち、事前設定により指定された種類の通信ログを、通信データ保存装置３０から取得する。そして、通信ログ整形部２３は、取得した通信ログに対して整形処理を行う。

【００４２】

整形処理では、事前設定で解析者が指定した規則や予め定められた規則に基づいて、通信ログの形式が整えられる。例えば、通信ログにおける発生日時、通信元ＩＰアドレス、宛先ＩＰアドレスなどが共通の形式に整えられる。また、例えば、通信ログに含まれる情報のうち、不正通信の検出には関係ない情報で分析処理に使用されない情報が削除される。さらに、例えば、コネクション型のプロトコルであるＴＣＰを用いる通信に関しては、データのリクエストとそれに応答するレスポンスとを１つの通信ログにまとめる処理等が行われる。

【００４３】

また、ステップ１の事前設定でホワイトリストを使用する設定が行われている場合、通信ログ整形部２３は、通信ログに対してホワイトリストを適用する。このホワイトリストは、解析者等により予め作成されたものであり、問題のない通信が登録されたリストである。例えば、問題のない外部のＩＰアドレスやホスト名（ドメイン名）などの情報がホワイトリストに登録されている。ホワイトリストを適用することで、ホワイトリストの情報に合致する情報を有する通信ログは、分析対象から除外される。付言すると、ホワイトリストは、分析対象の通信から問題のない通信を除外して、問題のある通信を残すためのリストである。即ち、ホワイトリストは、登録されている情報と同じ情報を含む通信ログを除外して問題のある通信ログを検出する、という分類条件が設定された分類リスト、と捉えることができる。

【００４４】

＜ステップ３：分析処理＞

図４のステップ３に示す分析処理について詳細に説明する。この分析処理では、ステップ２で整形された通信ログに対して分類リストが適用され、不正通信を検出するための情報が出力される。分析処理で適用される分類リストは、予め作成された複数の分類リストのうち、ステップ１の事前設定で指定されたものである。ここで、分類リストとしては、例えば、問題のある通信に関する情報が登録されており、登録されている情報と同じ情報を含む通信ログを抽出するという分類条件が定められたリスト（以下、ブラックリストと称する）が存在する。また、分類リストとしては、例えば、解析者がこれまでに不正通信として特定された通信の特徴を考慮し、不正通信の判定のために有用なものとして指定された項目（フィールド）を含む通信ログを抽出するという分類条件が定められたリスト（以下、フィールド抽出リストと称する）も存在する。

【００４５】

ブラックリストに登録された問題のある通信に関する情報とは、例えば、ユーザに関する情報を収集して外部に送信するソフトウェアであるスパイウェアの情報、広告を目的とするソフトウェアであるアドウェアの情報等である。また、例えば、公開プロキシに関する情報の一覧などもブラックリストとして用いられる。公開プロキシとは、一般に公開さ

れ誰でも自由に使える中継サーバ（プロキシサーバ）である。さらに、ブラックリストとして、解析者が独自に収集した問題のある通信の情報や、これまでの分析により問題があると判断された通信の情報などが登録されたリストを用いても良い。

【００４６】

また、フィールド抽出リストには、例えば、「ＨＴＴＰ（Hypertext Transfer Protocol）通信でＰＯＳＴメソッドを用いた通信ログについて、通信先ホストを出現回数順にソートする」という分類条件が定められている。別のフィールド抽出リストには、例えば、「ＨＴＴＰ通信でＧＥＴメソッドまたはＰＯＳＴメソッドを用いた通信ログについて、通信元ホスト及び通信先ホストを出現回数順にソートする」という分類条件が定められている。

【００４７】

また、分類リストには、その内容に応じて、不正通信を検出するための重要度が設定されている。重要度は、例えば、「高」、「中」、「低」の３段階で設定される。ブラックリストの場合、例えば、解析者が独自に収集した問題のある通信の情報は、不正と判断できる信頼度が高いため、そのブラックリストは重要度「高」と設定される。また、例えば、攻撃以外の用途でも使われるような正規の通信が含まれてしまう可能性のある分類リストや影響が小さい分類リストは、重要度を「中」、「低」と低く設定しても良い。

【００４８】

また、フィールド抽出リストの場合、例えば、不正通信の可能性が高い通信について、そのような分類条件を定めたフィールド抽出リストは重要度「高」と設定される。一方、例えば、不正通信の可能性が低い通信について、そのような分類条件を定めたフィールド抽出リストは重要度「低」と設定される。

さらに、ＨＴＴＰ通信のＰＯＳＴメソッドやＧＥＴメソッドは、例えばＷｅｂサーバへ送るリクエストとして一般に用いられるものであるが、マルウェアに感染した場合に不正な処理として用いられる場合も多い。このようなことに基づいて、フィールド抽出リストの重要度が設定される。

【００４９】

そして、分類リスト適用部２４は、整形後の通信ログに対して分類リストを適用し、分類リストごとに適用結果を出力する。ここで、各分類リストには、その分類リストを適用可能な通信ログの種類、及び分類リストを適用する上で必要な通信ログのフィールドが設定されている。そのため、分類リストの適用に際し、分類リスト適用部２４は、整形後の通信ログから、その分類リストを適用可能な種類の通信ログを抽出する。さらに、分類リスト適用部２４は、抽出した各通信ログから、その分類リストを適用する上で必要なフィールドの情報を収集し、収集した情報が分類条件に合致するか否かを判断して、適用結果を出力する。

【００５０】

例えば、分類リストとしてブラックリストを適用する場合、分類リスト適用部２４は、整形後の通信ログから、そのブラックリストを適用可能な種類の通信ログを抽出する。さらに、分類リスト適用部２４は、抽出した各通信ログから、そのブラックリストを適用する上で必要なフィールドの情報を収集する。そして、分類リスト適用部２４は、収集した各通信ログのフィールドの情報がブラックリストの情報に合致するか否かを、通信ログごとに順番に判断していく。その結果、分類リスト適用部２４は、ブラックリストごとに、ブラックリストの情報と同じ情報を含む通信ログを抽出し、出現回数（分析対象の期間内に記録されている通信ログの数）が多い順番に上から並べて出力する。

【００５１】

また、例えば、分類リストとしてフィールド抽出リストを適用する場合、分類リスト適用部２４は、まず、整形後の通信ログを、ＨＴＴＰ、ＳＳＬ、ＦＴＰ（File Transfer Protocol）、ＤＮＳ（Domain Name System）などの通信で用いられたプロトコル別に分けて、ベースファイルを作成する。このベースファイルでは、通信ログのフィールドのうち、分析に用いられる可能性のあるフィールドがプロトコルごとに設定されている。即ち、分

類リスト適用部２４は、整形後の通信ログをプロトコル別に区分けし、分析に用いられる可能性のあるフィールドをプロトコルに応じて各通信ログから抽出して、プロトコル別のベースファイルを作成する。

【００５２】

さらに、分類リスト適用部２４は、必要に応じてさらにベースファイルを分割し、中間ファイルを作成する。例えば、ＨＴＴＰ通信では、ＧＥＴメソッドやＰＯＳＴメソッドなどのメソッドが用いられるが、このメソッドが分類条件の要素として用いられる場合がある。そのため、分析を効率良く行うために、ＨＴＴＰのベースファイルをさらにメソッド別に分割した中間ファイルも作成される。

【００５３】

そして、分類リスト適用部２４は、整形後の通信ログ（ここでは、ベースファイルや中間ファイル）から、そのフィールド抽出リストを適用可能な種類の通信ログを抽出する。さらに、分類リスト適用部２４は、抽出した各通信ログから、そのフィールド抽出リストを適用する上で必要なフィールドの情報を収集する。そして、分類リスト適用部２４は、収集した各通信ログのフィールドの情報がフィールド抽出リストの分類条件に合致するか否かを、通信ログごとに順番に判断していく。その結果、分類リスト適用部２４は、フィールド抽出リストごとに、分類条件を満たす通信ログを抽出して、出現回数が多い順番に上から並べて出力する。

【００５４】

図５（ａ）、（ｂ）は、分析対象とする通信ログに分類リストを適用した結果の出力例を示す図である。ここでは、重要度「中」であるブラックリストを適用した出力結果を示している。図５（ａ）に示す例では、ブラックリストを適用する上で必要なフィールドとして、「ホスト名（通信先のホスト名）」が設定されている。その結果、図示するように、通信ログの「出現回数」、「ホスト名」が対応付けられて出力され、出現回数の多い通信ログから順番に表示される。

【００５５】

例えば、番号１には、通信先のホスト名が「aaa.abcd0.jp」である通信ログが示されている。ここで、図５（ａ）に示す例のブラックリストには、問題のある通信の情報として、例えば、通信先のホスト名に「abcd0.jp」が含まれるもの、という情報が登録されており、番号１の通信ログが抽出される。また、この通信ログの出現回数は「１３４８２」であり、分析対象とする通信ログにおいて、該当する通信ログが１３４８２個存在していることになる。さらに、図５（ａ）に示す例では、ブラックリストの情報に合致する箇所（番号１の通信ログでは、「abcd0.jp」）を解析者が認識し易いように、合致する箇所に下線を引いて表示されている。ただし、下線を引いて表示する構成に限られず、例えば、他の箇所とは違う色（例えば、他の箇所が黒色の場合に赤色）で表示したり、文字を大きくして表示したりしても良い。

【００５６】

また、図５（ｂ）も、重要度「中」である別のブラックリストを適用した出力結果を示しており、ここでは、ブラックリストを適用する上で必要なフィールドとして、「ＵＲＬ（Uniform Resource Locator）」が設定されている。その結果、図示するように、通信ログの「出現回数」、「ＵＲＬ」が対応付けられて出力され、出現回数の多い通信ログから順番に表示される。例えば、番号１には、通信先のＵＲＬが「http://ccc.abcd1.net/00/11」である通信ログが示されている。ここで、図５（ｂ）に示す例のブラックリストには、問題のある通信の情報として、例えば、通信先のＵＲＬに「abcd1.net」が含まれるもの、という情報が登録されており、番号１の通信ログが抽出される。また、この通信ログの出現回数は「２７３３」であり、分析対象とする通信ログにおいて、該当する通信ログが２７３３個存在していることになる。

【００５７】

図６（ａ）、（ｂ）も、分析対象とする通信ログに分類リストを適用した結果の出力例を示す図である。図６（ａ）は、「ＨＴＴＰ通信でＧＥＴメソッドを用いた通信ログにつ

いて、ホスト名（通信先のホスト名）を出現回数順にソートする」という分類条件を定めたフィールド抽出リストを適用した出力結果を示す。図示するように、通信ログの「出現回数」、「ホスト名」が対応付けられて出力され、出現回数の多い通信ログから順番に表示される。

【００５８】

例えば、番号１には、通信先ホストのホスト名が「aaa.office.sample1.com」である通信ログが示されている。また、メソッドは表示されていないが、ＧＥＴメソッドが用いられている。この通信ログの出現回数は「２９０９７３７」であり、分析対象とする通信ログにおいて、該当する通信ログが２９０９７３７個存在していることになる。

【００５９】

また、図６（ｂ）は、「ＨＴＴＰ通信でＧＥＴメソッドを用いた通信ログについて、通信元ＩＰアドレス及び通信先ホストを出現回数順にソートする」という分類条件を定めたフィールド抽出リストを適用した出力結果を示す。図示するように、通信ログの「出現回数」、「通信元ＩＰアドレス」、「メソッド」、「通信先ホスト（ホスト名）」が対応付けられて出力されており、出現回数の多い通信ログから順番に表示される。

【００６０】

＜ステップ４：不正通信の特定＞

図４のステップ４に示す不正通信を特定する処理について説明する。不正通信を特定する処理では、解析者が、ステップ３の出力内容を確認し、不正と判断される通信を特定する。ここで、ステップ３では、上述したように、分析対象の通信ログに適用された分類リストの分析結果が出力されるが、分析結果に示されている通信ログを解析者が選択すると、選択した通信ログに関して、複数の異なる分類リストの適用結果の相関を示す情報が出力される。付言すると、解析者が選択した通信ログについて、その通信ログの通信先と同じ通信先を有する通信ログが、各分類リストでどのように発生しているかを示す情報が出力される。解析者は、これらの出力内容を確認して不正通信を特定する。

【００６１】

また、詳細情報取得部２６は、解析者が不正通信を特定するために、不正通信の可能性がある通信ログにおける通信先の情報を収集する。ここで、表示部２１は、通信先の情報を収集することを受け付ける入力インターフェイスとなっている。解析者が、表示部２１に表示された通信ログの１つを選択することにより、選択された通信ログにおける通信先の情報が収集される。具体的には、解析者が通信ログの１つを選択すると、詳細情報取得部２６は、例えば、その通信ログにおける通信先に実際に接続を行い、現在も通信可能であるか、通信先のサイトが現時点も実在しているか等の情報を収集する。

【００６２】

さらに、詳細情報取得部２６は、必要に応じて通信ログに対応するパケットデータを通信データ保存装置３０から取得する。ここでも、表示部２１は、通信ログに対応するパケットデータを取得することを受け付ける入力インターフェイスとなっている。具体的には、解析者が、ある通信ログでパケットデータを取得する選択を行うと、詳細情報取得部２６は、通信データ保存装置３０からパケットデータを取得する。これにより、解析者は、パケットデータの中身を確認し、パケットデータに含まれるファイルや画像に不正なものがあるか否か等を判断することができる。

【００６３】

このようにして、解析者は、複数の分類リストの分析結果から判断される状況と、通信ログにおける通信先やパケットデータの情報とをもとにして、分析対象の通信が不正通信であるか否かの最終判断を行う。ここでは、不正通信か否か現時点では判断できない場合や正常な通信（不正ではない通信）と判断される場合もある。そのため、ステップ４の処理では、分析対象の通信が、不正通信と判断されるもの、不正通信か否か現時点では判断できないもの、正常な通信と判断されるものの３つのいずれかに区分される。

【００６４】

そして、不正通信と判断されるものについては、次のステップ５及びステップ６の処理

が行われる。また、不正通信と判断された場合に、その通信の情報をステップ３の分析処理で用いられるブラックリストに追加しても良い。

また、不正通信か否か現時点では判断できないものについては、継続して監視する対象とされ、要経過観察リストに追加される。そして、今回の全分析期間とは異なる期間の通信ログを対象に分析が行われた場合に、要経過観察リストに記録された通信ログと同じ通信先への通信が発生しているか否か等が確認される。このように継続して監視されることにより、最終的に不正通信と判断されるか、または正常な通信と判断されることとなる。

さらに、正常な通信と判断されるものについては、その通信の情報をステップ２の整形で用いられるホワイトリストに追加しても良い。

【００６５】

ステップ４の不正通信を特定する処理について、具体例を示して説明する。

まず、図５（ａ）に示すブラックリストの適用結果では、番号２８０の通信ログとして、ホスト名「malware.abcd4.jp」の通信ログが抽出されている。また、図５（ｂ）に示すブラックリストの適用結果では、番号３５０の通信ログとして、ＵＲＬ「http://malware.abcd4.jp/」の通信ログが抽出されている。これらは共通の通信先を示しており、共に５７件の出現回数で、図５（ａ）では２８０行目、図５（ｂ）では３５０行目に存在が確認される。ただし、他の上位にある通信ログと比較すると、それほど出現回数が多い通信先とはいえない。またこれらのブラックリストの重要度は「中」であるため、抽出された段階で不正通信の通信ログと断定されるものではない。そのため、図５（ａ）、（ｂ）に示すブラックリストの適用結果では、解析者は、この通信先（ホスト名：malware.abcd4.jp）が不正通信に関するものであるかの判断がまだ行えない。

【００６６】

一方、他の分類リストにおいても、「malware.abcd4.jp」に該当する通信ログが抽出されている。例えば、図６（ａ）に示すフィールド抽出リストでは、番号１５３２にて該当する通信ログが抽出されている。また、図６（ｂ）に示すフィールド抽出リストでは、番号９８６６にて該当する通信ログが抽出されている。ここで、解析者が、ブラックリストの適用結果として示された「malware.abcd4.jp」の通信ログを選択すると、分類リストの適用結果の相関を示す情報として、分類リスト適用部２４は、「malware.abcd4.jp」に該当する通信ログについて、同じ通信先を有する通信ログの各分類リストでの発生状況を出力する。

【００６７】

図７は、該当する通信ログの各分類リストでの発生状況の出力例を示す図である。図示するように、「malware.abcd4.jp」に該当する通信ログについては、番号１～６の６つの分類リストが該当した。ここで、番号１、２の分類リストは、図５（ａ）、図５（ｂ）に示すブラックリストである。また、番号３～６の分類リストはフィールド抽出リストであり、４つのＧＥＴ系列のフィールド抽出リストが該当した。ここで、番号３の「リスト３」、番号４の「リスト４」はそれぞれ、図６（ａ）、図６（ｂ）に示すフィールド抽出リストである。また、番号５の「リスト５」は、「ＨＴＴＰ通信でＧＥＴメソッドを用いた通信ログについて、通信元ＩＰアドレス、通信先ホスト及びＵＲＬを出現回数順にソートする」という分類条件が定められたフィールド抽出リストである。さらに、番号６の「リスト６」は、「ＨＴＴＰ通信でＧＥＴメソッドを用いた通信ログについて、ＵＲＬを出現回数順にソートする」という分類条件が定められたフィールド抽出リストである。

【００６８】

この出力結果から、「malware.abcd4.jp」について、例えば、ＨＴＴＰのＧＥＴ通信のみ発生していること、通信元ＩＰアドレスが「172.29.36.209」で１つであるため誰もが閲覧するようなサイトではないことが判断される。また、例えば、ＵＲＬのパターンが１種類であるためＷｅｂブラウジングされている可能性が低いことが判断される。

即ち、図５に示すブラックリストの分析結果だけでは、その通信は個人がサイトを閲覧している通信である可能性もあり、不正通信に関するものであるかの判断が行えない。しかし、他の分類リストの出力結果から、個人によるサイト閲覧の通信である可能性は低く

、不正通信である可能性が高いと判断される。

【００６９】

さらに、詳細情報取得部２６が、通信先のＵＲＬ「http://malware.abcd4.jp」に実際にアクセスした場合の状況も考慮し、解析者は、最終的に不正通信と判断することができた。付言すると、「malware.abcd4.jp」にアクセスするクライアント端末１０は、マルウェアに感染している可能性が高いと判断されたこととなる。

【００７０】

このように、解析者は、ある分類リストにて抽出された通信ログについて、他の分類リストでの分析結果も合わせて確認することにより、ある分類リストからは判断できない情報を入手することができる。さらに、解析者は、必要に応じて通信先等の情報も考慮して、対象とする通信が不正通信であるか否かの最終判断を行う。

【００７１】

また、図７に示す例では、ブラックリストの適用結果として示された通信ログについて、各分類リストの適用結果の相関を示す情報を出力したが、解析者が、フィールド抽出リストの適用結果として示された通信ログを選択すると、その通信ログについて、各分類リストの適用結果の相関を示す情報が出力される。また、相関を示す情報として、該当する全ての分類リストでの発生状況を示したが、分類リストの一部、例えば、ブラックリストでの発生状況（図７の例では、番号１、２）のみ示したり、フィールド抽出リストでの発生状況（図７の例では、番号３～６）のみ示したりしても良い。

【００７２】

さらに、分類リスト適用部２４は、解析者の入力によらず、分類リストにて抽出された通信ログのうち一定の条件を満たす通信ログについて、分類リストの適用結果の相関を示す情報を出力することとしても良い。例えば、分類リスト適用部２４は、いずれかの分類リストの適用結果に含まれる通信ログのうち、出現回数が予め定められた数以下の通信ログについて、不正通信に関するものであるかの判断が行えないとして、各分類リストでの発生状況を出力しても良い。また、例えば、分類リスト適用部２４は、一定の重要度以下の分類リスト（例えば、重要度「中」以下の分類リストの場合は、重要度「中」、「低」の分類リスト）の適用結果に含まれる通信ログは、不正通信に関するものであるかの判断が行えないとして、各分類リストでの発生状況を出力しても良い。

【００７３】

ステップ３の分析処理及びステップ４の不正通信を特定する処理について、フローチャートを示して説明する。図８は、分析処理及び不正通信を特定する処理の手順の一例を示したフローチャートである。

【００７４】

まず、ステップ２で通信ログの整形が行われると、分類リスト適用部２４は、分析処理で用いると指定された分類リストをリスト格納部２５から取得する（ステップ１０１）。そして、分類リスト適用部２４は、整形後の通信ログに対して分類リストを適用する（ステップ１０２）。ここで、分類リスト適用部２４は、取得した分類リストごとに、整形後の通信ログから適用可能な種類の通信ログを抽出し、分類リスト適用に必要なフィールドの情報を収集して、分類リストの分類条件に合致するか否かを判断する。そして、分類リスト適用部２４は、分類リストごとに分析結果を出力して表示部２１に表示する。

【００７５】

次に、例えば解析者が分類リストによる分析結果を確認し、不正通信に関するものであるかまだ判断できないような通信ログを選択すると、分類リスト適用部２４は、選択された通信ログの各分類リストでの発生状況を表示部２１に表示する（ステップ１０３）。ここで、分類リスト適用部２４は、分類リストの分析結果の中から、解析者に選択された通信ログの通信先と同じものを通信先とする通信ログを抽出し、抽出した通信ログの発生状況を表示部２１に表示する。

【００７６】

さらに、解析者が、通信ログにおける通信先の情報を収集する入力やパケットデータを

取得する入力を行うと、詳細情報取得部２６は、通信先に関する情報を取得し、またパケットデータを通信データ保存装置３０から取得する（ステップ１０４）。取得した情報は表示部２１に表示される。そして、本処理フローは終了する。

このように、分類リスト適用部２４、詳細情報取得部２６による出力内容をもとに、解析者は、分析対象の通信が不正通信であるか否かの最終判断を行う。

【００７７】

＜ステップ５：不正通信の深堀り調査＞

図４のステップ５に示す不正通信の深掘り調査について説明する。不正通信の深掘り調査では、ステップ４で不正通信と判断された通信ログに絞って詳細な情報が収集される。ステップ４で不正通信と判断されたものが複数あれば、それぞれの不正通信に対してステップ５の処理が行われる。

【００７８】

まず、詳細情報取得部２６は、分析対象の通信ログの中から、ステップ４で不正通信と判断された通信の通信ログを抽出する。そして、詳細情報取得部２６は、抽出した各通信ログの発生日時を取得し、この不正通信の発生期間を特定する。発生期間は、全分析期間内で、最初に不正通信が発生した時点から最後に不正通信が発生した時点までの期間である。

また、詳細情報取得部２６は、不正通信の通信元を特定する。具体的には、詳細情報取得部２６は、不正通信の通信ログにおいて、通信元のＩＰアドレスやホストの情報、即ち、通信元であるクライアント端末１０の情報を収集する。通信元のクライアント端末１０としては、１つの場合もあれば複数の場合もある。

【００７９】

さらに、詳細情報取得部２６は、不正通信の発生要因を特定するための情報を収集する。ここで、不正通信は、例えば、クライアント端末１０がマルウェアをダウンロードさせる不正なＷｅｂページにアクセスするなど、何らかの通信が要因となって発生すると考えられる。即ち、不正通信が最初に発生した時刻の直前の時間に、不正通信の発生要因となる何らかの通信が行われていると考えられる。そこで、詳細情報取得部２６は、不正通信の通信元であるクライアント端末１０から行われた通信の通信ログのうち、不正通信が最初に発生した時点より遡って予め定められた時間内に検知された通信の通信ログを収集する。

【００８０】

ステップ５の不正通信の深堀り調査について、フローチャートを示して説明する。図９は、不正通信の深堀り調査を行う処理の手順の一例を示したフローチャートである。

【００８１】

まず、ステップ４において、解析者が不正通信と判断される通信の通信ログを指定する入力を行うと、詳細情報取得部２６は、分析対象の通信ログの中から、不正通信と判断された通信の通信ログを抽出する（ステップ２０１）。そして、詳細情報取得部２６は、抽出した通信ログの発生日時を取得し、不正通信の発生期間を特定する（ステップ２０２）。次に、詳細情報取得部２６は、不正通信の通信元であるクライアント端末１０の情報を収集する（ステップ２０３）。発生期間や通信元であるクライアント端末１０の情報は、表示部２１に表示される。

【００８２】

さらに、詳細情報取得部２６は、不正通信の通信元であるクライアント端末１０から行われた通信の通信ログのうち、不正通信が最初に発生した時刻の直前の予め定められた時間内に検知された通信ログを収集する（ステップ２０４）。収集された通信ログの情報は、表示部２１に表示される。そして、本処理フローは終了する。

【００８３】

次に、通信ログをもとに不正通信の発生要因を特定する処理について、具体例を示して説明する。図１０は、不正通信の発生要因を特定するために表示される通信ログの一例を示す図である。ここで、番号１３の通信ログがホスト「mal.example.com」への不正通信

であり、ホスト「mal.example.com」に対して最初に通信が行われた際の通信ログである。そして、番号１３の通信ログが検知された時刻付近の通信ログが表示されている。実際には、不正通信が最初に発生した時刻の前後の特定の時間の通信ログが表示されるが、図１０ではそのうちの一部の通信ログを示している。また、不正通信の発生要因を特定するためには、不正通信が最初に発生した時刻の前に検知された通信ログがあれば足りるが、それ以降の通信ログもあれば、不正通信の発生状況がより詳細に把握される。

【００８４】

図１０に示す例では、番号１３の通信ログより前に発生した通信ログを確認すると、番号６の通信ログのホスト宛への通信は１回しか発生していない。ここで、通信分析装置２０は、番号６の通信先のＵＲＬ「http://malware2.downloadsite.com/it/xxxxxxx.jpg」に実際に接続したところ、マルウェアのダウンロード通信であることが判明した。さらに、例えば、番号６の通信ログの前に発生している番号１～５などの複数の通信ログの通信先に、通信分析装置２０が実際に接続した結果などをもとに、解析者により、不正通信の発生要因や影響被害などが判断される。

【００８５】

＜ステップ６：別の不正通信の調査＞

図４のステップ６に示す別の不正通信の調査について説明する。別の不正通信の調査では、ステップ４で不正通信と判断されたもの（以下、元の不正通信と称する）をキーにして、別の不正通信の有無が調査される。

【００８６】

不正通信の発生には、上述したように、その要因となる何らかの通信が存在すると考えられるが、クライアント端末１０がそのような通信を行った場合、１つの不正通信だけでなく別の不正通信も発生する場合がある。例えば、クライアント端末１０が不正なＷｅｂページにアクセスしために攻撃者サーバ４０に誘導された場合、攻撃者サーバ４０に加えて、攻撃者の別サーバにも誘導されることがあり得る。この場合には、攻撃者サーバ４０へアクセスする不正通信のほかに、攻撃者の別サーバへアクセスする不正通信も発生することになる。そこで、不正通信調査部２７は、元の不正通信と通信元が同じで、元の不正通信と発生時期が近い別の不正通信がないかどうかを調査する。

【００８７】

具体的には、不正通信調査部２７は、元の不正通信の通信元であるクライアント端末１０が通信元となっている通信ログに絞って、ステップ３の分析処理を実行する。また、別の不正通信は、元の不正通信と感染源が共通しているため、発生頻度や発生タイミングなどの発生状況も元の不正通信に類似していると考えられる。そのため、別の不正通信を特定するための期間（以下、特定期間と称する場合がある）、即ち、通信ログの分析対象とする期間は、元の不正通信の発生状況に基づいて設定される。そして、この分析処理の結果に対してステップ４の処理が行われ、別の不正通信が特定される。

【００８８】

付言すると、特定期間は、元の不正通信の通信元であるクライアント端末１０にて元の不正通信が最初に発生した時点から最後に発生した時点までの発生期間をもとに特定される。特定期間は、元の不正通信の発生状況に基づいて、例えば、１週間単位や１日単位、曜日単位で設定される。なお、特定期間は、不正通信調査部２７が予め定められた規則に従って設定するか、または解析者の入力により設定される。

【００８９】

ここで、元の不正通信を特定するために行われたステップ３の分析処理では、全分析期間の全通信ログが対象とされる。一方、別の不正通信を特定するために行われる分析処理では、元の不正通信の通信元であるクライアント端末１０が通信元となっている通信ログに絞り、さらに分析対象の期間（即ち、特定期間）も元の不正通信の発生状況に合わせて設定される。そのため、ステップ６の分析処理による分析結果は、元の不正通信を特定するために行われたステップ３の分析処理による分析結果とは異なるものとなる。

【００９０】

例えば、元の不正通信を特定するために行われた分析処理の結果では、別の不正通信の通信ログがどのブラックリスト及び分類リストにも上位に表示されず、解析者が見つけられない場合がある。このような場合に、通信ログを絞って分析処理を行うことで、別の不正通信の通信ログがブラックリストや分類リストの上位に表示される場合がある。結果として、元の不正通信を特定するために行われた分析処理では注目されなかった別の不正通信の通信ログが注目されることとなり、検出される可能性が高まる。

【００９１】

別の不正通信を特定する処理について、具体例を示して説明する。ここで、ステップ４において、例えば、通信先のＵＲＬが「http://www.malsample1.net/abcdefg/post.php」の通信が元の不正通信として特定されたものとする。この元の不正通信について、通信元のクライアント端末１０のＩＰアドレスは「192.168.100.100」であった。また、元の不正通信の発生状況を確認すると、2015年1月10日12時10分～2015年1月31日19時30分までの間に発生していた。

【００９２】

これらの情報より、別の不正通信の調査として、不正通信調査部２７は、「192.168.100.100」のクライアント端末１０が通信元となっている通信ログで、発生期間が2015年1月10日12時10分～2015年1月31日19時30分の通信ログを抽出する。そして、分類リスト適用部２４は、抽出された通信ログに対して分類リストを適用する。なお、ここでの分析処理では分類リストの一部、例えばフィールド抽出リストのみ適用することとしても良い。

【００９３】

図１１（ａ）、（ｂ）は、元の不正通信をもとに通信ログを絞って分類リストを適用した出力結果の一例について説明するための図である。ここで、図１１（ａ）、（ｂ）は、共に「ＨＴＴＰ通信でＰＯＳＴメソッドを用いた通信ログについて、通信元ＩＰアドレス及びＵＲＬを出現回数順にソートする」という分類条件を定めたフィールド抽出リストを適用した出力結果を示すが、適用対象の通信ログが異なる。図１１（ａ）は、全分析期間の全通信ログを対象とした出力例であり、図１１（ｂ）は、元の不正通信をもとに絞った通信ログを対象とした出力例である。

【００９４】

図１１（ａ）に示す例では、出現回数が多い順番に番号１～６の通信ログが表示されており、これらは不正ではない通信の通信ログである。一方、図１１（ｂ）に示す例では、番号１～５は不正ではない通信の通信ログであるが、番号６の通信ログは不正通信に関するものである。即ち、元の不正通信をもとに通信ログを絞ることにより、元の不正通信と感染源が共通する別の不正通信に関する通信ログが、上位に表示されたこととなる。この番号６の通信ログについては、解析者が、他の分類リストの適用結果を確認したりすることにより、不正通信か否かの判断を行う。また、通信先の情報の収集やパケットデータの取得が行われ、最終的に不正通信か否かの判断が行われる。

【００９５】

ここで、元の不正通信のＵＲＬ「http://www.malsample1.net/abcdefg/post.php」と、別の不正通信のＵＲＬ「http://www.malexample2.net/abcdefg/post.php」とは、ホスト「www.malsample1.net」より下位の「/abcdefg/post.php」の部分、即ち、ファイルパスを示すＵＲＩ部分が共通している。ファイルパスとは、サーバなどの通信先の内部でのリソース（ファイル）の所在地を示すものであり、ＨＴＴＰ通信では、サーバの公開領域内でのディレクトリ名及びファイル名を表す。ここで、攻撃者は、例えば、同じような仕組みを用いて複数の不正サイトを用意することがある。即ち、例えば、複数のマルウェアに感染した場合、ＵＲＬが異なる複数の不正通信が発生するが、ファイルパスなど、一部のＵＲＩ部分が共通して複数の不正通信が発生する場合がある。言い換えると、マルウェアの作成傾向として、マルウェアにより発生する複数の不正通信で一部のＵＲＩ部分が共通する場合がある。そこで、番号６の通信ログについて、通信先のＵＲＩ部分が元の不正通信の通信先のＵＲＩ部分と同じであるために、不正通信の可能性が高いと判断しても良い。

【００９６】
さらに、不正通信調査部２７は、通信先のＵＲＬが「/abcdefg/post.php」を含む通信ログが、番号６の通信ログ以外に存在するか否かを調査しても良い。そして、例えば、「http://www.xxx.yyy.zzz/abcdefg/post.php」、「http://www.xyz.xyz.co/abcdefg/post.php」、「http://aaa.bbb.ccc/abcdefg/post.php」、「http://eee.fff.ggg/abcdefg/post.php」などのＵＲＬを通信先とする通信ログが見つかれば、不正通信の可能性があると判断しても良い。
【００９７】
また、攻撃者がマルウェアを作成するにあたり、例えば、上述したようにファイルパスの記述を全く同じにするのではなく、ファイルパスの記述を一部変えてＵＲＬを構成する場合もある。そこで、元の不正通信の通信先であるＵＲＬのＵＲＩ部分と同じものを含む場合にその通信が不正通信の可能性が高いと判断するものに限られるわけではなく、元の不正通信とＵＲＩ部分が類似していれば不正通信の可能性が高いと判断しても良い。
【００９８】
さらに、元の不正通信において着目する箇所についても、ＵＲＬの一部であるファイルパスを示すＵＲＩ部分に限られるものではなく、例えば、元の不正通信の通信先であるＵＲＬの全部や、ホスト名単体、ＨＴＴＰリクエストメソッド等のヘッダ情報などに着目しても良い。例えばホスト名に着目する場合には、元の不正通信の通信先であるＵＲＬのホスト名と同じものが含まれる通信ログについて、不正通信の可能性が高いと判断される。
【００９９】
このように、元の不正通信の通信ログに含まれる情報に着目する場合には、解析者は、マルウェアが作成される傾向を考慮し、通信ログに含まれる情報の中で、不正通信としての特徴が示されているような、マルウェアの作成傾向に沿う部分、言い換えると、攻撃者が作成したマルウェアに応じて決まる場合のある情報に着目する。そして、不正通信の通信ログの特徴部分（マルウェアの作成傾向に沿う部分）と同じ情報が含まれる通信ログについて、不正通信の可能性が高いと判断される。
【０１００】
さらに、解析者は、元の不正通信の発生状況に着目しても良い。発生状況とは、例えば、通信が発生する周期や時間帯、通信間隔などの通信の発生傾向を示す。
【０１０１】
そして、例えば、通信先のＵＲＩ部分が元の不正通信の通信先のＵＲＩ部分と同じである上述の５つの通信（(1)「http://www.malexample2.net/abcdefg/post.php」、(2)「http://www.xxx.yyy.zzz/abcdefg/post.php」、(3)「http://www.xyz.xyz.co/abcdefg/post.php」、(4)「http://aaa.bbb.ccc/abcdefg/post.php」、(5)「http://eee.fff.ggg/abcdefg/post.php」）に対して、着目する箇所を中心に確認が行われる。
【０１０２】
例えば、(1)～(4)の通信については、元の不正通信の通信ログと比較すると、通信ログの幾つかの着目点が共通しており、通信が発生する傾向としてはほとんど同じであった。しかし、(5)の通信については、元の不正通信の通信ログと着目点が共通している部分はあるものの、(1)～(4)の通信とは発生状況が異なっていた。つまり、(1)～(4)の通信と(5)の通信とでは発生状況が異なるという通信事実が判明した。
以上より、(1)～(5)の全ての通信において、着目点および通信の発生状況が完全に一致した状態にはならなかったが、マルウェアの作成傾向に沿う情報としては元の不正通信と合致する点が多くあり、通信先となるホストに関する情報についても不審な部分が多いため、この場合全て不正通信であると判断が行われた。また元の不正通信以外にも不正通信が存在したという事実に加え、全体の不正通信の状況を把握できるため、特定期間内における全体の状況把握と影響確認を行うことができたといえる。
【０１０３】
図１２は、別の不正通信の調査手順の一例について説明するための図である。図１２に示す例では、ステップ４で元の不正通信として不正通信Ａが特定され、ステップ６で別の

不正通信として不正通信Ｂ及び不正通信Ｃが特定されるものとして説明する。また、不正通信Ａはクライアント端末１０ａから発生し、不正通信Ｂはクライアント端末１０ａ及びクライアント端末１０ｂから発生し、不正通信Ｃはクライアント端末１０ｂから発生したこととする。

【０１０４】

まず、ステップ４で不正通信Ａが特定されると、不正通信調査部２７は、不正通信Ａの発生状況に基づいて特定期間１を設定する。次に、不正通信調査部２７は、特定期間１に検知された通信ログのうち、不正通信Ａの通信元であるクライアント端末１０ａが通信元となっている通信ログに絞って、ステップ３の分析処理を実行する。この分析結果をもとに、解析者がステップ４の処理を行い、別の不正通信として不正通信Ｂを特定する。続けて、不正通信Ｂに対してステップ５の処理が行われ、発生期間、発生要因などの特定が行われる。

【０１０５】

ここで特定される不正通信Ｂは、クライアント端末１０ａを通信元として特定期間１に発生したものであるが、不正通信Ｂとしては、他のクライアント端末１０を通信元として発生している可能性もある。そのため、通信分析装置２０は、全分析期間の全通信ログの中で、不正通信Ｂの通信ログを抽出する。これにより、不正通信Ｂの通信元として、クライアント端末１０ａに加えてクライアント端末１０ｂが特定される。

【０１０６】

次に、不正通信調査部２７は、別の不正通信として特定された不正通信Ｂをもとに、さらに別の不正通信の有無を調査する。

具体的には、不正通信調査部２７は、クライアント端末１０ａを通信元とする不正通信Ｂの発生状況に基づいて、特定期間２を設定する。そして、不正通信調査部２７は、特定期間２に検知された通信ログのうち、不正通信Ｂの通信元であるクライアント端末１０ａが通信元となっている通信ログに絞って、ステップ３の分析処理を実行する。

同様に、不正通信調査部２７は、クライアント端末１０ｂを通信元とする不正通信Ｂの発生状況に基づいて、特定期間３を設定する。そして、不正通信調査部２７は、特定期間３に検知された通信ログのうち、不正通信Ｂの通信元であるクライアント端末１０ｂが通信元となっている通信ログに絞って、ステップ３の分析処理を実行する。

【０１０７】

これらの分析結果をもとに、解析者がステップ４の処理を行う。その結果、特定期間２では別の不正通信は特定されなかったが、特定期間３では新たに別の不正通信として不正通信Ｃが特定される。続けて、不正通信Ｃに対してステップ５の処理が行われ、発生期間、発生要因などの特定が行われる。

また、通信分析装置２０は、この不正通信Ｃについても、通信元を特定するとともに特定期間を定めて、さらに別の不正通信の有無を調査しても良い。

【０１０８】

このようにして、不正通信調査部２７は、ステップ４で特定された元の不正通信をキーにして、別の不正通信の有無を調査する。また、別の不正通信が特定されると、不正通信調査部２７は、特定された別の不正通信をキーにして、さらに別の不正通信の有無を調査しても良い。即ち、不正通信調査部２７は、別の不正通信をキーにしてさらに別の不正通信の有無を調査する処理を、繰り返し実行することとしても良い。

【０１０９】

また、図１１に示す例では、元の不正通信をもとに通信ログを絞って分析する例について説明したが、全分析期間の全通信ログを対象とし、不正通信の通信ログの特徴部分（即ち、マルウェアの作成傾向に沿う部分）と同じ情報が含まれる通信ログを探索して、別の不正通信の有無を調査することとしても良い。この場合、ステップ４で元の不正通信が特定されると、不正通信調査部２７は、全分析期間の全通信ログのうち、例えば通信先のＵＲＬに、元の不正通信の通信先であるＵＲＬのＵＲＩ部分と同じものが含まれる通信ログを抽出する。そして、不正通信調査部２７は、抽出した通信ログの情報を示してそれを出

現回数の多い順番にして表示したり、分類リストの適用結果等を表示したりして、不正通信か否かの判断が行われる。

この調査方法は、特定の期間に絞り込みを行い、分析に必要な通信ログ量を減らして迅速な判断を行う方法に比べると時間を要するが、この調査結果は全通信ログを対象にして抜け漏れをなくす目的で判断を行う場合などに活用する。また、期間を絞らないことで、不正通信が影響する範囲の全貌が明らかになることもある。

【０１１０】

ステップ６の別の不正通信の調査について、フローチャートを示して説明する。図１３は、別の不正通信の調査を行う処理の手順の一例を示したフローチャートである。

【０１１１】

まず、ステップ５において、不正通信の深堀り調査が行われた後、例えば解析者が元の不正通信をキーにして別の不正通信を調査する入力を行うと、不正通信調査部２７は、元の不正通信の発生状況に基づいて特定期間を設定する（ステップ３０１）。ここで、元の不正通信の発生状況については、図９のステップ２０２で特定された発生期間の情報が用いられる。また、不正通信調査部２７は、元の不正通信の通信元であるクライアント端末１０の情報を取得する（ステップ３０２）。ここで、元の不正通信のクライアント端末１０の情報は、図９のステップ２０３で収集された情報が用いられる。

【０１１２】

次に、不正通信調査部２７は、特定期間に検知された通信ログのうち、元の不正通信の通信元であるクライアント端末１０が通信元となっている通信ログを抽出する（ステップ３０３）。そして、分類リスト適用部２４は、抽出された通信ログに対して分類リストを適用する（ステップ３０４）。ここでは、例えば、元の不正通信を特定するための分析処理で用いられた分類リストと同じものが適用される。そして、分類リスト適用部２４は、分類リストごとに分析結果を出力して表示部２１に表示する。

【０１１３】

次に、解析者は、ステップ４の処理を行い、別の不正通信を特定する。そして、解析者が別の不正通信の通信ログを指定する入力を行うと、詳細情報取得部２６は、別の不正通信に関してステップ５の深堀り調査を実行する（ステップ３０５）。そして、本処理フローは終了する。この後、不正通信調査部２７は、ステップ３０５で取得された別の不正通信に関する情報をもとにしてステップ３０１の処理を開始して、さらに別の不正通信があるか否かを調査しても良い。

【０１１４】

また、元の不正通信の通信元であるクライアント端末１０が複数ある場合には、ステップ３０１～ステップ３０５の処理は、通信元であるクライアント端末１０ごとに行われる。

【０１１５】

なお、本発明の実施の形態を実現するプログラムは、磁気記録媒体（磁気テープ、磁気ディスクなど）、光記録媒体（光ディスクなど）、光磁気記録媒体、半導体メモリなどのコンピュータが読取可能な記録媒体に記憶した状態で提供し得る。また、インターネットなどの通信手段を用いて提供することも可能である。

【０１１６】

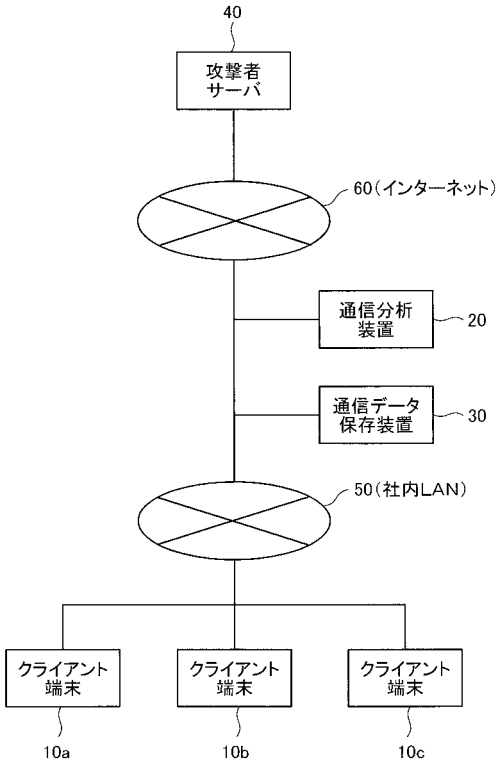
また、本発明を実施の形態を用いて説明したが、本発明の技術的範囲は上記実施の形態には限定されない。本発明の精神及び範囲から逸脱することなく様々に変更したり代替態様を採用したりすることが可能なことは、当業者に明らかである。

【符号の説明】

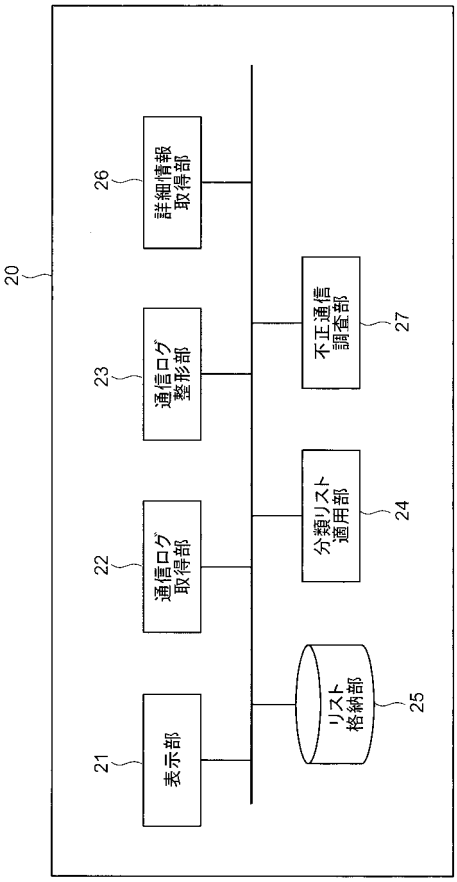
【０１１７】

１０ａ，１０ｂ，１０ｃ…クライアント端末、２０…通信分析装置、２１…表示部、２２…通信ログ取得部、２３…通信ログ整形部、２４…分類リスト適用部、２５…リスト格納部、２６…詳細情報取得部、２７…不正通信調査部、３０…通信データ保存装置、４０…攻撃者サーバ

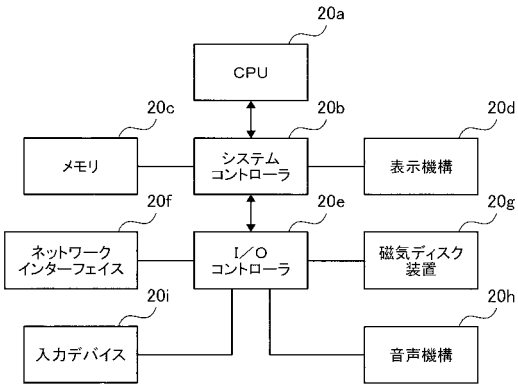
【図１】


40
攻撃者
サーバ
60（インターネット）
通信分析
装置
20
通信データ
保存装置
30
50（社内LAN）
クライアント
端末
クライアント
端末
クライアント
端末
10a
10b
10c

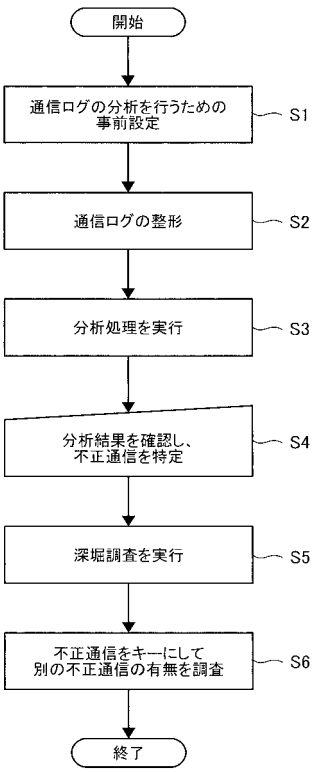
【図２】


20
詳細情報
取得部
26
通信ログ
整形部
23
通信ログ
取得部
22
表示部
21
不正通信
調査部
27
分類リスト
適用部
24
リスト
格納部
25

【図３】


20a
CPU
20c
メモリ
20b
システム
コントローラ
20d
表示機構
20f
ネットワーク
インターフェイス
20e
I／O
コントローラ
20g
磁気ディスク
装置
20i
入力デバイス
20h
音声機構

【図４】


開始
通信ログの分析を行うための
事前設定
S1
通信ログの整形
S2
分析処理を実行
S3
分析結果を確認し、
不正通信を特定
S4
深堀調査を実行
S5
不正通信をキーにして
別の不正通信の有無を調査
S6
終了

【図５】

(a)

番号	出現回数	ホスト名
1	13482	aaa.abcd0.jp
2	9790	bbb.abcd0.jp
3	5983	ccc.abcd1.net
4	2978	ddd.abcd2.com
：	：	：
280	57	malware.abcd4.jp

(b)

番号	出現回数	URL
1	2733	http://ccc.abcd1.net/00/11
2	2716	http://eee.abcd2.com/
3	2589	http://ccc.abcd1.net/test.php
4	1643	http://fff.abcd3.jp:443
：	：	：
350	57	http://malware.abcd4.jp/

【図６】

(a)

番号	出現回数	ホスト名
1	2909737	aaa.office.sample1.com
2	2710145	bbb.office.sample1.com
3	2480901	ccc.sample2.co.jp
4	1999295	ddd.sample3.com
：	：	：
1532	57	malware.abcd4.jp

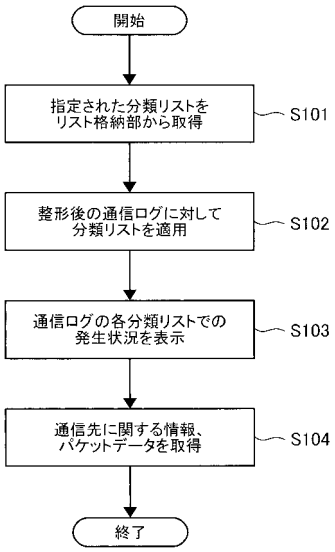
(b)

番号	出現回数	通信元IPアドレス	メソッド	通信先ホスト
1	735727	10.52.199.55	GET	streaming.aaa.jp:1935
2	439866	10.199.103.46	GET	cs.bbb.jp
3	439849	10.196.175.26	GET	sensor.ccc.edu:5280
4	434698	10.199.103.82	GET	cs.bbb.jp
：	：	：	：	：
9866	55	172.29.36.209	GET	malware.abcd4.jp

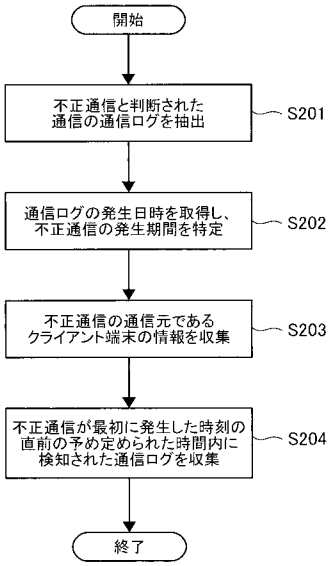
【図７】

番号	分類リスト	相関情報
1	リスト1 （ブラックリスト）	出現回数： 57 ホスト名： malware.abcd4.jp
2	リスト2 （ブラックリスト）	出現回数： 57 URL： http://malware.abcd4.jp/
3	リスト3 （フィールド抽出リスト）	出現回数： 57 ホスト名： malware.abcd4.jp
4	リスト4 （フィールド抽出リスト）	出現回数： 55 通信元IPアドレス： 172.29.36.209 通信先ホスト： malware.abcd4.jp メソッド： GET
5	リスト5 （フィールド抽出リスト）	出現回数： 1 通信元IPアドレス： 172.29.36.209 通信先ホスト： malware.abcd4.jp メソッド： GET URL： http://malware.abcd4.jp/
6	リスト6 （フィールド抽出リスト）	出現回数： 1 URL： http://malware.abcd4.jp/

【図８】



【図９】



【図１０】

番号	発生日時	通信元IPアドレス	メソッド	URL
1	2015/2/23 17:41	172.29.36.209	GET	http://sample.kaizan.jp/images/aa
2	2015/2/23 17:41	172.29.36.209	GET	http://sample.kaizan.jp/images/bb
3	2015/2/23 17:41	172.29.36.209	GET	http://sample.kaizan.jp/scripts/000.php
4	2015/2/23 17:41	172.29.36.209	GET	http://sample.kaizan.jp/scripts/111.php
5	2015/2/23 17:41	172.29.36.209	GET	http://sample.kaizan.jp/images/cc
6	2015/2/23 17:42	172.29.36.209	GET	http://malware2.downloadsite.com/it/xxxxxxx.jpg
7	2015/2/23 17:42	172.29.36.209	GET	http://sample.kaizan.jp/images/dd
8	2015/2/23 17:42	172.29.36.209	GET	http://sample.kaizan.jp/images/ee
9	2015/2/23 17:42	172.29.36.209	GET	http://sample.kaizan.jp/images/ff
10	2015/2/23 17:42	172.29.36.209	GET	http://sample.kaizan.jp/images/gg
11	2015/2/23 17:42	172.29.36.209	GET	http://sample.kaizan.jp/images/hh
12	2015/2/23 17:42	172.29.36.209	GET	http://sample.kaizan.jp/images/ii
13	2015/2/23 17:42	172.29.36.209	POST	http://mal.example.com/test/page/00
14	2015/2/23 17:42	172.29.36.209	GET	http://sample.kaizan.jp/images/jj

【図１１】

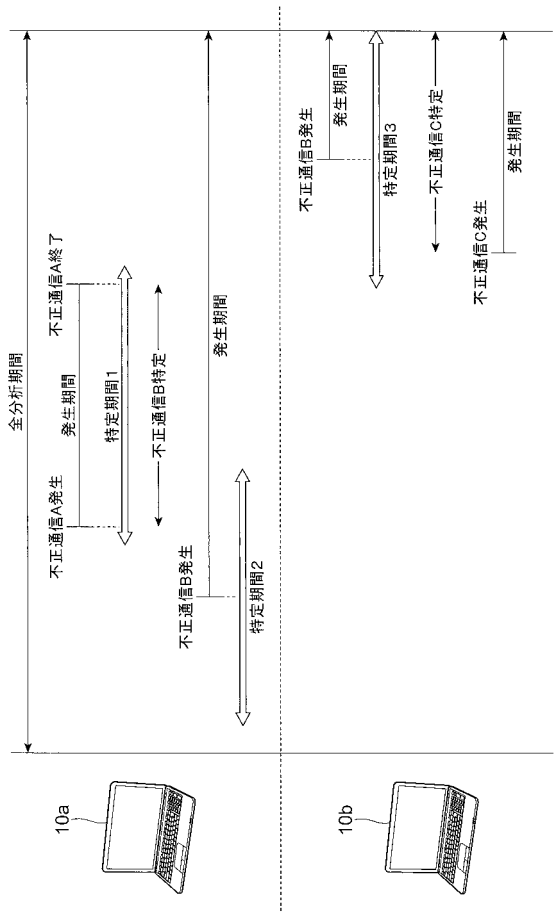
(a)

番号	出現回数	通信元IPアドレス	メソッド	URL
1	1016553	192.168.100.101	POST	http://www.aaa.office.sample1.com
2	933786	192.168.100.102	POST	http://www.bbb.office.sample1.com
3	922473	192.168.100.100	POST	http://www.ccc.sample2.com
4	948544	192.168.100.101	POST	http://www.ddd.test1.com
5	821350	192.168.100.102	POST	http://www.eee.test2.com
6	809022	192.168.100.101	POST	http://www.fff.test3.com

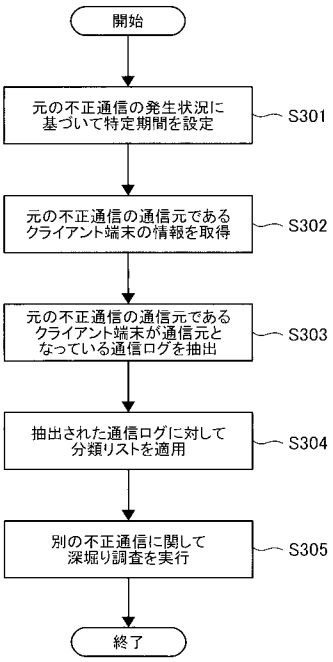
(b)

番号	出現回数	通信元IPアドレス	メソッド	URL
1	1013	192.168.100.100	POST	http://www.ccc.sample2.com
2	978	192.168.100.100	POST	http://www.aaa.office.sample1.com
3	943	192.168.100.100	POST	http://www.bbb.office.sample1.com
4	499	192.168.100.100	POST	http://www.xxx.test4.com
5	130	192.168.100.100	POST	http://www.zzz.test5.com
6	90	192.168.100.100	POST	http://www.malexample2.net/abcdefg/post.php

【図１２】



【図１３】



【手続補正書】
【提出日】平成28年5月20日(2016.5.20)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
監視対象とするネットワーク上で対象期間内に検知された通信の通信ログを取得する取得手段と、
前記取得手段が取得した通信ログをもとに不正通信が検出された場合に、当該取得手段が取得した当該通信ログの中から、通信元が当該不正通信の通信元と同一の通信で、当該不正通信の発生状況をもとに特定された特定期間内に検知された通信の通信ログを抽出する抽出手段とを備え、
前記特定期間は、前記不正通信の通信先を識別可能な情報の少なくとも一部が共通する通信のうち、前記対象期間内に前記通信元にて当該不正通信の前に発生し特定の条件を満たす通信を特定し、当該通信が発生した時点を始点とする期間をもとに特定されることを特徴とする情報処理装置。
【請求項２】
監視対象とするネットワーク上で対象期間内に検知された通信の通信ログを取得する取得手段と、
前記取得手段が取得した通信ログをもとに不正通信が検出された場合に、当該取得手段が取得した当該通信ログの中から、通信元が当該不正通信の通信元と同一の通信で、当該不正通信の発生状況をもとに特定された特定期間内に検知された通信の通信ログを抽出す

る抽出手段とを備え、
前記特定期間は、前記不正通信の通信先を識別可能な情報の少なくとも一部が共通する通信のうち、前記対象期間内に前記通信元にて当該不正通信の後に発生し特定の条件を満たす通信を特定し、当該通信が発生した時点を終点とする期間をもとに特定されること
を特徴とする情報処理装置。
【請求項３】
監視対象とするネットワーク上で対象期間内に検知された通信の通信ログを取得する取得手段と、
前記取得手段が取得した通信ログをもとに不正通信が検出された場合に、当該取得手段が取得した当該通信ログの中から、通信元が当該不正通信の通信元と同一の通信で、当該不正通信の発生状況をもとに特定された特定期間内に検知された通信の通信ログを抽出する抽出手段とを備え、
前記特定期間は、前記対象期間内に前記通信元にて前記不正通信が最初に発生した時点から最後に発生した時点までの期間をもとに特定されること
を特徴とする情報処理装置。
【請求項４】
前記抽出手段は、検出された前記不正通信の通信元が複数存在する場合、当該通信元ごとに、通信元が当該不正通信の通信元と同一の通信で、当該不正通信の発生状況をもとに特定された特定期間内に検知された通信の通信ログを抽出すること
を特徴とする請求項１乃至３のいずれか１項に記載の情報処理装置。
【請求項５】
前記抽出手段は、当該抽出手段が抽出した通信ログをもとに別の不正通信が検出された場合に、前記取得手段が取得した通信ログの中から、通信元が当該別の不正通信の通信元と同一の通信で、当該別の不正通信の発生状況をもとに特定された特定期間内に検知された通信の通信ログを抽出すること
を特徴とする請求項１乃至３のいずれか１項に記載の情報処理装置。
【請求項６】
監視対象とするネットワーク上で対象期間内に検知された通信の通信ログを取得するステップと、
取得された前記通信ログをもとに不正通信が検出された場合に、取得された当該通信ログの中から、通信元が当該不正通信の通信元と同一の通信で、当該不正通信の発生状況をもとに特定された特定期間内に検知された通信の通信ログを抽出するステップとを含み、
前記特定期間は、前記不正通信の通信先を識別可能な情報の少なくとも一部が共通する通信のうち、前記対象期間内に前記通信元にて当該不正通信の前に発生し特定の条件を満たす通信を特定し、当該通信が発生した時点を始点とする期間をもとに特定されること
を特徴とする情報処理方法。
【請求項７】
監視対象とするネットワーク上で対象期間内に検知された通信の通信ログを取得するステップと、
取得された前記通信ログをもとに不正通信が検出された場合に、取得された当該通信ログの中から、通信元が当該不正通信の通信元と同一の通信で、当該不正通信の発生状況をもとに特定された特定期間内に検知された通信の通信ログを抽出するステップとを含み、
前記特定期間は、前記不正通信の通信先を識別可能な情報の少なくとも一部が共通する通信のうち、前記対象期間内に前記通信元にて当該不正通信の後に発生し特定の条件を満たす通信を特定し、当該通信が発生した時点を終点とする期間をもとに特定されること
を特徴とする情報処理方法。
【請求項８】
監視対象とするネットワーク上で対象期間内に検知された通信の通信ログを取得するステップと、
取得された前記通信ログをもとに不正通信が検出された場合に、取得された当該通信ロ

グの中から、通信元が当該不正通信の通信元と同一の通信で、当該不正通信の発生状況をもとに特定された特定期間内に検知された通信の通信ログを抽出するステップとを含み、
前記特定期間は、前記対象期間内に前記通信元にて前記不正通信が最初に発生した時点から最後に発生した時点までの期間をもとに特定されること
を特徴とする情報処理方法。
【請求項９】
コンピュータに、
監視対象とするネットワーク上で対象期間内に検知された通信の通信ログを取得する機能と、
取得された前記通信ログをもとに不正通信が検出された場合に、取得された当該通信ログの中から、通信元が当該不正通信の通信元と同一の通信で、当該不正通信の発生状況をもとに特定された特定期間内に検知された通信の通信ログを抽出する機能とを実現させ、
前記特定期間は、前記不正通信の通信先を識別可能な情報の少なくとも一部が共通する通信のうち、前記対象期間内に前記通信元にて当該不正通信の前に発生し特定の条件を満たす通信を特定し、当該通信が発生した時点を始点とする期間をもとに特定されること
を特徴とするプログラム。
【請求項１０】
コンピュータに、
監視対象とするネットワーク上で対象期間内に検知された通信の通信ログを取得する機能と、
取得された前記通信ログをもとに不正通信が検出された場合に、取得された当該通信ログの中から、通信元が当該不正通信の通信元と同一の通信で、当該不正通信の発生状況をもとに特定された特定期間内に検知された通信の通信ログを抽出する機能とを実現させ、
前記特定期間は、前記不正通信の通信先を識別可能な情報の少なくとも一部が共通する通信のうち、前記対象期間内に前記通信元にて当該不正通信の後に発生し特定の条件を満たす通信を特定し、当該通信が発生した時点を終点とする期間をもとに特定されること
を特徴とするプログラム。
【請求項１１】
コンピュータに、
監視対象とするネットワーク上で対象期間内に検知された通信の通信ログを取得する機能と、
取得された前記通信ログをもとに不正通信が検出された場合に、取得された当該通信ログの中から、通信元が当該不正通信の通信元と同一の通信で、当該不正通信の発生状況をもとに特定された特定期間内に検知された通信の通信ログを抽出する機能とを実現させ、
前記特定期間は、前記対象期間内に前記通信元にて前記不正通信が最初に発生した時点から最後に発生した時点までの期間をもとに特定されること
を特徴とするプログラム。
【手続補正書】
【提出日】平成28年8月8日(2016.8.8)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
監視対象とするネットワーク上で対象期間内に検知された通信の通信ログを取得する取得手段と、
前記取得手段が取得した通信ログをもとに不正通信が検出された場合に、当該取得手段が取得した当該通信ログの中から、通信元が当該不正通信の通信元と同一の通信で、当該

不正通信の発生状況をもとに特定された特定期間内に検知された通信の通信ログを抽出する抽出手段とを備え、
前記特定期間は、前記対象期間内に前記通信元にて前記不正通信が最初に発生した時点から最後に発生した時点までの期間をもとに特定されること
を特徴とする情報処理装置。
【請求項２】
前記抽出手段は、検出された前記不正通信の通信元が複数存在する場合、当該通信元ごとに、通信元が当該不正通信の通信元と同一の通信で、当該不正通信の発生状況をもとに特定された特定期間内に検知された通信の通信ログを抽出すること
を特徴とする請求項１に記載の情報処理装置。
【請求項３】
前記抽出手段は、当該抽出手段が抽出した通信ログをもとに別の不正通信が検出された場合に、前記取得手段が取得した通信ログの中から、通信元が当該別の不正通信の通信元と同一の通信で、当該別の不正通信の発生状況をもとに特定された特定期間内に検知された通信の通信ログを抽出すること
を特徴とする請求項１に記載の情報処理装置。
【請求項４】
監視対象とするネットワーク上で対象期間内に検知された通信の通信ログを取得するステップと、
取得された前記通信ログをもとに不正通信が検出された場合に、取得された当該通信ログの中から、通信元が当該不正通信の通信元と同一の通信で、当該不正通信の発生状況をもとに特定された特定期間内に検知された通信の通信ログを抽出するステップとを含み、
前記特定期間は、前記対象期間内に前記通信元にて前記不正通信が最初に発生した時点から最後に発生した時点までの期間をもとに特定されること
を特徴とする情報処理方法。
【請求項５】
コンピュータに、
監視対象とするネットワーク上で対象期間内に検知された通信の通信ログを取得する機能と、
取得された前記通信ログをもとに不正通信が検出された場合に、取得された当該通信ログの中から、通信元が当該不正通信の通信元と同一の通信で、当該不正通信の発生状況をもとに特定された特定期間内に検知された通信の通信ログを抽出する機能とを実現させ、
前記特定期間は、前記対象期間内に前記通信元にて前記不正通信が最初に発生した時点から最後に発生した時点までの期間をもとに特定されること
を特徴とするプログラム。