(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2018-194880
(P2018-194880A)
(43)公開日　平成30年12月6日(2018.12.6)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/56	(2013.01)	G06F	21/56	360

審査請求 未請求　請求項の数 17　ＯＬ　（全 27 頁）

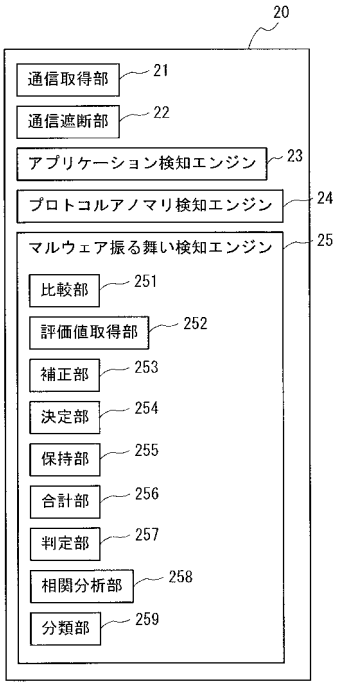
(21)出願番号　特願2017-95339(P2017-95339)
(22)出願日　平成29年5月12日(2017.5.12)

（特許庁注：以下のものは登録商標）
１．ＷＩＮＤＯＷＳ

(71)出願人　000136136
株式会社ＰＦＵ
石川県かほく市宇野気ヌ９８番地の２
(74)代理人　100113608
弁理士　平川　明
(74)代理人　100105407
弁理士　高田　大輔
(74)代理人　100145838
弁理士　畑添　隆人
(72)発明者　寺田　成吾
石川県かほく市宇野気ヌ９８番地の２　株式会社ＰＦＵ内
(72)発明者　道根　慶治
石川県かほく市宇野気ヌ９８番地の２　株式会社ＰＦＵ内

(54)【発明の名称】情報処理装置、不正活動分類方法および不正活動分類用プログラム

(57)【要約】　（修正有）
【課題】端末が行う通信の振る舞いに基づいて、当該端末がどれだけ危険な状態にあるかを判断するために役立つ情報を得ることが可能な情報処理装置を提供する。
【解決手段】ネットワーク監視装置２０は、ネットワークに接続された端末による通信と予め保持されたパターンとを比較する比較手段２５１と、前記比較の結果に従って、前記端末の活動のフェーズを決定する決定手段２５４と、前記端末が不正な活動を行っているか否かを判定する判定手段２５７と、該端末の第一の通信に基づいて決定された第一のフェーズと、該第一の通信の前または後に行われた第二の通信に基づいて決定された第二のフェーズとの相関分析を行うことで、振る舞いの種類を決定する相関分析手段２５８と、前記端末が不正な活動を行っていると判定された場合に、前記相関分析手段によって決定された振る舞いの種類に基づいて、該端末による不正な活動を分類する分類手段２５９と、を備える。
【選択図】図３



【特許請求の範囲】
【請求項１】
ネットワークに接続された端末による通信と予め保持されたパターンとを比較する比較手段と、
前記比較の結果に従って、前記端末の活動のフェーズを決定する決定手段と、
前記端末が不正な活動を行っているか否かを判定する判定手段と、
該端末の第一の通信に基づいて決定された第一のフェーズと、該第一の通信の前または後に行われた第二の通信に基づいて決定された第二のフェーズとの相関分析を行うことで、該第一の通信及び該第二の通信に係る該端末の振る舞いの種類を決定する相関分析手段と、
前記判定手段によって前記端末が不正な活動を行っていると判定された場合に、前記相関分析手段によって決定された振る舞いの種類に基づいて、該端末による不正な活動を分類する分類手段と、
を備える情報処理装置。
【請求項２】
前記決定手段は、前記比較の結果に従って、前記端末が不正な活動をしていると推測される程度を示す評価値を更に決定し、
前記判定手段は、前記評価値に基づいて、前記端末が不正な活動を行っているか否かを判定する、
請求項１に記載の情報処理装置。
【請求項３】
前記端末毎に、前記評価値の前記フェーズ毎の最大値を保持する保持手段を更に備え、
前記判定手段は、前記評価値の前記フェーズ毎の最大値に基づいて、前記端末が不正な活動を行っているか否かを判定する、
請求項２に記載の情報処理装置。
【請求項４】
前記相関分析手段は、前記端末の第一の通信について決定された第一のフェーズと、該端末の第二の通信について決定された第二のフェーズとが、予め設定された相関条件を満たす場合に、該相関条件に対応する振る舞いの種類を、該端末による振る舞いの種類として決定する、
請求項１から３の何れか一項に記載の情報処理装置。
【請求項５】
前記分類手段は、前記端末について決定された１または複数の振る舞いの種類に基づいて、該端末の不正な活動を分類する、
請求項１から４の何れか一項に記載の情報処理装置。
【請求項６】
前記分類手段は、不正な活動の分類と、該不正な活動に関連する１または複数の振る舞いの種類と、の対応関係を示す情報を参照することで、該端末の不正な活動を分類する、
請求項５に記載の情報処理装置。
【請求項７】
前記分類は、不正な活動の危険度を示す分類であり、
前記分類手段は、前記端末について決定された１または複数の振る舞いの種類に基づいて、該端末の不正な活動の危険度を決定する、
請求項１から６の何れか一項に記載の情報処理装置。
【請求項８】
前記分類手段は、高い危険度に係る振る舞いから順に検討していき、最初に一致した危険度を設定する、
請求項７に記載の情報処理装置。
【請求項９】
前記分類は、不正な活動に係るマルウェア種別を示す分類であり、

前記分類手段は、前記端末について決定された１または複数の振る舞いの種類に基づいて、該端末の不正な活動に係るマルウェア種別を決定する、
請求項１から６の何れか一項に記載の情報処理装置。
【請求項１０】
前記フェーズは、前記端末による不正な活動の遷移の状態を示し、
前記決定手段は、前記比較の結果、前記通信と一致または近似したパターンについて予め設定されているフェーズを、前記通信に係るフェーズとして決定する、
請求項１から９の何れか一項に記載の情報処理装置。
【請求項１１】
前記端末毎に、前記フェーズ毎の前記評価値の最大値を合計する合計手段を更に備え、
前記判定手段は、前記合計手段によって得られた合計値に基づいて、前記端末が不正な活動を行っているか否かを判定する、
請求項１から１０の何れか一項に記載の情報処理装置。
【請求項１２】
前記判定手段は、前記合計値または前記合計値に基づく値が所定の閾値を超えた場合に、前記端末が不正な活動を行っていると判定する、
請求項１１に記載の情報処理装置。
【請求項１３】
前記分類手段は、前記合計値または前記合計値に基づく値が所定値未満の場合には、前記不正な活動の分類を行わない、
請求項１２に記載の情報処理装置。
【請求項１４】
前記ネットワークに接続された端末による通信を取得する通信取得手段を更に備え、
前記比較手段は、取得された前記通信と予め保持されたパターンとを比較する、
請求項１から１３の何れか一項に記載の情報処理装置。
【請求項１５】
前記端末が不正な活動を行っていると判定された場合に該端末による通信を遮断する通信遮断手段を更に備える、
請求項１から１４の何れか一項に記載の情報処理装置。
【請求項１６】
コンピューターが、
ネットワークに接続された端末による通信と予め保持されたパターンとを比較する比較ステップと、
前記比較の結果に従って、前記端末の活動のフェーズを決定する決定ステップと、
前記端末が不正な活動を行っているか否かを判定する判定ステップと、
該端末の第一の通信に基づいて決定された第一のフェーズと、該第一の通信の前または後に行われた第二の通信に基づいて決定された第二のフェーズとの相関分析を行うことで、該第一の通信及び該第二の通信に係る該端末の振る舞いの種類を決定する相関分析ステップと、
前記判定ステップで前記端末が不正な活動を行っていると判定された場合に、前記相関分析ステップで決定された振る舞いの種類に基づいて、該端末による不正な活動を分類する分類ステップと、
を実行する不正活動分類方法。
【請求項１７】
コンピューターを、
ネットワークに接続された端末による通信と予め保持されたパターンとを比較する比較手段と、
前記比較の結果に従って、前記端末の活動のフェーズを決定する決定手段と、
前記端末が不正な活動を行っているか否かを判定する判定手段と、
該端末の第一の通信に基づいて決定された第一のフェーズと、該第一の通信の前または

後に行われた第二の通信に基づいて決定された第二のフェーズとの相関分析を行うことで、該第一の通信及び該第二の通信に係る該端末の振る舞いの種類を決定する相関分析手段と、

前記判定手段によって前記端末が不正な活動を行っていると判定された場合に、前記相関分析手段によって決定された振る舞いの種類に基づいて、該端末による不正な活動を分類する分類手段と、

として機能させる、不正活動分類用プログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、ネットワークに接続された端末を管理する技術に関する。

【背景技術】

【０００２】

従来、ネットワークに接続された端末による通信と予め保持されたパターンとを比較し、比較の結果に従って、端末が不正な活動をしていると推測される程度を示す評価値と不正な活動のフェーズとを決定し、評価値のフェーズ毎の最大値に基づいて、端末が不正な活動を行っているか否かを判定する、不正活動判定方法が提案されている（特許文献１を参照）。

【０００３】

また、システムへの攻撃を検知し、検知された攻撃を分類するための技術が種々提案されている（特許文献２から４を参照）。

【先行技術文献】

【特許文献】

【０００４】

【特許文献１】特許第６０９７８４９号公報

【特許文献２】米国特許第９５６５２０８号明細書

【特許文献３】特開２００８－１５２７７３号公報

【特許文献４】国際公開第２０１６／０３８６６２号

【発明の概要】

【発明が解決しようとする課題】

【０００５】

従来、組織内でマルウェア感染端末が検知された場合、対応の優先度付けの判断（トリアージ）を行うために、感染端末がどれだけ危険な状態にあるかの判断や、情報漏えいのリスクの判断を行う必要がある。しかし、通信内容だけでは、感染端末がどれだけ危険な状態にあるのかを判断することや、どのような機能を持ったマルウェアに感染しているかを判断することは難しく、正しくリスク判断することができない。

【０００６】

このため、従来、各マルウェア種別固有の通信の特徴（シグネチャ）を利用した検査を行い、マルウェアを分類することが提案されているが、従来の方法では、未知のマルウェアに対応することができず、また、解析結果を元に分析官が感染したマルウェアを分類するには、分析技術と経験が必要となる。

【０００７】

本開示は、上記した問題に鑑み、端末が行う通信の振る舞いに基づいて、当該端末がどれだけ危険な状態にあるかを判断するために役立つ情報を得ることを課題とする。

【課題を解決するための手段】

【０００８】

本開示の一例は、ネットワークに接続された端末による通信と予め保持されたパターンとを比較する比較手段と、前記比較の結果に従って、前記端末の活動のフェーズを決定する決定手段と、前記端末が不正な活動を行っているか否かを判定する判定手段と、該端末の第一の通信に基づいて決定された第一のフェーズと、該第一の通信の前または後に行わ

れた第二の通信に基づいて決定された第二のフェーズとの相関分析を行うことで、該第一の通信及び該第二の通信に係る該端末の振る舞いの種類を決定する相関分析手段と、前記判定手段によって前記端末が不正な活動を行っていると判定された場合に、前記相関分析手段によって決定された振る舞いの種類に基づいて、該端末による不正な活動を分類する分類手段と、を備える情報処理装置である。

【０００９】

本開示は、情報処理装置、システム、コンピューターによって実行される方法またはコンピューターに実行させるプログラムとして把握することが可能である。また、本開示は、そのようなプログラムをコンピューターその他の装置、機械等が読み取り可能な記録媒体に記録したものとしても把握できる。ここで、コンピューター等が読み取り可能な記録媒体とは、データやプログラム等の情報を電気的、磁気的、光学的、機械的または化学的作用によって蓄積し、コンピューター等から読み取ることができる記録媒体をいう。

【発明の効果】

【００１０】

本開示によれば、端末が行う通信の振る舞いに基づいて、当該端末がどれだけ危険な状態にあるかを判断するために役立つ情報を得ることが可能となる。

【図面の簡単な説明】

【００１１】

【図１】実施形態に係るシステムの構成を示す概略図である。

【図２】実施形態に係るネットワーク監視装置および管理サーバーのハードウェア構成を示す図である。

【図３】実施形態に係るネットワーク監視装置の機能構成の概略を示す図である。

【図４】実施形態のマルウェア振る舞い検知エンジンによって用いられる、マルウェアの活動遷移モデルを示す図である。

【図５】実施形態に係る、パケット毎の検知処理の流れの概要を示すフローチャートである。

【図６】実施形態に係る、マルウェア振る舞い検知エンジンによる検知処理の流れを示すフローチャート（Ａ）である。

【図７】実施形態に係る、マルウェア振る舞い検知エンジンによる検知処理の流れを示すフローチャート（Ｂ）である。

【図８】実施形態に係る、マルウェア振る舞い検知エンジンによる検知処理の流れを示すフローチャート（Ｃ）である。

【図９】実施形態に係る危険度分類処理の流れを示す図である。

【図１０】実施形態に係るマルウェア種別分類処理の流れを示す図（１）である。

【図１１】実施形態に係るマルウェア種別分類処理の流れを示す図（２）である。

【図１２】実施形態に係るシステムの構成のバリエーションを示す概略図である。

【発明を実施するための形態】

【００１２】

以下、本開示に係る情報処理装置、方法およびプログラムの実施の形態を、図面に基づいて説明する。但し、以下に説明する実施の形態は、実施形態を例示するものであって、本開示に係る情報処理装置、方法およびプログラムを以下に説明する具体的構成に限定するものではない。実施にあたっては、実施形態に応じた具体的構成が適宜採用され、また、種々の改良や変形が行われてよい。

【００１３】

本実施形態では、本開示に係る情報処理装置、方法およびプログラムを、ネットワーク上で不正な活動を行っている端末を発見し、通信遮断やアラート通知等の対処を行うためのシステムにおいて実施した場合の実施の形態について説明する。但し、本開示に係る情報処理装置、方法およびプログラムは、ネットワーク上の不正な活動を分類するための技術について広く用いることが可能であり、本開示の適用対象は、本実施形態において示した例に限定されない。

【００１４】
＜システムの構成＞
図１は、本実施形態に係るシステム１の構成を示す概略図である。本実施形態に係るシステム１は、複数の情報処理端末９０（以下、「ノード９０」と称する）が接続されるネットワークセグメント２と、ノード９０に係る通信を監視するためのネットワーク監視装置２０と、を備える。更に、管理サーバー５０が、ルータ１０を介してネットワークセグメント２と通信可能に接続されている。本実施形態において、ネットワーク監視装置２０は、スイッチまたはルータ（図１に示した例では、ルータ）のモニタリングポート（ミラーポート）に接続されることで、ノード９０によって送受信されるパケットやフレーム等を取得する。この場合、ネットワーク監視装置２０は、取得したパケットを転送しないパッシブモードで動作する。
【００１５】
管理サーバー５０は、ネットワーク監視装置２０から情報を収集し、ネットワーク監視装置２０を管理する。なお、外部ネットワークには、更に検疫サーバーが設けられ、ネットワークセグメント２に接続されたノード９０に対して検疫サービスを提供してもよいし、業務サーバーが設けられ、ノード９０に対して業務のためのサービスを提供してもよい（図示は省略する）。
【００１６】
本実施形態に係るシステム１では、ノード９０から接続される各種サーバーは、インターネットや広域ネットワークを介して遠隔地において接続されたものであり、例えばＡＳＰ（Ａｐｐｌｉｃａｔｉｏｎ Ｓｅｒｖｉｃｅ Ｐｒｏｖｉｄｅｒ）によって提供されるが、これらのサーバーは、必ずしも遠隔地に接続されたものである必要はない。例えば、これらのサーバーは、ノード９０やネットワーク監視装置２０が存在するローカルネットワーク上に接続されていてもよい。
【００１７】
図２は、本実施形態に係るネットワーク監視装置２０および管理サーバー５０のハードウェア構成を示す図である。なお、図２においては、ネットワーク監視装置２０および管理サーバー５０以外の構成（ルータ１０、ノード９０等）については、図示を省略している。ネットワーク監視装置２０および管理サーバー５０は、それぞれ、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）１１ａ、１１ｂ、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）１３ａ、１３ｂ、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）１２ａ、１２ｂ、ＥＥＰＲＯＭ（Ｅｌｅｃｔｒｉｃａｌｌｙ Ｅｒａｓａｂｌｅ ａｎｄ Ｐｒｏｇｒａｍｍａｂｌｅ Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）やＨＤＤ（Ｈａｒｄ Ｄｉｓｋ Ｄｒｉｖｅ）等の記憶装置１４ａ、１４ｂ、ＮＩＣ（Ｎｅｔｗｏｒｋ Ｉｎｔｅｒｆａｃｅ Ｃａｒｄ）１５ａ、１５ｂ等の通信ユニット、等を備えるコンピューターである。
【００１８】
図３は、本実施形態に係るネットワーク監視装置２０の機能構成の概略を示す図である。なお、図３においては、ネットワーク監視装置２０以外の構成（ルータ１０、ノード９０および管理サーバー５０等）については、図示を省略している。ネットワーク監視装置２０は、記憶装置１４ａに記録されているプログラムが、ＲＡＭ１３ａに読み出され、ＣＰＵ１１ａによって実行されることで、通信取得部２１、通信遮断部２２、アプリケーション検知エンジン２３、プロトコルアノマリ検知エンジン２４およびマルウェア振る舞い検知エンジン２５を備える情報処理装置として機能する。また、マルウェア振る舞い検知エンジン２５は、比較部２５１、評価値取得部２５２、補正部２５３、決定部２５４、保持部２５５、合計部２５６、判定部２５７、相関分析部２５８および分類部２５９を含む。なお、本実施形態では、ネットワーク監視装置２０の備える各機能は、汎用プロセッサであるＣＰＵ１１ａによって実行されるが、これらの機能の一部または全部は、１または複数の専用プロセッサによって実行されてもよい。また、これらの機能の一部または全部は、クラウド技術等を用いて、遠隔値に設置された装置や、分散設置された複数の装置に

よって実行されてもよい。

【００１９】

通信取得部２１は、ネットワークに接続された端末によって送受信される通信を取得する。なお、本実施形態において、ネットワーク監視装置２０による監視および検知の対象となる「端末」には、ネットワークセグメント２に接続されたノード９０の他、ノード９０とルータ１０を介して通信するその他の装置（他のネットワークに属するノードや外部サーバー等）を含む。

【００２０】

通信遮断部２２は、アプリケーション検知エンジン２３、プロトコルアノマリ検知エンジン２４またはマルウェア振る舞い検知エンジン２５によって、端末が不正な活動を行っていると判定された場合に、当該端末による通信を遮断する。なお、本実施形態では、端末が不正な活動を行っていると判定された場合、当該端末の通信を遮断する対処が採られる例について説明しているが、端末が不正な活動を行っていると判定された場合の対処方法は、通信の遮断に限定されない。ネットワーク監視装置２０は、端末が不正な活動を行っていると判定された場合に、アラート（警告）の通知を行ってもよいし、不正な活動を行っている端末の治癒（例えば、マルウェアの除去や脆弱性の除去）を行ってもよい。

【００２１】

アプリケーション検知エンジン２３は、マルウェアが利用する、業務に不要なアプリケーションがネットワーク上で通信を行っていることを検知するエンジンであり、例えば、既知のＲＡＴ（Ｒｅｍｏｔｅ Ａｃｃｅｓｓ Ｔｒｏｊａｎ）、Ｐ２Ｐ（Ｐｅｅｒ ｔｏ Ｐｅｅｒ）アプリケーション、Ｔｏｒ（Ｔｈｅ Ｏｎｉｏｎ Ｒｏｕｔｅｒ）、ＵｌｔｒａＳｕｒｆ（Ｐｒｏｘｙツール）および匿名プロキシ等による通信を検知することで、ノード９０において業務に不要なアプリケーションが動作していることを検知する。

【００２２】

プロトコルアノマリ検知エンジン２４は、ネットワーク上における、プロトコルに沿っていない通信を検知するエンジンであり、例えば、ＨＴＴＰアノマリ検知エンジン、ＳＳＬ／ＴＬＳアノマリ検知エンジンおよびＤＮＳアノマリ検知エンジン等が含まれる。プロトコルアノマリ検知エンジン２４は、これらのプロトコルに沿っていない通信を検知することで、ネットワーク上でプロトコルを遵守していない通信を行うノード９０を検知する。

【００２３】

マルウェア振る舞い検知エンジン２５は、マルウェアの活動遷移モデルに定義された、マルウェアによる不正な活動のフェーズごとに、ネットワーク上の通信と「マルウェア特有の通信パターン」との共通性を評価し、マルウェアの活動フェーズの遷移状況を監視することでマルウェアの振る舞い（挙動）を分析し、ノード９０におけるマルウェア感染を検知するエンジンである。

【００２４】

図４は、本実施形態のマルウェア振る舞い検知エンジン２５によって用いられる、マルウェアの活動遷移モデルを示す図である。なお、本実施形態において示されるマルウェアの活動遷移モデルにはフェーズＰ１からフェーズＰ９が定義されているが、これは本実施形態において用いられる一例であり、マルウェアの活動遷移モデルは、実施の形態に応じて、適宜変更されてよい。以下、本実施形態に係るマルウェアの活動遷移モデルにおける各フェーズについて説明する。

【００２５】

フェーズＰ１は、侵入フェーズ、即ち、標的型攻撃メールの添付ファイル、メールのＵＲＬのクリック、Ｗｅｂサイト（主に、ＳＮＳサイト）上のＵＲＬのクリック等を契機に、ＯＳやアプリケーションの脆弱性を利用して感染する悪性コンテンツ（悪性コード、攻撃コード、エクスプロイト等とも称される）が投下されるフェーズである。フェーズＰ１からの移行先は、ワーム等の自律型のマルウェアが侵入した場合、フェーズＰ２、フェーズＰ４またはフェーズＰ９であり、ボット系のマルウェアの場合、フェーズＰ２またはフ

ェーズＰ４である。
【００２６】
フェーズＰ２は、探索フェーズ、即ち、脆弱性を持った感染端末の探索フェーズである。
【００２７】
フェーズＰ３は、感染・浸潤フェーズ（拡散フェーズ）、即ち、脆弱な標的に対して攻撃コードを送り込んで感染させるかまたは他の端末から攻撃コードが送り込まれて感染させられるフェーズである。感染・浸潤フェーズでは、既に感染している端末を介して攻撃コードが標的の端末に送り込まれ、攻撃コードが送り込まれた端末がマルウェアに感染する。例えば、Ｗｉｎｄｏｗｓ　ＯＳのＭＳ－ＲＰＣやファイル共有の脆弱性を利用して拡散活動が行われる。ボット系のマルウェアの場合は、攻撃者（ハーダー）から発行される、Ｃ＆Ｃ（Ｃｏｍｍａｎｄ　ａｎｄ　Ｃｏｎｔｒｏｌ）サーバーを経由した指令（フェーズＰ６）に基づいて感染活動（マルウェアの拡散活動）が実行される。フェーズＰ３からの移行先は、ワーム等の自律型のマルウェアの場合、フェーズＰ４またはフェーズＰ９であり、ボット系のマルウェアの場合、フェーズＰ４である。感染・浸潤フェーズは、２つの側面を持つ。１つは、感染元端末が感染活動を実行するフェーズである。もう１つは、被害者（感染先）端末として、攻撃コードが送り込まれ感染させられるフェーズである。
【００２８】
フェーズＰ４は、実行ファイルのダウンロードフェーズ、即ち、攻撃コードが送り込まれたのち、マルウェアの配布サイトや既に感染している端末から、マルウェア本体である実行ファイルをダウンロードして活性化、またはアンチウィルス製品によるマルウェアの検出の回避や新しい機能の追加等の目的で、攻撃者からの指令（Ｃ＆Ｃサーバー経由）に従って、指定されたサイトから、新しいマルウェアがダウンロードされるフェーズである。マルウェア本体のダウンロードには、主に、ＨＴＴＰ、ＦＴＰ、ＴＦＴＰが使用される。また、マルウェア独自のプロトコルを利用する場合もある。フェーズＰ４からの移行先は、ボット等の遠隔操作タイプのマルウェアの場合、フェーズＰ５またはＰ６であり、ワーム等の自律型のマルウェアの場合、通常、フェーズＰ２またはフェーズＰ９である。
【００２９】
フェーズＰ５は、Ｃ＆Ｃ検索フェーズ、即ち、攻撃者からの指令を受け取るためのＣ＆Ｃサーバーを検索するフェーズである。このフェーズに遷移するマルウェアは、主に、ボット等の遠隔操作タイプのマルウェアである。マルウェアには、通常、複数のＣ＆ＣサーバーのＦＱＤＮが組み込まれており、ＤＮＳクエリを使用してアドレス解決を行う。Ｐ２Ｐタイプのボットネットの場合は、Ｐ２Ｐプロトコル（汎用または独自プロトコル）を使用してＣ＆Ｃノードを検索する。ＩＰアドレスがハードコーディングされているタイプのマルウェアは、このフェーズでは活動しない。フェーズＰ５からの移行先は、フェーズＰ６である。
【００３０】
フェーズＰ６は、Ｃ＆Ｃ通信（含む、インターネット接続確認）フェーズ、即ち、攻撃者からの指令の受信と指令の実行結果の報告（応答）等を行うために、Ｃ＆Ｃサーバーに接続してデータの送受信を行うフェーズである。Ｃ＆Ｃサーバーに接続する前に、インターネット接続確認を行うマルウェアが存在する。Ｃ＆Ｃサーバーとの接続には、フェーズＰ５でアドレス解決が成功したＩＰアドレスの何れか、またはマルウェアにハードコーディングされたＩＰアドレスの何れかが使用される。マルウェアの活動は、Ｃ＆Ｃサーバーから指令を受信すると、攻撃者からの指令に従って、フェーズＰ６から、フェーズＰ２、フェーズＰ４、フェーズＰ８またはフェーズＰ９に移行する。実行結果は、Ｃ＆Ｃサーバー経由で攻撃者に通知される。一方、マルウェアは、Ｃ＆Ｃサーバーへの接続に失敗した場合、別のＩＰアドレスで接続を再試行し、それでも失敗した場合には、フェーズＰ５に戻って別のＣ＆Ｃサーバーを検索するか、活動自体を停止する。なお、接続が成功するまで延々と再接続を繰り返すマルウェアの存在も報告されている。また、Ｃ＆Ｃ通信パスに異常が発生し、リカバリできない場合、マルウェアの活動はフェーズＰ５に移行する。更

に、一定期間でＣ＆Ｃサーバーを変更する動作を行うマルウェアも存在し、この場合も、マルウェアの活動はフェーズＰ５に移行する。また、フェーズＰ６は、攻撃者からの指令を待ち合わせているフェーズを含む。マルウェアは、定期的にＣ＆Ｃサーバーにアクセスして、通信パスを維持するとともに、攻撃者からの指令を待ち受ける。一定期間でＣ＆Ｃサーバーを変更する動作を行うマルウェアも存在し、この場合も、マルウェアの活動はフェーズＰ５に移行する。

【００３１】

フェーズＰ７は、搾取情報のアップロードフェーズ、即ち、マルウェア等が活動することによって得られた情報が、攻撃者側のサーバー等にアップロードされるフェーズである。

【００３２】

フェーズＰ８は、標的サイトへの通信フェーズ、即ち、マルウェアに侵入された端末が、標的のサイトに対して通信を行うフェーズである。例えば、ＭＩＴＢ（Ｍａｎ ｉｎ ｔｈｅ Ｂｒｏｗｓｅｒ）攻撃や、ＭＩＴＭ（Ｍａｎ ｉｎ ｔｈｅ Ｍｉｄｄｌｅ）攻撃等の、「端末と標的サイトとの間に立って不正な活動を行うマルウェア」に侵入された端末が、標的サイトとの通信を行うフェーズが、フェーズＰ８に相当する。このような攻撃では、端末と標的サイトとの間の通信は攻撃者による乗っ取りの対象となり、活動フェーズはフェーズＰ８からフェーズＰ６へ移行する。

【００３３】

フェーズＰ９は、攻撃活動フェーズ、即ち、攻撃者からの指令（ボット系）やマルウェア自体に組み込まれた攻撃コード（ワーム系）に従って、各種攻撃活動を行うフェーズである。攻撃標的を見つけるために、フェーズＰ１相当の活動が行われることもある。攻撃活動には、ＤｏＳ攻撃、スパムメール攻撃、Ｗｅｂ攻撃（Ｗｅｂ改ざん）、踏み台等が含まれる。

【００３４】

マルウェア振る舞い検知エンジン２５は、比較部２５１、評価値取得部２５２、補正部２５３、決定部２５４、保持部２５５、合計部２５６、判定部２５７、相関分析部２５８および分類部２５９を有することで（図３を参照）、上記のように定義されたマルウェアの活動フェーズの遷移状況を監視し、ノード９０におけるマルウェア感染を検知する。以下、マルウェア振る舞い検知エンジン２５が有する各機能部について説明する。

【００３５】

比較部２５１は、通信取得部２１によって新たに取得された通信（本実施形態では、新たに取得されて処理の対象となったパケット。以下「入力パケット」と称する）と、予め保持された通信パターンと、を比較する。通信パターンには、マルウェアの様々な活動の結果として現れる特異な通信パターンが、予め定義されている。本実施形態において、通信パターンは、マルウェアの活動遷移モデルのフェーズ毎に予め複数定義され、ネットワーク監視装置２０または管理サーバーによって保持されており、フェーズＰｎ（ここで、ｎは１から９までの整数）の通信パターンは、「Ｐｎ－ｍ」（ここで、ｍは１以上の数値）のように表される。但し、何れのフェーズにも依存しない（換言すれば、複数の異なるフェーズにおいて出現し得る）通信パターンも存在する。本実施形態において、フェーズＰ１からフェーズＰ９の何れにも依存しない通信パターンは、「Ｐ０－ｍ」で表される。

【００３６】

評価値取得部２５２は、比較部２５１による比較の結果、入力パケットと一致または近似した（以下、単に「対応する」と称する）通信パターンについて予め設定されているグレード（評価値）を、入力パケットのグレードとして取得する。グレード（Ｇｒ）は、個々の通信パターンに割り当てられる「端末が不正な活動（マルウェアの活動）をしていると推測される程度」を示す値である。本実施形態において、グレード（Ｇｒ）は、０ ≦ Ｇｒ ＜ １．０の範囲の値（小数点以下１桁）が設定されている。グレード（Ｇｒ）＝０は、マルウェアの活動の結果発生した通信パターンである可能性が極めて低いことを示し、１に近いグレードほどマルウェアの活動の結果発生した通信パターンである可能性

が高いことを示す。グレード（Ｇｒ）は、正当なアプリケーションの通信パターンとして出現する頻度に基づいて、通信パターン毎に予め決定されている。即ち、正当なアプリケーションによる通信として現れる可能性が低い通信にはより高い値のグレードが割り当てられ、正当なアプリケーションによる通信として現れる可能性が高い通信にはより低いグレードが割り当てられる。本実施形態では、通信パターンＰｎ－ｍに予め設定されたグレードが「Ｇｒ（Ｐｎ－ｍ）」、通信パターンＰｎ－ｍに該当する通信を行った端末（ｈ）に割り当てられたグレードが「Ｇｒ（ｈ，　Ｐｎ－ｍ）」で表される。

【００３７】

なお、同一の通信パターンであっても、条件に基づいて、異なるグレード（Ｇｒ）が割り当てられ得る。例えば、通信パターンに付随して２つの条件「Ａ：宛先がＣ＆Ｃサーバーに一致しない」、「Ｂ：宛先がＣ＆Ｃサーバーの１つに一致」が設定されている場合、以下のように条件判定され、宛先が登録済みのＣ＆Ｃサーバーに一致するか否かによって、異なるグレードが割り当てられる。

ＩＦ　（Ｐｎ－ｍ　＝　ＴＲＵＥ）　ＡＮＤ　（Ａ）　ＴＨＥＮ　Ｇｒ（Ｐｎ－ｍ）＝０．１、ＡＣＴＩＯＮ＝　Ｃ＆Ｃサーバー候補リストに記録

ＩＦ　（Ｐｎ－ｍ　＝　ＴＲＵＥ）　ＡＮＤ　（Ｂ）　ＴＨＥＮ　Ｇｒ（Ｐｎ－ｍ）＝０．６、ＡＣＴＩＯＮ＝Ｎｏ

【００３８】

更に、本実施形態において、評価値取得部２５２は、入力パケットと、入力パケットに係る端末によって入力パケットよりも前または後に送信または受信された他のパケット（以下、「先行パケット」「後続パケット」と称する）と、の相関分析の結果に従って、グレードを取得する。より具体的には、本実施形態において、評価値取得部２５２は、通信取得部２１によって取得された通信（入力パケット）に関して取得されたフェーズと、当該通信に係る端末に関して当該通信の前または後に行われた他の通信（先行パケットまたは後続パケット）に関して取得されたフェーズと、の間に連続性があるか否かを判定し、連続性があると判定された場合に、グレードを取得する。

【００３９】

補正部２５３は、入力パケットと先行パケットまたは後続パケットとの相関分析の結果に従って、評価値取得部２５２によって取得されたグレードを補正する。より具体的には、本実施形態において、補正部２５３は、通信取得部２１によって取得された通信（入力パケット）に関して取得されたフェーズと、当該通信に係る端末に関して当該通信の前または後に行われた他の通信（先行パケットまたは後続パケット）に関して取得されたフェーズと、の間に連続性があるか否かを判定し、連続性があると判定された場合に、評価値取得部２５２によって取得されたグレードを、連続性があると判定されなかった場合に比べてより大きく補正する。

【００４０】

換言すれば、本実施形態では、新たに取得された通信（入力パケット）と、当該通信に係る端末による過去または未来の通信（先行パケットまたは後続パケット）との相関分析が行われ、入力パケットと先行パケットまたは後続パケットとの間に、「マルウェア活動として推定される度合いをより高めるような連続性」が認められた場合に、過去または未来の通信（先行パケットまたは後続パケット）に対するグレードの取得や、新たに取得された通信（入力パケット）に対するグレードの補正が行われる。

【００４１】

決定部２５４は、入力パケットについて、当該端末に係るフェーズおよびグレードを決定する。決定部２５４は、比較部２５１による比較の結果、入力パケットに対応する通信パターンＰｎ－ｍについて予め設定されているフェーズＰｎを、当該端末に係るフェーズとして決定する。また、決定部２５４は、評価値取得部２５２によって取得されたグレードＧｒ（Ｐｎ－ｍ）をそのまま入力パケットのグレードとして決定することもあるが、補正部２５３によってグレードが補正された場合には、補正された値が、入力パケットのグレードとして決定される。

【００４２】
保持部２５５は、端末毎に、決定されたグレードのフェーズ毎の最大値を保持する。本実施形態では、保持部２５５は、マルウェア活動遷移モデルのフェーズＰｎ毎に、当該フェーズＰｎについて検出された通信パターンＰｎ－ｍのグレードＧｒ（Ｐｎ－ｍ）の最大値をフェーズＰｎのグレードとして保持し、「ＰＧｒ（Ｐｎ）」で表す。端末（ｈ）のフェーズＰｎのグレードは「ＰＧｒ（ｈ，　Ｐｎ）」で表され、以下の式を用いて取得される。
ＰＧｒ（ｈ，　Ｐｎ）　＝　ｍａｘ　｛Ｇｒ（Ｐｎ－ｍ）　｜　Ｐｎ－ｍ∈ｈ｝
【００４３】
本実施形態において、保持部２５５は、端末毎にフェーズ毎のグレード最大値を保持するグレード管理テーブルを用いて、端末毎、フェーズ毎のグレードを管理する（図示は省略する）。グレード管理テーブルには、ネットワーク監視装置２０が把握している端末（ｈ）毎に、各フェーズＰｎのグレードＰＧｒ（ｈ，　Ｐｎ）が保持される。各フェーズＰｎのグレードＰＧｒ（ｈ，　Ｐｎ）は、先述の通り、当該フェーズＰｎについて検出された通信パターンＰｎ－ｍのグレードＧｒ（Ｐｎ－ｍ）の最大値である。このため、何れかのフェーズについて新たにグレードが決定されると、新たに決定されたグレードとグレード管理テーブルに保持されているグレードＰＧｒ（ｈ，　Ｐｎ）とが比較され、最大値に更新される。なお、通信パターンＰｎ－ｍ毎のグレードＧｒ（Ｐｎ－ｍ）の最大値Ｇｒ（ｈ，　Ｐｎ－ｍ）についても、記憶装置１４ａに保持される。
【００４４】
合計部２５６は、端末毎に、フェーズＰ１からフェーズＰ９までの夫々のフェーズのグレードの最大値ＰＧｒ（ｈ，　Ｐｎ）を取得し、これらを合計する。
【００４５】
判定部２５７は、処理対象となっている端末（ｈ）の、フェーズ毎のグレードの最大値ＰＧｒ（ｈ，　Ｐｎ）に基づいて、端末が不正な活動を行っているか否かを判定する。本実施形態では、判定部２５７は、合計部２５６によって得られた合計値に基づいて、端末が不正な活動を行っているか否かを判定する。より具体的には、判定部２５７は、合計値に所定の重み付けを行うことで、「マルウェアが活動している可能性の高さを示す値」（以下、「マルウェア活動可能性」と称する）を算出し、この値が所定の閾値を超えた場合に、当該端末が不正な活動を行っていると判定する。端末（ｈ）のマルウェア活動可能性は、端末（ｈ）がマルウェアに感染している可能性の度合いを示し、「ＩＲ（ｈ）」で表される。端末（ｈ）のマルウェア活動可能性は、０（感染なし）～１００（感染の可能性大）の値を取る。即ち、本実施形態において、端末（ｈ）のマルウェア活動可能性は、以下のように定義される。ここで、ψはマルウェア活動係数を示す。
【００４６】
【数１】

$$IR(h) = min\left(\left(\varphi \sum_{n=1}^{9} PGr(h, Pn)\right), 1\right) \times 100$$

【００４７】
一般に、活動遷移モデルの多くの（連続した）フェーズ上で通信パターンが検出された端末は、より少ないフェーズ上で通信パターンが検出された端末よりも、マルウェアに感染している可能性が高いと判断できるため、マルウェア活動係数ψ（本実施形態では、具体的な値として０．５が設定される）を導入する。上記のマルウェア活動可能性ＩＲ（ｈ）は、端末（ｈ）に関連する通信パターンに対応する通信パターンが検出される都度、計算および更新される。
【００４８】
本実施形態では、マルウェア活動可能性が、０～４９の端末を「クリーン端末」、５０～８９の端末を「グレー端末」、９０～１００の端末を「ブラック端末」と定義する。管理者端末の管理画面（デバイス一覧画面）には、リアルタイムレポート情報として、端末

ごとに、マルウェア活動可能性と「クリーン」、「グレー」、「ブラック」が表示される。また、詳細情報として、端末ごとに、検出された「通信パターン」の概要と検知回数のリストが表示される。なお、「クリーン」、「グレー」、「ブラック」のマルウェア活動可能性の閾値は、管理者によって設定可能であってもよい。

【００４９】

相関分析部２５８は、入力パケットと、入力パケットに係る端末によって入力パケットよりも前または後に送信または受信された他のパケット（先行パケットまたは後続パケット）と、の相関分析を行う。即ち、本実施形態において実施される相関分析は、２つ以上の通信間または２つ以上のフェーズ間に連続性や共通性等の相関性の有無または程度を分析するものであり、相関分析の結果は、評価値取得部２５２、補正部２５３、判定部２５７および分類部２５９等によって用いられる。

【００５０】

より具体的には、本実施形態において、相関分析部２５８は、当該端末の第一の通信に基づいて決定された第一のフェーズと、当該第一の通信の前または後に行われた第二の通信に基づいて決定された第二のフェーズとの相関分析を行うことで、当該第一の通信及び当該第二の通信に係る当該端末の振る舞いの種類を決定する。相関分析部２５８は、第一のフェーズと第二のフェーズとが、予め設定された相関条件を満たす場合に、当該相関条件に対応する振る舞いの種類を、当該端末による振る舞いの種類として決定する。例えば、相関分析部２５８は、決定部２５４によって、侵入フェーズＰ１であると決定された第一の通信と、実行ファイルのダウンロードフェーズであると決定された第二の通信との相関分析を行うことで、第一の通信によるコンテンツのダウンロードと、第二の通信による実行ファイルのダウンロードとの間の相関性の有無または程度を判定する。

【００５１】

分類部２５９は、判定部２５７によって端末が不正な活動を行っていると判定された場合に、端末毎に決定された１または複数の振る舞いの種類に基づいて、当該端末による不正な活動を分類する。より具体的には、分類部２５９は、不正な活動の分類と、当該不正な活動に関連する１または複数の振る舞いの種類と、の対応関係を示す情報（例えば、マップ）を参照することで、当該端末の不正な活動を分類する。

【００５２】

ここで、分類部２５９によって決定される分類は、不正な活動の危険度を示す分類であってもよいし、不正な活動に係るマルウェア種別を示す分類であってもよい。決定される分類が不正な活動の危険度である場合、分類部２５９は、端末について決定された１または複数の振る舞いの種類に基づいて、当該端末の不正な活動の危険度を決定する。一方、決定される分類が不正な活動に係るマルウェア種別である場合、分類部２５９は、端末について決定された１または複数の振る舞いの種類に基づいて、当該端末の不正な活動に係るマルウェア種別を決定する。なお、危険度を分類する場合、分類部２５９は、高い危険度に係る振る舞いから順に検討していき、最初に一致した危険度を設定することが好ましい。

【００５３】

なお、分類部２５９は、合計部２５６によって算出されたマルウェア活動可能性が所定値（例えば、８０）未満の場合には、分類を行わないこととしてもよい。この場合、分類を示す値が設定されるフィールドには、「未分類（Ｕｎｃｌａｓｓｉｆｉｅｄ）」を示す値が設定される。

【００５４】

＜処理の流れ＞

次に、本実施形態に係るシステム１によって実行される処理の流れを、フローチャートを用いて説明する。なお、以下に説明するフローチャートに示された処理の具体的な内容および処理順序は、本発明を実施するための一例である。具体的な処理内容および処理順序は、本発明の実施の形態に応じて適宜選択されてよい。

【００５５】

ネットワーク監視装置２０は、新たなネットワークに接続されると、後述するパケット毎の検知処理を開始する前に、準備処理として、ネットワーク構成の解析／学習処理を実行する。具体的には、ネットワーク監視装置２０は、新たなネットワークに接続されると、所定時間パケットを取得して、取得されたパケットを解析することで、監視対象となるネットワークの構成を解析し、マルウェア検知に必要な情報（デバイス一覧（デバイスタイプ、ＯＳ種別、ＭＡＣ／ＩＰアドレス等）、監視対象ネットワークのアドレス体系、ＤＮＳサーバー情報、メールサーバー情報、プロキシ（ＨＴＴＰ／ＳＯＣＫＳ）情報、Ａｃｔｉｖｅ　Ｄｉｒｅｃｔｏｒｙ情報等）を学習し、記憶装置１４ａ等に保存する。

【００５６】

なお、ネットワーク構成の解析／学習処理は、後述する検知処理が開始された後も、ネットワーク監視装置２０によって継続的に実行される。即ち、ネットワーク監視装置２０は、取得されたパケットを解析して得られた情報と、以前の解析／学習処理によって学習され、ネットワーク監視装置２０の記憶装置１４ａに保持されている情報とを照合し、照合の結果、新たに得られた情報が保持されている情報と異なる場合、ネットワーク監視装置２０は、ネットワークセグメント２における構成が変更されたと判断し、新たに得られた情報を用いて、ネットワーク監視装置２０の記憶装置１４ａに保持されている情報を更新する。

【００５７】

図５は、本実施形態に係る、パケット毎の検知処理の流れの概要を示すフローチャートである。本実施形態に係る検知処理は、ネットワーク監視装置２０によって、ネットワーク上を流れるパケット（または、複数パケットからなるデータ）が取得される度に実行される。

【００５８】

ステップＳ００１では、パケット解析の前処理が実行される。ネットワーク監視装置２０は、通信取得部２１によって新たに通信（入力パケット）が取得されると、入力パケットの整形、分類、および有効な既存フローへの関連付けを行う。また、ネットワーク監視装置２０は、入力パケットを端末単位（送信元／宛先ＩＰアドレス（ＭＡＣアドレス）単位）、プロトコル（ＴＣＰ／ＵＤＰ、ＩＣＭＰ、ＤＮＳ、ＨＴＴＰ、ＨＴＴＰＳ、ＩＲＣ、ＦＴＰ、ＴＦＴＰ、ＳＯＣＫＳ、ＮｅｔＢＩＯＳ等）単位に分類、および既存フローとの関連付けを行う。その後、処理はステップＳ００２へ進む。

【００５９】

ステップＳ００２からステップＳ００５では、アプリケーション検知エンジン２３およびプロトコルアノマリ検知エンジン２４による処理が行われる。本実施形態に係るネットワーク監視装置２０は、上述した３種類の検知エンジン（検知プログラム）を用いて、ネットワークに接続された端末による不正な通信を検知するが、本実施形態において、ネットワーク監視装置２０は、パケットを取得すると、アプリケーション検知エンジン２３およびプロトコルアノマリ検知エンジン２４による検知を行った後で、マルウェア振る舞い検知エンジン２５による検知を行う。即ち、本実施形態において、マルウェア振る舞い検知エンジン２５は、他の検知手段（アプリケーション検知エンジン２３およびプロトコルアノマリ検知エンジン２４）によって不正な通信として検知されなかった通信に基づいて、ノード９０が不正な活動を行っているか否かを判定する。このようにすることで、本実施形態によれば、マルウェア振る舞い検知エンジン２５によって処理されるパケットの数を減らし、振る舞い検知エンジンの動作によって生じる負荷を減らすことが出来る。但し、マルウェア振る舞い検知エンジン２５は、単体で動作してもよいし、その他の検知エンジンと組み合わせて動作されてもよい。また、パケットが取得された際の検知エンジンの処理順序は、本実施形態に示した例に限定されない。

【００６０】

アプリケーション検知エンジン２３によって不要なアプリケーションが検知された場合や、プロトコルアノマリ検知エンジン２４によってプロトコルアノマリが検知された場合、処理はステップＳ０１２へ進み、遮断またはアラート発行が行われる。一方、不要なア

プリケーションやプロトコルアノマリが検知されなかった場合、処理はステップＳ００６へ進む。なお、本フローチャートにおいて、ステップＳ００６からステップＳ０１１までの処理は、マルウェア振る舞い検知エンジン２５による処理に相当する。

【００６１】

ステップＳ００６では、通信パターンの判定処理が行われる。比較部２５１は、入力パケットと予め定義された通信パターン（Ｐｎ－ｍ）とを比較することで、入力パケットと予め定義された通信パターン（Ｐｎ－ｍ）との共通性を判定する。ここで、通信パターン（Ｐｎ－ｍ）と共通性があると判定された場合、入力パケットに係る端末（ｈ）の活動遷移モデル上のフェーズはフェーズＰｎ（ｈ）に決定される。また、評価値取得部２５２は、判定の結果、一致または近似する（対応する）と判定された通信パターンのグレードＧｒ（Ｐｎ－ｍ）を、端末（ｈ）に関連づけて、入力パケットのグレードＧｒ（ｈ，　Ｐｎ－ｍ）として取得する。更に、ネットワーク監視装置２０は、検出した通信パターンに基づいて、対象通信の送信元端末または宛先端末を「マルウェア配布サーバー候補リスト」、または「Ｃ＆Ｃサーバー候補リスト」に登録する。ここでは、パケットロストを考慮して、すべてのフェーズの通信パターンを対象に判定および評価が行われる。なお、既知の判定済みフローと関連付いているために、追加の判定処理が不要な入力パケットについては、判定は行われず、統計情報の更新のみが行われる。その後、処理はステップＳ００７へ進む。

【００６２】

ステップＳ００７では、第一の相関分析が行われる。通信パターンの判定処理（ステップＳ００６）は、予め定義された「通信パターン」に基づいている。従って、この処理のみでは、通信パターンに一致しない通信を行うマルウェアを検知できない。このため、本実施形態では、第一の相関分析を行うこととしている。評価値取得部２５２は、ステップＳ００６で検出できなかったＣ＆Ｃ通信をピックアップする。評価値取得部２５２は、探索フェーズＰ２、感染・浸潤フェーズＰ３、実行ファイルのダウンロードフェーズＰ４、攻撃活動フェーズＰ９に遷移する際に、そのトリガーとなった通信をピックアップし、ネットワーク監視装置２０は、対象通信の送信元端末または宛先端末Ｃ＆Ｃサーバー候補リストに登録する。なお、第一の相関分析の処理内容については、図６から図８を参照して後述する。その後、処理はステップＳ００８へ進む。

【００６３】

ステップＳ００８では、第二の相関分析が行われる。マルウェアは、マルウェア活動遷移モデルのフェーズを遷移しながら活動を深化させていく。従って、遷移した直後のフェーズでの活動（通信）が、一つ前のフェーズでの活動（通信）をトリガーにして発生した可能性が高い場合（換言すれば、前後のフェーズに相関性がある場合）、当該端末はマルウェアに感染している確率が高いと判断できる。このトリガーを通信パターンに含まれるデータ内容（例えば、Ｃ＆Ｃサーバーからの指令内容）から判断する方法も考えられるが、データ部を暗号化や難読化しているマルウェアも多く、リアルタイムに解析・判定することは困難である。このため、本実施形態では、フェーズの遷移に要した時間（通信パターンＰｒ－ｓを検出してから通信パターンＰｍ－ｎを検出するまでの時間）、通信先（コールバック通信）の端末（ｈ）、マルウェア感染の可能性が高い複数端末の挙動の相関性および一致性、扱ったファイルの種類等の情報に基づいて第二の相関分析（ステップＳ００８を参照）を行う。分析の結果、マルウェアの挙動の疑いが高い通信であると判定できた場合は、その通信に対応する通信パターンＰｍ－ｎのグレードＧｒ（Ｐｍ－ｎ）を補正（マルウェアの挙動類似係数θ倍）し、より高いグレードを付与する。

【００６４】

補正部２５３は、ステップＳ００６で判定された端末（ｈ）の活動フェーズＰｎ（ｈ）について、その直前に活動していたフェーズとの連続性や他の（感染）端末の挙動との相関性を分析する。分析の結果、マルウェアの挙動である疑いの高い通信パターンが発見された場合、補正部２５３は、ステップＳ００６で判定した端末（ｈ）の通信パターン（Ｐｎ－ｍ）のグレードＧｒ（ｈ，　Ｐｎ－ｍ）を、以下の式を用いて補正し、より高いグレ

ードを割り当てる。
Ｇｒ（ｈ，　Ｐｎ－ｍ）　＝　θ・Ｇｒ（ｈ，　Ｐｎ－ｍ）
但し、マルウェア挙動類似係数θの範囲は１．０から２．０。ここで１．０は「類似性なし」を意味する。なお、第二の相関分析の処理内容、およびマルウェア挙動類似係数θについては、図６から図８を参照して後述する。その後、処理はステップＳ００９へ進む。
【００６５】
なお、相関分析は、端末による複数の通信が、マルウェアの活動に伴うフェーズの遷移の観点から相関性を有しているか否かを分析するものであればよく、本実施形態に示された例に限定されない。
【００６６】
ステップＳ００９では、活動フェーズのグレード（ＰＧｒ）が決定される。決定部２５４は、ステップＳ００６からステップＳ００８の処理結果に基づいて、対応する端末ｈの通信パターンのグレードＧｒ（ｈ，　Ｐｎ－ｍ）から、フェーズＰｎのグレードＰＧｒ（ｈ，　Ｐｎ）ｉを決定する。なお、ここで、ＰＧｒ（ｈ，　Ｐｎ）ｉ－１は、前回までのフェーズＰｎのグレードを示す。
ＰＧｒ（ｈ，　Ｐｎ）ｉ　＝　ｍａｘ　｛ＰＧｒ（ｈ，　Ｐｎ）ｉ－１　，　Ｇｒ（ｈ，　Ｐｎ－ｍ）｝
その後、処理はステップＳ０１０へ進む。
【００６７】
ステップＳ０１０では、マルウェア活動可能性（ＩＲ（ｈ））が算出される。合計部２５６および判定部２５７は、端末ｈのマルウェア活動可能性ＩＲ（ｈ）を算出する。具体的な算出方法については、合計部２５６および判定部２５７の説明において上述した通りである。その後、処理はステップＳ０１１へ進む。
【００６８】
ステップＳ０１１およびステップＳ０１２では、マルウェア活動可能性ＩＲ（ｈ）が所定の閾値以上である場合に、該当端末の遮断や管理者アラート発行等の対処が行われる。判定部２５７は、ステップＳ０１０で算出された端末のマルウェア活動可能性が「ブラック」を示す所定の閾値以上であるか否かを判定する（ステップＳ０１１）。そして、マルウェア活動可能性が「ブラック」の場合、通信遮断部２２は、該当端末による通信を遮断する、または管理者にアラートを発行する等の対処を行う（ステップＳ０１２）。また、マルウェア活動可能性が「グレー」の場合にも、ネットワーク監視装置２０は、管理者にアラートを発行してよい。マルウェア活動可能性が「クリーン」の場合は、遮断やアラートの発行等の対処は行われない。その後、本フローチャートに示された処理は終了する。
【００６９】
図６から図８は、本実施形態に係る、マルウェア振る舞い検知エンジン２５による検知処理の流れを示すフローチャートである。本フローチャートは、図５を用いて説明した検知処理のステップＳ００６からステップＳ０１２の処理をより詳細に説明するものである。より具体的には、ステップＳ１０１からステップＳ１０３は、図５のステップＳ００６で説明した通信パターン判定処理をより詳細に説明するものであり、ステップＳ１０４からステップＳ１１０は、ステップＳ００７で説明した第一の相関分析処理をより詳細に説明するものであり、ステップＳ１１１からステップＳ１１６は、ステップＳ００８で説明した第二の相関分析処理をより詳細に説明するものであり、ステップＳ１１７からステップＳ１２０は、ステップＳ００９で説明した活動フェーズのグレード決定処理をより詳細に説明するものである。また、ステップＳ１２１は、図５のステップＳ０１０に相当し、ステップＳ１２２およびステップＳ１２３は、ステップＳ０１１およびステップＳ０１２に相当する。
【００７０】
ステップＳ１０１およびステップＳ１０２では、取得されたパケット（入力パケット）が、予め定義された通信パターンの何れに該当するかが判定される。比較部２５１は、入力パケットと予め保持された通信パターンとを比較することで、入力パケットと予め定義

された通信パターン（Ｐｎ－ｍ）との共通性を判定する。判定の結果、何れの通信パターンにも該当しないと判定された場合、当該パケットに係る処理は終了し、本フローチャートに示された処理は終了する。一方、何れかの通信パターンに該当すると判定された場合、処理はステップＳ１０３へ進む。

【００７１】

ステップＳ１０３では、入力パケットに係る端末に関して、該当すると判定された通信パターン（Ｐｎ－ｍ）が検出されたことが記録される。また、評価値取得部２５２は、入力パケットに対応する通信パターン（Ｐｎ－ｍ）が属するフェーズＰｎおよび通信パターン（Ｐｎ－ｍ）に予め設定されているグレードＧｒ（Ｐｎ－ｍ）を、入力パケットに係る端末（ｈ）のフェーズＰｎ（ｈ）、および当該フェーズのグレードＧｒ（ｈ，　Ｐｎ－ｍ）として取得する。その後、処理はステップＳ１０４へ進む。

【００７２】

ステップＳ１０４およびステップＳ１０５では、入力パケットに対応する通信パターンに必須条件が設定されている場合に、必須条件に対応する通信が過去に取得されているか否かが判定される。必須条件が設定されていない場合、処理はステップＳ１０７へ進む。ここで、必須条件とは、ステップＳ１０１において入力パケットに対応すると判定された通信パターン（Ｐｎ－ｍ）に予め設定されているグレードＧｒ（Ｐｎ－ｍ）を、当該入力パケットに係る端末（ｈ）のフェーズＰｎ（ｈ）のグレードＧｒ（ｈ，　Ｐｎ－ｍ）として決定してよいか否かを判定するための条件である。例えば、「Ｐ６－４：　ＨＴＴＰ標準ポート（８０）を宛先ポートとしたＨＴＴＰ通信（プロキシ／非プロキシ）」の通信パターンはＨＴＴＰの一般的な通信であるが、この通信パターンは、「Ｐ０－１～Ｐ０－１５」に定義されている「ＨＴＴＰ悪性通信パターン」の何れかが検知されていることが必須条件である。このため、これらの必須条件が満たされた場合に、当該入力パケットについて通信パターンＰ６－４のグレードＧｒ（ｈ，　Ｐ６－４）が決定され、必須条件が満たされない場合は、当該入力パケットについて通信パターンＰ６－４のグレードＧｒ（ｈ，　Ｐ６－４）は決定されない。

【００７３】

即ち、評価値取得部２５２は、入力パケットに関して取得されたフェーズと、当該通信に係る端末に関して当該通信の前に行われた他の通信（先行パケット）に関して取得されたフェーズと、の間に連続性があるか否かを、過去に取得された通信が必須条件を満たしているか否かを判定することで判定する。必須条件が満たされないと判定された場合、処理はステップＳ１０６へ進み、当該入力パケットのグレードは０（ゼロ）に設定される。一方、必須条件が満たされると判定された場合、処理はステップＳ１０７へ進む。

【００７４】

ステップＳ１０７では、入力パケットに係る端末のフェーズにグレードが割り当てられる。評価値取得部２５２は、入力パケットについて、該当すると判定された通信パターンＰｎ－ｍに予め定義されたグレードＧｒ（Ｐｎ－ｍ）を取得し、端末（ｈ）のフェーズＰｎ（ｈ）のグレードＧｒ（ｈ，　Ｐｎ－ｍ）とする。その後、処理はステップＳ１０８へ進む。

【００７５】

ステップＳ１０８では、入力パケットが、過去に検知された通信パターンの必須条件に該当するか否かが判定される。換言すれば、ステップＳ１０８では、過去に取得された通信（先行パケット）から見て未来にあたる現時点において、必須条件に該当する通信（入力パケット）が検知されたか否かが判定される。評価値取得部２５２は、入力パケットの通信パターンが必須条件に設定されている通信パターンが、過去に検出されているか否かを判定する。判定の結果、入力パケットに係る通信パターンを必須条件とする通信パターンが過去に検出されていないと判定された場合、処理はステップＳ１１１へ進む。一方、判定の結果、入力パケットに係る通信パターンを必須条件とする通信パターンが過去に検出されていると判定された場合、処理はステップＳ１１０へ進む。

【００７６】

ステップＳ１１０では、過去に取得された通信（先行パケット）のフェーズにグレードが割り当てられる。評価値取得部２５２は、過去に検出された通信に、当該通信パターン（Ｐｎ－ｍ）に予め定義されたグレードＧｒ（Ｐｎ－ｍ）を取得し、割り当てる。その後、処理はステップＳ１１１へ進む。

【００７７】

ステップＳ１１１およびステップＳ１１２では、入力パケットに対応する通信パターンにグレード補正条件が設定されている場合に、グレード補正条件に該当する通信が過去に取得されているか否かが判定される。グレード補正条件が設定されていない場合、処理はステップＳ１１４へ進む。ここで、グレード補正条件とは、ステップＳ１０１において入力パケットに対応すると判定された通信パターン（Ｐｎ－ｍ）に予め設定されているグレードＧｒ（Ｐｎ－ｍ）をより大きな値に補正すべきか否かを判定するための条件である。補正部２５３は、グレード補正条件に該当する通信が、入力パケットに係る端末について過去に検知されているか否かを判定する。グレード補正条件が満たされないと判定された場合、グレードの補正は行われず、処理はステップＳ１１４へ進む。一方、必須条件が満たされると判定された場合、処理はステップＳ１１３へ進む。

【００７８】

ステップＳ１１３では、グレードの補正が行われる。補正部２５３は、ステップＳ１１２で満たされたと判定されたグレード補正条件について予め設定された補正値に従って、ステップＳ１０７で割り当てられたグレードＧｒ（ｈ，　Ｐｎ－ｍ）を補正する。例えば、補正値が１．５である場合、グレードＧｒ（ｈ，　Ｐｎ－ｍ）の値が１．５倍される。その後、処理はステップＳ１１４へ進む。

【００７９】

ステップＳ１１４では、入力パケットが、過去に検知された通信パターンのグレード補正条件に該当するか否かが判定される。換言すれば、ステップＳ１１４では、過去に取得された通信（先行パケット）から見て未来にあたる現時点において、グレード補正条件に該当する通信（入力パケット）が検知されたか否かが判定される。補正部２５３は、入力パケットの通信パターンがグレード補正条件に設定されている通信パターンが、過去に検出されているか否かを判定する。判定の結果、入力パケットに係る通信パターンをグレード補正条件とする通信パターンが過去に検出されていないと判定された場合、処理はステップＳ１１７へ進む。一方、判定の結果、入力パケットに係る通信パターンをグレード補正条件とする通信パターンが過去に検出されていると判定された場合、処理はステップＳ１１６へ進む。

【００８０】

ステップＳ１１６では、過去の通信（先行パケット）に係るグレードの補正が行われる。補正部２５３は、過去に検出された通信パターンに係る端末に割り当てられていたグレードを、当該グレード補正条件について予め定義された補正値で補正する。例えば、補正値が１．５である場合、グレードが１．５倍される。その後、処理はステップＳ１１７へ進む。

【００８１】

ステップＳ１１７からステップＳ１２０では、フェーズ毎の最大グレードの更新処理が行われる。まず、ネットワーク監視装置２０は、入力パケットに係る端末について、検知フェーズ（Ｐ１からＰ９）毎に保持されている最大グレード（補正されているグレードについては、補正後の値）を、グレード管理テーブルから取得し（ステップＳ１１７）、ステップＳ１０１からステップＳ１１６までの処理の結果決定部２５４によって決定されたグレードと比較することで、各フェーズにおいて、最大グレードが更新されたか否かを判定する（ステップＳ１１８）。ここで、最大グレードが更新されていないと判定された場合、処理はステップＳ１２１へ進む。一方、最大グレードが更新されたと判定された場合、保持部２５５は、新たに割り当てられたグレードをもって、グレード管理テーブルに記録された最大グレードを更新し、これを保持する（ステップＳ１２０）。なお、この過程で、証跡ログが採取される（ステップＳ１１９）。その後、処理はステップＳ１２１へ進

む。
【００８２】
ステップＳ１２１では、端末におけるマルウェア活動可能性が算出される。合計部２５６は、当該端末ｈの各フェーズで求められた最大グレードを合算し、判定部２５７は、マルウェア活動係数を乗算することで、端末ｈのマルウェア活動可能性ＩＲ（ｈ）を算出する。詳細な算出方法は、合計部２５６および判定部２５７の説明において上述した通りである。その後、処理はステップＳ１２２へ進む。
【００８３】
ステップＳ１２２およびステップＳ１２３では、対象ノード９０の、マルウェア感染の有無が判定される。判定部２５７は、ステップＳ１２１で算出されたマルウェア活動可能性ＩＲ（ｈ）が所定の閾値を超えているか否かを判定する（ステップＳ１２２）。ここで、マルウェア活動可能性ＩＲ（ｈ）が閾値を超えていると判定された場合、ネットワーク監視装置２０は、マルウェア感染が検知された際の所定の対応を行う。マルウェア感染が検知された際の対応としては、例えば、通信遮断部２２による当該ノード９０の通信遮断開始や、当該ノード９０がマルウェアに感染していることのアラート（警告）の通知等が挙げられる。一方、マルウェア活動可能性ＩＲ（ｈ）が閾値を超えていないと判定された場合には、通信遮断や警告等の、マルウェア感染が検知された際の対応は行われない。その後、本フローチャートに示された処理は終了する。
【００８４】
なお、ネットワーク監視装置２０は、例えば、Ｌ２／Ｌ３スイッチから取得された通信データを破棄する方法、Ｌ２／Ｌ３スイッチのポートを遮断する方法、ノード９０に対してＡＲＰ偽装によるパケット送信先の誘導を行う方法、ルータ１０に指示してノード９０に係る通信を破棄させる方法、またはノード９０が属するＶＬＡＮを変更して隔離する方法、等を用いて、ノード９０による通信を遮断することができる。また、ネットワーク監視装置２０がルータ１０に搭載（内包）されている場合には、ノード９０が受信または送信する通信を直接遮断することもできる。また、ネットワーク監視装置２０は、管理サーバーやノード９０、予め設定された管理者端末等に通知パケットやメール等を送信する方法や、ネットワーク監視装置２０自身に設けられた表示装置（ディスプレイやＬＥＤ等）を介して警告表示する方法等を用いて、アラートを通知することが出来る。
【００８５】
＜端末による活動の分類＞
マルウェアには、高度標的型攻撃に代表される、標的とした組織や企業の機密情報の窃取やシステムの破壊を目的とするもの、オンラインバンキングから金銭の窃取を目的とするもの、パソコン内のファイルの暗号化やパソコンをロックして身代金を要求するもの、利用者が望まない広告を表示して最終的に金銭的な利益を得ようとするもの、単に、嫌がらせの目的で恐怖を煽る画面を表示するものなど、致命的な被害を与えるものから軽微な被害で済むものまで、様々な脅威を有するマルウェアが存在する。
【００８６】
しかし、図６から図８を参照して説明した検知処理では、何らかのマルウェアに感染していることは検知できるが、感染したマルウェアの脅威（危険度）やマルウェア種別が判らないため、同時期に複数発生するマルウェア検知事象に対して「対処の優先度付け」ができないという課題や、攻撃手法の把握と適切な対策の決定に時間がかかるという課題があった。
【００８７】
このため、本実施形態では、相関分析部２５８が端末による振る舞いの種類を決定し、分類部２５９が振る舞いの種類に基づいて端末による不正な活動を分類することで、当該端末がどれだけ危険な状態にあるかを判断するために役立つ情報を得ることとした。
【００８８】
図９は、本実施形態に係る危険度分類処理の流れを示す図である。本フローチャートに示された処理は、ネットワーク監視装置２０が起動している間、図５から図８を用いて説

明した、パケット毎の検知処理と平行して実行される。

【００８９】

ステップＳ８０１及びステップＳ８０２では、端末（ｈ）において、何れかの相関条件に合致する振る舞いが新たに検出された場合に、合致した相関条件ＣＡが、当該端末（ｈ）の振る舞いの種類ＣＡとして蓄積される。相関分析部２５８は、図５から図８を用いて説明したパケット毎の検知処理において、入力パケットに係る端末（ｈ）について、何らかの新たな相関条件に合致したか否かを判定する（ステップＳ８０１）。新たな相関条件に合致した場合、相関分析部２５８は、当該相関条件に対応する振る舞いの種類を、当該端末による振る舞いの種類として決定し、ＲＡＭ１３ａ上のテーブル等に、端末（ｈ）の識別情報と関連づけて蓄積する（ステップＳ８０２）。

【００９０】

以下に、相関分析部２５８が端末による振る舞いの種類を決定するために用いられる、危険度の判定に使用される相関条件と当該相関条件に対応するマルウェアの振る舞いとの関係を例示する。ここで、相関条件ＣＡ（ｍ－ｎ－ｘ）は、端末（ｈ）の活動フェーズがフェーズＰｍからフェーズＰｎに遷移した際に観測されるトラフィックの振る舞いに関する相関条件を示す。

・ＣＡ（１－４－ｍ）（ｍ＝１～１１）：Ｅｘｐｌｏｉｔ　ＫｉｔによるＤｒｉｖｅ－ｂｙ　Ｄｏｗｎｌｏａｄ攻撃
・ＣＡ（２－６－ｍ）（ｍ＝２，３）：ネットワーク環境探索後のＣ＆Ｃ通信の検出
・ＣＡ（３－３－１）：感染拡大
・ＣＡ（３－６－ｍ）（ｍ＝１～３）：感染拡大後のＣ＆Ｃ通信の検出
・ＣＡ（４－２－２）：マルウェアのアクティベート直後のネットワーク環境の探索
・ＣＡ（４－４－３）：複数の攻撃用ツールまたは別のマルウェアのダウンロード
・ＣＡ（４－４－５）：メールに添付されたファイル操作によるダウンロード
・ＣＡ（４－６－ｍ）（ｍ＝１～４）：マルウェア侵入後のＣ＆Ｃ通信の検出
・ＣＡ（５－５－１）：有効なＣ＆Ｃサーバーの探索
・ＣＡ（５－６－１）：有効なＣ＆Ｃサーバーの探索後のＣ＆Ｃ通信の検出
・ＣＡ（６－３－ｍ）（ｍ＝１～３）：感染拡大
・ＣＡ（６－４－ｍ）（ｍ＝１～５）：攻撃用ツールまたは別のマルウェアのダウンロード
・ＣＡ（６－６－ｍ）（ｍ＝１，２）：有効なＣ＆Ｃサーバーの探索
・ＣＡ（６－６－ｍ）（ｍ＝３～６）：Ｃ＆Ｃビーコン
・ＣＡ（６－６－８）：セキュリティ装置を攪乱する疑わしい挙動の通信の検出
・ＣＡ（６－６－１０）：Ｃ＆Ｃビーコン
・ＣＡ（６－６－１１）：セキュリティ装置（プロキシ）がアクセスを禁止した疑わしい通信
・ＣＡ（６－６－ｍ）（ｍ＝１２～１４）：攻撃者によるリモートコントロール操作
・ＣＡ（６－６－１５）：Ｃ＆Ｃビーコン
・ＣＡ（６－７－ｍ）（ｍ＝１，２）：窃取情報のアップロード
・ＣＡ（７－６－１）：窃取情報のアップロード
・ＣＡ（８－６－ｍ）（ｍ＝１，２）：ＭＩＴＢ（Ｍａｎ　ｉｎ　ｔｈｅ　Ｂｒｏｗｓｅｒ）、ＭＩＴＭ（Ｍａｎ　ｉｎ　ｔｈｅ　Ｍｉｄｄｌｅ）

なお、遷移元のフェーズと遷移先のフェーズが同じであっても（例えば、フェーズＰ１からフェーズＰ４へのフェーズ遷移）、フェーズ遷移に伴うその他の付帯的条件に基づいて異なる振る舞いと扱われる場合がある。相関条件ＣＡ（ｍ－ｎ－ｘ）の符号ｘは、それらの付帯的条件に付される符号である。例えば、相関条件ＣＡ（１－４－１）は、入力パケットに係る端末（ｈ）がフェーズＰ１からフェーズＰ４へ遷移する振る舞い相関条件ＣＡ（１－４－ｘ）のうち、「フェーズＰ１の通信パターンＰ１－ｍを検出」、且つ「Ｐ１－ｍ検出後、検出したＰ１－ｍと同一のＴＣＰコネクション上で、フェーズＰ４の通信パターンＰ４－ｎを検出」という相関条件を満たした振る舞いである。

【００９１】
新たな相関条件が検出されていない場合、検出されるまで、ステップＳ８０１の処理は繰り返し実行される。一方、新たな相関条件が検出され、端末の振る舞いの種類が決定された場合、処理はステップＳ８０３へ進む。
【００９２】
ステップＳ８０３からステップＳ８１０では、端末の危険度が決定される。分類部２５９は、ステップＳ８０１からステップＳ８０２の処理が繰り返されることで蓄積された、端末（ｈ）について記録されている振る舞いの種類（相関条件）を読み出す（ステップＳ８０３）。そして、分類部２５９は、不正な活動の分類と、当該不正な活動に関連する１または複数の振る舞いの種類（相関条件）と、の対応関係を示す情報を参照することで、当該端末の不正な活動を分類する（ステップＳ８０４からステップＳ８１０）。
【００９３】
以下に、分類部２５９が端末の危険度を決定するために用いられる、危険度と当該危険度に対応する１または複数の相関条件（振る舞いの種類）との関係を例示する。ここで、危険度ＲＡ（ｍ－ｎ）は、危険度の高さｍ（Ｃ：重大、Ｈ：高、Ｍ：中、Ｌ：低）と、同一レベルの危険度における危険の種類ｎを示す。以下、「相関条件を検出する」との記載は、「端末の挙動が相関条件に合致することで、当該相関条件に対応する振る舞いの種類が検出された」ことを意味する。
ＲＡ（Ｃ－１）：継続的な攻撃に起因した複数の高リスクな活動を検出した。
条件：ＲＬ（ｈ）＝高の条件ＲＡ（Ｈ－ｍ）（ｍ＝１～１４）のうち、異なる２つ以上のＲＡ（Ｈ－ｍ）（ｍ＝１～１４）を検出した。
ＲＡ（Ｈ－１）：ドライブバイダウンロード攻撃に起因した侵入活動を検出した。
条件：相関条件ＣＡ（１－４－ｍ）（ｍ＝１～１１）のいずれかを検出し、
　上記の相関条件を検出後、
　　ＣＡ（４－６－ｎ）（ｎ＝１～４）のいずれか、
　　ＣＡ（６－６－ｎ）（ｎ＝３～６）のいずれか、または
　　ＣＡ（６－６－１０）またはＣＡ（６－６－１１）の何れかを検出し、かつ
　ＩＲ値がＲｅｄ（８０％）以上である、または、上記の条件を検出後にＲｅｄ（８０％）まで上昇した。
ＲＡ（Ｈ－２）：電子メールに添付された疑わしいファイルやＵＲＬリンクの操作に起因した侵入活動を検出した。
条件：相関条件ＣＡ（４－４－５）を検出し、
　上記の相関条件を検出後、
　　ＣＡ（４－６－ｎ）（ｎ＝１～４）のいずれか、
　　ＣＡ（６－６－ｎ）（ｎ＝３～６）のいずれか、または
　　ＣＡ（６－６－１０）またはＣＡ（６－６－１１）の何れかを検出し、かつ
　ＩＲ値がＲｅｄ（８０％）以上である、または、上記の条件を検出後にＲｅｄ（８０％）まで上昇した。
ＲＡ（Ｍ－３）：ドライブバイダウンロード攻撃によってダウンロードされた不審なファイルを検出した。
条件：相関条件ＣＡ（１－４－ｍ）（ｍ＝１～１１）のいずれかを検出した。
ＲＡ（Ｍ－４）：怪しいファイルを操作することによってダウンロードされた不審なファイルを検出した。
条件：相関条件ＣＡ（４－４－５）を検出した。
ＲＡ（Ｌ－１）：
条件：上記のＲＡ（Ｈ－ｍ）、ＲＡ（Ｍ－ｎ）のいずれにも一致しない。
【００９４】
分類の際、分類部２５９は、高い危険度に係る振る舞いから順に検討していき、最初に一致した危険度を設定することで、誤って低い危険度が設定されてしまうことを防ぐ（フローチャートを参照）。危険度の設定が完了すると、処理はステップＳ８０１へ戻る。

【００９５】
上記説明した危険度分類処理によれば、攻撃者の行動が組織や企業に与える被害の重大度に基づいて、端末による不正な活動の危険度を付与することが出来、対処の優先度付けの指針として重要な情報とすることが出来る。このような指標は、同時期に数十台のデバイスでマルウェア感染が検知されることもある規模の大きなネットワークにおいて効果が大きい。
【００９６】
また、感染マルウェアの危険度は、既知のマルウェアであれば、短時間で判明するが、昨今増加している亜種や未知のマルウェアに対しては、マルウェアが有する機能分析を通して明らかになるのが一般的であり、時間がかかる。しかし、本実施形態に係る危険度分類処理によれば、感染直後からの通信の振る舞いから危険度を推測することが可能であり、既知、未知（含む、亜種）マルウェアの機能分析を行うことなく危険度を判定でき、マルウェア感染に対する対処の優先度付けが可能になり、迅速な対応、対策を取ることができる。
【００９７】
図１０及び図１１は、本実施形態に係るマルウェア種別分類処理の流れを示す図である。本フローチャートに示された処理は、ネットワーク監視装置２０が起動している間、図５から図８を用いて説明した、パケット毎の検知処理と平行して実行される。
【００９８】
ステップＳ９０１及びステップＳ９０２では、端末（ｈ）のマルウェア活動可能性ＩＲ（ｈ）が所定値以上となった場合に、この際新たに検出された振る舞いの種類ＣＡが、当該端末（ｈ）の振る舞いの種類ＣＡとして蓄積される。相関分析部２５８は、図５から図８を用いて説明したパケット毎の検知処理において算出されたマルウェア活動可能性ＩＲ（ｈ）が、所定値（例えば、８０）以上となったか否かを判定する（ステップＳ９０１）。
【００９９】
マルウェア活動可能性ＩＲ（ｈ）が所定値未満である場合、正確なマルウェア種別の判定は困難であるため、端末（ｈ）において活動するマルウェア種別を示す値が設定されるフィールドには、「未分類（Ｕｎｃｌａｓｓｉｆｉｅｄ）」を示す値が設定される（図示は省略する）。
【０１００】
一方、端末（ｈ）のマルウェア活動可能性ＩＲ（ｈ）が所定値以上となった場合、相関分析部２５８は、この際新たに検出された振る舞いの種類を、当該端末による振る舞いの種類として決定し、ＲＡＭ１３ａ上のテーブル等に、端末（ｈ）の識別情報と関連づけて蓄積する（ステップＳ９０２）。
【０１０１】
以下に、ネットワーク上の振る舞いから推定できるマルウェアの代表的な機能と、その機能の有無を判定するために使用する相関条件を、昨日のカテゴリ毎に例示する。上記説明した危険度分類処理と同様、相関条件ＣＡ（ｍ－ｎ－ｘ）は、端末（ｈ）の活動フェーズがフェーズＰｍからフェーズＰｎに遷移した際に観測されるトラフィックの振る舞いに関する相関条件を示す。
［機能カテゴリＡ：機密情報の窃取とアップロード（Ｄａｔａ　Ｅｘｆｉｌｔｒａｔｉｏｎ）］
・ＣＡ（６－７－ｎ）ｎ＝１，２：窃取情報のアップロード
・ＣＡ（７－６－１）：窃取情報のアップロード
・ＣＡ（８－６－ｎ）ｎ＝１，２：ＭＩＴＢ、ＭＩＴＭ
［機能カテゴリＢ：疑わしいファイル（バイナリ、構成定義など）のダウンロード（Ｄｏｗｎｌｏａｄ　ｏｆ　Ｍａｌｉｃｉｏｕｓ　Ｆｉｌｅ）］
・ＣＡ（１－４－ｎ）ｎ＝１～１１：Ｅｘｐｌｏｉｔ　ＫｉｔによるＤｒｉｖｅ－ｂｙ　Ｄｏｗｎｌｏａｄ攻撃

・ＣＡ（４－４－５）：メールに添付されたファイル操作によるダウンロード
・ＣＡ（６－４－ｎ）ｎ＝１～５：攻撃用ツールまたは別のマルウェアのダウンロード
・ＣＡ（４－４－４）：別サイトからのダウンロード
［機能カテゴリＣ：ネットワーク環境の調査（Ｎｅｔｗｏｒｋ　Ｅｎｖｉｒｏｎｍｅｎｔ　Ｃｈｅｃｋ）］
・ＣＡ（４－２－２）：マルウェアのアクティベート直後のネットワーク環境の探索
［機能カテゴリＤ：Ｃ＆Ｃサーバーの検索（Ｎｅｔｗｏｒｋ　Ｅｎｖｉｒｏｎｍｅｎｔ　Ｃｈｅｃｋ）］
・ＣＡ（６－６－１）：有効なＣ＆Ｃサーバーの探索
・ＣＡ（６－６－２）：有効なＣ＆Ｃサーバーの探索
［機能カテゴリＥ：Ｃ＆Ｃサーバー通信］
・ＣＡ（６－６－３～６）：Ｃ＆Ｃビーコン
・ＣＡ（６－６－１０）：Ｃ＆Ｃビーコン
・ＣＡ（６－６－１５）：Ｃ＆Ｃビーコン
［機能カテゴリＦ：リモートコントロール］
・ＣＡ（６－６－１２）：攻撃者によるリモートコントロール操作
・ＣＡ（６－６－１３）：攻撃者によるリモートコントロール操作
・ＣＡ（６－６－１４）：攻撃者によるリモートコントロール操作
［機能カテゴリＧ：Ｃ＆Ｃサーバーの切り換え］
・ＣＡ（６－６－９）：Ｃ＆Ｃサーバーの切り換え
［機能カテゴリＨ：感染拡大（Ｉｎｆｉｌｔｒａｔｉｏｎ／Ｓｐｒｅａｄ　ｏｆ　Ｉｎｆｅｃｔｉｏｎ）］
・ＣＡ（３－３－１）：感染拡大
・ＣＡ（６－３－ｎ）ｎ＝１，２，３：感染拡大
［機能カテゴリＩ：マルウェア侵入に起因したＣ＆Ｃ通信］
・ＣＡ（４－６－ｎ）ｎ＝１～４：マルウェア侵入後のＣ＆Ｃ通信の検出

なお、図９の説明でも述べた通り、遷移元のフェーズと遷移先のフェーズが同じであっても、フェーズ遷移に伴うその他の付帯的条件に基づいて異なる振る舞いと扱われる場合があり、相関条件ＣＡ（ｍ－ｎ－ｘ）の符号ｘは、それらの付帯的条件に付される符号である。

【０１０２】

新たな相関条件が検出されていない場合、検出されるまで、ステップＳ９０１の処理は繰り返し実行される。一方、新たな相関条件が検出され、端末の振る舞いの種類が決定された場合、処理はステップＳ９０３へ進む。

【０１０３】

ステップＳ９０３からステップＳ９０６では、カテゴリＡ（侵入ステージのマルウェア群）に属するマルウェア種別について、端末（ｈ）において活動しているマルウェアのマルウェア種別が決定される。分類部２５９は、不正な活動の分類と、当該不正な活動に関連する振る舞いの種類（相関条件）と、の対応関係を示す情報を参照することで、当該端末の不正な活動を分類する。

【０１０４】

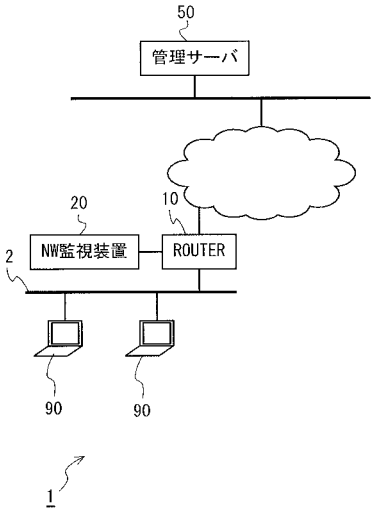
以下に、分類部２５９がカテゴリＡ（侵入ステージのマルウェア群）に属するマルウェア種別を決定するために用いられる、マルウェア種別と当該マルウェア種別に対応する相関条件（振る舞いの種類）との関係を例示する。
Ｄｏｗｎｌｏａｄｅｒ（Ｅｘｐｌｏｉｔ　Ｋｉｔ）：
条件：ＣＡ（１－４－ｎ）ｎ＝１～１１のいずれかを検出している。
Ｄｏｗｎｌｏａｄｅｒ（Ｍａｃｒｏ／Ｓｃｒｉｐｔ）：
条件：ＣＡ（４－４－５）を検出している。

一方、端末（ｈ）において活動しているマルウェアのマルウェア種別が、カテゴリＡ（侵入ステージのマルウェア群）に属するマルウェア種別でない場合、処理はステップＳ９

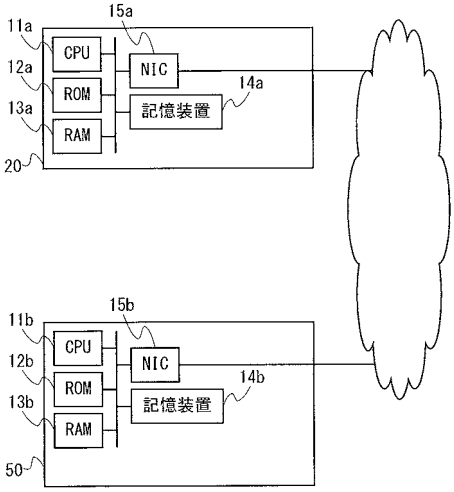
０７へ進む。
【０１０５】
ステップＳ９０７からステップＳ９１９では、カテゴリＢ（攻撃ステージのマルウェア群）に属するマルウェア種別について、端末（ｈ）において活動しているマルウェアのマルウェア種別が決定される。分類部２５９は、ステップＳ９０１からステップＳ９０２の処理が繰り返されることで蓄積された、端末（ｈ）について記録されている振る舞いの種類（相関条件）を読み出す（ステップＳ９０８）。そして、分類部２５９は、不正な活動の分類と、当該不正な活動に関連する１または複数の振る舞いの種類（相関条件）と、の対応関係を示す情報（ここでは、マップ）を参照することで、当該端末の不正な活動を分類する（ステップＳ９０９からステップＳ９１９）。
【０１０６】
以下に、分類部２５９がカテゴリＢ（攻撃ステージのマルウェア群）に属するマルウェア種別を決定するために用いられる、マルウェア種別と当該マルウェア種別に対応する１または複数の相関条件（振る舞いの種類）との関係を例示する。
Ｓｐｙｗａｒｅ：
条件：ＣＡ（６－７－ｎ）ｎ＝１，２、ＣＡ（７－６－１）、ＣＡ（８－６－ｎ）ｎ＝１，２のいずれかを検出しており、
　　ＣＡ（６－６－ｎ）ｎ＝１２，１３，１４のいずれも検出しておらず、かつ
　　ＣＡ（６－６－１５）を検出していない。
Ｇｅｎｅｒｉｃ　Ｔｒｏｊａｎ／Ｗｏｒｍ：
条件：カテゴリＢに属するその他のマルウェア種別であると決定するための条件の何れにも該当しない。
【０１０７】
なお、カテゴリＢに属するマルウェア種別には、上記で例示されたＳｐｙｗａｒｅ及びＧｅｎｅｒｉｃ　Ｔｒｏｊａｎ／Ｗｏｒｍの他に、Ｂａｃｋｄｏｏｒ／ＲＡＴ、Ｂｏｔ、Ｒａｎｓｏｍｗａｒｅ、Ａｄｗａｒｅ／Ｒｉｓｋｗａｒｅ等が挙げられる。これらのマルウェア種別についても、対応する振る舞い種別（相関条件）が設定されることで、分類を行うことが可能である。マルウェア種別の設定が完了すると、処理はステップＳ９０１へ戻る。
【０１０８】
即ち、本実施形態に係るマルウェア種別分類処理では、「マルウェアが送受信するトラフィックの相関条件」と、「マルウェアが有する機能が動作した際に発生する特徴的なトラフィックの振る舞い」をマッピングすることで、検出された相関条件の組み合わせ条件から、マルウェアの種別を推定することとしている。
【０１０９】
一般に、感染マルウェアの種別は、感染被害調査を通して、マルウェアが有する機能を調査して推定、決定されるものであるが、亜種や未知のマルウェアの種別の推定は、マルウェアの内部構造解析を必要とし、非常に時間がかかる。本実施形態に係るマルウェア種別分類処理によれば、マルウェアに感染した直後からの通信の振る舞いを追跡することで、亜種、未知マルウェアの内部構造解析を行うことなくマルウェアの種別を推定することが可能であり、マルウェア感染に対する感染マルウェアの種別に応じた、適切な対応、対策を取る上での有効な情報を与えることが可能となる。また、マルウェア種別が判明することで、使われたマルウェア種別から、攻撃手法や被害状況を推定することも可能である。
【０１１０】
また、図９から図１１に示された処理によって端末（ｈ）における不正な活動の分類が決定されると、ネットワーク監視装置２０は、決定された分類に対応する、予め設定された対応処理を実行する。例えば、ネットワーク監視装置２０は、通信遮断部２２による当該ノード９０の通信遮断開始や、当該ノード９０に感染したマルウェアの分類の通知等を行うことが可能である。

【０１１１】
＜バリエーション＞
上記実施形態では、ネットワーク監視装置２０が、スイッチまたはルータのモニタリングポート（ミラーポート）に接続されることでノード９０によって送受信されるパケットやフレーム等を取得し、取得したパケットを転送しないパッシブモードで動作する例について説明した（図１を参照）。但し、上記実施形態に示したネットワーク構成は、本開示を実施するための一例であり、実施にあたってはその他のネットワーク構成が採用されてもよい。
【０１１２】
例えば、ネットワーク監視装置２０は、モニタリングポート（ミラーポート）に接続されず、単にネットワークセグメント２に接続されている場合であっても、ネットワークセグメント２を流れるフレームを、自身のＭＡＣアドレス宛でないものも含めて全て取得することで、ノード９０によって送受信されるパケットやフレーム等を取得することが出来る。この場合も、ネットワーク監視装置２０は、パッシブモードで動作する。また、例えば、ネットワーク監視装置２０は、ネットワークセグメント２のスイッチまたはルータと、その上位にある他のスイッチまたはルータと、の間に接続されることで、通過するパケットやフレーム等を取得してもよい（図１２を参照）。この場合、ネットワーク監視装置２０は、取得したパケットのうち、遮断しなくてもよいパケットについては転送するインラインモードで動作する。また、ネットワーク監視装置２０は、ルータまたはスイッチに内包されてもよい。
【０１１３】
なお、本実施形態では、ネットワークを流れるパケットを取得して、上記した各種の検知エンジンによりリアルタイムで検知を行う実施形態について説明したが、本開示の適用範囲は、リアルタイム検知に限定されない。例えば、ネットワークを流れる通信に係るデータを蓄積しておいて、蓄積されたデータに対して上記した各種の検知エンジンによる処理を行うこととしてもよい。
【符号の説明】
【０１１４】
１　システム
２０　ネットワーク監視装置
５０　管理サーバー
９０　ノード

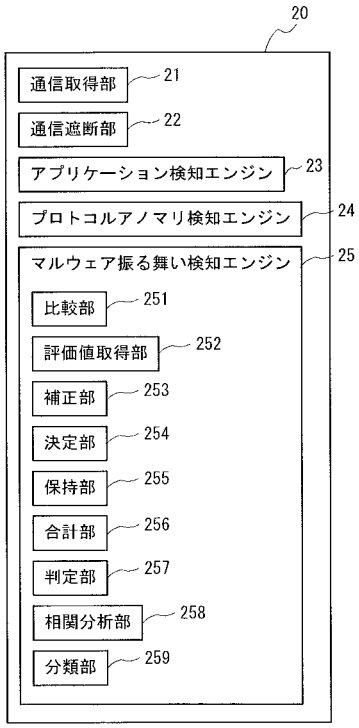
【図１】


50
管理サーバ
20
10
NW監視装置
ROUTER
2
90
90
1

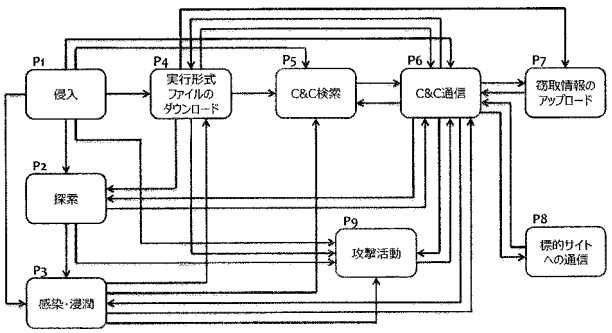
【図２】


15a
11a
CPU
12a
ROM
13a
RAM
NIC
14a
記憶装置
20
15b
11b
CPU
12b
ROM
13b
RAM
NIC
14b
記憶装置
50

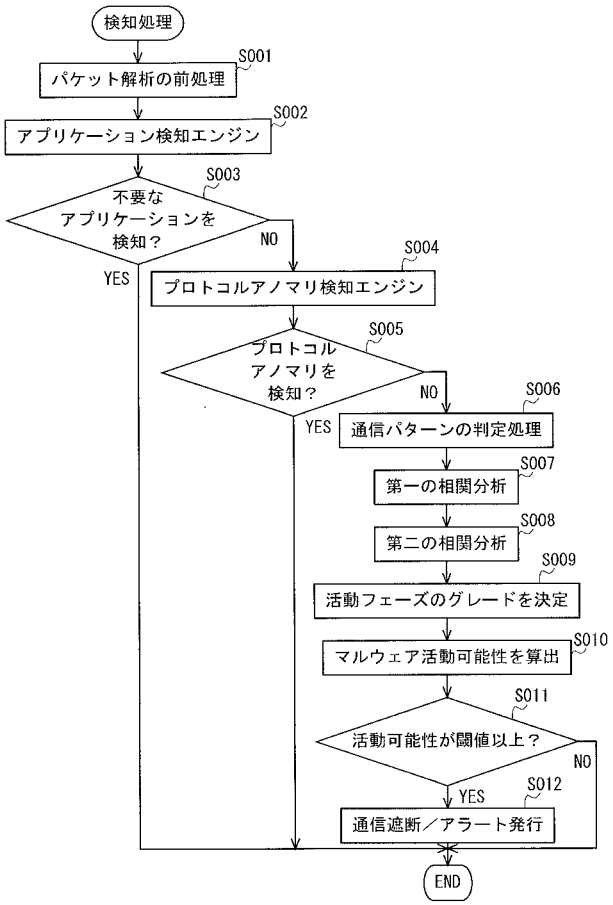
【図３】


20
通信取得部
21
通信遮断部
22
アプリケーション検知エンジン
23
プロトコルアノマリ検知エンジン
24
マルウェア振る舞い検知エンジン
25
比較部
251
評価値取得部
252
補正部
253
決定部
254
保持部
255
合計部
256
判定部
257
相関分析部
258
分類部
259

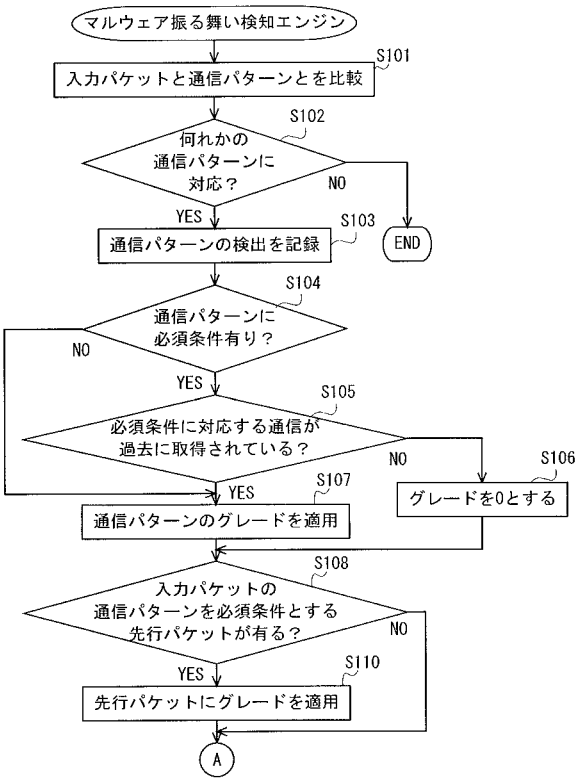
【図４】


P1
侵入
P4
実行形式
ファイルの
ダウンロード
P5
C&C検索
P6
C&C通信
P7
窃取情報の
アップロード
P2
探索
P9
攻撃活動
P8
標的サイト
への通信
P3
感染・浸潤

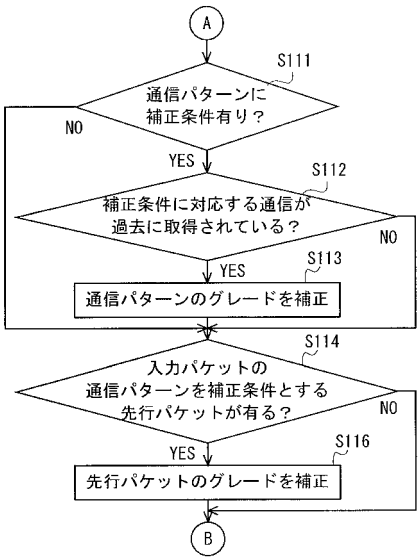
【図５】


検知処理
S001
パケット解析の前処理
S002
アプリケーション検知エンジン
S003
不要な
アプリケーションを
検知？
NO
YES
S004
プロトコルアノマリ検知エンジン
S005
プロトコル
アノマリを
検知？
NO
YES
S006
通信パターンの判定処理
S007
第一の相関分析
S008
第二の相関分析
S009
活動フェーズのグレードを決定
S010
マルウェア活動可能性を算出
S011
活動可能性が閾値以上？
NO
YES
S012
通信遮断／アラート発行
END

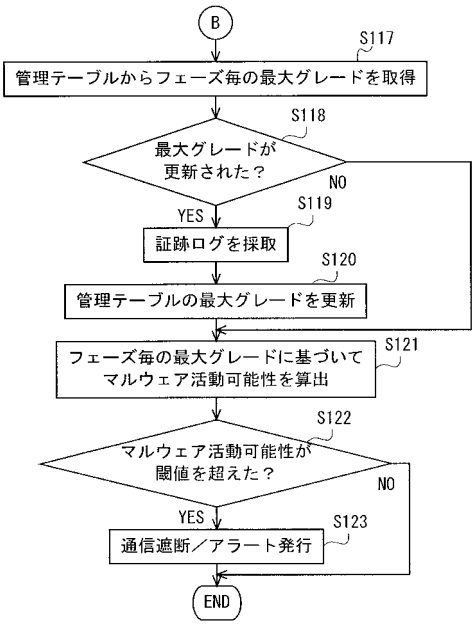
【図６】


マルウェア振る舞い検知エンジン
S101
入力パケットと通信パターンとを比較
S102
何れかの
通信パターンに
対応？
NO
YES
S103
通信パターンの検出を記録
END
S104
通信パターンに
必須条件有り？
NO
YES
S105
必須条件に対応する通信が
過去に取得されている？
NO
S106
グレードを0とする
YES
S107
通信パターンのグレードを適用
S108
入力パケットの
通信パターンを必須条件とする
先行パケットが有る？
NO
YES
S110
先行パケットにグレードを適用
A

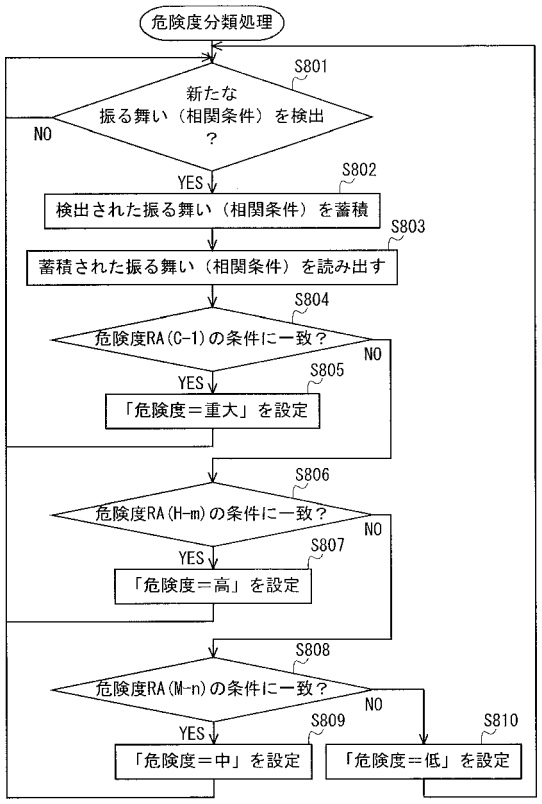
【図７】


A
S111
通信パターンに
補正条件有り？
NO
YES
S112
補正条件に対応する通信が
過去に取得されている？
NO
YES
S113
通信パターンのグレードを補正
S114
入力パケットの
通信パターンを補正条件とする
先行パケットが有る？
NO
YES
S116
先行パケットのグレードを補正
B

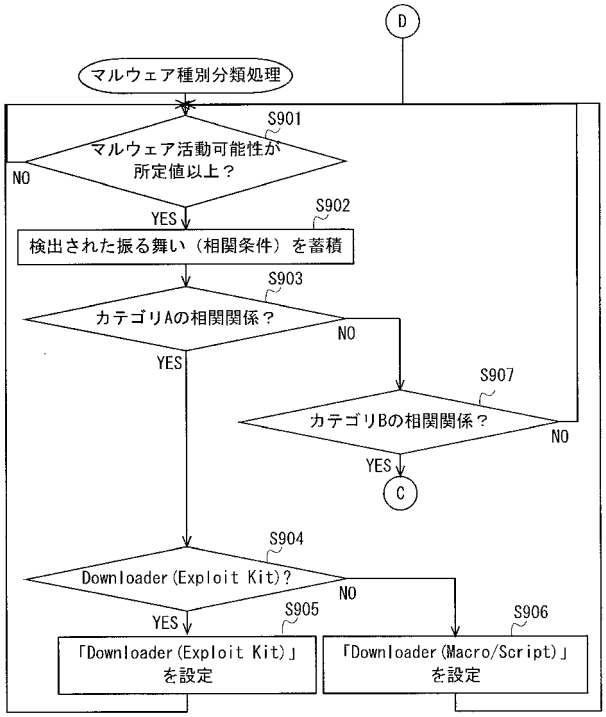
【図８】


B
S117
管理テーブルからフェーズ毎の最大グレードを取得
S118
最大グレードが
更新された？
NO
YES
S119
証跡ログを採取
S120
管理テーブルの最大グレードを更新
S121
フェーズ毎の最大グレードに基づいて
マルウェア活動可能性を算出
S122
マルウェア活動可能性が
閾値を超えた？
NO
YES
S123
通信遮断／アラート発行
END

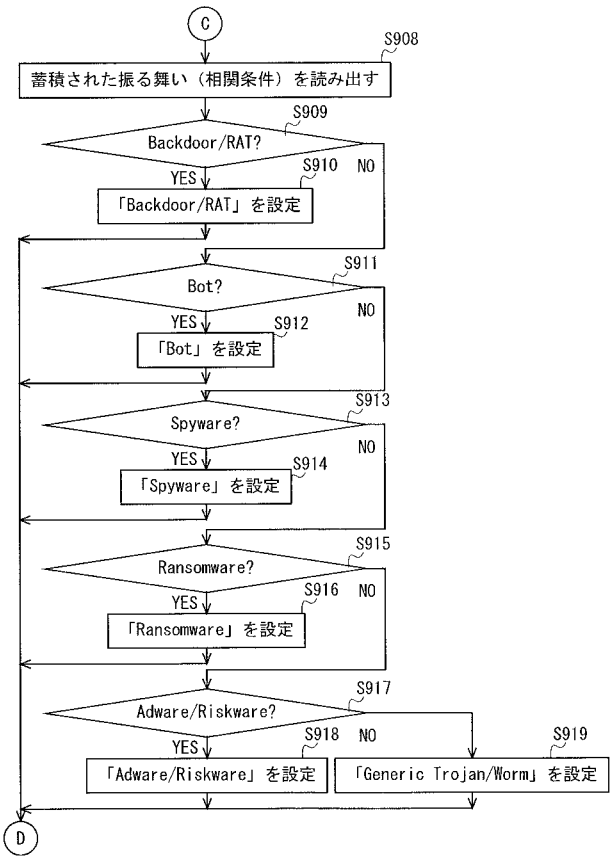
【図９】



【図１０】



【図１１】



【図１２】