(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6169497号
(P6169497)
(45)発行日　平成29年7月26日(2017.7.26)　(24)登録日　平成29年7月7日(2017.7.7)

(51)Int.Cl.　F I
G06F 21/56 (2013.01)　G06F 21/56 360
G06F 21/56 310

請求項の数 10　(全 14 頁)

(21)出願番号　特願2014-3518(P2014-3518)
(22)出願日　平成26年1月10日(2014.1.10)
(65)公開番号　特開2015-132942(P2015-132942A)
(43)公開日　平成27年7月23日(2015.7.23)
審査請求日　平成28年7月5日(2016.7.5)

(73)特許権者　399035766
エヌ・ティ・ティ・コミュニケーションズ株式会社
東京都千代田区内幸町一丁目１番６号
(74)代理人　100107766
弁理士　伊東　忠重
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　田中　恭之
東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内

最終頁に続く

(54)【発明の名称】接続先情報判定装置、接続先情報判定方法、及びプログラム

(57)【特許請求の範囲】
【請求項１】
ネットワーク上でマルウェアの配信元となる悪性の接続先を示す悪性接続先情報を判別する機能を備える接続先情報判定装置であって、
ネットワークを介して取得された被疑プログラムの識別情報と、当該被疑プログラムの取得元を示す接続先情報とを格納する接続先情報格納手段と、
前記接続先情報格納手段に格納された複数の接続先情報のうちの所定の接続先情報に対応する被疑プログラムについての解析を行う解析手段と、
前記解析手段により、解析の対象とした被疑プログラムがマルウェアであると判定された場合に、前記所定の接続先情報を悪性接続先情報であると判定するとともに、前記接続先情報格納手段に格納された複数の接続先情報のうち、前記マルウェアと判定された被疑プログラムの識別情報と同じ識別情報を持つ被疑プログラムに対応する接続先情報を悪性接続先情報であると判定する接続先情報判定手段と
を備えることを特徴とする接続先情報判定装置。
【請求項２】
前記接続先情報判定手段は、過去に悪性接続先情報ではないとされた接続先情報であっても、当該接続先情報が、前記マルウェアと判定された被疑プログラムの識別情報と同じ識別情報を持つ被疑プログラムに対応する接続先情報である場合に、当該接続先情報を悪性接続先情報であると判定する
ことを特徴とする請求項１に記載の接続先情報判定装置。

【請求項３】
所定の接続先情報に対応するサーバ装置へのアクセスを行うことにより被疑プログラムを取得するアクセス手段と、
前記アクセス手段により取得された被疑プログラムの識別情報と、当該被疑プログラムの取得元を示す接続先情報とを前記接続先情報格納手段に格納する接続先情報リスト作成手段と
を備えることを特徴とする請求項１又は２に記載の接続先情報判定装置。
【請求項４】
前記アクセス手段は、前記所定の接続先情報に対応するサーバ装置へのアクセスを行うことにより受ける攻撃を検知する機能を備えており、
前記アクセス手段により前記攻撃が検知された場合に、前記所定の接続先情報を悪性接続先情報であると判定する手段
を備えることを特徴とする請求項３に記載の接続先情報判定装置。
【請求項５】
前記所定の接続先情報に対応する被疑プログラムがマルウェアか否かを判定することにより、前記所定の接続先情報が悪性接続先情報であるか否かを判定するアンチウィルスソフトウェアの機能を有するマルウェア判定手段と、
前記アクセス手段と前記マルウェア判定手段のうちの少なくとも１つにより前記所定の接続先情報が悪性接続先情報であると判定された場合に、当該所定の接続先情報が悪性接続先情報であると判定する手段と
を備えることを特徴とする請求項４に記載の接続先情報判定装置。
【請求項６】
悪性接続先情報であると判定された接続先情報に対応するサーバ装置へのアクセスを行うことにより被疑ファイルを取得し、当該被疑ファイルの識別情報と、当該サーバ装置への過去のアクセスにより既に取得されている被疑ファイルの識別情報とが同一であるか否かを判定し、同一である場合に当該接続先情報は悪性接続先情報であると判定する接続先情報確認手段
を備えることを特徴とする請求項１ないし５のうちいずれか１項に記載の接続先情報判定装置。
【請求項７】
前記識別情報は、前記被疑プログラムのバイナリデータのハッシュ値であることを特徴とする請求項１ないし６のうちいずれか１項に記載の接続先情報判定装置。
【請求項８】
前記解析手段による解析は前記被疑プログラムを動作させてその挙動を解析する動的解析である
ことを特徴とする請求項１ないし７のうちいずれか１項に記載の接続先情報判定装置。
【請求項９】
ネットワーク上でマルウェアの配信元となる悪性の接続先を示す悪性接続先情報を判別する機能を備える接続先情報判定装置が実行する接続先情報判定方法であって、
前記接続先情報判定装置は、ネットワークを介して取得された被疑プログラムの識別情報と、当該被疑プログラムの取得元を示す接続先情報とを格納する接続先情報格納手段を備え、
前記接続先情報格納手段に格納された複数の接続先情報のうちの所定の接続先情報に対応する被疑プログラムについての解析を行う解析ステップと、
前記解析ステップにより、解析の対象とした被疑プログラムがマルウェアであると判定された場合に、前記所定の接続先情報を悪性接続先情報であると判定するとともに、前記接続先情報格納手段に格納された複数の接続先情報のうち、前記マルウェアと判定された被疑プログラムの識別情報と同じ識別情報を持つ被疑プログラムに対応する接続先情報を悪性接続先情報であると判定する接続先情報判定ステップと
を備えることを特徴とする接続先情報判定方法。

【請求項１０】
コンピュータを、請求項１ないし８のうちいずれか１項に記載の接続先情報判定装置における各手段として機能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、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であるマルウェアに関連する悪性ＵＲＬを取得する技術に関するものである。
【背景技術】
【０００２】
近年、様々なマルウェアが出現している。マルウェアは、特定のサーバ装置（ＵＲＬ）にアクセスすることでコンピュータにダウンロードされる場合が多い。あるＵＲＬにアクセスしてダウンロードされたプログラムがマルウェアであるかどうかを判断する手法として、プログラムコードを分析する静的解析を行う手法や、プログラムを実際に動作させて挙動を分析する動的解析を行う手法がある。このような解析を行って、マルウェアであると判断されたプログラムの取得元のＵＲＬは悪性ＵＲＬであると判断できる。
【０００３】
このような悪性ＵＲＬをブラックリストとして保持し、フィルタリング等に用いることでユーザを保護することができる。なお、ブラックリストの取得や維持管理に関する先行技術文献として特許文献１がある。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２０１２－１１８７１３号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
悪性ＵＲＬを取得するために、静的解析や動的解析を行う手法は解析コストが大きくなる上に、その方式上、解析により悪性であると判断されたマルウェアの取得元等しか悪性ＵＲＬとしての情報を取得できない。そのため、悪性ＵＲＬは日々増加しているにもかかわらず、既存技術では効率的に悪性ＵＲＬを取得することができないという問題がある。
【０００６】
本発明は上記の点に鑑みてなされたものであり、悪性ＵＲＬ等の悪性接続先情報を効率的に取得することを可能とした技術を提供することを目的とする。
【課題を解決するための手段】
【０００７】
本発明の実施の形態によれば、ネットワーク上でマルウェアの配信元となる悪性の接続先を示す悪性接続先情報を判別する機能を備える接続先情報判定装置であって、
ネットワークを介して取得された被疑プログラムの識別情報と、当該被疑プログラムの取得元を示す接続先情報とを格納する接続先情報格納手段と、
前記接続先情報格納手段に格納された複数の接続先情報のうちの所定の接続先情報に対応する被疑プログラムについての解析を行う解析手段と、
前記解析手段により、解析の対象とした被疑プログラムがマルウェアであると判定された場合に、前記所定の接続先情報を悪性接続先情報であると判定するとともに、前記接続先情報格納手段に格納された複数の接続先情報のうち、前記マルウェアと判定された被疑プログラムの識別情報と同じ識別情報を持つ被疑プログラムに対応する接続先情報を悪性接続先情報であると判定する接続先情報判定手段とを備えることを特徴とする接続先情報判定装置が提供される。
【０００８】
また、本実施の形態によれば、ネットワーク上でマルウェアの配信元となる悪性の接続

先を示す悪性接続先情報を判別する機能を備える接続先情報判定装置が実行する接続先情報判定方法であって、
前記接続先情報判定装置は、ネットワークを介して取得された被疑プログラムの識別情報と、当該被疑プログラムの取得元を示す接続先情報とを格納する接続先情報格納手段を備え、
前記接続先情報格納手段に格納された複数の接続先情報のうちの所定の接続先情報に対応する被疑プログラムについての解析を行う解析ステップと、
前記解析ステップにより、解析の対象とした被疑プログラムがマルウェアであると判定された場合に、前記所定の接続先情報を悪性接続先情報であると判定するとともに、前記接続先情報格納手段に格納された複数の接続先情報のうち、前記マルウェアと判定された被疑プログラムの識別情報と同じ識別情報を持つ被疑プログラムに対応する接続先情報を悪性接続先情報であると判定する接続先情報判定ステップとを備えることを特徴とする接続先情報判定方法が提供される。

【発明の効果】

【０００９】

本発明の実施の形態によれば、悪性ＵＲＬ等の悪性接続先情報を効率的に取得することを可能とした技術を提供することができる。

【図面の簡単な説明】

【００１０】

【図１】本発明の実施の形態に係るシステムの全体構成図である。
【図２】接続先情報管理装置１０の機能構成図である。
【図３】接続先情報管理装置１０の動作例を示すフローチャートである。
【図４】ＵＲＬリスト格納部１５に格納されるＵＲＬリストの例を示す図である。
【図５】接続先情報管理装置１０の動作例を示すフローチャートである。
【図６】動的解析結果を反映させた後のＵＲＬリストの例を示す図である。
【図７】ＵＲＬの確認方法を示すフローチャートである。

【発明を実施するための形態】

【００１１】

以下、図面を参照して本発明の実施の形態を説明する。なお、以下で説明する実施の形態は一例に過ぎず、本発明が適用される実施の形態は、以下の実施の形態に限られるわけではない。例えば、以下の実施の形態では、接続先情報管理装置１０が、ハニークライアントの機能とアンチウィルスソフトの機能を備え、それぞれで被疑ファイル取得元のＵＲＬが悪性ＵＲＬかどうかの判定を行うこととしているが、本発明においてこれらの機能は必須ではなく、これらのうちのいずれか又は両方を備えない構成をとることも可能である。

【００１２】

また、本実施の形態では、接続先を示す接続先情報としてＵＲＬを用いているが、接続先情報はＵＲＬに限られるわけではなく、その他のアドレスであってもよい。更に、本実施の形態では、悪性ＵＲＬの紐付け判定のために被疑ファイルの動的解析を行うこととしているが、解析手法は動的解析に限られるわけではない。

【００１３】

（システム構成）

図１に、本発明の実施の形態に係るシステムの構成図を示す。図１に示すように、本実施の形態に係るシステムは、複数のＷｅｂサーバ３０が存在するネットワーク２０に接続先情報管理装置１０が接続された構成を有している。

【００１４】

接続先情報管理装置１０は、所定のＵＲＬに対応するＷｅｂサーバ３０にアクセスし、当該ＵＲＬのＷｅｂサーバ３０から被疑ファイルをダウンロードし、当該被疑ファイルがマルウェアであるか否かを判定することで、ＵＲＬが悪性ＵＲＬか否かを判定する機能等を備える装置である。以下、接続先情報管理装置１０の機能構成をより詳細に説明する。

【００１５】
図２に、接続先情報管理装置１０の機能構成図を示す。図２に示すように、接続先情報管理装置１０は、アクセス部１１、被疑ファイル格納部１２、マルウェア判定部１３、ＵＲＬリスト作成部１４、ＵＲＬリスト格納部１５、動的解析部１６、ＵＲＬ判定部１７、ＵＲＬ確認制御部１８を備える。各機能部の機能概要は以下のとおりである。
【００１６】
アクセス部１１は、所定のＵＲＬにアクセスして、当該ＵＲＬのアクセス先（Ｗｅｂサーバ等）から被疑ファイルをダウンロードし、当該被疑ファイルを被疑ファイル格納部１２に格納する機能を含む。所定のＵＲＬとは、悪性ＵＲＬである可能性があると考えられるＵＲＬである。例えば、迷惑メール等に付されているＵＲＬを当該所定のＵＲＬとすることができる。
【００１７】
本実施の形態において、被疑ファイルは実行ファイル（ＥＸＥファイル）であり、被疑プログラムと称してもよい。当該被疑ファイルがマルウェアである場合、コンピュータにおいて当該被疑ファイルが実行されることで、例えば、不正に個人情報が外部に流出したり、更なるマルウェアがダウンロードされたり等の被害を受けることになる。
【００１８】
また、本実施の形態において、アクセス部１１はハニークライアントの機能を含む。ハニークライアントは、クライアント型ハニーポットの称してもよい。当該ハニークライアントは、上記のように所定のＵＲＬにアクセスして、当該ＵＲＬのアクセス先から被疑ファイルをダウンロードし、当該被疑ファイルを被疑ファイル格納部１２に格納する機能とともに、所定のＵＲＬにアクセスすることにより、Ｗｅｂブラウザ等の脆弱性を標的とした攻撃があった場合に、それを検知する機能を含む。本実施の形態では、アクセス部１１（ハニークライアント）により、当該攻撃が検知された場合、アクセス先のＵＲＬを悪性ＵＲＬであると判定する。
【００１９】
被疑ファイル格納部１２には、アクセス部１１により取得された被疑ファイルが、アクセス先のＵＲＬ及びアクセス日時（＝被疑ファイル取得日時）とともに格納される。
【００２０】
マルウェア判定部１３は、予め用意されたシグニチャと被疑ファイルとのパターンマッチング等により、被疑ファイルがマルウェアであるか否かを判定する機能を有する。本実施の形態において、マルウェア判定部１３は、複数種類のアンチウィルスソフトにより構成され、少なくとも１つのアンチウィルスソフトにより被疑ファイルがマルウェアであると判定された場合に、当該被疑ファイルをマルウェアであると判定する。
【００２１】
ＵＲＬリスト作成部１４は、アクセス部１１によるＵＲＬへのアクセスの結果やマルウェア判定結果等の情報をＵＲＬリスト格納部１５に格納することで、ＵＲＬリストを作成する。ＵＲＬリストの各レコードは、アクセス日時、当該アクセス日時にアクセスしたＵＲＬ、アクセスにより取得された被疑ファイルの識別情報、アクセス部１１（ハニークライアント）による判定結果、マルウェア判定部１３による被疑ファイルのマルウェア判定結果、及び総合判定結果を含む。
【００２２】
本実施の形態では、被疑ファイルの識別情報は、バイナリデータである被疑ファイルのハッシュ値であるがこれに限られるものではない。
【００２３】
アクセス部１１（ハニークライアント）による判定は、前述したように、攻撃が検知された場合、アクセス先のＵＲＬを悪性ＵＲＬ（「ブラック」とも呼び、以降、「Ｂ」と標記する場合がある）であると判定し、検知されない場合は正常（「ホワイト」とも呼び、以降、「Ｗ」と標記する場合がある）であると判定する。マルウェア判定部１３による被疑ファイルのマルウェア判定では、前述したように、少なくとも１つのアンチウィルスソ

フトによりマルウェアであると判定された場合に、アクセス先のＵＲＬを悪性ＵＲＬ（Ｂ）であると判定し、いずれのアンチウィルスソフトでもマルウェアであると判定されない場合に、アクセス先のＵＲＬを正常（Ｗ）であると判定する。

【００２４】

ＵＲＬリスト作成部１４は、アクセス部１１による判定結果とマルウェア判定部１３による判定結果のいずれか又は両方がＢである場合に総合判定結果をＢとし、アクセス部１１による判定結果とマルウェア判定部１３による判定結果の両方がＷである場合に総合判定結果をＷとする。なお、この判定処理はＵＲＬ判定部１７が行うこととしてもよい。

【００２５】

動的解析部１６は、ＵＲＬリスト格納部１５に格納されているＵＲＬリストにおける被疑ファイル（実行ファイル）を動作させ、その挙動を調べる動的解析を行うことで、当該被疑ファイルがマルウェアであるか否かを判定する。動的解析にはある程度の時間がかかるため、本実施の形態では、動的解析部１６による動的解析を、被疑ファイルを取得する時間間隔よりも長い周期のタイミングで行うこととしている。動的解析の対象とする被疑ファイルは、例えば、当該タイミングにおける最新の被疑ファイル（直近に取得された被疑ファイル）である。

【００２６】

ＵＲＬ判定部１７は、ＵＲＬリスト格納部１５に格納されたＵＲＬリストに対し、動的解析部１６によりマルウェアであると判定された被疑ファイルに対応するＵＲＬについて、総合判定結果がＷである場合に、それをＢであると判定し、ＷをＢに書き換えるとともに、動的解析部１６によりマルウェアであると判定された被疑ファイルのハッシュ値と同一のハッシュ値を持つ被疑ファイルに対応するＵＲＬについて、総合判定結果がＷである場合に、それをＢであると判定し、ＷをＢに書き換える。

【００２７】

動的解析部１６によりマルウェアであると判定された被疑ファイルと、ＵＲＬリスト格納部１５における他の被疑ファイルが同一かどうかを、被疑ファイル格納部１２に格納されている被疑ファイルを用いて、被疑ファイル（バイナリデータ）自体が同一であるかどうかを判定することで判定してもよい。

【００２８】

ＵＲＬ確認制御部１８は、例えば１日に1回等の所定のタイミングで、アクセス部１１に対し、ＵＲＬリスト格納部１５における総合判定結果がＢである各ＵＲＬにアクセスするよう指示し、アクセス部１１によるアクセス結果に基づき、当該ＵＲＬが確かにＢであるか否かを確認する。本実施の形態では、アクセス部１１により当該ＵＲＬにアクセスでき、かつ、被疑ファイルがダウンロードでき、かつ、当該被疑ファイルのハッシュ値が、既にダウンロードされた被疑ファイルのハッシュ値（ＵＲＬリストに既に存在するもの）と同一である場合に、当該ＵＲＬは確かにＢであると判定する。これ以外の場合でＵＲＬにアクセス可能である場合は、例えば、新たな被疑ファイルがダウンロードされたものとして、前述したように、アクセス部１１とマルウェア判定部１３による判定を行う。

【００２９】

なお、接続先情報管理装置１０における各機能部は、１つの装置（コンピュータ）に備える必要はない。例えば、ＵＲＬリスト格納部１５、動的解析部１６、及びＵＲＬ判定部１７を、その他の機能部とは別の装置に備えるといった構成が可能である。

【００３０】

本実施の形態に係る接続先情報管理装置１０は、１つ又は複数のコンピュータに、本実施の形態で説明する処理内容を記述したプログラムを実行させることにより実現可能である。すなわち、接続先情報管理装置１０が有する機能は、当該コンピュータに内蔵されるＣＰＵやメモリ、ハードディスクなどのハードウェア資源を用いて、接続先情報管理装置１０で実施される処理に対応するプログラムを実行することによって実現することが可能である。また、上記プログラムは、コンピュータが読み取り可能な記録媒体（可搬メモリ等）に記録して、保存したり、配布したりすることが可能である。また、上記プログラム

をインターネットや電子メールなど、ネットワークを通して提供することも可能である。
【００３１】
（接続先情報管理装置１０の動作例）
以下、上記の構成を備える接続先情報管理装置１０の動作例を、フローチャート等を参照して説明する。本例では、所定の周期でＵＲＬにアクセスして被疑ファイルを取得するとともに、当該所定の周期よりも長い周期で被疑ファイルの動的解析を行うこととしている。なお、ＵＲＬにアクセスした際に、被疑ファイルが取得されない場合もあるが、本例では、説明を分かり易くするために、ＵＲＬにアクセスする度に被疑ファイルが取得される例を説明している。また、各回においてアクセスするＵＲＬは予め準備され、アクセス部１１が保持しているものとする。
【００３２】
＜ＵＲＬへのアクセスを行う際の動作例＞
図３は、接続先情報管理装置１０においてＵＲＬへのアクセスを行う際の動作例を示すフローチャートである。
【００３３】
ステップ１０１において、アクセス部１１は、現在時刻がＵＲＬへのアクセスタイミングであるかどうかを判定し、アクセスタイミングであればステップ１０２に進む。
【００３４】
ステップ１０２において、アクセス部１１はＵＲＬにアクセスし、被疑ファイルを取得する。また、ステップ１０３において、アクセス部１１が、ハニークライアントの機能により、攻撃があったかどうかを判定することでアクセス先のＵＲＬがＢかどうかを判定し、更に、マルウェア判定部１３は、被疑ファイルがマルウェアであるかどうかを判定することでアクセス先のＵＲＬがＢかどうかを判定する。ＵＲＬリスト作成部１４は、アクセス部１１の判定結果とマルウェア判定部１３の判定結果のいずれか又は両方がＢである場合に、当該ＵＲＬについての総合判定結果をＢとする（ステップ１０３のＹｅｓ、ステップ１０４）。また、ＵＲＬリスト作成部１４は、アクセス部１１の判定結果とマルウェア判定部１３の判定結果の両方がＷである場合に、当該ＵＲＬについての総合判定結果をＷとする（ステップ１０３のＮｏ、ステップ１０５）。
【００３５】
ＵＲＬリスト作成部１４は、上記の判定結果に基づいてＵＲＬリストのレコードをＵＲＬリスト格納部１５に格納する（ステップ１０６）。その後、別のＵＲＬについて、ステップ１０１からの処理を繰り返す。
【００３６】
図４に、上記の処理により得られたＵＲＬリストの一例を示す。図４に示すとおり、ＵＲＬリストの各レコードは、アクセス日時、当該アクセス日時にアクセスしたＵＲＬ、アクセスにより取得された被疑ファイルのハッシュ値、アクセス部１１（ハニークライアント）による判定結果、マルウェア判定部１３による被疑ファイルのマルウェア判定結果、及び総合判定結果を含む。図４に示すとおり、アクセス部１１による判定結果、及びマルウェア判定部１３による判定結果のいずれかがＢであれば総合判定結果はＢになる。つまり、図４の例では、ＵＲＬ１とＵＲＬ３が悪性ＵＲＬである。
【００３７】
＜動的解析を行う際の動作例＞
図５は、接続先情報管理装置１０の動的解析部１６が被疑ファイルの動的解析を行う際の動作例を示すフローチャートである。
【００３８】
ステップ２０１において、動的解析部１６は、現在時刻が動的解析タイミングであるか否かを判定し、動的解析タイミングであればステップ２０２に進む。
【００３９】
ステップ２０２において、動的解析部１６は、ＵＲＬリスト格納部１５に格納されているＵＲＬリスト中から１つの被疑ファイルを選択し、当該被疑ファイルについての動的解

析を実行する。

【００４０】

動的解析を実行する対象の被疑ファイルとして、例えば、最も直近に取得された被疑ファイルを選択することができる。また、例えば、ＵＲＬリストの中で、動的解析も、後述する紐付けによる総合判定のいずれも行われていない被疑ファイルの中から最も数の多い被疑ファイル（つまり、同じハッシュ値を有する被疑ファイル群のうち、最も数の多いもの）を選択し、当該被疑ファイルの１つについて動的解析を行うこととしてもよい。

【００４１】

ステップ２０３において、ＵＲＬ判定部１７が、動的解析結果がＢ（マルウェア）であるかどうかを判定し、Ｂである場合はステップ２０４に進む。Ｂでない場合は、ステップ２０１からの処理を繰り返す。

【００４２】

ステップ２０４において、ＵＲＬ判定部１７は、ＵＲＬリスト格納部１５におけるＵＲＬリストに対して、動的解析部１６によりマルウェアであると判定された被疑ファイルに対応するＵＲＬの総合判定結果がＷであればそれをＢに書き換えるとともに、動的解析部１６によりマルウェアであると判定された被疑ファイルのハッシュ値と同一のハッシュ値を持つ被疑ファイルに対応するＵＲＬについても、総合判定結果がＷである場合に、それをＢであると判定し、ＷをＢに書き換える。すなわち、動的解析部１６によりマルウェアであると判定された被疑ファイルに直接に対応するＵＲＬのみでなく、ＵＲＬリストにおいて、当該被疑ファイルに紐付くＵＲＬも悪性ＵＲＬであると判定する。

【００４３】

図６に、動的解析結果を反映させた後のＵＲＬリストを示す。図６の例では、２０１３／１０／２　ＣＣ時ＣＣ分ＣＣ秒の時点で最新の被疑ファイル１について動的解析を行った結果、それがマルウェアであると判定されたたため、該当のＵＲＬ４の総合判定結果をＷからＢに書き換える。更に、被疑ファイル１のハッシュ値と同じハッシュ値である２０１３／１０／２　ＡＡ時ＡＡ分ＡＡ秒の被疑ファイル１に対応するＵＲＬ２についても総合判定結果をＷからＢに書き換えている。

【００４４】

ステップ２０４の後、ステップ２０１からの処理を繰り返す。なお、例えば、動的解析部１６での判定結果がＢであるＵＲＬ、及び当該ＵＲＬの被疑ファイルとハッシュ値が同じ被疑ファイルが取得されたＵＲＬ（つまり、紐付くＵＲＬ）についてはフラグを付け、フラグを付けたＵＲＬについて、以降の処理では、動的解析及び紐付け判定の対象としないこととしてもよい。また、フラグを付けたＵＲＬを後述するＵＲＬの確認の対象としてもよい。このようにしてフラグを付する場合、後述するＵＲＬの確認の処理により、フラグを付したＵＲＬがＢからＷになった場合には、フラグをはずすこととしてもよい。

【００４５】

例えば、上記の処理により得られたＵＲＬリストから、総合判定結果がＢであるＵＲＬを抽出し、当該ＵＲＬのリストを出力することで、ブラックリストを提供することができる。

【００４６】

上記の例では、アクセス部１１の判定結果とマルウェア判定部１３の判定結果に基づく総合判定結果を書き換えることとしているが、アクセス部１１の判定とマルウェア判定部１３の判定を行わないこととしてもよい。この場合、アクセス部１１は定期的にＵＲＬにアクセスして被疑ファイルを取得することで、図４、図６において、アクセス部１１の判定結果とマルウェア部１３の判定結果を含まないＵＲＬリストを作成する。そして、あるタイミングで１つの被疑ファイルについて動的解析を行って、それがＢであれば、当該被疑ファイルに対応するＵＲＬ、及び紐付くＵＲＬをＢとする。この手法によっても、悪性ＵＲＬを効率的に検出することができる。

【００４７】

＜ＵＲＬの確認時の動作例＞

図７に、接続先情報管理装置１０のＵＲＬ確認制御部１８によるＵＲＬ確認の動作のフローチャートを示す。この確認処理は、ＵＲＬリストの中で、被疑ファイルが取得され、かつ、総合判定がＢである各ＵＲＬについて、例えば１日に1回のように定期的に実行されるものである。

【００４８】

悪性ＵＲＬであっても、時間の経過によりＵＲＬとして機能しなくなったり、悪性でなくなったりする場合が生じる。本例のように、確認処理を行うことにより、一旦悪性であると判定したＵＲＬが確かに悪性であるか否かを的確に判断するので、ＵＲＬリストにおける悪性かどうかの情報の精度を高めることができ、結果として質の高いブラックリストを提供できる。

【００４９】

ステップ３０１において、ＵＲＬ確認制御部１８は、ＵＲＬリストにおいて確認の対象とする未処理のＵＲＬがあるかどうかを判定し、対象のＵＲＬがあればステップ３０２に進み、なければ今回のＵＲＬ確認処理を終了する。

【００５０】

ステップ３０２において、ＵＲＬ確認制御部１８は、アクセス部１１に対し、確認対象となるＵＲＬのうち１つのＵＲＬにアクセスするよう指示し、アクセス部１１は当該ＵＲＬへのアクセスを行う。ＵＲＬ確認制御部１８は、当該アクセスにより得られた被疑ファイルを取得し、その識別情報であるハッシュ値を求める。

【００５１】

ステップ３０３において、ＵＲＬ確認制御部１８は、ステップ３０２で得られた被疑ファイルのハッシュ値と、ＵＲＬリストの該当ＵＲＬに対応する被疑ファイルのハッシュ値とが同じか否かを判定する。これらが同じである場合はステップ３０４に進み、同じでない場合はステップ３０５に進む。

【００５２】

ステップ３０４において、ＵＲＬ確認制御部１８は、該当ＵＲＬは確かにＢであることを確認できたことになり、総合判定結果をＢのままとする。

【００５３】

ステップ３０５では、例えば、新たな被疑ファイルがダウンロードされたものとして、被疑ファイルのハッシュ値のＵＲＬリストへの記録を行うとともに、アクセス部１１とマルウェア判定部１３による判定を行う。すなわち、アクセス部１１の判定結果とマルウェア判定部１３の判定結果のいずれかがＢであれば総合判定結果をＢとし、それ以外であればＷとする。

【００５４】

ステップ３０４、３０５の後、ステップ３０１に戻る。確認対象のＵＲＬに対し同様の処理を繰り返す。

【００５５】

なお、ＵＲＬへのアクセスを試みた結果、ＵＲＬへのアクセスができない場合（ＵＲＬが生きていない場合）も発生し得るが、その場合には、当該ＵＲＬはＢではなくなるので、Ｗとする。もしくはＵＲＬが存在しない旨の情報を記録してもよい。

【００５６】

また、ＵＲＬから被疑ファイルがダウンロードされない場合も発生し得るが、その場合には、アクセス部１１（ハニークライアント）の判定結果を総合判定結果とする。

【００５７】

すなわち、本実施の形態では、アクセス部１１により当該ＵＲＬにアクセスでき、かつ、被疑ファイルがダウンロードでき、かつ、当該被疑ファイルのハッシュ値が、既にダウンロードされた被疑ファイルのハッシュ値と同一である場合に、当該ＵＲＬは確かにＢであると判定する。

【００５８】

なお、図５を参照して説明した動的解析結果に基づき、動的解析結果でＢとなったＵＲ

Ｌに紐付く各ＵＲＬ（同じハッシュ値の被疑ファイルが得られているＵＲＬ）について、図７を参照して説明した確認処理により、アクセス部１１により当該ＵＲＬにアクセスでき、かつ、被疑ファイルがダウンロードでき、かつ、当該被疑ファイルのハッシュ値が、既にダウンロードされた被疑ファイルのハッシュ値と同一であることが確認できた場合に、当該紐付くＵＲＬについての総合判定結果をＢとすることとしてもよい。

【００５９】

（実施の形態のまとめ、効果等）

以上、説明したように、本実施の形態では、ネットワーク上でマルウェアの配信元となる悪性の接続先を示す悪性接続先情報を判別する機能を備える接続先情報判定装置（例：接続先情報管理装置１０）であって、ネットワークを介して取得された被疑プログラムの識別情報と、当該被疑プログラムの取得元を示す接続先情報とを格納する接続先情報格納手段と、前記接続先情報格納手段に格納された複数の接続先情報のうちの所定の接続先情報に対応する被疑プログラムについての解析を行う解析手段と、前記解析手段により、解析の対象とした被疑プログラムがマルウェアであると判定された場合に、前記所定の接続先情報を悪性接続先情報であると判定するとともに、前記接続先情報格納手段に格納された複数の接続先情報のうち、前記マルウェアと判定された被疑プログラムの識別情報と同じ識別情報を持つ被疑プログラムに対応する接続先情報を悪性接続先情報であると判定する接続先情報判定手段とを備える接続先情報判定装置が提供される。

【００６０】

前記接続先情報判定手段は、過去に悪性接続先情報ではないとされた接続先情報であっても、当該接続先情報が、前記マルウェアと判定された被疑プログラムの識別情報と同じ識別情報を持つ被疑プログラムに対応する接続先情報である場合に、当該接続先情報を悪性接続先情報であると判定する。

【００６１】

前記接続先情報判定装置は、所定の接続先情報に対応するサーバ装置へのアクセスを行うことにより被疑プログラムを取得するアクセス手段と、前記アクセス手段により取得された被疑プログラムの識別情報と、当該被疑プログラムの取得元を示す接続先情報とを前記接続先情報格納手段に格納する接続先情報リスト作成手段とを備えることとしてもよい。

【００６２】

前記アクセス手段は、例えば、前記所定の接続先情報に対応するサーバ装置へのアクセスを行うことにより受ける攻撃を検知する機能を備えており、前記アクセス手段により前記攻撃が検知された場合に、前記所定の接続先情報を悪性接続先情報であると判定する。

【００６３】

また、前記接続先情報判定装置は、前記所定の接続先情報に対応する被疑プログラムがマルウェアか否かを判定することにより、前記所定の接続先情報が悪性接続先情報であるか否かを判定するアンチウィルスソフトウェアの機能を有するマルウェア判定手段と、前記アクセス手段と前記マルウェア判定手段のうちの少なくとも１つにより前記所定の接続先情報が悪性接続先情報であると判定された場合に、当該所定の接続先情報が悪性接続先情報であると判定する手段とを備えてもよい。

【００６４】

また、前記接続先情報判定装置は、悪性接続先情報であると判定された接続先情報に対応するサーバ装置へのアクセスを行うことにより被疑ファイルを取得し、当該被疑ファイルの識別情報と、当該サーバ装置への過去のアクセスにより既に取得されている被疑ファイルの識別情報とが同一であるか否かを判定し、同一である場合に当該接続先情報は悪性接続先情報であると判定する接続先情報確認手段を備えることとしてもよい。

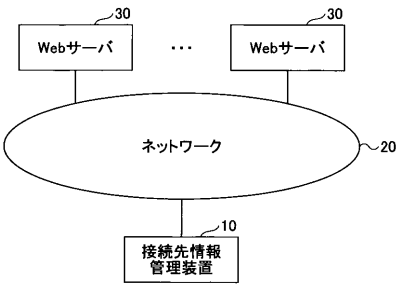
【００６５】

前記識別情報は、例えば、前記被疑プログラムのバイナリデータのハッシュ値である。また、前記解析手段による解析は、例えば、前記被疑プログラムを動作させてその挙動を解析する動的解析である。

【００６６】
本実施の形態によれば、被疑ファイルの動的解析によりマルウェアであると判定された被疑ファイルに紐付くＵＲＬを悪性ＵＲＬであると判定することで、過去にＷと判定されてブラックリストとして用いられなかったＵＲＬを復活させることができ、ブラックリストを拡大させることができる。
【００６７】
また、本実施の形態では、アンチウィルスソフトやハニークライアントによる判定よりも解析コストの高い動的解析を全ての被疑ファイルに対して行うのではなく、比較的低頻度で、所定の被疑ファイルのみに対して行うこととしているので、解析コストを大きく上昇させることなく、効率的にブラックリストを拡大させることができる。
【００６８】
また、本実施の形態では、ＵＲＬ確認制御部１８により、一旦悪性ＵＲＬと判定されたＵＲＬについて、確かに悪性であるかどうかを定期的に確認することとしているので、精度の高いブラックリストを提供することが可能である。
【００６９】
本発明は、上記の実施の形態に限定されることなく、特許請求の範囲内において、種々変更・応用が可能である。
【符号の説明】
【００７０】
１０　接続先情報管理装置
１１　アクセス部
１２　被疑ファイル格納部
１３　マルウェア判定部
１４　ＵＲＬリスト作成部
１５　ＵＲＬリスト格納部
１６　動的解析部
１７　ＵＲＬ判定部
１８　ＵＲＬ確認制御部
２０　ネットワーク
３０　Ｗｅｂサーバ

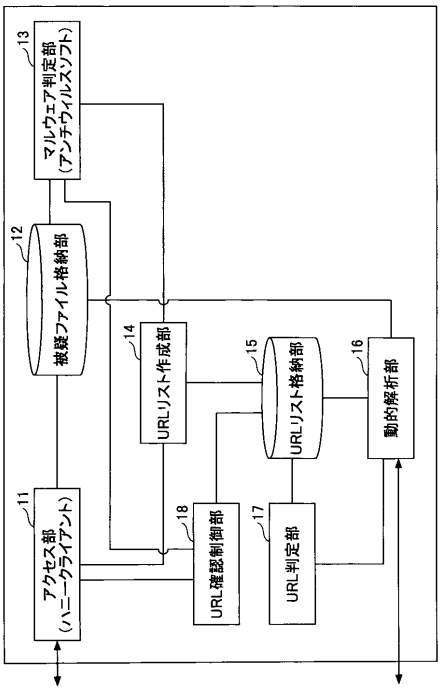
【図１】

本発明の実施の形態に係るシステムの全体構成図



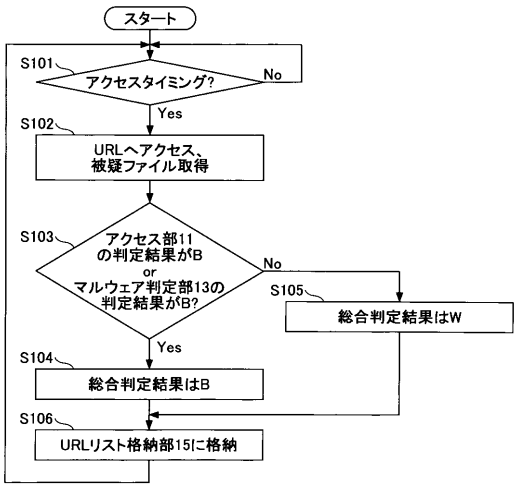
【図２】

接続先情報管理装置10の機能構成図



【図３】

接続先情報管理装置10の動作例を示すフローチャート



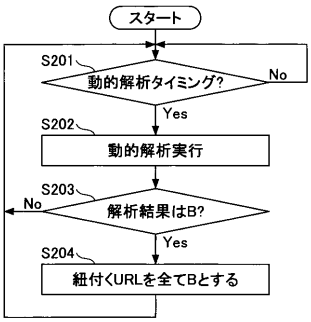
【図４】

URLリスト格納部15に格納されるURLリストの例を示す図

日時	URL	被疑ファイル	アクセス部11の判定結果	マルウェア判定部13の判定結果	総合判定結果
2013/10/1 XX時XX分XX秒	URL1	被疑ファイル1(ハッシュ値)	B	W	B
2013/10/2 AA時AA分AA秒	URL2	被疑ファイル1(ハッシュ値)	W	W	W
2013/10/2 BB時BB分BB秒	URL3	被疑ファイル2(ハッシュ値)	W	B	B
2013/10/2 CC時CC分CC秒	URL4	被疑ファイル1(ハッシュ値)	W	W	W
・・・	・・・	・・・	・・・	・・・	・・・

【図５】

接続先情報管理装置１０の動作例を示すフローチャート



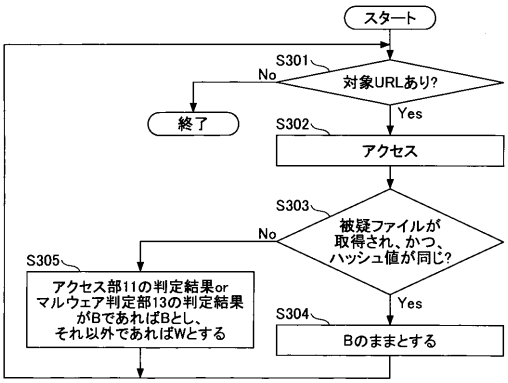
【図６】

動的解析結果を反映させた後のURLリスト

日時	URL	被疑ファイル	アクセス部11の判定結果	マルウェア判定部13の判定結果	総合判定結果
2013/10/1 XX時XX分XX秒	URL1	被疑ファイル1(ハッシュ値)	B	W	B
2013/10/2 AA時AA分AA秒	URL2	被疑ファイル1(ハッシュ値)	W	W	W→B
2013/10/2 BB時BB分BB秒	URL3	被疑ファイル2(ハッシュ値)	W	B	B
2013/10/2 CC時CC分CC秒	URL4	被疑ファイル1(ハッシュ値)	W	W	W→B
...	...	...	...	...	...

【図７】

URLの確認方法を示すフローチャート



フロントページの続き

(72)発明者　畑田　充弘
東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内
(72)発明者　有川　隼
東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内

審査官　青木　重徳

(56)参考文献　特開２０１２－０８３８４９（ＪＰ，Ａ）
米国特許出願公開第２０１１／０３１４５４６（ＵＳ，Ａ１）
八木　毅　ほか，Ｗｅｂサイト向けマルウェアダウンロードサイトの生存期間監視方式，電子情報通信学会技術研究報告，日本，社団法人電子情報通信学会，２０１０年　６月１０日，Ｖｏｌ．１１０，Ｎｏ．７９，ｐｐ．７５-８０
畑田　充弘　ほか，サンドボックス解析結果に基づくＵＲＬブラックリスト生成についての一検討，ＣＳＳ２０１３コンピュータセキュリティシンポジウム２０１３論文集，日本，一般社団法人情報処理学会，２０１３年１０月１４日，Ｖｏｌ．２０１３　Ｎｏ．４，ｐｐ.３８２-３８７

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／５６