(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5116577号
(P5116577)

(45)発行日　平成25年1月9日(2013.1.9)　(24)登録日　平成24年10月26日(2012.10.26)

(51)Int.Cl.		F I		
G06F 21/55	(2013.01)	G06F	21/00	155C
G06F 21/56	(2013.01)	G06F	21/00	156A
G06F 13/00	(2006.01)	G06F	13/00	351Z

請求項の数 5　(全 13 頁)

(21)出願番号　特願2008-165746 (P2008-165746)
(22)出願日　平成20年6月25日 (2008.6.25)
(65)公開番号　特開2010-9185 (P2010-9185A)
(43)公開日　平成22年1月14日 (2010.1.14)
審査請求日　平成23年1月31日 (2011.1.31)

（出願人による申告）平成１９年度、独立行政法人情報通信研究機構、「インターネットにおけるトレースバック技術に関する研究開発」委託研究、産業技術力強化法第１９条の適用を受ける特許出願

(73)特許権者　599108264
株式会社ＫＤＤＩ研究所
埼玉県ふじみ野市大原二丁目１番１５号
(74)代理人　100106909
弁理士　棚井　澄雄
(74)代理人　100064908
弁理士　志賀　正武
(74)代理人　100146835
弁理士　佐伯　義文
(74)代理人　100138759
弁理士　大房　直樹
(72)発明者　竹森　敬祐
埼玉県ふじみ野市大原２丁目１番１５号
株式会社ＫＤＤＩ研究所内

最終頁に続く

(54)【発明の名称】情報処理装置、情報処理システム、プログラム、および記録媒体

(57)【特許請求の範囲】
【請求項１】
既知の正常な通信の宛先の識別情報と、攻撃パケットの送信に利用されるポート番号とを記憶する既知情報記憶手段と、
監視対象となった通信の宛先の識別情報と、当該通信が利用したポート番号とを含む通信履歴を記憶する通信履歴記憶手段と、
前記通信履歴に含まれる識別情報が、前記既知情報記憶手段が記憶する識別情報と一致するか否かを判定する識別情報判定手段と、
前記通信履歴に含まれるポート番号が、前記既知情報記憶手段が記憶するポート番号と一致するか否かを判定するポート番号判定手段と、
前記通信履歴の中から、前記識別情報判定手段による判定の結果、前記既知情報記憶手段が記憶する識別情報と一致しないと判定された識別情報を含み、かつ前記ポート番号判定手段による判定の結果、前記既知情報記憶手段が記憶するポート番号と一致しないと判定されたポート番号を含む前記通信履歴を抽出する抽出手段と、
を備えたことを特徴とする情報処理装置。
【請求項２】
攻撃パケットを受信した装置の識別情報を含むメッセージを他の装置から受信する受信手段をさらに備え、
前記識別情報判定手段はさらに、前記通信履歴記憶手段が記憶する前記通信履歴に含まれる識別情報が、前記メッセージに含まれる識別情報と一致するか否かを判定し、

前記抽出手段は、前記識別情報判定手段による判定の結果、前記メッセージに含まれる識別情報と一致する識別情報が前記通信履歴に含まれる場合に前記通信履歴の抽出を行う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】

請求項１または請求項２に記載の情報処理装置としてコンピュータを機能させるためのプログラム。

【請求項４】

請求項３に記載のプログラムを格納したコンピュータ読み取り可能な記録媒体。

【請求項５】

第１の情報処理装置および第２の情報処理装置を備えた情報処理システムであって、

前記第１の情報処理装置は、

既知の正常な通信の宛先の識別情報と、攻撃パケットの送信に利用されるポート番号とを記憶する既知情報記憶手段と、

監視対象となった通信の宛先の識別情報と、当該通信が利用したポート番号とを含む通信履歴を記憶する通信履歴記憶手段と、

前記通信履歴に含まれる識別情報が、前記既知情報記憶手段が記憶する識別情報と一致するか否かを判定する識別情報判定手段と、

前記通信履歴に含まれるポート番号が、前記既知情報記憶手段が記憶するポート番号と一致するか否かを判定するポート番号判定手段と、

前記通信履歴の中から、前記識別情報判定手段による判定の結果、前記既知情報記憶手段が記憶する識別情報と一致しないと判定された識別情報を含み、かつ前記ポート番号判定手段による判定の結果、前記既知情報記憶手段が記憶するポート番号と一致しないと判定されたポート番号を含む前記通信履歴を抽出する第１の抽出手段と、

前記第１の抽出手段が抽出した前記通信履歴を前記第２の情報処理装置へ送信する送信手段とを備え、

前記第２の情報処理装置は、

複数の前記第１の情報処理装置から前記通信履歴を受信する受信手段と、

前記受信手段が受信した前記通信履歴の中から、共通の識別情報を有する前記通信履歴を抽出する第２の抽出手段とを備えた

ことを特徴とする情報処理システム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、通信に係る情報を処理する情報処理装置および情報処理システムに関する。また、本発明は、情報処理装置としてコンピュータを機能させるためのプログラム、およびそのプログラムを記録した記録媒体にも関する。

【背景技術】

【０００２】

近年、ウィルスに感染したコンピュータに悪質な動作を実行させる、ボットと呼ばれるウィルスによる被害が拡大している。ボットは、外部の指令サーバに通信セッションを確立して新たなコードをダウンロードする機能や、攻撃のための指令を受ける機能、指令に従って攻撃する機能などを持つ悪意のコードで構成されている。ボットに感染して加害者として攻撃を行うことになった加害者装置や上記の指令サーバを撲滅することは重要であり、被害者装置から通信経路を辿って攻撃元を追跡するIPトレースバック技術が注目されている。

【０００３】

IPトレースバックとは、送信元のIPアドレスを詐称して行う攻撃を、パケット中のIPレイヤの情報を用いて追跡する手法である。IPトレースバックの代表的な方式として、通過するパケットのハッシュ値を通信経路上の専用の装置で保存しておき、被害者側に届いた攻撃パケットのハッシュ値を、装置に残された情報から追跡するハッシュ方式がある（非

特許文献１，２参照）。

【０００４】

この他、ルータを通過するパケットをサンプリングして、パケット情報とルータ情報をICMPパケットに載せて、Destination IP（被害者のIPアドレス）へ送付するICMP方式がある（非特許文献３参照）。また、通過するパケットをサンプリングして、ルーティングに影響のないヘッダ領域にルータ情報を書き込むパケットマーキング方式もあり、被害者側でマーキング情報を組み立てることで、通信経路を追跡することができる（非特許文献４参照）。

【非特許文献１】Strayer, W. T. Jones, C. E. Tchakountio, F. Snoeren, A. C. Schwartz, B. Clements, R. C. Condell, M. Partridge, “Traceback of single IP packets using SPIE, ” DARPA Information Survivability Conference and Exposition, Proceedings, Vol. 2, pp. 266-270, April 2003.

【非特許文献２】A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, S. T. Kent, and W. T. Strayer “Hash-Based IP Traceback,” Proceeding or SIGCOMM ’01, August 2001.

【非特許文献３】Steven Bellovin, and Marcus Leech, Tom Taylor, “ICMP Traceback Messages,” IETF, Internet Draft, draft-ietf-itrace-04.txt, Aug. 2003.

【非特許文献４】D. Song and A Perrig, “Advanced and Authenticated Marking Schemes for IP Traceback,” Proc. of IEEE Inforcom, April, 2001.

【発明の開示】

【発明が解決しようとする課題】

【０００５】

図５は、ボットによる通信のモデルを示している。ボットによる通信には、攻撃を行う加害者PC（Personal Computer）５００，５０１と、攻撃を受ける被害者PC５１０，５１１，５１２，５１３と、攻撃コード（実行ファイル）の配信や攻撃指示を行う指令サーバ５２０，５２１とが関係している。外部の加害者PC５００は、ボットをダウンロードする初期コードを加害者PC５０１に埋め込む。加害者PC５０１は、この初期コードに従って指令サーバ５２０から新たなコードを受信する。さらに、加害者PC５０１は、指令サーバ５２１から指令を受け取り、被害者PCに対して各種攻撃を行う。

【０００６】

本発明者らは、通信プロセスと通信の宛先をモニタするツールを実装し、加害者PCの通信挙動をモニタした。図６はこの様子を示している。加害者PCは初期のコード“^21.tmp.exe”を起動すると、新たにコード“nbin.exe”を取得した（時刻14:06:51）。この53秒後、加害者PCはコード“nbin.exe”により外部サーバとの通信を開始してコード“EventLogger.exe”を取得した（時刻14:07:44）。また、90秒後には加害者PCはコード“EventLogger.exe”により新たな通信を開始した（時刻14:08:21）。上記の３種類のコードによる通信が指令サーバとの通信である。

【０００７】

上記のようにボットに感染した加害者PCが指令サーバと行う通信と、加害者PCが被害者PCと行う攻撃のための通信は別個の通信であり、通信に使用するパケットも異なる。このため、従来のIPトレースバック方式では、被害者PCに到着したパケットの情報に基づいて被害者PCから加害者PCまでの通信を追跡することはできるが、被害者PCに到着したパケットとは異なるパケットを用いている指令サーバまでの通信を追跡することはできなかった。

【０００８】

本発明は、上述した課題に鑑みてなされたものであって、ボットに感染した装置が指令サーバと行う通信を検出することができる情報処理装置、情報処理システム、プログラム、および記録媒体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】

【０００９】

本発明は、上記の課題を解決するためになされたもので、既知の正常な通信の宛先の識別情報と、攻撃パケットの送信に利用されるポート番号とを記憶する既知情報記憶手段と、監視対象となった通信の宛先の識別情報と、当該通信が利用したポート番号とを含む通信履歴を記憶する通信履歴記憶手段と、前記通信履歴に含まれる識別情報が、前記既知情報記憶手段が記憶する識別情報と一致するか否かを判定する識別情報判定手段と、前記通信履歴に含まれるポート番号が、前記既知情報記憶手段が記憶するポート番号と一致するか否かを判定するポート番号判定手段と、前記通信履歴の中から、前記識別情報判定手段による判定の結果、前記既知情報記憶手段が記憶する識別情報と一致しないと判定された識別情報を含み、かつ前記ポート番号判定手段による判定の結果、前記既知情報記憶手段が記憶するポート番号と一致しないと判定されたポート番号を含む前記通信履歴を抽出する抽出手段とを備えたことを特徴とする情報処理装置である。

【００１０】

既知の正常な通信とは、ボットに感染していないことが保証されている装置が行う通信である。通信履歴に含まれる識別情報が、既知の正常な通信の宛先の識別情報と一致した場合、当該識別情報を宛先とする通信は正常な通信であると判定することができる。これに対して、通信履歴に含まれる識別情報が、既知の正常な通信の宛先の識別情報と一致しなかった場合、当該識別情報を宛先とする通信は指令サーバとの通信である可能性がある。

【００１１】

しかし、当該通信の中には、被害者の装置を宛先とし、攻撃パケットの送信に利用した通信が含まれている可能性がある。そこで、攻撃パケットの送信に利用されることが既知であるポート番号を用いた判定を行うことにより、被害者の装置を宛先とする通信を除外することが可能となる。すなわち、通信履歴に含まれるポート番号が、攻撃パケットの送信に利用されるポート番号と一致した場合、当該ポート番号を利用した通信は、攻撃パケットの送信に利用した通信であると判定することができる。また、通信履歴に含まれるポート番号が、攻撃パケットの送信に利用されるポート番号と一致しなかった場合、当該ポート番号を利用した通信は指令サーバとの通信である可能性がある。

【００１２】

したがって、通信の宛先の識別情報に関する判定と、通信に利用したポート番号に関する判定とを組み合わせることによって、既知の正常な通信と、攻撃パケットの送信に利用した通信とを除外し、指令サーバとの通信を検出することができる。

【００１３】

また、本発明の情報処理装置は、攻撃パケットを受信した装置の識別情報を含むメッセージを他の装置から受信する受信手段をさらに備え、前記識別情報判定手段はさらに、前記通信履歴記憶手段が記憶する前記通信履歴に含まれる識別情報が、前記メッセージに含まれる識別情報と一致するか否かを判定し、前記抽出手段は、前記識別情報判定手段による判定の結果、前記メッセージに含まれる識別情報と一致する識別情報が前記通信履歴に含まれる場合に前記通信履歴の抽出を行うことを特徴とする。

【００１４】

本発明では、指令サーバから指令を受けて被害者の装置へ攻撃パケットを送信した加害者の装置の通信履歴を処理対象とすることが特に効果的である。加害者の装置の通信履歴には、被害者の装置へ攻撃パケットを送信した通信に係る通信履歴が含まれている。したがって、攻撃パケットを受信した装置の識別情報と一致する識別情報が通信履歴に含まれる場合に通信履歴の抽出を行うことによって、指令サーバとの通信の検出精度を向上することができる。

【００１５】

また、本発明は、上記の情報処理装置としてコンピュータを機能させるためのプログラムである。

【００１６】

また、本発明は、上記のプログラムを格納したコンピュータ読み取り可能な記録媒体で

ある。

【００１７】

また、本発明は、第１の情報処理装置および第２の情報処理装置を備えた情報処理システムであって、前記第１の情報処理装置は、既知の正常な通信の宛先の識別情報と、攻撃パケットの送信に利用されるポート番号とを記憶する既知情報記憶手段と、監視対象となった通信の宛先の識別情報と、当該通信が利用したポート番号とを含む通信履歴を記憶する通信履歴記憶手段と、前記通信履歴に含まれる識別情報が、前記既知情報記憶手段が記憶する識別情報と一致するか否かを判定する識別情報判定手段と、前記通信履歴に含まれるポート番号が、前記既知情報記憶手段が記憶するポート番号と一致するか否かを判定するポート番号判定手段と、前記通信履歴の中から、前記識別情報判定手段による判定の結果、前記既知情報記憶手段が記憶する識別情報と一致しないと判定された識別情報を含み、かつ前記ポート番号判定手段による判定の結果、前記既知情報記憶手段が記憶するポート番号と一致しないと判定されたポート番号を含む前記通信履歴を抽出する第１の抽出手段と、前記第１の抽出手段が抽出した前記通信履歴を前記第２の情報処理装置へ送信する送信手段とを備え、前記第２の情報処理装置は、複数の前記第１の情報処理装置から前記通信履歴を受信する受信手段と、前記受信手段が受信した前記通信履歴の中から、共通の識別情報を有する前記通信履歴を抽出する第２の抽出手段とを備えたことを特徴とする情報処理システムである。

【００１８】

ボットでは、加害者として機能する複数の装置が同一の指令サーバと通信を行う特徴がある。この特徴を利用して、複数の第１の通信装置で抽出した通信履歴の中から共通の識別情報を有する通信履歴を抽出することによって、指令サーバとの通信の検出精度を向上することができる。

【発明の効果】

【００１９】

本発明によれば、ボットに感染した装置が指令サーバと行う通信を検出することができるという効果が得られる。

【発明を実施するための最良の形態】

【００２０】

以下、図面を参照し、本発明の実施形態を説明する。図１は、本発明の一実施形態による情報処理システムの構成を示している。本情報処理システムは、ボットによる被害者または加害者となる端末装置１（例えばPC）と、端末装置１から受信する通信履歴に基づいて通信の解析を行うサーバ２とを備えている。本情報処理システムでは複数台の端末装置１が存在しているが、図１では１台のみを図示し、他の端末装置１の図示を省略している。

【００２１】

以下、端末装置１が備える構成およびその動作を説明する。端末装置１は、既知情報記憶部１００、通信監視部１０１、通信履歴記憶部１０２、被害報告部１０３、被害情報受信部１０４、被害情報記憶部１０５、加害者判定部１０６、通信解析部１０７、および通信履歴報告部１０８を備えている。端末装置１は被害者にも加害者にもなり得ることから、端末装置１は、被害者としての処理構成（被害報告部１０３）と、加害者としての処理構成（既知情報記憶部１００、通信解析部１０７、通信履歴報告部１０８）との両方を備えている。既知情報記憶部１００、通信履歴記憶部１０２、および被害情報記憶部１０５は、異なる記録媒体で構成されていてもよいし、同一の記録媒体上の異なる記憶領域で構成されていてもよい。

【００２２】

既知情報記憶部１００は、予め得られている既知情報を記憶する。サーバ２などの他の装置から既知情報を受信することによって端末装置１が既知情報を取得してもよいし、既知情報が格納された記録媒体から既知情報を読み出すことによって端末装置１が既知情報を取得してもよい。既知情報の詳細については後述する。

【００２３】
通信監視部１０１は、端末装置１が他の装置と行う通信を監視し、通信結果を通信履歴として通信履歴記憶部１０２に格納する。通信監視部１０１の機能は、例えばMicrosoft（登録商標）社から提供されているPort Reporterというツールにより実現することが可能である。あるいは、Windows（登録商標） XP標準のIPHLPAPI.DLLで、TCPについてはAllocateAndGetTcpExTableFromStack()、UDPについてはUDP:AllocateAndGetUdpExTableFromStack()というAPIを100msec程度の周期で呼び出すことによっても、通信監視部１０１の機能を実現することが可能である。

【００２４】
通信履歴記憶部１０２は通信履歴を記憶する。この通信履歴には、監視対象となった通信の宛先を識別する識別情報と、監視対象となった通信が利用したポート番号と、監視対象となった通信を行った時刻（通信時刻）とが含まれる。識別情報は、IPアドレスまたはドメイン名、もしくはその両方であり、ドメイン名はFQDN（Fully Qualified Domain Name）であってもよい。以下に登場する他の識別情報についても同様である。識別情報を構成するIPアドレスとドメイン名とを関連付けるには、通信時にDNSサーバに名前解決を依頼した後、DNSサーバから返信されるパケットにIPアドレスとドメイン名の両者が含まれていることを利用すればよい。また、監視対象となった通信を実行したときに起動した通信プロセスの名称（通信プロセス名）が通信履歴に含まれていてもよい。

【００２５】
被害報告部１０３は、端末装置１がボットによる攻撃パケットを受信し被害者となった場合に、攻撃パケットの受信に係る通信履歴を含むメッセージをサーバ２へ送信することによって、サーバ２に被害を報告する。サーバ２へ送信する通信履歴には、端末装置１の識別情報と攻撃パケットの受信時刻（攻撃時刻とする）が含まれる。この通信履歴を含むメッセージの送信は、例えば攻撃を受けたことを認識したユーザが端末装置１に入力した指示に基づいて行われる。

【００２６】
ボットによる攻撃に関する通信履歴を各端末装置１から受信したサーバ２は、各端末装置１の通信履歴を統合した被害情報を生成し、被害情報を含むメッセージを端末装置１へ送信する。この被害情報には、攻撃パケットを受信した端末装置１の識別情報と攻撃時刻（あるいは攻撃時刻を含む時間範囲でもよい）が含まれている。被害情報受信部１０４は、被害情報を含むサーバ２からのメッセージを受信し、メッセージに含まれる被害情報を被害情報記憶部１０５に格納する。被害情報記憶部１０５は被害情報を記憶する。

【００２７】
加害者判定部１０６は、端末装置１が加害者であるか否かを判定する。この判定には、被害情報記憶部１０５が記憶する被害情報に含まれる識別情報および攻撃時刻と、通信履歴記憶部１０２が記憶する通信履歴に含まれる識別情報および通信時刻とが用いられる。具体的には、加害者判定部１０６は、まず被害情報記憶部１０５から被害情報を読み出すと共に、通信履歴記憶部１０２から通信履歴を読み出す。続いて、加害者判定部１０６は、被害情報に含まれる攻撃時刻と、通信履歴に含まれる通信時刻とを比較し、攻撃時刻を基準とする前後の所定時間以内の通信時刻を含む通信履歴を以降の処理対象とする。

【００２８】
続いて、加害者判定部１０６は、被害情報に含まれる識別情報（攻撃パケットを受信した端末装置１の識別情報）と、通信履歴に含まれる識別情報（通信の宛先の装置の識別情報）とが一致するか否かを判定する。被害情報に含まれる識別情報が、通信履歴に含まれるいずれかの識別情報と一致した場合、自身の端末装置１が加害者であると判断することが可能である。また、被害情報に含まれる識別情報が、通信履歴に含まれるどの識別情報とも一致しなかった場合、自身の端末装置１が加害者ではないと判断することが可能である。

【００２９】
続いて、加害者判定部１０６は判定結果を通信解析部１０７に通知する。本実施形態で

は、端末装置１が加害者であると判断された場合に通信解析部１０７は以降の処理を行い、端末装置１が加害者ではないと判断された場合に通信解析部１０７は以降の処理を行わない。

【００３０】

通信解析部１０７は、既知情報記憶部１００が記憶する既知情報と、通信履歴記憶部１０２が記憶する通信履歴とに基づいて、端末装置１が行った通信を解析し、指令サーバとの通信に係る通信履歴を抽出する。通信解析部１０７のより具体的な動作については後述する。通信履歴報告部１０８は、通信解析部１０７が抽出した通信履歴を含むメッセージをサーバ２へ送信する。

【００３１】

次に、サーバ２が備える構成およびその動作を説明する。サーバ２は、被害情報受信部２００、被害情報記憶部２０１、被害情報配信部２０２、通信履歴受信部２０３、通信履歴記憶部２０４、および通信解析部２０５を備えている。被害情報記憶部２０１と通信履歴記憶部２０４は、異なる記録媒体で構成されていてもよいし、同一の記録媒体上の異なる記憶領域で構成されていてもよい。

【００３２】

被害情報受信部２００は、各端末装置１から送信された、被害情報を含むメッセージを受信し、メッセージに含まれる各被害情報を統合して被害情報記憶部２０１に格納する。被害情報記憶部２０１は被害情報を記憶する。被害情報配信部２０２は、被害情報記憶部２０１から被害情報を読み出し、被害情報を含むメッセージを端末装置１へ送信することによって、被害情報を各端末装置１に配信する。

【００３３】

通信履歴受信部２０３は、端末装置１から送信された、通信履歴を含むメッセージを受信し、メッセージに含まれる通信履歴を通信履歴記憶部２０４に格納する。通信履歴記憶部２０４は通信履歴を記憶する。通信解析部２０５は、通信履歴記憶部２０４が記憶する通信履歴に基づいて、各端末装置１が行った通信を解析する。通信解析部２０５のより具体的な動作については後述する。

【００３４】

次に、端末装置１が備える通信解析部１０７のより具体的な構成および動作を説明する。図２は通信解析部１０７の構成を示している。通信解析部１０７は、識別情報判定部１０７ａ、ポート番号判定部１０７ｂ、および通信履歴抽出部１０７ｃを備えている。通信解析部１０７による通信の解析には、既知情報記憶部１００に格納されている既知情報と、通信履歴記憶部１０２に格納されている通信履歴とが用いられる。

【００３５】

既知情報記憶部１００は、通信解析部１０７が参照する既知情報として、ホワイトリストおよびポート番号リストを記憶する。ホワイトリストは、ボットに感染していないことが保証されている装置の通信結果から得られた、既知の正常な通信の宛先を識別する識別情報をリスト化したものである。また、ポート番号リストは、攻撃パケットの送信に利用されるポート番号をリスト化したものである。ポート番号リストには、攻撃に頻繁に利用されるTCP-Port 25, TCP-Port 135-139, UDP-Port 53が含まれる。

【００３６】

識別情報判定部１０７ａは、通信履歴記憶部１０２から通信履歴を読み出すと共に、既知情報記憶部１００からホワイトリストを読み出す。続いて、識別情報判定部１０７ａは、通信履歴に含まれる識別情報がホワイトリスト内の識別情報と一致するか否かを判定する。通信履歴に含まれる識別情報がホワイトリスト内のいずれかの識別情報と一致した場合、この識別情報を宛先とする通信は正常な通信であると判定することができる。これに対して、通信履歴に含まれる識別情報がホワイトリスト内のどの識別情報とも一致しなかった場合、この識別情報を宛先とする通信は指令サーバとの通信である可能性がある。したがって、識別情報判定部１０７ａによる判定の結果から、指令サーバとの通信に係る通信履歴の候補を特定することが可能である。

【００３７】
識別情報判定部１０７ａは、ホワイトリスト内のどの識別情報とも一致しなかった識別情報を判定結果として通信履歴抽出部１０７ｃに通知する。この識別情報を含む通信履歴は、指令サーバとの通信に係る通信履歴の候補であるが、ボットは指令サーバとの通信以外に被害者への攻撃も行うため、上記の通信履歴の候補から、被害者への攻撃に係る通信履歴を除外する必要がある。ポート番号判定部１０７ｂは、このための判定を行う。
【００３８】
ポート番号判定部１０７ｂは、既知情報記憶部１００からポート番号リストを読み出すと共に、通信履歴記憶部１０２から通信履歴を読み出す。続いて、ポート番号判定部１０７ｂは、通信履歴に含まれるポート番号がポート番号リスト内のポート番号と一致するか否かを判定する。通信履歴に含まれるポート番号がポート番号リスト内のいずれかのポート番号と一致した場合、このポート番号を利用した通信は、攻撃パケットの送信に利用した通信であると判定することができる。また、通信履歴に含まれるポート番号がポート番号リスト内のどのポート番号とも一致しなかった場合、このポート番号を利用した通信は指令サーバとの通信である可能性がある。したがって、ポート番号判定部１０７ｂによる判定の結果から、被害者を宛先とする通信を除外し、指令サーバとの通信に係る通信履歴の候補を特定することが可能である。ポート番号判定部１０７ｂは、ポート番号リスト内のどのポート番号とも一致しなかったポート番号を判定結果として通信履歴抽出部１０７ｃに通知する。
【００３９】
通信履歴抽出部１０７ｃは、通信履歴記憶部１０２から通信履歴を読み出し、識別情報判定部１０７ａによる判定の結果と、ポート番号判定部１０７ｂによる判定の結果とに基づいて、指令サーバとの通信に係る通信履歴を抽出する。具体的には、通信履歴抽出部１０７ｃは、識別情報判定部１０７ａによる判定の結果、ホワイトリスト内のどの識別情報とも一致しないと判定された識別情報を含み、かつポート番号判定部１０７ｂによる判定の結果、ポート番号リスト内のどのポート番号とも一致しないと判定されたポート番号を含む通信履歴を抽出する。上記のようにして抽出された通信履歴が、指令サーバとの通信に係る通信履歴として特定されたものである。また、抽出された通信履歴に含まれる識別情報が指令サーバの識別情報となる。上記の通信履歴の抽出の際に、被害情報に含まれる攻撃時刻を基準とした前後の所定時間以内の通信時刻を含む通信履歴を処理対象としてもよい。
【００４０】
次に、既知情報記憶部１００が記憶するホワイトリストの作成方法を説明する。図３は、ホワイトリストの作成に係る端末装置の構成を示している。この端末装置は、ボットなどのウィルスに感染していないことが保証されているものとする。通信監視部３００は、端末装置が他の装置と行う通信を長期間（例えば１週間程度）監視し、通信の宛先を識別する識別情報をホワイトリストとしてホワイトリスト記憶部３０１に格納する。
【００４１】
ホワイトリスト記憶部３０１はホワイトリストを記憶する。ホワイトリスト記憶部３０１に格納されるホワイトリストは、各種通信の宛先の識別情報をリスト化したものである。この各種通信として、アプリケーションや各種ファイルの更新に係る通信や、LANおよびDNSのアドレスの通知に係る通信、Ajaxと呼ばれるWebアプリケーションがWebブラウザの起動などのユーザ操作と並行してWebサーバと行う通信などがある。
【００４２】
次に、サーバ２が備える通信解析部２０５のより具体的な動作を説明する。サーバ２の通信履歴記憶部２０４には、指令サーバとの通信に係る通信履歴として各端末装置１で抽出された通信履歴が格納されている。各通信履歴は、端末装置１毎に区別できるようになっている。通信解析部２０５は、通信履歴記憶部２０４から複数の端末装置１についての通信履歴を読み出し、それらに共通する識別情報があるか否かを判定する。
【００４３】

より具体的には、通信解析部２０５はまず、１つの端末装置１についての通信履歴から、互いに異なる１または複数の識別情報を抽出し、各識別情報と出現頻度のペアを記憶装置に格納する。ここで、「互いに異なる」と記載したのは、１つの端末装置１についての通信履歴が複数のレコードからなり、同一の識別情報が複数レコードに記録されている場合に、同一の識別情報を１回だけ抽出する（その結果、抽出された識別情報は全て異なる）ことを明示するためである。最初の端末装置１についての通信履歴を処理したときには各識別情報の出現頻度は１にセットされる。

【００４４】

続いて、通信解析部２０５は、他の１つの端末装置１についての通信履歴から、互いに異なる１または複数の識別情報を抽出し、記憶装置に格納されている各識別情報と比較する。通信履歴から抽出した識別情報が、記憶装置に格納されているいずれかの識別情報と一致した場合、その識別情報の出現頻度に１が加算される。また、通信履歴から抽出した識別情報が、記憶装置に格納されているどの識別情報とも一致しなかった場合、新たな識別情報と出現頻度（値は１）のペアが記憶装置に格納される。通信解析部２０５は、全ての端末装置１についての通信履歴を処理するまで上記の処理を繰り返す。上記の処理が終了したら、通信解析部２０５は記憶装置から出現頻度を読み出し、その出現頻度が所定値Ｎ（Ｎは２以上）以上である場合に、その出現頻度とペアになっている識別情報を記憶装置から読み出す。この識別情報は、指令サーバの識別情報として信頼度が高いものとなる。

【００４５】

ボットでは、加害者として機能する複数の端末装置１が同一の指令サーバと通信を行う特徴がある。したがって、複数の端末装置１で抽出した通信履歴の中から、共通の識別情報を有する通信履歴を抽出することによって、指令サーバとの通信に係る通信履歴の抽出精度を高めることができる。

【００４６】

図４は、共通の識別情報を有する通信履歴が抽出される様子を示している。加害者となった端末装置１ａ，１ｂ，１ｃ，１ｄから通信履歴がサーバ２に報告される。４つの端末装置の通信履歴のうち、端末装置１ｂ，１ｃからの通信履歴が、共通する識別情報を有している。この識別情報は、指令サーバの識別情報として、より信頼度が高いものとなる。通信プロセス名（図４の「nbin.exe」）も取得されている場合には、共通する通信プロセス名を有する通信履歴を抽出することによって、指令サーバとの通信に係る通信履歴の抽出精度をより高めることができる。

【００４７】

上述したように、本実施形態によれば、通信の宛先の識別情報に関する判定と、通信に利用したポート番号に関する判定とを組み合わせることによって、既知の正常な通信と、攻撃パケットの送信に利用した通信とを除外し、指令サーバとの通信を検出することができる。

【００４８】

また、加害者判定部１０６による判定の結果、端末装置１が加害者であると判断された場合に通信履歴の抽出を行うことによって、指令サーバとの通信の検出精度を向上することができる。さらに、加害者であると判断された端末装置１が、指令サーバ２との通信に係る通信履歴のみをサーバ２に報告することによって、端末装置１の正常な通信履歴の漏洩を防止することができる。

【００４９】

また、複数の端末装置１で抽出した通信履歴の中から、共通の識別情報を有する通信履歴を抽出することによって、指令サーバとの通信の検出精度を向上することができる。

【００５０】

以上、図面を参照して本発明の実施形態について詳述してきたが、具体的な構成は上記の実施形態に限られるものではなく、本発明の要旨を逸脱しない範囲の設計変更等も含まれる。例えば、上述した実施形態による端末装置１の動作および機能を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録された

プログラムをコンピュータに読み込ませ、実行させてもよい。

【００５１】

ここで、「コンピュータ」は、WWWシステムを利用している場合であれば、ホームページ提供環境（あるいは表示環境）も含むものとする。また、「コンピュータ読み取り可能な記録媒体」とは、フレキシブルディスク、光磁気ディスク、ＲＯＭ、ＣＤ－ＲＯＭ等の可搬媒体、コンピュータに内蔵されるハードディスク等の記憶装置のことをいう。さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムが送信された場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリ（ＲＡＭ）のように、一定時間プログラムを保持しているものも含むものとする。

【００５２】

また、上述したプログラムは、このプログラムを記憶装置等に格納したコンピュータから、伝送媒体を介して、あるいは伝送媒体中の伝送波により他のコンピュータに伝送されてもよい。ここで、プログラムを伝送する「伝送媒体」は、インターネット等のネットワーク（通信網）や電話回線等の通信回線（通信線）のように、情報を伝送する機能を有する媒体のことをいう。また、上述したプログラムは、前述した機能の一部を実現するためのものであってもよい。さらに、前述した機能を、コンピュータに既に記録されているプログラムとの組合せで実現できるもの、いわゆる差分ファイル（差分プログラム）であってもよい。

【図面の簡単な説明】

【００５３】

【図１】本発明の一実施形態による情報処理システムの構成を示すブロック図である。

【図２】本発明の一実施形態による端末装置が備える通信解析部の構成を示すブロック図である。

【図３】本発明の一実施形態におけるホワイトリストの作成方法を説明するためのブロック図である。

【図４】本発明の一実施形態によるサーバが備える通信解析部の動作を説明するための参考図である。

【図５】ボットによる通信のモデルを示す参考図である。

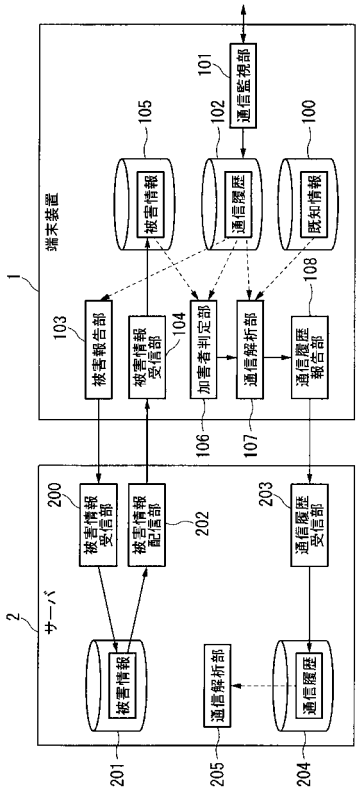
【図６】ボットによる通信をモニタした結果を示す参考図である。

【符号の説明】

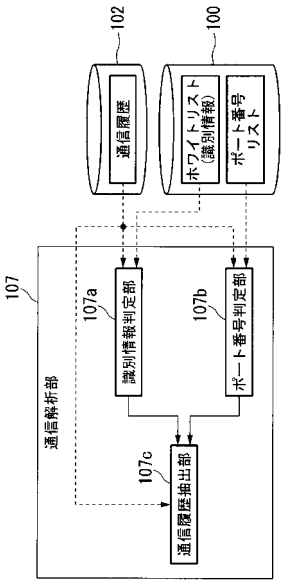
【００５４】

１・・・端末装置（第１の情報処理装置）、２・・・サーバ（第２の情報処理装置）、１００・・・既知情報記憶部（既知情報記憶手段）、１０１・・・通信監視部、１０２，２０４・・・通信履歴記憶部（通信履歴記憶手段）、１０３・・・被害報告部（送信手段）、１０４，２００・・・被害情報受信部（受信手段）、１０５，２０１・・・被害情報記憶部、１０６・・・加害者判定部、１０７，２０５・・・通信解析部（第１の抽出手段、第２の抽出手段）、１０７ａ・・・識別情報判定部（識別情報判定手段）、１０７ｂ・・・ポート番号判定部（ポート番号判定手段）、１０７ｃ・・・通信履歴抽出部（抽出手段）、１０８・・・通信履歴報告部、２０２・・・被害情報配信部、２０３・・・通信履歴受信部（受信手段）

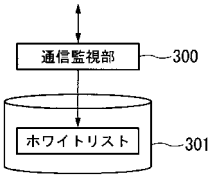
【図１】


端末装置
1
101
通信監視部
105
被害情報
102
通信履歴
100
既知情報
103
被害報告部
104
被害情報受信部
106
加害者判定部
107
通信解析部
108
通信履歴報告部
サーバ
2
200
被害情報受信部
202
被害情報配信部
203
通信履歴受信部
201
被害情報
205
通信解析部
204
通信履歴

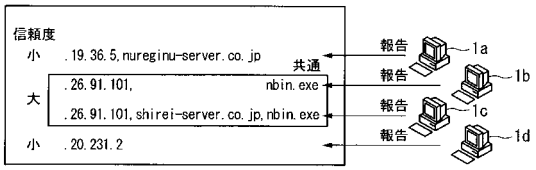
【図２】


102
通信履歴
100
ホワイトリスト
(識別情報)
ポート番号
リスト
107
通信解析部
107a
識別情報判定部
107b
ポート番号判定部
107c
通信履歴抽出部

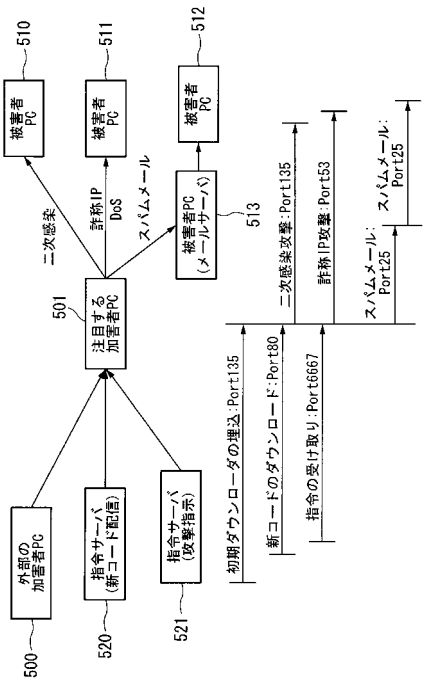
【図３】


通信監視部
300
ホワイトリスト
301

【図４】


信頼度
小 .19.36.5,nureginu-server.co.jp
共通
大 .26.91.101, nbin.exe
.26.91.101,shirei-server.co.jp,nbin.exe
小 .20.231.2
報告
1a
1b
1c
1d

【図５】


510
被害者PC
511
被害者PC
512
被害者PC
二次感染
詐称IP DoS
スパムメール
513
被害者PC(メールサーバ)
501
注目する加害者PC
二次感染攻撃:Port135
詐称IP攻撃:Port53
スパムメール:Port25
スパムメール:Port25
初期ダウンロードの埋込:Port135
新コードのダウンロード:Port80
指令の受け取り:Port6667
500
外部の加害者PC
520
指令サーバ(新コード配信)
521
指令サーバ(攻撃指示)

【図６】

ReportTime	Protocol	Local Port	Local IP	Remote Port	Remote IP	PID	Module
2008/03/10 14:06:51	TCP	1259	.168.236.36	smtp(25)	.54.244.136	4048	~21.tmp.exe
2008/03/10 14:06:58	TCP	1263	.168.236.36	http(80)	.215.15.145	4048	~21.tmp.exe
2008/03/10 14:06:59	TCP	1265	.168.236.36	http(80)	.79.36.123	4048	~21.tmp.exe
2008/03/10 14:07:31	TCP	1268	127.0.0.1	http(80)	127.0.0.1	3904	nbin.exe
2008/03/10 14:07:44	TCP	1269	.168.236.36	http(80)	.15.231.4	3904	nbin.exe
2008/03/10 14:07:50	TCP	1270	127.0.0.1	http(80)	127.0.0.1	3904	nbin.exe
2008/03/10 14:08:09	TCP	1271	127.0.0.1	http(80)	127.0.0.1	1436	EventLogger.exe
2008/03/10 14:08:21	TCP	1272	.168.236.36	http(80)	.15.231.4	1436	EventLogger.exe

フロントページの続き

(72)発明者　藤長　昌彦
埼玉県ふじみ野市大原２丁目１番１５号　株式会社ＫＤＤＩ研究所内

審査官　平井　誠

(56)参考文献　特開２００６－３５０５６１（ＪＰ，Ａ）
特開２００７－１２４４８２（ＪＰ，Ａ）
特開２００７－３２３４２８（ＪＰ，Ａ）
竹森　敬祐，セキュリティインシデントをトリガとしたボット検知方式：宛先ＩＰとドメインに注目した不正検知，コンピュータセキュリティシンポジウム２００７，日本，社団法人情報処理学会，２００７年１０月３１日，第2007巻　第１０号，ｐ．２５３－２５８

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／００
Ｇ０６Ｆ　１３／００