(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2010-161488
(P2010-161488A)
(43)公開日　平成22年7月22日(2010.7.22)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/56	(2006.01)	H04L	12/56	400Z	5B089
G06F 13/00	(2006.01)	G06F	13/00	351Z	5B285
G06F 21/20	(2006.01)	G06F	15/00	330A	5K030

審査請求 未請求　請求項の数 10　ＯＬ　（全 17 頁）

(21)出願番号　特願2009-1051(P2009-1051)
(22)出願日　平成21年1月6日(2009.1.6)

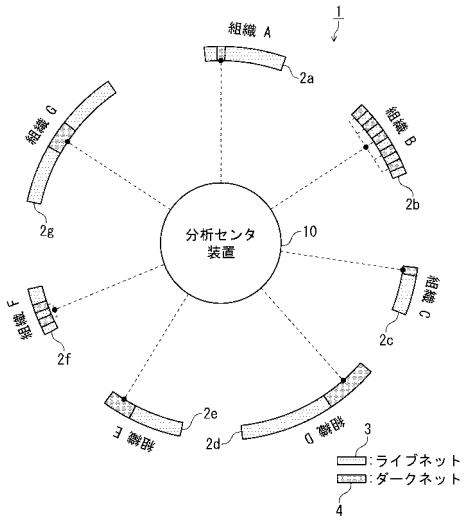
特許法第３０条第１項適用申請有り　研究集会名：情報通信システムセキュリティ研究会　主催者名：社団法人　電子情報通信学会　情報・システムソサエティ　：情報通信システムセキュリティ時限研究専門委員会　開催日　：平成２０年９月１０日　刊行物名：情報通信システムセキュリティ研究会　予稿集　発行日　：平成２０年９月３日

(71)出願人　301022471
独立行政法人情報通信研究機構
東京都小金井市貫井北町４－２－１
(74)代理人　100130111
弁理士　新保　斉
(72)発明者　井上　大介
東京都小金井市貫井北町４－２－１　独立行政法人情報通信研究機構内
(72)発明者　衛藤　将史
東京都小金井市貫井北町４－２－１　独立行政法人情報通信研究機構内
(72)発明者　中尾　康二
東京都小金井市貫井北町４－２－１　独立行政法人情報通信研究機構内

最終頁に続く

(54)【発明の名称】ネットワーク監視システム及びその方法

(57)【要約】
【課題】　ダークネット観測を広範囲に行い、その観測結果を用いて、サーバやホストが存在する組織の実ネットワークの保護の充実を図る技術を提供すること。
【解決手段】　ネットワーク上で用いられるアドレスであって到達可能かつ未使用のアドレス空間をなすダークネットを監視するネットワーク監視方法を提供する。監視対象とする各通信ネットワークの使用済みのアドレス情報を収集して格納した分析センタ装置１０を用い、異なる組織に管理される通信ネットワーク２ａ～２ｇ内に設置されたセンサ手段が、自ネットワーク内のダークネット宛の信号を検出する。そして、各センサ手段から少なくとも信号の存在と検出した信号の送信元アドレスとを含む検出結果を受理して、その送信元アドレスが、監視対象の各通信ネットワークにおける使用済みのアドレス情報であるかどうかを分析する。分析の結果、少なくとも該信号が使用済みのアドレスから発信されている場合にアラートを出力する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
ネットワーク上で用いられるアドレスであって到達可能かつ未使用のアドレス空間をなすダークネットを監視するネットワーク監視システムにおいて、
異なる組織に管理され、それぞれが所定のアドレス範囲をもつ通信ネットワークと、
該各通信ネットワーク内に設置され、自ネットワーク内のダークネット宛の信号を検出するセンサ手段と、
該各通信ネットワークのアドレス範囲の中で使用済みのアドレス情報を保持すると共に、該各センサ手段の検出結果を受信する分析センタ装置と
から構成され、
該分析センタ装置が、
監視対象とする各通信ネットワークにおける使用済みのアドレス情報を格納する使用済みアドレス情報記憶手段と、
該各センサ手段から少なくとも信号の存在と、検出した信号の送信元アドレスとを含む検出結果を受理する検出結果受理手段と、
検出結果を受理した際に、その信号の送信元アドレスが、監視対象の各通信ネットワークにおける使用済みのアドレス情報であるかどうかを分析する分析手段と、
分析の結果、少なくとも該信号が使用済みのアドレスから発信されている場合にアラートを出力するアラート手段と
からなることを特徴とするネットワーク監視システム。
【請求項２】
前記ネットワーク監視システムにおいて、
前記分析センタ装置のアラート手段が、
前記センサ手段が検出した信号の送信元アドレスをアドレス範囲に含む通信ネットワークの管理者に対して、送信元アドレスの情報を通知する
請求項１に記載のネットワーク監視システム。
【請求項３】
前記ネットワーク監視システムにおいて、
前記センサ手段が、検出した信号の宛先ポート番号を検出し、
前記分析センタ装置の分析手段が、所定の判定規則に従い、少なくとも該宛先ポート番号の情報から不正な通信であるか否かを判定すると共に、
該判定結果に従って、前記アラート手段がアラートを出力する
請求項1又は２に記載のネットワーク監視システム。
【請求項４】
前記センサ手段が、
送信元アドレスからの信号に対し何ら応答を行わないセンサである
請求項１ないし３のいずれかに記載のネットワーク監視システム。
【請求項５】
前記センサ手段が、
送信元アドレスからの既知の信号に対し所定の応答を行うセンサである
請求項１ないし３のいずれかに記載のネットワーク監視システム。
【請求項６】
ネットワーク上で用いられるアドレスであって到達可能かつ未使用のアドレス空間をなすダークネットを監視するネットワーク監視方法において、
監視対象とする各通信ネットワークの使用済みのアドレス情報を使用済みアドレス情報記憶手段に格納した分析センタ装置を用い、
異なる組織に管理され、それぞれが所定のアドレス範囲をもつ通信ネットワーク内に設置されたセンサ手段が、自ネットワーク内のダークネット宛の信号を検出する信号検出ステップ、
該分析センタ装置の検出結果受理手段が、該各センサ手段から少なくとも信号の存在と

、検出した信号の送信元アドレスとを含む検出結果を受理する検出結果受理ステップ、
該分析センタ装置の分析手段が、検出結果を受理した際に、その信号の送信元アドレスが、監視対象の各通信ネットワークにおける使用済みのアドレス情報であるかどうかを分析する分析ステップ、
該分析センタ装置のアラート手段が、分析の結果、少なくとも該信号が使用済みのアドレスから発信されている場合にアラートを出力するアラートステップ
を有することを特徴とするネットワーク監視方法。
【請求項７】
前記ネットワーク監視方法のアラートステップにおいて、
前記分析センタ装置のアラート手段が、
前記センサ手段が検出した信号の送信元アドレスをアドレス範囲に含む通信ネットワークの管理者に対して、送信元アドレスの情報を通知する
請求項６に記載のネットワーク監視方法。
【請求項８】
前記ネットワーク監視方法において、
前記センサステップにおいて、前記センサ手段が、検出した信号の宛先ポート番号を検出し、
前記分析ステップにおいて、前記分析手段が、所定の判定規則に従い、少なくとも該宛先ポート番号の情報から不正な通信であるか否かを判定し、
前記アラートステップにおいて、前記アラート手段が、該判定結果に従って、アラートを出力する
請求項６又は７に記載のネットワーク監視方法。
【請求項９】
前記ネットワーク監視方法の信号検出ステップにおいて、
前記センサ手段が、送信元アドレスからの信号に対し何ら応答を行わない
請求項６ないし８のいずれかに記載のネットワーク監視方法。
【請求項１０】
前記ネットワーク監視方法の信号検出ステップにおいて、
前記センサ手段が、送信元アドレスからの既知の信号に対し所定の応答を行う
請求項６ないし８のいずれかに記載のネットワーク監視方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明はネットワークの監視システムとその処理方法に関し、特に、ネットワーク上で到達可能かつ未使用のアドレス空間をなすダークネットを監視することで不正な信号を検出するシステム及び方法に関する。
【背景技術】
【０００２】
インターネットなどの通信ネットワークが社会の重要な基盤となるに伴い、ネットワーク上でのウイルス感染や、特定のホストコンピュータへの攻撃などが深刻な問題になっている。そのため、従来からネットワークを監視する様々な方法が提案されている。
【０００３】
そのうちの１つが、ダークネットを監視する方法である。ダークネットとは，インターネット上で到達可能かつ未使用のＩＰアドレス空間のことを指し、非特許文献１～３などに記載されている。未使用のＩＰアドレスに対しパケットが送信されることは、通常のインターネット利用の範囲においては起こる可能性が低いが、実際には相当数のパケットがダークネットに到着している。これらのパケットの多くは、リモート感染型のマルウェアが送信するスキャンやエクスプロイトコード、送信元ＩＰアドレスを詐称したＳＹＮフラッド攻撃に対する応答であるバックスキャッタ等、インターネット上での不正な活動に起因している。

【０００４】
そのため、ダークネットに到着するパケットを観測することで、インターネット上で発生している不正な活動の傾向把握が可能になる。ダークネット観測の最大の利点は、トラフィックを正・不正で区別する必要がなく、全てのパケットを不正なものと見なすことが出来る点にある。
【０００５】
出願人が研究開発を進めているインシデント分析センタnicter（Network ncident analysis Center for Tactical Emergency Response）では、日本国内に点在する複数のダークネット（合計１０万アドレス以上）にセンサを設置し、定常的な観測を行なっている。（非特許文献４～６参照）
【０００６】
このようなダークネットの定常的観測を通して、次に示す２つの課題が浮上してきている。
まず、実ネットワーク保護への直結ダークネット観測は、インターネット上の不正な活動の傾向把握に有用であるが、サーバやホストが存在する、組織の実ネットワークの保護に直結していない。
次に、センサの広域展開ダークネット観測の精度は、観測するアドレス数が多いほど向上する（非特許文献２参照）ため、センサの広域展開が重要であるが、ダークネットの情報もセキュリティ情報であり他組織にむやみに公開することはできない。また、ダークネットにセンサを設置することにもコストがかかる。
【０００７】
ここで、従来行われている主要なネットワーク観測プロジェクトについての概要を記す。
まず、Network Telescope（非特許文献２）を挙げることができる。これは、米国のCAIDA（Ｃｏｏｐｅｒａｔｉｖｅ Ａｓｓｏｃｉａｔｉｏｎ ｆｏｒ ＩｎｔｅｒｎｅｔＤａｔａ Ａｎａｌｙｓｉｓ）によるダークネット観測プロジェクトであり、１６万アドレス以上のダークネットを観測している。このプロジェクトでは、バックスキャッタやワームによるトラフィックのデータセットが公開されている。
【０００８】
次に、IMS（Ｉｎｔｅｒｎｅｔ Ｍｏｔｉｏｎ Ｓｅｎｓｏｒ）（非特許文献３）が挙げられる。これは、米国ミシガン大学による/8ネットワークを含む1700万アドレス以上の大規模ダークネット観測プロジェクトである。観測されたＴＣＰ ＳＹＮパケットの一部にセンサ側からＳＹＮ－ＡＣＫを返すことでＴＣＰコネクションの確立を試み、コネクション確立後の最初のパケットのペイロードを収集・分析する機能を持っている。
【０００９】
Leurre.com（非特許文献７、８参照）は、仏国のEurecomによる分散型ハニーポットを用いた情報収集・分析プロジェクトである。観測対象のＩＰアドレス数は比較的少数であるが、観測地域は世界各国に分散している。第１世代のLeurre.com v1.0は低インタラクションセンサのHoneyd（非特許文献９参照）を使用していたが、第２世代のLeurre.com v2.0ではSGNET（非特許文献１０参照）を使用して情報収集能力の向上を図っている。
【００１０】
REN-ISAC（非特許文献１１参照）は、米国の研究教育ネットワー（ＲＥＮ：Ｒｅｓｅａｒｃｈ ａｎｄ Ｅｄｕｃａｔｉｏｎ Ｎｅｔｗｏｒｋｉｎｇ）におけるセキュリティ情報の共有・分析プロジェクトである。Internet2で観測されたトラフィックを分析し、観測結果を公開している。
ISC（Ｉｎｔｅｒｎｅｔ Ｓｔｏｒｍ Ｃｅｎｔｅｒ）（非特許文献１２参照）は、米国のSANS（ＳｙｓＡｄｍｉｎ，Ａｕｄｉｔ，Ｎｅｔｗｏｒｋｉｎｇ，ａｎｄ Ｓｅｃｕｒｉｔｙ）による、セキュリティ情報の収集・分析プロジェクトである。５０万アドレス以上のファイアウォールログを、DShield（非特許文献１３参照）と呼ばれるシステムに集約し、統計情報やボランティアによる分析レポートを公開している。

【００１１】
これらの他、日本国内ではISDAS（非特許文献１４参照）、@police（非特許文献１５参照）、MUSTAN（非特許文献１６参照）、WCLSCAN（非特許文献１７参照）等のネットワーク観測プロジェクトが進行中である。
【００１２】
以上に示したこれまでの各種プロジェクトは、インターネット上の不正なトラフィックの傾向把握に主眼を置いており、組織の実ネットワークの保護に直結していないという課題を残している。
【先行技術文献】
【非特許文献】
【００１３】
【非特許文献１】D. Song, R. Malan, R. Stone, “A Snapshot of Global Internet Worm Activity,” The 14th Annual FIRST Conference onComputer Security Incident Handling and Response, 2002年
【非特許文献２】Moore, D.: Network telescopes: tracking Denial-of-Service attacksand internet worms around the globe, 17th Large Installation SystemsAdministration Conference (LISA’03), USENIX, 2003年
【非特許文献３】M. Bailey, E. Cooke, F.Jahanian, J. Nazario, D.Watson, “The Internet Motion Sensor: A Distributed Blackhole Monitoring System,” The 12th Annual Network andDistributed System Security Symposium (NDSS05), 2005年
【非特許文献４】K. Nakao, K. Yoshioka, D. Inoue,M. Eto, K. Rikitake, “nicter: An Incident Analysis System using Correlation betweenNetwork Monitoring and Malware Analysis,” The 1st Joint Workshop onInformation Security (JWIS06), pp. 363 - 377, 2006年
【非特許文献５】K. Nakao, K. Yoshioka, D. Inoue,M. Eto, “ANovel Concept of Network Incident Analysis based on Multi-layer Observations ofMalware Activities,” The2nd Joint Workshop on Information Security (JWIS07), pp. 267 - 279, 2007年
【非特許文献６】D. Inoue, M. Eto, K. Yoshioka,S. Baba, K. Suzuki, J. Nakazato, K. Ohtaka, K. Nakao, “nicter: An Incident Analysis Systemtoward Binding Network Monitoring with Malware Analysis,” WOMBAT Workshop on InformationSecurity Threats Data Collection and Sharing (WISTDCS 2008), pp. 58 - 66, 2008年
【非特許文献７】F. Pouget, M. Dacier, V.H.Pham, “Leurre.com: On the Advantages ofDeploying a Large Scale Distributed Honeypot Platform,” E-Crime and Computer Conference(ECCE’05),2005年
【非特許文献８】C. Leita, V. H. Pham, O. Thonnard,E. Ramirez-Silva, F. Pouget, E. Kirda, M. Dacier, “The Leurre.com Project: CollectingThreats Information using a Worldwide Distributed Honeynet,” WOMBAT Workshop on Information SecurityThreats Data Collection and Sharing (WISTDCS 2008), pp. 40 - 57, 2008年
【非特許文献９】N. Provos, “A Virtual Honeypot Framework,” The 13th USENIX SecuritySymposium, 2004年　インターネット http://www.honeyd.org/
【非特許文献１０】C. Leita, M. Dacier, “SGNET: A Worldwide DeployableFramework to Support the Analysis of Malware Threat Models,” The 7th European DependableComputing Conference (EDCC 2008), 2008年
【非特許文献１１】REN-ISAC: Research andEducation Networking Information Sharing and Analysis Center, インターネット http://www.ren-isac.net/
【非特許文献１２】M. V. Horenbeeck, “The SANS Internet Storm Center,” WOMBAT Workshop on InformationSecurity Threats Data Collection and Sharing (WISTDCS 2008), pp. 17 - 23, 2008年　インターネットhttp://isc.sans.org/.
【非特許文献１３】DShield,インターネット http://www.dshield.org/
【非特許文献１４】JPCERT/CCISDAS,インターネット http://www.jpcert.or.jp/isdas/.

【非特許文献１５】@police, インターネットhttp://www.cyberpolice.go.jp/english/obs_e.html
【非特許文献１６】MUSTAN, インターネット http://mustan.ipa.go.jp/mustan_web/.
【非特許文献１７】WCLSCAN, インターネット http://www.wclscan.org/.

【発明の概要】
【発明が解決しようとする課題】
【００１４】
本発明は上記従来技術が有する問題点に鑑みて創出されたものであり、ダークネット観測を広範囲に行い、その観測結果を用いて、サーバやホストが存在する組織の実ネットワークの保護の充実を図る技術を提供することを目的とする。
特に、ダークネットの情報提供や、センサの設置によりこれらを行う管理者側にも有益な情報を提供できるネットワーク監視システムやその処理方法を提供する。
【課題を解決するための手段】
【００１５】
本発明は、上記の課題を解決するために、次のようなネットワーク監視システムを提供する。最も特徴とする点は、これまでは疎な関係であったダークネット観測と実ネットワーク保護を直接的に結びつけることで、ダークネット観測の可能性を押し広げ、センサの広域展開の促進を図ることにある。
【００１６】
そこで、ネットワーク上で用いられるアドレスであって到達可能かつ未使用のアドレス空間をなすダークネットを監視するネットワーク監視システムを提供する。本システムは、異なる組織に管理され、それぞれが所定のアドレス範囲をもつ通信ネットワークと、その各通信ネットワーク内に設置され、自ネットワーク内のダークネット宛の信号を検出するセンサ手段と、各通信ネットワークのアドレス範囲の中で使用済みのアドレス情報を保持すると共に、各センサ手段の検出結果を受信する分析センタ装置とから構成される。
【００１７】
そして、分析センタ装置が、監視対象とする各通信ネットワークにおける使用済みのアドレス情報を格納する使用済みアドレス情報記憶手段と、各センサ手段から少なくとも信号の存在と、検出した信号の送信元アドレスとを含む検出結果を受理する検出結果受理手段と、検出結果を受理した際に、その信号の送信元アドレスが、監視対象の各通信ネットワークにおける使用済みのアドレス情報であるかどうかを分析する分析手段と、分析の結果、少なくとも該信号が使用済みのアドレスから発信されている場合にアラートを出力するアラート手段とからなることを特徴とする。
【００１８】
上記のネットワーク監視システムにおいて、センサ手段が、検出した信号の宛先ポート番号を検出し、分析手段が、所定の判定規則に従い、少なくとも宛先ポート番号の情報から不正な通信であるか否かを判定すると共に、判定結果に従ってアラート手段がアラートを出力する構成でもよい。
【００１９】
センサ手段が、送信元アドレスからの信号に対し何ら応答を行わないセンサであってもよい。また、センサ手段が、送信元アドレスからの既知の信号に対し所定の応答を行うセンサであってもよい。
【００２０】
本発明はネットワーク上で用いられるアドレスであって到達可能かつ未使用のアドレス空間をなすダークネットを監視するネットワーク監視方法として提供することもできる。本方法には、監視対象とする各通信ネットワークの使用済みのアドレス情報を使用済みアドレス情報記憶手段に格納した分析センタ装置を用いる。
【００２１】
そして、次の各ステップを有する。
（Ｓ１）　異なる組織に管理され、それぞれが所定のアドレス範囲をもつ通信ネットワー

ク内に設置されたセンサ手段が、自ネットワーク内のダークネット宛の信号を検出する信号検出ステップ、
（Ｓ２）　分析センタ装置の検出結果受理手段が、各センサ手段から少なくとも信号の存在と、検出した信号の送信元アドレスとを含む検出結果を受理する検出結果受理ステップ、
（Ｓ３）　分析センタ装置の分析手段が、検出結果を受理した際に、その信号の送信元アドレスが、監視対象の各通信ネットワークにおける使用済みのアドレス情報であるかどうかを分析する分析ステップ、
（Ｓ４）　分析センタ装置のアラート手段が、分析の結果、少なくとも該信号が使用済みのアドレスから発信されている場合にアラートを出力するアラートステップ。
【００２２】
上記のアラートステップにおいて、アラート手段が、センサ手段が検出した信号の送信元アドレスをアドレス範囲に含む通信ネットワークの管理者に対して、送信元アドレスの情報を通知する構成でもよい。
【００２３】
上記のセンサステップにおいて、センサ手段が、検出した信号の宛先ポート番号を検出し、分析ステップにおいて、分析手段が、所定の判定規則に従い、少なくとも該宛先ポート番号の情報から不正な通信であるか否かを判定し、さらにアラートステップにおいて、アラート手段が、判定結果に従って、アラートを出力することもできる。
【００２４】
ネットワーク監視方法の信号検出ステップにおいて、センサ手段が、送信元アドレスからの信号に対し何ら応答を行わない構成でもよい。
【００２５】
ネットワーク監視方法の信号検出ステップにおいて、センサ手段が、送信元アドレスからの既知の信号に対し所定の応答を行う構成でもよい。
【発明の効果】
【００２６】
本発明は、以上の構成を備えることにより、次の効果を奏する。
実際の組織内で用いられる通信ネットワークにおけるダークネットを監視することができるので、実ネットワークの保護に直結する監視活動を行うことができる。そして、分析センタ装置では各通信ネットワークのアドレス範囲と使用済みのアドレス情報を把握することで、実際に稼働しているホストからダークネット宛に信号が送られた場合に、それを検出することができるようになる。
これによって従来のように監視対象としているダークネットに他ネットワークから送信された信号だけを測定するのではなく、自ネットワークからダークネットに送信された信号を検出することで、自ネットワークにおけるウイルス感染や機器の設定ミスなどを早期発見することが可能となる。
【００２７】
通信ネットワークを運用する各組織は、ダークネットにセンサ手段を設置し、分析センタ装置に対して情報を提供しなければならないが、その一方で同じ分析センタ装置に情報を提供している通信ネットワークのダークネットに、自ネットワーク内から不正な信号が送信された場合には、分析センタ装置がそれを検出し、アラートを出力することができるので、自ネットワーク内の機器の不正な挙動を知ることができる。
【００２８】
すなわち、ダークネットで検出した信号の情報を分析センタ装置を介して共有することで、互いに自ネットワークから他の通信ネットワークへの不正な信号の送信を知ることができるようになる。この点、従来は研究目的で監視しているダークネットに着信する情報だけであったため、必ずしも実ネットワークの保護に直結するものではなかったが、本手法によれば、実際に稼働している通信ネットワークからの信号の送信を検出するため、より実際的な監視を行うことができる。

【００２９】
このように異なる組織間で実ネットワークの監視体制を共同で構築した場合、従来の手法ではセンサ手段の設置者が互いに通信ネットワークのアドレス範囲や使用済みアドレスの詳細を共有しなければならなかったため、普及が進まない原因の１つとなっていた。
本発明によれば、分析センタ装置が介在し、センサ手段で検出した発信元アドレスが本システムに加わっている組織のものかどうかも含めて分析センタ装置だけが管理すればよいので、参加組織間でもそれぞれの通信ネットワークに関わる情報を共有する必要がない。
これにより各組織のプライバシーやネットワークセキュリティの保護に寄与する。
【００３０】
その一方で、センサ手段の設置を負担した管理者は、自ネットワークから送信され、他のダークネットで検出されたという情報を知ることができるので、自ネットワーク内の機器に適切な対応をとることができる。
このような仕組みによってセンサ手段の設置者としては自ネットワークの管理に有用な情報を得ることができるので、センサ手段の設置にインセンティブが生じる。そのためセンサ手段が多くの通信ネットワークに設置されることが期待できる。
【００３１】
センサ手段が、検出した信号の宛先ポート番号を検出することもできる。宛先ポート番号がいずれであるかは感染しているウイルスの特定や、問題点の把握に有用な情報であり、分析手段が、所定の判定規則に従って不正な通信であるか否かを判定することに寄与する。
【００３２】
従来、ダークネットの監視にはさまざまなセンサが用いられているが、本発明においてセンサ手段に、送信元アドレスからの信号に対し何ら応答を行わないセンサを用いる構成によれば、メンテナンスが容易であり大規模にセンサ手段を設置することに適している。このようなセンサは、外部からセンサの存在を検知されないくいという利点もある。また、センサ手段の設置コストが低く、システム全体の低コスト化にも寄与する。
【００３３】
センサ手段が、送信元アドレスからの既知の信号に対し所定の応答を行うセンサを用いる構成によれば、センサ手段からパケットの送信元に対して一定レベルの応答を返し、それに対する反応を知ることができる。このため、送信元アドレスの機器の問題を特定しやすくなる利点がある。また、所定の応答のみを行うだけであるため、機器のメンテナンスが比較的容易である。
【図面の簡単な説明】
【００３４】
【図１】本発明に係るネットワーク監視システムの説明図である。
【図２】本発明に係る分析センタ装置の構成図である。
【図３】本発明に係る組織側センサ装置の構成図である。
【図４】本発明に係るネットワーク監視方法の処理フローチャートである。
【図５】内部ネットワークのスキャンを監視する様子を示す説明図である。
【図６】外部ネットワークのスキャンを監視する様子を示す説明図である。
【図７】ネットワーク監視システムによる観測結果である。
【発明を実施するための形態】
【００３５】
以下、本発明の実施形態を、図面に示す実施例を基に説明する。なお、実施形態は下記に限定されるものではない。まず、本発明の概要を説明する。
本発明では、従来のようにダークネットをトラフィックの傾向把握に利用するだけでなく、サーバやホストが存在する実ネットワーク（以下、ライブネットと言う。）の保護に直接的に活用するためのアーキテクチャをもつことに要点がある。すなわち、これまでのダークネット観測では、ある組織が保有するダークネットに到達したトラフィック（以下

、ダークネットトラフィック）を、組織内に設置したセンサに向けて転送し、センサがダークネットトラフィックを中央の分析センタに送信する。分析センタは各組織のセンサから集まったダークネットトラフィックを分析し、トラフィックの統計情報等を公開するというアーキテクチャが一般的である。

【００３６】

本発明では、従来のダークネット観測アーキテクチャを踏襲し、特に各組織に設置したセンサには変更を加えることを必要としない。しかし従来と異なるのは、各組織がライブネットとして使用しているＩＰアドレスの範囲を分析センタに登録しておく点である。

すなわち、図１のようなネットワーク監視システム（１）において、複数の組織、例えば組織Ａないし組織Ｇが管理する通信ネットワーク（２ａ）～（２ｇ）と、各通信ネットワーク（２ａ）～（２ｇ）を監視する分析センタ装置（１０）が設けられている。

【００３７】

各通信ネットワーク（２ａ）～（２ｇ）には、ネットワーク機器にアドレスが割り当てられて使用済みのライブネット（３）と、各組織が自由に割り当てることができるが、実際には機器に割り当てられていないダークネット（４）とが存在する。

本発明におけるアドレスとはネットワーク上で用いられるいかなるアドレスでもよく、ＩＰネットワークでは、ＩＰアドレスが代表的である。ネットワーク機器に割り当てられるＭＡＣアドレスなどの物理アドレスでもよい。

【００３８】

各組織は、ダークネットを観測するためのセンサ手段を配置している。そして、内部ネットワーク又は外部ネットワークから、ダークネット宛の信号を検出すると、そのダークネットトラフィックを分析センタ装置（１０）に転送する。

【００３９】

図２は、分析センタ装置（１０）の構成図、図３は各通信ネットワークに設置されるセンサ装置の構成図、図４は本発明によるネットワーク監視方法の処理フローチャートである。

分析センタ装置（１０）及びセンサ装置（２０）は、周知のパーソナルコンピュータや、ワークステーション等によって構成するのが簡便であり、ＣＰＵ（１１）（２１）と図示しないメモリが協働して、記憶手段に格納されたプログラムに従って各処理を行う。コンピュータの動作方法については周知の事項であるから、説明を省略する。

【００４０】

分析センタ装置（１０）には、ＣＰＵ（１１）の他、各通信ネットワークと接続する通信モジュール（１２）（１３）、情報を格納する記憶手段であるハードディスク（１４）が備えられている。なお、通信モジュール（１２）（１３）は各通信ネットワークに適合するものを設ければよく、複数の通信ネットワークに対応するモジュールを１基でもよい。

【００４１】

ＣＰＵ（１１）には、各センサ装置（２０）から少なくともダークネットトラフィックの存在と、検出した信号の送信元アドレスとを含む検出結果を受理する検出結果受理部（１１１）、検出結果を受理した際に、その信号の送信元アドレスが、監視対象の各通信ネットワーク（２ａ）～（２ｇ）のアドレス範囲であって、かつ使用済みのアドレス情報であるかどうかを分析する分析部（１１２）、分析の結果、少なくともダークネットトラフィックが使用済みのアドレスから発信されている場合にアラートを出力するアラート部（１１３）を備えている。

【００４２】

また、本発明の特徴として述べたように、ハードディスク（１４）には、監視対象とする各通信ネットワークにおける使用済みのアドレス情報（１４１）を格納している。このほか、各通信ネットワークのアドレス範囲をアドレス範囲情報（１４２）として備えておいてもよい。

【００４３】

各組織側に設置されるセンサ手段の構成は、本発明は任意であるが、一例として図３のようにＣＰＵ（２１）に信号センサ（２２）、モニタ（２３）を設けたセンサ装置（２０）を設置することができる。

信号センサ（２２）は、自ネットワーク（２）のダークネット（４）を監視し、不正なダークネットトラフィックが受信されるかどうかを監視する。

【００４４】

本実施例におけるセンサ装置（２０）の機能としては、ダークネットトラフィックを通知する他に、使用済みアドレス情報を送信する機能、分析センタ装置（１０）からアラートを受け取って出力する機能が備えられている。

【００４５】

図４を用いて、処理の流れを説明する。

まず、各通信ネットワークにおいて、センサ装置（２０）の自ネットワーク情報送信部（２１１）から、自ネットワークにおけるライブネットの情報、すなわち使用済みアドレス情報を送信する（自ネットワーク情報通知ステップ：Ｓ１０）。

分析センタ装置（２０）ではこれを通信モジュール（１２）（１３）で受信し、ハードディスク（１４）に使用済みアドレス情報（１４１）として格納する。（各通信ネットワーク情報収集ステップ：Ｓ１１）

【００４６】

この状態で、各通信ネットワーク（２ａ）～（２ｇ）の信号センサ（２２）はそれぞれのダークネットを監視した状態とする。

そして、例えば組織Ａの通信ネットワーク（２ａ）において、ダークネットトラフィックを信号センサ（２２）とそれを制御するセンサ処理部（２１２）が検出すると、検出結果送信部（２１３）から分析センタ装置（１０）に向けて送信する。

【００４７】

このとき、センサ処理部（２１２）では、信号センサ（２２）が受信したダークネットトラフィックの中から、少なくとも送信元ホストのアドレスを抽出して送信する。あるいは、単位ダークネットトラフィック全体を送信する構成でもよい。（信号検出ステップ：Ｓ１２）

【００４８】

分析センタ装置（１０）の検出結果受理部（１１１）が通信モジュール（１２）を介して検出結果を受理（Ｓ１３）する。（検出結果受理ステップ：Ｓ１３）

さらに、分析部（１１２）では、使用済みアドレス情報（１４２）を参照して、該ダークネットのトラフィックの送信元アドレスが、使用済みアドレス情報のアドレスに含まれるかを照合する。（分析ステップ：Ｓ１４）

【００４９】

ここで、分析部（１１２）の処理として、前記でセンサ処理部（２１２）が送信元アドレスを抽出してある場合には、単に照合すればよいし、ダークネットトラフィック全体が転送された場合には、その中から送信元ホストを分析する処理を行う。

例えばＩＰパケットの場合には、１２バイト目からの３２ビットが送信元ＩＰアドレス、１６バイト目から３２ビットが宛先ＩＰアドレスであり、これらを分析することで送信元アドレスが抽出される。

また、分析部（１１２）は従来行われているように、ダークネットトラフィックの内容を分析して、感染しているウイルスの種類や、挙動の解析、送信元ホストの設定ミスの判定などを行っても良い。

【００５０】

さらに、ダークネットトラフィックが送られてきた宛先のポート番号を分析することもできる。マルウェアの典型的な挙動として、ポート番号５００００番など、一般的にはあまり用いられないポート番号にランダムに送ってくる場合や、ＴＣＰが用いる８０番、８０８０番などに大量の信号を送ってくる場合がある。

一方、ＵＤＰの６７番ポートなどはＤＨＣＰサーバがＬＡＮ内部で用いるポート番号で

あり、これがダークネットに送信されるのはマルウェアよりは設定ミスの可能性が高い。
このように、ポート番号を分析することで、ウイルスに感染しているのか、設定ミスであるのか、などをある程度判定することができる。

【００５１】

そこで、ハードディスク（１４）に、例えばマルウェアを疑うべきプロトコルとポート番号、設定ミスを疑うべきプロトコルとポート番号、アラートの必要のないプロトコルとポート番号のリストを判定規則として格納しておき、分析部（１１２）でポート番号の照合を行う。
この結果、「マルウェア」「設定ミス」「アラート必要無し」に分類する。
その他、公知の手法を用いて、マルウェアの種類や設定ミスの内容の推定などを行ってもよい。

【００５２】

分析処理の結果、例えば検出されたダークネットトラフィックの送信元アドレスが、組織Ｂのライブネットのアドレスであった場合にアラート部（１１３）でアラートを出力する。本発明では最低限、分析センタ装置（１０）上で画面表示により出力したり、スピーカから音を出力したり、ハードディスク（１４）にアラートを記録する処理でもよい。
本実施例では、アラート部（１１３）から通信モジュール（１３）を介して、センサ装置（２０）のアラート受理部（２１４）にアラート情報を送信する。（アラート通知ステップ：Ｓ１５）

【００５３】

アラート受理部（２１４）がアラート情報を受理（アラート受理ステップ：Ｓ１６）し、モニタ（２３）からアラート情報を表示する。（アラート表示ステップ：Ｓ１７）
ここで、分析ステップ（Ｓ１４）において「マルウェア」や「設定ミス」と判定し、その結果をアラートとして送信している場合には、これも表示して、管理者にどのホストについてどのような疑いがあるのかを知らせることができる。

【００５４】

本発明において、ハードディスク（１４）にアドレス範囲情報（１４２）を備えておくとき、前記ダークネットトラフィックの送信元アドレスが使用済みアドレス情報（１４１）に含まれない場合でも、アドレス範囲情報（１４２）に含まれるときには、その通信ネットワークのセンサ装置（２０）にアラートする構成でもよい。これによりＤＨＣＰサーバなどから動的にＩＰアドレスを割り当てる場合など、使用済みアドレス情報の更新が間に合わない場合などでも、発信元として疑わしい通信ネットワークの管理者に通知することができる。

【００５５】

本発明によりどのようなダークトラフィックが検出できるのか、２つの具体例を説明する。
まず、図５に内部ネットワークのスキャンを監視する様子を示す説明図を示す。この図は組織Ｇの通信ネットワーク（２ｇ）内に、マルウェアに感染したホストコンピュータのアドレス（５）が存在しているパターンである。

【００５６】

このようにある組織において、自組織が管理するＩＰアドレスの範囲内に含まれるダークネットを、内部ダークネットと呼ぶこととする。組織内で、マルウェアに感染したホストがローカルスキャン（５０）（典型的には感染ホストを含む/24や/16ネットワークへのスキャン）を行ない、内部ダークネットにスキャンが到達した場合、分析センタ装置（１０）がそれを検出し、該当する組織にアラートを送信する。

【００５７】

図５の例では、組織Ｇ内でマルウェアに感染したホストがローカルスキャンを行なった結果、組織Ｇに設置されたセンサ装置（２０）の信号センサ（２２）がこれを検出しダークネットトラフィック（５１）を送信する。
そして、分析センタ装置（１０）の分析でこの送信元アドレスが、組織Ｇの感染ホスト

のアドレス（５）であることが判明する。

【００５８】

この分析結果に従って組織Ｇに対して分析センタ装置（１０）からアラート（５２）が送信されている。内部ダークネットではローカルスキャン以外にも、組織内でのネットワーク設定の間違い等によって、自組織からのパケットが検出される場合もあるが、いずれにせよ不正なパケットであるため、アラートはネットワーク管理上の有用な情報となり得る。

このような内部ダークネットの監視に使われる構成では、どちらにしても組織Ｇの通信ネットワーク内の情報であるため、ダークネット内にどのようにトラフィックがあったのか、全ての情報を管理者に通知してもよい。これにより、問題の特定が容易になることが考えられる。

【００５９】

一方、図６は外部ネットワークのスキャンを監視する様子を示す説明図を示す。この図は組織Ｇの通信ネットワーク（２ｇ）内に、マルウェアに感染したホストコンピュータのアドレス（５）が存在し、組織Ａのダークネットをスキャンしているパターンである。

ある組織において、自組織が管理するＩＰアドレスの範囲外のダークネットを、外部ダークネットと呼ぶこととする。組織内で、マルウェアに感染したホストがグローバルスキャン（６０）（感染ホストが属する組織外へのスキャン）を行ない、外部ダークネットにスキャンが到達した場合、分析センタ装置（１０）がそれを検出し、該当する組織にアラートを送信する。

【００６０】

図６の例では、組織Ｇ内でマルウェアに感染したホストがグローバルスキャンを行い、スキャンが組織Ａのダークネットに到達した結果、組織Ｇに設置されたセンサ装置（２０）の信号センサ（２２）がこれを検出しダークネットトラフィック（６１）を送信する。

そして、分析センタ装置（１０）の分析でこの送信元アドレスが、組織Ｇの感染ホストのアドレス（５）であることが判明する。

【００６１】

この分析結果に従って組織Ｇに対して分析センタ装置（１０）からアラート（６２）が送信されている。外部ダークネットではグローバルスキャン以外にも、分析センタに登録されたライブネットからのバックスキャッタが検出された結果、アラートが送信される場合もあるが、それは自組織のサーバが何らかの攻撃を受けている可能性を示唆しており、セキュリティ上重要な情報である。

【００６２】

このような外部ダークネットの監視に使われる構成では、組織Ｇの管理者としては組織Ａの管理者に自ネットワークの詳細な情報を送られることを欲しないのが通常である。一方、マルウェアの感染の場合には、組織Ａの管理者として組織Ｇが特定されてもほとんど意味をなさず、このような情報は必要ではない。

本発明によれば、分析センタ装置（１０）は組織Ａのセンサ手段を利用するものの、組織Ｇの管理者にだけアラートを通知すればよい。

【００６３】

この場合には、組織Ａの管理者としては、センサ手段を設置したことで直接的な利益を受けるものではないが、組織Ｇにおいてマルウェア感染から修復されることで自ネットワークへの攻撃も解消することができ、参加している通信ネットワーク全体のセキュリティの向上に寄与する。また当然、組織Ａ内でマルウェア感染が生じた場合には、参加する他のセンサ手段により原因を特定できることになるから、互恵的な効果があり、センサ手段を設置する十分な利益が存在していることになる。

【００６４】

ここで、センサ手段について２つの態様を示す。

本発明のセンサ手段としては、特にブラックホールセンサが好適である。ブラックホールセンサとは、パケットの送信元に対し、全く応答を行なわないセンサを言う。上記実施

例で述べたのはこのセンサであり、ただ入力する信号を監視しているだけなので、メンテナンスが容易である。そのため、本発明のような大規模なダークネット観測に向き、設置にも多くのコストがかからないことから、本発明システムに最適である。

【００６５】

ブラックホールセンサは、無応答であるため、外部からセンサの存在を検知することが困難であるという利点もある。また、センサ手段自体がマルウェアに感染するリスクは非常に小さい。

マルウェアの感染活動の初期段階であるスキャンは観測可能であるが、それ以降の挙動を観測することは出来ない。しかし、本発明において送信元ホストを特定する点では、十分な作用をもつと言うことができる。

【００６６】

ブラックホールセンサに次いで好適なセンサとしては、低インタラクションセンサが挙げられる。これはパケットの送信元に対し、一定レベルの応答を返すセンサである。TCP SYNパケットに対してSYN-ACK パケットを返すセンサや、ＯＳの既知の脆弱性をエミュレートする低インタラクションハニーポットがここに含まれる。このセンサでは、マルウェアの挙動をある程度監視できる他、既知の信号に対し所定の応答を行うだけであるため、マルウェアの攻撃は受けにくい。

しかし、リッスンしているポートの傾向等からセンサの存在を検知され易く、アドレスが連続した大規模なダークネットでの運用には不向きという特徴がある。

【００６７】

一方、高インタラクションセンサと呼ばれるセンサも知られている。これは、実ホストもしくはそれに準じた応答を返すセンサ（いわゆる、高インタラクションハニーポット）である。マルウェア感染時の挙動や攻撃者のキーストロークまで多様な情報が取得可能であるが、安全な運用を行うためのコストは高く、大規模運用には不向きである。

もっとも、本発明の各センサ手段は、同一のものでなくてもよく、このような高インタラクションセンサを用いる組織が混在していてもよい。

【００６８】

従来のダークネットの利用法は、組織外から飛来する不正なパケットを観測する、つまり外から内へのアクセスを捉えるという考え方であった。一方、提案方式は、組織内から送出された不正なパケットを分散配置されたダークネットで観測する、つまり内から外（または内から内）へのアクセスを捉えるという、従来とは逆転したダークネットの利用法を提示している。

【００６９】

本発明では、組織内で起こったマルウェア感染等を分析センタ装置（１０）が検出し、該当する組織にアラートを送信することで、ダークネットの観測結果が実ネットワークのセキュリティオペレーションのトリガとなることが期待される。

従来のダークネット観測の２つの課題の前者、すなわち実ネットワーク保護を図るものである。ダークネットを提供する組織側の観点から見ると、組織内の一部の使用済みＩＰアドレスの提供とブラックホールセンサの設置によって、広域のダークネット観測網からアラートという直接的なフィードバックが得られ、組織内のホストによる外部への不正アクセスを迅速に検出できるというインセンティブが働く。

【００７０】

このため、ダークネット観測の２つの課題の後者、センサの広域展開の進展が期待でき、さらにダークネット観測網の拡大、分析精度の向上、参加組織の増加という、正のスパイラルを実現することができる。

【００７１】

最後に、ｎｉｃｔｅｒのブラックホールセンサを設置している国内の２組織（便宜上、組織Ｘと組織Ｙと呼ぶ）のダークネット観測結果を基に、本発明の有効性を検証する実験結果を示す。組織Ｘは／１６ネットワークの中に、ダークネットとライブネットが混在する（図１の組織Ｂの様な）ネットワーク構成となっている。そこで、組織Ｘのライブネッ

トを分析センタ装置に登録するＩＰアドレスとし、組織Ｘのダークネットを内部ダークネットと見なす。

【００７２】

一方、組織Ｙは／１６ネットワーク全体が未使用であるダークネットを保有している。この組織Ｙのダークネットを外部ダークネットと見なす。図７は２００８年７月に、組織Ｘから内部ダークネットまたは外部ダークネットに対して、パケットを１つ以上送信したユニークホスト数を、１日毎にプロットしたものである。

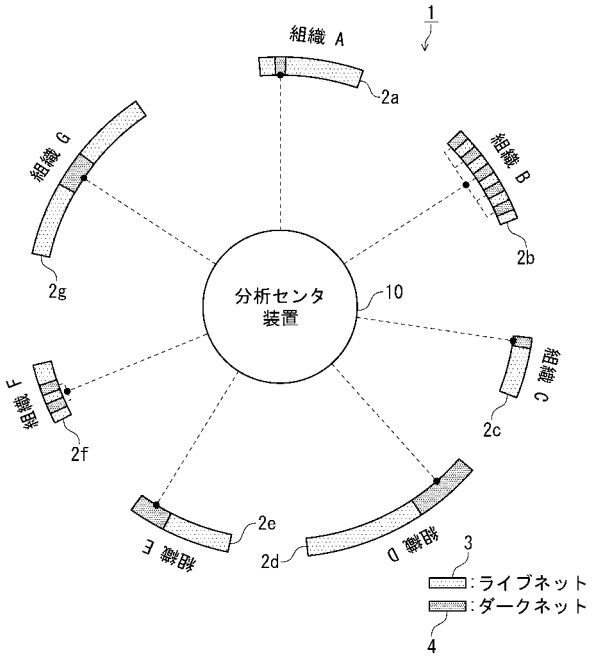
内部ダークネットでは１日平均約８３ホストのアクセスが検出され、７月１６日にはスパイク（１７６ホスト）が見られた。一方、外部ダークネットでは、１日平均約０．３ホストのアクセスが検出され、最大は７月５日の２ホストであった。これら検出されたホストは、通常のネットワーク利用では起こり得ない挙動をしており、アンチウイルスソフトの適用やＯＳの最新版へのアップデート、もしくはネットワーク設定の確認などの対応が必要であり、本発明によるアラートが有効であると考えられる。

【符号の説明】

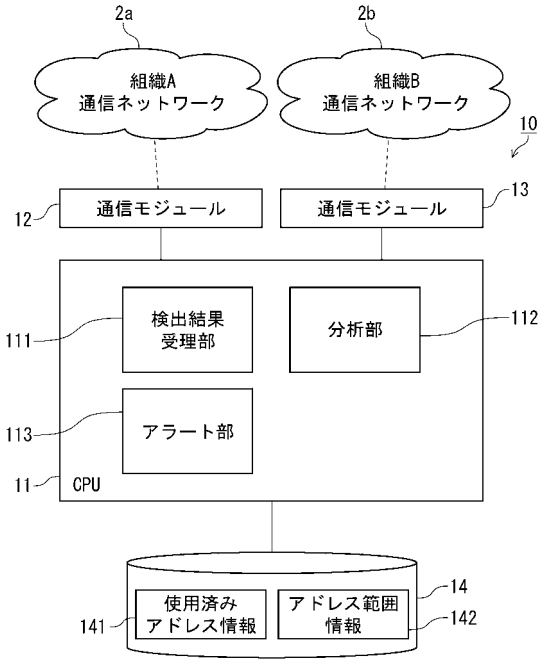
【００７３】

１　ネットワーク監視システム
２ａ　組織Ａの通信ネットワーク
２ｂ　組織Ｂの通信ネットワーク
２ｃ　組織Ｃの通信ネットワーク
２ｄ　組織Ｄの通信ネットワーク
２ｅ　組織Ｅの通信ネットワーク
２ｆ　組織Ｆ通信ネットワーク
２ｇ　組織Ｇの通信ネットワーク
３　ライブネット
４　ダークネット
１０　分析センタ装置

【図１】

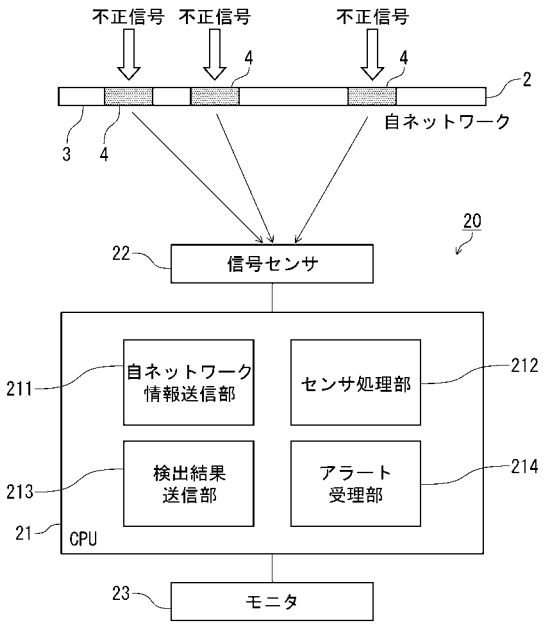


【図２】



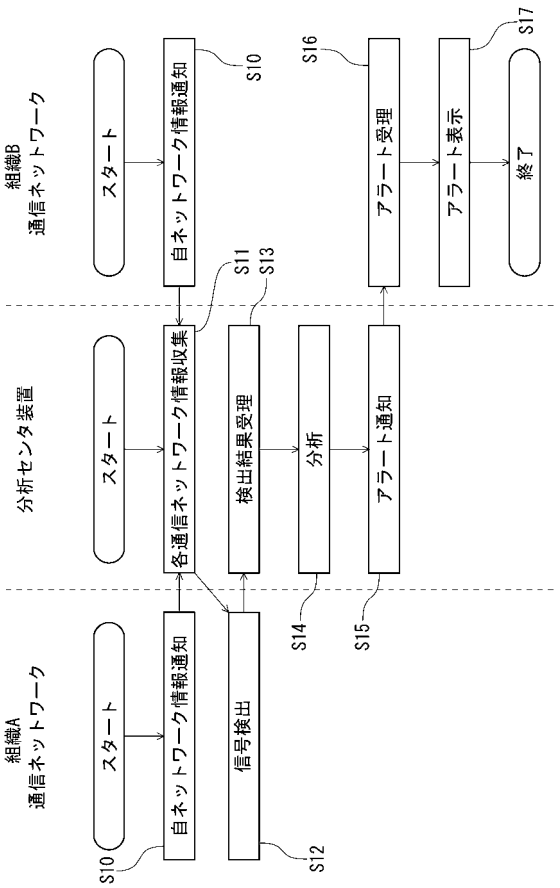
分析センタ装置

【図３】

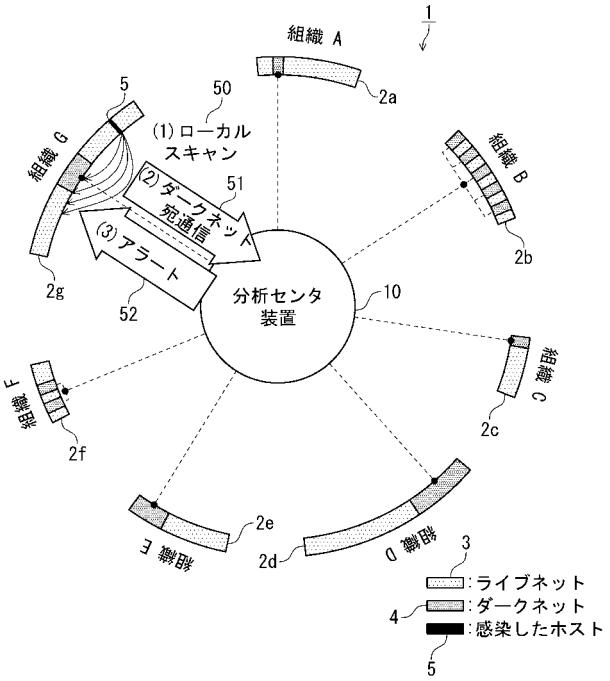


組織側センサ装置

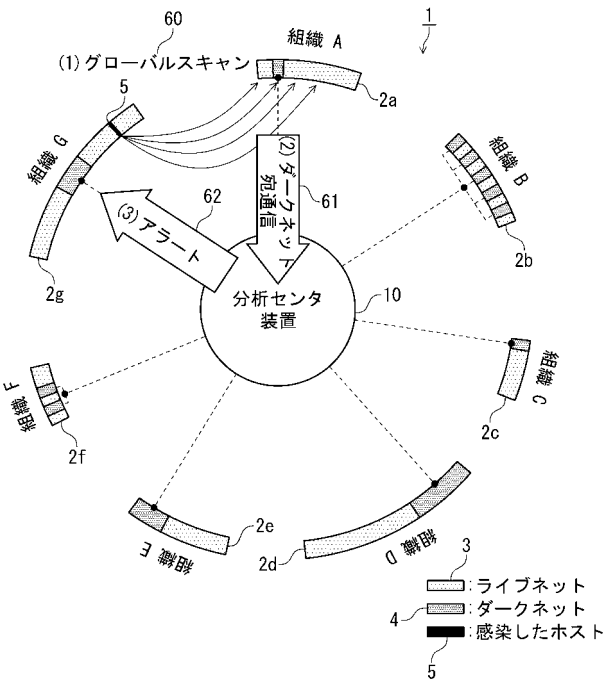
【図４】



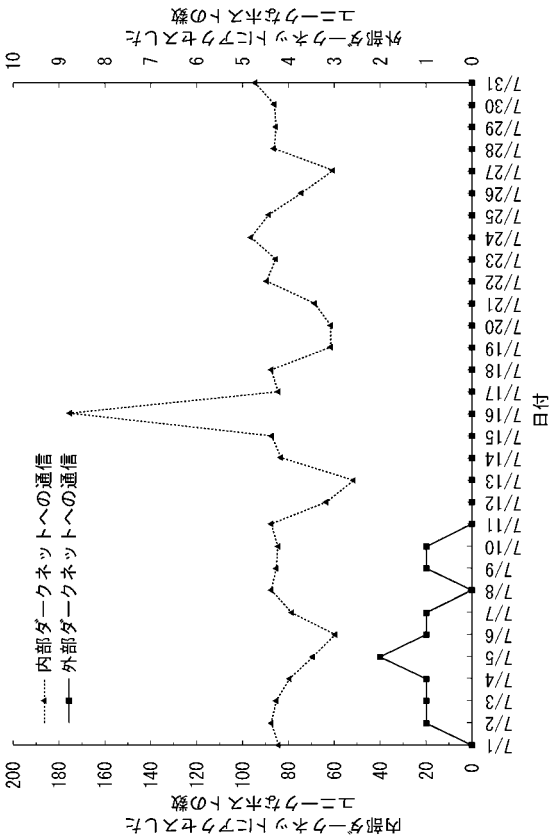
【図５】


1
組織 A
2a
組織 B
2b
組織 C
2c
組織 D
2d
組織 E
2e
組織 F
2f
組織 G
2g
5
50
(1) ローカル
スキャン
(2) ダークネット
宛通信
51
(3) アラート
52
分析センタ
装置
10
3
:ライブネット
4
:ダークネット
:感染したホスト
5

【図６】


60
(1) グローバルスキャン
1
組織 A
2a
組織 B
2b
組織 C
2c
組織 D
2d
組織 E
2e
組織 F
2f
組織 G
2g
5
(2) ダークネット
宛通信
61
62
(3) アラート
分析センタ
装置
10
3
:ライブネット
4
:ダークネット
:感染したホスト
5

【図７】


外部ダークネットにアクセスした
ユニークなホストの数
0
1
2
3
4
5
6
7
8
9
10
日付
7/1
7/2
7/3
7/4
7/5
7/6
7/7
7/8
7/9
7/10
7/11
7/12
7/13
7/14
7/15
7/16
7/17
7/18
7/19
7/20
7/21
7/22
7/23
7/24
7/25
7/26
7/27
7/28
7/29
7/30
7/31
内部ダークネットにアクセスした
ユニークなホストの数
0
20
40
60
80
100
120
140
160
180
200
内部ダークネットへの通信
外部ダークネットへの通信

フロントページの続き

Ｆターム(参考) 5B089 GB02 HA10 HB02 KA12 KB06 MC02
5B285 AA06 BA01 CA32 CA37 DA04
5K030 GA15 JA10 MB01 MC08