(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6033021号
(P6033021)
(45)発行日　平成28年11月30日(2016.11.30)　(24)登録日　平成28年11月4日(2016.11.4)

(51)Int.Cl.		F I		
G06F 21/56	(2013.01)	G06F	21/56	360
G06F 21/55	(2013.01)	G06F	21/55	320
H04L 12/66	(2006.01)	H04L	12/66	B

請求項の数 14　(全 80 頁)

(21)出願番号　特願2012-209346(P2012-209346)
(22)出願日　平成24年9月24日(2012.9.24)
(65)公開番号　特開2014-63424(P2014-63424A)
(43)公開日　平成26年4月10日(2014.4.10)
審査請求日　平成27年9月2日(2015.9.2)

(73)特許権者　591102095
三菱スペース・ソフトウエア株式会社
東京都港区浜松町２丁目４番１号
(74)代理人　100099461
弁理士　溝井　章司
(72)発明者　飯沢　拓也
神奈川県鎌倉市上町屋７９２番地　三菱スペース・ソフトウエア株式会社　鎌倉事業部内
(72)発明者　明石　敬
神奈川県鎌倉市上町屋７９２番地　三菱スペース・ソフトウエア株式会社　鎌倉事業部内

審査官　宮司　卓佳

最終頁に続く

(54)【発明の名称】不正通信検出装置及びサイバー攻撃検出システム及びコンピュータプログラム及び不正通信検出方法

(57)【特許請求の範囲】
【請求項１】
ネットワークを介した通信を取得する通信取得部と、
上記通信取得部が取得した通信を解析して、上記通信の特性値を算出する特性値算出部と、
１以上の通信について上記特性値算出部が算出した特性値に基づいて統計量を算出する統計量算出部と、
上記統計量算出部が算出した統計量に基づいて、上記特性値算出部が算出した特性値が異常値であるか否かを判定し、上記特性値が異常値であると判定した場合に、不正通信の可能性があると判定する不正判定部と、
宛先が同じ複数の通信について上記特性値算出部が算出した特性値を平均した宛先別平均値を算出する宛先別平均値算出部と
を有し、
上記不正判定部は、上記統計量算出部が算出した統計量に基づいて、上記宛先別平均値算出部が算出した宛先別平均値が異常値であるか否かを判定し、上記宛先別平均値が異常値であると判定した場合に、不正通信の可能性があると判定する不正通信検出装置。
【請求項２】
ネットワークを介した通信を取得する通信取得部と、
上記通信取得部が取得した通信を解析して、上記通信の特性値を算出する特性値算出部と、

１以上の通信について上記特性値算出部が算出した特性値に基づいて統計量を算出する統計量算出部と、
上記統計量算出部が算出した統計量に基づいて、上記特性値算出部が算出した特性値が異常値であるか否かを判定し、上記特性値が異常値であると判定した場合に、不正通信の可能性があると判定する不正判定部と、
所定の期間内に上記通信取得部が取得した通信の通信数を、上記通信の宛先ごとに計数する通信計数部と
を有し、
上記不正判定部は、いずれかの宛先について上記通信計数部が計数した通信数が１である場合に、不正通信の可能性があると判定する不正通信検出装置。

【請求項３】
ネットワークを介した通信を取得する通信取得部と、
上記通信取得部が取得した通信を解析して、上記通信の特性値を算出する特性値算出部と、
１以上の通信について上記特性値算出部が算出した特性値に基づいて統計量を算出する統計量算出部と、
上記統計量算出部が算出した統計量に基づいて、上記特性値算出部が算出した特性値が異常値であるか否かを判定し、上記特性値が異常値であると判定した場合に、不正通信の可能性があると判定する不正判定部と、
所定の期間内に上記通信取得部が取得した通信の数を、上記通信の宛先ごとに計数する通信計数部と、
複数の期間について上記通信計数部が計数した通信数の統計量を、上記宛先ごとに算出する通信数統計量算出部と
を有し、
上記不正判定部は、上記通信数統計量算出部が算出した統計量が所定の閾値より小さい場合に、不正通信の可能性があると判定する不正通信検出装置。

【請求項４】
上記統計量算出部は、上記宛先別平均値算出部が算出した宛先別平均値に基づいて、上記統計量を算出する請求項１に記載の不正通信検出装置。

【請求項５】
上記通信取得部は、上記通信として、ハイパーテキスト転送プロトコルにおけるリクエストを取得し、
上記特性値算出部は、上記通信取得部が取得した通信に基づいて、上記特性値として、統一資源識別子の長さと、上記統一資源識別子のうち絶対パス文字列の長さと、上記統一資源識別子のうちクエリー文字列の長さと、上記リクエスト全体の長さとのうち、少なくともいずれかを算出する請求項１から４のいずれか１項に記載の不正通信検出装置。

【請求項６】
上記統計量算出部は、上記統計量として、上記１以上の通信についての上記特性値を平均した平均値及び標準偏差を算出し、
上記不正判定部は、上記標準偏差に所定の定数を乗じた値を上記平均値に加えた値よりも上記特性値が大きい場合と、上記標準偏差に所定の定数を乗じた値を上記平均値から差し引いた値よりも上記特性値が小さい場合とのうち、少なくともいずれかの場合に、上記特性値が異常値であると判定する請求項１から５のいずれか１項に記載の不正通信検出装置。

【請求項７】
上記通信取得部は、上記通信として、ハイパーテキスト転送プロトコルにおけるリクエストを取得し、
上記統計量算出部は、上記統計量として、上記１以上の通信のうち、ゲットメソッドである通信についての上記特性値を平均した平均値及び標準偏差と、ポストメソッドである通信についての上記特性値を平均した平均値及び標準偏差と、ポストメソッド以外のメソ

ッドである通信についての上記特性値を平均した平均値及び標準偏差とのうち、少なくともいずれかの平均値及び標準偏差を算出する請求項６に記載の不正通信検出装置。
【請求項８】
上記通信取得部は、上記通信として、ハイパーテキスト転送プロトコルにおけるリクエストを取得し、
上記不正判定部は、上記通信取得部が取得した通信がポストメソッドである場合と、上記通信のフォーマットがハイパーテキスト転送プロトコルの規定に合致しない場合と、上記通信のユーザエージェントが所定のリストに含まれるユーザエージェントでない場合とのうち、少なくともいずれかの場合に、不正通信の可能性があると判定する請求項１から７のいずれか１項に記載の不正通信検出装置。
【請求項９】
上記不正判定部は、上記通信取得部が取得した通信の宛先が所定のリストに含まれる宛先である場合に、不正通信の可能性があると判定する請求項１から８のいずれか１項に記載の不正通信検出装置。
【請求項１０】
請求項１から９のいずれか１項に記載の不正通信検出装置と、
上記ネットワークを介した通信によって転送される電子メールのうちから、作成者を詐称した詐称メールを検出する詐称メール検出装置と
を有するサイバー攻撃検出システム。
【請求項１１】
コンピュータが実行することにより、上記コンピュータを請求項１から１０のいずれか１項に記載の不正通信検出装置として機能させるコンピュータプログラム。
【請求項１２】
ネットワークを介した通信を取得し、
取得した通信を解析して、上記通信の特性値を算出し、
１以上の通信について算出した特性値に基づいて、統計量を算出し、
算出した統計量に基づいて、上記特性値が異常値であるか否かを判定し、
上記特性値が異常値であると判定した場合に、不正通信の可能性があると判定し、
宛先が同じ複数の通信について、算出した特性値を平均した宛先別平均値を算出し、
算出した統計量に基づいて、算出した宛先別平均値が異常値であるか否かを判定し、上記宛先別平均値が異常値であると判定した場合に、不正通信の可能性があると判定する不正通信検出方法。
【請求項１３】
ネットワークを介した通信を取得し、
取得した通信を解析して、上記通信の特性値を算出し、
１以上の通信について算出した特性値に基づいて、統計量を算出し、
算出した統計量に基づいて、上記特性値が異常値であるか否かを判定し、
上記特性値が異常値であると判定した場合に、不正通信の可能性があると判定し、
所定の期間内に、取得した通信の通信数を、上記通信の宛先ごとに計数し、
いずれかの宛先について、計数した通信数が１である場合に、不正通信の可能性があると判定する不正通信検出方法。
【請求項１４】
ネットワークを介した通信を取得し、
取得した通信を解析して、上記通信の特性値を算出し、
１以上の通信について算出した特性値に基づいて、統計量を算出し、
算出した統計量に基づいて、上記特性値が異常値であるか否かを判定し、
上記特性値が異常値であると判定した場合に、不正通信の可能性があると判定し、
所定の期間内に、取得した通信の数を、上記通信の宛先ごとに計数し、
複数の期間について、計数した通信数の統計量を、上記宛先ごとに算出し、
算出した統計量が所定の閾値より小さい場合に、不正通信の可能性があると判定する不

正通信検出方法。

【発明の詳細な説明】

【技術分野】

【０００１】

この発明は、サイバー攻撃を検出する装置及び方法に関する。

【背景技術】

【０００２】

迷惑メールやスパムメールなどと呼ばれる歓迎されない電子メールを検出する技術がある。

また、コンピュータウィルスを検出する技術がある。

【先行技術文献】

【非特許文献】

【０００３】

【非特許文献１】「Ｓｅｎｄｅｒ Ｐｏｌｉｃｙ Ｆｒａｍｅｗｏｒｋ （ＳＰＦ） ｆｏｒ Ａｕｔｈｏｒｉｚｉｎｇ Ｕｓｅ ｏｆ Ｄｏｍａｉｎｓ ｉｎ Ｅ－Ｍａｉｌ, Ｖｅｒｓｉｏｎ １」ＲＦＣ４４０８、ｈｔｔｐ：／／ｔｏｏｌｓ．ｉｅｔｆ．ｏｒｇ／ｈｔｍｌ／ｒｆｃ４４０８。

【非特許文献２】「Ｓｅｎｄｅｒ ＩＤ： Ａｕｔｈｅｎｔｉｃａｔｉｎｇ Ｅ－Ｍａｉｌ」ＲＦＣ４４０６、ｈｔｔｐ：／／ｔｏｏｌｓ．ｉｅｔｆ．ｏｒｇ／ｈｔｍｌ／ｒｆｃ４４０６

【非特許文献３】「ＤｏｍａｉｎＫｅｙｓ Ｉｄｅｎｔｉｆｉｅｄ Ｍａｉｌ （ＤＫＩＭ） Ｓｉｇｎａｔｕｒｅｓ」ＲＦＣ４８７１、ｈｔｔｐ：／／ｔｏｏｌｓ．ｉｅｔｆ．ｏｒｇ／ｈｔｍｌ／ｒｆｃ４８７１

【発明の概要】

【発明が解決しようとする課題】

【０００４】

近年、標的型サイバー攻撃と呼ばれる新しい形のサイバー攻撃が出現してきた。

【０００５】

図１は、標的型サイバー攻撃を説明するための図である。

【０００６】

ローカルネットワークシステム１０は、例えば、会社内のコンピュータなどを接続したシステムである。ローカルネットワークシステム１０は、例えば、ローカルエリアネットワーク１１と、端末装置１２と、ファイルサーバ装置１３と、メールサーバ装置１４と、ウェブプロキシ装置１５とを有する。

【０００７】

端末装置１２は、例えば社員などが操作するコンピュータである。端末装置１２は、例えば、同じ会社内の他の社員や社外との間で電子メールをやり取りするためのメール機能や、インターネットなどで公開されているウェブページを閲覧するためのブラウザ機能などを有する。端末装置１２は、ローカルエリアネットワーク１１に接続している。端末装置１２は、ローカルエリアネットワーク１１を介して、他の端末装置１２、ファイルサーバ装置１３、メールサーバ装置１４及びウェブプロキシ装置１５と通信する。

【０００８】

ファイルサーバ装置１３は、電子ファイルを記憶するコンピュータである。ファイルサーバ装置１３は、例えば、端末装置１２などからの要求にしたがって、端末装置１２などから送信された電子ファイルを記憶する。あるいは、ファイルサーバ装置１３は、端末装置１２などからの要求にしたがって、外部のウェブサーバ装置８３などから受信した電子ファイルを記憶する。また、ファイルサーバ装置１３は、端末装置１２などからの要求にしたがって、記憶した電子ファイルを端末装置１２などに対して送信する。ファイルサーバ装置１３は、ローカルエリアネットワーク１１に接続している。ファイルサーバ装置１３は、ローカルエリアネットワーク１１を介して、端末装置１２などと通信する。

【０００９】
メールサーバ装置１４（ＭＴＡ）は、電子メールサービスを提供するコンピュータである。メールサーバ装置１４は、ローカルエリアネットワーク１１と接続している。メールサーバ装置１４は、ローカルエリアネットワーク１１を介して、端末装置１２などと通信する。メールサーバ装置１４は、インターネット８１と接続している。メールサーバ装置１４は、インターネット８１を介して、外部のメールサーバ装置８２などと通信する。
メールサーバ装置１４は、端末装置１２から社外へ向けて送信された電子メールを外部のメールサーバ装置８２などへ転送する。また、メールサーバ装置１４は、端末装置１２に対して、他の端末装置１２や外部のメールサーバ装置８２から送信された電子メールをメールボックスに記憶し、端末装置１２からの要求にしたがって、記憶した電子メールを端末装置１２に対して送信する。
【００１０】
ウェブプロキシ装置１５は、端末装置１２の代理として、外部のウェブサーバ装置８３などと通信するコンピュータである。ウェブプロキシ装置１５は、ローカルエリアネットワーク１１と接続している。ウェブプロキシ装置１５は、ローカルエリアネットワーク１１を介して、端末装置１２などと通信する。ウェブプロキシ装置１５は、インターネット８１と接続している。ウェブプロキシ装置１５は、インターネット８１を介して、外部のウェブサーバ装置８３などと通信する。
ウェブプロキシ装置１５は、端末装置からの要求にしたがって、外部のウェブサーバ装置からウェブページを取得し、端末装置１２に対して送信する。
【００１１】
端末装置１２やファイルサーバ装置１３には、顧客リストなどの秘密情報を含む電子ファイルが記憶されている場合がある。攻撃者は、それを盗み出そうとする。端末装置１２やファイルサーバ装置１３は、インターネット８１に直接接続していないので、外部からアクセスすることはできない。そこで、攻撃者は、端末装置１２やファイルサーバ装置１３をコンピュータウィルスに感染させ、コンピュータウィルスに秘密情報を盗ませる。
【００１２】
第一段階として、攻撃者は、攻撃者装置８４やメールサーバ装置８２などから電子メールを送りつける。この電子メールには、コンピュータウィルスを仕込んだ電子ファイルが添付されている。この添付ファイルを利用者が開かなければ、端末装置１２は、コンピュータウィルスに感染しない。あるいは、この電子メールには、端末装置１２をコンピュータウィルスに感染させるウェブサイトへのリンクが埋め込んである。このため、攻撃者が送る電子メールには、利用者が信用してついうっかり添付ファイルやリンクを開くような仕掛けが施してある。例えば、電子メールの作成者を詐称して、利用者の知り合いや他の社員から送られてきた電子メールであると、利用者に思わせる。電子メールの内容も、通常の業務連絡であるかのような内容である。利用者がこれに騙されて添付ファイルを開くと、端末装置１２は、コンピュータウィルスに感染する。
【００１３】
第二段階として、コンピュータウィルスは、ローカルネットワークシステム１０の構造、端末装置１２やファイルサーバ装置１３にどのような電子ファイルが記憶されているかを調査する。コンピュータウィルスは、攻撃者装置８４に対して調査結果を送信する。攻撃者は、この調査結果を見て、コンピュータウィルスに対して指示を出す。コンピュータウィルスに対する指示は、例えば攻撃者装置８４が、コンピュータウィルスに感染している端末装置１２などに対して送信する。
コンピュータウィルスと攻撃者との間の通信は、例えば、端末装置１２がウェブページを閲覧するときに用いるハイパーテキスト転送プロトコル（ＨＴＴＰ）におけるリクエストとそれに対するレスポンスの形式をとる。ウェブプロキシ装置１５がこれに騙されて通信を中継すると、攻撃者は、コンピュータウィルスによる調査結果に基づいて、徐々に秘密情報に肉薄していく。
【００１４】

最終段階として、秘密情報を含む電子ファイルが特定されると、攻撃者は、コンピュータウィルスに対して、その秘密情報の送信を指示する。コンピュータウィルスは、指示にしたがって、その電子ファイルを取得し、そこに含まれる秘密情報を送信する。これにより、秘密情報が漏洩する。

【００１５】

「標的型サイバー攻撃」が、従来のサイバー攻撃と異なるのは、秘密情報を盗み出す企業や、その企業から盗み出す秘密情報などを、標的として特定している点である。

【００１６】

従来の迷惑メール検出方式には、迷惑メールによく含まれている単語などを検出する方式がある。しかし、標的型サイバー攻撃の第一段階における電子メールは、なるべく怪しまれないような内容であるため、そのような単語などを含まない。このため、従来の方式では、標的型サイバー攻撃の第一段階における電子メールを検出できない。

【００１７】

また、従来のコンピュータウィルス検出方式には、既に発見されているコンピュータウィルスを登録しておき、電子メールにそれと類似するデータが添付されていることを検出する方式がある。しかし、標的型サイバー攻撃のコンピュータウィルスは、その「標的」用に作られた特別なものであり、広く出回るものではない。このため、従来の方式では、標的型サイバー攻撃の第一段階における電子メールに仕込まれたコンピュータウィルスを検出できない。

【００１８】

また、従来のコンピュータウィルス検出方式には、コンピュータウィルスによくある活動パターンを検出する方式がある。しかし、標的型サイバー攻撃のコンピュータウィルスは、単なる破壊活動や、見つけた電子ファイルを手当たり次第に送信するなどといった派手な活動はしない。このため、従来の方式では、感染を検出できない。

【００１９】

この発明は、例えば、不正通信を検出して警告することにより、仮に、端末装置がコンピュータウィルスに感染した場合でも、コンピュータウィルスを早期に発見することにより、標的型サイバー攻撃による秘密情報の漏洩を防ぐことを目的とする。

【課題を解決するための手段】

【００２０】

本発明に係る不正通信検出装置は、

ネットワークを介した通信を取得する通信取得部と、

上記通信取得部が取得した通信を解析して、上記通信の特性値を算出する特性値算出部と、

１以上の通信について上記特性値算出部が算出した特性値に基づいて統計量を算出する統計量算出部と、

上記統計量算出部が算出した統計量に基づいて、上記特性値算出部が算出した特性値が異常値であるか否かを判定し、上記特性値が異常値であると判定した場合に、不正通信の可能性があると判定する不正判定部と

を有することを特徴とする。

【００２１】

上記通信取得部は、上記通信として、ハイパーテキスト転送プロトコルにおけるリクエストを取得し、

上記特性値算出部は、上記通信取得部が取得した通信に基づいて、上記特性値として、統一資源識別子の長さと、上記統一資源識別子のうち絶対パス文字列の長さと、上記統一資源識別子のうちクエリー文字列の長さと、上記リクエスト全体の長さとのうち、少なくともいずれかを算出する

ことを特徴とする。

【００２２】

上記統計量算出部は、上記統計量として、上記１以上の通信についての上記特性値を平

均した平均値及び標準偏差を算出し、
上記不正判定部は、上記標準偏差に所定の定数を乗じた値を上記平均値に加えた値よりも上記特性値が大きい場合と、上記標準偏差に所定の定数を乗じた値を上記平均値から差し引いた値よりも上記特性値が小さい場合とのうち、少なくともいずれかの場合に、上記特性値が異常値であると判定することを特徴とする。
【００２３】
上記通信取得部は、上記通信として、ハイパーテキスト転送プロトコルにおけるリクエストを取得し、
上記統計量算出部は、上記統計量として、上記１以上の通信のうち、ゲットメソッドである通信についての上記特性値を平均した平均値及び標準偏差と、ポストメソッドである通信についての上記特性値を平均した平均値及び標準偏差と、ポストメソッド以外のメソッドである通信についての上記特性値を平均した平均値及び標準偏差とのうち、少なくともいずれかの平均値及び標準偏差を算出することを特徴とする。
【００２４】
宛先が同じ複数の通信について上記特性値算出部が算出した特性値を平均した宛先別平均値を算出する宛先別平均値算出部を有し、
上記不正判定部は、上記統計量算出部が算出した統計量に基づいて、上記宛先別平均値算出部が算出した宛先別平均値が異常値であるか否かを判定し、上記宛先別平均値が異常値であると判定した場合に、不正通信の可能性があると判定することを特徴とする。
【００２５】
上記統計量算出部は、上記宛先別平均値算出部が算出した宛先別平均値に基づいて、上記統計量を算出することを特徴とする。
【００２６】
所定の期間内に上記通信取得部が取得した通信の通信数を、上記通信の宛先ごとに計数する通信計数部を有し、
上記不正判定部は、いずれかの宛先について上記通信計数部が計数した通信数が１である場合に、不正通信の可能性があると判定することを特徴とする。
【００２７】
所定の期間内に上記通信取得部が取得した通信の数を、上記通信の宛先ごとに計数する通信計数部と、
複数の期間について上記通信計数部が計数した通信数の統計量を、上記宛先ごとに算出する通信数統計量算出部とを有し、
上記不正判定部は、上記通信数統計量算出部が算出した統計量が所定の閾値より小さい場合に、不正通信の可能性があると判定することを特徴とする。
【００２８】
上記通信取得部は、上記通信として、ハイパーテキスト転送プロトコルにおけるリクエストを取得し、
上記不正判定部は、上記通信取得部が取得した通信がポストメソッドである場合と、上記通信のフォーマットがハイパーテキスト転送プロトコルの規定に合致しない場合と、上記通信のユーザエージェントが所定のリストに含まれるユーザエージェントでない場合とのうち、少なくともいずれかの場合に、不正通信の可能性があると判定することを特徴とする。
【００２９】
上記不正判定部は、上記通信取得部が取得した通信の宛先が所定のリストに含まれる宛先である場合に、不正通信の可能性があると判定することを特徴とする。
【００３０】
本発明に係るサイバー攻撃検出システムは、
不正通信検出装置と、
上記ネットワークを介した通信によって転送される電子メールのうちから、作成者を詐称した詐称メールを検出する詐称メール検出装置と

を有することを特徴とする。
【００３１】
本発明に係るコンピュータプログラムは、
コンピュータが実行することにより、上記コンピュータを不正通信検出装置として機能させることを特徴とする。
【００３２】
本発明に係る不正通信検出方法は、
ネットワークを介した通信を取得し、
取得した通信を解析して、上記通信の特性値を算出し、
１以上の通信について算出した特性値に基づいて、統計量を算出し、
算出した統計量に基づいて、上記特性値が異常値であるか否かを判定し、
上記特性値が異常値であると判定した場合に、不正通信の可能性があると判定することを特徴とする。
【発明の効果】
【００３３】
本発明に係る不正通信検出装置は、ネットワークを介した通信を取得する通信取得部と、上記通信取得部が取得した通信を解析して、上記通信の特性値を算出する特性値算出部と、１以上の通信について上記特性値算出部が算出した特性値に基づいて統計量を算出する統計量算出部と、上記統計量算出部が算出した統計量に基づいて、上記特性値算出部が算出した特性値が異常値であるか否かを判定し、上記特性値が異常値であると判定した場合に、不正通信の可能性があると判定する不正判定部とを有するので、通信の特性値に基づいて不正通信を検出することができ、標的型サイバー攻撃による秘密情報の漏洩を防ぐことができる。
【図面の簡単な説明】
【００３４】
【図１】標的型サイバー攻撃を説明するための図。
【図２】実施の形態１におけるサイバー攻撃検出システム１６の構成の一例を示す図。
【図３】実施の形態１におけるコンピュータ９０のハードウェア資源の一例を示す図。
【図４】実施の形態１における詐称メール検出装置２０の機能ブロックの一例を示す図。
【図５】実施の形態１における詐称判定部２８の詳細な機能ブロックの一例を示す図。
【図６】実施の形態２においてメール通信取得部２１が取得する電子メール２４０の一例を示す図。
【図７】実施の形態２に係る内部ドメイン検査部２４の詳細な機能ブロックの一例を示す図。
【図８】実施の形態２に係るドメイン別メール数一覧２４２１の構成を示す図。
【図９】実施の形態２に係る内部ドメイン検査部２４の内部ドメイン検査方法を示すフローチャート。
【図１０】実施の形態２に係る内部作成計数部２４２による除外ドメイン学習処理を示すフローチャート。
【図１１】実施の形態３における外国経由検査部２５の構成図。
【図１２】実施の形態３における国内信頼ドメイン学習処理を示すフローチャート。
【図１３】実施の形態３における国内信頼ドメイン学習処理を示すフローチャート。
【図１４】実施の形態３における外国経由検査方法を示すフローチャート。
【図１５】実施の形態３における電子メールのメールヘッダの一例を示す概要図。
【図１６】実施の形態３における外国経由検査スコア一覧表２５９Ａの一例を示す図。
【図１７】実施の形態４におけるパケット連続度検査部２６の構成図。
【図１８】実施の形態４における統計量算出処理を示すフローチャート。
【図１９】実施の形態４における電子メールのパケット連続度の一例を示す図。
【図２０】実施の形態４における電子メールのパケット連続度の一例を示す図。
【図２１】実施の形態４における統計量一覧表２６２Ａの一例を示す図。

【図２２】実施の形態４における統計量一覧表２６２Ａの一例を示す図。
【図２３】実施の形態４におけるパケット連続度検査方法を示すフローチャート。
【図２４】実施の形態４におけるパケット連続度検査スコア一覧表２６９Ａの一例を示す図。
【図２５】実施の形態５における転送経路検査部２７の構成図。
【図２６】実施の形態５におけるドメイン経路学習処理を示すフローチャート。
【図２７】実施の形態５における電子メールのメールヘッダの一例を示す概要図。
【図２８】実施の形態５における転送経路データ２７１Ａの一例を示す図。
【図２９】実施の形態５におけるドメイン経路リスト２７２Ａの一例を示す図。
【図３０】実施の形態５における転送経路検査方法を示すフローチャート。
【図３１】実施の形態５における転送経路検査スコア一覧表２７９Ａの一例を示す図。
【図３２】実施の形態６に係る不正通信検出装置３０のブロック構成図。
【図３３】実施の形態６におけるＨＴＴＰリクエスト３１０の一例を示す図。
【図３４】実施の形態６に係る不正通信検出装置３０の不正通信検出方法を示すフローチャートチャート。
【図３５】実施の形態６に係る分析結果テーブル３７ａの構成の一例を示す図。
【図３６】実施の形態６に係る不正通信検出装置３０の特性値分析方法を示すフローチャート。
【図３７】実施の形態６に係る不正通信検出装置３０の通信数分析方法を示すフローチャート。
【図３８】実施の形態６に係る通信数蓄積部３５ａ及び通信数統計量記憶部３６ａの構成の一例を示す図。
【図３９】実施の形態６に係る不正通信検出装置３０の通信種別分析方法を示すフローチャート。
【図４０】実施の形態６に係るレポート作成処理により作成されたレポート３８０の一例を示す図。
【図４１】実施の形態７に係る不正通信検出装置３０ａのブロック構成図。
【図４２】実施の形態８に係るレポート作成処理により作成されたレポート３８０ａの一例を示す図。

【発明を実施するための形態】

【００３５】

実施の形態１.

実施の形態１について、図２～図５を用いて説明する。

【００３６】

図２は、この実施の形態におけるサイバー攻撃検出システム１６の構成の一例を示す図である。

【００３７】

サイバー攻撃検出システム１６は、標的型サイバー攻撃を検出する。サイバー攻撃検出システム１６は、例えば、上記説明したローカルネットワークシステム１０のなかに設置される。サイバー攻撃検出システム１６は、例えば、詐称メール検出装置２０と、不正通信検出装置３０とを有する。

【００３８】

詐称メール検出装置２０は、詐称メールを検出する。詐称メールとは、作成者を詐称した電子メールのことである。詐称メール検出装置２０は、例えば、メールサーバ装置１４がインターネット８１を介して受信する電子メールのなかから、詐称メールを検出する。

詐称メールを検出した場合、詐称メール検出装置２０は、その電子メールの受信者である端末装置１２の利用者や、ローカルネットワークシステム１０の管理者などに対して、警告する。これにより、利用者が添付ファイルを開いて端末装置１２がコンピュータウィルスに感染するのを防ぐ。また、端末装置１２がコンピュータウィルスに感染してしまったとしても、管理者が迅速な対応をすることを可能にする。

【００３９】
不正通信検出装置３０は、不正な通信を検出する。不正通信検出装置３０は、例えば、端末装置１２などがウェブプロキシ装置１５とインターネット８１とを介して行う通信のなかから、不正な通信を検出する。不正通信検出装置３０は、例えば、端末装置１２などとウェブプロキシ装置１５との間の通信を取得して検出の対象とする。これは、ウェブプロキシ装置１５が不正な通信であると判定して遮断する通信も検出の対象に含めるためである。なお、不正通信検出装置３０は、端末装置１２などの代理としてウェブプロキシ装置１５がインターネット８１を介して行う通信を取得して検出の対象とする構成であってもよい。また、端末装置１２がウェブプロキシ装置１５を介さずに直接インターネット８１を介して通信をする場合には、不正通信検出装置３０は、端末装置１２がインターネットを介して行う通信を取得して検出の対象とする。
不正な通信を検出した場合、不正通信検出装置３０は、ローカルネットワークシステム１０の管理者などに対して、警告する。これにより、管理者が迅速な対応をすることができるので、標的型サイバー攻撃のコンピュータウィルスを発見し、秘密情報の漏洩を防ぐことができる。
【００４０】
このように、標的型サイバー攻撃の第一段階におけるコンピュータウィルス感染を防ぐとともに、万一コンピュータウィルスに感染してしまっても、第二段階における不正な通信を検出することにより、第三段階まで進むのを防ぐ。これにより、標的型サイバー攻撃による秘密情報の漏洩を防ぐことができる。
【００４１】
図３は、この実施の形態におけるコンピュータ９０のハードウェア資源の一例を示す図である。
【００４２】
詐称メール検出装置２０や不正通信検出装置３０は、例えば、コンピュータ９０を用いて構成される。コンピュータ９０は、例えば、制御装置９１と、入力装置９２と、出力装置９３と、記憶装置９４と、演算装置９５とを有する。
【００４３】
制御装置９１は、記憶装置９４が記憶したコンピュータプログラムを実行することにより、コンピュータ９０全体を制御する。
記憶装置９４は、制御装置９１が実行するコンピュータプログラムや、演算装置９５が演算に用いるデジタルデータなどを記憶する。記憶装置９４は、例えば、揮発性メモリや不揮発性メモリなどの内部記憶装置、磁気ディスク装置や光学ディスク装置などの外部記憶装置である。
演算装置９５は、記憶装置９４が記憶したデジタルデータなどを用いて、算術演算や論理演算などの演算をする。演算装置９５は、演算の結果を表わすデジタルデータを生成する。演算装置９５が生成したデジタルデータは、例えば、記憶装置９４が記憶する。
入力装置９２は、コンピュータ９０の外部から情報を入力し、デジタルデータに変換する。入力装置９２が変換したデジタルデータは、例えば、記憶装置９４が記憶する。入力装置９２は、例えば、キーボードやマウスなどの操作入力装置、カメラやスキャナなどの画像入力装置、マイクなどの音声入力装置、温度や電圧などの物理量を測定する測定装置、他の装置が送信した信号を受信する受信装置である。
出力装置９３は、記憶装置９４が記憶したデジタルデータなどを、コンピュータ９０の外部へ出力できる形式に変換して出力する。出力装置９３は、例えば、文字や画像を表示する表示装置、文字や画像を印刷する印刷装置、スピーカなどの音声出力装置、他の装置に対して信号を送信する送信装置である。
【００４４】
以下に説明する詐称メール検出装置２０や不正通信検出装置３０の機能ブロックは、例えば、記憶装置９４が記憶したコンピュータプログラムを制御装置９１が実行することにより、実現することができる。なお、これらの機能ブロックは、コンピュータ９０以外の

装置により実現されるものであってもよい。また、詐称メール検出装置２０や不正通信検出装置３０は、１つのコンピュータ９０を用いて構成されるものであってよいし、複数のコンピュータ９０を用いて構成されるものであってもよい。また、１つのコンピュータ９０が、詐称メール検出装置２０を構成するとともに、不正通信検出装置３０を構成するものであってもよい。

【００４５】

図４は、この実施の形態における詐称メール検出装置２０の機能ブロックの一例を示す図である。

【００４６】

詐称メール検出装置２０は、例えば、メール通信取得部２１と、メール通信記憶部２２と、作成者ドメイン取得部２３と、内部ドメイン検査部２４と、外国経由検査部２５と、パケット連続度検査部２６と、転送経路検査部２７と、詐称判定部２８と、詐称警告部２９とを有する。

【００４７】

メール通信取得部２１は、入力装置９２を用いて、メールサーバ装置１４がインターネット８１を介して送受信する通信を取得する。メール通信取得部２１は、メールサーバ装置１４による通信のうち、メールの転送にかかる通信だけを取得する。

【００４８】

例えば、メール通信取得部２１は、メールサーバ装置１４が送受信するＩＰ（インターネットプロトコル）パケットをキャプチャする。ＩＰパケットのヘッダ部分には、バージョン、ヘッダ長、サービスタイプ、全長、識別子、フラグ、断片位置、生存時間、プロトコル、チェックサム、送信元アドレス、宛先アドレス、オプションなどの情報が格納されている。

メール通信取得部２１は、キャプチャしたＩＰパケットを解析して、トランスポート層のプロトコルにおけるメッセージを再構成する。トランスポート層のプロトコルには、例えばＴＣＰ（伝送制御プロトコル）やＵＤＰ（ユーザデータグラムプロトコル）などがある。

メール通信取得部２１は、再構成したトランスポート層におけるメッセージを解析して、アプリケーション層のプロトコルにおけるメッセージを再構成する。アプリケーション層のプロトコルには、例えばＨＴＴＰ（ハイパーテキスト転送プロトコル）やＳＭＴＰ（シンプルメール転送プロトコル）などがある。

メール通信取得部２１は、再構成したアプリケーション層におけるメッセージを解析して、ＳＭＴＰにかかるメッセージだけを抽出する。メール通信取得部２１は、抽出したメッセージのうちから、更に、メールサーバ装置１４がＳＭＴＰサーバ（電子メールを受信する側）であるメッセージだけを抽出する。

メール通信取得部２１は、抽出したメッセージを出力する。

【００４９】

また、メール通信取得部２１は、キャプチャしたＩＰパケットのうち、抽出したメッセージにかかるＩＰパケットだけを抽出する。メール通信取得部２１は、抽出したＩＰパケットに関する情報を出力する。メール通信取得部２１が出力する情報には、例えば、そのＩＰパケットをキャプチャした日時、そのＩＰパケットの送信元のＩＰアドレス、そのＩＰパケットの送受信方向などが含まれる。ＩＰパケットの送受信方向は、そのＩＰパケットをメールサーバ装置１４がインターネット８１から受信したのか、それとも、そのＩＰパケットをメールサーバ装置１４がインターネット８１へ送信したのかを表わす。

【００５０】

メール通信記憶部２２は、記憶装置９４を用いて、メール通信取得部２１が取得した通信に関する情報を記憶する。メール通信記憶部２２が記憶する情報には、例えば、電子メールのメールヘッダに記載された情報、ＳＭＴＰコマンドのパラメータなどの情報、ＩＰパケットに関する情報などが含まれる。これらの情報には、メール通信取得部２１が出力した情報のほか、メール通信取得部２１が出力したメッセージなどから、作成者ドメイン

取得部２３、内部ドメイン検査部２４、外国経由検査部２５、パケット連続度検査部２６、または、転送経路検査部２７が、取得し、算出し、あるいは、生成した情報も含まれる。

【００５１】

作成者ドメイン取得部２３は、演算装置９５を用いて、メール通信取得部２１が取得した通信によって転送される電子メールの作成者ドメインを取得する。作成者ドメインとは、電子メールに記載された作成者のメールアドレスが所属するドメインのことである。

【００５２】

例えば、作成者ドメイン取得部２３は、メール通信取得部２１が出力したメッセージを解析して、メールサーバ装置１４が受信した電子メールのメールヘッダを取得する。

作成者ドメイン取得部２３は、取得したメールヘッダの「Ｆｒｏｍ」フィールドに記載されたメールアドレスを取得する。

作成者ドメイン取得部２３は、取得したメールアドレスのうち、「@」より後ろの部分の文字列を、作成者ドメインとして取得する。

作成者ドメイン取得部２３は、取得した作成者ドメインを出力する。

【００５３】

内部ドメイン検査部２４は、演算装置９５を用いて、メールサーバ装置１４が受信した電子メールが詐称メールである可能性を検査する。以下、その時点で検査の対象である電子メールを「判定対象メール」と呼ぶ。内部ドメイン検査部２４は、次の観点から、詐称メールの可能性を検査する。

【００５４】

ローカルネットワークシステム１０のなかで作成された電子メールは、ローカルネットワークシステム１０のなかの端末装置１２から送信される。したがって、メールサーバ装置１４がローカルエリアネットワーク１１を介して受信することはあっても、インターネット８１を介して受信することはないはずである。

【００５５】

ローカルネットワークシステム１０のなかの端末装置１２に割り当てられたメールアドレスが所属するドメインを「内部ドメイン」と呼ぶ。

作成者ドメイン取得部２３が取得した作成者ドメインが内部ドメインである場合、判定対象メールが詐称メールである可能性がある。ただし、例外的に、作成者ドメインが内部ドメインである電子メールが外部から届く場合もある。

【００５６】

このような観点に基づいて、内部ドメイン検査部２４は、詐称メールの可能性を検査する。内部ドメイン検査部２４は、検査した結果を出力する。

【００５７】

外国経由検査部２５は、演算装置９５を用いて、判定対象メールが詐称メールである可能性を検査する。外国経由検査部２５は、内部ドメイン検査部２４とは異なる観点から、詐称メールの可能性を検査する。

【００５８】

ローカルネットワークシステム１０が存在する国のなかで作成された電子メールは、同じ国のなかだけを経由して届けることができる。したがって、その電子メールが他の国を経由して届けられることはないはずである。

【００５９】

メール通信取得部２１が取得した通信にかかる電子メールの宛先であるメールアドレスが所属するドメインを「宛先ドメイン」と呼ぶ。メール通信取得部２１が取得する通信は、メールサーバ装置１４が受信した電子メールにかかる通信であるから、宛先ドメインは、内部ドメインと同じである。また、宛先ドメインが属する国を「宛先国」と呼ぶ。

作成者ドメイン取得部２３が取得した作成者ドメインが属する国が宛先国と同じであるにもかかわらず、その電子メールが他の国を経由している場合、判定対象メールが詐称メールである可能性がある。ただし、例外的に、他の国を経由して届く場合もある。

【００６０】
このような観点に基づいて、外国経由検査部２５は、詐称メールの可能性を検査する。外国経由検査部２５は、検査した結果を出力する。
【００６１】
パケット連続度検査部２６は、演算装置９５を用いて、判定対象メールが詐称メールである可能性を検査する。パケット連続度検査部２６は、内部ドメイン検査部２４や外国経由検査部２５とは異なる観点から、詐称メールの可能性を検査する。
【００６２】
ＴＣＰなどのプロトコルでは、基本的に、データパケットを送信し、それに対する受信確認（ＡＣＫ）を受信してから、次のデータパケットを送信する。このため、ＩＰパケットの送受信方向は、「送信」「受信」「送信」「受信」…と交互に変化する。
ただし、送信側の装置と受信側の装置との間の距離が離れている場合など、データパケットが相手側に到達するまでに時間がかかる場合は、ＡＣＫを受信するまで次のデータパケットを送信しないと、通信速度が低くなる。これを避けるため、ＡＣＫを受信するのを待たずに、次のデータパケットを送信する。例えば、ＡＣＫを待たずに送信するデータパケットの数の上限をあらかじめ定めておき、その数に達するまでは、ＡＣＫを受信しなくても、データパケットを連続して送信する。このため、ＩＰパケットの送受信方向は、規則正しく「送信」「受信」を繰り返すのではなく、「送信」が連続したり、「受信」が連続したりする。
【００６３】
一連のＩＰパケットにおいて、「送信」や「受信」が連続している割合を「パケット連続度」と呼ぶ。
【００６４】
一般に、ＡＣＫを待たずに送信するデータパケットの数の上限は、送信側の装置が、通信の状況などに基づいて、自動的に最適な値を設定する。
このため、パケット連続度は、送信側の装置と受信側の装置との間の距離など、利用者が任意に設定することのできない要因によって、ある程度定まる。
【００６５】
そこで、作成者ドメインごとに、パケット連続度の統計を取っておく。判定対象メールと同じ作成者ドメインについて取った統計と比較して、判定対象メールのパケット連続度が異常値である場合、判定対象メールが詐称メールである可能性がある。
【００６６】
このような観点に基づいて、パケット連続度検査部２６は、詐称メールの可能性を検査する。パケット連続度検査部２６は、検査した結果を出力する。
【００６７】
転送経路検査部２７は、演算装置９５を用いて、判定対象メールが詐称メールである可能性を検査する。転送経路検査部２７は、内部ドメイン検査部２４や外国経由検査部２５やパケット連続度検査部２６とは異なる観点から、詐称メールの可能性を検査する。
【００６８】
電子メールは、送信者の装置から受信者のメールボックスがあるメールサーバ装置へ直接送られる場合もあるが、いくつかのメールサーバ装置が中継する場合もある。このように、電子メールが送られる経路を「転送経路」と呼ぶ。電子メールの転送経路は、ネットワークの構造や、ドメイン名称サーバ（ＤＮＳ）装置の設定などによって定まる。ただし、ネットワークの混雑やサーバ装置のダウンなどにより、迂回経路をとる場合もある。
【００６９】
そこで、作成者ドメインごとに、転送経路を記録しておく。判定対象メールと同じ作成者ドメインについて記録した転送経路と比較して、判定対象メールの転送経路が異なる場合、判定対象メールが詐称メールである可能性がある。
【００７０】
このような観点に基づいて、転送経路検査部２７は、詐称メールの可能性を検査する。

転送経路検査部２７は、検査した結果を出力する。

【００７１】

詐称判定部２８は、演算装置９５を用いて、判定対象メールが詐称メールである可能性があるか否かを判定する。例えば、詐称判定部２８は、内部ドメイン検査部２４による検査結果と、外国経由検査部２５による検査結果と、パケット連続度検査部２６による検査結果と、転送経路検査部２７による検査結果とを総合して、詐称メールの可能性を判定する。詐称判定部２８は、判定した結果を出力する。

【００７２】

詐称警告部２９は、判定対象メールが詐称メールである可能性があると詐称判定部２８が判定した場合、出力装置９３を用いて、判定対象メールが詐称メールである可能性があることを警告する。

例えば、詐称警告部２９は、メールサーバ装置１４に対して、判定対象メールを破棄するよう指示する。しかし、判定対象メールが詐称メールではない可能性もあるので、詐称警告部２９は、判定対象メールの宛先である利用者宛の電子メールを、判定対象メールの代わりに生成する。詐称警告部２９が生成する電子メールは、例えば、判定対象メールが詐称メールである可能性がある旨の警告文を、判定対象メールの情報に付加したものである。

また、例えば、詐称警告部２９は、詐称メールの可能性があると詐称判定部２８が判定した判定対象メールに関する情報をログに記録する。詐称警告部２９は、例えば、月に一度など定期的に、あるいは、管理者からの要求に基づいて不定期に、記録したログの内容をレポートとして出力する。

【００７３】

なお、詐称警告部２９は、判定対象メールに添付ファイルまたはリンク（添付ＵＲＬ）が含まれるか否かを判定し、添付ファイルまたはリンクが含まれる場合のみ、警告をする構成であってもよい。

上述したように、標的型サイバー攻撃の第一段階で送付される電子メールは、端末装置１２をコンピュータウィルスに感染させることを目的としている。詐称警告部２９が警告をするのは、利用者が添付ファイルやリンクを開いて端末装置１２がコンピュータウィルスに感染するのを防ぐためである。したがって、たとえ詐称メールであっても、添付ファイルやリンクが含まれていなければ、警告をする必要はない。

【００７４】

ただし、内部ドメイン検査部２４、外国経由検査部２５、パケット連続度検査部２６及び転送経路検査部２７は、添付ファイルが含まれていない電子メールであっても、メール通信取得部２１が取得した通信にかかるすべての電子メールを、判定対象メールとして検査することが望ましい。これは、詐称メールを見つけるためではなく、詐称メールでない電子メールの傾向を学習するためである。

【００７５】

図５は、この実施の形態における詐称判定部２８の詳細な機能ブロックの一例を示す図である。

【００７６】

詐称判定部２８は、例えば、詐称評価値算出部２８１と、詐称評価閾値記憶部２８２と、詐称評価値判定部２８３とを有する。

【００７７】

詐称評価値算出部２８１は、演算装置９５を用いて、内部ドメイン検査部２４による検査結果と、外国経由検査部２５による検査結果と、パケット連続度検査部２６による検査結果と、転送経路検査部２７による検査結果とに基づいて、詐称評価値を算出する。詐称評価値は、例えば０以上の整数である。詐称評価値は、数値が大きいほど、判定対象メールが詐称メールである可能性が高いことを表わす。

例えば、内部ドメイン検査部２４、外国経由検査部２５、パケット連続度検査部２６及び転送経路検査部２７は、検査結果を表わすスコアを出力する。スコアは、例えば、０以

上４以下の整数である。スコアは、数値が大きいほど、詐称メールである可能性が高いことを表わす。

詐称評価値算出部２８１は、内部ドメイン検査部２４、外国経由検査部２５、パケット連続度検査部２６及び転送経路検査部２７が出力したスコアを入力する。詐称評価値算出部２８１は、入力したスコアを合計した値を算出して、詐称評価値とする。

【００７８】

詐称評価閾値記憶部２８２は、記憶装置９４を用いて、あらかじめ設定された詐称評価閾値を記憶している。詐称評価閾値は、詐称評価値判定部２８３が詐称メールの可能性を判定する基準となる閾値である。詐称評価閾値は、例えば３である。

【００７９】

詐称評価値判定部２８３は、演算装置９５を用いて、詐称評価値算出部２８１が算出した詐称評価値と、詐称評価閾値記憶部２８２が記憶した詐称評価閾値とに基づいて、判定対象メールが詐称メールである可能性があるか否かを判定する。詐称評価値判定部２８３は、詐称評価値が詐称評価閾値より大きい場合に、判定対象メールが詐称メールである可能性があると判定する。

【００８０】

内部ドメイン検査部２４、外国経由検査部２５、パケット連続度検査部２６及び転送経路検査部２７が出力したスコアが、詐称評価閾値より大きい場合、他の観点からの検査結果にかかわらず、詐称評価値判定部２８３は、判定対象メールが詐称メールである可能性があると判定する。

内部ドメイン検査部２４、外国経由検査部２５、パケット連続度検査部２６及び転送経路検査部２７が出力したスコアが、０より大きく、かつ、詐称評価閾値以下である場合、詐称評価値判定部２８３は、その観点単独では、判定対象メールが詐称メールである可能性があると判定しない。しかし、他の観点と総合した結果、詐称評価値が詐称評価閾値より大きくなれば、詐称評価値判定部２８３は、判定対象メールが詐称メールである可能性があると判定する。

【００８１】

このように、複数の観点からの検査結果を総合して、判定対象メールが詐称メールである可能性があるか否かを判定することにより、より的確な判定をすることができる。

【００８２】

なお、詐称メール検出装置２０は、上述した４つの観点のすべてについて検査する必要はない。詐称メール検出装置２０は、４つの観点のうちの１つ、２つ、あるいは３つの観点について検査を行い、その結果を総合して、判定対象メールが詐称メールである可能性があるか否かを判定する構成であってもよい。しかし、検査する観点が多いほうが的確な判定ができるので望ましい。

【００８３】

また、上述した４つの観点に限らず、他の観点に基づく検査を行い、その結果も総合して、判定対象メールが詐称メールであるか否かを判定する構成であってもよい。そうすれば、更に的確な判定をすることができる。

【００８４】

例えば、詐称メール検出装置２０は、更に、送信者ポリシフレームワーク（ＳＰＦ）検査部を有する構成であってもよい。ＳＰＦ検査部は、例えば、ＳＭＴＰにおける「ＭＡＩＬ」コマンドのパラメータ「ＦＲＯＭ：」（「ＭＡＩＬ　ＦＲＯＭ：」）から、判定対象メールの送信者のメールアドレスを取得する。ＳＰＦ検査部は、取得したメールアドレスから、そのメールアドレスが所属するドメインを取得する。また、ＳＰＦ検査部は、判定対象メールの送信元のＩＰアドレスを取得する。ＳＰＦ検査部は、取得したドメインのＤＮＳ装置に対して、取得した送信元のＩＰアドレスにそのドメインを使う権限があるか否かを問い合わせる。ＳＰＦ検査部は、問い合わせの結果に基づいて、判定対象メールが詐称メールである可能性を検査する。例えば、問い合わせの結果が「Ｎｏｎｅ」または「Ｐａｓｓ」であれば、ＳＰＦ検査部は、スコア「０」を出力する。問い合わせの結果が「Ｎ

ｅｕｔｒａｌ」であれば、ＳＰＦ検査部は、スコア「２」を出力する。問い合わせの結果が「ＳｏｆｔＦａｉｌ」または「Ｆａｉｌ」であれば、ＳＰＦ検査部は、スコア「４」を出力する。

【００８５】

このように、更にＳＰＦ検査を組み合わせることにより、更に的確な判定をすることができる。

【００８６】

メール通信記憶部２２は、所定の期間内に転送された電子メールにかかる通信に関する情報だけを記憶する構成であってもよい。例えば、メール通信記憶部２２は、記憶している情報のうち、メール通信取得部２１がその通信を取得した時刻から所定の期間（例えば１年）経過した情報を消去する。これにより、メール通信記憶部２２が使用する記憶装置９４の記憶容量を減らすことができる。

【００８７】

また、メール通信記憶部２２は、所定の数の電子メールにかかる通信に関する情報だけを記憶する構成であってもよい。例えば、メール通信記憶部２２は、メール通信取得部２１が新しい電子メールにかかる通信を取得した際、情報を記憶している電子メールの数が所定の数（例えば２００万通）に達している場合、古い電子メール１通にかかる情報を消去する。これにより、メール通信記憶部２２が使用する記憶装置９４の記憶容量を減らすことができる。

なお、情報を消去する電子メールとして、メール通信記憶部２２は、情報を記憶している電子メールのなかで一番古いものを選択する構成であってもよいし、次のようにして選択する構成であってもよい。

【００８８】

例えば、メール通信記憶部２２は、新しく通信を取得した電子メールと同じ作成者ドメインについて情報を記憶している電子メールの数が所定の数（例えば１万通）に達している場合、新しく通信を取得した電子メールと同じ作成者ドメインについて情報を記憶している電子メールのなかから一番古いものを選択する。新しく通信を取得した電子メールと同じ作成者ドメインについて情報を記憶している電子メールの数が所定の数（例えば１万通）に達していない場合、情報を記憶している電子メールの作成者ドメインのなかから、作成者ドメインを１つ選択し、選択した作成者ドメインについて情報を記憶している電子メールのなかから一番古いものを選択する。

ここで、メール通信記憶部２２は、例えば、選択する作成者ドメインが偏らないようにする。例えば、メール通信記憶部２２は、情報を記憶している電子メールの数が所定の数（例えば１０通）以上ある作成者ドメインのなかで、情報を記憶している電子メールの数が一番多い作成者ドメインを選択する。ただし、メール通信記憶部２２は、選択した作成者ドメインを記憶しておき、次回は、選択したことのない作成者ドメインのなかから、作成者ドメインを選択する。したがって、二回目は、例えば、情報を記憶している電子メールの数が二番目に多い作成者ドメインが選択され、三回目は、例えば、情報を記憶している電子メールの数が三番目に多い作成者ドメインが選択される。情報を記憶している電子メールの数が所定の数（例えば１０通）以上ある作成者ドメインがすべて選択済になった場合、メール通信記憶部２２は、記憶している選択済の作成者ドメインを消去し、再び、情報を記憶している電子メールの数が一番多い作成者ドメインを選択する。これにより、それぞれの作成者ドメインから、情報を消去する電子メールを均等に選択することができる。

【００８９】

このようにして、情報を消去する電子メールを選択することにより、メール通信記憶部２２が情報を記憶している電子メールの作成者ドメインが適度にばらつく。上述したように、パケット連続度検査部２６は、作成者ドメインごとに統計を取り、転送経路検査部２７は、作成者ドメインごとに転送経路を記録するなど、詐称メールの検査には、作成者ドメインが深くかかわる。メール通信記憶部２２が情報を記憶している電子メールの作成者

ドメインが適度にばらついていることにより、詐称メールの検査の精度を高くすることができる。

【００９０】

また、内部ドメイン検査部２４や外国経由検査部２５などは、メール通信取得部が過去に取得した通信についてメール通信記憶部２２が記憶した情報に基づいて、判定対象メールが詐称メールであるか否かを判定する構成であってもよい。

【００９１】

これにより、判定対象メールが詐称メールであるか否かの判定精度を高くすることができる。

【００９２】

しかし、システム導入時には、過去に取得した通信が存在しないので、判定精度を高くすることができない。

そこで、メール通信記憶部２２は、あらかじめダミー通信についての情報を記憶しておく構成であってもよい。

ダミー通信とは、メール通信取得部２１が実際に取得した通信ではない架空の通信のことである。ダミー通信についての情報をメール通信記憶部２２が記憶していることにより、実際には転送されていないが、転送されたことになっている電子メールのことを「ダミーメール」と呼ぶ。例えば、メール通信記憶部２２は、ダミーメールが所定の数存在することを表わすダミー通信についての情報を記憶する。メール通信記憶部２２が記憶した情報によって表わされるダミーメールにかかるＩＰパケットの取得日時は、例えば、サイバー攻撃検出システム１６の稼働開始時（システム導入時）である。

【００９３】

これにより、システム導入当初であっても、判定対象メールが詐称メールであるか否かの判定精度を高くすることができる。

【００９４】

以上のようにして、詐称メール検出装置２０が詐称メールを検出して警告することにより、端末装置１２がコンピュータウィルスに感染するのを防ぐ。これにより、標的型サイバー攻撃による秘密情報の漏洩を防ぐことができる。

【００９５】

また、不正通信検出装置３０が不正通信を検出して警告することにより、仮に、端末装置１２がコンピュータウィルスに感染した場合でも、コンピュータウィルスを早期に発見することができる。これにより、標的型サイバー攻撃による秘密情報の漏洩を防ぐことができる。

【００９６】

以上説明したサイバー攻撃検出システム（１６）は、詐称メール検出装置（２０）と、不正通信検出装置（３０）とを有する。

詐称メール検出装置は、ネットワークを介した通信によって転送される電子メールのうちから、作成者を詐称した詐称メールを検出する。

不正通信検出装置は、ネットワークを介した通信のうちから、不正通信の可能性がある通信を検出する。

【００９７】

これにより、標的型サイバー攻撃による秘密情報の漏洩を防ぐことができる。

【００９８】

実施の形態２.

実施の形態２について、図６～図１０を用いて説明する。

この実施の形態では、実施の形態１で説明した詐称メール検出装置２０のうち、内部ドメイン検査部２４の構成例について、詳しく説明する。

なお、実施の形態１と共通する構成には、同一の符号を付し、説明を省略する場合がある。

【００９９】

図６は、本実施の形態においてメール通信取得部２１が取得する通信の一例を示す図である。図７は、本実施の形態に係る内部ドメイン検査部２４の詳細な機能ブロックの一例を示す図である。

図６及び図７を用いて、本実施の形態に係る内部ドメイン検査部２４の機能構成について説明する。

【０１００】

メール通信取得部２１は、ＳＭＴＰプロトコルによる通信を取得する。図６に示すように、ＳＭＴＰプロトコルによる通信は、ＳＭＴＰプロトコル情報２４０ａから構成される。“ＤＡＴＡ”コマンドの後には、電子メール２４０が設定される。電子メール２４０は、メールヘッダ２４０ｂ、メッセージボディ２４０ｃから構成される。

【０１０１】

ＳＭＴＰプロトコル情報２４０ａには、“ＭＡＩＬ”コマンドの引数に送信者メールアドレス２４９ａが設定されている。送信者メールアドレス２４９ａのうち、「@」より後ろの部分の文字列「ｘｘｙｙｚｚｐｐ．ｏｒ．ｊｐ」は送信者ドメイン２４９ｂである。送信者ドメイン２４９ｂは、送信者メールアドレス２４９ａが所属するドメインのことである。

【０１０２】

電子メール２４０のメールヘッダ２４０ｂには、“Ｆｒｏｍ”フィールドに作成者メールアドレス２４８ａが設定されている。作成者メールアドレス２４８ａのうち、「@」より後ろの部分の文字列「ａａａｂｂｂｃｃ．ｏｒ．ｊｐ」は作成者ドメイン２４８ｂである。作成者ドメイン２４８ｂは、作成者メールアドレス２４８ａが所属するドメインのことである。

電子メール２４０のメッセージボディ２４０ｃには、メッセージテキストが設定される。

【０１０３】

図７に示すように、内部ドメイン検査部２４は、送信者ドメイン取得部２４１、内部作成計数部２４２、内部ドメイン詐称スコア算出部２４３を備える。また、内部ドメイン検査部２４は、ドメイン別メール数一覧２４２１、除外判定値２４２２、計数時間２４２３、対象メール数２４２４、除外ドメイン一覧２４２５を記憶装置９４に記憶する。

【０１０４】

作成者ドメイン取得部２３は、メール通信取得部２１が取得した判定対象メールである電子メール２４０の作成者ドメイン２４８ｂを取得する。

【０１０５】

作成者ドメイン取得部２３は、メール通信取得部２１が出力したメッセージを解析して、メールサーバ装置１４が受信した電子メール２４０のメールヘッダ２４０ｂを取得する。作成者ドメイン取得部２３は、取得したメールヘッダ２４０ｂの「Ｆｒｏｍ」フィールドに記載された作成者メールアドレス２４８ａを取得する。

作成者ドメイン取得部２３は、取得したメールアドレスのうち、「@」より後ろの部分の文字列「ａａａｂｂｂｃｃ．ｏｒ．ｊｐ」を作成者ドメイン２４８ｂとして取得する。

作成者ドメイン取得部２３は、取得した作成者ドメイン２４８ｂを内部ドメイン検査部２４に出力する。

【０１０６】

送信者ドメイン取得部２４１は、作成者ドメイン取得部２３から判定対象メールの作成者ドメイン２４８ｂを入力する。

送信者ドメイン取得部２４１は、対象判定メールの作成者ドメイン２４８ｂが所定の内部ドメイン、すなわち、ローカルネットワークシステム１０により付与された内部ドメインである場合は、メール通信記憶部２２に記憶されている判定対象メールである電子メール２４０の情報から、送信者ドメイン２４９ｂを取得する。

【０１０７】

送信者ドメイン取得部２４１は、対象判定メールの作成者ドメイン２４８ｂが内部ドメ

インである場合、判定対象メールである電子メール２４０を解析して、判定対象メールである電子メール２４０のＳＭＴＰプロトコル情報２４０ａを取得する。送信者ドメイン取得部２４１は、取得したＳＭＴＰプロトコル情報２４０ａの“ＭＡＩＬ”コマンドの引数に記載された送信者メールアドレス２４９ａを取得する。

送信者ドメイン取得部２４１は、取得した送信者メールアドレス２４９ａのうち、「@」より後ろの部分の文字列「ｘｘｙｙｚｚｐｐ．ｏｒ．ｊｐ」を送信者ドメイン２４９ｂとして取得する。

送信者ドメイン取得部２４１は、取得した送信者ドメイン２４９ｂを出力する。

【０１０８】

対象判定メールの作成者ドメイン２４８ｂが内部ドメイン、すなわち、ローカルネットワークシステム１０のなかの端末装置１２に割り当てられたメールアドレスが所属するドメインである場合は、対象判定メールが詐称メールである可能性がある。

これは、通常、内部ドメインのメールアドレスからの電子メールが外部から届くことがないと考えられるからである。

【０１０９】

しかし、送信者（外部のメールサーバ装置８２）が、例えば、大手のメーリングリストサービス業者（以下「大手ＭＬ」と呼ぶ。）などの場合には、受信者のアドレスをメールヘッダの「Ｆｒｏｍ」フィールドに設定して配信する場合がある。メーリングリスト（以下「ＭＬ」と呼ぶ。）は、参加者の誰かが送信したメールを、参加者全員に送信するサービスである。ＭＬでは、送信者のメールアドレスを他の参加者に知られないようにするため、「Ｆｒｏｍ」フィールドを改変して、ＭＬのアドレスや受信者のアドレスにする場合がある。

【０１１０】

このようなドメイン（大手ＭＬ等）から送られてくるメールは、基本的にすべて「Ｆｒｏｍ」フィールドに「受信者メールアドレス」が記載されている。したがって、多数の内部作成メールが送られてくることになる。

これに対して、標的型サイバー攻撃のメールは、基本的に、１通か、多くても数通程度である。したがって、そのドメインから送信された内部作成メールの数で、攻撃メールか否かを判定できる。

【０１１１】

内部ドメイン検査部２４では、判定対象メールの作成者ドメイン２４８ｂが内部ドメインであっても、判定対象メールの送信者ドメイン２４９ｂから過去に所定の閾値以上の電子メール２４０の受信がある場合は、その送信者ドメイン２４９ｂは信頼できるドメイン（以下、除外ドメインという）であると判定する。

【０１１２】

内部ドメイン検査部２４は、判定対象メールの送信者ドメイン２４９ｂが除外ドメインであるか否かを判定するために、過去の判定対象メールの送信者ドメイン２４９ｂからのメールの受信数を所定の閾値と比較する。内部ドメイン検査部２４は、この所定の閾値を除外判定値２４２２として記憶装置９４に予め記憶している。除外判定値２４２２は、例えば、詐称メール検出装置２０のシステム導入時の初期設定の際に設定される。

【０１１３】

内部作成計数部２４２は、判定対象メールと送信者ドメイン２４９ｂが同じ１以上の電子メールのうち、作成者ドメイン２４８ｂが内部ドメインである内部作成メールの数を計数する。内部作成計数部２４２は、メール通信記憶部２２に記憶された電子メールの情報を検索し、送信者ドメイン２４９ｂが判定対象メールの送信者ドメイン２４９ｂと同一であり、かつ、作成者ドメイン２４８ｂが内部ドメインである内部作成メールを計数する。

【０１１４】

図８は、本実施の形態に係るドメイン別メール数一覧２４２１の構成を示す図である。図８に示すように、ドメイン別メール数一覧２４２１には、ドメイン名と、当該ドメイン名について内部作成計数部２４２が計数した内部作成メール数とが対応付けられて記憶さ

れている。
内部作成計数部２４２は、計数した内部作成メール数を、判定対象メールの送信者ドメイン２４９ｂに対応付けてドメイン別メール数一覧２４２１に記憶する。
【０１１５】
また、内部作成計数部２４２は、メール通信記憶部２２に記憶された１以上の電子メールのうち、所定の期間内に転送された内部作成メールの数だけを計数する。この所定の期間は、現時点から過去に計数時間２４２３遡った時点から現時点までの期間のことである。計数時間２４２３は、例えば、１週間、１ヶ月、３ヶ月、半年、１年等、予め記憶装置９４に記憶されている。
【０１１６】
また、内部作成計数部２４２は、転送時刻が新しい順に所定の数以内の電子メールのなかで、判定対象メールと送信者ドメイン２４９ｂが同じ内部作成メールの数を計数する構成としてもよい。内部作成計数部２４２は、この所定の数を対象メール数２４２４として記憶装置９４に記憶する。例えば、内部作成計数部２４２は、転送時刻が新しい順に対象メール数２４２４以内の電子メールのなかで、判定対象メールと送信者ドメイン２４９ｂが同じ内部作成メールの数を計数する。
【０１１７】
内部ドメイン詐称スコア算出部２４３は、判定対象メールについて内部ドメイン詐称スコア２４６を算出する。
内部ドメイン詐称スコア２４６とは、判定対象メールの作成者ドメインが内部ドメインに詐称された詐称メールである度合いを示す値である。
【０１１８】
内部ドメイン詐称スコア算出部２４３は、判定対象メールの作成者ドメイン２４８ｂが内部ドメインでない場合は、詐称メールの可能性が低いことを表わす値（例えば「０」）を、内部ドメイン詐称スコア２４６に設定する。
【０１１９】
内部ドメイン詐称スコア算出部２４３は、判定対象メールの作成者ドメイン２４８ｂが内部ドメインであって、判定対象メールの送信者ドメイン２４９ｂに対応する内部作成メール数が除外判定値２４２２以上である場合は、判定対象メールが詐称メールである可能性が低いことを表わす値（例えば「０」）を、内部ドメイン詐称スコア２４６に設定する。
【０１２０】
内部ドメイン詐称スコア算出部２４３は、判定対象メールの作成者ドメイン２４８ｂが内部ドメインであって、判定対象メールの送信者ドメイン２４９ｂに対応する内部作成メール数が除外判定値２４２２より少ない場合は、判定対象メールは詐称メールの可能性が高いことを表わす値（例えば「４」）を、内部ドメイン詐称スコア２４６に設定する。
【０１２１】
内部ドメイン詐称スコア算出部２４３が設定する内部ドメイン詐称スコア２４６の値は、「０」、「４」に限られず、システム導入時等に適宜設定される値でよい。内部ドメイン詐称スコア算出部２４３は、算出した内部ドメイン詐称スコア２４６を内部ドメイン検査部２４が出力するスコアとして詐称判定部２８に出力する。
【０１２２】
詐称判定部２８は、内部ドメイン検査部２４が出力した内部ドメイン詐称スコア２４６に基づいて、判定対象メールが詐称メールであるか否かを判定する。
【０１２３】
なお、内部作成計数部２４２は、所定の時期に所定の内部作成除外ドメインから送信された内部作成メールが所定の数あるものとして、内部作成メールの数を計数する。内部作成除外ドメインとは、上述した大手ＭＬのように、内部作成メールを送信してくることがあらかじめわかっているため、そのドメインから送信された電子メールが内部作成メールであっても、詐称メールではないと判定してよいドメインのことである。

【０１２４】
内部ドメイン検査部２４は、内部作成除外ドメインの一覧を、除外ドメイン一覧２４２５として記憶装置９４にあらかじめ記憶しておく。
内部ドメイン検査部２４は、システム導入時から計数時間２４２３の期間において、除外ドメイン一覧２４２５のなかに、送信者ドメイン２４９ｂが含まれている場合、計数した内部作成メール数に所定の数を加算する。この所定の数は、例えば、除外判定値２４２２である。
内部ドメイン検査部２４は、所定の数を加算した内部作成メール数を、判定対象メールの送信者ドメイン２４９ｂに対応付けてドメイン別メール数一覧２４２１に記憶する。
【０１２５】
システム導入当初の段階においては、内部作成メール数が除外判定値２４２２に達しない。内部作成除外ドメインから送信された内部作成メール数に所定の数を加算することにより、内部作成メール数が除外判定値２４２２以上となるので、内部ドメイン詐称スコア算出部２４３は、判定対象メールが詐称メールである可能性が低いと判定する。
【０１２６】
これにより、内部作成メールを送信してくることがあらかじめわかっているドメインから内部作成メールが送信された場合に、その電子メールを詐称メールであると判定するのを防ぐことができる。
【０１２７】
なお、所定の数を加算するのを、例えば、システム導入時から計数時間２４２３の期間が経過するまでに限るのは、その間に、メール通信記憶部２２に内部作成メールが蓄積され、内部作成メール数が除外判定値２４２２に達すると考えられるからである。
逆に、計数時間２４２３が経過してもまだ内部作成メール数が除外判定値２４２２に達していない場合は、例えばＭＬの設定が変更になり、そのドメインから内部作成メールが送信されなくなったものと考えられる。
その場合、そのドメインからの電子メールを除外する必要がなくなるため、他のドメインからの電子メールと同様、実際の内部作成メール数に基づいて、詐称メールか否かを判定する。
【０１２８】
あるいは、内部ドメイン検査部２４において、内部ドメイン詐称スコア算出部２４３の処理を詐称判定部２８が実行するものとしてもよい。この場合は、詐称判定部２８が、ドメイン別メール数一覧２４２１と除外判定値２４２２に基づいて、判定対象メールの内部ドメイン詐称スコア２４６を算出する。
例えば、詐称判定部２８が備える詐称評価値算出部２８１は、判定対象メールについてスコアを算出し、判定対象メールの送信者ドメイン２４９ｂに対応する内部作成メール数が除外判定値２４２２より小さい場合に、スコアに所定の値（内部ドメイン詐称スコア２４６「４」）を加算する。
【０１２９】
図９は、本実施の形態に係る内部ドメイン検査部２４の内部ドメイン検査方法を示すフローチャートである。図９を用いて、本実施の形態に係る内部ドメイン検査部２４の内部ドメイン検査方法について説明する。
【０１３０】
Ｓ２４１０において、送信者ドメイン取得部２４１は、判定対象メールの作成者ドメイン２４８ｂを作成者ドメイン取得部２３から入力する。
内部ドメイン検査部２４は、予め、内部ドメインを記憶装置９４に記憶している。
Ｓ２４２０において、送信者ドメイン取得部２４１は、入力した作成者ドメイン２４８ｂと記憶装置９４に記憶している内部ドメインとを処理装置により比較して、判定対象メールの作成者ドメイン２４８ｂが内部ドメインであるか否かを判定する。
【０１３１】
判定対象メールの作成者ドメイン２４８ｂが内部ドメインであると判定された場合（Ｓ

２４２０においてＹＥＳ）は、処理はＳ２４３０に進む。判定対象メールの作成者ドメイン２４８ｂが内部ドメインでないと判定された場合（Ｓ２４２０においてＮＯ）は、処理はＳ２４５０に進む。

【０１３２】

Ｓ２４３０において、送信者ドメイン取得部２４１は、メール通信記憶部２２に記憶されている判定対象メールの情報から、判定対象メールの送信者ドメイン２４９ｂを取得し、内部作成計数部２４２に出力する。

【０１３３】

Ｓ２４４０において、内部作成計数部２４２は、入力した判定対象メールの送信者ドメイン２４９ｂと、計数時間２４２３とに基づいて、メール通信記憶部２２に記憶されている電子メールを計数し、ドメイン別の内部作成メール数をドメイン別メール数一覧２４２１に設定する。

ドメイン別メール数一覧２４２１には、ドメイン毎の内部作成メール数が設定されている。内部ドメイン検査部２４では、内部作成メール数が除外判定値２４２２以上になったドメインを、詐称メールであるか否かの判定から除外する。内部作成計数部２４２によるドメイン別メール数一覧２４２１への設定処理を「除外ドメイン学習処理」と呼ぶ。

【０１３４】

Ｓ２４５０において、内部ドメイン詐称スコア算出部２４３は、判定対象メールについて内部ドメイン詐称スコア２４６を算出する。

【０１３５】

内部ドメイン詐称スコア算出部２４３は、判定対象メールの作成者ドメイン２４８ｂが内部ドメインでない場合、詐称メールの可能性が低いので、内部ドメイン詐称スコア２４６に「０」を設定する。

【０１３６】

内部ドメイン詐称スコア算出部２４３は、判定対象メールの作成者ドメイン２４８ｂが内部ドメインである場合、ドメイン別メール数一覧２４２１の判定対象メールの送信者ドメイン２４９ｂに対応する内部作成メール数を取得する。

内部ドメイン詐称スコア算出部２４３は、取得した内部作成メール数が除外判定値２４２２以上である場合、内部ドメイン詐称スコア２４６に「０」を設定する。

内部ドメイン詐称スコア算出部２４３は、取得した内部作成メール数が除外判定値２４２２より小さい値である場合、内部ドメイン詐称スコア２４６に「４」を設定する。

【０１３７】

内部ドメイン詐称スコア算出部２４３は、内部ドメイン詐称スコア２４６を内部ドメイン検査部２４が出力するスコアとして詐称判定部２８に出力する。

【０１３８】

詐称判定部２８は、内部ドメイン検査部２４が出力した内部ドメイン詐称スコア２４６に基づいて、判定対象メールが詐称メールであるか否かを判定する。

【０１３９】

図１０は、本実施の形態に係る内部作成計数部２４２による除外ドメイン学習処理を示すフローチャートである。

【０１４０】

Ｓ２４４１において、内部作成計数部２４２は、送信者ドメイン取得部２４１から判定対象メールの送信者ドメイン２４９ｂを入力する。

Ｓ２４４２において、内部作成計数部２４２は、記憶装置９４に記憶されている計数時間２４２３を取得する。

【０１４１】

Ｓ２４４３において、内部作成計数部２４２は、判定対象メールの送信者ドメイン２４９ｂと計数時間２４２３とに基づいて、メール通信記憶部２２に記憶されている電子メールから送信者ドメインが判定対象メールの送信者ドメイン２４９ｂであり、かつ、作成者ドメインが内部ドメインである内部作成メールを処理装置により計数する。

【０１４２】
特に、内部作成計数部２４２は、メール通信記憶部２２に記憶されている電子メールのうち、現時点から計数時間２４２３遡った時点から現時点までの期間に取得された電子メールについて、送信者ドメインが判定対象メールの送信者ドメイン２４９ｂであり、かつ、作成者ドメインが内部ドメインである内部作成メールを処理装置により計数する。
例えば、現時点が２０１２年９月１０日であり、計数時間２４２３が「３ヶ月」であるとすると、内部作成計数部２４２は、メール通信記憶部２２に記憶されている電子メールのうち、過去３ヶ月分の電子メール（２０１２年６月１０日から計数時間２４２３遡った時点から現時点までの期間に取得された電子メール）について、送信者ドメインが判定対象メールの送信者ドメイン２４９ｂであり、かつ、作成者ドメインが内部ドメインである内部作成メールを処理装置により計数する。
【０１４３】
内部ドメイン検査部２４は、除外すべきドメインとして予め判明している除外ドメイン一覧２４２５を記憶装置９４に記憶している。
Ｓ２４４４において、内部作成計数部２４２は、判定対象メールの送信者ドメイン２４９ｂが除外ドメイン一覧２４２５に含まれているが否かを処理装置により判定する。判定対象メールの送信者ドメイン２４９ｂが除外ドメイン一覧２４２５に含まれていないと判定した場合（Ｓ２４４４）は、処理はＳ２４４６に進む。
【０１４４】
判定対象メールの送信者ドメイン２４９ｂが除外ドメイン一覧２４２５に含まれている判定した場合は、内部作成計数部２４２は、現時点が所定の時期であるか否かを処理装置により判定する。所定の時期とは、例えば、システム導入時から計数時間２４２３以内の時期である。内部作成計数部２４２は、現時点が所定の時期でないと判定した場合（Ｓ２４４４でＮＯ）には、処理はＳ２４４６に進む。
【０１４５】
Ｓ２４４６において、内部作成計数部２４２は、ドメイン別メール数一覧２４２１のドメイン名のうち、判定対象メールの送信者ドメイン２４９ｂに対応するドメイン名の内部作成メール数の欄に、Ｓ２４４３において算出した内部作成メール数を設定する。
【０１４６】
現時点が所定の時期であると判定した場合（Ｓ２４４４でＹＥＳ）には、処理はＳ２４４５に進む。
【０１４７】
Ｓ２４４５において、内部作成計数部２４２は、Ｓ２４４３で計数した判定対象メールの送信者ドメインの内部作成メール数に、所定の数（例えば、除外判定値２４２２）を処理装置により加算する。内部作成計数部２４２は、ドメイン別メール数一覧２４２１のドメイン名のうち、判定対象メールの送信者ドメイン２４９ｂに対応するドメイン名の内部作成メール数の欄に、算出した内部作成メール数を設定する。
【０１４８】
例えば、図８において、ドメイン名“ＡＢＣ．ｃｏｍ”が、除外ドメイン一覧２４２５に含まれているものとする。判定対象メールの送信者ドメイン２４９ｂが“ＡＢＣ．ｃｏｍ”であり、Ｓ２４４３において計数した内部作成メール数が「３」であったとする。さらに、現時点が「２０１２年９月１０日」、計数時間２４２３が「３ヶ月」、除外判定値２４２２が「１０通」であるとする。そしてシステム導入時が「２０１２年８月１０日」であったとする。
【０１４９】
このとき、内部作成計数部２４２は、Ｓ２４４４において、送信者ドメイン２４９ｂ“ＡＢＣ．ｃｏｍ”が除外ドメイン一覧２４２５に含まれており、かつ、現時点「２０１２年９月１０日」がシステム導入時「２０１２年８月１０日」から計数時間２４２３「３ヶ月」以内であり、所定の時期であると判定する。したがって、内部作成計数部２４２は、Ｓ２４４５において、Ｓ２４４３で計数した内部作成メール数「３」に、除外判定値２４

２２「１０」を処理装置により加算し、ドメイン名“ＡＢＣ．ｃｏｍ”に対応する内部作成メール数に「１３」を設定する。

【０１５０】

Ｓ２４４６において、内部作成計数部２４２は、ドメイン別メール数一覧２４２１のドメイン名のうち、判定対象メールの送信者ドメイン２４９ｂに対応するドメイン名の内部作成メール数の欄に、算出した内部作成メール数を設定する。

【０１５１】

以上で、除外ドメイン学習処理の説明を終わる。

【０１５２】

なお、システム導入当初において、内部作成メールを送信してくることがあらかじめわかっているドメインから送信された電子メールを詐称メールとして判定しないための構成として、内部作成計数部２４２が計数した内部作成メール数の所定の数を加算する構成について説明したが、他の構成であってもよい。

【０１５３】

例えば、メール通信記憶部２２は、ダミーメールについての情報をあらかじめ記憶しておく。

この場合におけるダミーメールの取得日時は、例えば、システム導入時である。ダミーメールの送信者ドメイン２４９ｂは、上述した内部作成除外ドメインである。ダミーメールの作成者ドメイン２４８ｂは、内部ドメインである。

メール通信記憶部２２は、１つの内部作成除外ドメインにつき所定の数（例えば除外判定値２４２２）のダミーメールについての情報を記憶しておく。

【０１５４】

内部作成計数部２４２は、実際に取得した電子メールのほかにダミーメールも含めた電子メールのなかで、取得日時からの経過時間が計数時間２４２３以下である内部作成メールの数を計数する。

したがって、システム導入時から計数時間２４２３が経過するまでの間において、内部作成除外ドメインについて内部作成計数部２４２が計数する内部作成メール数には、ダミーメールの数が上乗せされる。

しかし、システム導入時から計数時間２４２３が経過したのちは、内部作成除外ドメインについて内部作成計数部２４２が計数する内部作成メール数に、ダミーメールの数は上乗せされない。内部作成計数部２４２は、実際の内部作成メールの数を計数する。

【０１５５】

このような構成としても、システム導入当初において、内部作成メールを送信してくることがあらかじめわかっているドメインから送信された電子メールを詐称メールとして判定しないようにすることができる。

【０１５６】

なお、内部ドメイン検査方法において、除外ドメイン学習処理を実行したのちに、内部ドメイン詐称スコアを算出する構成について説明したが、内部ドメイン詐称スコアを算出したのちに、除外ドメイン学習処理を実行する構成であってもよい。

【０１５７】

除外ドメイン学習処理を、内部ドメイン詐称スコアの算出に先だって実行する構成の場合、常に最新の学習結果に基づいてスコアを算出するので、判定精度を高くすることができる。

【０１５８】

逆に、除外ドメイン学習処理を、内部ドメイン詐称スコアの算出後に実行する構成の場合、スコアを算出するまでにかかる時間を短縮することができる。これにより、判定対象メールが詐称メールであると判定した場合における警告が出力されるまでにかかる時間を短縮できるので、警告が発せられる前に詐称メールが開かれてしまうのを防ぐことができる。

【０１５９】

以上説明した詐称メール検出装置（２０）は、
ネットワークを介した通信のうち、メール転送プロトコルである通信を取得するメール通信取得部（２１）と、
上記メール通信取得部が取得した通信によって転送される電子メールの作成者フィールドに記載された作成者が属する作成者ドメインを取得する作成者ドメイン取得部（２３）と、
上記作成者ドメイン取得部が取得した作成者ドメインが所定の内部ドメインである場合に、上記電子メールの送信者が属する送信者ドメインを取得する送信者ドメイン取得部（２４１）と、
判定対象メールと送信者ドメインが同じ１以上の電子メールのうち、作成者ドメインが上記内部ドメインである内部作成メールの数を計数する内部作成計数部（２４２）と、
上記内部作成計数部が計数した内部作成メールの数が所定の内部作成閾値より小さい場合に、上記判定対象メールが作成者を詐称した詐称メールである可能性があると判定する詐称判定部（２８，内部ドメイン詐称スコア算出部２４３）とを有する。

【０１６０】
上記内部作成計数部（２４２）は、上記１以上の電子メールのうち、所定の期間内に転送された上記内部作成メールの数だけを計数する。

【０１６１】
上記内部作成計数部（２４２）は、転送時刻が新しい順に所定の数以内の電子メールのなかで、上記判定対象メールと送信者ドメインが同じ内部作成メールの数を計数する。

【０１６２】
上記内部作成計数部（２４２）は、所定の時期に所定の内部作成除外ドメインから送信された内部作成メールが所定の数あるものとして、上記内部作成メールの数を計数する。

【０１６３】
上記詐称判定部（２８，２４３）は、
判定対象メールについて詐称評価値を算出し、上記内部作成計数部が計数した内部作成メールの数が所定の内部作成閾値より小さい場合に、上記詐称評価値に所定の値を加算する詐称評価値算出部（２８１，２４３）と、
上記詐称評価値算出部が算出した詐称評価値が所定の詐称評価閾値より大きい場合に、上記判定対象メールが作成者を詐称した詐称メールである可能性があると判定する詐称評価値判定部（２８３）とを有する。

【０１６４】
以上のように、本実施の形態に係る詐称メール検出装置の内部ドメイン検査部によれば、除外ドメインを学習しつつ、詐称メールを判定することができるので、より的確な詐称メールの判定が可能となる。

【０１６５】
また、本実施の形態に係る詐称メール検出装置の内部ドメイン検査部によれば、内部作成計数部は、現時点から計数時間遡った時点から現時点までに転送された内部作成メールの数だけを計数するので、最新の電子メールの動向を詐称メールの判定に反映させることができるので、より的確な詐称メールの判定が可能となる。

【０１６６】
また、本実施の形態に係る詐称メール検出装置の内部ドメイン検査部によれば、内部作成計数部は、転送時刻が新しい順に所定の数以内の電子メールのなかで、判定対象メールと送信者ドメインが同じ内部作成メールの数を計数するので、最新の電子メールの動向を詐称メールの判定に反映させることができるので、より的確な詐称メールの判定が可能となる。

【０１６７】
また、本実施の形態に係る詐称メール検出装置の内部ドメイン検査部によれば、内部作成計数部は、所定の時期に所定の内部作成除外ドメインから送信された内部作成メールが所定の数あるものとして、内部作成メールの数を計数するので、予め除外ドメインと判明

しているドメインからの電子メールを詐称メールと判定するのを防ぐことができる。
【０１６８】
実施の形態３.
実施の形態３について、図１１～図１６を用いて説明する。
この実施の形態では、実施の形態１で説明した詐称メール検出装置２０のうち、外国経由検査部２５の構成例について、詳しく説明する。
なお、実施の形態１または実施の形態２と共通する構成には、同一の符号を付し、説明を省略する場合がある。
【０１６９】
図１１は、実施の形態３における外国経由検査部２５の構成図である。
実施の形態３における外国経由検査部２５の構成について、図１１に基づいて説明する。
【０１７０】
外国経由検査部２５は、外国経由判定部２５１、国内信頼ドメイン学習部２５２、中継装置ドメイン取得部２５３、中継時刻取得部２５４、パケット送信元取得部２５５および外国経由検査スコア決定部２５９を備える。
【０１７１】
以下に、外国経由検査部２５が備える各構成の概要について説明する。外国経由検査部２５が備える各構成の詳細については別途説明する。
外国経由判定部２５１は、中継装置ドメイン取得部２５３、中継時刻取得部２５４またはパケット送信元取得部２５５によって取得される情報に基づいて、作成国と宛先国とが同じである電子メールが宛先国と異なる外国を経由して通信された外国経由メールであるか否かを判定する。作成国とは、電子メールの作成者のドメインが属する国のことである。宛先国とは、電子メールの宛先ドメインが属する国のことである。
国内信頼ドメイン学習部２５２（外国経由計数部の一例）は、外国経由判定部２５１の判定結果に基づいて、電子メールの作成者が属する作成者ドメインのうち電子メールが外国を経由しないで通信される可能性が高い作成者ドメインを国内信頼ドメインとして学習し、国内信頼ドメイン一覧２５２Ａを生成する。
中継装置ドメイン取得部２５３は、電子メールのヘッダを参照し、電子メールを中継した中継装置（メールサーバ）が属する中継装置ドメインを電子メールのヘッダから取得する。
中継時刻取得部２５４は、電子メールのヘッダを参照し、電子メールが中継された中継時刻のタイムゾーンを電子メールのヘッダから取得する。
パケット送信元取得部２５５は、電子メールの少なくとも一部を含んだＩＰパケットからＩＰパケットの送信元アドレスを取得する。
外国経由検査スコア決定部２５９は、外国経由判定部２５１の判定結果に基づいて、詐称メールであるか否かを判定する対象の電子メール（以下、「判定対象メール」という）が詐称メールである可能性の度合いを表す外国経由検査スコアを算出する。
【０１７２】
図１２、図１３は、実施の形態３における国内信頼ドメイン学習処理を示すフローチャートである。
国内信頼ドメイン一覧２５２Ａを生成する国内信頼ドメイン学習処理について、図１２および図１３に基づいて説明する。
【０１７３】
外国経由検査部２５は、メール通信取得部２１が電子メールを取得する毎に、以下に説明する国内信頼ドメイン学習処理を実行する。
【０１７４】
図１２のＳ２５０１－１から国内信頼ドメイン学習処理の説明を始める。
【０１７５】
Ｓ２５０１－１において、外国経由判定部２５１は、メール通信取得部２１によって取

得された電子メールの作成国と宛先国とが同じであるか否かを判定する。
電子メールの作成国とは、電子メールを作成した作成者のドメインが属する国のことである。
電子メールの宛先国とは、電子メールの宛先のドメインが属する国のことである。
【０１７６】
例えば、作成者のメールアドレス「ｘｘｘ@ｙｙｙ．ｃｏ．ｊｐ」を構成する文字列のうちアットマークの後ろの文字列「ｙｙｙ．ｃｏ．ｊｐ」が作成者ドメインを表し、作成者ドメイン「ｙｙｙ．ｃｏ．ｊｐ」の最後のドット以降にある末尾の文字列「．ｊｐ」が作成国を表す。末尾の文字列が「．ｊｐ」である場合、作成国は日本である。
例えば、電子メールの宛先アドレス「ａａａ@ｂｂｂ．ｕｓ」を構成する文字列のうちアットマークの後ろの文字列「ｂｂｂ．ｕｓ」が宛先ドメインを表し、宛先ドメイン「ｂｂｂ．ｕｓ」の末尾の文字列「．ｕｓ」が宛先国を表す。末尾の文字列が「．ｕｓ」である場合、宛先国は米国である。
実施の形態の場合、電子メールの宛先国は、ローカルネットワークシステム１０のメールサーバ装置１４のドメイン（宛先ドメイン）が属する国と同じである。
【０１７７】
電子メールの作成国と電子メールの宛先国とが同じであるか否かを以下のように判定する。
外国経由判定部２５１は、電子メールの作成者ドメインを作成者ドメイン取得部２３から取得し、取得した作成者ドメインから作成国を表す文字列を抽出する。
外国経由判定部２５１は、作成国を表す文字列と宛先国を表す文字列とが同じであるか否かを判定する。宛先国を表す文字列は、記憶装置９４に予め記憶しておくか、または、電子メールの宛先アドレスから取得する。
【０１７８】
作成者ドメインの末尾の文字列が「．ｃｏｍ」などのように国を表す文字列でない場合、外国経由判定部２５１は、電子メールの作成国と電子メールの宛先国とが同じであるか否かを以下のように判定する。
外国経由判定部２５１は、電子メールの作成者ドメインを作成者ドメイン取得部２３から取得し、取得した作成者ドメインに対応するＩＰアドレスをＤＮＳサーバ（図示省略）から取得する。
外国経由判定部２５１は、ＤＮＳサーバから取得したＩＰアドレスが、宛先国に割り当てられているＩＰアドレスの範囲に含まれるか否かを判定する。
ＤＮＳサーバから取得したＩＰアドレスが、宛先国に割り当てられているＩＰアドレスの範囲に含まれる場合、電子メールの作成国と電子メールの宛先国は同じ国である。宛先国に割り当てられているＩＰアドレスの範囲に関する情報は記憶装置に予め記憶しておく。
宛先ドメインの末尾の文字列が国を表す文字列でない場合も、同様である。あるいは、外国経由判定部２５１は、あらかじめ宛先国を記憶しておく構成であってもよい。
【０１７９】
以下、作成国と宛先国とが同じである電子メールを「国内メール」という。
作成国と宛先国とが同じである国内メールは、原則として、国内のメールサーバから送信され、外国のメールサーバを経由しない。したがって、外国のメールサーバを経由した国内メールは、詐称メールである可能性がある。
【０１８０】
但し、外国のメールサーバを経由した国内メールであっても、詐称メールではない場合がある。
例えば、大手ＭＬなどのメールサーバは、電子メールの作成者メールアドレスに、電子メールの宛先アドレスを設定する場合がある。この場合、作成国と宛先国とが同じになるが、実際の作成者が外国から送信した電子メールであれば、外国のメールサーバを経由する。

あるいは、国内の作成者が、外国のクラウドサービスを利用して送信した電子メールの場合も、作成国と宛先国とが同じになるが、外国のメールサーバを経由する。
したがって、実施の形態３における国内メールの中には、外国のメールサーバを経由していても詐称メールでないものが存在する。
Ｓ２５０１－１の後、Ｓ２５０１－２に進む。
【０１８１】
Ｓ２５０１－２において、メール通信取得部２１によって取得された電子メールが国内メールであると判定された場合（ＹＥＳ）、Ｓ２５０２－１に進む。
また、メール通信取得部２１によって取得された電子メールが国内メールでないと判定された場合（ＮＯ）、国内信頼ドメイン学習処理は終了する。
【０１８２】
Ｓ２５０２－１において、外国経由判定部２５１は、メール通信取得部２１によって取得された電子メールが、外国のメールサーバを経由したか否かを判定する。以下、外国のメールサーバを経由した電子メールを「外国経由メール」と呼ぶ。
電子メールが外国経由メールであるか否かの判定方法は、後述する外国経由検査方法のＳ２５２０からＳ２５２２及びＳ２５３０と同様なので、外国経由検査方法についての説明を参照されたい。
Ｓ２５０２－１の後、Ｓ２５０２－２に進む。
【０１８３】
Ｓ２５０２－２において、外国経由判定部２５１は、作成者ドメイン取得部２３から、電子メールの作成者ドメインを取得する。
Ｓ２５０２－２の後、Ｓ２５０２－３に進む。
【０１８４】
Ｓ２５０２－３において、外国経由判定部２５１は、メール通信取得部２１によって取得された電子メールの通信日時と、Ｓ２５０２－２で取得した作成者ドメインと、Ｓ２５０２－１で判定した判定結果（以下、「外国経由判定結果」という）とを対応付けてメール通信記憶部２２に記憶する。
電子メールの通信日時とは、例えば、メール通信取得部２１が電子メールを取得した日時、または電子メールのメールヘッダに含まれる送信日時である。
Ｓ２５０２－３の後、図１３のＳ２５０３に進む。
【０１８５】
Ｓ２５０３において、国内信頼ドメイン学習部２５２は、メール通信記憶部２２に記憶されている外国経由判定結果のうち、Ｓ２５０２で取得された作成者ドメインと同じドメインに対応付けられている外国経由判定結果の数を計数する。ここで、計数した外国経由判定結果の数を「電子メール数」という。
国内信頼ドメイン学習部２５２は、計数した電子メール数と所定の蓄積閾値（例えば、１００個）とを比較する。
電子メール数（外国経由判定結果の数）が蓄積閾値以上である場合（ＹＥＳ）、Ｓ２５０４に進む。
電子メール数が蓄積閾値未満である場合（ＮＯ）、国内信頼ドメイン学習処理は終了する。
【０１８６】
Ｓ２５０４において、国内信頼ドメイン学習部２５２は、メール通信記憶部２２から、Ｓ２５０２－２で取得された作成者ドメインと同じドメインに対応付けられている外国経由判定結果を取得する。
国内信頼ドメイン学習部２５２は、取得した外国経由判定結果のうち、電子メールが外国経由メールであることを示す外国経由判定結果の数を計数する。ここで、計数した外国判定結果の数を「外国経由メール数」という。
Ｓ２５０４の後、Ｓ２５０５に進む。
【０１８７】

なお、国内信頼ドメイン学習部２５２は、電子メールが外国経由メールであることを示す外国経由判定結果のうち、所定期間（例えば、計数する直前の１カ月）の通信日時に対応付けられている外国経由判定結果の数を外国経由メール数として計数してもよい。
また、国内信頼ドメイン学習部２５２は、通信日時が新しい順に、所定数（例えば、上記蓄積閾値と同じ数）の外国経由判定結果を対象にして外国経由メール数を計数してもよい。

【０１８８】
Ｓ２５０５において、国内信頼ドメイン学習部２５２は、Ｓ２５０４で計数した外国経由メール数に基づいて、Ｓ２５０２－２で取得した作成者ドメインが国内信頼ドメインであるか否かを判定する。
国内信頼ドメインとは、外国を経由せずに通信される可能性が高い電子メールを作成する作成者のドメイン（作成者ドメイン）である。

【０１８９】
例えば、国内信頼ドメイン学習部２５２は、作成者ドメインが国内信頼ドメインであるか否かを以下の（１）または（２）の判定方法によって判定する。
（１）国内信頼ドメイン学習部２５２は、外国経由メール数と所定の外国経由閾値（例えば、１０通）とを大小比較する。外国経由メール数が所定の外国経由閾値より小さい場合、国内信頼ドメイン学習部２５２は、作成者ドメインが国内信頼ドメインであると判定する。
（２）国内信頼ドメイン学習部２５２は、Ｓ２５０４で計数した電子メール数に対する外国経由メール数の割合と所定の外国経由閾値（例えば、１割）とを大小比較する。外国経由メール数の割合が所定の外国経由閾値より小さい場合、国内信頼ドメイン学習部２５２は、作成者ドメインが国内信頼ドメインであると判定する。
Ｓ２５０５の後、Ｓ２５０６に進む。

【０１９０】
なお、国内信頼ドメイン学習部２５２は、上記（１）または（２）以外の方法で、作成者ドメインが国内信頼ドメインであるか否かを判定する構成であってもよい。
例えば、国内信頼ドメイン学習部２５２は、上記（１）と（２）とを組み合わせて判定する構成であってもよい。
すなわち、外国経由メール数が第一の外国経由閾値より小さく、且つ、外国経由メール数の割合が第二の外国経由閾値より小さい場合に、国内信頼ドメイン学習部２５２は、作成者ドメインが国内信頼ドメインであると判定する構成であってもよい。
あるいは、外国経由メール数が第一の外国経由閾値より小さいか、または、外国経由メール数の割合が第二の外国経由閾値より小さい場合に、国内信頼ドメイン学習部２５２は、作成者ドメインが国内信頼ドメインであると判定する構成であってもよい。

【０１９１】
Ｓ２５０６において、作成者ドメインが国内信頼ドメインであると判定した場合（ＹＥＳ）、Ｓ２５０７に進む。

【０１９２】
また、作成者ドメインが国内信頼ドメインでないと判定した場合（ＮＯ）、国内信頼ドメイン学習処理は終了する。
但し、国内信頼ドメイン学習部２５２は、国内信頼ドメイン学習処理を終了する前に、以下の処理を行ってもよい。
まず、国内信頼ドメイン学習部２５２は、当該作成者ドメインが国内信頼ドメイン一覧２５２Ａに設定されているか否かを判定する。
そして、当該作成者ドメインが国内信頼ドメイン一覧２５２Ａに設定されている場合、国内信頼ドメイン学習部２５２は、国内信頼ドメイン一覧２５２Ａから当該作成者ドメインを削除する。

【０１９３】
Ｓ２５０７において、国内信頼ドメイン学習部２５２は、Ｓ２５０２－２で取得された

作成者ドメインが国内信頼ドメイン一覧２５２Ａに設定されているか否かを判定する。
当該作成者ドメインが国内信頼ドメイン一覧２５２Ａに設定されていない場合、国内信頼ドメイン学習部２５２は、作成者ドメインを国内信頼ドメインとして国内信頼ドメイン一覧２５２Ａに設定する。
そして、国内信頼ドメイン学習処理は終了する。

【０１９４】

上記の国内信頼ドメイン学習処理では電子メール数（外国経由判定結果の数）が所定の蓄積閾値未満である場合、国内信頼ドメインを学習していない（Ｓ２５０３参照）。
但し、国内信頼ドメイン学習部２５２は、電子メール数が所定の蓄積閾値未満である場合にも国内信頼ドメインを学習しても構わない。
この場合、学習に用いることができる外国経由判定結果の数が少ないため、国内信頼ドメインを適切に学習することができない可能性がある。つまり、国内信頼ドメインとして登録すべきでない作成者ドメインを国内信頼ドメインとして登録してしまう可能性がある。
そこで、電子メール数が所定の蓄積閾値未満である場合、国内信頼ドメイン学習部２５２は、所定数の外国経由メールを既に受信しているものとして、作成者ドメインが国内信頼ドメインであるか否かを判定する（Ｓ２５０５）。
例えば、国内信頼ドメイン学習部２５２は、実際の外国経由メール数に所定数を加えた値を判定用の外国経由メール数として算出する。そして、国内信頼ドメイン学習部２５２は、算出した判定用の外国経由メール数に基づいて、作成者ドメインが国内信頼ドメインであるか否かを判定する。

【０１９５】

また、国内信頼ドメイン一覧２５２Ａには、国内信頼ドメインであることが分かっている作成者ドメインを予め設定しておいても構わない。

【０１９６】

図１４は、実施の形態３における外国経由検査方法を示すフローチャートである。
実施の形態３における外国経由検査方法（詐称メール検出方法の一例）について、図１４に基づいて説明する。

【０１９７】

ここで、国内信頼ドメイン学習部２５２は、国内信頼ドメイン一覧２５２Ａを予め生成しているものとする。
例えば、国内信頼ドメイン一覧２５２Ａが生成された後、作成者ドメイン取得部２３が電子メールを取得したときに、外国経由検査部２５が当該電子メールを判定対象メールとして図１４に示す処理を実行する。

【０１９８】

Ｓ２５１０において、外国経由判定部２５１は、作成者ドメイン取得部２３から判定対象メールの作成者ドメインを取得する。
Ｓ２５１０の後、Ｓ２５１１に進む。

【０１９９】

Ｓ２５１１において、外国経由判定部２５１は、Ｓ２５１０で取得した判定対象メールの作成者ドメインが国内信頼ドメイン一覧２５２Ａに設定されている国内信頼ドメインと同じドメインであるか否かを判定する。
判定対象メールの作成者ドメインが国内信頼ドメインと同じドメインである場合（ＹＥＳ）、Ｓ２５２０からＳ２５２２の各処理に進む。
判定対象メールの作成者ドメインが国内信頼ドメインと同じドメインでない場合（ＮＯ）、Ｓ２５４０に進む。

【０２００】

なお、判定対象メールの作成者ドメインが国内信頼ドメイン一覧２５２Ａに設定されている国内信頼ドメインと同じドメインであれば、判定対象メールの作成国は、必ず宛先国と同じであるので、判定対象メールが国内メールであるか否かを判定する必要はない。

【０２０１】
Ｓ２５２０からＳ２５２２の各処理は、所定の順番で実行しても、並行して実行しても構わない。
【０２０２】
Ｓ２５２０において、中継装置ドメイン取得部２５３は、メール通信取得部２１から判定対象メールを取得し、取得した判定対象メールのメールヘッダから中継装置ドメイン（中継装置のＩＰアドレスを含む）を取得する。
Ｓ２５２０の後、Ｓ２５３０に進む。
【０２０３】
図１５は、実施の形態３における電子メールのメールヘッダの一例を示す概要図である。
３台の中継装置Ａ、Ｂ、Ｃを中継して通信された電子メール（例えば、判定対象メール）のメールヘッダについて、図１５に基づいて説明する。
電子メールのメールヘッダは、電子メールを中継した中継装置毎に「Ｒｅｃｅｉｖｅｄ：」で始まるＲｅｃｅｉｖｅｄフィールドを備える。
各Ｒｅｃｅｉｖｅｄフィールドは、中継装置ドメイン（中継装置のＩＰアドレスを含む）および中継時刻（中継時刻のタイムゾーンを含む）などの情報を含む。Ｒｅｃｅｉｖｅｄフィールドのｆｒｏｍ句は、中継装置が中継した電子メールをその中継装置に対して送信した送信元の装置（電子メールを送信した装置または一つ前の中継装置）のドメインを示し、ｂｙ句は、中継装置自身のドメインを示す。なお、ｂｙ句は、ない場合もあある。
電子メールのメールヘッダは、「Ｄａｔｅ：」で始まるＤａｔｅフィールドと、「Ｆｒｏｍ：」で始まるＦｒｏｍフィールドと、「Ｔｏ：」で始まるＴｏフィールドとを備える。
Ｄａｔｅフィールドは、電子メールの送信日時を示す。
Ｆｒｏｍフィールドは、電子メールを作成した作成者のメールアドレスを示す。このメールアドレスのアットマーク以降の文字列が作成者ドメインに相当する。
Ｔｏフィールドは電子メールの宛先のメールアドレスを示す。このメールアドレスのアットマーク以降の文字列が宛先ドメインに相当する。
【０２０４】
例えば、中継装置ドメイン取得部２５３は、図１５に示す判定対象メールのメールヘッダから、各Ｒｅｃｅｉｖｅｄフィールドに記載されている中継装置Ａドメイン、中継装置Ｂドメインおよび中継装置Ｃドメイン（それぞれＩＰアドレスを含む）を取得する。
【０２０５】
図１４に戻り、外国経由検査方法の説明をＳ２５２１から続ける。
【０２０６】
Ｓ２５２１において、中継時刻取得部２５４は、メール通信取得部２１から判定対象メールを取得し、取得した判定対象メールのメールヘッダから中継時刻（タイムゾーンを含む）を取得する。
例えば、中継時刻取得部２５４は、図１５に示す判定対象メールのメールヘッダから、各Ｒｅｃｅｉｖｅｄフィールドに記載されている中継時刻「・・・　＋９００（ＪＳＴ）」を取得する。中継時刻の最後の部分「＋９００（ＪＳＴ）」は中継時刻のタイムゾーンを示す。
例えば、タイムゾーン「＋９００（ＪＳＴ）」の「＋９００」および「ＪＳＴ」は、中継時刻がグリニッジ標準時（ＧＭＴ）より９時間進んでいる日本時間の時刻であることを意味する。
Ｓ２５２１の後、Ｓ２５３０に進む。
【０２０７】
Ｓ２５２２において、パケット送信元取得部２５５は、判定対象メールを通信するために用いられた少なくともいずれかのＩＰパケット、つまり、判定対象メールの少なくとも一部を含んだＩＰパケットをメール通信取得部２１から取得する。

パケット送信元取得部２５５は、メール通信取得部２１から取得したＩＰパケットのパケットヘッダからＩＰパケットの送信元アドレスを取得する。

Ｓ２５２２の後、Ｓ２５３０に進む。

【０２０８】

Ｓ２５３０において、外国経由判定部２５１は、Ｓ２５２０で取得された中継装置ドメイン（中継装置のＩＰアドレスを含む）と、Ｓ２５２１で取得された中継時刻（タイムゾーンを含む）と、Ｓ２５２２で取得された判定対象メールの送信元アドレスとの少なくともいずれかに基づいて、判定対象メールが外国経由メールであるか否かを判定する。

例えば、外国経由判定部２５１は、判定対象メール（電子メールの一例）が外国経由メールであるか否かを以下のように判定する。

【０２０９】

（１）外国経由判定部２５１は、Ｓ２５２０で取得された中継装置ドメイン毎に、中継装置ドメインに含まれる国名（中継国）と、ローカルネットワークシステム１０のメールサーバ装置１４のドメイン（宛先ドメイン）に含まれる国名（宛先国）とを比較する。宛先国は記憶装置に予め記憶しておくものとする。

例えば、中継装置ドメイン「ｘｘｘ．ｃｏ．ｊｐ」に含まれる「．ｊｐ」は、中継国が日本であることを意味する。

宛先国と少なくともいずれかの中継国とが異なる場合、外国経由判定部２５１は、判定対象メールが外国経由メールであると判定する。それ以外の場合、外国経由判定部２５１は判定対象メールが外国経由メールでないと判定する。

【０２１０】

（２）外国経由判定部２５１は、Ｓ２５２０で取得された中継装置のＩＰアドレス毎に、中継装置のＩＰアドレスと、ローカルネットワークシステム１０のメールサーバ装置１４のドメイン（宛先ドメイン）が属する宛先国に割り当てられているＩＰアドレスとを比較する。宛先国に割り当てられているＩＰアドレスの範囲に関する情報は記憶装置に予め記憶しておくものとする。

少なくともいずれかの中継装置のＩＰアドレスが宛先国に割り当てられているＩＰアドレスの範囲に含まれないＩＰアドレスである場合、外国経由判定部２５１は、判定対象メールが外国経由メールであると判定する。それ以外の場合、外国経由判定部２５１は判定対象メールが外国経由メールでないと判定する。

【０２１１】

（３）外国経由判定部２５１は、Ｓ２５２１で取得された中継時刻のタイムゾーン毎に、中継時刻のタイムゾーンと、ローカルネットワークシステム１０のメールサーバ装置１４のドメイン（宛先ドメイン）が属する宛先国のタイムゾーンとを比較する。宛先国のタイムゾーンは記憶装置に予め記憶しておくものとする。

少なくともいずれかの中継時刻のタイムゾーンが宛先国のタイムゾーンと異なる場合、外国経由判定部２５１は、判定対象メールが外国経由メールであると判定する。それ以外の場合、外国経由判定部２５１は判定対象メールが外国経由メールでないと判定する。

【０２１２】

（４）外国経由判定部２５１は、Ｓ２５２２で判定対象メールのＩＰアドレスから取得された送信元アドレスと、ローカルネットワークシステム１０のメールサーバ装置１４のドメイン（宛先ドメイン）が属する宛先国に割り当てられているＩＰアドレスとを比較する。宛先国に割り当てられているＩＰアドレスの範囲に関する情報は記憶装置に予め記憶しておくものとする。

判定対象メールの送信元アドレスが宛先国に割り当てられているＩＰアドレスの範囲に含まれないＩＰアドレスである場合、外国経由判定部２５１は、判定対象メールが外国経由メールであると判定する。それ以外の場合、外国経由判定部２５１は判定対象メールが外国経由メールでないと判定する。

【０２１３】

例えば、上記の（１）から（４）の少なくともいずれかの判定で判定対象メールが外国

経由メールであると判定した場合、外国経由判定部２５１は判定対象メールが外国経由メールであると判定する。
但し、外国経由判定部２５１は、上記の（１）から（４）のいずれかの判定結果に基づいて、判定対象メールが外国経由メールであるか否かを判定しても構わない。また、外国経由判定部２５１は、上記の（１）から（４）のうち２つまたは３つの判定結果に基づいて、判定対象メールが外国経由メールであるか否かを判定しても構わない。
Ｓ２５３０の後、Ｓ２５４０に進む。
【０２１４】
Ｓ２５４０において、外国経由検査スコア決定部２５９は、Ｓ２５１１の判定結果またはＳ２５３０の判定結果に基づいて、判定対象メールの外国経由検査スコアを決定する。
外国経由検査スコアとは、判定結果メールが詐称メールである可能性の度合いを表す値である。例えば、判定結果メールが詐称メールである可能性が高いほど外国経由検査スコアは高く、判定結果メールが詐称メールである可能性が低いほど外国経由検査スコアは低い。
【０２１５】
図１６は、実施の形態３における外国経由検査スコア一覧表２５９Ａの一例を示す図である。
例えば、図１６に示すような外国経由検査スコア一覧表２５９Ａを記憶装置に予め記憶しておく。
外国経由検査スコア一覧表２５９Ａは、条件と外国経由検査スコアとを対応付けている。
外国経由検査スコア決定部２５９は、Ｓ２５１１またはＳ２５３０の判定結果に対応する外国経由検査スコアを外国経由検査スコア一覧表２５９Ａから取得する。
【０２１６】
判定対象メールが国内信頼ドメインでない場合、外国経由検査スコア決定部２５９は、判定対象メールが詐称メールであるか否かを判断できないことを意味する外国経由検査スコア「０点」を外国経由検査スコア一覧表２５９Ａから取得する。
判定対象メールが外国経由メールでない場合、外国経由検査スコア決定部２５９は、判定対象メールが詐称メールである可能性が低いことを意味する外国経由検査スコア「０点」を外国経由検査スコア一覧表２５９Ａから取得する。
判定対象メールが外国経由メールである場合、外国経由検査スコア決定部２５９は、判定対象メールが詐称メールである可能性が高いことを意味する外国経由検査スコア「４点」を外国経由検査スコア一覧表２５９Ａから取得する。
Ｓ２５４０の後、Ｓ２５５０に進む。
【０２１７】
Ｓ２５５０において、詐称判定部２８は、Ｓ２５４０で決定された外国経由検査スコアに基づいて、判定対象メールが詐称メールであるか否かを判定する。
例えば、詐称判定部２８は、Ｓ２５４０で決定された判定対象メールの外国経由検査スコアと他の実施の形態で決定される判定対象メールのスコアとの合計値と、所定の詐称評価閾値とを比較する。判定対象メールのスコアの合計値が所定の詐称評価閾値より大きい場合、詐称判定部２８は、判定対象メールが詐称メールであると判定する。
但し、詐称判定部２８は、外国経由検査スコアを所定の詐称評価閾値と比較し、判定対象メールが詐称メールであるか否かを判定しても構わない。
Ｓ２５５０により、外国経由検査方法の処理は終了する。
【０２１８】
上記の外国経由検査方法（図１４参照）では、判定対象メールの作成者ドメインが国内信頼ドメインである場合に、判定対象メールが外国経由メールであるか否かを判定している（Ｓ２５１１からＳ２５３０参照）。
但し、外国経由検査部２５は、判定対象メールの作成者ドメインが国内信頼ドメインであるか否かに関わらず、判定対象メールが外国経由メールであるか否かを判定しても構わ

ない。
例えば、外国経由検査部２５は、外国経由検査方法のＳ２５１１で判定対象メールの作成者ドメインが国内信頼ドメインであるか否かを判定する代わりに、判定対象メールが国内メールであるか否かを判定する。外国経由検査部２５は、判定対象メールが国内メールである場合にＳ２５２０以降の処理を実行する。
例えば、判定対象メールが国内メールでない場合の外国経由検査スコアは、判定対象メールの作成者ドメインが国内信頼ドメインでない場合の外国経由検査スコアと同じスコアである。
判定対象メールが国内メールであるか否かを判定する方法は、国内信頼ドメイン学習処理（図１２参照）のＳ２５０１－１と同じである。
【０２１９】
また、外国経由検査部２５は、外国経由検査方法のＳ２５１１で判定対象メールの作成者ドメインが国内信頼ドメインであるか否かを判定する代わりに、判定対象メールの作成者ドメインが外国経由除外ドメインであるか否かを判定してもよい。
外国経由除外ドメインとは、国内信頼ドメインとは反対に、外国のメールサーバを経由する可能性が高い電子メールの作成者ドメインである。
外国経由検査部２５は、判定対象メールの作成者ドメインが外国経由除外ドメインでない場合にＳ２５２０以降の処理を実行する。
例えば、判定対象メールの作成者ドメインが外国経由除外ドメインである場合の外国経由検査スコアは、判定対象メールの作成者ドメインが国内信頼ドメインでない場合の外国経由検査スコアと同じスコアである。
また、外国経由検査部２５は、国内信頼ドメイン学習部２５２の代わりに、外国経由除外ドメイン学習部を備える。
外国経由除外ドメイン学習部は、国内信頼ドメイン学習処理（図１２、図１３参照）において国内信頼ドメインを外国経由除外ドメインに置き換えた処理を、外国経由除外ドメイン学習処理として実行する。
つまり、外国経由除外ドメイン学習部は、電子メールの作成者ドメインが外国経由除外ドメインであるか否かを判定し（図１３のＳ２５０５）、外国経由除外ドメインである作成者ドメインを外国経由除外ドメイン一覧に設定する（図１３のＳ２５０７）。
電子メールが外国経由除外ドメインである条件は、電子メールが国内信頼ドメインである条件と反対の条件である。
【０２２０】
国内信頼ドメイン学習部２５２は、国内信頼ドメインを学習する対象の電子メールとして、判定対象メールを利用してもよい。
その場合、国内信頼ドメイン学習部２５２は、外国経由検査方法（図１４参照）で得られた判定対象メールの外国経由判定結果と作成者ドメインとを記憶し、国内信頼ドメイン学習処理（図１３参照）のＳ２５０３からＳ２５０７を実行すればよい。
【０２２１】
以上説明した詐称メール検出装置（２０）は、
ネットワークを介した通信のうち、メール転送プロトコルである通信を取得するメール通信取得部（３１）と、
上記メール通信取得部が取得した通信によって転送される電子メールの作成者フィールドに記載された作成者が属する作成者ドメインを取得する作成者ドメイン取得部（２３）と、
上記作成者ドメイン取得部が取得した作成者ドメインが属する国が、上記電子メールの宛先ドメインが属する宛先国と同じである場合に、上記電子メールが上記宛先国と異なる国を経由したか否かを判定する外国経由判定部（２５１）と、
判定対象メールと作成者ドメインが同じ１以上の電子メールのうち、上記宛先国と異なる国を経由した外国経由メールの数を計数する外国経由計数部（国内信頼ドメイン学習部２５２）と、

上記判定対象メールが上記宛先国と異なる国を経由したと上記外国経由判定部が判定し、かつ、上記外国経由計数部が計数した外国経由メールの数が所定の外国経由閾値より小さい場合に、上記判定対象メールが作成者を詐称した詐称メールである可能性があると判定する詐称判定部（２８，外国経由検査スコア決定部２５９）とを有する。

【０２２２】

上記詐称メール検出装置（２０）は、

上記電子メールの中継装置フィールドに記載された中継装置ドメインを取得する中継装置ドメイン取得部（２５３）を有し、

上記外国経由判定部（２５１）は、上記中継装置ドメイン取得部が取得した中継装置ドメインが属する国が上記宛先国と異なる場合に、上記電子メールが上記宛先国と異なる国を経由したと判定する。

【０２２３】

上記詐称メール検出装置（２０）は、

上記電子メールの中継装置フィールドに記載された中継時刻を取得する中継時刻取得部（２５４）を有し、

上記外国経由判定部（２５１）は、上記中継時刻取得部が取得した中継時刻のタイムゾーンが上記宛先国のタイムゾーンと異なる場合に、上記電子メールが上記宛先国と異なる国を経由したと判定する。

【０２２４】

上記詐称メール検出装置（２０）は、

上記メール通信取得部が取得した通信に基づいて、上記通信を構成するパケットの送信元アドレスを取得するパケット送信元取得部（２５５）を有し、

上記外国経由判定部（２５１）は、上記パケット送信元取得部が取得した送信元アドレスが属する国が上記宛先国と異なる場合に、上記電子メールが上記宛先国と異なる国を経由したと判定する。

【０２２５】

上記外国経由計数部（２５２）は、上記１以上の電子メールのうち、所定の期間内に転送された上記外国経由メールの数だけを計数する。

【０２２６】

上記外国経由計数部（２５２）は、転送時刻が新しい順に所定の数以内の電子メールのなかで、上記判定対象メールと作成者ドメインが同じ外国経由メールの数を計数する。

【０２２７】

上記外国経由計数部（２５２）は、所定の時期に所定のドメインから送信された外国経由メールまたは外国経由メールでない電子メールが所定の数あるものとして、上記外国経由メールの数を計数する。

【０２２８】

上記詐称判定部（２８，２５９）は、

判定対象メールについて詐称評価値を算出し、上記判定対象メールが上記宛先国と異なる国を経由したと上記外国経由判定部が判定し、かつ、上記外国経由計数部が計数した外国経由メールの数が所定の外国経由閾値より小さい場合に、上記詐称評価値に所定の値を加算する詐称評価値算出部（２８１，２５９）と、

上記詐称評価値算出部が算出した詐称評価値が所定の詐称評価閾値より大きい場合に、上記判定対象メールが作成者を詐称した詐称メールである可能性があると判定する詐称評価値判定部（２８３）とを有する。

【０２２９】

実施の形態３により、外国経由検査部２５は、ローカルネットワークシステム１０のメールサーバ装置１４のドメインが属する国内だけを経由して通信されるはずの電子メールのうち、外国のメールサーバ装置を経由して通信された電子メールを外国経由メールとして判定することができる。

また、外国経由検査部２５は、電子メールが外国経由メールであるか否かに基づいて、

電子メールが詐称メールである可能性の度合いを表す外国経由検査スコアを決定することができる。

そして、詐称判定部２８は、外国経由検査スコアに基づいて、電子メールが詐称メールであるか否かを判定することができる。

【０２３０】

実施の形態４.

実施の形態４について、図１７～図２４を用いて説明する。

この実施の形態では、実施の形態１で説明した詐称メール検出装置２０のうち、パケット連続度検査部２６の構成例について、詳しく説明する。

なお、実施の形態１～実施の形態３と共通する構成には、同一の符号を付し、説明を省略する場合がある。

【０２３１】

図１７は、実施の形態４におけるパケット連続度検査部２６の構成図である。

実施の形態４におけるパケット連続度検査部２６の構成について、図１７に基づいて説明する。

【０２３２】

パケット連続度検査部２６は、連続度算出部２６１、統計量算出部２６２およびパケット連続度検査スコア決定部２６９を備える。

以下に、パケット連続度検査部２６が備える各構成の概要について説明する。パケット連続度検査部２６が備える各構成の詳細については別途説明する。

【０２３３】

連続度算出部２６１は、電子メールが通信された際のセッションで、通信方向が同じであるＩＰパケットが連続して送信された割合を算出する。

セッションとは、１つ以上のメッセージを所定の手順で送受信することによって構成される単位である。例えば、ＳＭＴＰでは、１つのセッションで１つの電子メールが送信される。

以下、連続度算出部２６１によって算出される割合を「パケット連続度」という。

【０２３４】

統計量算出部２６２は、電子メールの作成者が属する作成者ドメイン毎に、作成者ドメインが同じである電子メールのパケット連続度の統計量を算出する。

以下、統計量算出部２６２によって算出されるパケット連続度の統計量を「連続度統計量」という。

また、作成者ドメイン毎に作成者ドメインと連続度統計量とを対応付けて設定したデータを「統計量一覧表２６２Ａ」という。

【０２３５】

パケット連続度検査スコア決定部２６９は、判定対象メールのパケット連続度と、判定対象メールと作成者ドメインが同じである電子メールの連続度統計量とを比較する。

パケット連続度検査スコア決定部２６９は、比較結果に基づいて、判定対象メールが詐称メールである可能性の度合いを表すパケット連続度検査スコアを算出する。

判定対象メールとは、詐称メールであるか否かを判定する対象の電子メールである。

【０２３６】

図１８は、実施の形態４における統計量学習処理を示すフローチャートである。

作成者ドメイン別に連続度統計量を学習する統計量学習処理について、図１８に基づいて説明する。

【０２３７】

パケット連続度検査部２６は、メール通信取得部２１が電子メールを取得する毎に、以下に説明する統計量学習処理を実行する。

【０２３８】

Ｓ２６０１において、連続度算出部２６１は、メール通信取得部２１によって取得された電子メールのパケット連続度を算出する。

【０２３９】
図１９、図２０は、実施の形態４における電子メールのパケット連続度の一例を示す図である。
実施の形態４における電子メールのパケット連続度について、図１９および図２０に基づいて説明する。
【０２４０】
図１９および図２０において、「ＴＸ」は、外部のメールサーバ装置８２からローカルネットワークシステム１０のメールサーバ装置１４へ送信されたＩＰパケット（ＴＸパケット、送信パケットともいう）を表す。例えば、電子メールの少なくとも一部を含んだＩＰパケットはＴＸパケットの一例である。
また、「ＲＸ」は、ローカルネットワークシステム１０のメールサーバ装置１４から外部のメールサーバ装置８２へ送信されたＩＰパケット（ＲＸパケット、受信パケットともいう）を表す。例えば、ＴＸパケットを受信したことを応答するＡＣＫパケットはＲＸパケットの一例である。
【０２４１】
図１９において、電子メールＡが通信された際のセッションＡで、４つのＩＰパケットが「ＴＸ」「ＲＸ」「ＴＸ」「ＲＸ」の順で通信されたものとする。
この場合、「ＴＸ」「ＲＸ」のいずれも連続して通信されていない。
つまり、２つ目以降の３つのＩＰパケットのいずれも１つ前のＩＰパケットと連続していない。
したがって、電子メールＡのパケット連続度は「０％（＝０／３）」である。
【０２４２】
図２０において、電子メールＢが通信された際のセッションＢで、４つのＩＰパケットが「ＴＸ」「ＴＸ」「ＲＸ」「ＲＸ」の順で通信されたものとする。
この場合、先頭のＩＰパケット「ＴＸ」と２つ目のＩＰパケット「ＴＸ」とが連続し、３つ目のＩＰパケット「ＲＸ」と４つ目のＩＰパケット「ＲＸ」とが連続している。
つまり、２つ目以降の３つのＩＰパケットのうち、２つのＩＰパケットが１つ前のＩＰパケットと連続している。
したがって、電子メールＢのパケット連続度は「６６．７％（＝２／３）」である。
【０２４３】
但し、連続度算出部２６１は、「ＴＸ」と「ＲＸ」とのいずれかの連続度をパケット連続度として算出しても構わない。
例えば、連続度算出部２６１は、「ＴＸ」毎に、「ＴＸ」と「ＴＸ」の１つ後のＩＰパケットとが連続しているか否か判定する。
図２０の場合、１つ目の「ＴＸ」は１つ後のＩＰパケット「ＴＸ」と連続し、２つ目の「ＴＸ」は１つ後のＩＰパケット「ＲＸ」と連続していない。
つまり、２つの「ＴＸ」のうち、１つの「ＴＸ」が１つ後のＩＰパケットと連続している。したがって、パケット連続度は「５０％（＝１／２）」である。
【０２４４】
ＴＣＰ（伝送制御プロトコル）では、通常、送信パケットと、それに対するＡＣＫパケットとが交互に同期通信される。この場合、パケット連続度は「０％」になる。しかし、ウィンドウ制御やフロー制御、輻輳制御により、ＴＸパケットが連続して届く場合があり、パケット連続度は「０％」にならない。このような制御は、ＭＴＡ間の経路が長い場合や混雑している場合など、１回のパケットの往復に時間がかかる場合に行われることが多い。同じ送信者ドメインから送信された電子メールが中継される経路は、通常一定であるから、パケット連続度もほぼ一定になると考えられる。このため、パケット連続度を、送信者ドメインの特徴として利用することできる。
したがって、同じ送信者ドメインから送信された電子メールにかかるパケット連続度が、いつもの値と異なる異常値である場合、送信者ドメインを詐称した詐称メールである可能性がある。

【０２４５】
図１８に戻り、連続度統計量算出処理の説明をＳ２６０２から続ける。
【０２４６】
Ｓ２６０２において、連続度算出部２６１は、作成者ドメイン取得部２３から、電子メールの作成者ドメインを取得する。
Ｓ２６０２の後、Ｓ２６０３に進む。
【０２４７】
Ｓ２６０３において、連続度算出部２６１は、メール通信取得部２１によって取得された電子メールの通信日時と、Ｓ２６０２で取得した作成者ドメインと、Ｓ２６０１で算出したパケット連続度とを対応付けてメール通信記憶部２２に記憶する。
電子メールの通信日時とは、例えば、メール通信取得部２１が電子メールを取得した日時、または電子メールのメールヘッダに含まれる送信日時である。
Ｓ２６０３の後、Ｓ２６０４に進む。
【０２４８】
Ｓ２６０４において、統計量算出部２６２は、メール通信記憶部２２に記憶されているパケット連続度のうち、Ｓ２６０２で取得された作成者ドメインと同じドメインに対応付けられているパケット連続度を計数する。
統計量算出部２６２は、計数したパケット連続度の数が所定の蓄積閾値（例えば、１００個）以上であるか否かを判定する。
当該パケット連続度の数が蓄積閾値以上である場合（ＹＥＳ）、Ｓ２６０５に進む。
当該パケット連続度の数が蓄積閾値未満である場合（ＮＯ）、統計量学習処理は終了する。
【０２４９】
Ｓ２６０５において、統計量算出部２６２は、Ｓ２６０４で計数したパケット連続度をメール通信記憶部２２から取得する。
【０２５０】
例えば、統計量算出部２６２は、Ｓ２６０４で計数した全てのパケット連続度をメール通信記憶部２２から取得する。
但し、統計量算出部２６２は、Ｓ２６０４で計数したパケット連続度のうち、所定期間（例えば、直前の１カ月）の通信日時に対応付けられているパケット連続度を取得してもよい。
また、統計量算出部２６２は、電子メールの通信日時が新しい順に、所定数（例えば、上記蓄積閾値と同じ数）のパケット連続度を取得してもよい。
Ｓ２６０５の後、Ｓ２６０６に進む。
【０２５１】
Ｓ２６０６において、統計量算出部２６２は、Ｓ２６０５で取得したパケット連続度に基づいて、パケット連続度の統計量（連続度統計量）を算出する。
例えば、統計量算出部２６２は、パケット連続度の平均値および標準偏差を連続度統計量として算出する。
但し、統計量算出部２６２は、パケット連続度の最小値または最大値など、平均値または標準偏差以外の統計量を連続度統計量として算出しても構わない。
Ｓ２６０６の後、Ｓ２６０７に進む。
【０２５２】
Ｓ２６０７において、統計量算出部２６２は、Ｓ２６０２で取得された作成者ドメインと同じドメインに対応付けて、Ｓ２６０６で算出した連続度統計量を統計量一覧表２６２Ａに設定する。
既に、当該ドメインに対応付けられて連続度統計量が設定されている場合、統計量算出部２６２は、設定されている連続度統計量を今回算出した新たな連続度統計量に更新する。これにより、連続度統計量を最新の状態にすることができる。
Ｓ２６０７により、統計量学習処理は終了する。

【０２５３】
上記の統計量学習処理（図１８参照）では、作成者ドメイン毎に連続度統計量を算出している。
但し、統計量算出部２６２は、作成者ドメイン毎のパケット連続度を複数のグループに分類し、分類したグループ毎に連続度統計量を算出してもよい。
例えば、統計量算出部２６２は、作成者ドメイン毎のパケット連続度を電子メールの通信日時に基づいて、時間帯別、曜日別（平日休日別）またはこれらの組み合わせ別の複数のグループに分類し、分類したグループ毎に連続度統計量を算出してもよい。
【０２５４】
図２１は、実施の形態４における統計量一覧表２６２Ａの一例を示す図である。
例えば、統計量算出部２６２は、作成者ドメイン毎に連続度統計量（平均値、標準偏差）を算出し、作成者ドメインと連続度統計量とを対応付けて統計量一覧表２６２Ａに設定する。
【０２５５】
図２２は、実施の形態４における統計量一覧表２６２Ａの一例を示す図である。
例えば、統計量算出部２６２は、作成者ドメイン毎のパケット連続度を時間帯別のグループに分類し、時間帯別に連続度統計量を算出し、作成者ドメインと時間帯と連続度統計量とを対応付けて統計量一覧表２６２Ａに設定する。
【０２５６】
パケット連続度は、ＭＴＡ間の混雑度の影響を受ける場合がある。時間帯別や曜日別にパケット連続度を集計して、連続度統計量を算出することにより、パケット連続度が異常値であるか否かの判定精度を高くすることができる。
【０２５７】
図２３は、実施の形態４におけるパケット連続度検査方法を示すフローチャートである。
実施の形態４におけるパケット連続度検査方法（詐称メール検出方法の一例）について、図２３に基づいて説明する。
【０２５８】
ここで、統計量算出部２６２は、統計量一覧表２６２Ａを予め生成しているものとする。
【０２５９】
Ｓ２６１０において、連続度算出部２６１は、判定対象メールのパケット連続度を算出する。
パケット連続度の算出方法は、図１８で説明したＳ２６０１と同じである。
Ｓ２６１０の後、Ｓ２６２０に進む。
【０２６０】
Ｓ２６２０において、パケット連続度検査スコア決定部２６９は、作成者ドメイン取得部２３から判定対象メールの作成者ドメインを取得する。
Ｓ２６２０の後、Ｓ２６２１に進む。
【０２６１】
Ｓ２６２１において、パケット連続度検査スコア決定部２６９は、Ｓ２６２０で取得した判定対象メールの作成者ドメインに対応する連続度統計量を、統計量一覧表２６２Ａ（図２１参照）から取得する。
Ｓ２６２１の後、Ｓ２６３０に進む。
【０２６２】
Ｓ２６３０において、パケット連続度検査スコア決定部２６９は、Ｓ２６１０で算出されたパケット連続度と、Ｓ２６２１で取得した連続度統計量とを比較し、比較結果に基づいてパケット連続度検査スコアを決定する。
パケット連続度検査スコアは、判定対象メールが詐称メールである可能性の度合いを表す値である。

例えば、判定対象メールが詐称メールである可能性が高いほどパケット連続度検査スコアは高く、判定対象メールが詐称メールである可能性が低いほどパケット連続度検査スコアは低い。

【０２６３】

判定対象メールのパケット連続度と連続度統計量の平均値との差が大きい場合、判定対象メールをローカルネットワークシステム１０のメールサーバ装置１４に中継したメールサーバと、作成者ドメインが同じである他の電子メールをメールサーバ装置１４に中継したメールサーバとが異なる装置である可能性が高い。したがって、他の電子メールと異なるメールサーバによって中継された判定対象メールは詐称メールである可能性が高い。

【０２６４】

図２４は、実施の形態４におけるパケット連続度検査スコア一覧表２６９Ａの一例を示す図である。

例えば、図２４に示すようなパケット連続度検査スコア一覧表２６９Ａを記憶装置に予め記憶しておく。

パケット連続度検査スコア一覧表２６９Ａは、パケット連続度の範囲とパケット連続度検査スコア（異常値の一例）とを対応付けている。図中において「α」はパケット連続度を意味し、「μ」は平均値（連続度統計量の一例）を意味し、「σ」は標準偏差（連続度統計量の一例）を意味している。

パケット連続度検査スコア決定部２６９は、パケット連続度と連続度統計量との関係に基づいて、パケット連続度検査スコアをパケット連続度検査スコア一覧表２６９Ａから取得する。

【０２６５】

パケット連続度（α）が「μ－１σ≦α≦μ＋１σ」の関係を満たす場合、パケット連続度検査スコア決定部２６９は、判定対象メールが詐称メールである可能性が低いことを意味するパケット連続度検査スコア「０点」をパケット連続度検査スコア一覧表２６９Ａから取得する。

パケット連続度（α）が「μ－２σ≦α＜μ－１σ」または「μ＋１σ＜α≦μ＋２σ」の関係を満たす場合、パケット連続度検査スコア決定部２６９は、判定対象メールが詐称メールである可能性が比較的高いことを意味するパケット連続度検査スコア「１点」をパケット連続度検査スコア一覧表２６９Ａから取得する。

パケット連続度（α）が「α＜μ－２σ」または「μ＋２σ＜α」の関係を満たす場合、パケット連続度検査スコア決定部２６９は、判定対象メールが詐称メールである可能性が高いことを意味するパケット連続度検査スコア「２点」をパケット連続度検査スコア一覧表２６９Ａから取得する。

【０２６６】

但し、パケット連続度検査スコア決定部２６９は、上記以外の方法でパケット連続度検査スコアを決定しても構わない。

例えば、パケット連続度検査スコア決定部２６９は、パケット連続度と連続度統計量の平均値（または、最小値、最大値）との差（例えば、絶対値）を算出し、算出した差に応じてパケット連続度検査スコアを決定しても構わない。この場合、パケット連続度検査スコア一覧表２６９Ａには、差の範囲とパケット連続度検査スコアとを対応付けて設定しておく。

例えば、パケット連続度検査スコア決定部２６９は、パケット連続度と連続度統計量の平均値との差を、連続度統計量の標準偏差で割ることによって得られる商（異常値の一例）をパケット連続度検査スコアとして算出しても構わない。

Ｓ２６３０の後、Ｓ２６４０に進む。

【０２６７】

Ｓ２６４０において、詐称判定部２８は、Ｓ２６３０で決定されたパケット連続度検査スコアに基づいて、判定対象メールが詐称メールであるか否かを判定する。

例えば、詐称判定部２８は、Ｓ２６３０で決定された判定対象メールのパケット連続度

検査スコアと他の実施の形態で決定される判定対象メールのスコアとの合計値と、所定の詐称評価閾値とを比較する。判定対象メールのスコアの合計値が所定の詐称評価閾値より大きい場合、詐称判定部２８は、判定対象メールが詐称メールであると判定する。

但し、詐称判定部２８は、パケット連続度検査スコアを所定の詐称評価閾値と比較し、判定対象メールが詐称メールであるか否かを判定しても構わない。

Ｓ２６４０により、パケット連続度検査方法の処理は終了する。

【０２６８】

上記のパケット連続度検査方法（図２３参照）では、判定対象メールの作成者ドメインに対応する連続度統計量を統計量一覧表２６２Ａから取得し、取得した連続度統計量に基づいてパケット連続度検査スコアを決定している。

但し、統計量算出部２６２が作成者ドメイン別のパケット連続度を複数のグループ（例えば、時間帯別）に分類して連続度統計量を算出している場合、パケット連続度検査スコア決定部２６９は、判定対象メールが属するグループの連続度統計量を統計量一覧表２６２Ａ（図２２参照）から取得する。

そして、パケット連続度検査スコア決定部２６９は、判定対象メールが属するグループの連続度統計量に基づいて、Ｓ２６３０と同様にパケット連続度検査スコアを決定する。

この際、パケット連続度検査スコア一覧表２６９Ａ（図２４参照）をグループ別に記憶装置に記憶し、判定対象メールが属するグループ用のパケット連続度検査スコア一覧表２６９Ａを用いてパケット連続度検査スコアを算出してもよい。

【０２６９】

統計量算出部２６２は、連続度統計量を学習する対象の電子メールとして、判定対象メールを利用してもよい。

その場合、統計量算出部２６２は、パケット連続度検査方法（図２３参照）で得られた判定対象メールのパケット連続度と作成者ドメインとを記憶し、統計量学習処理（図１８参照）のＳ２６０４からＳ２６０７を実行すればよい。

【０２７０】

以上説明した詐称メール検出装置（２０）は、

ネットワークを介した通信のうち、メール転送プロトコルである通信を取得するメール通信取得部（２１）と、

上記メール通信取得部が取得した通信によって転送される電子メールの作成者フィールドに記載された作成者が属する作成者ドメインを取得する作成者ドメイン取得部（２３）と、

上記電子メールの転送にかかるセッションを構成する一連のパケットそれぞれの送信方向を判定し、上記一連のパケットのうち２番目以降のパケットの送信方向が、１つ前のパケットと同じであるパケットの割合を算出して、上記電子メールのパケット連続度とする連続度算出部（２６１）と、

判定対象メールと作成者ドメインが同じ１以上の電子メールについて上記連続度算出部が算出したパケット連続度に基づいて統計量を算出する統計量算出部（２６２）と、

上記統計量算出部が算出した統計量に基づいて、上記判定対象メールについて上記連続度算出部が算出したパケット連続度が異常値であるか否かを判定し、上記パケット連続度が異常値であると判定した場合に、上記判定対象メールが作成者を詐称した詐称メールである可能性があると判定する詐称判定部（２８，パケット連続度検査スコア決定部２６９）とを有する。

【０２７１】

上記統計量算出部（２６２）は、上記統計量として、上記１以上の電子メールのパケット連続度を平均した平均値及び標準偏差を算出し、

上記詐称判定部（２８，２６９）は、上記標準偏差に所定の定数を乗じた値を上記平均値に加えた値よりも上記パケット連続度が大きい場合と、上記標準偏差に所定の定数を乗じた値を上記平均値から差し引いた値よりも上記パケット連続度が小さい場合とのうち、少なくともいずれかの場合に、上記パケット連続度が異常値であると判定する。

【０２７２】
上記詐称判定部（２８，２６９）は、
判定対象メールについて詐称評価値を算出し、上記統計量算出部が算出した統計量に基づいて、上記連続度算出部が算出したパケット連続度が異常値であるか否かを判定し、上記パケット連続度が異常値であると判定した場合に、上記詐称評価値に所定の値を加算する詐称評価値算出部（２８１，２６９）と、
上記詐称評価値算出部が算出した詐称評価値が所定の詐称評価閾値より大きい場合に、上記判定対象メールが作成者を詐称した詐称メールである可能性があると判定する詐称評価値判定部（２８３）とを有する。
【０２７３】
上記詐称評価値算出部（２６９）は、
上記連続度算出部が算出したパケット連続度の異常度を算出し、算出した異常度に応じた値を上記詐称評価値に加算する。
【０２７４】
上記統計量算出部（２６２）は、上記統計量として、上記１以上の電子メールのパケット連続度を平均した平均値及び標準偏差を算出し、
上記詐称評価値算出部は、上記判定対象メールのパケット連続度と、上記統計量算出部が算出した平均値との差を、上記標準偏差で割った商を算出して、上記異常度とする。
【０２７５】
上記統計量算出部（２６２）は、上記１以上の電子メールを、上記電子メールが転送された時間帯と、曜日と、平日休日の別とのうち少なくともいずれかに基づいて、複数のグループに分類し、分類したそれぞれのグループについて、上記統計量を算出する。
【０２７６】
上記統計量算出部（２６２）は、上記１以上の電子メールのうち、所定の期間内に転送された電子メールに基づいて、上記統計量を算出する。
【０２７７】
上記統計量算出部（２６２）は、転送時刻が新しい順に所定の数以内の電子メールに基づいて、上記統計量を算出する。
【０２７８】
実施の形態４により、パケット連続度検査部２６は、電子メールを通信する際のセッションで通信されたＩＰパケットの通信順序に基づいて、ＩＰパケットの通信順序に関する指標値（パケット連続度）を算出することができる。
また、パケット連続度検査部２６は、電子メールの指標値と指標値の統計量との差に基づいて、電子メールが詐称メールである可能性の度合いを表すパケット連続度検査スコアを決定することができる。
そして、詐称判定部２８は、パケット連続度検査スコアに基づいて、電子メールが詐称メールであるか否かを判定することができる。
【０２７９】
このように、パケット連続度を送信者ドメインの特徴として捉え、パケット連続度が異常値である場合に、詐称メールの可能性があると判定する。パケット連続度は、通信の結果として得られる値なので、攻撃者が意図的に設定することが困難である。
これにより、判定対象メールが詐称メールであるか否かの判定精度を高くすることができ、標的型サイバー攻撃による秘密情報の漏洩を防ぐことができる。
【０２８０】
実施の形態５.
実施の形態５について、図２５～図３１を用いて説明する。
この実施の形態では、実施の形態１で説明した詐称メール検出装置２０のうち、転送経路検査部２７の構成例について、詳しく説明する。
なお、実施の形態１～実施の形態４と共通する構成には、同一の符号を付し、説明を省略する場合がある。

【０２８１】
図２５は、実施の形態５における転送経路検査部２７の構成図である。
実施の形態５における転送経路検査部２７の構成について、図２５に基づいて説明する。
【０２８２】
転送経路検査部２７は、転送経路算出部２７１、ドメイン経路学習部２７２、経路情報取得部２７３および転送経路検査スコア決定部２７９を備える。
以下に、転送経路検査部２７が備える各構成の概要について説明する。転送経路検査部２７が備える各構成の詳細については別途説明する。
【０２８３】
転送経路算出部２７１は、経路情報取得部２７３によって取得された経路情報に基づいて、電子メールが通信された際の転送経路を算出する。
転送経路は、電子メールを中継（転送）した１つ以上の中継装置（メールサーバ）を示す情報である。
以下、転送経路を示すデータを「転送経路データ２７１Ａ」という。
【０２８４】
ドメイン経路学習部２７２（経路一致計数部、経路部分一致計数部の一例）は、電子メールの作成者ドメイン毎に、作成者ドメインから送信された電子メールが転送される転送経路を学習する。
作成者ドメインとは、電子メールを作成した作成者が属するドメインである。
以下、ドメイン経路学習部２７２によって学習された転送経路を「ドメイン経路」という。また、ドメイン経路を一覧にしたリストを「ドメイン経路リスト２７２Ａ」という。
【０２８５】
経路情報取得部２７３は、電子メールのメールヘッダ、および、電子メールを通信するために用いられたＩＰパケット（例えば、電子メールの少なくとも一部を含んだＩＰパケット）から、転送経路を算出するための経路情報を取得する。
ＩＰパケットを中継した中継装置のドメイン（中継装置ドメイン）およびＩＰパケットの送信元アドレスは、経路情報取得部２７３によって取得される経路情報の一例である。
【０２８６】
転送経路検査スコア決定部２７９は、判定対象メールの転送経路と、判定対象メールの作成者ドメインについてのドメイン経路とを比較し、判定対象メールが詐称メールである可能性の度合いを表す転送経路検査スコアを算出する。
判定対象メールとは、詐称メールであるか否かを判定する対象の電子メールである。
【０２８７】
図２６は、実施の形態５におけるドメイン経路学習処理を示すフローチャートである。
電子メールの作成者ドメイン別にドメイン経路を学習するドメイン経路学習処理について、図２６に基づいて説明する。
【０２８８】
転送経路検査部２７は、メール通信取得部２１が電子メールを取得する毎に、以下に説明する転送経路学習処理を実行する。
【０２８９】
Ｓ２７０１において、経路情報取得部２７３は、メール通信取得部２１によって取得された電子メールのメールヘッダから、電子メールの転送経路を算出するための経路情報を取得する。
また、経路情報取得部２７３は、当該電子メールを通信するために用いられたＩＰパケット（例えば、電子メールの少なくとも一部を含んだＩＰパケット）をメール通信取得部２１から取得し、取得したＩＰパケットから経路情報を取得する。
【０２９０】
図２７は、実施の形態５における電子メールのメールヘッダの一例を示す概要図である。

３台の中継装置Ａ、Ｂ、Ｃを中継して通信された電子メールのメールヘッダについて、図２７に基づいて説明する。

【０２９１】

電子メールのメールヘッダは、電子メールを中継した中継装置毎に「Ｒｅｃｅｉｖｅｄ：」で始まるＲｅｃｅｉｖｅｄフィールドを備える。

Ｒｅｃｅｉｖｅｄフィールドは、電子メールを受信した中継装置が電子メールを中継する際に設定する。ここで、電子メールを受信した中継装置を「受信中継装置」といい、電子メールを受信中継装置へ中継した中継装置を「送信中継装置」という。

Ｒｅｃｅｉｖｅｄフィールドは、中継装置のドメイン（中継装置のＩＰアドレスを含む）などの情報を含む。

Ｒｅｃｅｉｖｅｄフィールドのｆｒｏｍ句は送信中継装置のドメインを示し、ｂｙ句は受信中継装置のドメインを示す。

但し、受信中継装置は、電子メールを中継する際、Ｒｅｃｅｉｖｅｄフィールドにｂｙ句を設定しなくても構わない。この場合、電子メールを最後に中継した中継装置のドメインを電子メールのメールヘッダから取得することはできない。

【０２９２】

電子メールのメールヘッダは、「Ｄａｔｅ：」で始まるＤａｔｅフィールドと、「Ｆｒｏｍ：」で始まるＦｒｏｍフィールドと、「Ｔｏ：」で始まるＴｏフィールドとを備える。

Ｄａｔｅフィールドは電子メールの送信日時を示す。

Ｆｒｏｍフィールドは電子メールを作成した作成者のメールアドレスを示す。このメールアドレスのアットマーク以降の文字列が作成者ドメインに相当する。

Ｔｏフィールドは電子メールの宛先のメールアドレスを示す。このメールアドレスのアットマーク以降の文字列が宛先ドメインに相当する。

【０２９３】

例えば、経路情報取得部２７３は、図２７に示す電子メールのメールヘッダから、各Ｒｅｃｅｉｖｅｄフィールドに記載されている中継装置Ａドメイン、中継装置Ｂドメインおよび中継装置Ｃドメイン（それぞれＩＰアドレスを含む）を経路情報として取得する。

このとき、ｆｒｏｍ句とｂｙ句とで重複している中継装置Ｂドメインは二重に取得する必要はない。

また、Ｒｅｃｅｉｖｅｄフィールドに中継装置のＩＰアドレスが記載されていない場合、経路情報取得部２７３は、中継装置ドメインに対応するＩＰアドレスをＤＮＳサーバ（図示省略）から取得する。

【０２９４】

電子メールを最後に中継した中継装置がＲｅｃｅｉｖｅｄフィールドにｂｙ句を設定していない場合、経路情報取得部２７３は、この中継装置のドメインをＲｅｃｅｉｖｅｄフィールドから取得することができない。

そこで、経路情報取得部２７３は、この中継装置のＩＰアドレスとして、ＩＰパケットのパケットヘッダからＩＰパケットの送信元アドレスを取得する。

【０２９５】

図２６に戻り、転送経路学習処理の説明をＳ２７０２から続ける。

【０２９６】

Ｓ２７０２において、転送経路算出部２７１は、Ｓ２７０１で取得された経路情報に基づいて電子メールの転送経路を算出する。

転送経路算出部２７１は、例えば、以下のように電子メールの転送経路を算出する。

【０２９７】

ここで、ローカルネットワーク（プライベートネットワークまたはローカルエリアネットワークともいう）で用いられるローカルＩＰアドレス（プライベートＩＰアドレスともいう）を経路情報から抽出するために、ローカルＩＰリストが記憶装置に予め記憶されているものとする。

ローカルＩＰリストには、「１９２．１６８．…」、「１７２．１６．…」～「１７２．３１．…」、「１０．…」など、ローカルＩＰアドレスに用いられるアドレス（以下、「ローカルアドレス」という）を設定しておく。
転送経路算出部２７１は、このローカルＩＰリストを用いて、経路情報に含まれるＩＰアドレスからローカルＩＰアドレスを抽出する。
ローカルＩＰリストに含まれるいずれかのアドレスから始まるＩＰアドレスがローカルＩＰアドレスである。例えば、「１９２．１６８．ｘｘｘ．ｘｘｘ」「１７２．１６．ｘｘｘ．ｘｘｘ」～「１７２．３１．ｘｘｘ．ｘｘｘ」または「１０．ｘｘｘ．ｘｘｘ．ｘｘｘ」はローカルＩＰアドレスである。
転送経路算出部２７１は、抽出したローカルＩＰアドレス毎に、ローカルＩＰアドレスから、ローカルＩＰリストに設定されているローカルアドレスを抽出する。

【０２９８】
転送経路算出部２７１は、経路情報に含まれるＩＰアドレスのうちローカルＩＰアドレスとして抽出しなかった残りのＩＰアドレスを、グローバルＩＰアドレスとして抽出する。
グローバルＩＰアドレスは、グローバルネットワーク（例えば、インターネット８１）で用いられるＩＰアドレスである。
転送経路算出部２７１は、抽出したグローバルＩＰアドレス毎に、グローバルＩＰアドレス（３２ビット）の先頭から所定のバイト数（例えば、２４ビット）をネットワークアドレスとして抽出する。

【０２９９】
転送経路算出部２７１によって抽出されたローカルアドレスおよびグローバルアドレスが転送経路である。
以下、転送経路のうち１つ以上のローカルアドレスによって表される経路を「ローカル経路」といい、１つ以上のグローバルアドレスによって表される経路を「グローバル経路」という。
転送経路算出部２７１は、転送経路（ローカル経路およびグローバル経路）を示す転送経路データ２７１Ａを生成する。

【０３００】
図２８は、実施の形態５における転送経路データ２７１Ａの一例を示す図である。
図２８に示す転送経路データ２７１Ａは、ローカル経路としてローカルアドレスのリスト「IP_1、IP_2」を示し、グローバル経路としてグローバルアドレス（IP_3、IP_4）を示している。
ローカル経路を示すローカルアドレスのリストおよびグローバル経路を示すグローバルアドレスのリストは、電子メールの転送順（メールヘッダのＲｅｃｅｉｖｅｄフィールドの昇順）にアドレスを並べた順序有りリストであってもよいし、電子メールの転送順に関係なくアドレスを並べた順序無しリストであってもよい。
Ｓ２７０２の後、Ｓ２７０３に進む。

【０３０１】
Ｓ２７０３において、転送経路算出部２７１は、作成者ドメイン取得部２３から、電子メールの作成者ドメインを取得する。
Ｓ２７０３の後、Ｓ２７０４に進む。

【０３０２】
Ｓ２７０４において、転送経路算出部２７１は、メール通信取得部２１によって取得された電子メールの通信日時と、Ｓ２７０３で取得された作成者ドメインと、Ｓ２７０２で算出した転送経路（転送経路データ２７１Ａ）とを対応付けてメール通信記憶部２２に記憶する。
電子メールの通信日時とは、例えば、メール通信取得部２１が電子メールを取得した日時、または電子メールのメールヘッダに含まれる送信日時である。
Ｓ２７０４の後、Ｓ２７０５に進む。

【０３０３】
Ｓ２７０５において、ドメイン経路学習部２７２は、ドメイン経路リスト２７２Ａから、Ｓ２７０３で取得された作成者ドメインと同じドメインに対応付けられているドメイン経路を抽出する。
ドメイン経路学習部２７２は、Ｓ２７０２で算出した転送経路がドメイン経路リスト２７２Ａから抽出したいずれかのドメイン経路と同じ経路であるか否かを判定する。
【０３０４】
図２９は、実施の形態５におけるドメイン経路リスト２７２Ａの一例を示す図である。
図２９に示すように、ドメイン経路リスト２７２Ａは、作成者ドメインと、ドメイン経路（ローカル経路およびグローバル経路）と、ドメイン経路の使用日時とを対応付けている。
【０３０５】
転送経路がいずれかのドメイン経路と同じ経路である場合（ＹＥＳ）、ドメイン経路学習部２７２は、ドメイン経路リスト２７２Ａ（図２９参照）に設定されている当該ドメイン経路の使用日時を更新する。
例えば、ドメイン経路学習部２７２は、現在日時、メール通信取得部２１が電子メールを取得した日時または電子メールの送信日時を用いて当該使用日時を更新する。
これにより、ドメイン経路学習処理は終了する。
【０３０６】
転送経路がいずれのドメイン経路とも異なる経路である場合（ＮＯ）、Ｓ２７０６に進む。
【０３０７】
Ｓ２７０６において、ドメイン経路学習部２７２は、メール通信記憶部２２に記憶されている転送経路のうち、Ｓ２７０３で取得された作成者ドメインと同じドメインに対応付けられている転送経路を選択する。
【０３０８】
ドメイン経路学習部２７２は、Ｓ２７０３で取得された作成者ドメインと同じドメインに対応付けられている転送経路のうち、所定期間（例えば、直前の１カ月）の通信日時に対応付けられている転送経路を選択してもよい。つまり、ドメイン経路学習部２７２は、所定期間に通信された電子メールの転送経路を選択してもよい。
ドメイン経路学習部２７２は、電子メールの通信日時が新しい順に、所定数の転送経路を選択してもよい。
以下に、Ｓ２７０６の説明を続ける。
【０３０９】
ドメイン経路学習部２７２は、選択した転送経路のうち、Ｓ２７０２で算出された転送経路と同じ転送経路の数を計数する。
ドメイン経路学習部２７２は、計数した転送経路の数と所定の学習閾値（例えば、１０個）とを比較し、計数した転送経路の数が所定の学習閾値（例えば、１０個）以上であるか否かを判定する。
【０３１０】
転送経路の数が学習閾値以上である場合（ＹＥＳ）、Ｓ２７０７に進む。
転送経路の数が学習閾値未満である場合（ＮＯ）、ドメイン経路学習処理は終了する。
【０３１１】
Ｓ２７０７において、ドメイン経路学習部２７２は、Ｓ２７０２で算出した転送経路をドメイン経路としてドメイン経路リスト２７２Ａ（図２９参照）に設定する。
このとき、ドメイン経路学習部２７２は、Ｓ２７０３で取得した作成者ドメインと、Ｓ２７０２で算出した転送経路（ドメイン経路）と、ドメイン経路の使用日時とを対応付けて設定する。
例えば、ドメイン経路学習部２７２は、現在日時、メール通信取得部２１が電子メールを取得した日時または電子メールの送信日時をドメイン経路の使用日時として設定する。

Ｓ２７０２により、ドメイン経路学習処理は終了する。

【０３１２】

上記のドメイン経路学習処理（図２６参照）によって学習するドメイン経路は、転送経路の全経路、転送経路内のグローバル経路またはその両方のいずれであってもよい。

転送経路の全経路と転送経路内のグローバル経路との両方を学習する場合、以下のような条件で転送経路の全経路および転送経路内のグローバル経路が学習される。ここで、メール通信取得部２１が取得した転送経路を対象経路とする。

対象経路の全経路と一致する転送経路が学習閾値より多く記憶されている場合（Ｓ２７０６）、ドメイン経路学習部２７２は、対象経路の全経路（転送経路内のグローバル経路を含む）をドメイン経路としてドメイン経路リスト２７２Ａに設定する。

対象経路の全経路と一致する転送経路が学習閾値より少なく、対象経路とグローバル経路が一致する転送経路が学習閾値より多く記憶されている場合（Ｓ２７０６）、ドメイン経路学習部２７２は、対象経路内のグローバル経路だけをドメイン経路としてドメイン経路リスト２７２Ａに設定する。この場合、ドメイン経路リスト２７２Ａのローカル経路欄は空欄である。

【０３１３】

ドメイン経路学習部２７２は、定期的またはユーザに指定されたときなどの所定のタイミングでドメイン経路リスト２７２Ａ（図２９参照）を参照し、使用日時が現在日時より所定の保持時間以上前の日時であるドメイン経路をドメイン経路リスト２７２Ａから削除してもよい。これにより、ドメイン経路リスト２７２Ａのデータサイズを小さくすることができる。

【０３１４】

図３０は、実施の形態５における転送経路検査方法を示すフローチャートである。

実施の形態５における転送経路検査方法（詐称メール検出方法の一例）について、図３０に基づいて説明する。

【０３１５】

ここで、ドメイン経路学習部２７２は、ドメイン経路リスト２７２Ａを予め生成しているものとする。

【０３１６】

Ｓ２７１０において、経路情報取得部２７３は、判定対象メールから中継装置のＩＰアドレスおよび判定対象メールの送信元アドレスなどの経路情報を取得する。

経路情報の取得方法は、ドメイン経路学習処理（図２６参照）のＳ２７０１と同様である。

Ｓ２７１０の後、Ｓ２７２０に進む。

【０３１７】

Ｓ２７２０において、転送経路算出部２７１は、Ｓ２７１０で取得された経路情報に基づいて、判定対象メールの転送経路を算出する。

転送経路の算出方法は、ドメイン経路学習処理（図２６参照）のＳ２７０２と同様である。

Ｓ２７２０の後、Ｓ２７３０に進む。

【０３１８】

Ｓ２７３０において、転送経路検査スコア決定部２７９は、作成者ドメイン取得部２３から判定対象メールの作成者ドメインを取得する。

Ｓ２７３０の後、Ｓ２７３１に進む。

【０３１９】

Ｓ２７３１において、転送経路検査スコア決定部２７９は、ドメイン経路リスト２７２Ａ（図２９参照）から、Ｓ２７３０で取得した判定対象メールの作成者ドメインと同じドメインに対応付けられたドメイン経路を取得する。

Ｓ２７３１の後、Ｓ２７４０に進む。

【０３２０】

Ｓ２７４０において、転送経路検査スコア決定部２７９は、Ｓ２７２０で算出した転送経路がＳ２７３１で取得したいずれかのドメイン経路と同じ経路であるか否かを判定し、判定結果に基づいて転送経路検査スコアを決定する。

転送経路検査スコアは、判定対象メールが詐称メールである可能性の度合いを表す値である。

例えば、判定対象メールが詐称メールである可能性が高いほど転送経路検査スコアは高く、判定対象メールが詐称メールである可能性が低いほど転送経路検査スコアは低い。

【０３２１】

転送経路がドメイン経路と同じ経路であるか否かを判定する判定方法は、ドメイン経路学習処理（図２６参照）のＳ２７０５と同様である。

このとき、転送経路検査スコア決定部２７９は、転送経路の全経路がドメイン経路と同じであるか否かを判定すると共に、転送経路内のグローバル経路がドメイン経路内のグローバル経路と同じであるか否かを判定する。但し、転送経路検査スコア決定部２７９は、いずれか一方の判定だけを行っても構わない。

【０３２２】

図３１は、実施の形態５における転送経路検査スコア一覧表２７９Ａの一例を示す図である。

例えば、図３１に示すような転送経路検査スコア一覧表２７９Ａを記憶装置に予め記憶しておく。

転送経路検査スコア一覧表２７９Ａは、条件と転送経路検査スコアとを対応付けている。

転送経路検査スコア決定部２７９は、Ｓ２７２０で算出した転送経路とＳ２７３１で取得したドメイン経路との関係に基づいて、転送経路検査スコアを転送経路検査スコア一覧表２７９Ａから取得する。

【０３２３】

転送経路の全経路（ローカル経路およびグローバル経路）がいずれかのドメイン経路と一致する場合、転送経路検査スコア決定部２７９は、判定対象メールが詐称メールである可能性が低いことを意味する転送経路検査スコア「０点」を転送経路検査スコア一覧表２７９Ａから取得する。

転送経路のグローバル経路がいずれかのドメイン経路のグローバル経路と一致する場合、転送経路検査スコア決定部２７９は、判定対象メールが詐称メールである可能性が比較的低いことを意味する転送経路検査スコア「２点」を転送経路検査スコア一覧表２７９Ａから取得する。

転送経路のグローバル経路がいずれのドメイン経路のグローバル経路とも一致しない場合、転送経路検査スコア決定部２７９は、判定対象メールが詐称メールである可能性が高いことを意味する転送経路検査スコア「４点」を転送経路検査スコア一覧表２７９Ａから取得する。

また、Ｓ２７３１でドメイン経路が取得されなかった場合、転送経路検査スコア決定部２７９は、判定対象メールが詐称メールであるか否かを判定できないことを意味する転送経路検査スコア「０点」を転送経路検査スコア一覧表２７９Ａから取得する。

Ｓ２７４０の後、Ｓ２７５０に進む。

【０３２４】

Ｓ２７５０において、詐称判定部２８は、Ｓ２７４０で決定された転送経路検査スコアに基づいて、判定対象メールが詐称メールであるか否かを判定する。

例えば、詐称判定部２８は、Ｓ２７４０で決定された判定対象メールの転送経路検査スコアと他の実施の形態で決定される判定対象メールのスコアとの合計値と、所定の詐称評価閾値とを比較する。判定対象メールのスコアの合計値が所定の詐称評価閾値より大きい場合、詐称判定部２８は、判定対象メールが詐称メールであると判定する。

但し、詐称判定部２８は、転送経路検査スコアを所定の詐称評価閾値と比較し、判定対象メールが詐称メールであるか否かを判定しても構わない。

Ｓ２７５０により、転送経路検査方法の処理は終了する。

【０３２５】

ドメイン経路学習部２７２は、ドメイン経路を学習する対象の電子メールとして、判定対象メールを利用してもよい。

その場合、ドメイン経路学習部２７２は、転送経路検査方法（図３０参照）で得られた判定対象メールの転送経路と作成者ドメインとを記憶し、ドメイン経路学習処理（図２６参照）のＳ２７０５からＳ２７０７を実行すればよい。

【０３２６】

以上説明した詐称メール検出装置（２０）は、

ネットワークを介した通信のうち、メール転送プロトコルである通信を取得するメール通信取得部（２１）と、

上記メール通信取得部が取得した通信によって転送される電子メールの作成者フィールドに記載された作成者が属する作成者ドメインを取得する作成者ドメイン取得部（２３）と、

上記電子メールの転送経路を算出する転送経路算出部（２７１）と、

判定対象メールと作成者ドメインが同じ１以上の電子メールのうち、上記判定対象メールと転送経路が一致する経路一致メールの数を計数する経路一致計数部（ドメイン経路学習部２７２）と、

上記経路一致計数部が計数した経路一致メールの数が所定の経路一致閾値より小さい場合に、上記判定対象メールが作成者を詐称した詐称メールである可能性があると判定する詐称判定部（２８，転送経路検査スコア決定部２７９）とを有する。

【０３２７】

上記詐称メール検出装置（２０）は、

上記電子メールの中継装置フィールドに記載された中継装置ドメインを取得する中継装置ドメイン取得部（経路情報取得部２７３）を有し、

上記転送経路算出部（２７１）は、上記中継装置ドメイン取得部が取得した中継装置ドメインに基づいて、上記転送経路を算出する。

【０３２８】

上記詐称メール検出装置（２０）は、

上記メール通信取得部が取得した通信に基づいて、上記通信を構成するパケットの送信元アドレスを取得するパケット送信元取得部（経路情報取得部２７３）を有し、

上記転送経路算出部（２７１）は、上記パケット送信元取得部が取得した送信元アドレスに基づいて、上記転送経路を算出する。

【０３２９】

上記転送経路算出部（２７１）は、上記電子メールを中継した１以上のホスト装置のネットワークアドレスを算出し、算出したネットワークアドレスの順序なしリストまたは順序ありリストを、上記転送経路とする。

【０３３０】

上記転送経路算出部（２７１）は、サブネットマスクが所定の値であるものと仮定して、上記ネットワークアドレスを算出する。

【０３３１】

上記詐称判定部（２８，２７９）は、上記判定対象メールと作成者ドメインが同じ電子メールのうち転送経路が互いに一致する電子メールの数が上記経路一致閾値以上である転送経路が存在し、かつ、上記経路一致計数部が計数した経路一致メールの数が上記経路一致閾値より小さい場合に、上記判定対象メールが作成者を詐称した詐称メールである可能性があると判定する。

【０３３２】

上記詐称判定部（２８，２７９）は、

判定対象メールについて詐称評価値を算出し、上記経路一致計数部が計数した経路一致メールの数が所定の経路一致閾値より小さい場合に、上記詐称評価値に所定の値を加算す

る詐称評価値算出部（２８１，２７９）と、
上記詐称評価値算出部が算出した詐称評価値が所定の詐称評価閾値より大きい場合に、上記判定対象メールが作成者を詐称した詐称メールである可能性があると判定する詐称評価値判定部（２８３）とを有する。
【０３３３】
上記詐称メール検出装置（２０）は、
上記転送経路算出部が算出した転送経路からプライベートネットワーク内における転送経路を除外したグローバル経路について、上記判定対象メールと作成者ドメインが同じ１以上の電子メールのうち、上記判定対象メールと上記グローバル経路が一致する経路部分一致メールの数を計数する経路部分一致計数部（ドメイン経路学習部２７２）を有し、
上記詐称評価値算出部（２７９）は、
上記経路一致計数部が計数した経路一致メールの数が所定の経路一致閾値より小さく、かつ、上記経路部分一致計数部が計数した経路部分一致メールの数が所定の経路部分一致閾値以上である場合に、第一の値を上記詐称評価値に加算し、上記経路一致計数部が計数した経路一致メールの数が所定の経路一致閾値より小さく、かつ、上記経路部分一致計数部が計数した経路部分一致メールの数が所定の経路部分一致閾値より小さい場合に、上記第一の値よりも大きい第二の値を上記詐称評価値に加算する。
【０３３４】
上記経路一致計数部（２７２）は、上記１以上の電子メールのうち、所定の期間内に転送された上記経路一致メールの数だけを計数する。
【０３３５】
上記経路一致計数部（２７２）は、転送時刻が新しい順に所定の数以内の電子メールのなかで、上記判定対象メールと作成者ドメインが同じ経路一致メールの数を計数する。
【０３３６】
実施の形態５により、転送経路検査部２７は、電子メールの作成者ドメイン毎に、電子メールが転送される可能性が高い転送経路をドメイン経路として学習することができる。
また、転送経路検査部２７は、電子メールの転送経路と学習したドメイン経路とに基づいて、電子メールが詐称メールである可能性の度合いを表す転送経路検査スコアを決定することができる。
そして、詐称判定部２８は、転送経路検査スコアに基づいて、電子メールが詐称メールであるか否かを判定することができる。
【０３３７】
電子メールは、通常、同一の送信者ドメインからは同一の経路で届く。このため、送信者ドメインごとの転送経路を学習しておき、異なる経路で届いた電子メールを、詐称メールの可能性があると判定する。
しかし、ローカルネットワーク内での経路は、人や組織によって異なる可能性がある。そこで、転送経路を、グローバル経路とローカル経路とに分け、全経路が一致した転送経路と、グローバル経路のみが一致した転送経路とを学習する。判定対象メールが詐称メールであるか否かの判定は、全経路が一致する場合、グローバル経路は一致するがローカル経路は一致しない場合、グローバル経路も一致しない場合の３段階で行う。
これにより、判定対象メールが詐称メールであるか否かの判定精度を高くすることができ、標的型サイバー攻撃による秘密情報の漏洩を防ぐことができる。
【０３３８】
実施の形態６．
実施の形態６について、図３２～図４０を用いて説明する。
この実施の形態では、実施の形態１で説明した不正通信検出装置３０の構成例について、詳しく説明する。
なお、実施の形態１～実施の形態５と共通する構成には、同一の符号を付し、説明を省略する場合がある。
【０３３９】

図３２は、本実施の形態に係る不正通信検出装置３０のブロック構成図である。
不正通信検出装置３０は、通信取得部３１、通信記憶部３１ａ、特性値算出部３２、特性値蓄積部３２ａ、統計量算出部３３、統計量記憶部３３ａ、通信計数部３５、通信数蓄積部３５ａ、通信数統計量算出部３６、通信数統計量記憶部３６ａ、不正判定部３７、分析結果テーブル３７ａを備える。

【０３４０】
通信記憶部３１ａ、特性値蓄積部３２ａ、統計量記憶部３３ａ、通信数蓄積部３５ａ、通信数統計量記憶部３６ａ、分析結果テーブル３７ａは記憶装置に備えられている。

【０３４１】
通信取得部３１は、入力装置９２を用いて、端末装置１２がウェブプロキシ装置１５（図２参照）やインターネット８１を介して送受信するウェブ通信を取得する。ウェブプロキシ装置１５は、端末装置１２（図１参照）からの要求にしたがって、外部のウェブサーバ装置８３（図１参照）からウェブページを取得し、端末装置１２に対して送信する。通信取得部３１は、特に、端末装置１２からウェブサーバ装置８３へ向けて送信するリクエスト側のウェブ通信を取得する。

【０３４２】
例えば、通信取得部３１は、端末装置１２がウェブプロキシ装置１５に対して送信するＩＰ（インターネットプロトコル）パケットをキャプチャする。ＩＰパケットのヘッダ部分には、バージョン、ヘッダ長、サービスタイプ、全長、識別子、フラグ、断片位置、生存時間、プロトコル、チェックサム、送信元アドレス、宛先アドレス、オプションなどの情報が格納されている。

【０３４３】
通信取得部３１は、キャプチャしたＩＰパケットを解析して、トランスポート層のプロトコルにおけるメッセージを再構成する。トランスポート層のプロトコルには、例えばＴＣＰ（伝送制御プロトコル）やＵＤＰ（ユーザデータグラムプロトコル）などがある。

【０３４４】
通信取得部３１は、再構成したトランスポート層におけるメッセージを解析して、アプリケーション層のプロトコルにおけるメッセージを再構成する。アプリケーション層のプロトコルは、端末装置１２のウェブブラウザとウェブサーバ装置８３との間のプロトコルであり、例えば、ＨＴＴＰ（ハイパーテキスト転送プロトコル）などである。

【０３４５】
通信取得部３１は、アプリケーション層のプロトコルにおけるメッセージを再構成することにより、再構成したメッセージのなかから、所定のメッセージ（例えば、ＨＴＴＰリクエスト）を取得する。例えば、通信取得部３１は、ウェブプロキシ装置１５からウェブサーバ装置８３へ送信されるＨＴＴＰによるリクエスト（以下、ＨＴＴＰリクエスト３１０とする）を取得する。通信取得部３１は、取得したＨＴＴＰリクエスト３１０を、通信記憶部３１ａに蓄積する。

【０３４６】
特性値算出部３２は、通信取得部３１が取得したＨＴＴＰリクエスト３１０（通信の一例）を通信記憶部３１ａから入力する。特性値算出部３２は、入力したＨＴＴＰリクエスト３１０（以下、判定対象のＨＴＴＰリクエスト３１０ともいう）に基づいて、ＨＴＴＰリクエスト３１０の特性値３２０を算出する。

【０３４７】
図３３は、本実施の形態におけるＨＴＴＰリクエスト３１０の一例を示す図であり、（ａ）はゲットメソッドによるＨＴＴＰリクエスト３１０（以下「ゲットリクエスト３１０ｇ」と呼ぶ。）及びゲットリクエスト３１０ｇから取得されるＵＲＩ３１１の一例、（ｂ）はポストメソッドによるＨＴＴＰリクエスト３１０（以下「ポストリクエスト３１０ｐ」と呼ぶ。）及びポストリクエスト３１０ｐから取得されるＵＲＩ３１１の一例である。図３３を用いて、特性値算出部３２による特性値３２０の算出について説明する。

【０３４８】

図３３（ａ）（ｂ）に示すように、ＨＴＴＰリクエスト３１０は、先頭から、メソッド名３１４、リソース名、通信プロトコルバージョンを備える。ＨＴＴＰリクエスト３１０の「Ｈｏｓｔ」フィールドには、宛先ホスト３１７のホスト名が設定されている。

また、「Ｕｓｅｒ－Ａｇｅｎｔ」フィールドには、ＵＡが設定されている。ＵＡは、そのＨＴＴＰリクエストを生成したウェブブラウザなどのプログラムを識別するための文字列である。

【０３４９】

メソッド名３１４には、ＨＴＴＰリクエスト３１０がゲットメソッドによるものの場合には「ＧＥＴ」が設定され、ポストメソッドによるものの場合には「ＰＯＳＴ」が設定される。

【０３５０】

リソース名には、宛先ホストのリソース名が設定される。

リソース名は、絶対パス文字列を含む。リソース名は、クエリー文字列を含む場合がある。クエリー文字列は、リソース名のうち、文字「？」より後ろの部分である。クエリー文字列は、パラメータを表わす。リソース名がクエリー文字列を含む場合、絶対パス文字列は、リソース名のうち、文字「？」より前の部分である。

ＨＴＴＰリクエスト３１０がゲットリクエスト３１０ｇの場合のクエリー文字列をＧＥＴパラメータ３１２と呼ぶ。

リソース名に文字「？」が含まれない場合、リソース名は、クエリー文字列を含まない。その場合、リソース名全体が絶対パス文字列である。

【０３５１】

なお、リソース名は、「ｈｔｔｐ：」などのプロトコル文字列及びホスト名を含む場合がある。リソース名がプロトコル文字列及びホスト名を含む場合、プロトコル文字列及びホスト名は、絶対パス文字列の前に付加されている。

【０３５２】

図３３（ａ）に示すように、ゲットリクエスト３１０ｇの宛先ホスト名とリソース名と連結した文字列をＵＲＩ３１１（統一資源識別子）と呼ぶ。ＵＲＩ３１１のうち、ＧＥＴパラメータ３１２（及び文字「？」）を除いた部分をＵＲＬ３１３と呼ぶ。

【０３５３】

図３３（ａ）に示すように、ゲットリクエスト３１０ｇのＵＲＩ３１１「ｗｗｗ．ａａａａａ．ｃｏ．ｊｐ／ｍｙｓｅｒｖｌｅｔ１？ｎａｍｅ＝ｘｙｚ＆ｃｏｌｏｒ＝ｒｅｄ」は、ＵＲＬ３１３部分「ｗｗｗ．ａａａａａ．ｃｏ．ｊｐ／ｍｙｓｅｒｖｌｅｔ１」と、ＧＥＴパラメータ３１２部分「ｎａｍｅ＝ｘｙｚ＆ｃｏｌｏｒ＝ｒｅｄ」とから構成される。

【０３５４】

図３３（ｂ）に示すように、リソース名にクエリー文字列が含まれない場合は、ＵＲＩ３１１とＵＲＬ３１３とは、同一の文字列である。

【０３５５】

図３３（ｂ）に示すように、ポストリクエスト３１０ｐのＵＲＩ３１１「ｗｗｗ．ａａａａａ．ｃｏ．ｊｐ／ｍｙｓｅｒｖｌｅｔ２」は、宛先を示すＵＲＬ３１３部分のみであり、ＧＥＴパラメータ３１２部分はない。

ポストリクエスト３１０ｐは、ＧＥＴパラメータ３１２を含まない代わりに、ポストメッセージ３１１ｐをメッセージボディに含む。ポストメッセージ３１１ｐは、パラメータを表わす。

【０３５６】

ＵＲＩ３１１のＵＲＬ３１３は、宛先（宛先ホスト３１７、宛先サイト、宛先ウェブサーバ装置等ともいう）を示している。

【０３５７】

特性値算出部３２は、入力した判定対象のＨＴＴＰリクエスト３１０を解析して、特性値３２０を取得する。特性値３２０は、例えば、ＨＴＴＰリクエスト３１０のＵＲＩ全体

長３２１、ＧＥＴパラメータ長３２２、ＵＲＬ長３２３、リクエスト全体長３２４等である。

【０３５８】

ＵＲＩ全体長３２１とは、ＵＲＩ３１１全体の長さのことである。例えば、特性値算出部３２は、入力した判定対象のＨＴＴＰリクエスト３１０を解析して、ＵＲＩ３１１を取得する。特性値算出部３２は、取得したＵＲＩ３１１に基づいて、ＵＲＩ全体長３２１を算出する。

ＧＥＴパラメータ長３２２とは、ＧＥＴパラメータ３１２の長さ（クエリー文字列の長さ）のことである。例えば、特性値算出部３２は、取得したＵＲＩ３１１からクエリー文字列を抽出する。特性値算出部３２は、抽出したクエリー文字列に基づいて、ＧＥＴパラメータ長３２２を算出する。

ＵＲＬ長３２３とは、ＵＲＬ３１３の長さのことである。例えば、特性値算出部３２は、取得したＵＲＩ３１１からＵＲＬ３１３を抽出する。特性値算出部３２は、抽出したＵＲＬ３１３に基づいて、ＵＲＬ長３２３を算出する。

リクエスト全体長３２４とは、ＨＴＴＰリクエスト３１０全体の長さのことである。例えば、特性値算出部３２は、入力したＨＴＴＰリクエスト３１０に基づいて、リクエスト全体長３２４を算出する。

【０３５９】

例えば、特性値算出部３２は、１つのＨＴＴＰリクエスト３１０に対して、ＵＲＩ全体長３２１と、ＧＥＴパラメータ長３２２と、ＵＲＬ長３２３と、リクエスト全体長３２４とを、特性値３２０として算出する。なお、特性値算出部３２は、ＵＲＩ全体長３２１と、ＧＥＴパラメータ長３２２と、ＵＲＬ長３２３と、リクエスト全体長３２４とのうち少なくともいずれか１つを特性値３２０として算出する構成であってもよい。

【０３６０】

特性値蓄積部３２ａは、特性値算出部３２により算出された特性値３２０を蓄積する。特性値算出部３２は、１つのＨＴＴＰリクエスト３１０について、１つの特性値情報を特性値蓄積部３２ａに記憶させる。特性値情報は、宛先ホスト３１７と、メソッド名３１４と、ＵＲＩ全体長３２１と、ＧＥＴパラメータ長３２２と、ＵＲＬ長３２３と、リクエスト全体長３２４とを含む。特性値蓄積部３２ａには、端末装置１２のウェブブラウザとウェブサーバ装置８３との間の通信（ＨＴＴＰリクエスト３１０）に対応付けられた特性値情報（ＵＲＩ全体長３２１、ＧＥＴパラメータ長３２２、ＵＲＬ長３２３、リクエスト全体長３２４などの特性値３２０を含む。）が蓄積される。特性値蓄積部３２ａは、多数のＨＴＴＰリクエスト３１０についての特性値情報を記憶する。

【０３６１】

統計量算出部３３は、特性値算出部３２が算出した１つ以上の通信（ＨＴＴＰリクエスト３１０）に対応付けられた特性値３２０に基づいて、統計量３３０を算出する。統計量算出部３３が算出する統計量３３０には、例えば、特性値の平均値や標準偏差（または分散）などがある。

【０３６２】

統計量算出部３３は、統計量３３０として、特性値蓄積部３２ａに蓄積されている１つ以上の通信（ＨＴＴＰリクエスト３１０）に対応付けられた特性値３２０を平均した平均値と、１つ以上の通信（ＨＴＴＰリクエスト３１０）に対応付けられた特性値３２０の標準偏差とを演算装置９５により算出する。

【０３６３】

統計量算出部３３は、特性値蓄積部３２ａに蓄積されたすべての通信についての特性値３２０に基づく統計量３３０を算出してもよいし、所定の種類の通信についての特性値３２０だけを抽出して統計量３３０を算出してもよい。例えば、統計量算出部３３は、すべてのＨＴＴＰリクエスト３１０について、ＵＲＩ全体長３２１の統計量３３０を算出する。統計量算出部３３は、ゲットリクエスト３１０ｇについて、リクエスト全体長３２４の統計量３３０を算出する。また、統計量算出部３３は、ポストリクエスト３１０ｐについ

ても、リクエスト全体長３２４の統計量を算出する。

【０３６４】

統計量算出部３３は、特性値蓄積部３２ａに蓄積されている特性値情報によって表わされる特性値のうち、例えば、ＵＲＩ全体長３２１、ＧＥＴパラメータ長３２２、ＵＲＬ長３２３について、それぞれの平均値及び標準偏差を統計量３３０として演算装置９５により算出する。

【０３６５】

図３３（ａ）（ｂ）に示すように、ＨＴＴＰリクエスト３１０には、ゲットメソッドによるゲットリクエスト３１０ｇと、ポストメソッドによるポストリクエスト３１０ｐとがある。

【０３６６】

統計量算出部３３は、特性値蓄積部３２ａに蓄積されている特性値情報によって表わされる特性値のうち、例えば、リクエスト全体長３２４について、メソッド名３１４が「ＧＥＴ」であるＨＴＴＰリクエスト３１０（すなわち、ゲットリクエスト３１０ｇ）についてのリクエスト全体長３２４だけの平均値及び標準偏差を、統計量３３０として算出する。また、統計量算出部３３は、メソッド名３１４が「ＰＯＳＴ」であるＨＴＴＰリクエスト３１０（すなわち、ポストリクエスト３１０ｐ）についてのリクエスト全体長３２４だけの平均値及び標準偏差を、統計量３３０として算出する。

【０３６７】

統計量算出部３３が統計量３３０を算出するタイミングは、例えば、特性値算出部３２から判定対象のＨＴＴＰリクエスト３１０の特性値３２０が出力されるたびである。すなわち、統計量算出部３３は、特性値算出部３２から特性値３２０が出力されるたびに、出力された特性値３２０を統計量３３０算出の母集団に含め、最新のデータに基づく統計量３３０を算出する。

【０３６８】

統計量算出部３３は、判定対象のＨＴＴＰリクエスト３１０がゲットメソッドである場合にはゲットリクエスト３１０ｇについてのリクエスト全体長３２４の平均値及び標準偏差を算出する。一方、統計量算出部３３は、判定対象のＨＴＴＰリクエスト３１０がポストメソッドである場合にはポストリクエスト３１０ｐについてのリクエスト全体長３２４の平均値及び標準偏差を算出する。

統計量算出部３３は、判定対象のＨＴＴＰリクエスト３１０がゲットメソッドであるかポストメソッドであるかにかかわらず、ＵＲＩ全体長３２１、ＧＥＴパラメータ長３２２、ＵＲＬ長３２３などの平均値及び標準偏差を算出する。

【０３６９】

統計量記憶部３３ａは、統計量算出部３３により算出された統計量３３０を記憶する。統計量算出部３３が算出する統計量３３０は、例えば、ＵＲＩ全体長３２１の平均値及び標準偏差、ＧＥＴパラメータ長３２２の平均値及び標準偏差、ＵＲＬ長３２３の平均値及び標準偏差、ゲットリクエスト３１０ｇのリクエスト全体長３２４の平均値及び標準偏差、ポストリクエスト３１０ｐのリクエスト全体長３２４の平均値及び標準偏差である。統計量算出部３３は、算出した統計量３３０を統計量記憶部３３ａに記憶する。

【０３７０】

統計量算出部３３は、統計量３３０を算出すると、統計量記憶部３３ａに既に記憶されている統計量３３０を、新たに算出した最新の統計量３３０に更新する。統計量３３０は母集団が大きいほど信頼性が高いと考えられるので、統計量記憶部３３ａには常に一番信頼性の高い統計量３３０（ＵＲＩ全体長３２１の平均値及び標準偏差、ＧＥＴパラメータ長３２２の平均値及び標準偏差、ＵＲＬ長３２３の平均値及び標準偏差、ゲットリクエスト３１０ｇのリクエスト全体長３２４の平均値及び標準偏差、ポストリクエスト３１０ｐのリクエスト全体長３２４の平均値及び標準偏差）が記憶されていることになる。

【０３７１】

通信計数部３５は、所定の期間内に通信取得部３１が取得した通信の数を、通信の宛先

ごとに計数する。例えば、通信計数部３５は、所定の期間（例えば、２４時間とする）に取得したＨＴＴＰリクエスト３１０の数を、宛先（以下、宛先ホスト３１７ともいう）ごとに計数し、所定期間通信数３５０として通信数蓄積部３５ａに蓄積する。所定の期間は、例えば、６時間、１２時間、１週間、３週間、１ヶ月等、適宜設定することができるものとする。通信数蓄積部３５ａには、宛先ホスト３１７ごとに、複数の所定期間通信数３５０が蓄積される。

【０３７２】

通信数統計量算出部３６は、通信数蓄積部３５ａに蓄積されている宛先ホスト３１７ごとの複数の所定期間通信数３５０の通信数統計量３６０（統計量の一例）を宛先ホスト３１７ごとに算出する。通信数統計量算出部３６は、宛先ホスト３１７ごとの複数の所定期間通信数３５０の平均値と標準偏差とを算出し、標準偏差を平均値で割った変動係数を宛先ホスト３１７ごとの通信数統計量３６０として演算装置９５により算出する。通信数統計量算出部３６は、宛先ホスト３１７ごとの通信数統計量３６０を通信数統計量記憶部３６ａに記憶する。

【０３７３】

通信数統計量算出部３６が通信数統計量３６０を算出するタイミングは、例えば、通信計数部３５が所定期間通信数３５０を通信数蓄積部３５ａに蓄積したタイミングである。

【０３７４】

不正判定部３７は、特性値分析部３７１、通信数分析部３７２、通信種別分析部３７３を備える。

【０３７５】

特性値分析部３７１は、統計量記憶部３３ａに記憶されている統計量３３０に基づいて、判定対象のＨＴＴＰリクエスト３１０の特性値３２０（以下、判定対象特性値３２５とする）が異常値であるか否かを演算装置９５により判定する。特性値分析部３７１は、判定対象特性値３２５が異常値であると判定した場合に、判定対象のＨＴＴＰリクエスト３１０が不正通信の可能性があると判定する。

【０３７６】

特性値分析部３７１は、例えば、判定対象特性値３２５が、標準偏差に所定の定数を乗じた値を平均値に加えた値よりも大きい場合に、判定対象特性値３２５が異常値であると判定する。あるいは、特性値分析部３７１は、判定対象特性値３２５が、標準偏差に所定の定数を乗じた値を平均値から差し引いた値よりも小さい場合に、判定対象特性値３２５が異常値であると判定する。あるいは、特性値分析部３７１は、上記２つの場合のどちらであっても、判定対象特性値３２５が異常値であると判定する。

例えば、特性値分析部３７１は、判定対象特性値３２５と平均値Ｘとの差が、標準偏差σの３倍以内である場合には正常と判定し、判定対象特性値３２５と平均値Ｘとの差が、標準偏差σの３倍を超える場合には異常値であると判定する。

【０３７７】

特性値３２０の分布が正規分布であると仮定すると、特性値３２０と平均値Ｘとの差が３σ以下である確率は、９９．７％である。特性値３２０がＸ＋３σより大きい確率は０．１５％、特性値３２０がＸ－３σより小さい確率は同じく０．１５％である。したがって、特性値３２０と平均値Ｘとの差が３σより大きいケースは、稀にしか発生しない。

【０３７８】

なお、標準偏差に乗じる所定の定数は、３に限らず、例えば２など、０より大きい実数であればよい。例えば、特性値３２０と平均値Ｘとの差が２σ以下である確率は、９５％である。特性値３２０がＸ＋２σより大きい確率は２．５％、特性値３２０がＸ－２σより小さい確率は同じく２．５％である。したがって、特性値３２０と平均値Ｘとの差が２σより大きいケースは、３σより大きいケースよりは頻繁であるが、やはり稀にしか発生しない。

【０３７９】

標的型サイバー攻撃に使われるコンピュータウィルスは、ローカルネットワークシステ

ム１０の構造などを調査し、調査結果をＨＴＴＰリクエストの形式で、攻撃者のサーバ装置に対して送信する。コンピュータウィルスは、調査結果を表わす情報を、例えばＧＥＴパラメータ３１２やポストメッセージ３１１ｐなど、ＨＴＴＰリクエストのどこか埋め込んで送信する。このため、コンピュータウィルスが送信するＨＴＴＰリクエストのＧＥＴパラメータ長３２２やリクエスト全体長３２４などは、通常のＨＴＴＰリクエストと比べて大きくなる可能性が高い。

そこで、これらの特性値３２０が異常に大きい場合は、標的型サイバー攻撃のコンピュータウィルスによる不正通信である可能性がある。

【０３８０】

逆に、これらの特性値３２０が異常に小さい場合も、なんらかの偽装が行われている可能性がある。すなわち、標的型サイバー攻撃のコンピュータウィルスによる不正通信である可能性がある。

【０３８１】

そこで、特性値分析部３７１は、判定対象特性値３２５が異常値であるか否かを判定し、異常値である場合に、判定対象のＨＴＴＰリクエスト３１０が不正通信の可能性があると判定する。

【０３８２】

判定対象特性値３２５が異常値であるか否かの判定に用いる閾値は、多数のＨＴＴＰリクエストの特性値３２０から算出した統計量３３０に基づいて算出する。これにより、あらかじめ定めた閾値を用いる場合よりも適切な閾値を使うことができるので、不正通信の可能性を精度よく判定することができる。

【０３８３】

なお、統計量算出部３３が算出した統計量３３０が、特性値蓄積部３２ａに蓄積された通信のうち所定の種類のＨＴＴＰリクエストについての特性値３２０だけを抽出して算出したものである場合には、特性値分析部３７１は、判定対象のＨＴＴＰリクエスト３１０の種類に応じて、それと同じ種類のＨＴＴＰリクエストについての特性値３２０から算出した統計量３３０に基づいて閾値を算出し、判定対象特性値３２５と比較する。

【０３８４】

例えば、統計量算出部３３は、リクエスト全体長３２４について、ゲットリクエスト３１０ｇについての統計量３３０と、ポストリクエスト３１０ｐについての統計量３３０とを算出する。

判定対象のＨＴＴＰリクエスト３１０がゲットリクエストである場合、特性値分析部３７１は、判定対象のＨＴＴＰリクエスト３１０から算出したリクエスト全体長３２４を、ゲットリクエスト３１０ｇについての統計量３３０から算出した閾値と比較する。また、判定対象のＨＴＴＰリクエスト３１０がゲットリクエストである場合、特性値分析部３７１は、判定対象のＨＴＴＰリクエスト３１０から算出したリクエスト全体長３２４を、ポストリクエスト３１０ｐについての統計量３３０から算出した閾値と比較する。

【０３８５】

リクエスト全体長３２４は、メソッドによって大きく異なることが予想される。

このように通信の種類によって大きく異なる可能性がある特性値３２０の場合、特性値３２０が正規分布していると仮定することができない。したがって、通信の種類に関わらず算出した統計量３３０を使ったのでは、よい閾値を算出することができない。

そこで、そのような特性値３２０については、通信を種類によって分類し、それぞれの種類の通信についての統計量３３０を算出する。

それぞれの分類のなかでは、特性値３２０が正規分布しているとの仮定が成り立つ。これにより、通信の種類に関わらず算出した統計量３３０を用いる場合よりも適切な閾値を使うことができるので、不正通信の可能性を精度よく判定することができる。

【０３８６】

特性値分析部３７１は、判定対象のＨＴＴＰリクエスト３１０の判定対象特性値３２５（ＵＲＩ全体長３２１、ＧＥＴパラメータ長３２２、ＵＲＬ長３２３、リクエスト全体長

３２４）についての分析結果を分析結果テーブル３７ａに記憶する。不正判定部３７による分析結果テーブル３７ａへの書込処理については後述する。

【０３８７】

通信数分析部３７２は、１つ１つのＨＴＴＰリクエストについて不正通信の可能性があるかどうかを判定するのではなく、ある宛先に対する１つ以上のＨＴＴＰリクエストを全体として見て、不正通信の可能性があるか否かを判定する。

【０３８８】

例えば、通信数分析部３７２は、いずれかの宛先（宛先ホスト３１７）について、通信計数部３５が計数した所定期間通信数３５０が１である場合に、不正通信の可能性があると判定する。通信数分析部３７２は、通信計数部３５が通信数蓄積部３５ａに蓄積した所定期間通信数３５０が１であると判定した場合に、その宛先ホスト３１７に対する通信が不正通信である可能性があると判定する。

【０３８９】

標的型サイバー攻撃に使われるコンピュータウィルスは、不正通信が露見しないように、様々な形での偽装を行う可能性がある。

例えば、同じサーバ装置に対して繰り返しＨＴＴＰリクエストを送信すると、不正通信を疑われる可能性があるので、攻撃者は、サーバ装置を複数用意しておき、コンピュータウィルスは、ＨＴＴＰリクエストを送信する相手のサーバ装置を、送信のたびに変える可能性がある。

そのような攻撃パターンの可能性を考えると、一定期間に１アクセスしかないサイトは、逆に怪しいと考えられる。通常のウェブページ閲覧に伴うＨＴＴＰリクエストであれば、そのページに含まれる画像データにアクセスしたり、同じサイトの別のページにアクセスしたりするため、同じサーバ装置に対して、一定期間に複数のＨＴＴＰリクエストを送信するほうが、むしろ普通である。

【０３９０】

そこで、通信数分析部３７２は、ある宛先ホスト３１７に対するアクセスが一定期間に１つしかない場合、不正通信の可能性があると判定する。

【０３９１】

通信数分析部３７２は、例えば、通信計数部３５が所定期間通信数３５０を算出する度に、所定期間通信数３５０の分析を実行する。通信数分析部３７２は、宛先ホスト３１７に対する通信が不正通信である可能性があると判定した場合に、その分析結果を分析結果テーブル３７ａに記憶する。不正判定部３７による分析結果テーブル３７ａへの書込処理については後述する。

【０３９２】

また、通信数分析部３７２は、通信数統計量算出部３６が算出した通信数統計量３６０（変動係数）が所定の閾値より小さい場合に、不正通信の可能性があると判定する。通信数分析部３７２は、通信数統計量算出部３６が通信数統計量３６０（変動係数）を算出する度に、通信数統計量３６０（変動係数）と所定の閾値とを演算装置９５により比較し、通信数統計量３６０（変動係数）が前記所定の閾値より小さい場合に、算出した通信数統計量３６０に対応する宛先ホスト３１７に対する通信が不正通信である可能性があると判定する。

【０３９３】

上述したように、標的型サイバー攻撃に使われるコンピュータウィルスは、ローカルネットワークシステム１０の構造などを調査し、調査結果をＨＴＴＰリクエストの形式で、攻撃者のサーバ装置に対して送信する。この送信は、定期的に行われるなど、決まったパターンにしたがって機械的に行われる可能性がある。

通信数統計量３６０（変動係数）の値が小さいということは、所定期間通信数３５０の変動が小さいことを意味し、アクセスが機械的であることを意味する。

そこで、通信数分析部３７２は、通信数統計量３６０（変動係数）が前記所定の閾値より小さい場合に、その宛先ホスト３１７に対する通信が不正通信である可能性があると判

定する。
【０３９４】
通信数分析部３７２は、宛先ホスト３１７に対する通信が不正通信である可能性があると判定した場合に、その分析結果を分析結果テーブル３７ａに記憶する。不正判定部３７による分析結果テーブル３７ａへの書込処理については後述する。
【０３９５】
通信種別分析部３７３は、判定対象のＨＴＴＰリクエスト３１０（通信）について、特性値分析部３７１や通信数分析部３７２とは異なる観点から、判定対象のＨＴＴＰリクエスト３１０が不正通信である可能性があるか否かを判定する。通信種別分析部３７３は、例えば、ＨＴＴＰリクエスト３１０（通信）のメソッド、フォーマット、ユーザエージェント（以下、ＵＡとする）、宛先（宛先ホスト３１７）等の内容に基づいて、不正通信の可能性を判定する。
【０３９６】
また、通信種別分析部３７３は、通信取得部３１が取得したＨＴＴＰリクエスト３１０（通信）がポストリクエスト３１０ｐである場合に、そのポストリクエスト３１０ｐは不正通信である可能性があると判定する。
例えば、セキュリティポリシーによりポストリクエスト３１０ｐの使用が禁止されている場合、ポストリクエスト３１０ｐがあるというだけで、その通信が不正通信であると判定できる。
【０３９７】
また、通信種別分析部３７３は、通信取得部３１が取得したＨＴＴＰリクエスト３１０（通信）のフォーマットがＨＴＴＰの規定に合致しない場合に、そのＨＴＴＰリクエスト３１０は不正通信である可能性があると判定する。
例えば、標的型サイバー攻撃のコンピュータウィルスは、表面上は、ＨＴＴＰにしたがったＨＴＴＰリクエスト３１０であると見せかけているが、内容をよく見ると、ＨＴＴＰの規定にしたがっていないものを送信する可能性がある。
【０３９８】
また、通信種別分析部３７３は、通信取得部３１が取得したＨＴＴＰリクエスト３１０（通信）のＵＡが所定のリスト（以下、ＵＡホワイトリストという）に含まれるＵＡでない場合に、そのＨＴＴＰリクエスト３１０は不正通信である判定する。通信種別分析部３７３は、あらかじめＵＡホワイトリストを記憶している。ＵＡホワイトリストに含まれるＵＡは、例えば、一般的なウェブブラウザが使用しているＵＡである。
【０３９９】
ＨＴＴＰリクエストのＵＡフィールドには、比較的自由な文字列を設定することができる。このため、標的型サイバー攻撃のコンピュータウィルスは、調査結果を表わす情報を、Ｕｓｅｒ－Ａｇｅｎｔフィールドに埋め込む可能性がある。
そこで、通信種別分析部３７３は、ＨＴＴＰリクエストのＵＡが、一般的なウェブブラウザが使用しているものと異なる場合、その通信が不正通信である可能性があると判定する。
【０４００】
また、通信種別分析部３７３は、通信取得部３１が取得したＨＴＴＰリクエスト３１０（通信）の宛先（宛先ホスト３１７）が所定のリスト（以下、ホストブラックリストという）に含まれる宛先である場合に、不正通信の可能性があると判定する。通信種別分析部３７３は、あらかじめホストブラックリストを記憶している。ホストブラックリストに含まれる宛先ホストは、例えば、不正サイトとして知られている宛先ホストである。
【０４０１】
ウェブブラウザには、利用者が間違って不正サイトにアクセスしないよう、不正サイトに対するアクセスを遮断する機能を有するものがある。その場合、ウェブブラウザは、不正サイトに対するＨＴＴＰリクエストを送信しないので、不正サイトに対するＨＴＴＰリクエストがあれば、それは、ウェブブラウザ以外のプログラムが送信したものである。し

たがって、そのＨＴＴＰリクエストを送信したプログラムが標的型サイバー攻撃のコンピュータウィルスである可能性がある。
そこで、通信種別分析部３７３は、ＨＴＴＰリクエストの宛先が、不正サイトである場合、その通信が不正通信である可能性があると判定する。
【０４０２】
なお、通信種別分析部３７３は、ＨＴＴＰリクエスト３１０（通信）がポストリクエスト３１０ｐである場合と、上記通信のフォーマットがＨＴＴＰの規定に合致しない場合と、上記通信のＵＡがＵＡホワイトリストに含まれるユーザエージェントでない場合と、宛先ホスト３１７がＨｏｓｔブラックリストに含まれる宛先ホスト３１７である場合とのうち、いずれかの場合に、不正通信の可能性があると判定する構成であってもよい。あるいは、通信種別分析部３７３は、４つの条件のうちの２つ、あるいは、３つの条件だけを判定する構成であってもよい。
【０４０３】
通信種別分析部３７３は、宛先ホスト３１７に対する通信が不正通信である可能性があると判定した場合に、その分析結果を分析結果テーブル３７ａに記憶する。不正判定部３７による分析結果テーブル３７ａへの書込処理については後述する。
【０４０４】
レポート生成部３８は、特性値分析部３７１、通信数分析部３７２、通信種別分析部３７３による分析結果に基づいて、レポート３８０を出力する。レポート生成部３８は、分析結果テーブル３７ａに基づいて、宛先ホスト３１７ごとに、特性値３２０（ＵＲＩ全体長３２１、ＧＥＴパラメータ長３２２、ＵＲＬ長３２３、リクエスト全体長３２４）が異常値と判定された件数、所定期間通信数３５０が異常値と判定された件数、通信種別３７４が異常であると判定された件数等が示されたレポート３８０を生成して出力する。このレポート３８０に基づいて、ローカルネットワークシステム１０の管理者は、例えば、コンピュータウィルスの駆除を行うなどの防御対策を講じることができる。これにより、標的型サイバー攻撃による被害を未然に防ぐことができる。
【０４０５】
図３４は、本実施の形態に係る不正通信検出装置３０の不正通信検出方法を示すフローチャートである。図３５は、本実施の形態に係る分析結果テーブル３７ａの構成の一例を示す図である。図３６は、本実施の形態に係る不正通信検出装置３０の特性値分析方法を示すフローチャートである。図３７は、本実施の形態に係る不正通信検出装置３０の通信数分析方法を示すフローチャートである。図３８は、本実施の形態に係る通信数蓄積部３５ａ及び通信数統計量記憶部３６ａの構成の一例を示す図である。図３９は、本実施の形態６に係る不正通信検出装置３０の通信種別分析方法を示すフローチャートである。
図３４～図３９を用いて、不正通信検出装置３０の不正通信検出方法の概要について説明する。
【０４０６】
図３４に示すように、不正通信検出装置３０の不正通信検出方法は、通信取得処理（Ｓ３１０）、特性値分析処理（Ｓ３２０）、通信数分析処理（Ｓ３３０）、通信種別分析処理（Ｓ３４０）、レポート生成処理（Ｓ３５０）を備える。
【０４０７】
通信取得処理（Ｓ３１０）において、通信取得部３１は、上述したようにＨＴＴＰリクエスト３１０を取得し、判定対象のＨＴＴＰリクエスト３１０として通信記憶部３１ａに記憶する。
【０４０８】
図３５は、本実施の形態に係る分析結果テーブル３７ａの構成の一例を示す図である。図３５に示すように、分析結果テーブル３７ａは、宛先ホスト名に対して、複数の項目が対応付けられている。複数の項目とは、リクエスト数、ＵＲＩ全体長、ＵＲＬ長、ＧＥＴパラメータ長、ゲットリクエスト全体長、ポストリクエスト全体長、リクエスト数＝１、リクエスト分散（通信数変動係数）、ＰＯＳＴ数、不正ＨＴＴＰ、不正ＵＡ、不正サイト

等である。項目は、リクエスト数、ＵＲＩ全体長、ＵＲＬ長、ＧＥＴパラメータ長、ゲットリクエスト全体長、ポストリクエスト全体長、リクエスト数＝１、通信数変動係数、ＰＯＳＴ数、不正ＨＴＴＰ、不正ＵＡ、不正サイトのうちの少なくともいずれかでもよい。

【０４０９】

通信取得部３１は、ＨＴＴＰリクエスト３１０を取得すると、ＨＴＴＰリクエスト３１０の「Ｈｏｓｔ」から（図３３参照）、宛先ホスト３１７を特定し、分析結果テーブル３７ａのなかに特定した宛先ホスト３１７があるか否かを演算装置９５により判定する。通信取得部３１は、分析結果テーブル３７ａのなかに特定した宛先ホスト３１７があると判定した場合には、特定した宛先ホスト３１７のレコードの「リクエスト数」の項目をカウントアップする。通信取得部３１は、特定した宛先ホスト３１７のレコードが分析結果テーブル３７ａに無いと判定した場合には、特定した宛先ホスト３１７のレコードを生成し、「リクエスト数」の項目に１を設定する。

【０４１０】

次に、図３６を用いて、特性値分析方法（特性値分析処理）（Ｓ３２０）について説明する。

【０４１１】

＜Ｓ３２１：特性値算出工程＞

特性値算出部３２は、通信記憶部３１ａから判定対象のＨＴＴＰリクエスト３１０を読み込む。特性値算出部３２は、判定対象のＨＴＴＰリクエスト３１０のＵＲＩ３１１（図３３参照）を取得する。

【０４１２】

特性値算出部３２は、ＵＲＩ３１１の全体の文字数を演算装置９５によりカウントし、ＵＲＩ全体長３２１として特性値蓄積部３２ａに書き込む。また、特性値算出部３２は、ＵＲＩ３１１のうち、“？”より後のクエリー文字列（ＧＥＴパラメータ３１２の文字列）の文字数を演算装置９５によりカウントし、ＧＥＴパラメータ長３２２として特性値蓄積部３２ａに書き込む。特性値算出部３２は、ＵＲＩ３１１において“？”がない場合には、ＧＥＴパラメータ長３２２を「０」とする。

【０４１３】

また、特性値算出部３２は、ＵＲＩ３１１の文字列のうち、“？”よりも前の文字列（絶対パス文字列）の文字数を演算装置９５によりカウントし、ＵＲＬ長３２３として特性値蓄積部３２ａに書き込む。図３３（ａ）に示すように、特性値算出部３２は、ＵＲＩ３１１の“ｗｗｗ”の１文字目から“？”の前までの文字数をカウントし、ＵＲＬ長３２３とする。ＵＲＩ３１１において“？”がない場合は、ＧＥＴパラメータ３１２部分がないので、特性値算出部３２は、ＵＲＩ全体長３２１をそのままＵＲＬ長３２３とし、特性値蓄積部３２ａに書き込む。

【０４１４】

また、特性値算出部３２は、ＨＴＴＰリクエスト３１０の全体の文字数を演算装置９５によりカウントし、リクエスト全体長３２４とする。

上述したように、リクエスト全体長３２４は、ゲットリクエスト３１０ｇの場合と、ポストリクエスト３１０ｐの場合とで大きく異なる可能性が高い。これは、ウェブページの設計において、パラメータの数が少ない場合は、ゲットメソッドを用いることが多く、パラメータの数が多い場合や、ファイルのアップロードなどＧＥＴパラメータ３１２として記述することができない場合は、ポストメソッドを用いることが多いからである。したがって、リクエスト全体長３２４は、ポストリクエスト３１０ｐの方がゲットリクエスト３１０ｇよりも長いと考えられる。

【０４１５】

図３３（ａ）（ｂ）に示すように、ＨＴＴＰリクエスト３１０の先頭文字列は、“ＧＥＴ”、あるいは、“ＰＯＳＴ”といったメソッド名３１４になっている。特性値算出部３２は、メソッド名３１４を演算装置９５により判定し、判定対象のＨＴＴＰリクエスト３１０のメソッドが“ＧＥＴ”であるか“ＰＯＳＴ”であるかを判定する。

なお、メソッドには、“ＧＥＴ”及び“ＰＯＳＴ”以外のものもある。判定対象のＨＴＴＰリクエスト３１０のメソッドが“ＧＥＴ”でも“ＰＯＳＴ”でもない場合、特性値算出部３２は、例えば、判定対象のＨＴＴＰリクエスト３１０のメソッドが「その他」であると判定する。

【０４１６】

以上のように、特性値算出部３２は、ＵＲＩ全体長３２１、ＧＥＴパラメータ長３２２、ＵＲＬ長３２３、メソッドの種別、リクエスト全体長３２４を、ＨＴＴＰリクエスト３１０に対応付けて特性値蓄積部３２ａに蓄積する。特性値算出部３２は、ＵＲＩ全体長３２１、ＧＥＴパラメータ長３２２、ＵＲＬ長３２３、リクエスト全体長３２４のうちの少なくともひとつを特性値３２０としてもよい。

【０４１７】

＜Ｓ３２２：統計量算出工程＞

統計量算出部３３は、特性値蓄積部３２ａに蓄積されているＨＴＴＰリクエスト３１０について、ＵＲＩ全体長３２１の平均値及び標準偏差、ＧＥＴパラメータ長３２２の平均値及び標準偏差、ＵＲＬ長３２３の平均値及び標準偏差を統計量３３０として演算装置９５により算出する。統計量算出部３３は、算出したＵＲＩ全体長３２１の平均値及び標準偏差、ＧＥＴパラメータ長３２２の平均値及び標準偏差、ＵＲＬ長３２３の平均値及び標準偏差を、統計量記憶部３３ａに記憶する。

【０４１８】

このとき、不正通信検出装置３０が最初にＨＴＴＰリクエスト３１０を取得して不正通信検出処理を開始する場合には、特性値３２０の母集団の構成要素は１つということになる。母集団の構成要素の数があまりにも少ない場合には、統計量３３０の信頼度が低い。したがって、統計量３３０を算出するための母集団の構成要素の数が所定の数以上になってから、統計量算出処理を開始する構成であってもよい。

【０４１９】

具体的には、特性値算出部３２が特性値３２０を算出して、特性値蓄積部３２ａに蓄積したＨＴＴＰリクエスト３１０の数が所定数を超えたら、統計量算出部３３が起動するように設計してもよい。

【０４２０】

また、統計量算出部３３は、特性値蓄積部３２ａに蓄積されているＨＴＴＰリクエスト３１０について、ゲットリクエスト３１０ｇのリクエスト全体長３２４（ゲットリクエスト全体長３２４ｇとする）の平均値及び標準偏差、ポストリクエスト３１０ｐのリクエスト全体長（ポストリクエスト全体長３２４ｐとする）の平均値及び標準偏差を統計量３３０として演算装置９５により算出する。

【０４２１】

統計量算出部３３は、特性値蓄積部３２ａに蓄積されているＨＴＴＰリクエスト３１０のなかのメソッド種別が“ＧＥＴ”のもののリクエスト全体長３２４の平均値及び標準偏差を演算装置９５により算出してゲットリクエスト全体長３２４ｇの平均値及び標準偏差とする。また、統計量算出部３３は、特性値蓄積部３２ａに蓄積されているＨＴＴＰリクエスト３１０のなかのメソッド種別が“ＰＯＳＴ”のもののリクエスト全体長３２４の平均値及び標準偏差を演算装置９５により算出してポストリクエスト全体長３２４ｐの平均値及び標準偏差とする。統計量算出部３３は、算出したゲットリクエスト全体長３２４ｇの平均値及び標準偏差及びポストリクエスト全体長３２４ｐの平均値及び標準偏差を統計量記憶部３３ａに記憶する。

【０４２２】

なお、メソッドが「その他」であるＨＴＴＰリクエスト３１０について、統計量算出部３３は、ゲットリクエスト３１０ｇやポストリクエスト３１０ｐとは別に、例えばリクエスト全体長３２４などの特性値から、例えば平均値や標準偏差などの統計量を算出する構成であってもよい。

あるいは、統計量算出部３３は、メソッドが「その他」であるＨＴＴＰリクエスト３１

０をゲットリクエスト３１０ｇであるとみなして、特性値の統計量を算出する構成であってもよい。すなわち、統計量算出部３３は、ポストメソッド以外のメソッドであるＨＴＴＰリクエスト３１０についての統計量と、ポストメソッドであるＨＴＴＰリクエスト３１０についての統計量とを算出する構成であってもよい。

【０４２３】

＜Ｓ３２３：特性値分析工程＞

特性値分析部３７１は、特性値算出部３２が特性値蓄積部３２ａに蓄積した判定対象のＨＴＴＰリクエスト３１０について、統計量記憶部３３ａに記憶されている統計量３３０に基づいて、判定対象特性値３２５を分析する。

【０４２４】

特性値分析部３７１は、特性値蓄積部３２ａから判定対象のＨＴＴＰリクエスト３１０のＵＲＩ全体長３２１を読み出す。特性値分析部３７１は、統計量記憶部３３ａからＵＲＩ全体長３２１の平均値（Ｘとする）及び標準偏差（σとする）を読み出す。特性値分析部３７１は、判定対象のＵＲＩ全体長３２１が、（Ｘ－３σ）以上（Ｘ＋３σ）以下であるか否かを演算装置９５により判定する。

【０４２５】

判定対象のＵＲＩ全体長３２１が、（Ｘ－３σ）以上（Ｘ＋３σ）以下であると判定した場合、判定対象のＵＲＩ全体長３２１はＵＲＩ全体長３２１全体の約９９．７％に入っているので、特性値分析部３７１は、正常範囲であると判定する。判定対象のＵＲＩ全体長３２１が、（Ｘ－３σ）以上（Ｘ＋３σ）以下でないと判定した場合、判定対象のＵＲＩ全体長３２１はＵＲＩ全体長３２１全体の約９９．７％に入っていないので、特性値分析部３７１は、異常値であると判定する。

【０４２６】

特性値分析部３７１は、判定対象のＨＴＴＰリクエスト３１０のＧＥＴパラメータ長３２２及びＵＲＬ長３２３についても同様に、それぞれが（Ｘ－３σ）以上（Ｘ＋３σ）以下であるか否かを演算装置９５により判定し、異常値であるか否かを判定する。

【０４２７】

特性値分析部３７１は、判定対象のＨＴＴＰリクエスト３１０のメソッド名３１４から、判定対象のＨＴＴＰリクエスト３１０がゲットメソッドであるかポストメソッドであるかを判定する。特性値分析部３７１は、判定対象のＨＴＴＰリクエスト３１０がゲットメソッドである場合には、統計量記憶部３３ａからゲットリクエスト全体長３２４ｇの平均値（Ｘとする）及び標準偏差（σとする）を読み出す。特性値分析部３７１は、判定対象のリクエスト全体長３２４が、（Ｘ－３σ）以上（Ｘ＋３σ）以下であるか否かを演算装置９５により判定し、異常値であるか否かを判定する。特性値分析部３７１は、判定対象のＨＴＴＰリクエスト３１０がポストメソッドである場合も、同様に（Ｘ－３σ）以上（Ｘ＋３σ）以下であるか否かを演算装置９５により判定し、異常値であるか否かを判定する。

【０４２８】

特性値分析部３７１は、判定対象の特性値３２０が異常値であると判定した場合には、分析結果テーブル３７ａの判定対象のＨＴＴＰリクエスト３１０の宛先ホスト３１７名に対応する特性値３２０の項目に設定されている数をカウントアップする。ＨＴＴＰリクエスト３１０の宛先ホスト３１７名は、上述したように、「Ｈｏｓｔ」から取得する。

【０４２９】

例えば、特性値分析部３７１は、判定対象のＨＴＴＰリクエスト３１０のＧＥＴパラメータ長３２２が異常値であると判定したとする。特性値分析部３７１は、判定対象のＨＴＴＰリクエスト３１０の「Ｈｏｓｔ」から宛先ホスト３１７の名称（例えば、“ｄｄｄｄ．ｃｏ．ｊｐ”であるとする）を取得する。そして、特性値分析部３７１は、宛先ホスト３１７が“ｄｄｄｄ．ｃｏ．ｊｐ”であるレコードのＧＥＴパラメータ長の項目をカウントアップする（図３５参照）。

【０４３０】

次に、図３７を用いて、通信数分析処理（Ｓ３３０）（通信数分析方法）について説明する。

【０４３１】

＜Ｓ３３１：通信計数工程＞

通信計数部３５は、所定の期間内に通信取得部３１が取得した通信の数を、通信の宛先ホスト３１７ごとに計数する。通信計数部３５は、例えば、２４時間の間（所定の期間）に取得したＨＴＴＰリクエスト３１０の数を、宛先ホスト３１７ごとに計数し、所定期間通信数３５０として通信数蓄積部３５ａに蓄積する。図３８（ａ）に示すように、通信計数部３５は、宛先ホスト３１７ごとに２４時間の所定期間通信数３５０を通信数蓄積部３５ａに蓄積する。通信計数部３５は、所定の期間を２４時間とした場合は、宛先ホスト３１７ごとに、かつ、１日ごとに計数した所定期間通信数３５０を通信数蓄積部３５ａに蓄積する。

【０４３２】

＜Ｓ３３２：通信数統計量算出工程＞

通信数統計量算出部３６は、通信計数部３５が宛先ホスト３１７ごとに複数の所定の期間について計数した所定期間通信数３５０の通信数統計量３６０を宛先ホスト３１７ごとに算出する。通信数統計量算出部３６は、宛先ホスト３１７ごとの複数の所定期間通信数３５０の平均値と標準偏差とを算出し、標準偏差を平均値で割った変動係数を宛先ホスト３１７ごとの通信数統計量３６０として演算装置９５により算出する。通信数統計量算出部３６は、宛先ホスト３１７ごとの通信数統計量３６０を通信数統計量記憶部３６ａに記憶する（図３８（ｂ）参照）。

【０４３３】

具体的には、通信数統計量算出部３６は、通信数蓄積部３５ａに蓄積されている宛先ホスト３１７ごと、かつ、１日ごとの所定期間通信数３５０を複数日分取得し、宛先ホスト３１７ごとの所定期間通信数３５０の平均値と標準偏差とを算出する。通信数統計量算出部３６は、宛先ホスト３１７ごとの所定期間通信数３５０の平均値と標準偏差とに基づいて、標準偏差を平均値で割った変動係数を算出する。この変動係数は、宛先ホスト３１７ごとの２４時間の所定期間通信数３５０のばらつきを相対的に示したものである。通信数統計量算出部３６は、宛先ホスト３１７ごとの変動係数（通信数統計量３６０）を通信数統計量記憶部３６ａに記憶する。通信数統計量記憶部３６ａには、宛先ホスト３１７ごとに変動係数（通信数統計量３６０）が常に最新のものに更新されて記憶されている。

【０４３４】

＜Ｓ３３３～Ｓ３３４：通信数分析工程＞

Ｓ３３３において、通信数分析部３７２は、通信計数部３５が所定期間通信数３５０を算出する度に、所定期間通信数３５０が１であるか否かを演算装置９５により判定する。所定期間通信数３５０が１であるとは、例えば、１日（２４時間）に特定の宛先ホスト３１７にＨＴＴＰリクエスト３１０を送信した数が１回だけであることを意味する。このような場合は、宛先ホスト３１７に不正通信をしている可能性があると判定する。

【０４３５】

通信数分析部３７２は、所定期間通信数３５０が１であると判定した場合には、分析結果テーブル３７ａの対応する宛先ホスト３１７のレコードの「リクエスト数＝１」の項目をカウントアップする（図３５参照）。

【０４３６】

Ｓ３３４において、通信数分析部３７２は、通信数統計量算出部３６が通信数統計量３６０（変動係数）を算出する度に、通信数統計量３６０（変動係数）と所定の閾値とを演算装置９５により比較し、通信数統計量３６０（変動係数）が所定の閾値より小さい場合に、算出した通信数統計量３６０に対応する宛先ホスト３１７に不正通信があったと判定する。変動係数は、所定期間通信数３５０のばらつきの相対的な値を示すものである。したがって、変動係数が小さいということは、所定期間通信数３５０のばらつきが少なく所定期間通信数３５０が一定に近いことを意味し、機械的な通信である可能性が高いことを

意味している。したがって、通信数分析部３７２は、（変動係数）が所定の閾値より小さいと判定した場合には、その変動係数に対応する宛先ホスト３１７に不正通信があったと判定し、分析結果テーブル３７ａの対応する宛先ホスト３１７のレコードの「リクエスト分散」の項目をカウントアップする（図３５参照）。

【０４３７】

次に、図３９を用いて、通信種別分析処理（Ｓ３４０）（通信種別分析方法）について説明する。

【０４３８】

＜Ｓ３４１～Ｓ３４２：ポスト数判定工程＞

Ｓ３４１において、通信種別分析部３７３は、判定対象のＨＴＴＰリクエスト３１０のメソッド名３１４（図３３参照）を演算装置９５より判定する。通信種別分析部３７３は、メソッド名３１４がポストメソッドであると判定した場合（Ｓ３４１でＹＥＳ）、Ｓ３４２に進む。

【０４３９】

ＨＴＴＰリクエスト３１０がポストメソッドである場合、ポストメッセージ３１１ｐに機密情報などの不正取得した情報を記載した不正通信である場合があると判断し、通信種別分析部３７３は、不正通信の可能性があると判断する。

【０４４０】

Ｓ３４２において、通信種別分析部３７３は、分析結果テーブル３７ａにおいて、判定対象のＨＴＴＰリクエスト３１０に対応する宛先ホスト３１７のレコードの「ポスト数」の項目をカウントアップする。

【０４４１】

＜Ｓ３４３～Ｓ３４４：不正ＨＴＴＰ判定工程＞

Ｓ３４３において、通信種別分析部３７３は、判定対象のＨＴＴＰリクエスト３１０のプロトコルを演算装置９５より判定する。通信種別分析部３７３は、判定対象のＨＴＴＰリクエスト３１０のプロトコルがＨＴＴＰ以外の独自のプロトコルであると判定した場合（Ｓ３４１でＹＥＳ）、Ｓ３４４に進む。判定対象のＨＴＴＰリクエスト３１０のプロトコルがＨＴＴＰ以外の独自のプロトコルである場合は、判定対象のＨＴＴＰリクエスト３１０はＨＴＴＰのポートを使用して独自プロトコルを使用している可能性が高く、通信種別分析部３７３は、不正通信の可能性があると判断する。

【０４４２】

Ｓ３４４において、通信種別分析部３７３は、分析結果テーブル３７ａにおいて、判定対象のＨＴＴＰリクエスト３１０に対応する宛先ホスト３１７のレコードの「不正ＨＴＴＰ」の項目をカウントアップする。

【０４４３】

＜Ｓ３４５～Ｓ３４６：不正ＵＡ判定工程＞

Ｓ３４５において、通信種別分析部３７３は、判定対象のＨＴＴＰリクエスト３１０の「Ｕｓｅｒ－Ａｇｅｎｔ」（ＵＡ）（図３３参照）を演算装置９５により判定する。不正通信検出装置３０では、予めＵＡとして設定されるＵＡ名（各種ブラウザなど）のＵＡホワイトリストを記憶装置９４に記憶している。通信種別分析部３７３は、判定対象のＨＴＴＰリクエスト３１０のＵＡに設定されているＵＡ名がＵＡホワイトリストにあるか否かを演算装置９５により判定する。ＵＡホワイトリストにないと判定した場合（Ｓ３４５でＹＥＳ）、不正ＵＡであると判断してＳ３４６に進む。

【０４４４】

Ｓ３４６において、通信種別分析部３７３は、分析結果テーブル３７ａにおいて、判定対象のＨＴＴＰリクエスト３１０に対応する宛先ホスト３１７のレコードの「不正ＵＡ」の項目をカウントアップする。

【０４４５】

＜Ｓ３４７～Ｓ３４８：不正サイト判定工程＞

Ｓ３４７において、通信種別分析部３７３は、判定対象のＨＴＴＰリクエスト３１０の

「Ｈｏｓｔ」（図３３参照）を演算装置９５より判定する。不正通信検出装置３０では、予め「Ｈｏｓｔ」として設定されるサイト名のＨｏｓｔブラックリストを記憶装置９４に記憶している。通信種別分析部３７３は、判定対象のＨＴＴＰリクエスト３１０の「Ｈｏｓｔ」に設定されるサイト名（ホスト名）がＨｏｓｔブラックリストにあるか否かを演算装置９５により判定する。Ｈｏｓｔブラックリストにあると判定した場合（Ｓ３４７でＹＥＳ）、不正サイトであると判断してＳ３４８に進む。

【０４４６】

Ｓ３４８において、通信種別分析部３７３は、分析結果テーブル３７ａにおいて、判定対象のＨＴＴＰリクエスト３１０に対応する宛先ホスト３１７のレコードの「不正サイト」の項目に「ＮＧ」を設定する。通信種別分析部３７３は、分析結果テーブル３７ａにおいて、判定対象のＨＴＴＰリクエスト３１０に対応する宛先ホスト３１７のレコードの「不正サイト」の項目に「ＮＧ」が設定されているか否かを演算装置９５により判定し、「ＮＧ」が設定されていたら不正サイト判定処理を実行しないことにしてもよい。

【０４４７】

次に、図３３及び図４０を用いて、レポート生成処理（Ｓ３５０）（レポート生成方法）について説明する。

【０４４８】

レポート生成部３８は、図３３に示す分析結果テーブル３７ａに基づいて、レポート３８０を生成する。レポート生成部３８は、例えば、１週間毎、３週間毎、１ヶ月毎等の、予め設定された期間ごとにレポート３８０を生成する。レポート生成部３８がレポート３８０を生成するタイミングは、ユーザが指定することにしてもよい。

【０４４９】

レポート生成部３８は、分析結果テーブル３７ａに基づいて、宛先ホスト３１７毎に、リクエスト数、ＵＲＩ全体長、ＵＲＬ長、ＧＥＴパラメータ長、ゲットリクエスト全体長、ポストリクエスト全体長、リクエスト数＝１、リクエスト分散（通信数変動係数）、ＰＯＳＴ数、不正ＨＴＴＰ、不正ＵＡ、不正サイトの項目に設定された値を出力する。

【０４５０】

レポート生成部３８がレポート３８０として出力する項目は、上記全ての項目でなくともよい。例えば、ユーザが予め指定した項目でもよいし、レポート３８０を出力する都度、ユーザが出力項目を設定できることにしてもよい。例えば、図４０に示すようにレポート３８０には、ＵＲＩ全体長の項目がなくてもよい。

【０４５１】

図４０に示すように、レポート生成部３８は、宛先ホスト３１７毎のスコア項目を出力する。レポート生成部３８は、宛先ホスト３１７毎に、項目に設定されている値に基づいて、演算装置９５によりスコアを算出する。レポート生成部３８は、例えば、値が設定されている項目の数をスコアとして算出する。

【０４５２】

レポート生成部３８は、図４０に示すように、宛先ホスト３１７をスコアの高い順から順番に並べてレポート３８０を出力する。これにより、ユーザは危険な宛先ホスト３１７をすぐに検出することができる。

【０４５３】

なお、レポート生成部３８は、スコアが所定の閾値以上である宛先ホスト３１７だけについてのレポート３８０を出力する構成であってもよい。

あるいは、レポート生成部３８は、スコアが高い宛先ホスト３１７から順に順位を付け、順位が所定の閾値以下である宛先ホスト３１７だけについてのレポート３８０を出力する構成であってもよい。

【０４５４】

なお、宛先ホスト３１７に対するアクセスが機械的であるか否かを判定する方式として、所定の周期ごとにその宛先ホスト３１７に対して送信されたＨＴＴＰリクエストの数（所定期間通信数３５０）を集計し、所定期間通信数３５０の変動係数（標準偏差を平均値

で割った商）を閾値と比較して、変動係数が閾値より小さい場合に、アクセスが機械的であると判定する方式について説明したが、他の方式で判定する構成であってもよい。
例えば、通信計数部３５は、ある宛先ホスト３１７に対して送信されたＨＴＴＰリクエストの数をカウントする。カウントした数が所定の数に達したら、通信計数部３５は、カウントした数をリセットして０にする。通信計数部３５は、これを繰り返し、カウントした数をリセットしてから次にリセットするまでにかかった時間（以下「所定数通信期間」と呼ぶ。）を算出する。通信数統計量算出部３６は、通信計数部３５が算出した所定数通信期間の平均値及び標準偏差を算出し、変動係数を算出する。通信数分析部３７２は、所定数通信期間の変動係数を閾値と比較して、変動係数が閾値より小さい場合に、アクセスが機械的であると判定する。

【０４５５】
以上説明した不正通信検出装置（３０）は、
ネットワークを介した通信を取得する通信取得部（３１）と、
上記通信取得部が取得した通信を解析して、上記通信の特性値を算出する特性値算出部（３２）と、
１以上の通信について上記特性値算出部が算出した特性値に基づいて統計量を算出する統計量算出部（３３）と、
上記統計量算出部が算出した統計量に基づいて、上記特性値算出部が算出した特性値が異常値であるか否かを判定し、上記特性値が異常値であると判定した場合に、不正通信の可能性があると判定する不正判定部（３７）とを有する。

【０４５６】
上記通信取得部（３１）は、上記通信として、ハイパーテキスト転送プロトコルにおけるリクエストを取得し、
上記特性値算出部（３２）は、上記通信取得部が取得した通信に基づいて、上記特性値として、統一資源識別子の長さと、上記統一資源識別子のうち絶対パス文字列の長さと、上記統一資源識別子のうちクエリー文字列の長さと、上記リクエスト全体の長さとのうち、少なくともいずれかを算出する。

【０４５７】
上記統計量算出部（３３）は、上記統計量として、上記１以上の通信についての上記特性値を平均した平均値及び標準偏差を算出し、
上記不正判定部（３７）は、上記標準偏差に所定の定数を乗じた値を上記平均値に加えた値よりも上記特性値が大きい場合と、上記標準偏差に所定の定数を乗じた値を上記平均値から差し引いた値よりも上記特性値が小さい場合とのうち、少なくともいずれかの場合に、上記特性値が異常値であると判定する。

【０４５８】
上記通信取得部（３１）は、上記通信として、ハイパーテキスト転送プロトコルにおけるリクエストを取得し、
上記統計量算出部（３３）は、上記統計量として、上記１以上の通信のうち、ゲットメソッドである通信についての上記特性値を平均した平均値及び標準偏差と、ポストメソッドである通信についての上記特性値を平均した平均値及び標準偏差と、ポストメソッド以外のメソッドである通信についての上記特性値を平均した平均値及び標準偏差とのうち、少なくともいずれかの平均値及び標準偏差を算出する。

【０４５９】
上記不正通信検出装置（３０）は、
所定の期間内に上記通信取得部が取得した通信の通信数を、上記通信の宛先ごとに計数する通信計数部（３５）を有し、
上記不正判定部（３７）は、いずれかの宛先について上記通信計数部が計数した通信数が１である場合に、不正通信の可能性があると判定する。

【０４６０】
上記不正通信検出装置（３０）は、

所定の期間内に上記通信取得部が取得した通信の数を、上記通信の宛先ごとに計数する通信計数部（３５）と、
複数の期間について上記通信計数部が計数した通信数の統計量を、上記宛先ごとに算出する通信数統計量算出部（３６）とを有し、
上記不正判定部（３７）は、上記通信数統計量算出部が算出した統計量が所定の閾値より小さい場合に、不正通信の可能性があると判定する。
【０４６１】
上記通信取得部（３１）は、上記通信として、ハイパーテキスト転送プロトコルにおけるリクエストを取得し、
上記不正判定部（３７）は、上記通信取得部が取得した通信がポストメソッドである場合と、上記通信のフォーマットがハイパーテキスト転送プロトコルの規定に合致しない場合と、上記通信のユーザエージェントが所定のリストに含まれるユーザエージェントでない場合とのうち、少なくともいずれかの場合に、不正通信の可能性があると判定する。
【０４６２】
上記不正判定部（３７）は、上記通信取得部が取得した通信の宛先が所定のリストに含まれる宛先である場合に、不正通信の可能性があると判定する。
【０４６３】
実施の形態７.
実施の形態７について、図４１を用いて説明する。図４１は、本実施の形態に係る不正通信検出装置３０ａのブロック構成図である。
【０４６４】
この実施の形態では、実施の形態６で説明した不正通信検出装置３０の構成の他の例（不正通信検出装置３０ａ）について説明する。
なお、実施の形態６と共通する構成には、同一の符号を付し、説明を省略する場合がある。
【０４６５】
図４１において、図３２と異なる点は、不正通信検出装置３０ａでは、不正通信検出装置３０に加えて、宛先別統計量算出部３４、宛先別統計量記憶部３４ａを有している点である。
【０４６６】
宛先別統計量算出部３４は、宛先ホスト３１７が同じ複数のＨＴＴＰリクエスト３１０について、特性値３２０の平均値（宛先別平均値とする）と標準偏差（宛先別標準偏差とする）とを宛先別統計量３４０として算出する。宛先別統計量算出部３４は、算出した宛先別統計量３４０を宛先別統計量記憶部３４ａに記憶する。つまり、宛先別統計量記憶部３４ａには、宛先ホスト３１７毎に、特性値３２０の宛先別平均値と宛先別標準偏差とが記憶されている。
【０４６７】
特性値分析部３７１は、判定対象のＨＴＴＰリクエスト３１０の宛先ホスト３１７に対応する宛先別統計量３４０に基づいて、判定対象のＨＴＴＰリクエスト３１０の判定対象特性値３２５が異常値であるか否かを演算装置９５により判定する。
特性値分析部３７１は、判定対象のＨＴＴＰリクエスト３１０の宛先ホスト３１７を取得して、取得した宛先ホスト３１７に対応する宛先別統計量３４０を宛先別統計量記憶部３４ａから取得する。
【０４６８】
例えば、判定対象のＨＴＴＰリクエスト３１０の宛先ホスト３１７が“ｄｄｄｄ．ｃｏ．ｊｐ”であり、判定対象特性値３２５がＵＲＬ長３２３である場合について説明する。特性値分析部３７１は、宛先別統計量記憶部３４ａから、宛先ホスト３１７が“ｄｄｄｄ．ｃｏ．ｊｐ”に対応するＵＲＬ長３２３の宛先別平均値と宛先別標準偏差とを取得する。特性値分析部３７１は、取得したＵＲＬ長３２３の宛先別平均値と宛先別標準偏差とに基づいて、判定対象特性値３２５であるＵＲＬ長３２３が異常値であるか否かを演算装置

９５により判定する。

【０４６９】

具体的には、特性値分析部３７１は、宛先別平均値をＸとし、宛先別標準偏差をσとすると、判定対象のＵＲＩ全体長３２１が（Ｘ－３σ）以上（Ｘ＋３σ）以下であるか否かを演算装置９５により判定する。

特性値分析部３７１は、判定対象のＵＲＬ長３２３が（Ｘ－３σ）以上（Ｘ＋３σ）以下であると判定した場合には、判定対象のＵＲＬ長３２３は、宛先ホスト３１７が“ｄｄｄｄ．ｃｏ．ｊｐ”であるＵＲＬ長３２３全体の約９９．７％に入っているので、正常範囲であると判定する。

特性値分析部３７１は、判定対象のＵＲＬ長３２３が（Ｘ－３σ）以上（Ｘ＋３σ）以下でないと判定した場合には、判定対象のＵＲＬ長３２３は、宛先ホスト３１７が“ｄｄｄｄ．ｃｏ．ｊｐ”であるＵＲＬ長３２３全体の約９９．７％に入っていないので、異常値であると判定する。

【０４７０】

例えば、不正な宛先ホスト３１７へのリクエストにおいて、不正通信をカモフラージュするために、特性値３２０が正常値であるリクエストの中に、たまに特性値３２０が異常値である不正通信のリクエストを混在させる可能性がある。

このような場合に、本実施の形態に係る不正通信検出装置３０ａによれば、宛先別に算出された宛先別統計量３４０に基づいて、特性値３２０を分析することができるので、高い精度で異常な特性値３２０を検出することができる。

【０４７１】

実施の形態８．

実施の形態８について、図４１及び図４２を用いて説明する。図４２は、本実施の形態に係るレポート作成処理により作成されたレポート３８０を示す図である。

【０４７２】

この実施の形態では、実施の形態７で説明した不正通信検出装置３０ａの特性値分析方法の他の例について説明する。

なお、実施の形態６，７と共通する構成には、同一の符号を付し、説明を省略する場合がある。

【０４７３】

特性値分析部３７１は、レポート生成部３８がレポート３８０を生成するタイミングで、宛先別統計量記憶部３４ａに記憶されている宛先別統計量３４０のうちの宛先別平均値が所定の閾値よりも大きいか否かを判定する。特性値分析部３７１は、宛先別統計量記憶部３４ａに記憶されている全ての宛先ホスト３１７について、宛先別平均値の判定を実行する。

【０４７４】

分析結果テーブル３７ａは、さらに、宛先別平均値の項目を備えるものとする。特性値分析部３７１は、判定対象の宛先ホスト３１７の宛先別平均値が異常値であると判定した場合には、判定対象の宛先ホスト３１７の宛先別平均値の項目に「ＮＧ」を設定する。

例えば、特性値分析部３７１は、統計量記憶部３３ａに記憶されている統計量３３０に基づいて、判定対象の宛先別平均値が異常値であるか否かを判定する。

【０４７５】

判定対象の宛先別平均値としては、例えば、ＵＲＩ全体長３２１の宛先別平均値、ＧＥＴパラメータ長３２２の宛先別平均値、ＵＲＬ長３２３の宛先別平均値、ゲットリクエストのリクエスト全体長３２４の宛先別平均値、ポストリクエストのリクエスト全体長３２４の宛先別平均値などがある。

【０４７６】

以下、判定対象の宛先別平均値がゲットリクエストのリクエスト全体長３２４の宛先別平均値である場合について説明する。

判定対象の宛先ホスト３１７が“ａａｂｂ．ｃｏｍ”であり、ゲットリクエストのリク

エスト全体長３２４の宛先別平均値（以下、ゲット平均値とする）について判定を実行する場合について説明する。特性値分析部３７１は、宛先別統計量記憶部３４ａから、宛先ホスト３１７が“ａａｂｂ．ｃｏｍ”に対応するゲット平均値を取得する。特性値分析部３７１は、統計量記憶部３３ａに記憶されているゲットリクエストのリクエスト全体長３２４の統計量３３０（平均値及び標準偏差）に基づいて、判定対象のゲット平均値が異常値であるか否かを演算装置９５により判定する。

【０４７７】

具体的には、特性値分析部３７１は、統計量記憶部３３ａに記憶されているゲットリクエストのリクエスト全体長３２４の統計量３３０（平均値（Ｘとする）及び標準偏差（σとする））を読み出す。特性値分析部３７１は、判定対象のゲット平均値が（Ｘ－３σ）以上（Ｘ＋３σ）以下であるか否かを演算装置９５により判定する。

【０４７８】

特性値分析部３７１は、判定対象のゲット平均値が、（Ｘ－３σ）以上（Ｘ＋３σ）以下であると判定した場合には、判定対象のゲット平均値は、ゲットリクエストのリクエスト全体長３２４全体の約９９．７％に入っているので、正常範囲であると判定する。

特性値分析部３７１は、判定対象のゲット平均値が、（Ｘ－３σ）以上（Ｘ＋３σ）以下でないと判定した場合には、判定対象のゲット平均値は、ゲットリクエストのリクエスト全体長３２４全体の約９９．７％に入っていないので、異常値であると判定する。

【０４７９】

特性値分析部３７１は、判定対象の宛先別平均値（宛先ホスト３１７が“ａａｂｂ．ｃｏｍ”であるゲット平均値）が異常値であると判定した場合に、宛先ホスト３１７“ａａｂｂ．ｃｏｍ”はゲット平均値が異常値であるとして、分析結果テーブル３７ａの「ゲット平均値」項目に「ＮＧ」を設定する。

【０４８０】

また、特性値分析部３７１は、宛先別統計量記憶部３４ａに記憶されている宛先ホスト３１７毎の宛先別平均値を平均した値に基づいて、判定対象の宛先別平均値を判定するための判定閾値を算出する構成であってもよい。

例えば、統計量算出部３３は、それぞれの宛先について算出した宛先別平均値を母集団として、宛先別統計量記憶部３４ａが記憶している宛先別平均値の平均値及び標準偏差を算出する。統計量記憶部３３ａは、宛先別平均値の平均値Ｘ’及び標準偏差σ’を記憶する。

特性値分析部３７１は、判定対象の宛先別平均値が（Ｘ’－３σ’）以上（Ｘ’＋３σ’）以下でない場合に、判定対象の宛先別平均値が異常値であると判定する。

【０４８１】

あるいは、特性値分析部３７１は、予め記憶装置９４に記憶された固定値を判定対象の宛先別平均値を判定するための判定閾値としてもよい。

【０４８２】

図４２に示すように、本実施の形態に係るレポート３８０では、実施の形態７に係るレポート３８０における「ゲット全体量」項目及び「ポスト全体量」項目に替えて、「ゲット平均量」項目及び「ポスト平均量」項目を備える。

【０４８３】

レポート生成部３８は、分析結果テーブル３７ａに設定されている宛先ホスト３１７毎の「ゲット平均値」項目、「ポスト平均値」項目に設定されている内容に基づいて、レポート３８０を生成する。

【０４８４】

レポート生成部３８は、分析結果テーブル３７ａが備える項目すべてについてレポート３８０に出力するものとしてもよいし、例えば、ユーザがレポート３８０として出力する項目を選択することができるとしてもよい。

【０４８５】

以上説明した不正通信検出装置（３０ａ）は、

宛先が同じ複数の通信について上記特性値算出部（３２）が算出した特性値を平均した宛先別平均値を算出する宛先別平均値算出部（宛先別統計量算出部３４）を有し、

上記不正判定部（３７）は、上記統計量算出部（３３）が算出した統計量に基づいて、上記宛先別平均値算出部が算出した宛先別平均値が異常値であるか否かを判定し、上記宛先別平均値が異常値であると判定した場合に、不正通信の可能性があると判定する。

【０４８６】

上記統計量算出部（３３）は、上記宛先別平均値算出部が算出した宛先別平均値に基づいて、上記統計量を算出する。

【０４８７】

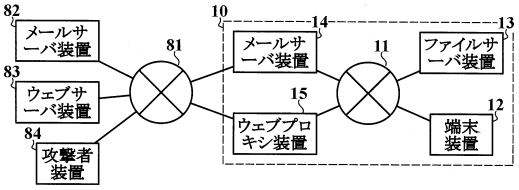
以上のように、本実施の形態に係る不正通信検出装置３０ａによれば、特性値３２０の宛先別平均値について異常か否かを判定することができるので、宛先ホストの分析の精度が向上する。

【符号の説明】

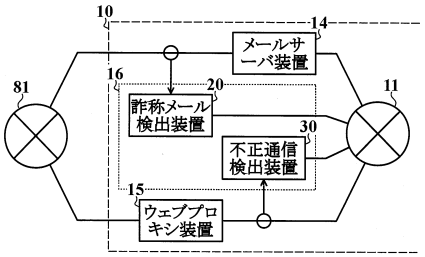
【０４８８】

１０　ローカルネットワークシステム、１１　ローカルエリアネットワーク、１２　端末装置、１３　ファイルサーバ装置、１４，８２　メールサーバ装置、１５　ウェブプロキシ装置、１６　サイバー攻撃検出システム、２０　詐称メール検出装置、２１　メール通信取得部、２２　メール通信記憶部、２３　作成者ドメイン取得部、２４　内部ドメイン検査部、２４０　電子メール、２４０ａ　ＳＭＴＰプロトコル情報、２４０ｂ　メールヘッダ、２４０ｃ　メッセージボディ、２４１　送信者ドメイン取得部、２４２　内部作成計数部、２４３　内部ドメイン詐称スコア算出部、２４６　内部ドメイン詐称スコア、２４８ａ　作成者メールアドレス、２４８ｂ　作成者ドメイン、２４９ａ　送信者メールアドレス、２４９ｂ　送信者ドメイン、２４２１　ドメイン別メール数一覧、２４２２　除外判定値、２４２３　計数時間、２４２４　対象メール数、２４２５　除外ドメイン一覧、２５　外国経由検査部、２５１　外国経由判定部、２５２　国内信頼ドメイン学習部、２５２Ａ　国内信頼ドメイン一覧、２５３　中継装置ドメイン取得部、２５４　中継時刻取得部、２５５　パケット送信元取得部、２５９　外国経由検査スコア決定部、２５９Ａ　外国経由検査スコア一覧表、２６　パケット連続度検査部、２６１　連続度算出部、２６２　統計量算出部、２６２Ａ　統計量一覧表、２６９　パケット連続度検査スコア決定部、２６９Ａ　パケット連続度検査スコア一覧表、２７　転送経路検査部、２７１　転送経路算出部、２７１Ａ　転送経路データ、２７２　ドメイン経路学習部、２７２Ａ　ドメイン経路リスト、２７３　経路情報取得部、２７９　転送経路検査スコア決定部、２７９Ａ　転送経路検査スコア一覧表、２８　詐称判定部、２８１　詐称評価値算出部、２８２　詐称評価閾値記憶部、２８３　詐称評価値判定部、２９　詐称警告部、３０，３０ａ　不正通信検出装置、３１　通信取得部、３１ａ　通信記憶部、３２　特性値算出部、３２ａ　特性値蓄積部、３３　統計量算出部、３３ａ　統計量記憶部、３４　宛先別統計量算出部、３４ａ　宛先別統計量記憶部、３５　通信計数部、３５ａ　通信数蓄積部、３６　通信数統計量算出部、３６ａ　通信数統計量記憶部、３７　不正判定部、３７ａ　分析結果テーブル、３８　レポート生成部、３１０　ＨＴＴＰリクエスト、３１０ｇ　ゲットリクエスト、３１０ｐ　ポストリクエスト、３１１　ＵＲＩ、３１１ｐ　ポストメッセージ、３１２　ＧＥＴパラメータ、３１３　ＵＲＬ、３１４　メソッド名、３１７　宛先ホスト、３２０　特性値、３２１　ＵＲＩ全体長、３２２　ＧＥＴパラメータ長、３２３　ＵＲＬ長、３２４　リクエスト全体長、３２５　判定対象特性値、３３０　統計量、３４０　宛先別統計量、３５０　所定期間通信数、３６０　通信数統計量、３７１　特性値分析部、３７２　通信数分析部、３７３　通信種別分析部、３７４　通信種別、３８０　レポート、８１　インターネット、８３　ウェブサーバ装置、８４　攻撃者装置、９０　コンピュータ、９１　制御装置、９２　入力装置、９３　出力装置、９４　記憶装置、９５　演算装置。

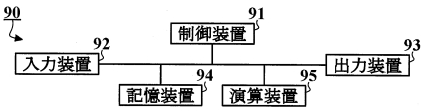
【図１】



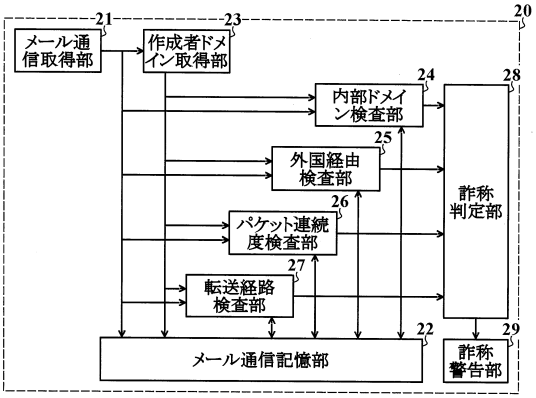
【図２】



【図３】

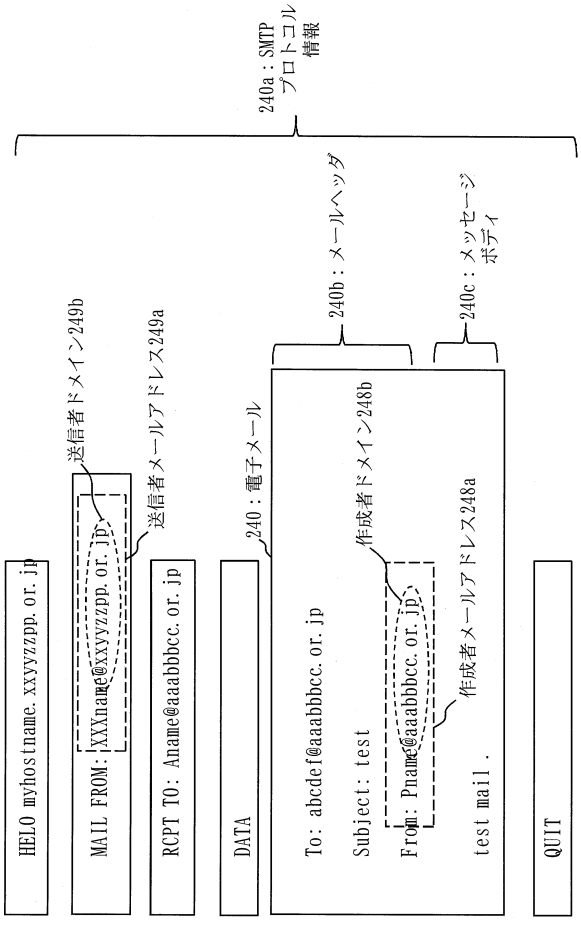


【図４】

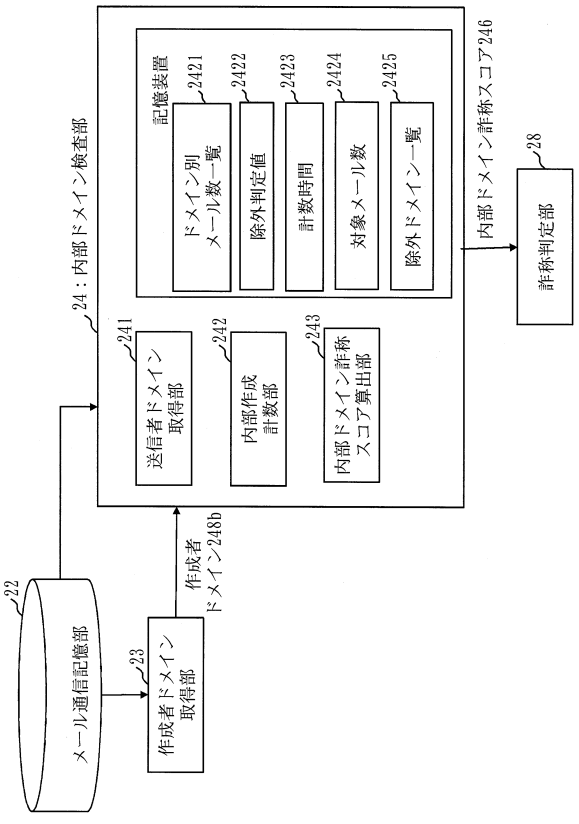


【図５】

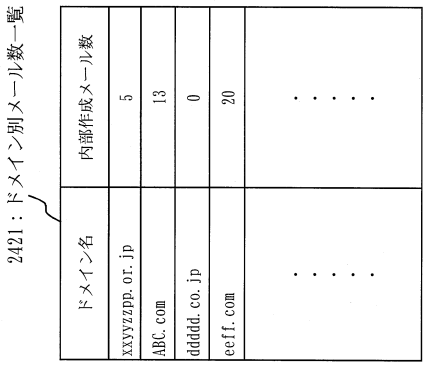
【図６】



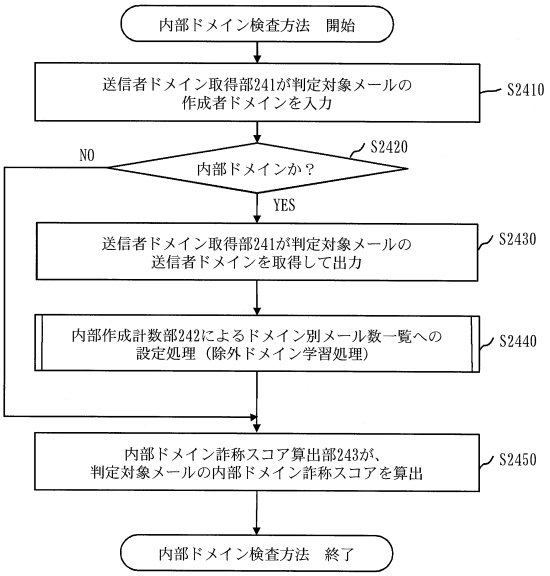
【図７】



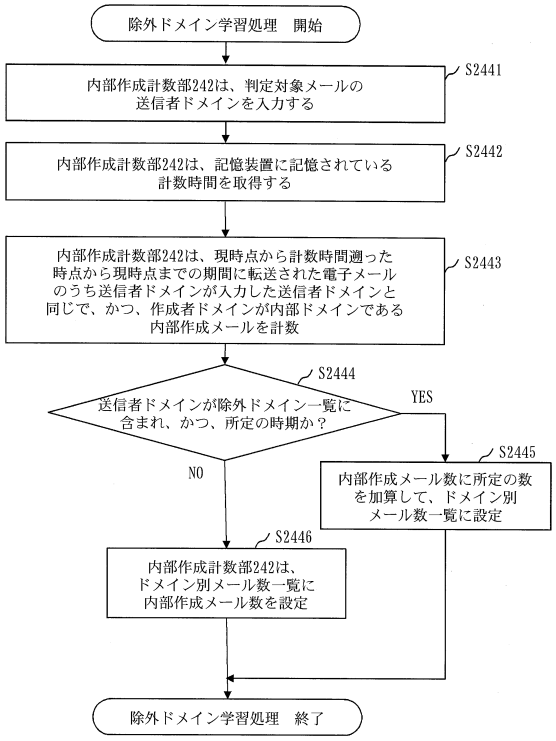
【図８】


2421：ドメイン別メール数一覧
ドメイン名
内部作成メール数
xxyyzzpp.or.jp
5
ABC.com
13
ddddd.co.jp
0
eeff.com
20

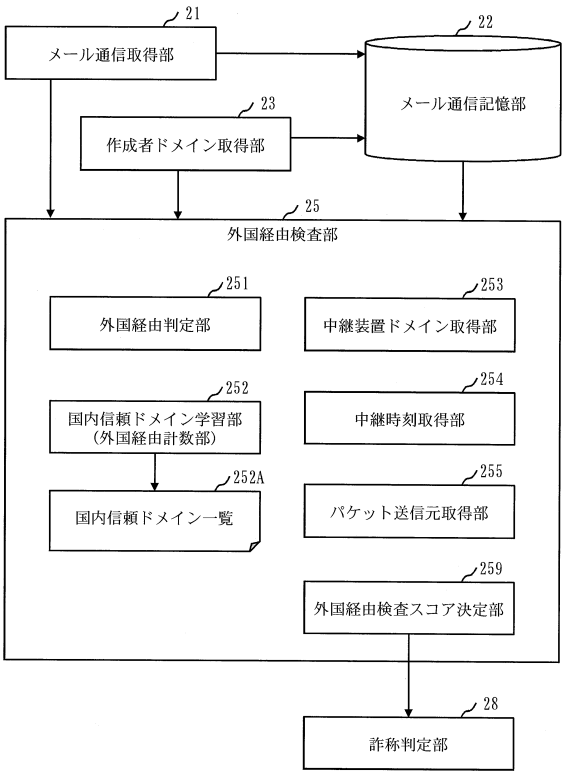
【図９】


内部ドメイン検査方法　開始
送信者ドメイン取得部241が判定対象メールの作成者ドメインを入力
S2410
内部ドメインか？
S2420
NO
YES
送信者ドメイン取得部241が判定対象メールの送信者ドメインを取得して出力
S2430
内部作成計数部242によるドメイン別メール数一覧への設定処理（除外ドメイン学習処理）
S2440
内部ドメイン詐称スコア算出部243が、判定対象メールの内部ドメイン詐称スコアを算出
S2450
内部ドメイン検査方法　終了

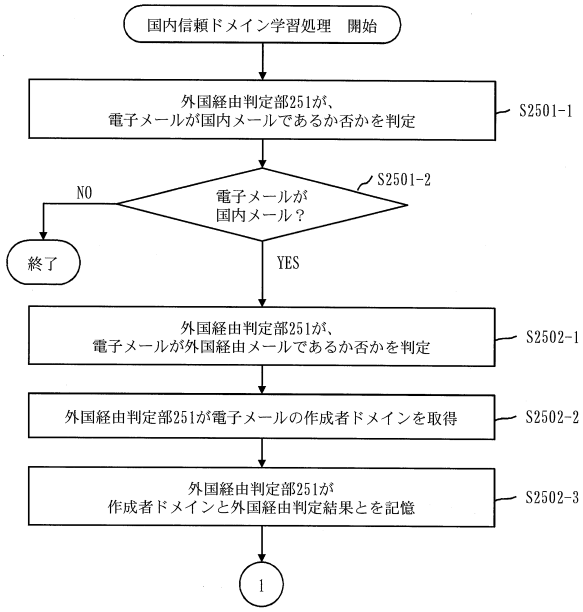
【図１０】


除外ドメイン学習処理　開始
内部作成計数部242は、判定対象メールの送信者ドメインを入力する
S2441
内部作成計数部242は、記憶装置に記憶されている計数時間を取得する
S2442
内部作成計数部242は、現時点から計数時間遡った時点から現時点までの期間に転送された電子メールのうち送信者ドメインが入力した送信者ドメインと同じで、かつ、作成者ドメインが内部ドメインである内部作成メールを計数
S2443
送信者ドメインが除外ドメイン一覧に含まれ、かつ、所定の時期か？
S2444
YES
NO
内部作成メール数に所定の数を加算して、ドメイン別メール数一覧に設定
S2445
内部作成計数部242は、ドメイン別メール数一覧に内部作成メール数を設定
S2446
除外ドメイン学習処理　終了

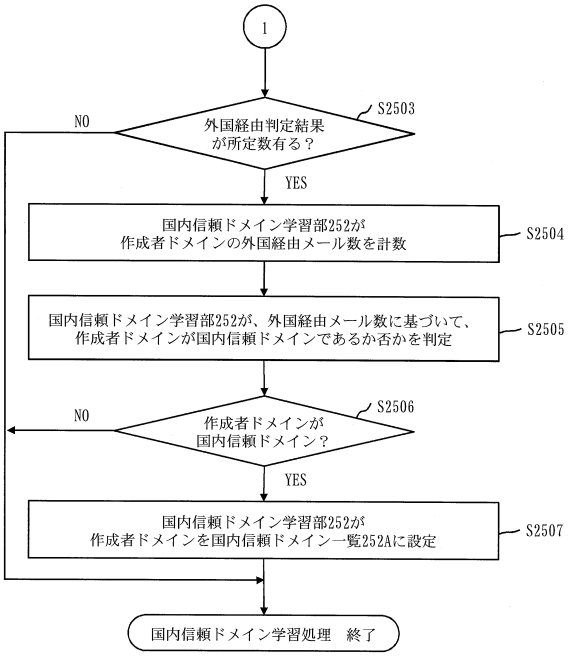
【図１１】


21
メール通信取得部
22
メール通信記憶部
23
作成者ドメイン取得部
25
外国経由検査部
251
外国経由判定部
253
中継装置ドメイン取得部
252
国内信頼ドメイン学習部（外国経由計数部）
254
中継時刻取得部
252A
国内信頼ドメイン一覧
255
パケット送信元取得部
259
外国経由検査スコア決定部
28
詐称判定部

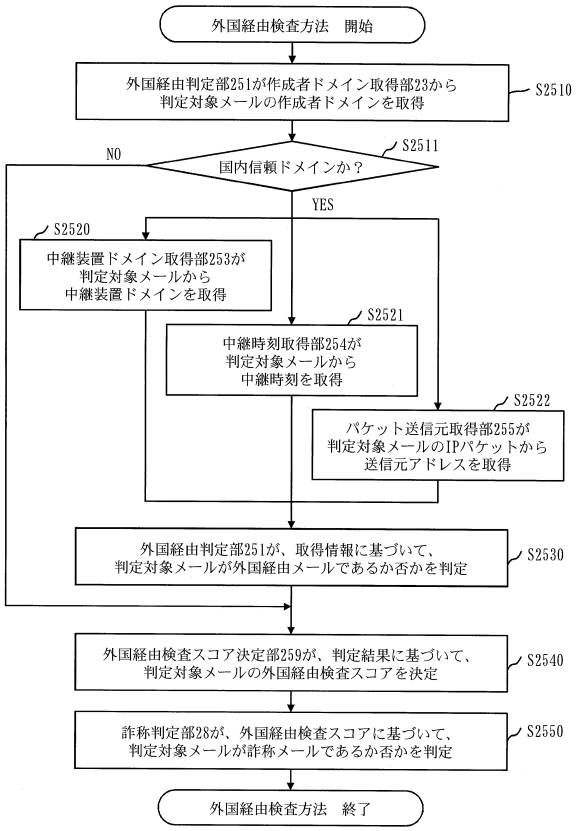
【図１２】



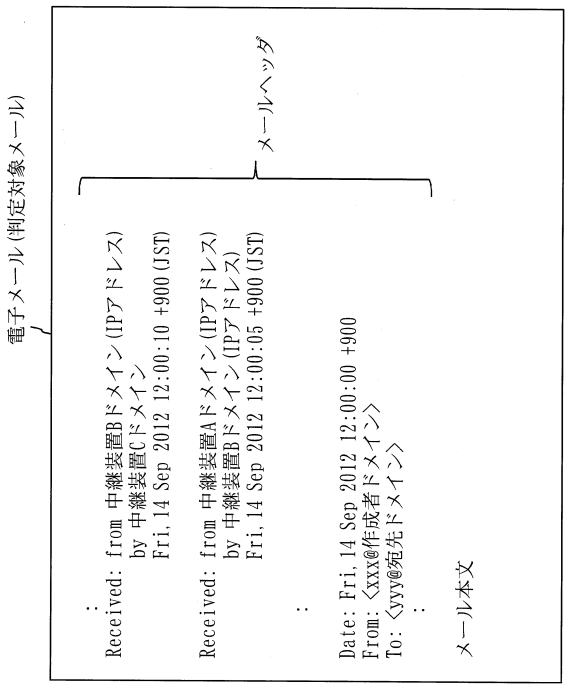
【図１３】



【図１４】



【図１５】

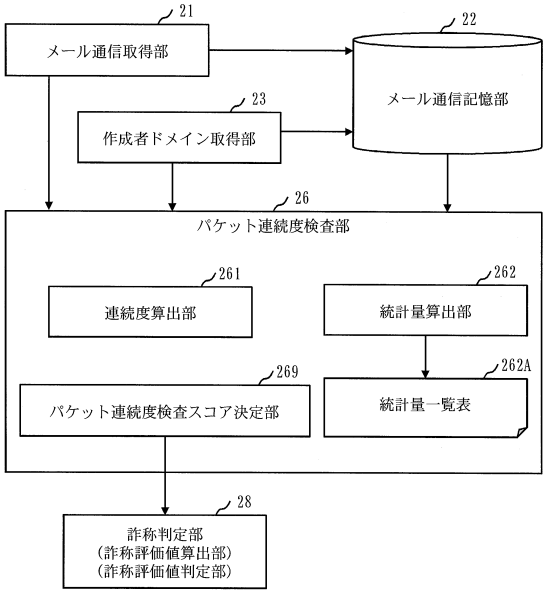


【図１６】

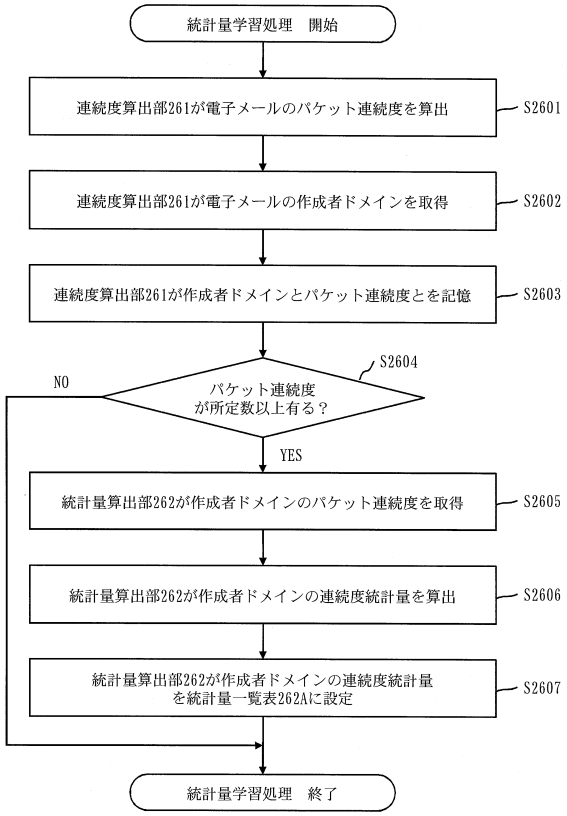
259A

条件	外国経由検査スコア
判定対象メールは 国内信頼ドメインでない	0
判定対象メールは 外国経由メールでない	0
判定対象メールは 外国経由メールである	4

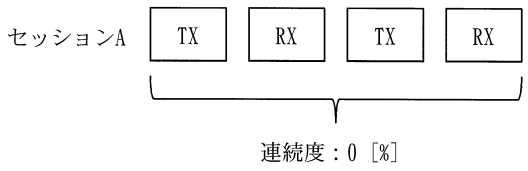
【図１７】



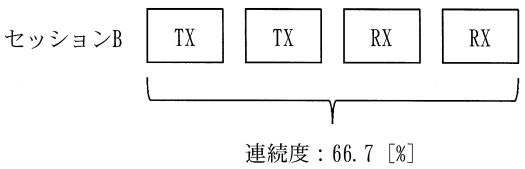
【図１８】



【図１９】



【図２０】



【図２１】

262A

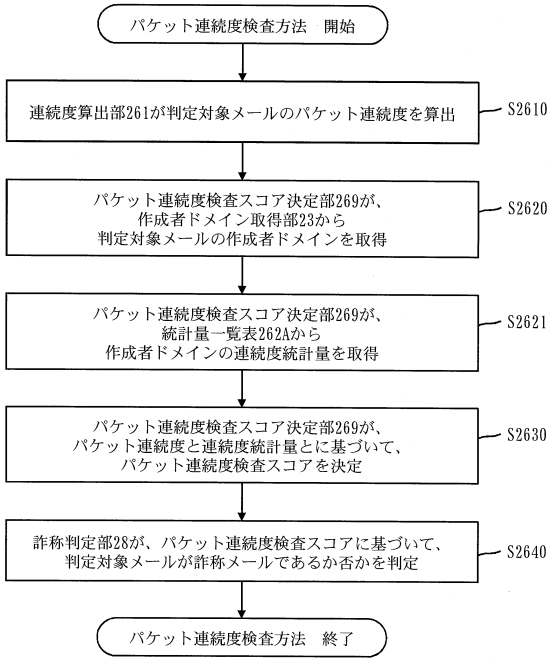
作成者ドメイン	連続度統計量	
	平均値(μ)	標準偏差(σ)
ドメインA	μ_1	σ_1
ドメインB	μ_2	σ_2
:	:	:

【図２２】

262A

作成者ドメイン	時間帯	連続度統計量	
		平均値(μ)	標準偏差(σ)
ドメインA	0時台	μ_1	σ_1
	1時台	μ_3	σ_3
	:	:	:
ドメインB	0時台	μ_2	σ_2
	:	:	:
:	:	:	:

【図２３】

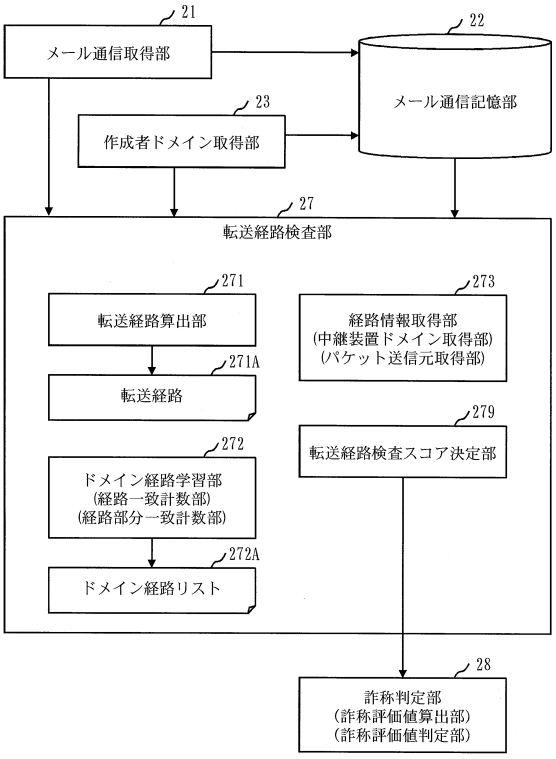


【図２４】

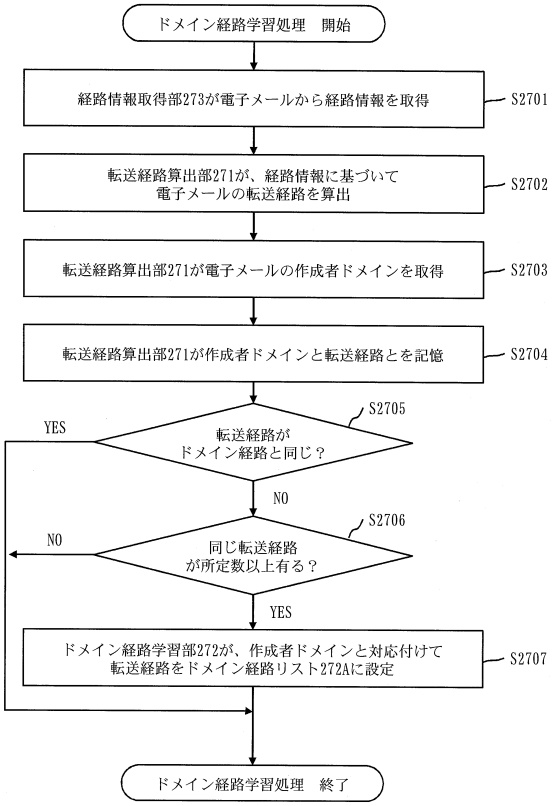
269A

パケット連続度(α)の範囲	パケット連続度検査スコア
$\alpha < \mu-2\sigma$	2
$\mu-2\sigma \leqq \alpha < \mu-1\sigma$	1
$\mu-1\sigma \leqq \alpha \leqq \mu+1\sigma$	0
$\mu+1\sigma < \alpha \leqq \mu+2\sigma$	1
$\mu+2\sigma < \alpha$	2

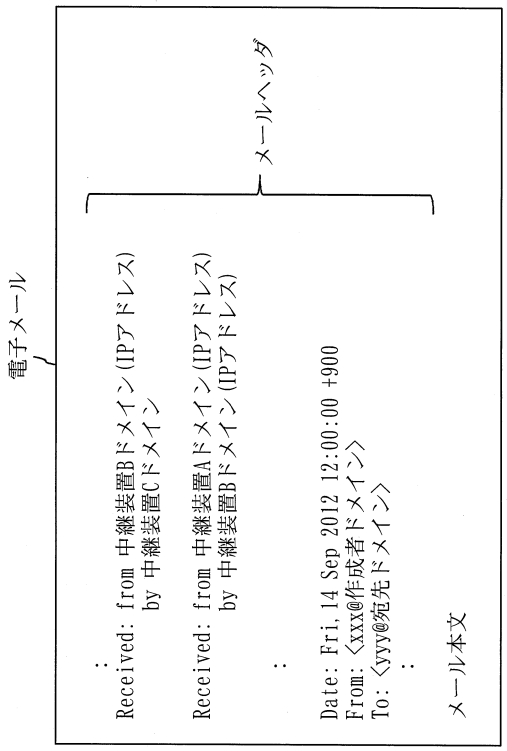
【図２５】



【図２６】



【図２７】



【図２８】

271A

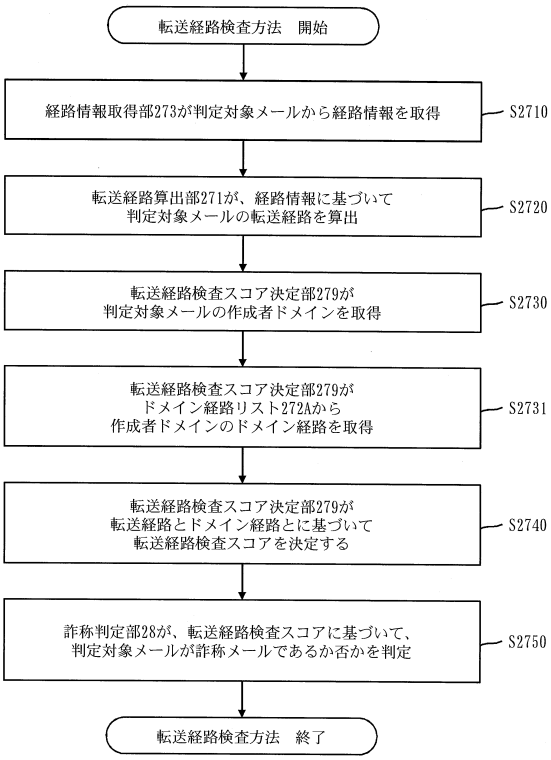
ローカル経路	グローバル経路
IP_1, IP_2	IP_3, IP_4

【図２９】

272A

作成者ドメイン	ドメイン経路		使用日時
	ローカル経路	グローバル経路	
ドメインA	IP_1, IP_2	IP_3, IP_4	2012.9.14 00:00:00
	IP_5	IP_3, IP_4	2012.9.14 01:00:00
：	：		：

【図３０】

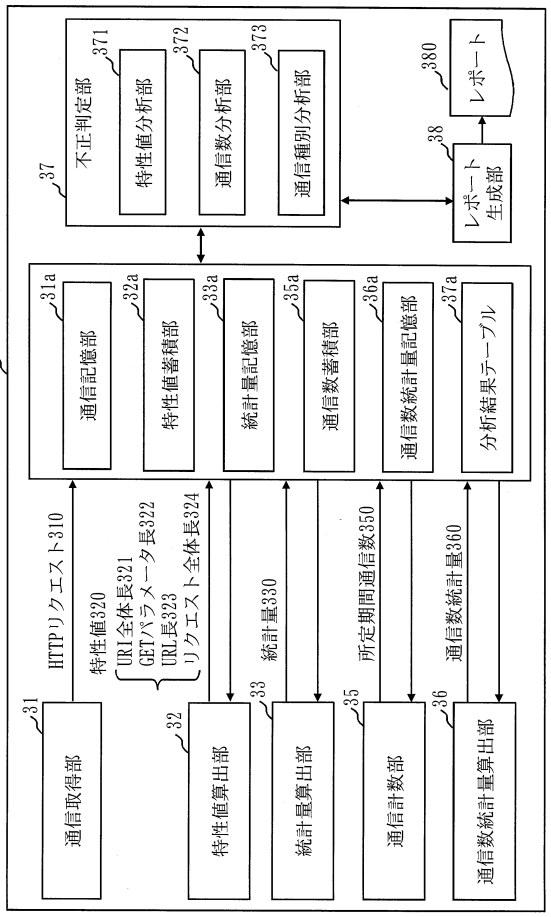


【図３１】

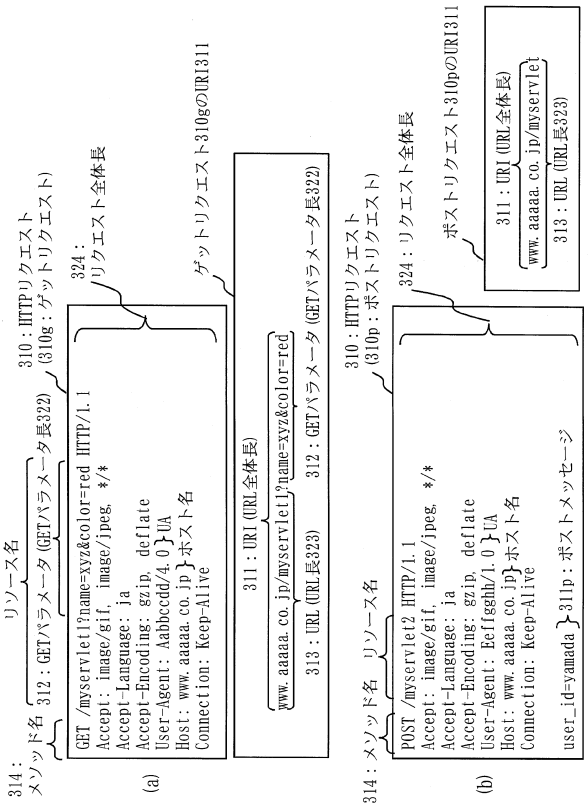
279A

条件	転送経路検査スコア
全経路が一致	0
グローバル経路のみが一致	2
グローバル経路が不一致	4
ドメイン経路が無い	0

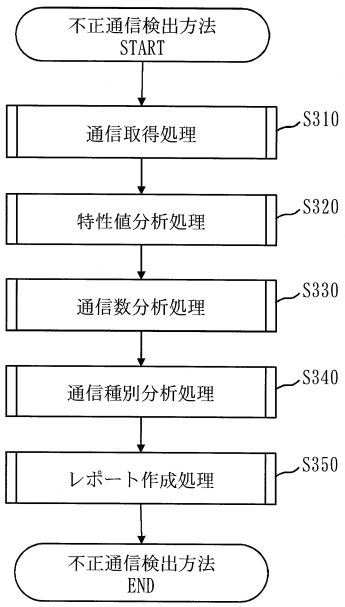
【図３２】



【図３３】



【図３４】

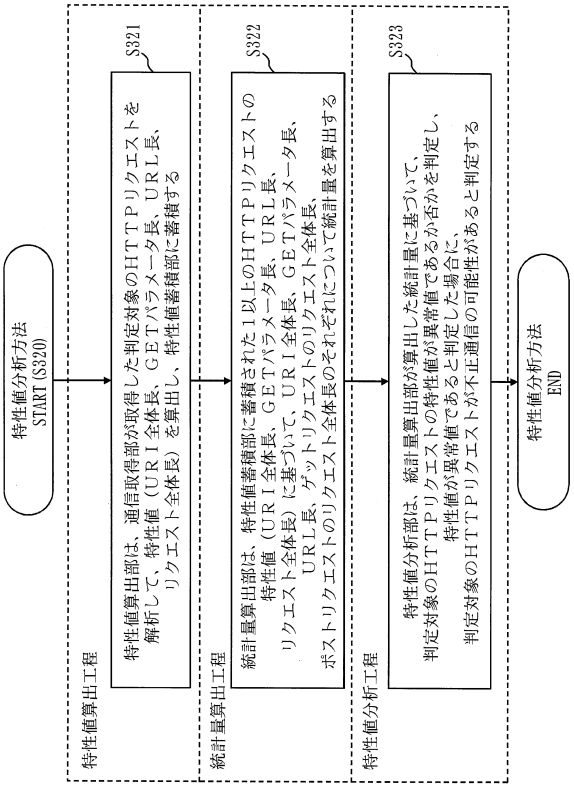


【図３５】

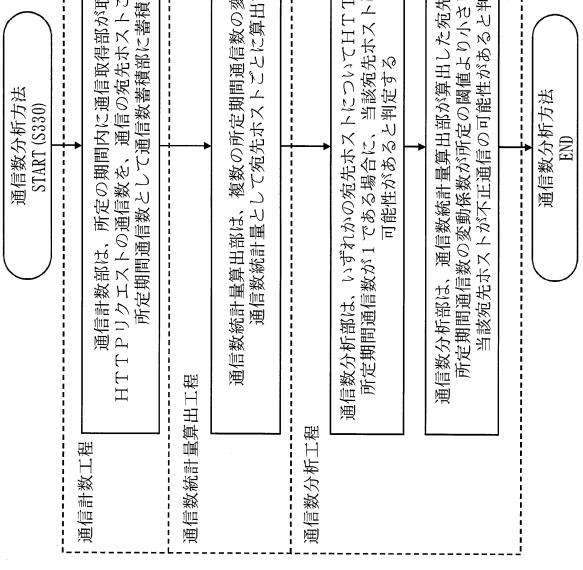
37a：分析結果テーブル

宛先ホスト名	リクエスト数	URI全体長	URL長	GETパラメータ	ゲット全体長	ポスト全体長	リクエスト数(=1)	リクエスト分散	POST数	不正HTTP	不正UA	不正サイト
aabb.com	24	—	—	3	—	—	—	1	20	1	—	—
XYZZ.ne.jp	30	—	—	—	—	—	—	—	15	1	30	NG
○×△aABC.com	2	3	3	3	—	—	—	—	1	—	—	—
ddddd.co.jp	1	—	—	—	—	—	1	—	—	—	—	—
eeff.com	85	—	—	—	—	—	—	—	—	—	—	—
・・・	・・・	・・・	・・・	・・・	・・・	・・・	・・・	・・・	・・・	・・・	・・・	・・・

【図３６】



【図３７】



【図３８】

35a：通信数蓄積部

宛先ホスト名 / 所定の期間	aabb.com	ddddd.co.jp	eeff.com	…
0801 00:00～24:00	10	3	23	…
0802 00:00～24:00	10	10	15	…
0803 00:00～24:00	10	7	12	…
0804 00:00～24:00	10	1	12	…
・・・	・・・	・・・	・・・	・・・

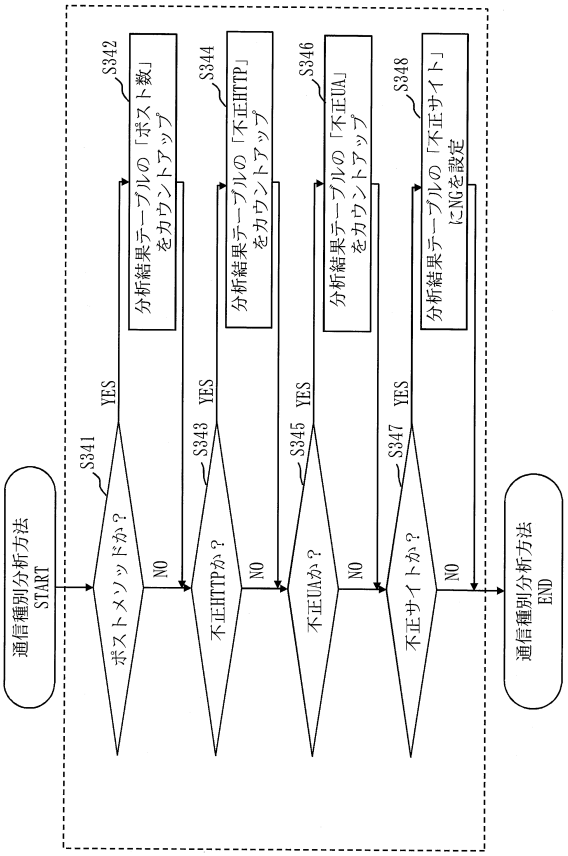
(a)

36a：通信数統計量記憶部

宛先ホスト名	変動係数
aabb.com	0.01
ddddd.co.jp	4.2
eeff.com	1.5
・・・	・・・

(b)

【図３９】

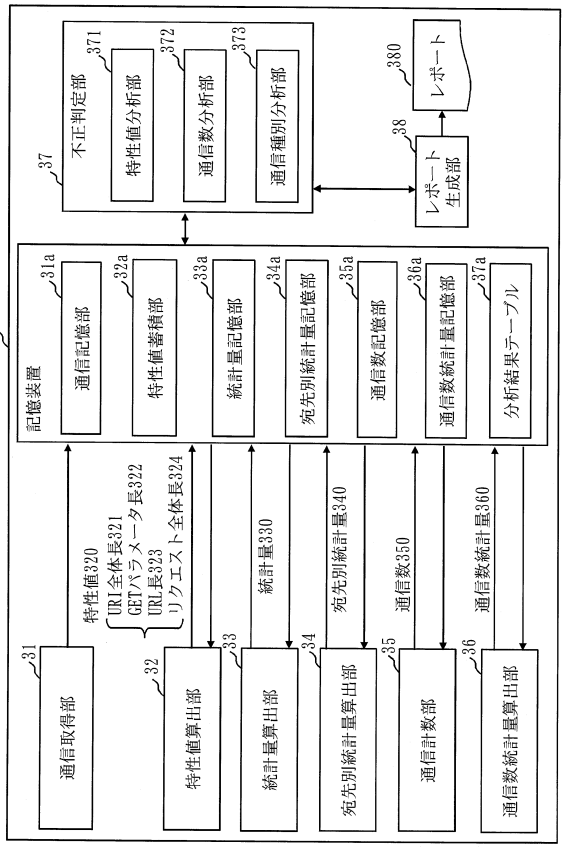


【図４０】

380：レポート

宛先ホスト名	スコア欄	リクエスト数	URL長	GETパラメータ	ゲット全体量	ポスト全体量	リクエスト数(=1)	リクエスト分散	POST数	不正HTTP	不正UA	不正サイト
aabb.com	4	24	—	3	—	—	—	—	20	1	—	—
XYZZ.ne.jp	4	30	—	—	—	—	—	—	15	1	30	NG
○×△aABC.com	4	2	3	3	—	—	—	—	1	—	—	—
ddddd.co.jp	2	1	—	—	—	—	1	—	—	—	—	—
eeff.com	1	85	—	—	—	—	—	—	—	—	—	—

【図４１】



【図４２】

380：レポート

宛先ホスト名	スコア欄	リクエスト数	URL長	GETパラメータ	ゲット平均量	ポスト平均量	リクエスト数(=1)	リクエスト分散	POST数	不正HTTP	不正UA	不正サイト
aabb.com	5	24	—	3	NG	—	—	1	20	1	—	—
XYZZ.ne.jp	5	30	—	—	—	NG	—	—	15	1	30	NG
○×△aABC.com	4	2	3	3	—	—	—	—	1	—	—	—
ddddd.co.jp	2	1	—	—	—	—	1	—	—	—	—	—
eeff.com	1	85	—	—	—	—	—	—	—	—	—	—

フロントページの続き

(56)参考文献 特開２００５－０１１２３４（ＪＰ，Ａ）
特開２００６－２７７４１４（ＪＰ，Ａ）
特表２００５－５３８６２０（ＪＰ，Ａ）
特開２０１０－０６１４０６（ＪＰ，Ａ）
米国特許出願公開第２００８／００８６４３４（ＵＳ，Ａ１）
特開２０１１－０４００６４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／００－２１／８８
Ｈ０４Ｌ　１２／６６