【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成29年5月18日(2017.5.18)

【公開番号】特開2015-76879(P2015-76879A)
【公開日】平成27年4月20日(2015.4.20)
【年通号数】公開・登録公報2015-026
【出願番号】特願2014-158292(P2014-158292)
【国際特許分類】
Ｈ０４Ｌ　12/70　(2013.01)
Ｇ０９Ｃ　1/00　(2006.01)
Ｈ０４Ｌ　12/741　(2013.01)
【ＦＩ】
Ｈ０４Ｌ　12/70　１００Ｚ
Ｇ０９Ｃ　1/00　６６０Ｅ
Ｈ０４Ｌ　12/741

【手続補正書】
【提出日】平成29年3月30日(2017.3.30)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
少なくとも１つのウェブクライアントと少なくとも１つのウェブサーバとの間で発生する暗号化されたデータフローを分類する方法であって、
前記暗号化されたデータフローは、前記少なくとも１つのウェブクライアントと前記少なくとも１つのウェブサーバとの間にセットアップされたトランスポート接続を介して移送され、
前記方法は解析装置によって実行される、
方法において、
前記方法は、
‐前記トランスポート接続がそれぞれ開始された時刻を表す情報と、前記トランスポート接続のエンドポイントのアドレシングに関する情報と、前記トランスポート接続によって移送されたデータの量および／またはセグメントの量に関する情報とを決定する、第１の決定ステップ（Ｓ３０１）と、
‐いずれかのトランスポート接続のエンドポイントである各ウェブサーバが関連付けられたドメイン名を決定する、第２の決定ステップ（Ｓ３０２）と、
‐前記トランスポート接続がそれぞれ開始された時刻と、前記トランスポート接続のエンドポイントである前記ウェブクライアントのアドレシングとに関する基準に従って、トランスポート接続をクラスタにグルーピングする、グルーピングステップ（Ｓ３０３）と、
‐各クラスタについて、そのクラスタの前記トランスポート接続に関連付けられたドメイン名およびそのクラスタの前記トランスポート接続によって移送されたデータの量および／またはセグメントの量と、事前定義ウェブ閲覧セッションプロファイルとを比較する、比較ステップ（Ｓ３０５）と、
‐前記比較ステップの結果に基づき、前記暗号化されたデータフローを分類する、分類ステップ（Ｓ３０６）と

を備える、方法。
【請求項２】
前記暗号化されたデータフローはＨＴＴＰＳに従い、前記トランスポート接続はＴＣＰに従うことを特徴とする、請求項１に記載の方法。
【請求項３】
前記トランスポート接続が開始された時刻は、前記解析装置が前記トランスポート接続それぞれのＳＹＮ　ＴＣＰセグメントを受信した時刻に対応することを特徴とする、請求項２に記載の方法。
【請求項４】
前記アドレシングは、アドレスおよびポートから構成され、
前記グルーピングステップは、
‐各クラスタは、同一のウェブクライアントアドレスを持つトランスポート接続のみを含み、
‐各クラスタは、各前記トランスポート接続のウェブクライアントポートに従って前記トランスポート接続を順序付けする時に、２つの連続するウェブクライアントポートの間の差が第１の事前定義閾値を超えない範囲内のウェブクライアントポートを持つトランスポート接続のみを含み、
‐各クラスタは、前記トランスポート接続が開始された時刻に従って前記トランスポート接続を順序付けする時に、２つの連続する前記トランスポート接続が開始された時刻の間の差が第２の事前定義閾値を超えない範囲内に開始されたトランスポート接続のみを含む
ように実行されることを特徴とする、請求項１～３のいずれか一項に記載の方法。
【請求項５】
クラスタにグルーピングされたいかなるトランスポート接続も、第３の事前定義閾値を超える持続時間を有することを特徴とする、請求項１～４のいずれか一項に記載の方法。
【請求項６】
クラスタにグルーピングされたいかなるトランスポート接続も、第４の事前定義閾値未満の持続時間を有し、前記第４の事前定義閾値は、前記第３の事前定義閾値より厳密に大きいことを特徴とする、請求項５に記載の方法。
【請求項７】
前記解析装置は、前記解析装置が前記トランスポート接続それぞれのＦＩＮ　ＡＣＫ　ＴＣＰセグメントを受信した時刻に基づいて前記トランスポート接続の持続時間を決定することを特徴とする、請求項２を引用する場合の請求項５に記載の方法、または、請求項２を引用する場合の請求項６に記載の方法。
【請求項８】
前記解析装置は、前記解析装置が前記トランスポート接続の有効なペイロードを伴う最新のＴＣＰセグメントを受信した時刻に基づいて前記トランスポート接続の持続時間を決定することを特徴とする、請求項１～７のいずれか一項に記載の方法。
【請求項９】
前記解析装置は、クラスタのトランスポート接続に関連付けられたドメイン名が、前記事前定義ウェブ閲覧セッションプロファイルにリストされたドメイン名に一致しない時には、前記クラスタは事前定義ウェブ閲覧セッションプロファイルにマッチしないと考えることを特徴とする、請求項１～８のいずれか一項に記載の方法。
【請求項１０】
前記解析装置は、前記クラスタに関連する情報と、前記事前定義ウェブ閲覧セッションプロファイルに関連する情報との差を表す情報が、第５の事前定義閾値未満である時には、前記クラスタは事前定義ウェブ閲覧セッションプロファイルにマッチすると考えることを特徴とする、請求項１～９のいずれか一項に記載の方法。
【請求項１１】
事前定義ウェブ閲覧セッションプロファイルと比較されるクラスタの任意のトランスポ

ート接続に関連付けられた各ドメインについて、
前記方法は、
‐前記クラスタのトランスポート接続の量と、前記事前定義ウェブ閲覧セッションプロファイルによって期待されるトランスポート接続の量との間の、第１の距離を決定する、第３の決定ステップと、
‐前記クラスタのトランスポート接続を介して送信されたセグメントの量と、前記事前定義ウェブ閲覧セッションプロファイルによって期待されるセグメントの量との間の、第２の距離を決定する、第４の決定ステップと、
‐前記クラスタのトランスポート接続を介して送信されたデータの量と、前記事前定義ウェブ閲覧セッションプロファイルによって期待されるデータの量との間の、第３の距離を決定する、第５の決定ステップと、
‐前記第１、第２および第３の距離の合計を決定するとともに、前記合計を第６の事前定義閾値と比較する、第６の決定ステップと
を備えることを特徴とし、かつ、
前記方法はさらに、
‐前記第１、第２および第３の距離の前記合計が前記第６の事前定義閾値未満である前記クラスタのトランスポート接続のいずれかに関連付けられたドメインの量を決定する、第７の決定ステップと、
‐前記ドメインの量が第７の事前定義閾値より大きい時に、前記クラスタは前記事前定義ウェブ閲覧セッションプロファイルにマッチすると考えることと
を備えることを特徴とする、請求項１０に記載の方法。
【請求項１２】
暗号化されたデータフローを分類する装置であって、
前記暗号化されたデータフローは、少なくとも１つのウェブクライアントと少なくとも１つのウェブサーバとの間で発生することを目的とし、かつ、前記少なくとも１つのウェブクライアントと前記少なくとも１つのウェブサーバとの間にセットアップされたトランスポート接続を介して移送されることを目的とする
装置において、
前記装置は、
‐前記トランスポート接続がそれぞれ開始された時刻を表す情報と、前記トランスポート接続のエンドポイントのアドレシングに関する情報と、前記トランスポート接続によって移送されたデータの量および／またはセグメントの量に関する情報とを決定する、第１の決定手段と、
‐いずれかのトランスポート接続のエンドポイントである各ウェブサーバが関連付けられたドメイン名を決定する、第２の決定手段と、
‐前記トランスポート接続がそれぞれ開始された時刻と、前記トランスポート接続のエンドポイントである前記ウェブクライアントのアドレシングとに関する基準に従って、トランスポート接続をクラスタにグルーピングする、グルーピング手段と、
‐各クラスタについて、そのクラスタの前記トランスポート接続に関連付けられたドメイン名およびそのクラスタの前記トランスポート接続によって移送されたデータの量および／またはセグメントの量と、事前定義ウェブ閲覧セッションプロファイルとを比較する、比較手段と、
‐前記比較手段を実施した結果に基づき、前記暗号化されたデータフローを分類する、分類手段と
を備える、装置。
【請求項１３】
プログラムコード命令を含むコンピュータプログラムであって、
前記プログラムコード命令は、前記プログラムコード命令がプログラム可能な装置によって実行される時に、請求項１～１１のいずれか一項に記載の方法を実行するために前記プログラム可能な装置にロードすることができる、

コンピュータプログラム。
【請求項１４】
プログラムコード命令を含むコンピュータプログラムを記憶する情報記憶手段であって、
前記プログラムコード命令は、前記プログラムコード命令がプログラム可能な装置によって実行される時に、請求項１～１１のいずれか一項に記載の方法を実行するために前記プログラム可能な装置にロードすることができる、
情報記憶手段。