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

特許第6836773号
(P6836773)

(45)発行日　令和3年3月3日(2021.3.3)　(24)登録日　令和3年2月10日(2021.2.10)

(51)Int.Cl.		F I		
H04L 12/66	(2006.01)	H04L	12/66	B
H04L 12/58	(2006.01)	H04L	12/58	100A
G06F 13/00	(2006.01)	G06F	13/00	625
		G06F	13/00	520A

請求項の数 13　(全 14 頁)

(21)出願番号　特願2016-222515(P2016-222515)
(22)出願日　平成28年11月15日(2016.11.15)
(65)公開番号　特開2018-82271(P2018-82271A)
(43)公開日　平成30年5月24日(2018.5.24)
審査請求日　令和1年6月19日(2019.6.19)

(73)特許権者　510068091
株式会社エヴリカ
東京都港区高輪２丁目１９番１７号４０７号
(74)代理人　100145838
弁理士　畑添　隆人
(72)発明者　山田　直樹
東京都港区高輪２丁目１９番１７号４０７号　株式会社エヴリカ内

審査官　中川　幸洋

最終頁に続く

(54)【発明の名称】情報処理装置、方法およびプログラム

(57)【特許請求の範囲】
【請求項１】
クライアントからサーバー宛に送信されたデータ要求メッセージを取得する要求取得手段と、
前記データ要求メッセージとは異なるメッセージを前記サーバーに送信することで、該データ要求メッセージによる要求の対象データを含むデータセットの構成情報を前記サーバーから取得する構成情報取得手段と、
前記データ要求メッセージに応じて前記サーバーから送信された、データ及び該データの構成情報を含む応答メッセージを、前記クライアントに代わって取得する応答取得手段と、
前記データセットの構成情報及び前記データの構成情報を、互いの整合性を維持したまま改変する構成情報改変手段と、
前記構成情報改変手段による改変後の前記データの構成情報に合致するように前記データを改変するデータ改変手段と、
前記クライアントから前記サーバー宛に送信されたデータ要求メッセージへの応答として、前記データ改変手段による改変後のデータ及び前記構成情報改変手段による改変後の該データの構成情報を含む応答メッセージを、該クライアントに対して送信するデータ送信手段と、
を備える情報処理装置。
【請求項２】

前記構成情報改変手段は、前記データの構成情報のうち、該データのサイズ情報を増加させる改変を行い、更に、前記データセットの構成情報を、増加した前記データのサイズ情報に合わせて調整する改変を行う、
請求項１に記載の情報処理装置。
【請求項３】
前記データ改変手段は、前記構成情報改変手段によって増加されたサイズ分の情報を前記データに追加する改変を行う、
請求項２に記載の情報処理装置。
【請求項４】
前記データを検査する検査手段を更に備え、
前記データ改変手段は、前記検査手段による検査結果に応じて前記データを改変する、
請求項１から３の何れか一項に記載の情報処理装置。
【請求項５】
前記データ改変手段は、前記検査手段による検査結果をユーザーに通知するための情報を前記データに追加する改変を行う、
請求項４に記載の情報処理装置。
【請求項６】
前記検査手段は、該データが前記クライアントへの転送が許可されるデータであるか否かを検査し、
前記データ改変手段は、前記検査手段による検査結果が、該データが前記クライアントへの転送が許可されるデータではないという検査結果であった場合に、前記データを、クライアントが受信してよいデータで置換する改変を行う、
請求項４または５に記載の情報処理装置。
【請求項７】
前記要求取得手段によってクライアントからサーバー宛に送信されたデータ要求メッセージが取得された後、前記サーバーに対して、前記クライアントに代わって前記データ要求メッセージを送信する要求送信手段を更に備え、
前記応答取得手段は、前記要求送信手段によって送信されたデータ要求メッセージに応じて前記サーバーから送信された応答メッセージを取得する、
請求項１から６の何れか一項に記載の情報処理装置。
【請求項８】
前記構成情報取得手段は、対象データを含むデータセットに固有の識別子を指定して、前記データセットの構成情報を前記サーバーから取得する、
請求項１から７の何れか一項に記載の情報処理装置。
【請求項９】
前記データ要求メッセージが要求の対象データを含むデータセットの識別子を指定しないメッセージである場合に、前記サーバーから該データセットの識別子を取得する識別子取得手段を更に備え、
前記構成情報取得手段は、前記識別子取得手段によって取得された前記識別子を指定して、前記データセットの構成情報を前記サーバーから取得する、
請求項８に記載の情報処理装置。
【請求項１０】
前記データ送信手段は、前記検査手段による検査が行われている間、改変後の前記構成情報の少なくとも一部を前記クライアントに送信し、前記検査手段による前記データの検査が完了した後に、未送信部分を前記クライアントに送信する、
請求項４から６の何れか一項に記載の情報処理装置。
【請求項１１】
前記データ送信手段は、前記クライアントにおける前記データの受信待ち時間がタイムアウトしない間隔で、改変後の前記構成情報の少なくとも一部を該クライアントに送信する、

請求項１０に記載の情報処理装置。
【請求項１２】
コンピューターが、
クライアントからサーバー宛に送信されたデータ要求メッセージを取得する要求取得ステップと、
前記データ要求メッセージとは異なるメッセージを前記サーバーに送信することで、該データ要求メッセージによる要求の対象データを含むデータセットの構成情報を前記サーバーから取得する構成情報取得ステップと、
前記データ要求メッセージに応じて前記サーバーから送信された、データ及び該データの構成情報を含む応答メッセージを、前記クライアントに代わって取得する応答取得ステップと、
前記データセットの構成情報及び前記データの構成情報を、互いの整合性を維持したまま改変する構成情報改変ステップと、
前記構成情報改変ステップにおける改変後の前記データの構成情報に合致するように前記データを改変するデータ改変ステップと、
前記クライアントから前記サーバー宛に送信されたデータ要求メッセージへの応答として、前記データ改変ステップにおける改変後のデータ及び前記構成情報改変ステップにおける改変後の該データの構成情報を含む応答メッセージを、該クライアントに対して送信するデータ送信ステップと、
を実行する方法。
【請求項１３】
コンピューターを、
クライアントからサーバー宛に送信されたデータ要求メッセージを取得する要求取得手段と、
前記データ要求メッセージとは異なるメッセージを前記サーバーに送信することで、該データ要求メッセージによる要求の対象データを含むデータセットの構成情報を前記サーバーから取得する構成情報取得手段と、
前記データ要求メッセージに応じて前記サーバーから送信された、データ及び該データの構成情報を含む応答メッセージを、前記クライアントに代わって取得する応答取得手段と、
前記データセットの構成情報及び前記データの構成情報を、互いの整合性を維持したまま改変する構成情報改変手段と、
前記構成情報改変手段による改変後の前記データの構成情報に合致するように前記データを改変するデータ改変手段と、
前記クライアントから前記サーバー宛に送信されたデータ要求メッセージへの応答として、前記データ改変手段による改変後のデータ及び前記構成情報改変手段による改変後の該データの構成情報を含む応答メッセージを、該クライアントに対して送信するデータ送信手段と、
として機能させるプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、ネットワーク上のデータを改変するための技術に関する。
【背景技術】
【０００２】
従来、メールの転送（ＳＭＴＰ通信）とメールの取得（ＩＭＡＰ（Ｉｎｔｅｒｎｅｔ Ｍｅｓｓａｇｅ Ａｃｃｅｓｓ Ｐｒｏｔｏｃｏｌ）通信）を中継する中継装置をキャリア設備網に設置したシステムにおいて、中継装置が、メール転送サーバーから転送されたメールを、ヘッダーを含めて圧縮し、新たなヘッダーを付与しカプセル化して、圧縮メールとしてＩＭＡＰサーバーに転送し、通信端末からのメール取得要求に対し、ＩＭＡＰサ

ーバーから取得した圧縮メールをデカプセル化して、圧縮を復元して、通信端末へ送信し、ここでメールの圧縮・復元によりＩＭＡＰの各種コマンドで不整合が発生しないように、中継装置がメールサイズなどのパラメータを変更する技術が提案されている（特許文献１を参照）。

【０００３】

また、ネットワークを流れる、ヘッダーとコンテンツを含むデータを、宛先に到達する前に取得するデータ取得部と、前記コンテンツを検査する検査部と、前記検査部による検査が行われている間、前記データの少なくとも一部を前記宛先に送信する検査中送信部と、前記検査部によるコンテンツの検査が完了した後に、該コンテンツを含むデータのうち前記検査中送信部によって送信済みの部分を除く前記データを、前記宛先に転送する転送部と、を備える情報処理装置が提案されている（特許文献２を参照）。

【先行技術文献】

【特許文献】

【０００４】

【特許文献１】特開２０１０－２７８４８４号公報

【特許文献２】特開２０１６－１６３１６２号公報

【発明の概要】

【発明が解決しようとする課題】

【０００５】

従来、ネットワーク上を流れるデータが宛先に到達する前にデータを取り込み、何らかの改変を加えてから当該宛先に転送する技術が種々存在する。しかし、通信プロトコルによっては、送受信されるデータや当該データを含むデータセットに構成情報が付されるものがあるため、このようなプロトコルが採用されている通信の場合、構成情報と矛盾しない改変しか行うことができない。また、送受信されるデータの改変に合わせて当該データに係る構成情報を改変したとしても、当該データがデータセットの一部である場合（例えば、メールの一部としてのＳＵＢＪＥＣＴである場合など）当該データを含むデータセット全体に係る構成情報との整合性が失われてしまうため、データまたはデータセットを受信するクライアント側でエラーが生じるおそれがある。

【０００６】

本開示は、上記した問題に鑑み、構成情報を伴うデータセットの一部または全部を改変する場合にも、当該構成情報の整合性が失われないようにすることを課題とする。

【課題を解決するための手段】

【０００７】

本開示の一例は、クライアントからサーバー宛に送信されたデータ要求メッセージを取得する要求取得手段と、前記データ要求メッセージによる要求の対象データを含むデータセットの構成情報を前記サーバーから取得する構成情報取得手段と、前記サーバーから送信された、データ及び該データの構成情報を含む応答メッセージを、前記クライアントに代わって取得する応答取得手段と、前記データセットの構成情報及び前記データの構成情報を、互いの整合性を維持したまま改変する構成情報改変手段と、前記構成情報改変手段による改変後の前記データの構成情報に合致するように前記データを改変するデータ改変手段と、前記クライアントから前記サーバー宛に送信されたデータ要求メッセージへの応答として、前記データ改変手段による改変後のデータ及び前記構成情報改変手段による改変後の該データの構成情報を含む応答メッセージを、該クライアントに対して送信するデータ送信手段と、を備える情報処理装置である。

【０００８】

本開示は、情報処理装置、システム、コンピューターによって実行される方法またはコンピューターに実行させるプログラムとして把握することが可能である。また、本開示は、そのようなプログラムをコンピューターその他の装置、機械等が読み取り可能な記録媒体に記録したものとしても把握できる。ここで、コンピューター等が読み取り可能な記録媒体とは、データやプログラム等の情報を電気的、磁気的、光学的、機械的または化学的

作用によって蓄積し、コンピューター等から読み取ることができる記録媒体をいう。
【発明の効果】
【０００９】
本開示によれば、構成情報を伴うデータセットの一部または全部を改変する場合にも、当該構成情報の整合性が失われないようにすることが可能となる。
【図面の簡単な説明】
【００１０】
【図１】実施形態に係るシステムの構成を示す概略図である。
【図２】実施形態に係る通信検査装置のハードウェア構成を示す図である。
【図３】実施形態に係る通信検査装置の機能構成の概略を示す図である。
【図４】実施形態に係るメッセージ処理の流れの概要を示すフローチャート（１）である。
【図５】実施形態に係るメッセージ処理の流れの概要を示すフローチャート（２）である。
【図６】実施形態においてメッセージ処理を実行した場合の通信の流れを示す図である。
【発明を実施するための形態】
【００１１】
以下、本開示に係る情報処理装置、方法およびプログラムの実施の形態を、図面に基づいて説明する。但し、以下に説明する実施の形態は、実施形態を例示するものであって、本開示に係る情報処理装置、方法およびプログラムを以下に説明する具体的構成に限定するものではない。実施にあたっては、実施の態様に応じた具体的構成が適宜採用され、また、種々の改良や変形が行われてよい。
【００１２】
本実施形態では、本開示に係る情報処理装置、方法およびプログラムを、通信検査装置において実施した場合の実施の形態について説明する。但し、本開示に係る情報処理装置、方法およびプログラムは、ネットワーク上のデータを改変するための技術について広く用いることが可能であり、本開示の適用対象は、本実施形態において示した例に限定されない。
【００１３】
＜システムの構成＞
図１は、本実施形態に係るシステム１の構成を示す概略図である。本実施形態に係るシステム１は、複数の情報処理端末９０（以下、「クライアント９０」と称する）が接続されるネットワークセグメント２と、クライアント９０に係る通信を中継するための通信検査装置２０と、を備える。また、ネットワークセグメント２内のクライアント９０は、インターネットや広域ネットワークを介して遠隔地において接続された各種のサーバーと、通信検査装置２０を介して通信可能である。本実施形態において、通信検査装置２０は、ネットワークセグメント２において、クライアント９０とインターネットとの間に接続されることで、通過するメッセージを取得する。そして、通信検査装置２０は、取得したメッセージのうち、検査対象でないメッセージ、および検査の結果転送してもよいと判定されたメッセージを転送する。
【００１４】
図２は、本実施形態に係る通信検査装置２０のハードウェア構成を示す図である。通信検査装置２０は、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）１１、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）１２、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）１３、ＥＥＰＲＯＭ（Ｅｌｅｃｔｒｉｃａｌｌｙ Ｅｒａｓａｂｌｅ ａｎｄ Ｐｒｏｇｒａｍｍａｂｌｅ Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）やＨＤＤ（Ｈａｒｄ Ｄｉｓｋ Ｄｒｉｖｅ）等の記憶装置１４、ＮＩＣ（Ｎｅｔｗｏｒｋ Ｉｎｔｅｒｆａｃｅ Ｃａｒｄ）１５等の通信ユニット、等を備えるコンピューターである。但し、通信検査装置２０の具体的なハードウェア構成に関しては、実施の態様に応じて適宜省略や置換、追加が可能である。また、通信検査装置２０は、単一の装置に限定されない。

通信検査装置２０は、所謂クラウドや分散コンピューティングの技術等を用いた、複数の装置によって実現されてよい。

【００１５】

図３は、本実施形態に係る通信検査装置２０の機能構成の概略を示す図である。通信検査装置２０は、記憶装置１４に記録されているプログラムが、ＲＡＭ１３に読み出され、ＣＰＵ１１によって実行されることで、要求取得部２１、識別子取得部２２、構成情報取得部２３、要求送信部２４、応答取得部２５、構成情報改変部２６、検査部２７、データ改変部２８およびデータ送信部２９を備える情報処理装置として機能する。なお、本実施形態では、通信検査装置２０の備える各機能は、汎用プロセッサであるＣＰＵ１１によって実行されるが、これらの機能の一部または全部は、１または複数の専用プロセッサによって実行されてもよい。また、これらの機能の一部または全部は、クラウド技術等を用いて、遠隔値に設置された装置や、分散設置された複数の装置によって実行されてもよい。

【００１６】

要求取得部２１は、クライアント９０からサーバー宛に送信されたデータ要求メッセージを取得する。要求取得部２１は、送信元、宛先およびプロトコルの種類の少なくとも何れかが所定の条件に合致するパケットを検知することで、所望のデータ要求メッセージを取得する。本実施形態では、クライアント９０からサーバー宛に送信されたデータ要求メッセージとして、ＩＭＡＰのＦＥＴＣＨメッセージが取得される場合について説明する。但し、上述の通り、本開示に係る技術の適用範囲は、本実施形態における例示に限定されない。本開示に係る技術は、データの構成を確定させる情報がデータと併せて送受信されるプロトコルを用いた通信について好適である。

【００１７】

識別子取得部２２は、データ要求メッセージが要求の対象データを含むデータセット（ＩＭＡＰの場合、一通のメール全体）に固有の（ユニークな）識別子（ＩＭＡＰの場合、ＵＩＤ）を指定しないメッセージである場合に、サーバーから当該データセットの識別子を取得する。例えば、ＩＭＡＰの場合、データ要求メッセージであるＦＥＴＣＨメッセージには、ＵＩＤが指定されている場合と、指定されていない場合がある。クライアント９０から受信したＦＥＴＣＨメッセージにＵＩＤが指定されておらず、メール番号（同一セッション内でのみ有効な識別子）のみが指定されている場合、識別子取得部２２は、サーバーに対して、当該セッション中の当該メール番号を指定して当該メール（データセット）のＵＩＤを問い合わせることで、対象データ（本実施形態では、メールの一部または全部。例えば、メール内のＨＥＡＤＥＲやＳＵＢＪＥＣＴ、ＢＯＤＹ等）を含むデータセット（メール全体）のＵＩＤを取得する。

【００１８】

構成情報取得部２３は、要求取得部２１によってデータ要求メッセージが取得されると、当該データ要求メッセージによる要求の対象データを含むデータセットの構成情報（ＩＭＡＰの場合、あるメール全体の構成情報）を、サーバーから取得する。この際、構成情報取得部２３は、対象データを含むデータセットに固有の識別子を指定して、データセットの構成情報をサーバーから取得する。ここで指定される識別子は、データ要求メッセージにおいてクライアント９０に指定されたものであってもよいし、識別子取得部２２によって取得されたものであってもよい。

【００１９】

要求送信部２４は、要求取得部２１によってデータ要求メッセージが取得された後、サーバーに対して、クライアント９０に代わってデータ要求メッセージを送信する。即ち、本実施形態において、通信検査装置２０は、クライアント９０とサーバーとの間で一種のプロキシとして動作し、要求送信部２４は、クライアント９０から送信されたサーバー宛のデータ要求メッセージを、クライアント９０に代わって、サーバーに対して送信する。

【００２０】

応答取得部２５は、要求送信部２４によって送信されたデータ要求メッセージに応じてサーバーから送信された、データ及び当該データの構成情報を含む応答メッセージを、ク

ライアント９０に代わって、宛先（クライアント９０）に到達する前に取得する。
【００２１】
構成情報改変部２６は、データセットの構成情報及びデータの構成情報を、互いの整合性を維持したまま改変する。例えば、構成情報改変部２６は、データの構成情報のうち、当該データのサイズ情報を所定量分増加させる改変（例えば、メールのＳＵＢＪＥＣＴのサイズ情報を１０バイト増加させる改変）を行い、更に、データセットの構成情報を、増加したデータのサイズ情報に合わせて調整する改変（例えば、メール全体のサイズ情報を１０バイト増加させる改変）を行う。
【００２２】
検査部２７は、応答取得部２５によって取得されたデータが、クライアント９０への転送が許可されるデータであるか否かを、予め定められた検査項目に従って検査する。例えば、検査部２７は、コンテンツにマルウェアが含まれているか否か、コンテンツに望ましくない表現が含まれているか否か、等を検査する。検査手法としては、例えば、パターンマッチングやハッシュ演算等を採用することができる。但し、本開示に係る検査において採用され得る具体的な検査項目や検査手法は、本実施形態における例示に限定されない。具体的な検査項目や検査手法には、既知の、または将来開発される様々な検査項目および検査手法が採用されてよい。
【００２３】
データ改変部２８は、検査部２７による検査結果に応じてデータを改変する。例えば、データ改変部２８は、検査結果をユーザーに通知するための情報をデータに追加する改変（例えば、メールのＳＵＢＪＥＣＴに検査結果を示す文字列を追加する改変）や、データが有害なデータであり、クライアント９０への転送が許可されないとの検査結果であった場合に、当該データを無害化する改変等を行う。無害化とは、例えば、データの一部または全部を、クライアント９０が受信してよいデータで置換する処理などである。
【００２４】
改変の際、データ改変部２８は、構成情報改変部２６による改変後のデータの構成情報に合致するようにデータを改変する。例えば、構成情報改変部２６によってデータのサイズ情報を増加させる改変が行われた場合、データ改変部２８は、増加されたサイズ分の情報をデータに追加する改変を行う。
【００２５】
データ送信部２９は、クライアント９０からサーバー宛に送信されたデータ要求メッセージへの応答として、データ改変部２８による改変後のデータ及び構成情報改変部２６による改変後の構成情報を含む応答メッセージを、当該クライアント９０に対して送信する。また、データ送信部２９は、検査部２７による検査が行われている間、クライアント９０におけるデータの受信待ち時間がタイムアウトしない間隔で、改変後の構成情報の少なくとも一部をクライアント９０に送信する。そして、データ送信部２９は、検査部２７によるデータの検査が完了した後に、未送信部分をクライアント９０に送信する。
【００２６】
＜処理の流れ＞
次に、本実施形態に係るシステム１によって実行される処理の流れを、フローチャートを用いて説明する。なお、以下に説明するフローチャートに示された処理の具体的な内容および処理順序は、本開示を実施するための一例である。具体的な処理内容および処理順序は、本開示の実施の形態に応じて適宜選択されてよい。
【００２７】
図４および図５は、本実施形態に係るメッセージ処理の流れの概要を示すフローチャートである。本実施形態に係るメッセージ処理は、通信検査装置２０によって、ネットワーク上を流れるメッセージが受信されたことを契機として実行される。
【００２８】
ステップＳ１０１では、データ要求メッセージ（本実施形態では、クライアント９０からサーバーへのＩＭＡＰのＦＥＴＣＨメッセージ）が取得される。要求取得部２１は、受

信されたパケットのヘッダーに設定されている送信元、宛先及びプロトコル番号等を参照して、取り込みの対象となるパケットであるか否かを判定し、取り込みの対象となるパケットを取り込み、ＲＡＭ１２に記憶する（所謂フック処理）。ここで取り込まれたメッセージの転送は、ステップＳ１０８まで保留される。取り込みの対象でないと判定されたパケットは、通信検査装置２０に取り込まれることなく、宛先に転送される（図示は省略する）。

【００２９】

取り込みの対象であるか否かは、パケットの送信元および宛先が、予め設定された送信元ＩＰアドレスおよび宛先ＩＰアドレスのリストに登録されているか否かを照合すること、及びパケットの種類があらかじめ設定された種類のもの（本実施形態では、ＩＭＡＰのＦＥＴＣＨメッセージ）であるか否かを照合することによって判定される。なお、パケットが取り込みの対象であるか否かの判定には、本開示とは異なる手法が採用されてもよい。その後、処理はステップＳ１０２へ進む。

【００３０】

ステップＳ１０２では、ＦＥＴＣＨメッセージの要求対象がＵＩＤのみであるか否かが判定される。ＣＰＵ１１は、ステップＳ１０１で取り込まれたＦＥＴＣＨメッセージによって要求されるデータが、データセット（本実施形態では、ＩＭＡＰメール）に固有の識別子であるＵＩＤのみであるか否かを判定する。要求されたデータがＵＩＤのみである場合、この要求のみではクライアント９０にはメールの構成情報は渡されず構成情報の改変も不要であるため、ステップＳ１０３からステップＳ１０７の処理はスキップされ、処理はステップＳ１０８へ進む。一方、要求されたデータがＵＩＤ以外のデータを含む場合、この要求に応じてクライアント９０に対して渡される構成情報を改変する必要があるため、処理はステップＳ１０３へ進む。

【００３１】

ステップＳ１０３及びステップＳ１０４では、ＦＥＴＣＨメッセージに要求対象のＵＩＤが指定されていない場合に、ＵＩＤが取得される。識別子取得部２２は、ステップＳ１０１で取り込まれたＦＥＴＣＨメッセージに、要求されるデータが属するメールのＵＩＤが指定されているか否かを判定する（ステップＳ１０３）。ＦＥＴＣＨメッセージでＵＩＤが指定されている場合、処理はステップＳ１０５へ進む。一方、ＦＥＴＣＨメッセージでＵＩＤが指定されていない場合、メール全体の構成情報の取得に先立ってメールのＵＩＤを取得するため、識別子取得部２２は、サーバーから当該メールの識別子を取得する（ステップＳ１０４）。

【００３２】

具体的には、識別子取得部２２は、サーバーに対して、ＦＥＴＣＨメッセージ中に指定されたメール番号（当該メッセージが属するセッション内でのみ有効な識別子）を指定して、当該メールのＵＩＤを問い合わせることで、対象データ（例えば、メールのＨＥＡＤＥＲやＳＵＢＪＥＣＴ、ＢＯＤＹ等）を含むメール全体のＵＩＤを取得する。その後、処理はステップＳ１０５へ進む。

【００３３】

ステップＳ１０５では、ＦＥＴＣＨメッセージに係るＵＩＤ及びメール全体の構成情報が既に保持されているか否かが判定される。ＣＰＵ１１は、ＦＥＴＣＨメッセージに指定されたＵＩＤまたはステップＳ１０４で取得されたＵＩＤと、通信検査装置２０に保持されているＵＩＤのリストとを比較することで、ＦＥＴＣＨメッセージに係るＵＩＤと、このＵＩＤが示すメール全体の構成情報とが、通信検査装置２０に保持されているか否かを判定する。対象メールのＵＩＤ及び構成情報が保持されている場合、処理はステップＳ１０８へ進む。一方、対象メールのＵＩＤ及び構成情報が保持されていない場合、処理はステップＳ１０６へ進む。

【００３４】

ステップＳ１０６では、要求の対象となっているデータを含むメール全体の構成情報が取得される。構成情報取得部２３は、ステップＳ１０１で取得されたＦＥＴＣＨメッセー

ジによる要求の対象データを含むメールの構成情報を、サーバーから取得する。この際、構成情報取得部２３は、対象データを含むメールのＵＩＤを指定して、メールの構成情報をサーバーから取得する。

【００３５】

ここで、メールの構成情報の取得方法について、より具体的な例を挙げて説明する。構成情報取得部２３は、メール全体に係る構成情報を取得するため、メールヘッダーを含むメール全体のサイズ情報、メールヘッダーのサイズ情報、及びメール本体に含まれる各構成要素（例えば、件名及び本文）のサイズ情報を要求するための複数のメッセージを、サーバーに対して送信する。これらのメッセージが、ＵＩＤを指定して通信検査装置２０からサーバー宛に送信され、サーバーから送信された応答を受信することで、通信検査装置２０は、指定されたＵＩＤに係るメール全体の構成情報を得ることができる。構成情報を取得するために通信検査装置２０からサーバー宛に送信されるメッセージと、サーバーから応答される内容との対応関係は、以下の通りである。

UID FETCH 1 RFC822.HEADER：メールヘッダー及びそのサイズ情報

UID FETCH 1 FULL ：メールの全情報およびメールのサイズ情報

UID FETCH 1 BODY[header.fields (subject)] ：ＳＵＢＪＥＣＴ及びそのサイズ情報

その後、処理はステップＳ１０７へ進む。

【００３６】

ステップＳ１０７では、ＵＩＤ及び構成情報が保存される。ＣＰＵ１１は、ステップＳ１０６で取得された構成情報（ヘッダーのサイズ情報、ＳＵＢＪＥＣＴのサイズ情報、メール全体のサイズ情報及びメール全体の構造）を、対応するＵＩＤに関連付けてＲＡＭ１３または記憶装置１４等に保存する。ここで保存されたＵＩＤ及び対応する構成情報は、クライアント９０から送信された他のＦＥＴＣＨメッセージが受信された際のメッセージ処理において、ステップＳ１０５で参照される。その後、処理はステップＳ１０８へ進む。

【００３７】

ステップＳ１０８では、ＦＥＴＣＨメッセージが送信される。要求送信部２４は、ステップＳ１０１で取得されたＦＥＴＣＨメッセージの宛先に設定されていたサーバーに接続し、ステップＳ１０１で取得されたＦＥＴＣＨメッセージを、サーバーに送信する。即ち、通信検査装置２０は、クライアント９０に代わって、サーバーに対するデータ要求を行う。この際、要求送信部２４は、ステップＳ１０１で取得されたＦＥＴＣＨメッセージに指定されていたＵＩＤ、ステップＳ１０４で取得されたＵＩＤ、または通信検査装置２０が保持していたＵＩＤを指定したＦＥＴＣＨメッセージを送信してもよい。また、要求送信部２４は、ステップＳ１０１で受信されたメッセージをそのままサーバーに転送してもよいし、必要に応じて送信元ＩＰアドレスを通信検査装置２０のＩＰアドレスに変換してからサーバーに送信してもよい。その後、処理はステップＳ１０９へ進む。

【００３８】

ステップＳ１０９では、サーバーから送信されたデータが受信される。応答取得部２５は、ステップＳ１０８で送信されたＦＥＴＣＨメッセージへの応答メッセージとしてサーバーから送信された、データ及び当該データの構成情報を含む応答メッセージを、クライアント９０に到達する前に取得する。この時点において、通信検査装置２０は、クライアント９０の要求に係るデータを、クライアント９０には送信しない。なお、応答メッセージは複数パケットに分けて取得される場合があるが、検査部２７による応答メッセージに含まれるデータの検査は、複数のパケットの全て受信される前に開始されてもよい。その後、処理はステップＳ１１０へ進む。

【００３９】

ステップＳ１１０及びステップＳ１１１では、ＦＥＴＣＨメッセージによって取得されたデータがＵＩＤのみであった場合に、取得されたＵＩＤが保存される。ステップＳ１１０における具体的な判定内容はステップＳ１０２と同様であるため、説明を省略する。ステップＳ１０８で取得されたデータがＵＩＤのみである場合、ＣＰＵ１１は、当該ＵＩＤ

をＲＡＭ１３または記憶装置１４等に保存する（ステップＳ１１１）。ここで保存されたＵＩＤは、クライアント９０から送信された他のＦＥＴＣＨメッセージが受信された際に、ステップＳ１０５で参照される。

【００４０】

そして、取得されたデータがＵＩＤのみである場合、検査は不要であるため、ステップＳ１１２からステップＳ１１５の処理はスキップされ、処理はステップＳ１１６へ進む。一方、要求されたデータがＵＩＤ以外のデータを含む場合、その応答として受信されたデータを検査する必要があるため、処理はステップＳ１１２へ進む。

【００４１】

ステップＳ１１２では、構成情報が改変される。構成情報改変部２６は、ステップＳ１０６で取得されたメール全体の構成情報、及びステップＳ１０９で取得されたデータの構成情報を、互いの整合性を維持したまま改変する。本実施形態に示す例では、構成情報改変部２６は、メール全体の構成情報のうち、メールの件名のサイズ情報を所定量分（例えば、１０バイト）増加させる改変を行う。更に、これに伴って、構成情報改変部２６は、メール全体の構成情報を、件名のサイズ情報の増加に合わせて調整する改変を行う。具体的には、構成情報改変部２６は、メール全体のサイズ情報を所定量分（例えば、１０バイト）増加させる改変を行う。その後、処理はステップＳ１１３およびステップＳ１１４へ進む。

【００４２】

ステップＳ１１３では、受信されたデータが検査される。検査部２７は、ステップＳ１０９で取得されたデータが、クライアント９０への転送が許可されるコンテンツであるか否かを、予め定められた検査項目に従って検査する。なお、検査結果は、対応するＵＩＤに関連付けてＲＡＭ１３または記憶装置１４等に保存される。その後、処理はステップＳ１１５へ進む。

【００４３】

ステップＳ１１４では、応答メッセージの一部が送信される。データ送信部２９は、ステップＳ１１３の検査が行われている間、改変後の構成情報またはデータの少なくとも一部を、クライアント９０に送信する。本ステップにおける構成情報／データの一部送信処理は、クライアント９０におけるデータの受信待ち時間がタイムアウトしない間隔で、検査が終了するまで繰り返される。この場合、検査中に送信される構成情報にはデータのサイズ情報等も含まれるが、サイズ情報はステップＳ１１２で改変済みであるため、クライアントに送信しても問題ない。検査が終了した場合、処理はステップＳ１１５へ進む。

【００４４】

より具体的には、データ送信部２９は、改変後の構成情報を、前方から順に所定のバイト数または所定の行数ずつ切り出して、所定の時間ごとに送信する、このような処理を行うことで、データの検査中に、クライアント９０におけるデータ待受時間がタイムアウトすることを防止できる。例えば、ある種のクライアント９０では、１行受信するごとにデータ待受時間をリセットする（換言すれば、改行コードが受信されるまでデータ待受時間がリセットされない）ため、データ送信部２９は、検査中、応答メッセージを少なくとも１行ずつ送信する。

【００４５】

なお、検査に長い時間がかかる場合、構成情報のみではタイムアウト防止のために送信するデータが不足する可能性がある。この場合、データ送信部２９は、検査済みのデータ本体を少しずつ順に送信してもよいし、宛先に受信されるコンテンツを確定させない構成情報（例えば、名称が「X-」から始まる、自由に追加できるメールヘッダー。以下、「Ｘヘッダー」と称する）を新たに生成して送信してもよい。但し、構成情報にＸヘッダー等を追加する場合、追加するＸヘッダーの量に応じた構成情報の改変を、ステップＳ１１２において事前に行っておく必要がある。この場合、ステップＳ１０９で構成情報およびデータを含む応答メッセージを取得した後、取得された構成情報およびデータのサイズおよび検査部２７の処理能力に基づいて検査に必要な時間を算出し、必要な検査時間に応じて

、生成すべきＸヘッダーの量を算出することが好ましい。

【００４６】

ステップＳ１１５では、データ本体が改変される。データ改変部２８は、検査部２７による検査結果に応じてデータを改変する。具体的には、データ改変部２８は、検査結果をユーザーに通知するために、メールの件名を改変する。

【００４７】

本実施形態では、サイズ情報を所定量分（ここでは１０バイトとして説明する）増加させる改変が行われている。このため、例えば、検査の結果、メールがフィッシングメールであると判定された場合、件名に、「[PHISHING]」という１０バイト分の文字列を追加する改変を行う。また、検査の結果、メールがスパムメールであると判定された場合、件名に、「[SPAM]」の６バイト及び4バイトの空白、合わせて１０バイト分の文字列を追加する改変を行う。ステップＳ１１２で予め件名データのサイズ情報を１０バイト増加させる改変を行っているため、以降クライアント９０へ当該ＵＩＤに関して送信されるデータの構成情報を改変後のものとすることで、クライアント９０においてメール全体の構成情報を矛盾させることなく、情報の追加を行うことができる。なお、検査の結果、データに何も問題がなく、そのままクライアント９０へ送信されて良いデータであるとの検査結果が得られた場合にも、構成情報は１０バイト分増加済みであるため、１０バイト分の空白を件名に追加する改変が行われる。

【００４８】

データ改変部２８は、検査結果をユーザーに通知するために、メールヘッダーを改変してもよい。例えば、メールヘッダーであれば、自由に追加できるＸヘッダーを利用して、「X-SPAM-CORE: 111/222 Rating 5」のように、より詳細な検査結果を付すことも可能である（例えば、例示したＸヘッダーは、閾値２２２のうちスパムらしさのポイントが１１１であり、危険度が５であることを示している）。この場合、ステップＳ１１２において、メールヘッダーのサイズ情報を、予め必要なバイト数分増加させる改変を行えばよい。

【００４９】

また、データ改変部２８は、データが有害なデータであり、クライアント９０への転送が許可されないとの検査結果であった場合に、当該データを無害化する改変等を行ってもよい。データ改変部２８は、例えば、データの一部または全部を、クライアント９０が受信してよいデータで置換することで、データを無害化することが出来る。その後、処理はステップＳ１１６へ進む。

【００５０】

ステップＳ１１６では、クライアント９０宛に応答メッセージの未送信部分が送信される。データ送信部２９は、ステップＳ１０１で取得されたクライアント９０からサーバー宛のＦＥＴＣＨメッセージへの応答メッセージを、クライアント９０に対して送信する。

【００５１】

ここで、ＦＥＴＣＨメッセージの要求対象がＵＩＤであった場合（ステップＳ１１０のＹＥＳ）、データ送信部２９は、応答メッセージとしてのＵＩＤをそのままクライアントに対して送信する。

【００５２】

一方、ＦＥＴＣＨメッセージの要求対象がＵＩＤ以外のデータを含む場合、データ送信部２９は、ステップＳ１１５での改変後のデータ及びステップＳ１１２での改変後の当該データの構成情報を含む応答メッセージの未送信部分（即ち、ステップＳ１１４で送信済みの部分を除いた応答メッセージ）を、クライアントに対して送信する。その後、本フローチャートに示された処理は終了する。

【００５３】

図６は、本実施形態において上記説明したメッセージ処理を実行した場合の通信の流れを示す図である。クライアントがデータ要求メッセージ（FETCH 1 BODY）を送信すると、はこれを取得し（ステップＳ１０１）、サーバーから対象メールのＵＩＤ、メールヘッダーサイズ情報、メールサイズ情報及びＳＵＢＪＥＣＴサイズ情報、即ち、メール全体の構

成情報を取得する（ステップＳ１０６）。

【００５４】

メール全体の構成情報が取得されると、通信検査装置２０は、クライアントが要求するデータを取得するためのデータ要求メッセージ（FETCH 1 BODY）をサーバーに送信する（ステップＳ１０８）。そして、通信検査装置２０は、要求されたデータ及び構成情報をサーバーから受信すると、検査を開始し（ステップＳ１１３）、検査中にはクライアント側でのセッションタイムアウトを防止するために改変済みの構成情報を少しずつ送信する（ステップＳ１１４）。ここで送信される構成情報は、改変済（ステップＳ１１２）の構成情報である。検査が終了すると、通信検査装置２０は、検査結果に応じて改変（ステップＳ１１５）したデータを、未送信の構成情報とともにクライアントへ送信する（ステップＳ１１６）。

【００５５】

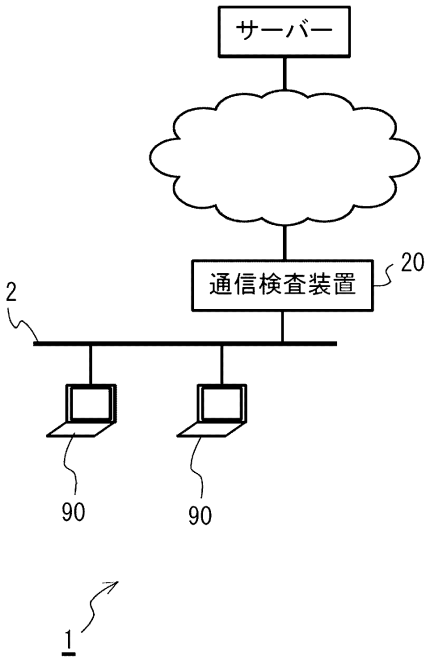
なお、本実施形態では、本発明をＩＭＡＰにおいて用いる例について説明したが、本発明を適用可能なプロトコルは、本実施形態における開示に限定されない。本発明は、データの構成を確定させる情報がデータと併せて送受信されるプロトコル全般に適用することが可能である。

【符号の説明】

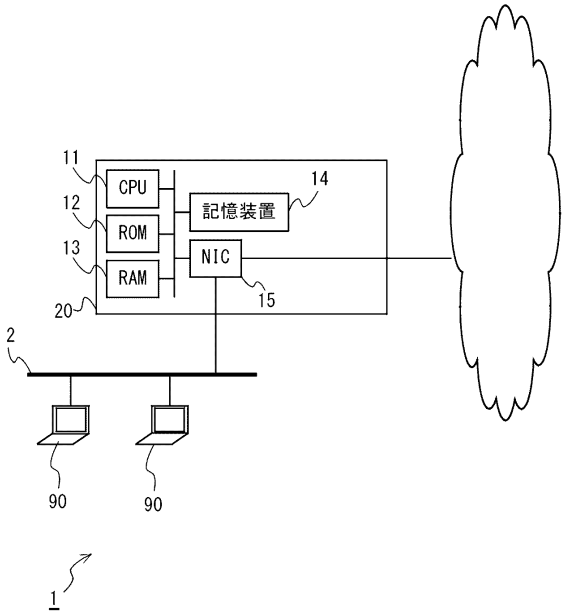
【００５６】

１　システム
２０　通信検査装置
９０　クライアント

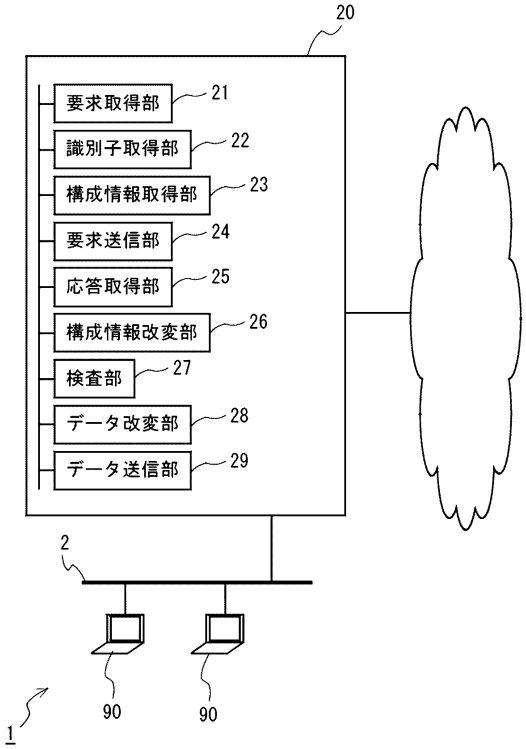
【図１】



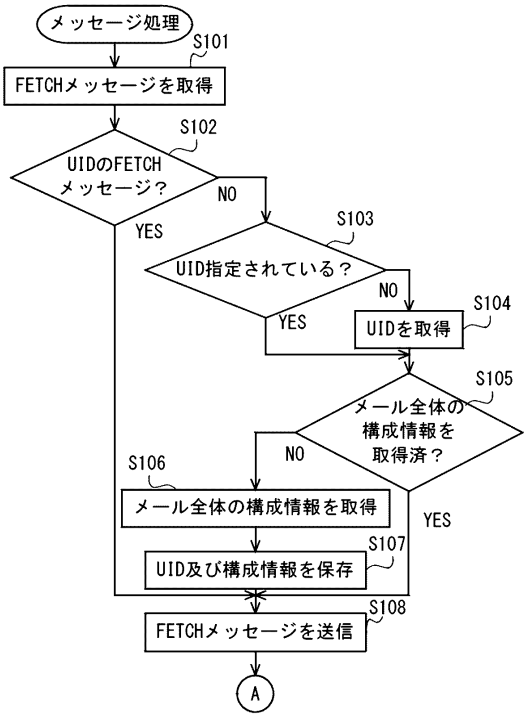
【図２】



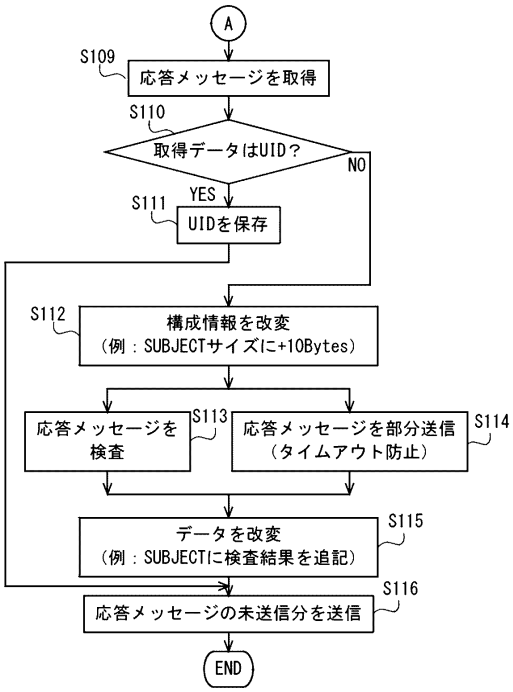
【図３】


20
要求取得部
21
識別子取得部
22
構成情報取得部
23
要求送信部
24
応答取得部
25
構成情報改変部
26
検査部
27
データ改変部
28
データ送信部
29
2
90
90
1

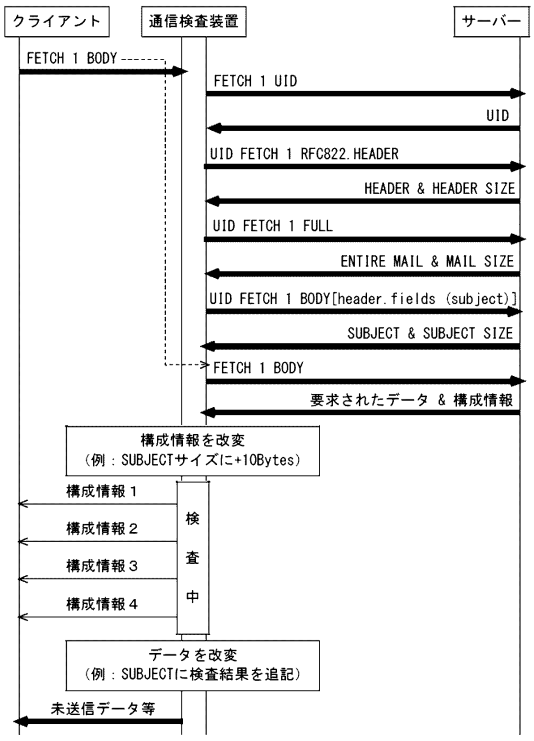
【図４】


メッセージ処理
S101
FETCHメッセージを取得
S102
UIDのFETCH
メッセージ？
NO
YES
S103
UID指定されている？
NO
YES
S104
UIDを取得
S105
メール全体の
構成情報を
取得済？
NO
YES
S106
メール全体の構成情報を取得
S107
UID及び構成情報を保存
S108
FETCHメッセージを送信
A

【図５】


A
S109
応答メッセージを取得
S110
取得データはUID？
NO
YES
S111
UIDを保存
S112
構成情報を改変
（例：SUBJECTサイズに+10Bytes）
応答メッセージを
検査
S113
応答メッセージを部分送信
（タイムアウト防止）
S114
データを改変
（例：SUBJECTに検査結果を追記）
S115
応答メッセージの未送信分を送信
S116
END

【図６】


クライアント
通信検査装置
サーバー
FETCH 1 BODY
FETCH 1 UID
UID
UID FETCH 1 RFC822.HEADER
HEADER & HEADER SIZE
UID FETCH 1 FULL
ENTIRE MAIL & MAIL SIZE
UID FETCH 1 BODY[header.fields (subject)]
SUBJECT & SUBJECT SIZE
FETCH 1 BODY
要求されたデータ & 構成情報
構成情報を改変
（例：SUBJECTサイズに+10Bytes）
構成情報１
構成情報２
構成情報３
構成情報４
検査中
データを改変
（例：SUBJECTに検査結果を追記）
未送信データ等

フロントページの続き

(56)参考文献 特開２０１６－１６３１６２（ＪＰ，Ａ）
特開２０１０－０６２７７６（ＪＰ，Ａ）
特開２００５－１４９１２４（ＪＰ，Ａ）
国際公開第２００５／０９１５８１（WO，Ａ１）
迷惑メール完全撃退法，YOMIURI PC，２００８年 3月 1日，第１３巻 第３号

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ １２／６６
Ｇ０６Ｆ １３／００
Ｈ０４Ｌ １２／５８