(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6085978号
(P6085978)
(45)発行日　平成29年3月1日(2017.3.1)　(24)登録日　平成29年2月10日(2017.2.10)

(51)Int.Cl.　F I
G06F 13/00 (2006.01)　G06F 13/00 610Q

請求項の数 8　(全 20 頁)

(21)出願番号　特願2013-17237(P2013-17237)
(22)出願日　平成25年1月31日(2013.1.31)
(65)公開番号　特開2014-149619(P2014-149619A)
(43)公開日　平成26年8月21日(2014.8.21)
審査請求日　平成27年10月7日(2015.10.7)

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100107766
弁理士　伊東　忠重
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100146776
弁理士　山口　昭則
(72)発明者　吉岡　孝司
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

審査官　佐々木　洋

最終頁に続く

(54)【発明の名称】メール処理方法、メール処理プログラム及びメール処理装置

(57)【特許請求の範囲】
【請求項１】
送信メールの対象ヘッダ項目と秘密共有情報とを基に検証情報を生成する処理と、
前記検証情報に前記対象ヘッダ項目のメタ情報を結合する処理と、
前記メタ情報が結合された前記検証情報を前記送信メールのメールヘッダに結合する処理と、をメールを送信する第１のコンピュータが実行し、
受信メールのメールヘッダから、検証情報とメタ情報とを分離する処理と、
分離した前記メタ情報を基に前記メールヘッダから対象ヘッダ項目を取得する処理と、
取得した前記対象ヘッダ項目と前記秘密共有情報とを基に検証情報を再生成する処理と、
分離した前記検証情報と再生成した前記検証情報とを比較する処理と、をメールを受信する第２のコンピュータが実行し、
前記第１のコンピュータは、
前記検証情報に前記対象ヘッダ項目のメタ情報を結合する処理にて、前記検証情報にさらに前記対象ヘッダ項目の所定の部分から算出した特徴量を結合し、
前記第２のコンピュータは、
前記分離する処理にて、前記受信メールのメールヘッダからさらに前記特徴量を分離し、
取得した前記対象ヘッダ項目から特徴量を算出する処理と、
算出した前記特徴量と分離した前記特徴量とを比較する処理を実行するメール処理方法

。
【請求項２】
前記第１のコンピュータは、
前記算出する処理にて、前記対象ヘッダ項目の指定部分について特徴量を算出する請求項１に記載のメール処理方法。
【請求項３】
コンピュータが電子メールを送信する際に、該コンピュータを、
情報の入出力を行う入出力部と、
送信メールの対象ヘッダ項目と秘密共有情報とを基に検証情報を生成し、前記検証情報に前記対象ヘッダ項目のメタ情報を結合する検証情報生成部と、
前記メタ情報が結合された前記検証情報を前記送信メールのメールヘッダに結合する処理部として機能させ、
前記検証情報生成部は、前記検証情報にさらに前記対象ヘッダ項目の所定の部分から算出した特徴量を結合するメール処理プログラム。
【請求項４】
コンピュータが電子メールを受信する際に、該コンピュータを、
情報の入出力を行う入出力部と、
受信メールのメールヘッダから、検証情報とメタ情報と特徴量とを分離する分離部と、
分離した前記メタ情報を基に前記メールヘッダから対象ヘッダ項目を取得する取得部と、
取得した前記対象ヘッダ項目と秘密共有情報とを基に検証情報を再生成する再生成部と、
分離した前記検証情報と再生成した前記検証情報とを比較する検証部と、
取得した前記対象ヘッダ項目から特徴量を算出する特徴量算出部と、
算出した前記特徴量と分離した前記特徴量とを比較する比較部として機能させるメール処理プログラム。
【請求項５】
送信メールの対象ヘッダ項目と秘密共有情報とを基に検証情報を生成する検証情報生成部と、
前記検証情報に前記対象ヘッダ項目のメタ情報を結合し、前記メタ情報が結合された前記検証情報を前記送信メールのメールヘッダに結合する検証情報結合部と、を備え、
前記検証情報生成部は、前記検証情報にさらに前記対象ヘッダ項目の所定の部分から算出した特徴量を結合するメール処理装置。
【請求項６】
受信メールのメールヘッダから、検証情報とメタ情報と特徴量とを分離する分離部と、
分離した前記メタ情報を基に前記メールヘッダから対象ヘッダ項目を取得する取得部と、
取得した前記対象ヘッダ項目と秘密共有情報を基に検証情報を再生成する再生成部と、
分離した前記検証情報と再生成した前記検証情報とを比較する検証部と、
取得した前記対象ヘッダ項目から特徴量を算出する特徴量算出部と、
算出した前記特徴量と分離した前記特徴量とを比較する比較部を備えたメール処理装置。
【請求項７】
送信メールの対象ヘッダ項目と秘密共有情報とを基に検証情報を生成する処理と、
前記検証情報に前記対象ヘッダ項目のメタ情報を結合する処理と、
前記メタ情報が結合された前記検証情報を前記送信メールのメールヘッダに結合する処理と、をメールを送信するコンピュータが実行し、
前記検証情報に前記対象ヘッダ項目のメタ情報を結合する処理にて、前記検証情報にさらに前記対象ヘッダ項目の所定の部分から算出した特徴量を結合する、メール処理方法。
【請求項８】

受信メールのメールヘッダから、検証情報とメタ情報とを分離する処理と、
分離した前記メタ情報を基に前記メールヘッダから対象ヘッダ項目を取得する処理と、
取得した前記対象ヘッダ項目と秘密共有情報とを基に検証情報を再生成する処理と、
分離した前記検証情報と再生成した前記検証情報とを比較する処理と、
前記分離する処理にて、前記受信メールのメールヘッダからさらに特徴量を分離し、
取得した前記対象ヘッダ項目から特徴量を算出する処理と、
算出した前記特徴量と分離した前記特徴量とを比較する処理と、をメールを受信するコンピュータが実行するメール処理方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、メール処理方法、メール処理プログラム及びメール処理装置に関する。

【背景技術】

【０００２】

近年，メールを送りつける当事者を特定し、メールの中に組み込まれた不正プログラムにより機密情報の窃取や個人情報の流出を実行させる標的型メールが増加している。標的型メールの特徴は、受信者が思わず開いてしまいそうになる、実在の人物を装った送信者、メールの件名、あるいは添付ファイルの名称等を使用して、受信者に一見して怪しいとは思わせない偽装がされている点にあり、電子メールヘッダのチェックだけでは標的型メールによる攻撃を防ぐことが難しかった。メールの受信者がメールヘッダの偽装に気付かずに添付ファイルやリンク先を開いてしまうと、不正プログラムが実行されて、受信者のコンピュータに記憶された情報が流出したり、受信者のコンピュータがコンピュータウイルスに感染したりする場合があった。

【０００３】

従来の対策技術は、メールサーバ側での対策を行うものと、クライアントベースで対策を行うものの２種類の対策が存在していた。

【０００４】

メールサーバ側で対策を行うものとして、例えば「送信ドメイン認証」がある。これは、送信メールサーバの正当性、送信経路の証跡をサーバベースで実現する技術である。具体的には、電子メールアドレスのドメインをチェックし、その電子メールが正規のサーバから発信されているか否かを検証し、送信者のアドレスが正規のものであることを証明する技術である。送信ドメイン認証の種類として、主に、ＩＰアドレスによる認証と、電子署名による認証の２つがある。

【０００５】

ＩＰアドレスによる認証としては、例えば、ＳＰＦ（Ｓｅｎｄｅｒ Ｐｏｌｉｃｙ Ｆｒａｍｅｗｏｒｋ）／Ｓｅｎｄｅｒ ＩＤで、電子メールサーバのドメインと送信者のＩＰアドレスの関連（ＳＰＦレコード）をＤＮＳ（Ｄｏｍａｉｎ Ｎａｍｅ Ｓｙｓｔｅｍ）サーバに公開し、受信時に送信者ＩＰアドレスをＤＮＳサーバに問い合わせ、照合を行うことで、送信者のアドレスが正規のものであることを確認する技術があった。

【０００６】

電子署名による認証としては、例えば、ＤＫＩＭ（ＤｏｍａｉｎＫｅｙｓ Ｉｄｅｎｔｉｆｉｅｄ Ｍａｉｌ）で、電子メールサーバの公開鍵情報をＤＮＳサーバに公開し、秘密鍵で電子署名を結合して電子メール送信。受信時に公開鍵情報をＤＮＳサーバに問い合わせ、照合を行うことで、送信者のアドレスが正規のものであることを確認する技術があった。また、送信者から送信されたメールを受信者に中継する中継サーバにて、メールの正当性を判定して、判定結果をメールヘッダ等に追記する方法があった（例えば、非特許文献１、非特許文献２、特開２００６－９４４２２号公報を参照）。

【０００７】

一方、クライアントベースで対策を行うものとして、ウイルス対策ソフトによる検出方法があったが、従来のウイルス対策ソフトでは、問題のあるプログラムをシグネチャとし

て登録し、合致するものを不正メールとして検出していたが、シグネチャのないプログラムでは検出できず、不正なプログラムを予想するウイルス対策ソフトであっても、標的型メールを防ぐことは困難であった。

【０００８】

発明者らは、上記問題を解決するために、クライアントベースで標的型攻撃メールなどの不正メールを検知することを目的としたメール配送システムを発明している（特願２０１２－１０８０９２、以下「先願発明」という。）。先願発明では、送受信端末で連携し、攻撃者が知り得ない秘密情報を共有し、送信端末側で送信するメールヘッダを基にして生成した秘密情報をメールヘッダに結合することにより、受信側でメールヘッダを秘密情報により検証して、不正メールの可能性を判定する方法を提案している。

【先行技術文献】

【非特許文献】

【０００９】

【非特許文献１】Ｓｅｎｄｅｒ　Ｐｏｌｉｃｙ　Ｆｒａｍｅｗｏｒｋ　Ｐｒｏｊｅｃｔ　Ｏｖｅｒｖｉｅｗ、インターネット＜ｈｔｔｐ：／／ｗｗｗ．ｏｐｅｎｓｐｆ．ｏｒｇ／＞

【非特許文献２】ＤＫＩＭ．ｏｒｇ、インターネット＜ｈｔｔｐ：／／ｗｗｗ．ｄｋｉｍ．ｏｒｇ／＞

【特許文献】

【００１０】

【特許文献１】特開２００６－９４４２２号公報

【発明の概要】

【発明が解決しようとする課題】

【００１１】

しかしながら、標的型メールは送信アドレスも偽装されるため、正規サーバを利用して送信された場合には、本人性を担保することができなかった。また、ＤＮＳサーバを設置する必要があり、運用コストが大きくなる問題があった。

【００１２】

また、先願発明では、メーリングリストのように、件名（Ｓｕｂｊｅｃｔ）の先頭に連番等の独自項目を結合するなど、メールヘッダを善意で買い換えた場合、送信側端末で生成した秘密情報とメールヘッダの情報とが対応しなくなり、受信側端末での検証ができなくなってしまう場合があった。

【００１３】

そこで、一側面では、メーリングリストのソフトウエアによってメールヘッダが書き換えられた場合であっても受信側端末でメールヘッダの検証可能な不正メールの検知方法、その検知プログラム及びその検知装置を提供することを目的とする。

【課題を解決するための手段】

【００１４】

一つの案では、メール処理方法は、送信メールの対象ヘッダ項目と秘密共有情報とを基に検証情報を生成する処理と、前記検証情報に前記対象ヘッダ項目のメタ情報を結合する処理と、前記メタ情報が結合された前記検証情報を前記送信メールのメールヘッダに結合する処理と、をメールを送信する第１のコンピュータが実行し、受信メールのメールヘッダから、検証情報とメタ情報とを分離する処理と、分離した前記メタ情報を基に前記メールヘッダから対象ヘッダ項目を取得する処理と、取得した前記対象ヘッダ項目と前記秘密共有情報とを基に検証情報を再生成する処理と、分離した前記検証情報と再生成した前記検証情報とを比較する処理と、をメールを受信する第２のコンピュータが実行し、前記第１のコンピュータは、前記検証情報に前記対象ヘッダ項目のメタ情報を結合する処理にて、前記検証情報にさらに前記対象ヘッダ項目の所定の部分から算出した特徴量を結合し、前記第２のコンピュータは、前記分離する処理にて、前記受信メールのメールヘッダからさらに前記特徴量を分離し、取得した前記対象ヘッダ項目から特徴量を算出する処理と、

算出した前記特徴量と分離した前記特徴量とを比較する処理を実行する。

【発明の効果】

【００１５】

一態様によれば、メーリングリストのソフトウエアによってメールヘッダが書き換えられた場合であっても受信側端末でメールヘッダの検証可能な不正メールの検知方法、その検知プログラム及びその検知装置を提供することができる。

【図面の簡単な説明】

【００１６】

【図１】システム構成図

【図２】電子メール送信端末構成図

【図３】電子メール送信端末の検証情報生成装置構成図

【図４】電子メール受信端末の構成図

【図５】電子メール受信端末の検証装置構成図

【図６】対象ヘッダ項目の管理処理を示したフローチャート

【図７】対象ヘッダ項目候補一覧表

【図８】検証情報生成装置の処理を示したフローチャート

【図９】検証装置の処理を示したフローチャート

【図１０】第１の実施形態における検証情報生成処理を説明した図

【図１１】第１の実施形態における検証処理を説明した図

【図１２】第２の実施形態における検証情報生成処理を説明した図

【図１３】第２の実施形態における検証処理を説明した図

【図１４】第３の実施形態における検証情報生成処理を説明した図

【図１５】第３の実施形態における検証処理を説明した図

【発明を実施するための形態】

【００１７】

以下、図面に基づいて本発明の実施の形態を説明する。

【００１８】

まず、本実施例に係るシステム構成について、図１を用いて説明する。図１は、システム構成図の一例である。

【００１９】

図１において、送信者が利用する電子メール送信端末２と、受信者が利用する電子メール受信端末５は、ネットワーク１を介して送信メール（ＳＭＴＰ）サーバ３と受信メール（ＰＯＰ）サーバ４によってメールの送受信を行う。

【００２０】

ＳＭＴＰ（Ｓｉｍｐｌｅ　Ｍａｉｌ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）は、電子メールを送信するために使用するアプリケーション層のプロトコルであり、電子メール送信端末２に含まれる電子メールソフトから、送信メールサーバ３へ電子メールを送信する際に使用されるプロトコルである。また、ＰＯＰ（Ｐｏｓｔ　Ｏｆｆｉｃｅ　Ｐｒｏｔｏｃｏｌ）は、電子メールを受信するために使用するアプリケーション層のプロトコルであり、電子メール受信端末５に含まれる電子メールソフトウェアが受信メールサーバ４から電子メールを受信する際に使用されるプロトコルである。

【００２１】

図１では、電子メール送信端末２と電子メール受信端末５は、それぞれ送信メールサーバ３と受信メールサーバ４を介してネットワークに１に接続されている場合を例示しているが、例えば、電子メール送信端末２と電子メール受信端末５がネットワーク１に接続されて、ネットワーク１上の送信メールサーバ３と受信メールサーバ４にネットワーク１を介して接続されていても良い。

【００２２】

次に、電子メール送信端末２の詳細を、図２を用いて説明する。図２は、電子メール送信端末の構成の一例を示した構成図である。

【００２３】
図２において、電子メール送信端末２は、電子メールソフトウェア２１、検証情報生成装置２２、通信装置２３を備える。
【００２４】
電子メールソフトウェア２１は、送信者が電子メールの作成及び送信指示を行うソフトウエアであり、例えばメーラーである。検証情報生成装置２２は、電子メール送信端末２から電子メール受信端末５に送信するメールに含ませる「検証情報」の生成を行う。検証情報は、電子メール受信端末５にて標的型メールの可能性があるか否かを判定するときに使用される情報である。通信装置２３は、送信メールサーバ３へ電子メールの送信を行うためのインターフェイス装置である。電子メールソフトウェア２１は、検証情報生成装置２２に対して送信メールを送信し、検証情報付き送信メールを受信すると、通信装置２３を介して送信メールを送信メールサーバ３へ送信する。
【００２５】
次に、検証情報生成装置２２の詳細を、図３を用いて説明する。図３は、電子メール送信端末の検証情報生成装置２２の構成の一例を示す構成図である。
【００２６】
図３において、検証情報生成装置２２は、要求受付手段２２１、管理手段２２２、秘密情報管理手段２２３、検証情報生成手段２２４を備える。
【００２７】
要求受付手段２２１は入出力部２２１１を備え、電子メールソフトウェア２１から入力される送信メールを受け付け、検証情報が結合された返信メールを電子メールソフトウェア２１に出力する。管理手段２２２は、対象ヘッダ項目管理部２２２１を備え、後述する対象ヘッダ項目を管理する。
【００２８】
秘密情報管理手段２２３は、秘密情報保管部２２３１を備え、検証情報を生成する際に使用する秘密情報の取り扱いを行う。秘密情報は、事前に電子メール送信端末２と電子メール受信端末５で共有する必要がある。
【００２９】
秘密情報は、例えば、秘密情報管理手段２２３によって作成されて、電子メール受信端末５と事前に共有しておく。また、電子メール受信端末５の検証装置５２で同一のアルゴリズムで作成して、同一の秘密情報を共有しても良い。攻撃者は秘密情報を知らなければ検証情報が生成できないため、送信メールの安全な検証が可能になる。
【００３０】
作成された秘密情報は、秘密情報保管部２２３１で保管される。保管された秘密情報は、外部に漏えいしないよう安全に保管する必要がある。このため、秘密情報保管部２２３１は、例えば秘密情報を暗号化して保存する。
【００３１】
検証情報生成手段２２４は、特徴量情報生成部２２４１、検証情報生成部２２４２、及び検証情報結合部２２４３を備え、検証情報を生成して、返信メールに作成した検証情報の結合を行う。
【００３２】
次に、電子メール受信端末５の詳細を、図４を用いて説明する。図４は、電子メール受信端末の構成の一例を示した構成図である。
【００３３】
図４において、電子メール受信端末５は、電子メールソフトウェア５１、検証装置５２、通信装置５３、及び表示装置５４を備える。
【００３４】
電子メールソフトウェア５１は、受信者が受信サーバ４からの電子メールの受信指示を行うソフトウエアであり、例えばメーラーである。検証装置５２は、受信した電子メールに結合されている検証情報の検証を行う。通信装置５３は、受信メールサーバ４から電子

メールの受信を行うためのインターフェイスである。表示装置５４は、検証装置５２による検証結果を表示する。

【００３５】

次に、検証装置５２の詳細を、図５を用いて説明する。図５は、電子メール受信端末の検証装置５２の構成の一例を示す構成図である。

【００３６】

図５において、検証装置５２は、要求受付手段５２１、秘密情報管理手段５２２、及び検証手段５２３を備える。

【００３７】

要求受付手段５２１は、入出力部５２１１を備え、電子メールソフトウェア５１から入力される検証情報付き受信メールを受け付け、検証結果を電子メールソフトウェア５１に出力する。

【００３８】

秘密情報管理手段５２２は、秘密情報保管部５２２１を備え、検証情報の検証に使用する秘密情報の管理を行う。

【００３９】

検証手段５２３は、特徴量情報生成部５２３１、及び検証部５２３２を備え、対象ヘッダ項目からの特徴量情報生成や検証情報の検証を行う。

【００４０】

次に、図３で説明した管理手段２２２による対象ヘッダ項目の管理の方法を、図６を用いて説明する。図６は、対象ヘッダ項目の管理処理を示したフローチャートの一例である。

【００４１】

図６において、検証情報生成装置２２は、対象ヘッダ項目を生成する（Ｓ３００１）。対象ヘッダ項目とは、電子メール検証の対象となる電子メールヘッダの項目である。対象ヘッダ項目は、例えば、検証情報生成装置２２に備えられた、図３で図示しない対象ヘッダ項目生成ポリシーに従って生成される。対象ヘッダ項目ポリシーは、対象ヘッダ項目の生成方法を表しており、検証情報生成装置２２は、入力された送信メールに対して対象ヘッダ項目ポリシーを適用することにより対象ヘッダ項目を生成する。対象ヘッダ項目ポリシーを使用することにより、送信メールに応じた適切な対象ヘッダ項目が生成される。対象ヘッダ項目ポリシーは、例えば複数の電子メール送信端末に一律に適用することができる。一律に適用された対象ヘッダ項目ポリシーによって、例えば送信者の指示の有無に拘わらず、送信メールに対して自動的に一律の対象ヘッダ項目ポリシーを適用させることができる。例えば、「社外秘」、「極秘」などの特定の単語を有する送信メールに対して、所定の対象ヘッダ項目ポリシーを自動的に適用させることができる。一方、対象ヘッダ項目を送信者が個別に選択して生成しても良い。

【００４２】

対象ヘッダ項目は、例えば送信メールの重要度を予め規定しておき、その重要度に応じて対象ヘッダ項目を生成することができる。図７は、対象ヘッダ項目候補一覧の一例を説明する一覧表である。

【００４３】

図７において、送信メールは重要度がＡ、Ｂ、Ｃ及びＤのように分類され、それぞれの重要度に対してpattern１、２、３及び４のヘッダ項目のパターンが割り振られている。それぞれのパターンには、ヘッダ項目である、「From」、「To」、「Subject」、「Received」、「Date」、「Message-ID」、「X-Mailer」、「Body」及び「File」が設定されている。例えば、重要度Ｃを選択すると、ヘッダ項目は、「From、Subject、Date、Body」として一意的に生成される。メールの重要度は、例えば、送信者が適宜選択できる。また、上述した対象ヘッダ項目ポリシーによって自動的に選択することができる。

【００４４】

図６に戻り、生成された対象ヘッダ項目は、対象ヘッダ項目管理部２２２１により保管

されて（Ｓ３００２）、対象ヘッダ項目の管理処理を終了する。

【００４５】

次に、検証情報生成装置２２における検証情報の生成処理の動作を、図３を参照しながら、図８を用いて説明する。図８は、検証情報生成装置の処理の一例を示したフローチャートである。

【００４６】

図８において、スタート条件として、先ず送信者が電子メール送信端末２の電子メールソフトウェア２１を起動し、送信用メールを作成する。電子メールソフトウェア２１は、検証情報生成装置２２の入出力部２２１１を介して、要求受付手段２２１に対して、ヘッダ情報、および本文情報を含む送信メールを入力する。

【００４７】

先ず、メールが入力された要求受付手段２２１は、検証情報生成手段２２４に対して、検証情報生成依頼を発行する（Ｓ４００１）。このとき、要求受付手段２２１は、電子メールソフトウェア２１から受け取った、ヘッダ情報、および本文情報を含む送信メールの情報を検証情報生成手段２２４に対して送信する。

【００４８】

検証情報生成手段２２４は、検証情報生成依頼を受信し（Ｓ４００２）、秘密情報管理手段２２３に対して、送信メールのヘッダ情報を含む秘密情報取得依頼を送信する（Ｓ４００３）。

【００４９】

秘密情報管理手段２２３は、検証情報生成手段２２４から秘密情報取得依頼を受信し（Ｓ４００４）、秘密情報保管部２２３１から秘密情報を取得し（Ｓ４００５）、さらに、取得した秘密情報を検証情報生成手段２２４に送信する（Ｓ４００６）。

【００５０】

検証情報生成手段２２４は、秘密情報管理手段２２３から秘密情報を受信し（Ｓ４００７）、管理手段２２２に対して、対象ヘッダ項目取得依頼を送信する（Ｓ４００８）。

【００５１】

管理手段２２２は、検証情報生成手段２２４から対象ヘッダ項目取得依頼を受信し（Ｓ４００９）、図６で説明した対象ヘッダ項目管理部２２２１により保管された対象ヘッダ項目を取得して（Ｓ４０１０）、さらに、検証情報生成手段２２４に対して、対象ヘッダ項目を送信する（Ｓ４０１１）。

【００５２】

検証情報生成手段２２４は、管理手段２２２から対象ヘッダ項目を取得する（Ｓ４０１２）。検証情報生成手段２２４は、対象ヘッダ項目に対して秘密情報により検証情報を生成する（Ｓ４０１３）。なお、検証情報の生成方法及び検証方法については、図１０～図１５を用いて後述する。

【００５３】

検証情報生成手段２２４の検証情報結合部２２４３は、対象ヘッダ項目管理部２２２１から対象ヘッダ項目の取得と同時に取得した「ｐａｔｔｅｒｎ ３形式」によるヘッダ項目を新たに追加し、追加したヘッダ項目に生成された検証情報を結合する（Ｓ４０１４）。「ｐａｔｔｅｒｎ ３形式」とは、対象ヘッダ項目を直接ヘッダに記述する代わりに、対象ヘッダ項目に関する情報を、別途ヘッダ項目を追加してそのヘッダ項目に結合する形式である。対象ヘッダ項目は、メール受信端末で受信メールを検証する際に検証情報を生成するために指定されるが、対象ヘッダ項目を直接ヘッダに記述すると、攻撃者が記述された対象ヘッダ項目から偽装した検証情報を生成してヘッダに結合することが可能になってしまう。「ｐａｔｔｅｒｎ ３形式」により対象ヘッダ項目を結合すれば、攻撃者による偽装した検証情報の生成を防止できる。なお、メール受信端末側の検証装置５２も、図７で説明した対象ヘッダ項目候補一覧が管理されて、共有されている。

【００５４】

検証情報生成手段２２４は、要求受付手段２２１に対して、検証情報ヘッダ付きメール

の情報を送信する（Ｓ４０１５）。
【００５５】
要求受付手段２２１は、検証情報生成手段２２４から検証情報ヘッダ付きメールの情報を受信し、電子メールソフトウェア２１に対して検証情報ヘッダ付きメールの情報を送信し（Ｓ４０１６）、図８で説明する検証情報生成装置の処理を終了する。
【００５６】
図２で説明した通り、電子メールソフトウェア２１は、要求受付手段２２１から検証情報ヘッダ付きメールの情報を受信すると、通信装置２３を介して送信メールサーバ３に検証情報付き送信メールを送信し、受信メールサーバ４を介してメール受信端末５にメールが送信される。
【００５７】
次に、メール受信端末５の検証装置５２における検証処理を、検証装置５２の詳細を説明した図５を参照して、図９のフローチャートを用いて説明する。図９は、検証装置５２の処理の一例を示したフローチャートである。
【００５８】
図９において、電子メールソフトウェア５１から検証情報付き受信メールを受信した要求受付手段５２１は、検証手段５２３に対して、検証依頼を送信する（Ｓ５００１）。
【００５９】
検証手段５２３は、要求受付手段５２１から検証依頼を受信し（Ｓ５００２）、検証情報付きメールのヘッダ情報、および本文情報の解析を行う（Ｓ５００３）。検証手段５２３は、ヘッダ情報から対象ヘッダ項目を取得する（Ｓ５００４）。検証手段５２３は、さらに、秘密情報管理手段５２２に対して秘密情報取得依頼を送信する（Ｓ５００５）。
【００６０】
秘密情報管理手段５２２は、検証手段５２３から秘密情報取得依頼を受信すると（Ｓ５００６）、秘密情報保管部５２２１が管理している秘密情報を取得して（Ｓ５００７）、取得した秘密情報を検証手段５２３に送信する（Ｓ５００８）。
【００６１】
検証部５２３２は、秘密情報管理手段５２２から秘密情報を受信すると（Ｓ５００９）、Ｓ５００４で取得した対象ヘッダ項目の情報を基に秘密情報から検証情報の再生成を行う（Ｓ５０１０）。次に、検証手段５２３は、検証情報生成手段２２４がヘッダ情報に結合したヘッダ項目から検証情報を取得する（Ｓ５０１１）。
【００６２】
検証手段５２３の検証部３２３２は、再生成した検証情報とヘッダ項目から取得した検証情報とを比較して、両者が一致するかの確認を行う（Ｓ５０１２）。検証手段５２３は、検証結果を要求受付手段５２１に送信する（Ｓ５０１３）。
【００６３】
要求受付手段５２１は、検証手段５２３から検証結果を受信すると（Ｓ５０１４）、電子メールソフトウェア５１に対して検証結果を送信して、電子メールソフトウェア５１は、出力装置５４を介して、受信者に検証結果を報知する。
【００６４】
次に、上述した電子メール送信端末２における検証情報生成処理と、電子メール受信端末５における検証処理の詳細を、３つの実施形態にて説明する。図１０及び図１１を用いて第１の実施形態を説明する。図１２及び図１３を用いて第２の実施形態を説明する。さらに、図１４及び図１５を用いて第３の実施形態を説明する。なお、図中の（Ｓ４０１０）等で示すステップ番号は、図８及び図９で説明したフローチャートのステップ番号に対応している。
[第１の実施形態]
【００６５】
第１の実施形態は、送信メール情報の「Ｓｕｂｊｅｃｔ：」ヘッダ項目の文字列サイズを検証情報に結合して検証情報ヘッダを生成し、検証する方式である。

【００６６】
図１０は、第１の実施形態における検証情報生成処理の一例を説明した図である。図１０において、検証情報生成部２２４２は、送信メールヘッダ情報の「Ｆｒｏｍ：」ヘッダ、「Ｔｏ：」ヘッダ、「Ｓｕｂｊｅｃｔ：」ヘッダ、「Ｄａｔｅ：」ヘッダ、「Ｂｏｄｙ：」本文情報（本文情報には、「Ｆｉｌｅ：」添付ファイルを含む）の５つのヘッダ項目に対する検証情報を生成する。検証情報生成部２２４２は、秘密情報保管部２２３３から取得した秘密情報によって、上記５つのヘッダ項目から検証情報「ＢＣ７３ＤＡ１２５４２３１Ｆ」を生成する。ここでヘッダ項目から生成された検証情報を「第１の検証情報」とする。

【００６７】
検証情報を生成するアルゴリズムは、例えば一方向性ハッシュ関数を用いる。但し、ハッシュ関数以外の生成アルゴリズムを使用しても良い。検証情報生成時に使用する秘密情報と生成アルゴリズムは、検証時の整合性を確保するため、検証装置５２の検証部５２３２と共有している。

【００６８】
「Ｓｕｂｊｅｃｔ：」ヘッダについては、メーリングリスト（以下、「ＭＬ」と省略する。）サーバにて、連番等の文字が結合される可能性がある。本実施例では、ＭＬサーバによる文字の結合がされる前のオリジナルの「Ｓｕｂｊｅｃｔ：」ヘッダの内容の文字列サイズ「１８」（ｘ１８：１６進数）を算出して、第１の検証情報に結合する。第１の検証情報に文字列のサイズを結合したものを「第２の検証情報」とする。

【００６９】
この実施例では、ＭＬサーバによる「Ｓｕｂｊｅｃｔ：」ヘッダへの文字の結合が行われる場合を説明しているが、例えば、ＭＬサーバにより他のヘッダ項目に対する変更が加えられる場合、メールヘッダの所定項目に対して文字列のサイズを取得して第１の検証情報に結合しても良い。また、文字列のサイズ以外のヘッダ項目に関するメタデータを取得して第１の検証情報に結合しても良い。この場合のメタデータとは、ヘッダ項目の変更前の状態を特定し、メール受信端末における検証処理で変更前のヘッダ項目を識別でれば良い。文字数以外では、例えば、文字列の先頭部分と末尾部分を特定する情報や、先頭文字と文字列のバイト数等が利用できる。また、第１の検証情報への結合方法として、本実施例では生成した第１の検証情報の後方にメタデータを結合する方法を説明しているが、例えば、第１の検証情報の前方にメタデータを結合しても良い。なお、これらの検証情報のフォーマット定義（結合するメタデータの種類、結合方法）については、検証装置５２の検証部５２３２と共有している。

【００７０】
検証情報結合部２２４３は、対象ヘッダ項目の新たなヘッダ情報として、「X-ＩｎｂｏｕｎｄＴａｒｇｅｔＨｅａｄ：」ヘッダを生成して、対象ヘッダ項目となる「ｐａｔｔｅｒｎ 3」を結合している。また、検証情報結合部２２４３は、検証情報の新たなヘッダ情報として、「X-ＩｎｂｏｕｎｄＭＡＣ：」ヘッダを生成し、検証情報となる「ＢＣ７３ＤＡ１２５４２３１Ｆ１８」を結合している（Ｓ４０１４）。

【００７１】
図１１は、第１の実施形態における検証処理の一例を説明した図である。

【００７２】
図１１において、検証手段５２３は、対象ヘッダ項目を特定する「X-ＩｎｂｏｕｎｄＴａｒｇｅｔＨｅａｄ：」ヘッダを参照して、どのヘッダ項目が検証情報の生成対象か確認する。本実施例では、「ｐａｔｔｅｒｎ 3」に相当する、「Ｆｒｏｍ：」ヘッダ、「Ｔｏ：」ヘッダ、「Ｓｕｂｊｅｃｔ：」ヘッダ、「Ｄａｔｅ：」ヘッダ、及び「Ｂｏｄｙ：」本文情報（本文情報には、「Ｆｉｌｅ：」添付ファイルを含む）の５つのヘッダ項目が対象ヘッダ項目である。

【００７３】
ここで、ＭＬサーバによって、「Ｓｕｂｊｅｃｔ：」ヘッダに、[ｃｙｂｅｒｓｅｃ０

０１１２]という文字列が追加されたとする。受信したメールの対象ヘッダ項目をそのまま使用して検証情報を再生成したとすると、メール送信端末２が作成したオリジナルのメールヘッダとは異なるため、ＭＬサーバによって対象ヘッダ項目の文字列が追加されたメールは不正メールと判定してしまうことになる。

【００７４】

本実施例では、ヘッダ情報に結合された「Ｘ-ＩｎｂｏｕｎｄＭＡＣ：」ヘッダを参照して、メタデータである文字サイズの情報が結合された検証情報から文字サイズの情報を分離して、「Ｓｕｂｊｅｃｔ：」ヘッダの後部から分離した文字サイズ分を取得することにより、オリジナルの「セキュリティ脆弱性報告書」の文字列を取得することができる。

【００７５】

検証部５２３２は、「Ｓｕｂｊｅｃｔ：」ヘッダの文字列と、他の対象ヘッダ項目を基に、秘密情報管理手段５２２から取得した秘密情報によって検証情報を再生成する。この実施例では検証情報として、"ＢＣ７３ＤＡ１２５４２３１Ｆ"を再生成している。

【００７６】

次に、検証部５２３２は、「Ｘ-ＩｎｂｏｕｎｄＭＡＣ：」ヘッダから分離した検証情報である、「ＢＣ７３ＤＡ１２５４２３１Ｆ」と再生成した検証情報とを比較して、両者が一致することを確認する。検証情報が一致していれば、受信メールは正当な送信者から送信されたものであると検証できる。

【００７７】

なお、第一の実施形態では、「Ｓｕｂｊｅｃｔ：」ヘッダの文字列を、一方向性ハッシュ関数等を用いた特徴量情報で置き換えて検証情報を生成することもできる。「Ｓｕｂｊｅｃｔ：」ヘッダを特徴量情報とすることにより、攻撃者による偽装識別情報の生成を防止することができる。

[第２の実施形態]

【００７８】

第２の実施形態は、「Ｓｕｂｊｅｃｔ：」ヘッダの内容の文字サイズの情報に加え、「Ｓｕｂｊｅｃｔ：」ヘッダの内容の特徴量情報を検証情報に結合して検証情報ヘッダを生成し、検証する方式である。

【００７９】

第２の実施形態では、ＭＬサーバによって、「Ｓｕｂｊｅｃｔ：」ヘッダの後ろにも何らかの文字が追記されてしまう場合であっても検証処理が可能となる。

【００８０】

図１２は、第２の実施形態における検証情報生成処理の一例を説明した図である。第２の実施形態における検証情報生成処理と図１０で説明した第１の実施形態における検証情報生成処理の相違点は以下の通りである。第１の実施形態は「Ｓｕｂｊｅｃｔ：」ヘッダの文字列サイズを算出して検証情報に結合している。これに対して、第２の実施形態では、特徴量情報生成部２２４１が「Ｓｕｂｊｅｃｔ：」ヘッダの内容である文字列の特徴量を算出して、「Ｓｕｂｊｅｃｔ：」ヘッダの文字列サイズを検証情報に結合することに加えて、算出された特徴量をさらに検証情報に結合している。

【００８１】

本実施例では、「Ｓｕｂｊｅｃｔ：」ヘッダの「セキュリティ脆弱性報告書」の文字列から、"５２Ａ６Ａ３９Ｃ３３"の特徴量が算出されて、検証情報に結合されている。なお、検証情報との結合方法は、第１の実施例同様に、本実施例に限定されるものではない。

【００８２】

図１３は、第２の実施形態における検証処理の一例を説明した図である。図１３で説明する第２の実施形態における検証処理は、図１１で説明した第１の実施形態における検証処理と、「Ｓｕｂｊｅｃｔ：」ヘッダの「セキュリティ脆弱性報告書」の文字列から、「５２Ａ６Ａ３９Ｃ３３」の特徴量を算出して、検証情報に結合された特徴量と比較する点が異なる。特徴量を比較することにより、検証情報に結合された文字サイズの情報を基に取得された「セキュリティ脆弱性報告書」の文字列が正しいか否かの確認ができる。例え

ば、「Ｓｕｂｊｅｃｔ：」ヘッダの文字列の最後から文字サイズ分を取得した文字の特徴量が検証情報に結合された特徴量と異なる場合、文字列の最後から１文字分先頭側に取得位置をずらして再度取得して情報量を比較する。この動作を繰り返すことにより、例えばＭＬサーバによって「Ｓｕｂｊｅｃｔ：」ヘッダの後ろにも何らかの文字が追記された場合であっても、オリジナルの文字列を見出すことができる。検証部５２３２は、正しい「Ｓｕｂｊｅｃｔ：」ヘッダの文字列によって、他の４つの対象ヘッダ項目とともに検証情報を再生成することができる。

【００８３】

なお、本実施例では、検証情報に結合されたメタデータは文字サイズの情報であり、「Ｓｕｂｊｅｃｔ：」ヘッダの後ろから文字サイズ分の文字列を順次抽出していったが、例えばオリジナルの文字列の最後の文字と文字サイズをメタデータとすれば、「Ｓｕｂｊｅｃｔ：」ヘッダの中で文字の一致した場所から文字サイズ分を抽出することにより繰り返し処理をしなくても正しいオリジナルの文字列を抽出が可能となる。

【００８４】

他の動作については図１１で説明した第１の実施形態における検証処理と同じであるため説明を省略する。

[第３の実施形態]

【００８５】

第３の実施形態は、対象ヘッダ項目となる「Ｓｕｂｊｅｃｔ：」ヘッダの内容の文字サイズ情報に加え、「Ｓｕｂｊｅｃｔ：」ヘッダの内容の特徴量情報も含めて検証情報を生成し、検証する方式である。

【００８６】

第３の実施形態では、例えば、ＭＬサーバによって、「Ｓｕｂｊｅｃｔ：」ヘッダの後ろが一部削除されてしまう場合であっても検証処理が可能となる。携帯電話やタブレット端末、スマートフォンのようなモバイル環境でのメール送受信では、「Ｓｕｂｊｅｃｔ：」ヘッダの文字列が所定サイズを超えると後方の一部が削除される場合があり、第３の実施形態によって検証処理が可能となる。

【００８７】

図１４は、第３の実施形態における検証情報生成処理の一例を説明した図である。図１４で説明する第３の実施形態における検証情報生成処理と図１２で説明した第２の実施形態における検証情報生成処理の相違点は以下の通りである。第２の実施形態では、「Ｓｕｂｊｅｃｔ：」ヘッダのオリジナルの全文字列のサイズと全文字列の特徴量を検証情報に結合している。これに対して、第３の実施形態では、「Ｓｕｂｊｅｃｔ：」ヘッダの文字列の指定部分のサイズと特徴量を検証情報に結合する。文字列の指定は、例えば、「文字列の先頭何文字目から文字サイズ分」という指定方法が可能である。また、オリジナルの全文字列のサイズに応じて指定方法を変更し、指定方法をメタデータとして検証情報に結合しても良い。例えば、「２０文字以内であれば全文字を指定し、２０文字より大きい場合は先頭１０文字」という指定方法が可能である。これにより、携帯電話のキャリアの仕様で受信可能な「Ｓｕｂｊｅｃｔ：」ヘッダの文字数が異なる場合を考慮した検証処理が可能になる。

【００８８】

本実施例では、「Ｓｕｂｊｅｃｔ：」ヘッダの内容から「脆弱性報告書」の文字を指定し、指定した文字のサイズ「０Ｃ」と、指定文字の特徴量「２９３Ｂ２９４ＣＤＡ」を検証情報に結合している。また、検証情報の新たなヘッダ情報である、「Ｘ-ＩｎｂｏｕｎｄＭＡＣ：」ヘッダには、「ＣＦ７４３Ａ２４Ｄ９４Ｃ９３０Ｃ２９３Ｂ２９４ＣＤＡ」の検証情報が結合される。

【００８９】

その他の処理については、図１２で説明した第２の実施形態と同じであるので説明を省略する。

【００９０】

図１５は、第３の実施形態における検証処理の一例を説明した図である。図１５で説明する第３の実施形態における検証処理は、図１３で説明した第２の実施形態における検証処理と、「Ｓｕｂｊｅｃｔ：」ヘッダの文字の指定方法が異なる。第２の実施形態では、ヘッダの文字列全てが特徴量算出の対象であり、検証情報再生成の対象であったのに対して、第３の実施形態では、ヘッダの指定された文字が対象となる。従って、文字数が制限されて一部の文字が削除される場合であっても、検証処理が可能になる。

【００９１】

他の処理については図１３の説明と同じであるので説明を省略する。

なお、複数の端末とメールの送受信を行う場合、送受信相手の端末毎に秘密情報等が異なる場合がある。その場合は「Ｔｏ：」ヘッダにより、送信先を特定し、送信先に応じた検証情報付きメールヘッダを作成する。また、複数の宛先が記載された送信メールは、送信するメールを宛先毎に作成して、順次送信しても良い。

【００９２】

また、本実施例で説明したメール送信端末２は、検証情報装置２２とメールソフトウェア２１を別個に構成しており、また、メール受信端末５は、検証装置５２とメールソフトウェア５１を別個に構成しているため、メールソフトウェアは適宜使用者が選択でき、また、検証装置５２等を備えていない送受信先とも通常のメールの送受信が可能となる。

【００９３】

なお、検証情報装置２２の機能、及び検証装置５２の機能は、メールソフトウェアのアドオン機能により実施しても良い。

【００９４】

また、説明した実施形態ではメールの検証をクライアントベースで行ったが、例えば秘密情報の管理をネットワークに接続された管理サーバで行い、各送受信端末は、適宜管理サーバに接続して秘密情報を取得しても良い。

【００９５】

以上、本発明を実施するための形態について詳述したが、本発明は斯かる特定の実施形態に限定されるものではなく、特許請求の範囲に記載された本発明の要旨の範囲内において、種々の変形・変更が可能である。

【００９６】

本発明は、以下に記載する付記のような構成が考えられる。

（付記１）

送信メールの対象ヘッダ項目と秘密共有情報とを基に検証情報を生成する処理と、

前記検証情報に前記対象ヘッダ項目のメタ情報を結合する処理と、

前記メタ情報が結合された前記検証情報を前記送信メールのメールヘッダに結合する処理と、をメールを送信する第１のコンピュータが実行し、

受信メールのメールヘッダから、検証情報とメタ情報とを分離する処理と、

分離した前記メタ情報を基に前記メールヘッダから対象ヘッダ項目を取得する処理と、

取得した前記対象ヘッダ項目と前記秘密共有情報とを基に検証情報を再生成する処理と、

分離した前記検証情報と再生成した前記検証情報とを比較する処理と、をメールを受信する第２のコンピュータが実行するメール処理方法。

（付記２）

前記第１のコンピュータは、

前記検証情報に前記対象ヘッダ項目のメタ情報を結合する処理にて、前記検証情報にさらに前記対象ヘッダ項目の所定の部分から算出した特徴量を結合し、

前記第２のコンピュータは、

前記分離する処理にて、前記受信メールのメールヘッダからさらに前記特徴量を分離し、

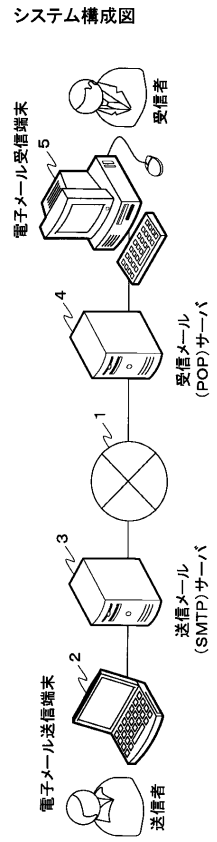
取得した前記対象ヘッダ項目から特徴量を算出する処理と、

算出した前記特徴量と分離した前記特徴量とを比較する処理と、をさらに実行する付記

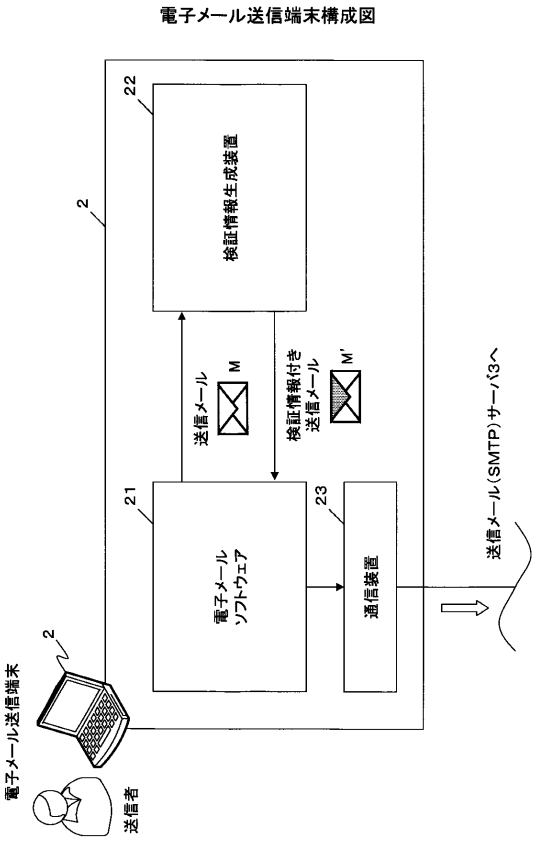
１に記載のメール処理方法。
（付記３）
前記第１のコンピュータは、
前記算出する処理にて、前記対象ヘッダ項目の指定部分について特徴量を算出する付記２に記載のメール処理方法。
（付記４）
コンピュータが電子メールを送信する際に、該コンピュータを、
情報の入出力を行う入出力部と、
送信メールの対象ヘッダ項目と秘密共有情報とを基に検証情報を生成し、前記検証情報に前記対象ヘッダ項目のメタ情報を結合する検証情報生成部と、
前記メタ情報が結合された前記検証情報を前記送信メールのメールヘッダに結合する処理部として機能させるメール処理プログラム。
（付記５）
前記コンピュータを、
前記対象ヘッダ項目の所定の部分から特徴量を算出する特徴量情報生成部としてさらに機能させ、
前記検証情報生成部は、前記検証情報にさらに前記特徴量を結合する付記４に記載のメール処理プログラム。
（付記６）
前記特徴量情報生成部は、前記対象ヘッダ項目の指定部分について特徴量を算出する付記５に記載のメール処理プログラム。
（付記７）
コンピュータが電子メールを受信する際に、該コンピュータを、
情報の入出力を行う入出力部と、
受信メールのメールヘッダから、検証情報とメタ情報とを分離し、分離した前記メタ情報を基に前記メールヘッダから対象ヘッダ項目を取得し、取得した前記対象ヘッダ項目と前記秘密共有情報とを基に検証情報を再生成し、さらに、分離した前記検証情報と再生成した前記検証情報とを比較する検証部として機能させるメール処理プログラム。
（付記８）
前記コンピュータを、
前記対象ヘッダ項目から特徴量を算出する特徴量情報生成部としてさらに機能させ、
前記検証部は、
前記受信メールのメールヘッダから前記検証情報と前記メタ情報に加えてさらに特徴量を分離し、
前記算出した前記特徴量と分離した前記特徴量とを比較する付記７に記載のメール処理プログラム。
（付記９）
前記特徴量情報生成部は、前記対象ヘッダ項目の指定部分について特徴量を算出する付記８に記載のメール処理プログラム。
（付記１０）
送信メールの対象ヘッダ項目と秘密共有情報とを基に検証情報を生成する検証情報生成部と、
前記検証情報に前記対象ヘッダ項目のメタ情報を結合し、前記メタ情報が結合された前記検証情報を前記送信メールのメールヘッダに結合する検証情報結合部と、を備えたメール処理装置。
（付記１１）
受信メールのメールヘッダから、検証情報とメタ情報とを分離し、分離した前記メタ情報を基に前記メールヘッダから対象ヘッダ項目を取得し、取得した前記対象ヘッダ項目と前記秘密共有情報を基に検証情報を再生成し、さらに、分離した前記検証情報と再生成した前記検証情報とを比較する検証部と、を備えたメール処理装置。

（付記１２）
送信メールの対象ヘッダ項目と秘密共有情報とを基に検証情報を生成する処理と、
前記検証情報に前記対象ヘッダ項目のメタ情報を結合する処理と、
前記メタ情報が結合された前記検証情報を前記送信メールのメールヘッダに結合する処理と、をメールを送信するコンピュータが実行するメール処理方法。
（付記１３）
受信メールのメールヘッダから、検証情報とメタ情報とを分離する処理と、
分離した前記メタ情報を基に前記メールヘッダから対象ヘッダ項目を取得する処理と、
取得した前記対象ヘッダ項目と前記秘密共有情報とを基に検証情報を再生成する処理と、
分離した前記検証情報と再生成した前記検証情報とを比較する処理と、をメールを受信するコンピュータが実行するメール処理方法。
【符号の説明】
【００９７】
１　ネットワーク
２　電子メール送信端末
２１　電子メールソフトウェア
２２　検証情報生成装置
２３　通信装置
２２１　要求受付手段
２２２　管理手段
２２３　秘密情報管理手段
２２４　検証情報生成手段
２２１１　入出力部
２２２１　対象ヘッダ項目管理部
２２３１　秘密情報保管部
２２４１　特徴量情報生成部
２２４２　検証情報生成部
２２４３　検証情報結合部
３　送信メール（ＳＭＴＰ）サーバ
４　受信メール（ＰＯＰ）サーバ
５　電子メール受信端末
５１　電子メールソフトウェア
５２　検証装置
５３　通信装置
５４　表示装置
５２１　要求受付手段
５２２　秘密情報管理手段
５２３　検証手段
５２１１　入出力部
５２２１　秘密情報保管部
５２３１　特徴量情報生成部
５２３２　検証部

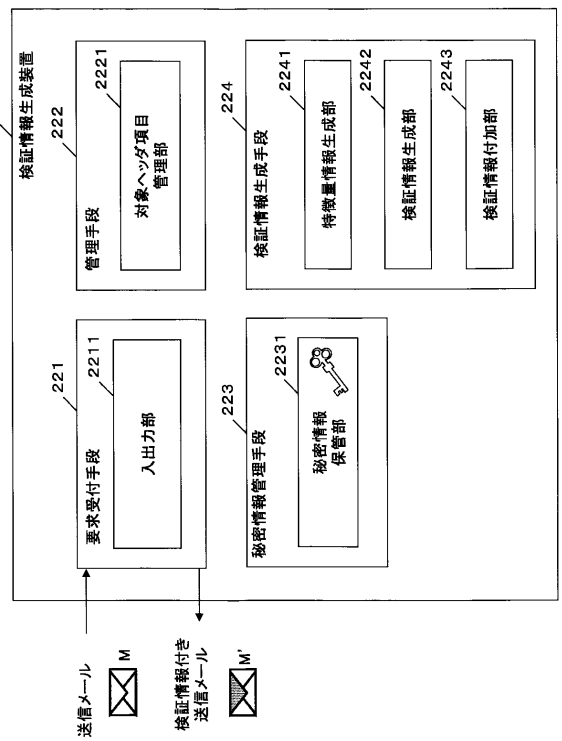
【図１】


システム構成図
電子メール受信端末
5
受信者
4
受信メール
(POP)サーバ
1
3
送信メール
(SMTP)サーバ
2
電子メール送信端末
送信者

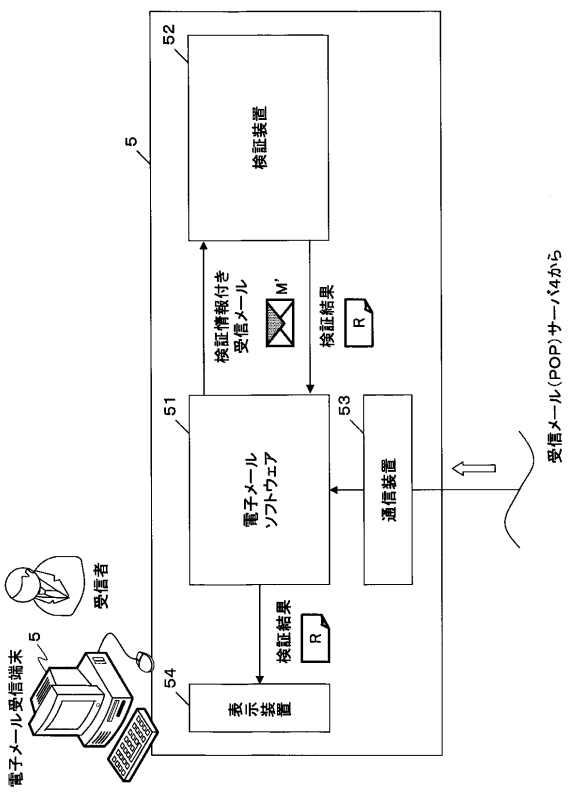
【図２】


電子メール送信端末構成図
2
22
検証情報生成装置
送信メール
M
検証情報付き
送信メール
M'
21
電子メール
ソフトウェア
23
通信装置
送信メール(SMTP)サーバ3へ
2
電子メール送信端末
送信者

【図３】

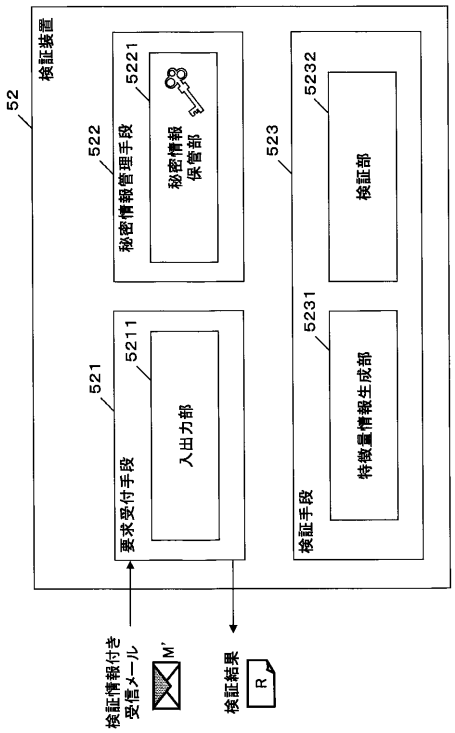

電子メール送信端末の検証情報生成装置構成図
22
検証情報生成装置
222
管理手段
2221
対象ヘッダ項目
管理部
224
検証情報生成手段
2241
特徴量情報生成部
2242
検証情報生成部
2243
検証情報付加部
221
要求受付手段
2211
入出力部
223
秘密情報管理手段
2231
秘密情報
保管部
送信メール
M
検証情報付き
送信メール
M'

【図４】


電子メール受信端末の構成図
5
52
検証装置
検証情報付き
受信メール
M'
検証結果
R
51
電子メール
ソフトウェア
53
通信装置
受信メール(POP)サーバ4から
受信者
電子メール受信端末
5
検証結果
R
54
表示装置

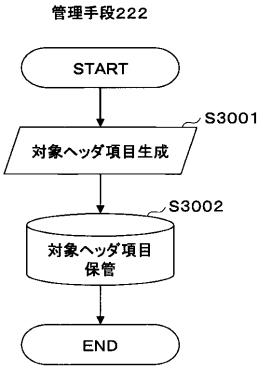
【図５】

電子メール受信端末の検証装置構成図



【図６】

対象ヘッダ項目の管理処理を示したフローチャート



【図７】

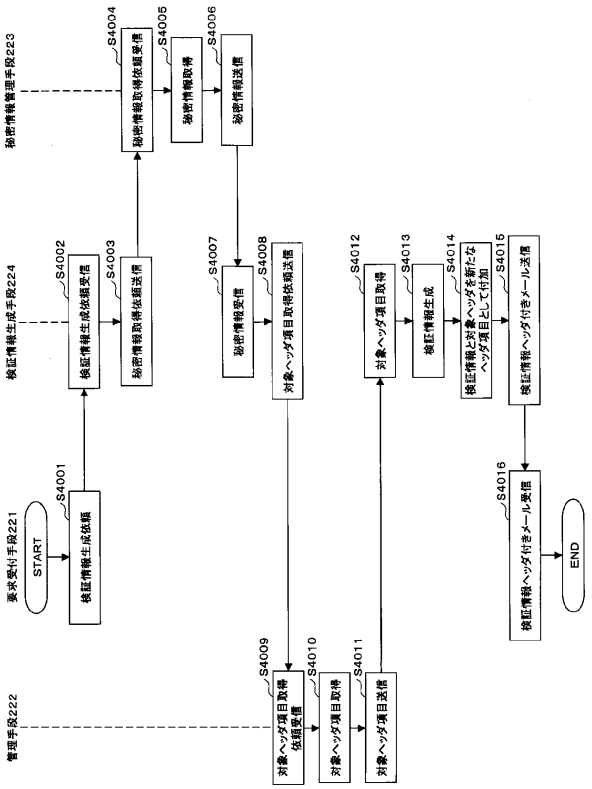
対象ヘッダ項目候補一覧表

対象ヘッダ項目候補一覧の例

重要度A	pattern 1	From, To, Subject, Received, Date, Message-Id, X-Mailer, Body, File
重要度B	pattern 2	From, To, Subject, Received, Date, Message-Id, Body, File
重要度C	pattern 3	From, Subject, Date, Body, File
重要度D	pattern 4	From, Subject, Date, Body
…		…

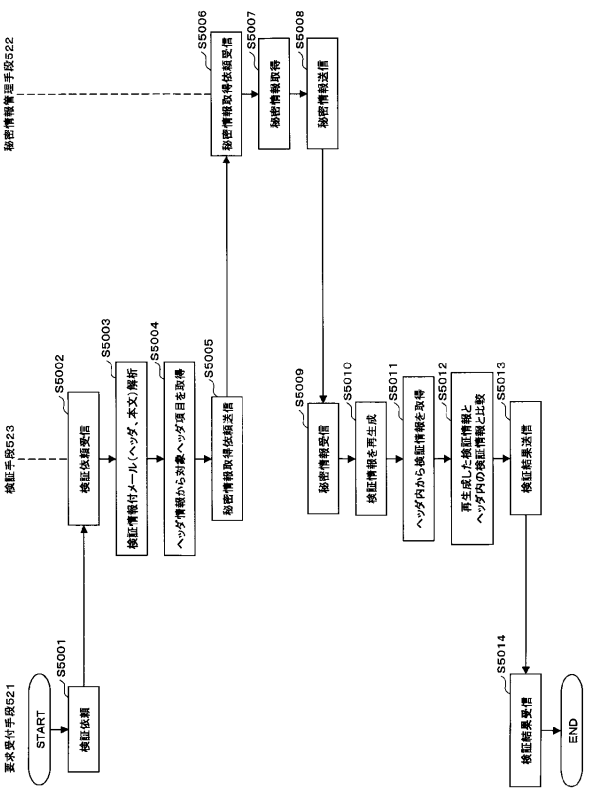
【図８】

検証情報生成装置の処理を示したフローチャート



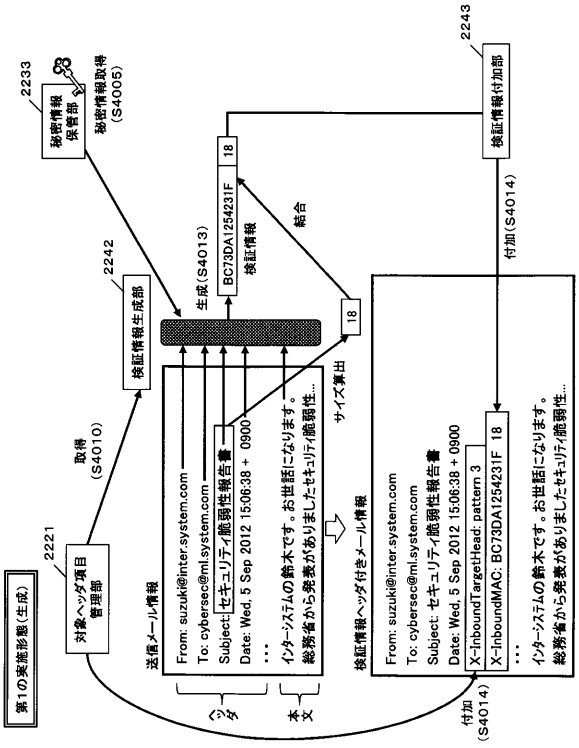
【図９】

検証装置の処理を示したフローチャート



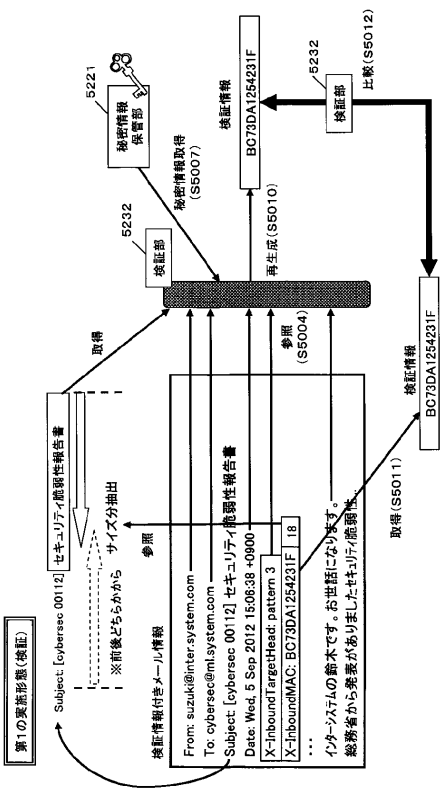
【図１０】

第1の実施形態における検証情報生成処理を説明した図



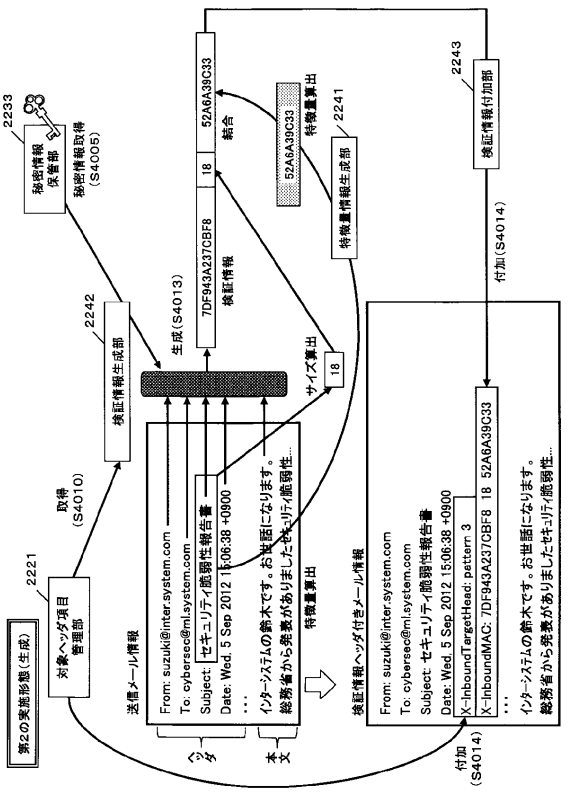
【図１１】

第1の実施形態における検証処理を説明した図



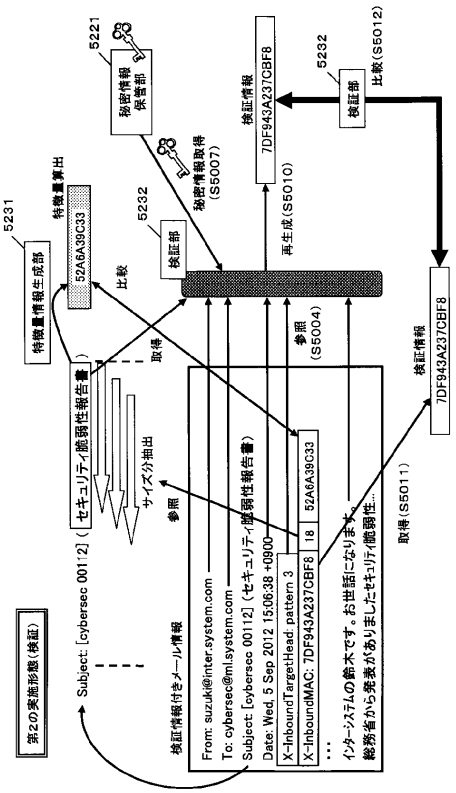
【図１２】

第2の実施形態における検証情報生成処理を説明した図



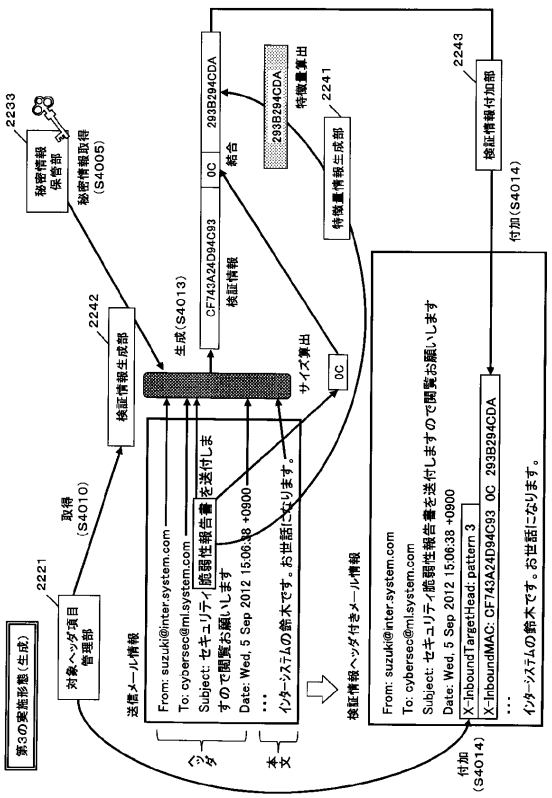
【図１３】

第2の実施形態における検証処理を説明した図



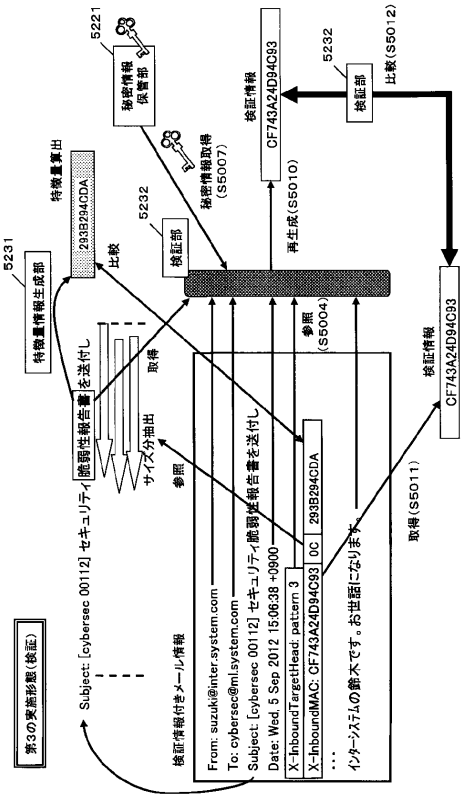
【図１４】

第3の実施形態における検証情報生成処理を説明した図



【図１５】

第3の実施形態における検証処理を説明した図



フロントページの続き

(56)参考文献 特開２００９－０９３５７６（ＪＰ，Ａ）
国際公開第２０１０／０８２２８９（WO，Ａ１）
特開２００９－０１７３４８（ＪＰ，Ａ）
吉岡孝司 他，電子メールの特徴情報を用いた標的型メールへのクライアント対策技術の提案，
情報処理学会研究報告，一般社団法人情報処理学会，２０１２年 7月２０日，pp. 1-8

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ １３／００