(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6531373号
(P6531373)
(45)発行日　令和1年6月19日(2019.6.19)　(24)登録日　令和1年5月31日(2019.5.31)

(51)Int.Cl.　F I
G06F 13/00 (2006.01)　G06F 13/00 610S
G06F 21/62 (2013.01)　G06F 21/62 309

請求項の数 9　(全 18 頁)

(21)出願番号　特願2014-222134(P2014-222134)
(22)出願日　平成26年10月31日(2014.10.31)
(65)公開番号　特開2016-91132(P2016-91132A)
(43)公開日　平成28年5月23日(2016.5.23)
審査請求日　平成29年10月31日(2017.10.31)

(73)特許権者　390002761
キヤノンマーケティングジャパン株式会社
東京都港区港南２丁目１６番６号
(73)特許権者　592135203
キヤノンＩＴソリューションズ株式会社
東京都品川区東品川２丁目４番１１号
(74)代理人　100189751
弁理士　木村　友輔
(72)発明者　北防　拓也
東京都品川区東品川２丁目４番１１号　キヤノンソフトウェア株式会社内
(72)発明者　高山　寛子
東京都品川区東品川２丁目４番１１号　キヤノンソフトウェア株式会社内

最終頁に続く

(54)【発明の名称】情報処理装置、情報処理装置の制御方法、プログラム

(57)【特許請求の範囲】
【請求項１】
検出すべき文字列ごとに、文字列と当該文字列を基準としてマスクする範囲とを対応付けて記憶した検出文字列記憶手段と、
送信者からの電子メールを受信するメール受信手段と、
前記メール受信手段により受信した前記送信者からの電子メールであって、前記検出文字列記憶手段に記憶された検出すべき文字列を含む電子メールを暗号化する暗号化手段と、
前記検出文字列記憶手段に記憶された検出すべき文字列を含む電子メールのメール本文のうち、前記検出文字列記憶手段に当該検出すべき文字列と対応付けて記憶されている当該文字列を基準としてマスクする範囲に基づきマスクするマスク手段と、
前記マスク手段により前記メール本文がマスクされた電子メールに、前記暗号化手段により暗号化された電子メールが添付されたマスクメールを作成するマスクメール生成手段と、
前記送信者からの電子メールの受信者に対して、前記マスクメール生成手段により作成されたマスクメールを配信するメール配信手段と、
を有する情報処理装置。
【請求項２】
前記マスク手段は、
前記送信者からの電子メールの宛先に基づき、マスクするかを決定すること

を特徴とする請求項１に記載の情報処理装置。
【請求項３】
前記検出した文字列に対応するセキュリティレベルを記憶するセキュリティレベル記憶手段を更に有し、
前記マスク手段は、
前記送信者からの電子メールに含まれる検出すべき文字列に対応するセキュリティレベルに基づき、マスクするかを決定すること
を特徴とする請求項１又は２記載の情報処理装置。
【請求項４】
前記暗号化手段は、
前記検出された文字列の数が所定数より多い場合は、前記送信者からの電子メール全体を暗号化し、一方、所定数より少ない場合は、マスク部分のみを暗号化すること
を特徴とする請求項１乃至３のいずれか１項に記載の情報処理装置。
【請求項５】
前記受信者が受信した電子メールを所持している場合、前記暗号化手段により生成された暗号化された電子メールの復号化ができるように制御すること
を特徴とする請求項１乃至４のいずれか１項に記載の情報処理装置。
【請求項６】
前記暗号化手段より生成された暗号化された電子メールは、前記検出した文字列に対応するセキュリティレベルに基づき、復号により生成されるファイル形式を決定すること
を特徴とする請求項１乃至５のいずれか１項に記載の情報処理装置。
【請求項７】
電子メールを配信することが可能な情報処理装置と、前記配信された電子メールを閲覧することが可能なクライアント端末からなるメールシステムであって、
前記情報処理装置は、
検出すべき文字列ごとに、文字列と当該文字列を基準としてマスクする範囲とを対応付けて記憶した検出文字列記憶手段と、
送信者からの電子メールを受信するメール受信手段と、
前記メール受信手段により受信した前記送信者からの電子メールであって、前記検出文字列記憶手段に記憶された検出すべき文字列を含む電子メールを暗号化する暗号化手段と、
前記検出文字列記憶手段に記憶された検出すべき文字列を含む電子メールのメール本文のうち、前記検出文字列記憶手段に当該検出すべき文字列と対応付けて記憶されている当該文字列を基準としてマスクする範囲に基づきマスクするマスク手段と、
前記マスク手段により前記メール本文がマスクされた電子メールに、前記暗号化手段により暗号化された電子メールが添付されたマスクメールを作成するマスクメール生成手段と、
前記送信者からの電子メールの受信者に対して、前記マスクメール生成手段により作成されたマスクメールを配信するメール配信手段と、
を有し、
前記クライアント端末は、
前記メール配信手段により配信されたマスクメールを受信する配信メール受信手段を有し、
前記メール配信手段により配信されたマスクメールを所持している場合に、前記配信メール受信手段により受信したマスクメールに添付された前記暗号化された電子メールの復号化ができるように制御すること、
を有するメールシステム。
【請求項８】
検出すべき文字列ごとに、文字列と当該文字列を基準としてマスクする範囲とを対応付けて記憶した検出文字列記憶手段を有する情報処理装置の処理方法であって、

前記情報処理装置が、
送信者からの電子メールを受信するメール受信ステップと、
前記メール受信ステップにより受信した前記送信者からの電子メールであって、前記検出文字列記憶手段に記憶された検出すべき文字列を含む電子メールのを暗号化する暗号化ステップと、
前記検出文字列記憶手段に記憶された検出すべき文字列を含む電子メールのメール本文のうち、前記検出文字列記憶手段に当該検出すべき文字列と対応付けて記憶されている当該文字列を基準としてマスクする範囲に基づきマスクするマスクステップと、
前記マスクステップにより前記メール本文がマスクされた電子メールに、前記暗号化ステップにより暗号化された電子メールが添付されたマスクメールを作成するマスクメール生成ステップと、
前記送信者からの電子メールの受信者に対して、前記マスクメール生成ステップにより作成されたマスクメールを配信するメール配信ステップと、
を実行することを特徴とする処理方法。
【請求項９】
コンピュータを請求項１乃至６のいずれか１項に記載の情報処理装置の各手段として機能させるためのプログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、電子メールを送信することが可能な情報処理装置、情報処理装置の制御方法、およびプログラムに関する。
【背景技術】
【０００２】
日常業務などを遂行する中で、メールの送受信を行う電子メールは必要不可欠なツールである。しかし利用頻度の向上や利便性の良さから、故意か故意であるかにかかわらず、企業における機密情報の流出の危険性も高まってきている。
【０００３】
企業においては自己防衛の観点などから、機密情報の外部漏えいを防止する取り組みを行っている。例えば、機密情報の外部漏えいを防止する仕組としては、送信するメール本文をチェックして問題のキーワードなどが含まれているメールを抽出することが行われている。
【０００４】
また、特許文献１にはメール送信時に機密情報が含まれた場合、確認をユーザに促すシステムが提案されている。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特開２０１３－１３０９４２号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
これら先行技術によれば、メール送信時に、メール本文やメールの添付ファイルに特定の文言を含む内容が含まれた場合にユーザに対しての確認を促すようになっている。
【０００７】
すなわち先行技術においては、特定の文言を含む内容が含まれた場合は、あらかじめ決められた動作（例えば通知したり、送信を禁止したり）をするようになっている。例えば、添付ファイルを暗号する場合の暗号方式はあらかじめ決められたものが採用される。つまり電子メールに含まれる機密情報のレベルによって暗号すべき部分と必要ない部分があ

った場合であっても、先行文献によれば必要でない文言まで暗号化されてしまうことがあった。この場合、受信者は暗号化が必要でなかった部分まで複号する手間が発生してしまうという問題点があった。

【０００８】

そこで本願発明では、検出すべき文字列を基準とするマスク範囲に基づき、機密情報を含む電子メールを柔軟にマスクすることが可能な情報処理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】

【０００９】

検出すべき文字列ごとに、文字列と当該文字列を基準としてマスクする範囲とを対応付けて記憶した検出文字列記憶手段と、送信者からの電子メールを受信するメール受信手段と、前記メール受信手段により受信した前記送信者からの電子メールであって、前記検出文字列記憶手段に記憶された検出すべき文字列を含む電子メールを暗号化する暗号化手段と、前記検出文字列記憶手段に記憶された検出すべき文字列を含む電子メールのメール本文のうち、前記検出文字列記憶手段に当該検出すべき文字列と対応付けて記憶されている当該文字列を基準としてマスクする範囲に基づきマスクするマスク手段と、前記マスク手段により前記メール本文がマスクされた電子メールに、前記暗号化手段により暗号化された電子メールが添付されたマスクメールを作成するマスクメール生成手段と、前記送信者からの電子メールの受信者に対して、前記マスクメール生成手段により作成されたマスクメールを配信するメール配信手段と、を有する。

【発明の効果】

【００１０】

本発明によれば、検出すべき文字列を基準とするマスク範囲に基づき、機密情報を含む電子メールを柔軟にマスクする情報処理装置を提供することが可能となる。

【図面の簡単な説明】

【００１１】

【図１】本発明の実施形態に係わるメールシステムの構成の一例を示す図である。

【図２】本発明の実施形態に係わるメールシステムにおける情報処理装置のハードウェア構成の一例を示すブロック図である。

【図３】本発明の実施形態に係わるメールシステムにおける情報処理装置のソフトウェア構成の一例を示すブロック図である。

【図４】本発明の実施形態に係わるメールシステムの備えるメール機能の一例を示す図である。

【図５】本発明の実施形態に係わるメールシステムの全体処理の一例を示すフローチャートである。

【図６】本発明の実施形態に係わるメールシステムのメール解析処理の一例を示すフローチャートである。

【図７】本発明の実施形態に係わるメールシステムのマスクメール生成処理の一例を示すフローチャートである。

【図８】本発明の実施形態に係わるメールシステムのメール送信画面の一例を示す図である。

【図９】本発明の実施形態に係わるメールシステムのパスワード通知用メール画面の一例を示す図である。

【図１０】本発明の実施形態に係わるメールシステムのマスクメールの受信画面の一例を示す図である。

【図１１】本発明の実施形態に係わるメールシステムの添付ファイルを開いた画面の一例を示す図である。

【図１２】本発明の実施形態に係わるメールシステムの添付ファイルを開く処理の一例を

示すフローチャートである。
【図１３】本発明の実施形態に係わるメールシステムの各種定義ファイルの一例を示す図である。
【発明を実施するための形態】
【００１２】
以下、本発明の実施の形態を、図面を参照して詳細に説明する。
【００１３】
図１は、本発明の実施形態に係わるメールシステムの構成の一例を示す図である。
【００１４】
このメールシステムでは、少なくとも一台のクライアント装置１０２（情報処理装置）とメールサーバ１０１およびＷｅｂメールサーバ１０４がネットワーク１０３（ＬＡＮ・ＷＡＮ）を介して接続されており、互いに電子メール（以下、単にメールとも呼ぶ）の送受信が可能となっている。また、必ずしもサーバはメールサーバ１０１およびＷｅｂメールサーバ１０４を必要とするものではなく、どちらか１種類のサーバで構成されるようにしてもよい。
【００１５】
なお、この図１では例として３台のクライアント装置１０２ａ～１０２ｃが設けられている場合を示しているが、何台あってもよい。また、情報処理装置の種類は、電子メールのクライアントとして利用することができる情報処理装置であればよく、ＰＣや携帯電話などの携帯端末などを適用可能である。
【００１６】
メールの送信者がいずれかのクライアント装置（ここではクライアント装置１０２ａ）からメールを送信すると、このメールはネットワーク１０３を介してメールサーバ１０１に受信される。
【００１７】
メールの受信者は、メールサーバ１０１からメールを受信し、受信したメールをメールクライアントのメールボックスから参照する。
【００１８】
メールサーバ１０１に対して送信されたメールは、クライアント端末１０２の送信トレイを利用して参照することが可能である。
【００１９】
また、メールサーバ１０１やＷｅｂメールサーバ１０４が複数存在し、クライアント装置１０２ａ、１０２ｃの間において複数のメールサーバやＷｅｂメールサーバを経由してメールの送受信をしてもよい。
【００２０】
Ｗｅｂメールサーバ１０４は、クライアント装置１０２に対してＷｅｂメールサービスを提供可能なサーバである。ユーザはクライアント装置１０２にはデータを持たず、Ｗｅｂブラウザなどを利用してサービスを利用する。この場合、メールの送受信データ（履歴データ含む）やアドレス帳はＷｅｂメールサーバに保存される。Ｗｅｂメールサーバを利用する場合、ユーザはＷｅｂメールサーバ上で電子メールの送信を行い、Ｗｅｂメールサーバが受信した電子メールを、Ｗｅｂブラウザを利用して閲覧する。
【００２１】
また、Ｗｅｂメールサーバ１０４は、クライアント装置１０２からＷｅｂブラウザを利用してアクセスされるため、クライアント装置１０２におけるファイル操作の制御も可能なようになっている。
【００２２】
図２は、本発明の実施形態に係わるメールシステムにおける情報処理装置のハードウェア構成の一例を示すブロック図である。
【００２３】
情報処理装置２００は、メールサーバ１０１、Ｗｅｂメールサーバ１０４、およびクラ

イアント装置１０２に適応可能である。
【００２４】
システムバス２０４を介してＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）２０１、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）２０３、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）２０２、入力コントローラ２０５、ビデオコントローラ２０６、メモリコントローラ２０７、通信Ｉ／Ｆコントローラ２０８等が接続された構成を採る。
【００２５】
ＣＰＵ２０１は、システムバス２０４に接続される各デバイスやコントローラを統括的に制御する。
【００２６】
また、ＲＯＭ２０２あるいは外部メモリ２１１には、ＣＰＵ２０１の制御プログラムであるＢＩＯＳ（Ｂａｓｉｃ Ｉｎｐｕｔ／Ｏｕｔｐｕｔ Ｓｙｓｔｅｍ）やＯＳ（Ｏｐｅｒａｔｉｎｇ Ｓｙｓｔｅｍ）や、各サーバあるいは各ＰＣが実行する機能を実現するために必要な後述する各種プログラム等が記憶されている。
【００２７】
また、本発明を実施するために必要な情報が記憶されている。なお外部メモリはデータベースであってもよい。
【００２８】
ＲＡＭ２０３は、ＣＰＵ２０１の主メモリ、ワークエリア等として機能する。ＣＰＵ２０１は、処理の実行に際して必要なプログラム等をＲＯＭ２０２あるいは外部メモリ２１１からＲＡＭ２０３にロードし、ロードしたプログラムを実行することで各種動作を実現する。
【００２９】
また、入力コントローラ２０５は、キーボード（ＫＢ）２０９や不図示のマウス等のポインティングデバイス等からの入力を制御する。
【００３０】
ビデオコントローラ２０６は、ディスプレイ２１０等の表示器への表示を制御する。尚、表示器は液晶ディスプレイ等の表示器でもよい。これらは、必要に応じて管理者が使用する。
【００３１】
メモリコントローラ２０７は、ブートプログラム、各種のアプリケーション、フォントデータ、ユーザファイル、編集ファイル、各種データ等を記憶する外部記憶装置（ハードディスク（ＨＤ））や、フレキシブルディスク（ＦＤ）、あるいは、ＰＣＭＣＩＡ（Ｐｅｒｓｏｎａｌ Ｃｏｍｐｕｔｅｒ Ｍｅｍｏｒｙ Ｃａｒｄ Ｉｎｔｅｒｎａｔｉｏｎａｌ Ａｓｓｏｃｉａｔｉｏｎ）カードスロットにアダプタを介して接続されるコンパクトフラッシュ（登録商標）メモリ等の外部メモリ２１１へのアクセスを制御する。
【００３２】
通信Ｉ／Ｆコントローラ２０８は、ネットワーク１０３を介して外部機器と接続・通信し、ネットワークでの通信制御処理を実行する。例えば、ＴＣＰ／ＩＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｒｏｌ Ｐｒｏｔｏｃｏｌ／Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）を用いた通信等が可能である。
【００３３】
なお、ＣＰＵ２０１は、例えばＲＡＭ２０３内の表示情報用領域へアウトラインフォントの展開（ラスタライズ）処理を実行することにより、ディスプレイ２１０上に表示することが可能である。また、ＣＰＵ２０１は、ディスプレイ２１０上のマウスカーソル（図示しない）等によるユーザ指示を可能とする。
【００３４】
本発明を実現するための後述する各種プログラムは、外部メモリ２１１に記録されており、必要に応じてＲＡＭ２０３にロードされることによりＣＰＵ２０１によって実行され

るものである。さらに、上記プログラムの実行時に用いられる定義ファイルおよび各種情報テーブル等も、外部メモリ２１１に格納されている。

【００３５】

図３は、本発明の実施形態に係わるメールシステムにおける情報処理装置のソフトウェア構成の一例を示すブロック図である。

【００３６】

情報処理装置３０１（メールサーバ１０１）の有する機能構成を示す図である。また、Ｗｅｂメールサーバでも本機能の提供することが可能となっており、その場合、本機能はＷｅｂメールサーバ１０４が有するものとする。

【００３７】

情報処理装置３０１は、メール受付部３０２、メール判定部３０３、添付ファイル生成部３０４、メール本文変更部３０６、パスワード生成部３０７、マスクメール生成部３０８、およびマスクメール送信部３０９を有する。

【００３８】

また、情報処理装置３０１がＷｅｂメールサーバ１０４であった場合、添付ファイル制御部３０５を備える。

【００３９】

メール受付部３０２は、メール送信者からのメールを受け付ける。メール判定部３０３は、受け付けたメールにマスクが必要などうかの判定を行う。判定には、あらかじめ設定された条件定義が利用される。

【００４０】

添付ファイル生成部３０４は、マスクが必要であったときに添付するための暗号化ファイルを生成する。暗号化ファイルは、設定されたパスワードの入力を受付けることで複号できるようになっている。なお、暗号化ファイルは圧縮ファイルであることが望ましいがこれに限ったものではない。

【００４１】

メール本文変更部３０６は、あらかじめ設定された条件定義をもとに、本文に必要な部分にマスクをする。パスワード生成部３０７は、作成された暗号化ファイルに付与するためのパスワードを生成する。付与するパスワードは事前に管理者が決めていてもよいし、ランダムに付与するようになっていてもよい。

【００４２】

マスクメール生成部３０８、本文がマスクされたメールに作成された暗号化ファイルを添付する。マスクメール送信部３０９は、生成されたマスクメールを送信者が宛先としていた受信者に配信（送信）する。

【００４３】

添付ファイル制御部３０５は、Ｗｅｂメールサーバ１０４が備える機能で、Ｗｅｂメールサーバに接続したクライアントが添付ファイルを操作する時の制御をする。

【００４４】

図４は、本発明の実施形態に係わるメールシステムの備えるメール機能の一例を示す図である。

【００４５】

本メールシステムにおける電子メールの送受信の流れを概念的に説明する図である。まず送信者４０１が平文のまま電子メール（１）を送信すると、メールサーバ４０２は、記憶している各種定義ファイル４０４を利用して、当該受信したメールの内容からマスクが必要かどうかの判定を行う。

【００４６】

マスクが必要であった場合、送信者４０１に対して、マスク時にパスワードが付与された場合、パスワード通知メール（２）の通知を行う。また、パスワード通知メール（２）は、送信者４０１に対して送信しなくてもよくその場合は、メールサーバ４０２が送信者４０３に対して直接送信するようにすればよい。

【００４７】
マスクされたメール（３）は、メール本文の該当箇所がマスクされた状態で送信され、元々送信されたメールの内容は、添付ファイルとして、受信者４０３に対して送信される。また、この時添付ファイルが暗号化された場合のパスワードは、送信者４０１から送信されるか、メールサーバ４０２から通知される。
【００４８】
送信者４０１から送信される電子メールは、メールの内容に応じて、各種定義ファイル４０４で設定された内容に応じてマスクされる。必ずしも全てのメールがマスクされるわけではなく、メールの内容によっては、マスクされない場合もある。各種定義ファイル４０４の内容については、図１３を使って説明する。
【００４９】
なお、本実施形態では、メールサーバ４０２とは、メールサーバ１０１およびＷｅｂメールサーバ１０４のことを指すものとし、特に説明のない限りどちらのサーバでも同様の処理を行うものとする。
【００５０】
図１３は、本発明の実施形態に係わるメールシステムの各種定義ファイルの一例を示す図である。
【００５１】
定義ファイルの一例として、検出条件定義１３００、宛先条件定義１３１０、およびオプション条件定義１３２０が記憶されている。
【００５２】
検出条件定義１３００は、電子メールの本文に書かれた文字からマスクすべき文字列を検出するための条件が定義されている（検出文字列記憶手段）。なお、便宜上、説明では文字列として説明するが、検出条件を１文字が検出されるように設定した場合の文字（１文字）も本発明の文字列に含むものとする。
【００５３】
パラメータ１３０１は、検出条件のタイトルであって、管理者が設定する際に自由に命名することが可能である。検出条件１３０２は、メール本文に対して書かれている文字列を検出するためのパラメータであって、検出手段１３０３に設定された方法で検出する。
【００５４】
検出された文字列は、マスク範囲１３０４で指定された範囲がマスクされる範囲となり、セキュリティレベル１３０５で指定されたセキュリティレベルが設定される。
【００５５】
例えば、パラメータ１３０１「ＩＰアドレス」で検出条件１３０２が「１１１．２２２．＊」の場合、検出条件１３０３が「部分一致」となっているので、「１１１．２２２．」を含む文字列がマスクの対象となり、マスク範囲１３０４が「該当箇所のみ」となっているので、当該文字列を含む箇所だけがマスクの対象となり、セキュリティレベル１３０５で指定されているようにセキュリティレベル「Ａ」となる。
【００５６】
セキュリティレベル１３０５は、宛先条件定義１３１０の宛先に応じたマスクの設定の条件に利用される。
【００５７】
同様に、パラメータ１３０２「ＩＰアドレス」で検出条件１３０２が「／＾（（［１－９］？［０－９］｜１［０－９］｛２｝｜２［０－４］［０－９］｜２５［０－５］）．）｛３｝（［１－９］？［０－９］｜１［０－９］｛２｝｜２［０－４］［０－９］｜２５［０－５］）＄／」である場合、検出手段１３０３が「正規表現」なので、「＊＊＊．＊＊＊．＊＊＊．＊＊＊」の文字列がマスクの対象となる。
【００５８】
なお、本実施形態では、検出手段１３０３として、「部分一致」「正規表現」「完全一致」を例に説明しているが、これに限ったものである必要がないのはいうまでもない。こ

の検出手段１３０３で検出条件１３０２に一致するものを検出することで、「ＩＰアドレス」「ＵＲＬ」「契約金額」「特定メール（メールアドレス）」「電話番号」「アカウント（社員番号）」などの文字列を検出することができる。

【００５９】

また、検出した文字列のみ（該当部分のみ）をマスクするのか、該当する文字列を含む行（該当行）をマスクするのか、検出した文字列の前後行（該当行の前後）をマスクするのかを、マスク範囲１３０４で指定することができる。

【００６０】

宛先条件定義１３１０では、検出条件定義１３００で決定したセキュリティレベルを用いて、宛先に応じたマスクの設定状態を設定することができる。なお、セキュリティレベルを利用した宛先条件定義によるマスクの設定を行うようにするか、行わないようにするかは、設定により変更することが可能になっている。

【００６１】

セキュリティレベル１３１１で指定されたセキュリティレベルごとに宛先に応じてマスクの有無が設定されている。

【００６２】

例えば、セキュリティレベル１３１１が「Ａ」の文字列は、社内宛て１３１２、グループ会社宛て（Ｇ会社宛て）１３１３、および社外宛て１３１４のいずれの場合であっても「マスク有」と設定されている。

【００６３】

オプション条件定義１３２０では、上述した２つの条件により決定したマスクに関連した設定によって、付加的なオプション設定を行う条件が設定されている。

【００６４】

条件１３２１で、「本文のマスク箇所が２つ以下」の場合、「添付ファイルはマスク部分のみ」とする。同様に条件１３２１で「セキュリティレベルがＣのみ」の場合、「添付ファイルはメール送信可能形式」で開かれるように制御される。また、条件１３２１が「元メールがある場合のみ開く」の場合、「元メールがなければ開けないようにする」と設定されている。詳細については後述する。

【００６５】

なお、本条件についても、宛先条件定義１３１０と同様に、管理者により指定されている条件のみ実行される。

【００６６】

図５は、本発明の実施形態に係わるメールシステムの全体処理の一例を示すフローチャートである。

【００６７】

送信者４０１からメールを受信した時のメールサーバ４０２の処理に対応する。

【００６８】

ステップステップＳ５０１で、電子メールを受信すると、ステップＳ５０２で受信したメールに対してマスク処理の有無を解析する解析処理を行う。

【００６９】

解析処理の結果の判定をステップＳ５０３で行い、マスク処理が必要でないと判定された場合は、ステップＳ５０６に進み通常のメール送信を受信者４０３に対して行う。メール送信とは、受信者に対してメールをプッシュ送信する方式であっても、受信者のメールボックスにメールを保存する処理でもよい。

【００７０】

一方、マスク処理が必要と判定された場合はステップＳ５０４に進み、マスクメール生成処理を行い、ステップＳ５０５でメール受信者に対してマスクメールの送信（配信）を行い、処理を終了する。メール解析処理およびマスクメール生成処理の詳細については、図６および図７を利用して説明する。

【００７１】

図６は、本発明の実施形態に係わるメールシステムのメール解析処理の一例を示すフローチャートである。

【００７２】

ステップＳ６０１で、メールサーバ４０２の記憶領域から検出条件定義１３００を取得し、ステップＳ６０２で送信メールの本文を解析する。送信メールの一例を図８に示す。

【００７３】

図８は、本発明の実施形態に係わるメールシステムのメール送信画面の一例を示す図である。

【００７４】

本画面は、クライアント端末１０２の画面でメール送信者４０１が作成するメール送信画面８０１である。メール送信者４０１は、本文８０２、宛先８０４、宛先（ＣＣ）８０５、および件名８０６を記入し、送信８０３が押下されることでメールサーバ４０２に対してメールが送信される。

【００７５】

ステップＳ６０２においては、本文８０２に記載された文字列に、検出条件定義１３００で定義された文字列を検出する解析を行う。

【００７６】

図の例ではＩＰＡｄｄｒｅｓｓ（１）とＩＰＡｄｄｒｅｓｓ（２）の「１９２．１６８．１．１」および「１９２．１６８．１１．１」が検出され、セキュリティレベル１３０５が「Ａ」となる。

【００７７】

フローチャート（図６）の説明に戻る。ステップＳ６０３で文字列が検出されなかった場合は、ステップＳ６０９に進み、解析結果は「マスク不要」とする。一方、図８に示すように対象となる文字列が検出された場合は、ステップＳ６０４に進み、宛先条件定義１３１０を取得する。

【００７８】

ステップＳ６０５で宛先を解析する。図８の例では、宛先が、宛先８０４と宛先（ＣＣ）８０５の２つ設定されているので、２つに対して解析を行う。宛先８０４を優先するようにしてもよいし、セキュリティレベルの高い方（Ａ＞Ｂ＞Ｃ）を優先するようにしてもよし、本実施形態で示すように、全ての宛先に対して処理を行い、異なるメールとして（例えばエンベロープ情報を利用して）送信するようにしてもよい。

【００７９】

マスクが必要かどうかの判定は、ステップＳ６０２で解析されたセキュリティレベルを利用する。図８の例では、「ＩＰアドレス」パラメータ１３０１が検出されたので、セキュリティレベルは「Ａ」となり、どの宛先に対してもマスク有と判定される。

【００８０】

仮に、パラメータ１３０１で「アカウント」が検出されたとすると、その場合は、宛先８０４に対しては、社外宛てなので「マスク有」、宛先（ＣＣ）８０５に対しては、社内宛てなので「マスク無」と判定される。なお、社内宛てか社外宛てか（またはグループ会社宛てか）については、宛先の電子メールアドレスのドメイン名などを利用して判定するようにすればよい。

【００８１】

ステップＳ６０７では判定されたマスク状態とマスク有を解析結果として記憶し、ステップＳ６０８に進む。ステップＳ６０８では、送信されたメールに設定された全ての宛先に対して解析したかどうかを判定し、全宛先に対して処理を行うまで、ステップＳ６０５に戻り処理を繰り返し、全宛先に対して解析処理を行った場合に処理を終了する。

【００８２】

図７は、本発明の実施形態に係わるメールシステムのマスクメール生成処理の一例を示すフローチャートである。

【００８３】

ステップＳ７０１でマスクするメール本文を抽出し、ステップＳ７０２でメール本文をパスワード付きファイルに暗号化する。パスワードはあらかじめ設定された付与ルールに従って付与される。

【００８４】

ステップＳ７０３では、メール本文の該当箇所をマスクする。マスクされたメール本文について、図１０を利用して説明する。

【００８５】

図１０は、本発明の実施形態に係わるメールシステムのマスクメールの受信画面の一例を示す図である。

【００８６】

図８で作成された電子メールの受信画面１００１である。本文１００２のＩＰＡｄｄｒｅｓｓ（１）とＩＰＡｄｄｒｅｓｓ（２）がそれぞれ「＊＊＊＊＊＊＊＊＊＊＊＊」とマスクされている。パラメータ１３０１の「ＩＰアドレス」に対するマスク範囲１３０４が「該当箇所のみ」となっているので、図のようにマスクされている。

【００８７】

仮に、マスク範囲１３０１が「該当行」となっていれば、ＩＰＡｄｄｒｅｓｓ（１）とＩＰＡｄｄｒｅｓｓ（２）の部分も「＊」でマスクされ、「該当行の前後」となっていれば、「ＩＰアドレスをご連絡いたします。」および「以上、よろしくお願いいたします。」の行も「＊」でマスクされることになる。

【００８８】

差出人１００３、宛先１００４、および件名には、送信メール８０１と同じものが付与され、添付１００６に、ステップＳ７０２で生成された暗号化されたファイル「ｓａ００１．ｚｉｐ」が添付されている。

【００８９】

フローチャート（図７）の説明に戻る。ステップＳ７０４では、受信者４０３に送信するための送信用のマスクメール（図１０）を作成して処理を終了する。

【００９０】

図９は、本発明の実施形態に係わるメールシステムのパスワード通知用メール画面の一例を示す図である。

【００９１】

ステップＳ７０２（図７）で作成された暗号化ファイルのパスワードの通知メール９０１の一例である。本メールは、メールサーバ４０２から送信者４０１に対して送信される通知メールである。

【００９２】

本文９０２には、パスワードに関する通知が書かれており、差出人９０３には、メールシステムのａｄｍｉｎが設定され、宛先９０４は、送信者４０１のアドレスである「ｎｅｔｎｅｔ@ａａａ．ｃｏ．ｊｐ」宛てになっている。

【００９３】

件名９０５は、元のメールに件名である「ＩＰアドレスのご連絡」に「パスワード通知」が付加されている。

【００９４】

このメールを受信した送信者４０１は、受信者４０３宛てにパスワード通知することで、受信者４０３は添付ファイルを開くことができるようになる。また、パスワードに関するメールをメールサーバ４０２が直接受信者４０３に対して送信するようにしてもよいことは言うまでもない。

【００９５】

図１１は、本発明の実施形態に係わるメールシステムの添付ファイルを開いた画面の一例を示す図である。

【００９６】

送信者４０３が、添付１００６の「ｓａ００１．ｚｉｐ」にパスワード入力後（不図示

）、開いた内容である。
【００９７】
受信メールビューア１１０１は、このメールに対して直接返信や転送を行うことができるような電子メール形式のメールソフトで開ける形式になっている。
【００９８】
一方、テキストビューア１１１１は、このメールに対して直接返信や転送を行うことができないようなファイル形式（電子メール形式でない）で開くようになっている。基本的には、返信や転送による情報の漏えい防止の観点からは、テキストビューア１１１１形式の方が望ましい。しかしながら、セキュリティレベルが低いなどは、このまま返信や転送の可能な受信メールビューア１１０１形式の方が望ましい場合もある。
【００９９】
そこで、本発明では、オプション条件定義１３２０で、「セキュリティレベルがＣのみ」の場合、「添付ファイルはメール送信可能形式」（すなわちメールソフト）で開けるようにすることができる。この場合、メールサーバ１０１でマスクメールを生成する時に、開く形式のとの対応付けをするようにしてもよいし、Ｗｅｂメールサーバ１０４であれば、クライアントが開く際に、オプション条件定義１３２０を参照し、添付ファイルを開く形式を決定するようにしてもよい。
【０１００】
また、オプション条件定義１３２０で、「本文のマスク箇所が２つ以下」の場合「添付ファイルはマスク部分のみ」と設定されていた場合、１１０１や１１１１の本文に表示される文字列を「１９２．１６８．１．１」および「１９２．１６８．１１．１」だけにすることができる。これにより、電子メール全体が暗号化された場合と比べて余計な情報が含まれないので、万一漏えいしてしまった場合のリスクを低く抑えることができる。なおマスクの箇所は２つ以下に限ったものではなく、あらかじめ所定数を設定しておくことができる。
【０１０１】
ただし、マスク部分が多いと、マスクされたどの部分に対応するのか不明になる恐れがあるので、元メールを同じ内容が表示されるようにしておいた方が望ましい。
【０１０２】
また、オプション定義１３２０で、「元メールがある場合のみ開く設定」が「元メールがなければ開けないようにする」と設定されている場合の例について、図１２を利用して説明する。
【０１０３】
図１２は、本発明の実施形態に係わるメールシステムの添付ファイルを開く処理の一例を示すフローチャートである。
【０１０４】
本フローは、送信先４０３のクライアント端末１０２で処理されるもので、メールに添付された暗号化ファイルを開く時の処理である。
【０１０５】
ステップＳ１２０１で、添付されていた元メールを保持するかを確認する。元メールがあれば、ステップＳ１２０２で複号を許可し、なければステップＳ１２０３で複号を許可しないようになっている。
【０１０６】
これは、添付ファイルとパスワードが同時に流出してしまった場合のリスクを下げるものであって、添付ファイルを開く時に、例えば添付された元メールが同一のクライアント端末１０２に存在（所持）するかどうかの判定を行うことにより実現する。この場合は、メールサーバ１０１で暗号化ファイルを生成するときにこのような動作をするスクリプトなどを暗号化ファイルに埋め込んでおくことにより実現可能である。
【０１０７】
また、Ｗｅｂメールサーバ１０４の場合は、暗号化ファイルを開く際に、本フローチャ

ートの処理をクライアント端末に実行させるか、Ｗｅｂメールサーバのプログラムがサーバ上で実行することで実現可能である。

【０１０８】

なお、上述した各種データの構成及びその内容はこれに限定されるものではなく、用途や目的に応じて、様々な構成や内容で構成されることは言うまでもない。

【０１０９】

以上、一実施形態について示したが、本発明は、例えば、システム、装置、方法、プログラムもしくは記録媒体等としての実施態様をとることが可能であり、具体的には、複数の機器から構成されるシステムに適用しても良いし、また、一つの機器からなる装置に適用しても良い。

【０１１０】

また、本発明におけるプログラムは、フローチャートにおける処理方法をコンピュータが実行可能なプログラムであり、本発明の記憶媒体はフローチャートにおける処理方法をコンピュータが実行可能なプログラムが記憶されている。なお、本発明におけるプログラムは各装置の処理方法ごとのプログラムであってもよい。

【０１１１】

以上のように、前述した実施形態の機能を実現するプログラムを記録した記録媒体を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはＣＰＵやＭＰＵ）が記録媒体に格納されたプログラムを読出し実行することによっても、本発明の目的が達成されることは言うまでもない。

【０１１２】

この場合、記録媒体から読み出されたプログラム自体が本発明の新規な機能を実現することになり、そのプログラムを記憶した記録媒体は本発明を構成することになる。

【０１１３】

プログラムを供給するための記録媒体としては、例えば、フレキシブルディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＤＶＤ－ＲＯＭ、磁気テープ、不揮発性のメモリカード、ＲＯＭ、ＥＥＰＲＯＭ、シリコンディスク、ソリッドステートドライブ等を用いることができる。

【０１１４】

また、コンピュータが読み出したプログラムを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムの指示に基づき、コンピュータ上で稼働しているＯＳ（オペレーティングシステム）等が実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【０１１５】

さらに、記録媒体から読み出されたプログラムが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵ等が実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【０１１６】

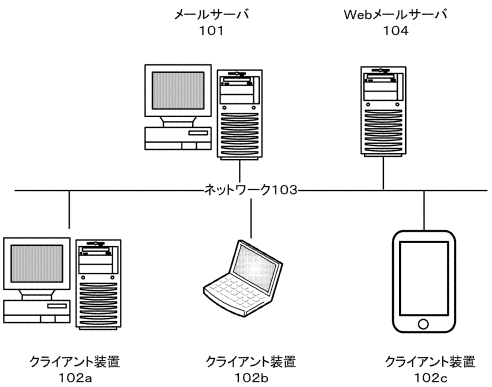
また、本発明は、複数の機器から構成されるシステムに適用しても、１つの機器からなる装置に適用してもよい。また、本発明は、システムあるいは装置にプログラムを供給することによって達成される場合にも適応できることは言うまでもない。この場合、本発明を達成するためのプログラムを格納した記録媒体を該システムあるいは装置に読み出すことによって、そのシステムあるいは装置が、本発明の効果を享受することが可能となる。

【０１１７】

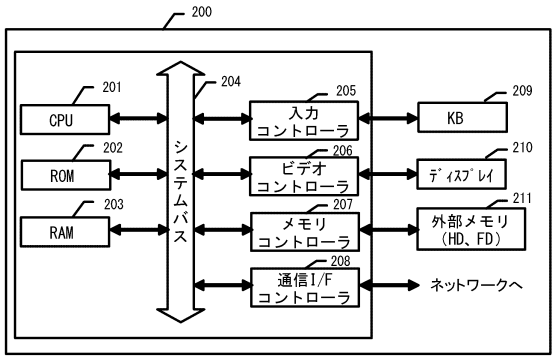
さらに、本発明を達成するためのプログラムをネットワーク上のサーバ、データベース等から通信プログラムによりダウンロードして読み出すことによって、そのシステムあるいは装置が、本発明の効果を享受することが可能となる。

【０１１８】
　なお、上述した各実施形態およびその変形例を組み合わせた構成も全て本発明に含まれるものである。
【符号の説明】
【０１１９】
１０１　メールサーバ
１０２　クライアント装置
１０３　ネットワーク
１０４　Ｗｅｂメールサーバ
２０１　ＣＰＵ
２０２　ＲＯＭ
２０３　ＲＡＭ
２０４　システムバス
２０５　入力コントローラ
２０６　ビデオコントローラ
２０７　メモリコントローラ
２０８　通信Ｉ／Ｆコントローラ

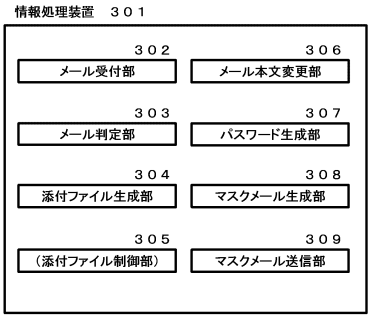
【図１】



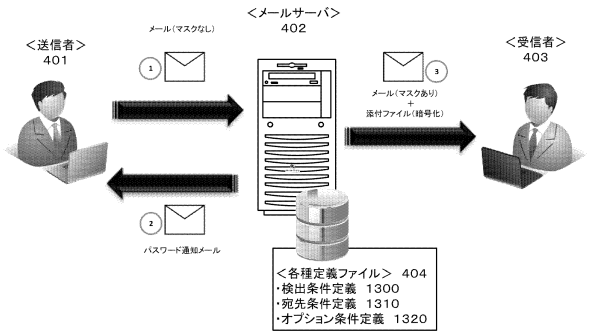
【図２】



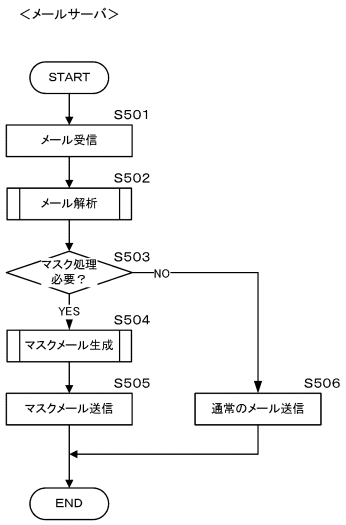
【図３】


情報処理装置　３０１
３０２
メール受付部
３０３
メール判定部
３０４
添付ファイル生成部
３０５
（添付ファイル制御部）
３０６
メール本文変更部
３０７
パスワード生成部
３０８
マスクメール生成部
３０９
マスクメール送信部

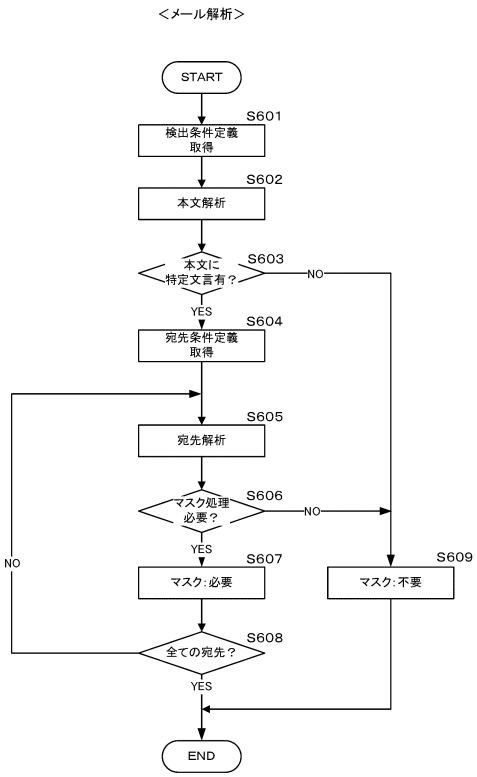
【図４】


<送信者>
401
メール（マスクなし）
<メールサーバ>
402
<受信者>
403
メール（マスクあり）
＋
添付ファイル（暗号化）
パスワード通知メール
<各種定義ファイル>　404
・検出条件定義　1300
・宛先条件定義　1310
・オプション条件定義　1320

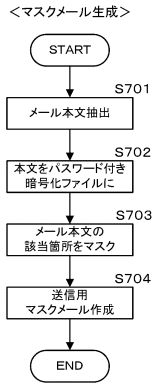
【図５】


<メールサーバ>
START
S501
メール受信
S502
メール解析
S503
マスク処理必要？
NO
YES
S504
マスクメール生成
S505
マスクメール送信
S506
通常のメール送信
END

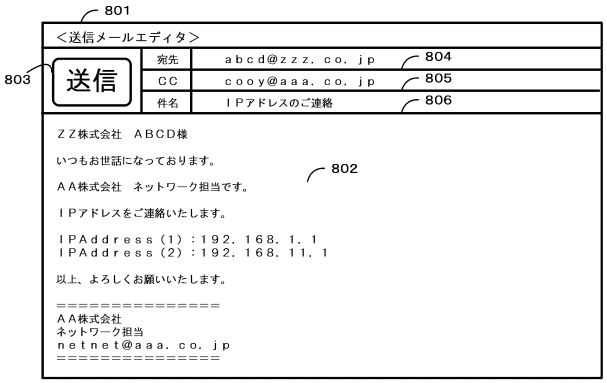
【図６】


<メール解析>
START
S601
検出条件定義取得
S602
本文解析
S603
本文に特定文言有？
NO
YES
S604
宛先条件定義取得
S605
宛先解析
S606
マスク処理必要？
NO
YES
S607
マスク：必要
S608
全ての宛先？
NO
YES
S609
マスク：不要
END

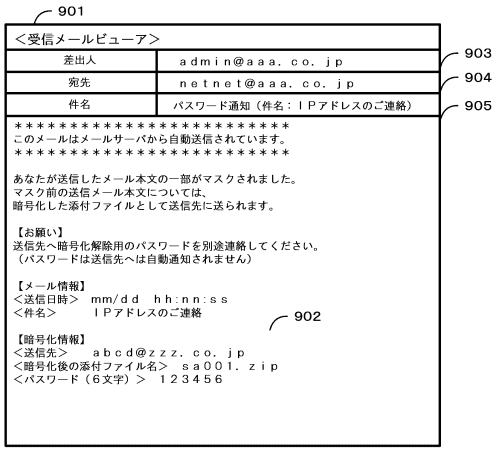
【図７】


＜マスクメール生成＞
START
S701
メール本文抽出
S702
本文をパスワード付き
暗号化ファイルに
S703
メール本文の
該当箇所をマスク
S704
送信用
マスクメール作成
END

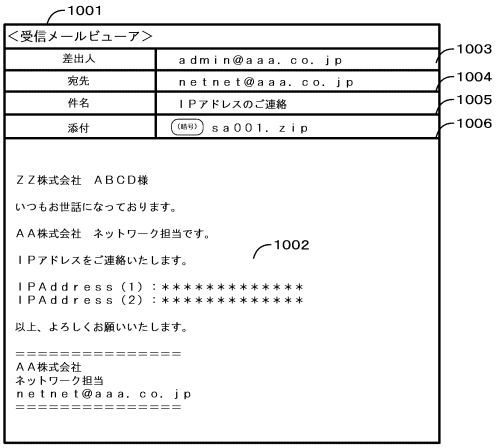
【図８】


801
＜送信メールエディタ＞
803
送信
宛先
ａｂｃｄ@ｚｚｚ．ｃｏ．ｊｐ
804
ＣＣ
ｃｏｏｙ@ａａａ．ｃｏ．ｊｐ
805
件名
ＩＰアドレスのご連絡
806
ＺＺ株式会社　ＡＢＣＤ様
いつもお世話になっております。
802
ＡＡ株式会社　ネットワーク担当です。
ＩＰアドレスをご連絡いたします。
ＩＰＡｄｄｒｅｓｓ（１）：１９２．１６８．１．１
ＩＰＡｄｄｒｅｓｓ（２）：１９２．１６８．１１．１
以上、よろしくお願いいたします。
＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝
ＡＡ株式会社
ネットワーク担当
ｎｅｔｎｅｔ@ａａａ．ｃｏ．ｊｐ
＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

【図９】


901
＜受信メールビューア＞
差出人
ａｄｍｉｎ@ａａａ．ｃｏ．ｊｐ
903
宛先
ｎｅｔｎｅｔ@ａａａ．ｃｏ．ｊｐ
904
件名
パスワード通知（件名：ＩＰアドレスのご連絡）
905
＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊
このメールはメールサーバから自動送信されています。
＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊
あなたが送信したメール本文の一部がマスクされました。
マスク前の送信メール本文については、
暗号化した添付ファイルとして送信先に送られます。
【お願い】
送信先へ暗号化解除用のパスワードを別途連絡してください。
（パスワードは送信先へは自動通知されません）
【メール情報】
＜送信日時＞　ｍｍ/ｄｄ　ｈｈ:ｎｎ:ｓｓ
＜件名＞　　ＩＰアドレスのご連絡
902
【暗号化情報】
＜送信先＞　　ａｂｃｄ@ｚｚｚ．ｃｏ．ｊｐ
＜暗号化後の添付ファイル名＞　ｓａ００１．ｚｉｐ
＜パスワード（６文字）＞　１２３４５６

【図１０】


1001
＜受信メールビューア＞
差出人
ａｄｍｉｎ@ａａａ．ｃｏ．ｊｐ
1003
宛先
ｎｅｔｎｅｔ@ａａａ．ｃｏ．ｊｐ
1004
件名
ＩＰアドレスのご連絡
1005
添付
（暗号）ｓａ００１．ｚｉｐ
1006
ＺＺ株式会社　ＡＢＣＤ様
いつもお世話になっております。
ＡＡ株式会社　ネットワーク担当です。
1002
ＩＰアドレスをご連絡いたします。
ＩＰＡｄｄｒｅｓｓ（１）：＊＊＊＊＊＊＊＊＊＊＊＊
ＩＰＡｄｄｒｅｓｓ（２）：＊＊＊＊＊＊＊＊＊＊＊＊
以上、よろしくお願いいたします。
＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝
ＡＡ株式会社
ネットワーク担当
ｎｅｔｎｅｔ@ａａａ．ｃｏ．ｊｐ
＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

【図１１】

1101

＜受信メールビューア＞

差出人	ａｄｍｉｎ@ａａａ．ｃｏ．ｊｐ
宛先	ｎｅｔｎｅｔ@ａａａ．ｃｏ．ｊｐ
件名	ＩＰアドレスのご連絡
添付	

ＺＺ株式会社　ＡＢＣＤ様

いつもお世話になっております。

ＡＡ株式会社　ネットワーク担当です。

ＩＰアドレスをご連絡いたします。

ＩＰＡｄｄｒｅｓｓ（１）：１９２．１６８．１．１
ＩＰＡｄｄｒｅｓｓ（２）：１９２．１６８．１１．１

以上、よろしくお願いいたします。

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝
ＡＡ株式会社
ネットワーク担当
ｎｅｔｎｅｔ@ａａａ．ｃｏ．ｊｐ
＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

1111

＜テキストビューア＞

ファイル（Ｆ）　書式（Ｗ）　表示（Ｖ）　ヘルプ（Ｈ）

ＺＺ株式会社　ＡＢＣＤ様

いつもお世話になっております。

ＡＡ株式会社　ネットワーク担当です。

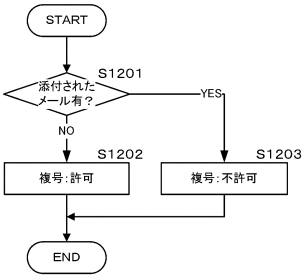
ＩＰアドレスをご連絡いたします。

ＩＰＡｄｄｒｅｓｓ（１）：１９２．１６８．１．１
ＩＰＡｄｄｒｅｓｓ（２）：１９２．１６８．１１．１

以上、よろしくお願いいたします。

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝
ＡＡ株式会社
ネットワーク担当
ｎｅｔｎｅｔ@ａａａ．ｃｏ．ｊｐ
＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

【図１２】



【図１３】

1301 パラメータ	1302 検出条件	1303 検出手段	1304 マスク範囲	1305 セキュリティレベル
IPアドレス	111.222.*	部分一致	該当箇所のみ	A
IPアドレス	/^(([1-9]?[0-9]|1[0-9][2]|2[0-4][0-9]|25[0-5]).){3}([1-9]?[0-9]|1[0-9][2]|2[0-4][0-9]|25[0-5])$/	正規表現	該当箇所のみ	A
URL	https*	正規表現	該当行	C
契約金額	¥b¥d{1,3}(,¥d{3})*¥b	正規表現	該当箇所のみ	B
特定メール	aaa.bb@xx.co.jp	完全一致	該当箇所のみ	B
電話番号	03-XXX-XXXX	完全一致	該当箇所のみ	C
アカウント	ADK*	正規表現	該当行の前後	C

＜検出条件定義　1300＞

1311 セキュリティレベル	1312 社内宛て	1313 G会社宛て	1314 社外宛て
A	マスク有	マスク有	マスク有
B	マスク無	マスク有	マスク有
C	マスク無	マスク無	マスク有

＜宛先条件定義　1310＞

1321 条件	1322 設定
本文のマスク箇所が2つ以下	添付ファイルはマスク部分のみ
セキュリティレベルがCのみ	添付ファイルはメール送信可能形式
「元メールがある場合のみ開く」設定	元メールがなければ開けないようにする

＜オプション条件定義　1320＞

フロントページの続き

(72)発明者　藤野　智大
東京都品川区東品川２丁目４番１１号　キヤノンソフトウェア株式会社内

審査官　今川　悟

(56)参考文献　特開２０１０－０４９４４９（ＪＰ，Ａ）
特開２００７－１６４６１３（ＪＰ，Ａ）
特開２００８－２１９８４９（ＪＰ，Ａ）
特開２００７－２３３７１５（ＪＰ，Ａ）
特開２０１４－１４９７７２（ＪＰ，Ａ）
特開２００２－１４９６３８（ＪＰ，Ａ）
特開２０１４－１８６４２５（ＪＰ，Ａ）
特開２０１２－２０８７０３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　１３／００
Ｇ０６Ｆ　２１／６２