(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2010-134832
(P2010-134832A)
(43)公開日　平成22年6月17日(2010.6.17)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/20	(2006.01)	G06F 15/00	330A	5B285

審査請求 未請求　請求項の数 5　ＯＬ　（全 13 頁）

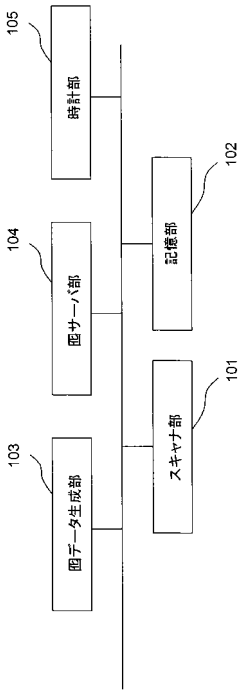
(21)出願番号　特願2008-312218 (P2008-312218)
(22)出願日　平成20年12月8日 (2008.12.8)

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(74)代理人　100084250
弁理士　丸山　隆夫
(72)発明者　神保　潤哉
東京都大田区中馬込１丁目３番６号　株式会社リコー内

Ｆターム(参考)　5B285 AA06　BA03　BA07　CA32　CB52
CB55　CB62　CB72　CB85　DA10

(54)【発明の名称】情報処理装置及びプログラム

(57)【要約】
【課題】悪意のある第三者の存在を検出することが可能な情報処理装置を提供する。
【解決手段】　データを傍受した第三者を特定の機器にアクセスさせるように仕向けるための囮データを生成する囮データ生成部（103）と、囮データを含めたデータを送信するスキャナ部（101）と、を有し、囮データ生成部（103）は、第三者にとって興味を惹かせる囮情報と、その囮情報が参照可能な特定の機器にアクセスさせるためのアクセス情報と、を少なくとも含めた囮データを生成する。
【選択図】図３



【特許請求の範囲】
【請求項１】
データを送信する情報処理装置であって、
前記データを傍受した第三者を特定の機器にアクセスさせるように仕向けるための囮データを生成する囮データ生成手段と、
前記囮データを含めたデータを送信する送信手段と、を有し、
前記囮データ生成手段は、
前記第三者にとって興味を惹かせる囮情報と、前記囮情報が参照可能な特定の機器にアクセスさせるためのアクセス情報と、を少なくとも含めた前記囮データを生成することを特徴とする情報処理装置。
【請求項２】
前記送信手段は、
前記第三者が解読可能な形式の前記囮データを前記データに含めて送信することを特徴とする請求項１記載の情報処理装置。
【請求項３】
前記囮データ生成手段は、
前記囮情報が参照可能な画面に遷移可能な形式の前記囮データを生成することを特徴とする請求項１または２記載の情報処理装置。
【請求項４】
前記特定の機器は、前記情報処理装置であり、
前記情報処理装置にアクセスした前記第三者に関する情報を記録する記憶手段を有することを特徴とする請求項１から３の何れか１項に記載の情報処理装置。
【請求項５】
データを送信する情報処理装置に実行させるプログラムであって、
前記データを傍受した第三者を特定の機器にアクセスさせるように仕向けるための囮データを生成する囮データ生成工程と、
前記囮データを含めたデータを送信する送信工程と、を前記情報処理装置に実行させ、
前記囮データ生成工程は、
前記第三者にとって興味を惹かせる囮情報と、前記囮情報が参照可能な特定の機器にアクセスさせるためのアクセス情報と、を少なくとも含めた前記囮データを生成することを特徴とするプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、データを傍受し、その傍受したデータに含まれる情報を利用して不正なアクセスを試みる悪意のある第三者の存在を検出する技術に関するものである。
【背景技術】
【０００２】
現在、インターネットの利用者は増加の一途を辿っており、コミュニケーションの一手段として、電子メール等を利用する利用者が増大している。
【０００３】
しかし、電子メール等のデータを傍受し、その傍受したデータに含まれる情報を利用して不正なアクセスを試みる悪意のある第三者が存在するのも現状である。
【０００４】
このようなことから、本発明より先に出願された技術文献として、第三者にデータを傍受されないように秘密通信を行う技術について開示された文献がある（例えば、特許文献１参照）。上記特許文献１には、量子相関性の良い光ビーム対の量子相関性を利用し、秘密通信を行う技術について開示されている。
【特許文献１】特許第３５６４４８９号公報
【発明の開示】

【発明が解決しようとする課題】
【０００５】
しかし、上記特許文献１のような量子通信技術が市場に普及するかどうかは不明であるため、既存の通信技術を用いて悪意のある第三者の存在を検出し、その第三者の不正なアクセスを防止するようにしたいのが現状である。
【０００６】
本発明は上記事情に鑑みてなされたものであり、悪意のある第三者の存在を検出することが可能な情報処理装置及びプログラム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】
【０００７】
かかる目的を達成するために、本発明は、以下の特徴を有することとする。
【０００８】
＜情報処理装置＞
本発明にかかる情報処理装置は、データを送信する情報処理装置であって、前記データを傍受した第三者を特定の機器にアクセスさせるように仕向けるための囮データを生成する囮データ生成手段と、前記囮データを含めたデータを送信する送信手段と、を有し、前記囮データ生成手段は、前記第三者にとって興味を惹かせる囮情報と、前記囮情報が参照可能な特定の機器にアクセスさせるためのアクセス情報と、を少なくとも含めた前記囮データを生成することを特徴とする。
【０００９】
＜プログラム＞
また、本発明にかかるプログラムは、データを送信する情報処理装置に実行させるプログラムであって、前記データを傍受した第三者を特定の機器にアクセスさせるように仕向けるための囮データを生成する囮データ生成工程と、前記囮データを含めたデータを送信する送信工程と、を前記情報処理装置に実行させ、前記囮データ生成工程は、前記第三者にとって興味を惹かせる囮情報と、前記囮情報が参照可能な特定の機器にアクセスさせるためのアクセス情報と、を少なくとも含めた前記囮データを生成することを特徴とする。
【発明の効果】
【００１０】
本発明によれば、悪意のある第三者の存在を検出することが可能となる。
【発明を実施するための最良の形態】
【００１１】
＜通信システムの概要＞
まず、図１を参照しながら、本実施形態の通信システムの概要について説明する。
【００１２】
本実施形態の通信システムは、情報処理装置100と、メールサーバ200と、クライアントPC300と、通信装置400と、がネットワークNWを介して接続して構成している。
【００１３】
情報処理装置100は、メールサーバ200にメールを送信し、メールサーバ200にメールを保存する。正規のユーザは、クライアントPC300を使用し、メールサーバ200にアクセスし、メールサーバ200に保存されているメールを閲覧する。これにより、正規のユーザは、メールサーバ200に保存されているメールを閲覧することが可能となる。
【００１４】
なお、上述した本実施形態の通信システムでは、悪意のある第三者が通信装置400を利用し、ネットワークNW上に存在するメールを傍受し、その傍受したメールに含まれる情報を利用して不正なアクセスが行われる虞がある。このため、悪意のある第三者の存在を検出し、第三者の不正なアクセスを防止するようにすることが可能なシステムの開発が必要視されることになる。
【００１５】
本実施形態の通信システムでは、上記の問題を解決すべく、情報処理装置100は、悪意

のある第三者を情報処理装置100にアクセスさせるように仕向けるための囮データを作成し、その作成した囮データを含めたメールをネットワークNWに送信する。囮データは、悪意のある第三者にとって興味を惹かせる囮情報と、その囮情報が参照可能な情報処理装置100にアクセスさせるためのアクセス情報と、を少なくとも含めて作成する。

【００１６】

これにより、悪意のある第三者が囮データを含むメールを傍受した場合に、その傍受した囮データに含まれる囮情報に興味を惹き、囮データに含まれるアクセス情報を基に、情報処理装置100にアクセスさせるように仕向けることが可能となる。その結果、悪意のある第三者の存在を検出し、第三者の不正なアクセスを防止させることが可能となる。以下、添付図面を参照しながら、本実施形態の通信システムについて詳細に説明する。

【００１７】

＜通信システムのシステム構成例＞

まず、図１を参照しながら、本実施形態の通信システムのシステム構成例について説明する。図１は、本実施形態の通信システムのシステム構成例を示す図である。

【００１８】

本実施形態の通信システムは、情報処理装置100と、メールサーバ200と、クライアントPC300と、通信装置400と、がネットワークNWを介して接続して構成している。なお、ネットワークNWの通信形態は特に限定するものではなく、有線、無線を問わずあらゆる通信形態が適用可能である。

【００１９】

情報処理装置100は、メールサーバ200にメールを送信するものである。本実施形態の情報処理装置100は、囮データを含めたメールをメールサーバ200に送信する。メールの送信方法としては、例えば、e-mail配信が挙げられる。囮データは、メールを傍受した第三者（盗聴者、攻撃者等）が、そのメールに含まれる囮データを基に、情報処理装置100にアクセスさせるように仕向けるための情報である。盗聴者は、メールを傍受する者であり、攻撃者は、傍受したメールに含まれる情報を基に、任意の機器を攻撃する者である。

【００２０】

メールサーバ200は、メールを保存するものであり、公知のメールサーバの機能を有して構成する。

【００２１】

クライアントPC300は、メールサーバ200に保存されたメールを閲覧する正規のユーザが使用する機器であり、公知の機能を有して構成する。

【００２２】

通信装置400は、メールを傍受する第三者（盗聴者、攻撃者等）が使用する機器であり、公知の通信機能を有して構成する。

【００２３】

＜情報処理装置100のハードウェア構成例＞

次に、図２を参照しながら、本実施形態の情報処理装置100のハードウェア構成例について説明する。図２は、本実施形態の情報処理装置100のハードウェア構成例を示す図である。

【００２４】

本実施形態の情報処理装置100は、図２に示すように、システムコントローラ110と、スキャナ120と、画像処理部130と、通信インタフェース140と、操作表示部150と、HDD160と、を含んで構成している。

【００２５】

システムコントローラ110は、情報処理装置100の制御を行うものであり、CPU111、ROM112、RAM113を含んで構成している。CPU111は、例えば、ROM112、HDD160等からプログラムを読み出し、その読み出したプログラムをRAM113上に展開して実行する。また、CPU111は、通信インタフェース140から入力された画像データをRAM113上に展開して実行する。

【００２６】

スキャナ120は、画像読取処理を行うものである。画像処理部130は、画像処理を行うものである。通信インタフェース140は、外部の通信機器と通信を行うものである。なお、通信インタフェース140は、第三者がメールを傍受し易いようにするために、ワイヤレスネットワークアダプタで構成することが好ましい。但し、通信インタフェース140は、必ずしもワイヤレスである必要はなく、通常のEthernet（登録商標）アダプタで構成することも可能である。操作表示部150は、システムコントローラ110から通知された情報を表示したり、ユーザから入力された情報をシステムコントローラ110に通知したりするものである。HDD160は、各種データやプログラムを格納するものである。

【００２７】

＜情報処理装置100の機能構成＞

次に、図３を参照しながら、本実施形態の情報処理装置100の機能構成例について説明する。図３は、本実施形態の情報処理装置100の機能構成例を示す図である。

【００２８】

本実施形態の情報処理装置100は、スキャナ部101と、記憶部102と、囮データ生成部103と、囮サーバ部104と、時計部105と、を含んで構成している。

【００２９】

スキャナ部101は、公知のネットワークスキャナの機能を実現するものである。

【００３０】

記憶部102は、各種情報を記憶するものである。

【００３１】

囮データ生成部103は、囮データを生成する機能を実現するものである。

【００３２】

囮サーバ部104は、第三者からのアクセスを受け付け、第三者の情報を記録する機能を実現するものである。

【００３３】

時計部105は、現在時刻を計測する機能を実現するものである。

【００３４】

＜スキャナ部101の処理動作＞

次に、図４を参照しながら、スキャナ部101の処理動作について説明する。なお、一般的なネットワークスキャナの処理動作については割愛し、メールを生成する際の処理動作について説明する。

【００３５】

まず、スキャナ部101は、メールサーバ200宛に送信するためのメールヘッダを生成する（ステップS1）。

【００３６】

次に、スキャナ部101は、囮データを含むメッセージパート１（プレーンテキスト）を生成し、その生成したメッセージパート１をメールのボディ部分に追加する（ステップS2）。囮データの具体的な生成方法については後述する。次に、スキャナ部101は、スキャンデータを含むメッセージパート２を生成し、その生成したメッセージパート２をメールのボディ部分に追加する（ステップS3）。スキャンデータは、公知の画像読取処理を行って取得したデータである。

【００３７】

なお、スキャナ部101は、囮データを含むメッセージパート１を、第三者が解読容易な暗号化方式（平文やBase64のようなスクランブル、或いは、DES等）で暗号化する。また、スキャンデータを含むメッセージパート２を、第三者が解読困難な暗号化方式（S/MIME等）で暗号化する。これにより、スキャナ部101は、囮データの部分のみを第三者に解読させることが可能な形式のメールを作成し、その作成したメールをメールサーバ200宛に送信することが可能となる。その結果、第三者に漏洩してもよい情報（囮データ）だけを第三者に公開させることが可能となる。

【００３８】

なお、暗号化方式は、上述した暗号化方式に限定するものではなく、SOAPなどのXMLベースの書式でも部分的に暗号化することが可能であるため、それらの技術を適用し、上述したメールを作成することも可能である。

【００３９】

＜囮データ生成部103の処理動作＞

次に、図５を参照しながら、囮データ生成部103の処理動作について説明する。囮データ生成部103は、時計部105で計測した時刻情報を基に、毎月１日の午前０時に以下の処理動作を行い、囮データを生成する。

【００４０】

まず、囮データ生成部103は、以下のテンプレート文字列を記憶部102から読み出す（ステップA1）。

【００４１】

＜テンプレート文字列＞

http:/機器IPアドレスorホスト名:18888/administrator/confidencial/scandatafile/image.html?ID=admin?PASS=パスワード文字列

【００４２】

但し、『機器IPアドレスorホスト名』の部分と、『パスワード文字列』の部分と、は変動部分であり、それ以外の部分が固定部分となる。テンプレート文字列は、予め記憶部102に記憶しておく。

【００４３】

次に、囮データ生成部103は、パスワード文字列を生成する（ステップA2）。パスワード文字列の生成方法は特に限定するものではなく、公知の手法を適用して生成することが可能である。本実施形態では、ランダムに選択した８文字をパスワード文字列とする。

【００４４】

次に、囮データ生成部103は、機器IPアドレスorホスト名を記憶部102から読み出す（ステップA3）。機器IPアドレスorホスト名は、情報処理装置100のIPアドレス、または、ホスト名であり、予め記憶部102に記憶しておく。

【００４５】

次に、囮データ生成部103は、テンプレート文字列と、パスワード文字列と、機器IPアドレスorホスト名と、を合成し、囮データを生成する（ステップA4）。

【００４６】

次に、囮データ生成部103は、上記生成した囮データを記憶部102に記憶する（ステップA5）。

【００４７】

このように、囮データ生成部103は、テンプレート文字列を記憶部102から読み出し、そのテンプレート文字列の変動部分である『機器IPアドレスorホスト名』の部分と、『パスワード文字列』の部分と、にステップA2,A3の処理で取得した新たな文字列を合成し、新たな囮データを生成し、記憶部102に記憶することになる。

【００４８】

なお、上述した囮データの生成方法は一例であり、上述した囮データをユーザが人手操作で生成するように構築することも可能である。また、複数のパターンの囮データを予め記憶部102に記憶しておき、その記憶部102に記憶した複数のパターンの囮データの中からユーザが人手操作で任意に選択し、上述した囮データを生成するように構築することも可能である。

【００４９】

また、上記実施形態では、囮データの生成を月に１回行うことにしたが、囮データの生成は、１回である必要はなく、現実のパスワードポリシーが半年に一度の更新ということが多いため、囮データの生成を半年に一度行うように構築することも可能である。

【００５０】

＜囮サーバ部104の処理動作＞

次に、図６、図７を参照しながら、囮サーバ部104の処理動作について説明する。

【００５１】

まず、図６を参照しながら、第三者に参照させる画像データを設定する処理動作について説明する。

【００５２】

まず、囮サーバ部104は、乱数を用いて公開用画像データ数を決定する（ステップB1）。本実施形態では、公開用画像データ数として3が決定されたと仮定する。

【００５３】

次に、囮サーバ部104は、各画像データに付与される公開月パラメータを基に、検索対象月の画像データを検索し（ステップB2）、その検索した画像データに付与されている公開月パラメータを０に更新する（ステップB3）。例えば、検索対象月の画像データとして３月の画像データを検索したい場合には、公開月パラメータである３を基に、検索対象月である３月の画像データを検索する。そして、その検索して得られた３月の画像データに付与されている公開月パラメータを０に更新することになる。

【００５４】

次に、囮サーバ部104は、公開月パラメータが０の画像データの中から公開用画像データ数分だけランダムに画像データを選択する（ステップB4）。本実施形態では、公開用画像データをランダムに3つ選択する。

【００５５】

次に、上記選択した選択画像データに付与される公開月パラメータを、該当月の値（例えば、３）に更新する（ステップB5）。

【００５６】

次に、囮サーバ部104は、上記選択した選択画像データのアクセス権を公開用に設定し、その他の残りの画像データのアクセス権を非公開用に設定する（ステップB6）。

【００５７】

次に、囮サーバ部104は、公開用に設定した画像データにリンクするためのリンク情報をimage_list.htmlに含ませるように設定する（ステップB7）。

【００５８】

本実施形態の囮データに含まれるURLの『image.html』は、ログイン画面に遷移する情報であり、そのログイン画面からログインすると、image_list.htmlに対応する画像データを選択することが可能な画像選択画面に遷移するように構築している。このため、公開用に設定した画像データにリンクするためのリンク情報をimage_list.htmlに含ませるように設定することで、公開用に設定した画像データを画像選択画面から第三者に選択させるようにすることが可能となる。

【００５９】

本実施形態では、機密文書のスキャン画像を模した画像データを囮情報として利用する。このため、例えば、３６パターンの画像データを記憶部102に記憶しておき、月ごとにランダムに最大３つの画像データを外部の通信装置からアクセス可能な状態に設定し、先月以前の画像データについては外部の通信装置からアクセス不可能な状態に設定する。また、ステップB4で選択する３つの画像データは、過去１２ヶ月の間にアクセス可能な状態になっていないものを選択する。

【００６０】

なお、囮情報として画像データを用いているのは、URLの中にスキャン画像を想起させる情報『scandatafile』が含まれている為である。このため、上述したテンプレート文字列とは異なるテンプレート文字列を適用する場合は、囮情報として画像データを用いる必要はなく任意の情報を囮情報にすることが可能である。

【００６１】

また、本実施形態では、３６パターンの画像データを記憶部102に記憶することにしたが、画像データは３６パターンである必要はなく、任意のパターンの画像データを記憶部102に記憶することも可能である。但し、囮情報に相当する画像データが常に同じである

と、その画像データが囮情報と第三者が察知してしまう虞がある。このため、複数のパターンの画像データを記憶部102に記憶しておき、囮情報とする画像データを動的に変更するように構築することが好ましい。

【００６２】

また、囮情報としては、業績情報、新製品情報、秘密情報、新技術情報、個人情報等が含まれていることが好ましい。これにより、メールを傍受した第三者を情報処理装置100にアクセスさせるように仕向ける確率を向上させることが可能となる。

【００６３】

次に、図７を参照しながら、第三者が通信装置300を用いて囮サーバ部104にアクセスした際の処理動作について説明する。

【００６４】

まず、第三者が通信装置300を用いてネットワークNW上に存在するメールを傍受し、そのメールに含まれる囮データ（ URL:http://機器IPアドレスorホスト名:18888/administrator/confidencial/scandatafile/image.html）を基に、情報処理装置100にアクセスする。囮サーバ104は、囮データのURLにアクセスがあった場合に（ステップC1/Yes）、ログイン画面を通信装置300の表示部に表示する（ステップC2）。

【００６５】

第三者は、ユーザ名（?ID）としてadminを入力し、パスワード(?PASS)としてパスワード文字列をログイン画面から入力する。囮サーバ104は、ログイン画面から入力されたユーザ名、パスワードを基に、正しいパスワードが入力された場合に、認証OKと判定し（ステップC3/Yes）、画像選択画面を通信装置300の表示部に表示する（ステップC4）。正しいパスワードが入力されたか否かは、パスワード(?PASS)として入力されたパスワード文字列と、囮データ生成部103がステップA2で生成したパスワード文字列と、が一致しているか否かで判定する。画像選択画面は、image_list.htmlに含ませたリンク情報先の画像データを選択することが可能な画面である。

【００６６】

本実施形態では、公開用に設定した３つの画像データimage1～image3にリンクするためのリンク情報をimage_list.htmlに含ませるように設定しているため、image1～image3の３つの画像データを選択することが可能な画像選択画面を通信装置300の表示部に表示する。

【００６７】

第三者は、画像選択画面の中から画像データを選択する。囮サーバ104は、画像選択画面の中から任意の画像データが選択された場合に（ステップC5/Yes）、その選択された画像データ（選択画像）を通信装置300の表示部に表示する（ステップC6）。

【００６８】

例えば、囮サーバ104は、画像選択画面の中からimage1に対応する画像データが選択された場合には、そのimage1に対応する画像データ（選択画像）を通信装置300の表示部に表示する。

【００６９】

なお、囮サーバ104は、第三者が通信装置300を用いて情報処理装置100にアクセスした際のHTTPリクエスト、IPアドレス、MACアドレス、時刻等の情報を記憶部102に記録し、第三者が情報処理装置100にアクセスした際の情報を記憶部102に記録して管理する。これにより、情報処理装置100は、メールを傍受した情報を利用して不正なアクセスを試みた悪意のある第三者の存在を特定したり、その第三者の行動等を把握したりすることが可能となる。

【００７０】

なお、囮サーバ104は、認証OKと判定した場合に（ステップC3/Yes）、ネットワーク管理者の機器（図示せず）に、悪意のある第三者の存在を検出した旨の情報を通知するように構築することも可能である。

【００７１】

また、囮データ（URL:http://機器IPアドレスorホスト名:18888/administrator/confidencial/scandatafile/image.html）が充分複雑であり、そのURLの情報が公開されていなければ、囮サーバ104は、そのURLにアクセスした段階で、ネットワーク管理者の機器に、悪意のある第三者の存在を検出した旨の情報を通知するように構築することも可能である。

【００７２】

＜本実施形態の通信システムの作用・効果＞

このように、本実施形態の通信システムでは、情報処理装置100は、悪意のある第三者にとって興味を惹かせる囮情報（画像データ等の情報）と、その囮情報が参照可能な情報処理装置100にアクセスさせるためのアクセス情報（IPアドレス、ホスト名、ドメイン名、通信ポート番号等の情報）と、を少なくとも含めた囮データを生成し、その生成した囮データを含むメールをネットワークNWに送信する。これにより、悪意のある第三者がメールを傍受し、そのメールに含まれる囮データを基に、囮機器である情報処理装置100にアクセスさせるように仕向けることが可能となる。その結果、悪意のある第三者の存在を検出し、第三者の不正なアクセスを防止することが可能となる。

【００７３】

また、情報処理装置100は、囮データに含まれる囮情報を動的に更新するようにする。これにより、囮データが囮であることを第三者に察知されてしてしまうことを回避することが可能となる。

【００７４】

また、情報処理装置100は、囮情報がデータベース、サーバ等の囮機器に格納されている旨を示唆する情報を含めた囮データを作成することが好ましい。これにより、第三者にとって魅力的な情報が囮機器に存在するように思わせ、第三者を囮機器にアクセスさせるように仕向ける確率を向上させることが可能となる。また、囮情報が格納されている機器が囮機器であることを第三者に察知され難くすることが可能となる。

【００７５】

また、情報処理装置100は、囮情報が参照可能な画面に遷移することが可能な情報（アクセスパス、URL、ユーザID、パスワード等の情報）を含めた囮データを作成することが好ましい。これにより、第三者が情報処理装置100にアクセスした後に、複数のステップを踏んだ上で第三者が囮情報を参照できるように構築することが可能となる。その結果、第三者が情報処理装置100にアクセスした際に、直ちに囮情報を第三者に参照させるのではなく、複数のステップを踏んだ上で囮情報を第三者に参照させるように構築することが可能となる。

【００７６】

また、情報処理装置100は、第三者が囮機器である情報処理装置100にアクセスした際に、第三者が情報処理装置100にアクセスした際の情報を記録して管理する。これにより、情報処理装置100は、メールを傍受した情報を利用して不正なアクセスを試みた悪意のある第三者の存在を特定したり、その第三者の行動等を把握したりすることが可能となる。

【００７７】

なお、上述する実施形態は、本発明の好適な実施形態であり、上記実施形態のみに本発明の範囲を限定するものではなく、本発明の要旨を逸脱しない範囲において種々の変更を施した形態での実施が可能である。

【００７８】

例えば、上記実施形態では、囮データを含むメールを送信することにしたが、送信データは、メールに限定するものではなく、各種のデータに囮データを含めることも可能である。また、データを送信する際のプロトコルも特に限定するものではなく、SMTP、FTP、SOAP等の各種プロトコルが適用可能である。

【００７９】

また、上記実施形態では、情報処理装置100は、スキャナ部101と、囮データ生成部103と、囮サーバ部104と、を有して構成することにしたが、囮データを含む送信データを送

信する送信機能（スキャナ部101、囮データ生成部103）と、第三者のアクセスを受け付けるアクセス機能（囮サーバ部104）と、を別々の情報処理装置に設けるように構築することも可能である。

【００８０】

但し、囮データを含む送信データを送信する送信機能（スキャナ部101、囮データ生成部103）と、第三者のアクセスを受け付けるアクセス機能（囮サーバ部104）と、を別々の情報処理装置に設けるように構築する場合は、各々の情報処理装置で管理する情報の同期が取れるように構築する必要がある。

【００８１】

また、上記実施形態では、情報処理装置100は、スキャナ部101を有し、公知のネットワークスキャナ機能を有する構成としたが、情報処理装置100は、ネットワーク上の機器と通信することが可能であれば、ネットワークスキャナ機能を設ける必要はない。但し、情報処理装置100は、囮データを含む送信データを送信する為に、送信データを日常的に送信する機器であることが好ましい。

【００８２】

また、情報処理装置100が囮機器であることを第三者に察知されないようにするためには、上述した本実施形態のように、他の機能（ネットワークスキャナ機能）を持つように構築し、囮データを含めた送信データを送信するように構成することが望ましい。

【００８３】

また、上述した本実施形態における通信システムを構成する各装置における制御動作は、ハードウェア、または、ソフトウェア、あるいは、両者の複合構成を用いて実行することも可能である。

【００８４】

なお、ソフトウェアを用いて処理を実行する場合には、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれているコンピュータ内のメモリにインストールして実行させることが可能である。あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

【００８５】

例えば、プログラムは、記録媒体としてのハードディスクやROM（Read Only Memory）に予め記録しておくことが可能である。あるいは、プログラムは、リムーバブル記録媒体に、一時的、あるいは、永続的に格納（記録）しておくことが可能である。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウエアとして提供することが可能である。なお、リムーバブル記録媒体としては、フロッピー（登録商標）ディスク、CD-ROM（Compact Disc Read Only Memory）、MO（Magneto optical）ディスク、DVD（Digital Versatile Disc）、磁気ディスク、半導体メモリなどが挙げられる。

【００８６】

なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールすることになる。また、ダウンロードサイトから、コンピュータに無線転送することになる。また、ネットワークを介して、コンピュータに有線で転送することになる。

【００８７】

また、本実施形態における通信システムは、上記実施形態で説明した処理動作に従って時系列的に実行されるのみならず、処理を実行する装置の処理能力、あるいは、必要に応じて並列的にあるいは個別に実行するように構築することも可能である。

【産業上の利用可能性】

【００８８】

本発明は、セキュリティを必要とするサービスに適用可能である。

【図面の簡単な説明】

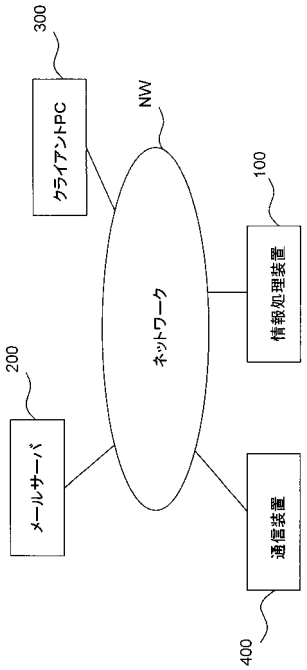
【００８９】

【図１】本実施形態の通信システムのシステム構成例を示す図である。

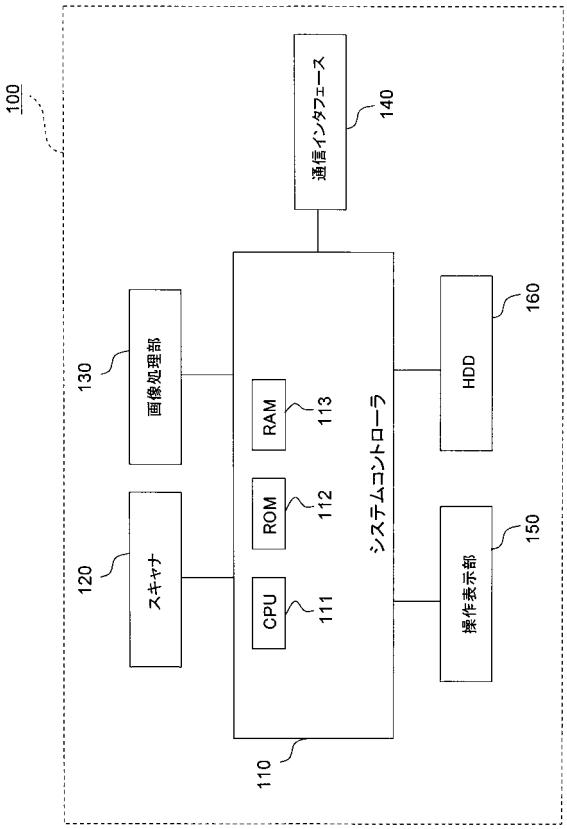
【図２】本実施形態の情報処理装置100のハードウェア構成例を示す図である。

【図３】本実施形態の情報処理装置100の機能構成例を示す図である。
【図４】本実施形態のスキャナ部101の処理動作例を示す図である。
【図５】本実施形態の囮データ生成部103の処理動作例を示す図である。
【図６】本実施形態の囮サーバ部104の処理動作例を示す図である。
【図７】本実施形態の囮サーバ部104の処理動作例を示す図である。
【符号の説明】
【００９０】
１００　情報処理装置
２００　メールサーバ
３００　通信装置
１０１　作業量取得部
１１０　コントローラ
１１１　CPU
１１２　ROM
１１３　RAM
１２０　スキャナ
１３０　画像処理部
１４０　通信インタフェース
１５０　操作表示部
１６０　HDD
１０１　スキャナ部（送信手段）
１０２　記憶部
１０３　囮データ生成部
１０４　囮サーバ部
１０５　時計部

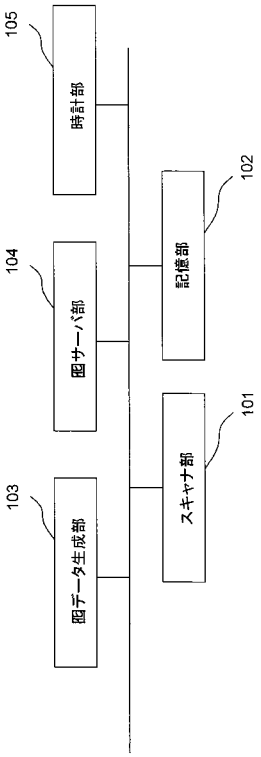
【図１】



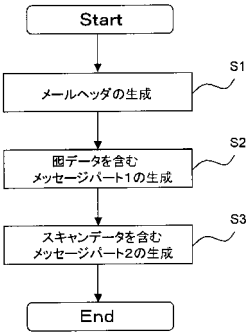
【図２】



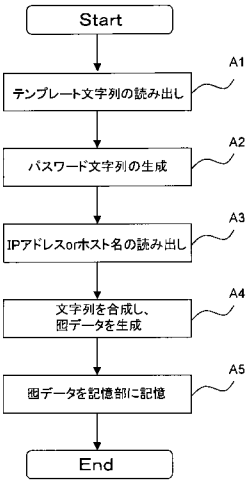
【図３】


105
時計部
104
画サーバ部
103
画データ生成部
102
記憶部
101
スキャナ部

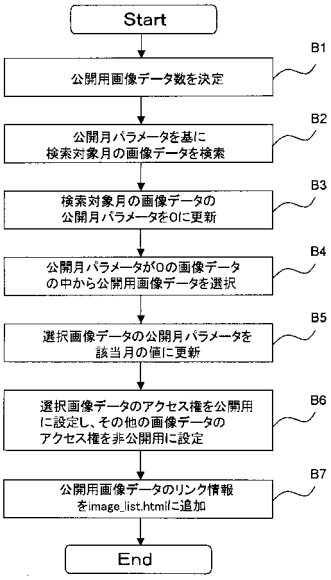
【図４】


Start
メールヘッダの生成
S1
画データを含む
メッセージパート1の生成
S2
スキャンデータを含む
メッセージパート2の生成
S3
End

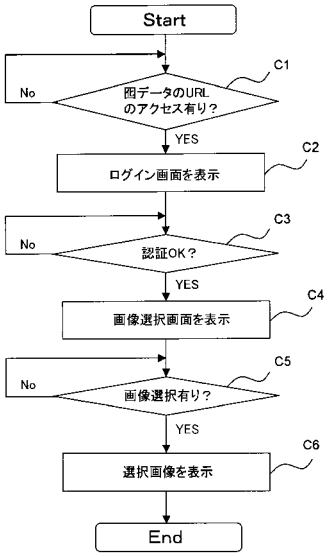
【図５】


Start
テンプレート文字列の読み出し
A1
パスワード文字列の生成
A2
IPアドレスorホスト名の読み出し
A3
文字列を合成し、
画データを生成
A4
画データを記憶部に記憶
A5
End

【図６】


Start
公開用画像データ数を決定
B1
公開月パラメータを基に
検索対象月の画像データを検索
B2
検索対象月の画像データの
公開月パラメータを0に更新
B3
公開月パラメータが0の画像データ
の中から公開用画像データを選択
B4
選択画像データの公開月パラメータを
該当月の値に更新
B5
選択画像データのアクセス権を公開用
に設定し、その他の画像データの
アクセス権を非公開用に設定
B6
公開用画像データのリンク情報
をimage_list.htmlに追加
B7
End

【図７】


Start
C1
No
画データのURL
のアクセス有り？
YES
C2
ログイン画面を表示
C3
No
認証OK？
YES
C4
画像選択画面を表示
C5
No
画像選択有り？
YES
C6
選択画像を表示
End