(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2008-312156
(P2008-312156A)
(43)公開日　平成20年12月25日(2008.12.25)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601A	5B017
G06F 21/24	(2006.01)	G06F	12/14	540A	5J104
		G06F	12/14	540P	
		H04L	9/00	601E	

審査請求 未請求　請求項の数 8　OL　（全 18 頁）

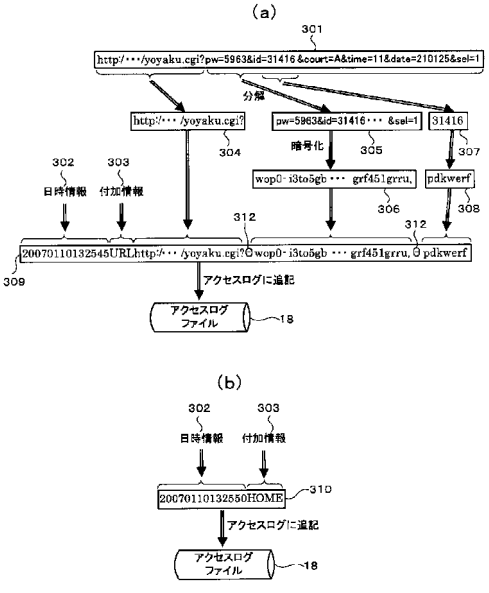
(21)出願番号　特願2007-160509 (P2007-160509)
(22)出願日　平成19年6月18日 (2007.6.18)

(71)出願人　000153443
株式会社日立情報制御ソリューションズ
茨城県日立市大みか町５丁目２番１号
(74)代理人　100122884
弁理士　角田　芳末
(72)発明者　山田　洋一
茨城県日立市大みか町五丁目２番１号　株式会社日立情報制御ソリューションズ内
(72)発明者　白土　雅之
茨城県日立市大みか町五丁目２番１号　株式会社日立情報制御ソリューションズ内

Ｆターム(参考)　5B017 AA03　BA07　CA16
5J104 AA16　EA04　EA19　PA14

(54)【発明の名称】情報処理装置、暗号化処理方法及び暗号化処理プログラム

(57)【要約】
【課題】ログファイルの流出に備えて、復号困難な暗号化を行うとともに暗号化処理時間を短縮する。
【解決手段】アクセスログファイル１８に記録する情報３０１を、一般的なＵＲＬの書式の区切り文字３１２を利用して、自動的に機密情報３０４と非機密情報３０５に分解する。そして、非機密情報３０４は平文で記録し、機密情報３０５は暗号化して記録することで、暗号化演算を行うデータ量を減少させて高速化を図る。さらに、アクセスログの生成時に共通暗号鍵方式の鍵を生成し、共通暗号鍵方式の鍵を公開鍵暗号方式により暗号化（以下、第一の暗号化方式）する。これにより、暗号化した機密情報３０４の復号が困難となり、アクセスログファイル１８を保存したハードディスクなどの不揮発性記憶装置の盗難の際にも暗号化に使用する鍵が容易に判明することがない。
【選択図】図３



アクセスログの暗号化手順例

【特許請求の範囲】
【請求項１】
当該情報処理装置で生成される任意の文字列よりなるログ情報を所定の規則に従って非機密情報と第一機密情報に分解する文字列分解部と、
前記ログ情報を分解して得られた第一機密情報を第一暗号化方式で暗号化処理する第一暗号化部と、
時計部と、
該時計部から供給される日時情報と、前記ログ情報を分解して得られた非機密情報及び前記暗号化処理された第一機密情報を、所定の規則に従い合成して記録用文字列情報を生成する記録用合成部と、
前記記録用合成部で生成された記録用文字列情報を、前記第一暗号化方式で用いられる第一暗号化鍵を所定の公開鍵を用いて暗号化処理した復号用鍵とともにログファイルに記憶する不揮発性記憶部と、を備えることを特徴とする情報処理装置。
【請求項２】
請求項１に記載の情報処理装置において、
ユーザの操作内容を検知し、表示装置の画面に表示する画像を生成するとともにユーザの操作内容に応じたログ情報を生成する表示処理部を備え、
前記文字列分解部は、前記表示処理部から前記ログ情報を入手し、前記ログ情報を所定の規則により非機密情報と第一機密情報に分解する、ことを特徴とする情報処理装置。
【請求項３】
請求項１に記載の情報処理装置において、
前記文字列分解部は、前記ログ情報を構成する文字列に含まれる所定の文字もしくは所定の文字列を基準にして前記ログ情報を構成する文字列の分割を行う、ことを特徴とする情報処理装置。
【請求項４】
請求項１に記載の情報処理装置において、
第二暗号化方式による暗号化処理を行う第二暗号化部をさらに備え、
前記文字列分解部は前記ログ情報を分解して得た前記第一機密情報をさらに分解して第二機密情報を抽出し、前記第二暗号化部は前記第二機密情報を第二暗号化方式で暗号化処理し、暗号化処理前の文字列と異なる文字列であって前記暗号化処理前の文字列と一対一に対応する文字列に変換する、ことを特徴とする情報処理装置。
【請求項５】
請求項４に記載の情報処理装置において、
前記不揮発性記憶部は、第二暗号化部による暗号化処理の対象となる暗号化項目が登録された暗号化項目指定テーブルを記憶しており、
前記文字列分解部は、前記暗号化項目指定テーブルに登録された暗号化項目と合致する文字列を前記第一機密情報から抽出し、前記第二暗号化部は前記第一機密情報から抽出した前記文字列を第二暗号化方式で暗号化処理する、ことを特徴とする情報処理装置。
【請求項６】
請求項４に記載の情報処理装置において、
前記第一暗号化部による暗号化処理に用いられる第一暗号化鍵、及び、第二暗号化部による暗号化処理に用いられる第二暗号化鍵を、揮発性記憶部に一時記憶する、ことを特徴とする情報処理装置。
【請求項７】
文字列からなるログ情報を所定の規則に従って非機密情報と第一機密情報に分解するステップと、
前記ログ情報を分解して得られた第一機密情報を第一暗号化方式で暗号化処理するステップと、
日時情報と、前記ログ情報を分解して得られた非機密情報及び前記暗号化処理された第一機密情報とを、所定の規則に従い合成して記録用文字列情報を生成するステップと、

前記第一暗号化方式で用いられる第一暗号化鍵を公開鍵方式で暗号化処理して復号用鍵を生成するステップと、
前記記録用文字列情報と前記復号用鍵を記録したログファイルを生成し、不揮発性記憶部に記憶するステップと、を含むことを特徴とするログ情報の暗号化処理方法。
【請求項８】
文字列からなるログ情報を所定の規則に従って非機密情報と第一機密情報に分解する手順と、
前記ログ情報を分解して得られた第一機密情報を第一暗号化方式で暗号化処理する手順と、
日時情報と、前記ログ情報を分解して得られた非機密情報及び前記暗号化処理された第一機密情報を、所定の規則に従い合成して記録用文字列情報を生成する手順と、
前記第一暗号化方式で用いられる第一暗号化鍵を公開鍵方式で暗号化処理して復号用鍵を生成する手順と、
前記記録用文字列情報と前記復号用鍵を記録したログファイルを生成し、不揮発性記憶部に記憶する手順を、コンピュータに実行させることを特徴とするログ情報の暗号化処理プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、例えば、公衆への情報提供、公共施設の予約、飛行機の搭乗券等チケット類の予約及び発券、その他の取引等を行う際に、端末装置が取得するユーザの個人情報等の機密情報を管理するのに好適な情報処理装置、暗号化処理方法及び暗号化処理プログラムに関する。
【背景技術】
【０００２】
従来、パーソナルコンピュータ等の端末装置に組み込まれたＷＥＢ（World Wide Web）ブラウザは、ユーザの操作に応じて所望の画面を表示装置に表示することができる。ＷＥＢブラウザは、例えばＨＴＭＬ（Hyper Text Markup Language）又はＨＴＭＬ内に組み込んだＪａｖａＳｃｒｉｐｔ（登録商標）、あるいはその他の言語によって記述された不特定のアプリケーションプログラムを実行して画面に表示する。このＷＥＢブラウザによって表示された画面上には、上記アプリケーションプログラム中の記述により指定され、ユーザが選択したＷＥＢページへ移動するためのリンクボタンが設けられている。また上記ＷＥＢブラウザには、例えば、ＷＥＢブラウザが現在表示しているページの１つ前のページへ戻る「戻る」ボタンなどの機能ボタンが設けられている。端末装置の利用者は、これらのリンクボタンあるいは機能ボタンを操作することにより、ＷＥＢブラウザを利用して、公衆への情報提供、公共施設の予約、飛行機の搭乗券等チケット類の予約及び発券、その他各種取引等のサービスの提供を受けることができる。
【０００３】
一般に端末装置は、アプリケーション画面上の利用者の操作による不特定のＵＲＬ（Uniform Resource Locator ）へのアクセス履歴、利用者の機能ボタンの操作内容を取得し、この取得した情報をその日時とともにハードディスクその他の不揮発性記憶装置上のアクセスログファイルに保存する機能を有する。このアクセスログファイルの他に、ログ情報として保存される内容としては、利用者が近づいたか否かを検出する人感センサの状態、カードリーダの操作の記録などがある。
【０００４】
アクセスログファイルのログ情報はさまざまな調査目的で用いられる。主なところでは、例えば端末装置の不調が発生した場合の原因調査、端末装置の利用頻度の統計調査、コンテンツの利用頻度の統計調査などが挙げられる。しかし、アクセスログファイルの中には利用者の氏名、住所、性別、年齢、誕生日、電話番号、クレジットカード番号などの個人情報や、取引の金額、その他の機密情報も含まれることがある。そのため、アクセスロ

グファイルを格納したハードディスク等の不揮発性記憶装置の盗難、通信回線を介した不正アクセスによるアクセスログファイルの盗難等によって、アクセスログファイルが流出した際には大きな不利益を被る可能性がある。

【０００５】

ところで、端末装置の不調の原因を調査する等の目的で、調査担当者がアクセスログを使用する場合、上記機密情報は必要とされない。そのため、機密情報が含まれるアクセスログファイルにアクセスできる権限者が、調査担当者にアクセスログファイルを渡す場合、アクセスログファイルから機密情報に関する部分を削除した調査用のアクセスログファイルを作成して渡す方法が取られていた。また、端末装置の利用者を特定するために上記機密情報の一部が必要である場合には、機密情報が特定されないように、上記権限者が機密情報部分を他のコードに置き換えた調査用のアクセスログファイルを作成して渡す方法などが用いられていた。これらの方法では、権限者が端末装置のアクセスログファイルから調査用のアクセスログファイルを作成する必要がある。

【０００６】

上述した技術の他にも、アクセスログファイルの不正利用を防止する技術として、特許文献１～４に記載されているようなものがある。

【０００７】

特許文献１には、機密文書管理技術に関する発明が開示されている。特許文献１に記載の機密文書管理技術は、サーバ上に機密文書ファイルを暗号化して保管しておき、編集作業はクライアント装置に読み出して行う。つまり、暗号化したファイルを編集する際には、クライアント装置側で目的の機密文書ファイルをサーバから取得して復号し、復号した機密文書ファイル（一時ファイル）をクライアント装置側で編集する。そして、編集が終了したら一時ファイルを再度暗号化してサーバに保管し直す。この機密文書管理技術を使用すると、ハードディスク等の不揮発性記憶装置の盗難や通信回線を介した不正アクセスによるアクセスログファイルの盗難にあった場合、機密文書ファイル内のデータの読み取り防止に有効である。

【０００８】

また、特許文献２には、サーバ上のファイルもクライアント上のファイルも平文であるが、通信路上の機器で対象ファイルを暗号化して相手側に伝送する技術が開示されている。

【０００９】

また、特許文献３には、サーバ上の暗号化したアクセスログファイルを、他の画像データ等のファイルに秘匿するステガノグラフィ(Steganography)技術を応用して、アクセスログファイルの存在自体を秘密にする技術が開示されている。

【００１０】

また、特許文献４には、機密データに対して機密度レベルを設定して、機密度レベルが最低の機密データは平文で記録し、かつ、機密度レベルによって暗号化鍵を使い分けて暗号化する技術が開示されている。

【００１１】

このように、暗号化技術を用いたさまざま機密文書管理技術が提案されている。この暗号化技術には主に二つの方法がある。一つは、暗号化処理と復号処理に同一の鍵を用いる共通鍵暗号方式である。もう一つは、暗号化処理と復号処理にそれぞれ異なる鍵を用いる公開鍵暗号方式であり、この公開鍵暗号方式は、一方の鍵（公開鍵）が公開されても危険の少ないことが特徴とされている。

【００１２】

後者の公開鍵暗号方式はさらに複数の方式が存在し、代表的なものにＲＳＡ（Rivest Shamir Adleman）暗号方式がある。しかし、公開鍵暗号方式は、一般に暗号化処理に時間がかかるため、電子計算機による処理ではしばしば専用のハードウェアを用いる場合もある。一方、前者の共通鍵暗号方式はＤＥＳ（Data Encryption Standard）暗号に代表される方式である。電子計算機による処理に適したアルゴリズムが工夫されたことに伴い、公

開鍵暗号方式に比べて暗号化処理時間が少なくなっている。それでも相当の演算量が必要であり、暗号化処理に時間がかかるという問題は残る。

【００１３】

そこで、電子文書やファイルの暗号化には比較的処理時間の少ない共通鍵暗号方式を使用し、その共通鍵の暗号化にのみ公開鍵暗号を使用する手法（ハイブリッド暗号方式）が提案されている。例えば、非特許文献１及び非特許文献２に、経済産業省より電子政府向けに推奨されている暗号リストが公表されている。一例として、共通鍵の暗号化には公開鍵暗号である非特許文献５及び非特許文献６に記載のブロック暗号を用い、電子文書及びファイルの暗号化には非特許文献４に記載のストリーム暗号を用いることを推奨し、さらに、暗号化処理に必要となる擬似乱数の発生には非特許文献３に記載の擬似乱数発生アルゴリズムを推奨している。

【００１４】

【特許文献１】特開２００６－２６０１７６号公報
【特許文献２】特開２００５－３２２２０１号公報
【特許文献３】特開２００６－２５２０３３号公報
【特許文献４】特許第２８８７２９９号明細書
【非特許文献１】「電子政府推奨暗号リスト」，経済産業省，２００３年
【非特許文献２】「各府省の情報システム調達における暗号の利用方針」，経済産業省，２００２年２月２８日
【非特許文献３】「疑似乱数生成器ＭＵＧＩ 仕様書Ver. 1.3」，株式会社日立製作所，２００２年５月８日
【非特許文献４】「ＭＵＬＴＩ－Ｓ０１暗号仕様書第１．２版」，株式会社日立製作所，２００２年５月１２日
【非特許文献５】「１２８ビットブロック暗号Ｃａｍｌｌｉａアルゴリズム仕様書 第２．０版」，日本電信電話株式会社，三菱電機株式会社，２００１年９月２１日
【非特許文献６】「Federal Information Processing Standards Publication 197」 November 26, 2001 Announcing the ADVANCED ENCRYPTION STANDARD (AES)

【発明の開示】

【発明が解決しようとする課題】

【００１５】

ところで、権限者が端末装置のアクセスログファイルから調査用のアクセスログファイルを作成するという従来の保存管理では、端末装置内のアクセスログファイルを保持した不揮発性記憶装置の盗難またはアクセスログファイルへの不正アクセス等によりアクセスログファイルが流出するという問題点があった。さらに、端末装置の不調の原因調査などの際、担当者の故意または過失により機密情報が漏洩してしまうという可能性もあった。さらに、権限者が端末装置のアクセスログファイルから調査用のアクセスログファイルを作成するという作業が必要となるので煩わしかった。

【００１６】

また、特許文献１に記載された技術は、その都度、サーバに保存された機密文書ファイルをクライアント装置側で復号し、編集後に再度暗号化してサーバに戻すので、アクセスログのように逐次追記していく用途では、時間がかかってしまい実用的でないという問題があった。また、端末装置がサーバに接続されない使用形態の場合には上記方法は適用不可能であった。

【００１７】

また、特許文献２に記載された技術は、アクセスログファイルを格納した記録媒体の盗難について考慮されていない。さらに、端末装置がサーバに接続されない使用形態には適用不可能であった。

【００１８】

また、特許文献３に記載された技術は、アクセスログファイルを格納した不揮発性記憶装置の盗難の際の読み取り防止に対しては有効である。しかし、アクセスログファイルの

容量は使用目的によって大きく異なり、数百ＭＢから数ＧＢにまで達することがある。アクセスログファイルの秘匿先が画像データ等のファイルの場合、さらに数百倍の容量が必要となる。つまり、上記アクセルログファイルは、最終的に数ＴＢもの巨大なファイルとなってしまい、実用性に問題があった。

【００１９】

また、特許文献４に記載された技術は、予め機密データ毎に機密度レベルを設定するか、または、機密データの原文中に空白などの区切り符号を挿入しておく必要がある。そのため、この技術は、不特定多数のアプリケーションプログラムを対象とする街頭に設置された端末装置には適用できなかった。

【００２０】

さらに、現在知られている暗号化処理方法は、いずれの暗号方式も、ファイル全体を暗号化及び復号するので、ある程度の計算量が必要である。そのため、莫大な処理時間が必要となる。さらに、暗号化対象ファイルの撹乱またはパディングを実現するために乱数を挿入する必要があり、それによって暗号化後のデータ長が元のデータ長よりも長くなるという欠点があった。

【００２１】

本発明は上記課題を解決するためになされたものであり、街頭等に設置した端末装置内のログファイルを保持した不揮発性記憶装置の盗難またはログファイルへの不正アクセス等により、ログファイルが流出する事態に備えてログファイルに対して復号困難な暗号化を行い、かつ、暗号化に要する時間を短縮することを目的とする。

【００２２】

さらに、調査担当者の故意または過失により記録媒体に記録した機密情報の漏洩を回避するため、その実データ（機密情報部分）を公表せずに、暗号化された後のデータが復号困難で、かつその暗号化された後のデータにおいてもデータの識別ができるようにすることを目的とする。

【課題を解決するための手段】

【００２３】

上記課題を解決し、本発明の目的を達成するため、本発明の第１の側面は、文字列からなるログ情報を暗号化処理する際、まず文字列からなるログ情報を所定の規則に従って非機密情報と第一機密情報に分解し、ログ情報を分解して得られた第一機密情報を第一暗号化方式で暗号化処理する。次に日時情報と、ログ情報を分解して得られた非機密情報及び暗号化処理された第一機密情報とを、所定の規則に従い合成して記録用文字列情報を生成する。そして、第一暗号化方式で用いられる第一暗号化鍵を公開鍵方式で暗号化処理して復号用鍵を生成し、複数の記録用文字列情報と復号用鍵を記録したログファイルを生成して不揮発性記憶部に記憶することを特徴とする。

【００２４】

また、本発明の第２の側面は、上記ログ情報を分解して得た上記第一機密情報をさらに分解して第二機密情報を抽出し、この第二機密情報を第二暗号化方式で暗号化処理する。そして、暗号化処理前の文字列と異なる文字列であって暗号化処理前の文字列と一対一に対応する文字列に変換することを特徴とする。

【発明の効果】

【００２５】

本発明によれば、ログファイルを格納した不揮発性記憶装置の盗難や、通信回線を介した不正アクセスによるログファイルの盗難等によりログファイルが第三者に流出した場合でも、ログファイル内の機密情報の漏洩を防止できる。また、記録媒体に記録した機密情報の、調査担当者の故意または過失による漏洩を防止できる。

【００２６】

また、ログファイル内の機密情報のみを暗号化するので、暗号化に要する時間を短縮できる。さらに、ログファイル内の識別情報については暗号化処理後も識別可能となるように暗号化処理を行うので、ログファイルの調査等において機密情報を開示することなくデ

ータを容易に識別することができる。

【発明を実施するための最良の形態】

【００２７】

以下、図１～図７を参照して、本発明の実施の形態の例について説明する。本実施形態に係る情報処理装置は、公衆への情報提供、公共施設の予約、飛行機の搭乗券その他チケット類の予約及び発券、その他の取引等を行うことを目的として、例えば街頭や店舗に設置される端末装置に適用した例としてある。この端末装置は、ユーザによるアクセスや操作が行われたこと等を検出して、機密情報と非機密情報が混合したログ情報を随時生成する。そして、各ログ情報を機密情報と非機密情報に分解し、非機密情報は平文で記録し、機密情報を暗号化して記録することにより、安全かつ無駄のないログ情報の暗号化処理を実現する。

【００２８】

図１は、本発明の一実施形態に係る端末装置の全体構成図である。図１に示すように、本実施形態に係る端末装置１００は主に、情報処理装置２と、揮発性記憶装置１２と、不揮発性記憶装置１５と、時計２２を備え、例えばインターネットよりなるネットワーク（電気通信回線）を介してサーバ１１と通信可能に接続されている。また、端末装置１００にはディスプレイ２０及びタッチパネル２１が接続されている。本実施形態に係る端末装置１００（情報処理装置２）としては、例えば表示装置と接続されたパーソナルコンピュータ等を利用することができる。

【００２９】

なお、本実施形態では、情報処理装置２と揮発性記憶装置１２、不揮発性記憶装置１５及び時計２２が別個の構成となっているが、それらの一部または全部を情報処理装置２の内部に設けるようにしてもよい。例えば、情報処理装置２内に揮発性記憶装置１２、不揮発性記憶装置１５及び時計２２を格納して一体構成としてもよい。

【００３０】

端末装置１００は、ユーザのタッチパネル２１に対する操作内容に基づいたアプリケーションソフトウェア（以下、「アプリケーション」という。）をサーバ１１から取得し、ディスプレイ２０にアプリケーションのウィンドウ（所定形状の表示領域）を表示させる。そして、端末装置１００は、サーバ１１へのアクセス履歴や操作履歴等のログ情報を揮発性記憶装置１２に記憶されている鍵を用いて暗号化し、不揮発性記憶装置１５のアクセスログファイル１８に書き込む。

【００３１】

なお、本実施形態では、ログ情報としてアクセスログを例に挙げたが、端末装置１００のアクセスログ（ユーザによるアクセス履歴や操作履歴等）に限らず、端末装置１００の動作全般の履歴をログ情報として取得することができる。

【００３２】

次に、端末装置１００の構成要素の一つである情報処理装置２について説明する。情報処理装置２は、例えばＣＰＵ（Central Processing Unit）からなる制御部（図示略）を備え、この制御部の制御の下、暗号化処理機能を持つＷＥＢブラウザ１を動作させている。このＷＥＢブラウザ１は、ＨＴＭＬ表示・処理部３と、機能ボタン表示・処理部４と、ＵＲＬ文字列分解部５と、共通鍵方式暗号化部６と、一方向暗号化部７と、記録用合成部８ａ，８ｂと、鍵編成部９と、公開鍵暗号化部１０の機能を備えている。ＷＥＢブラウザ１のプログラムは、情報処理装置２内のＲＯＭ（図示略）、あるいは不揮発性記憶装置１５に記録しておいてもよい。

【００３３】

また、ＨＴＭＬ表示・処理部３は、機能ボタン表示・処理部４とともに表示処理部（ログ情報生成手段）を構成する。このＨＴＭＬ表示・処理部３は、タッチパネル２１の操作内容に基づいて、サーバ１１よりＨＴＭＬで記述されたアプリケーションを取得し、前記アプリケーションを処理して、アプリケーションウィンドウをディスプレイ２０に表示させる。

【００３４】
また、機能ボタン表示・処理部４は、ディスプレイ２０に機能ボタンを表示し、タッチパネル２１よりなされた機能ボタン操作に基づいた情報を前述ＨＴＭＬ表示・処理部３に送信する。
【００３５】
また、ＵＲＬ文字列分解部５は、上記ＨＴＭＬ表示・処理部３より非機密情報と機密情報が混合したＵＲＬ文字列が入力された際、その文字列を非機密情報部分、機密情報部分に分解するとともに、機密情報部分の中の一部を抽出する。そして、このＵＲＬ文字列分解部５は分解された非機密情報部分を記録用合成部８ａに出力するとともに、機密情報部分及び該機密情報部の中の一部をそれぞれ記録用合成部８ａ、共通鍵方式暗号化部６及び一方向暗号化部７へ出力する。
【００３６】
また、共通鍵方式暗号化部６は第一暗号化部の一例である。共通鍵方式暗号化部６は、上記ＵＲＬ文字列分解部５から入力された文字列に対し、揮発性記憶装置１２に記憶されている共通鍵１３を用い共通鍵暗号化方式で暗号化（第一の暗号化）を行い、暗号化した文字列を記録用合成部８ａに出力する。
【００３７】
また、一方向暗号化部７は第二暗号化部の一例である。一方向暗号化部７は、上記ＵＲＬ文字列分解部５から入力された文字列に対し、揮発性記憶装置１２に記憶されている一方向鍵１４を用い同一平文であれば同一暗号文に変換する暗号化（第二の暗号化）を行い、暗号化した文字列を記録用合成部８ａに出力する。ここでいう一方向暗号化とは、暗号化処理前と異なる文字列かつ暗号化処理前の文字列と一対一に対応する文字列に変換することをいう。一方向暗号化処理に使用した暗号鍵すなわち一方向鍵１４は破棄することで暗号化後の復号を困難にしてもよい。これにより、暗号化後の文字列を復号するのは極めて困難となるが、暗号化後の文字列から暗号化前の文字列を判別することができるようになる。
【００３８】
また、記録用合成部８ａ及び記録合成部８ｂは、入力された複数の文字列を所定の形式で合成を行う。記録合成部８ａは、ＵＲＬ文字列分解部５、共通鍵方式暗号化部６及び一方向暗号化部７から入力された文字列に、時計２２から出力された日時情報の文字列とＵＲＬ文字列分解部５から入力されるログ情報の内容を記号で簡単に表した付加情報を加えて合成する。一方、記録用合成部８ｂは、時計２２から出力された日時情報と機能ボタン表示・処理部４の操作内容である付加情報を合成する。記録用合成部８ａ及び記録合成部８ｂで生成された文字列（記録用文字列情報）はアクセスログファイル１８として不揮発性記憶装置１５に記録される。この記録用合成部８ａと記録用合成部８ｂは一体構成としてもよい。
【００３９】
鍵生成部９は、文字列の暗号化に用いる共通鍵１３及び一方向鍵１４を生成する。鍵生成後、この鍵生成部９は、公開鍵方式暗号化部１０に共通鍵のみ出力する。また、この鍵生成部９で生成された鍵は、揮発性記憶装置１２に記憶される。
【００４０】
公開鍵方式暗号化部１０は、不揮発性記憶装置１５から提供される暗号化用公開鍵１７を用いて、鍵生成部９から出力された共通鍵１３の暗号化を行う。ここで、暗号化された共通鍵１３はログファイルの所定位置に記録される。
【００４１】
揮発性記憶装置１２は、例えばＲＡＭ（Random Access Memory）で構成される。揮発性記憶装置１２は、鍵生成部９で生成された共通鍵１３及び一方向鍵１４を記憶している。共通鍵１３は、共通鍵方式暗号化部６の暗号化処理に使用される。また、一方向鍵１４は一方向暗号化部７の暗号化処理に使用される。
【００４２】

不揮発性記憶装置１５は、例えばＲＯＭ（Read Only Memory）で構成される。不揮発性記憶装置１５には、暗号化項目指定テーブル１６と、暗号化用公開鍵１７と、アクセスログファイル１８が記憶されている。暗号化項目指定テーブル１６には、一方向暗号化部７での暗号化対象となる文字列（暗号化項目）が登録されている。暗号化用公開鍵１７は、後述するように情報処理装置２で生成された鍵を暗号化するための公開鍵である。アクセスログファイル１８は、ログ情報の一例であり、端末装置へのアクセス履歴、操作履歴等である。

【００４３】

次に、実際のログ情報の取得処理について、施設予約アプリケーションの操作を例にとり説明する。図２はＷＥＢブラウザ１を使用した、施設予約アプリケーションによる画面遷移例を示すものである。表示画面はＨＴＭＬで記述されたアプリケーションのウィンドウと、ＷＥＢブラウザの機能ボタンから構成される。ＨＴＭＬで記述されたアプリケーションのウィンドウ上には、施設名、空き状況及び予約確認等の名称が付けられたいくつかのリンクボタンが配置される。

【００４４】

ここで、機能ボタンとは、ウィンドウ５０１下部の、「戻る」、「進む」、「最初」、「上へ」、「下へ」、「右へ」、「左へ」、「印刷」の各ボタンの総称である。また、アプリケーションのウィンドウとは、画面に表示された機能ボタン部分以外の表示領域を指す。なお、図２において、初期画面５０１の上方に示したＵＲＬ文字列３１６は当該初期画面５０１のＵＲＬに対応している。

【００４５】

例えば、公共施設予約の初期画面５０１上で、利用者がタッチパネル２１によりリンクボタン「テニスコート」を選択したとする。この際、端末装置１００のＨＴＭＬ表示・処理部３が、利用者の操作を検出してＵＲＬ文字列３１７にリンクされている「テニスコート希望日選択」のアプリケーションをサーバ１１に要求する。そして、端末装置１００は、サーバ１１から送信されるＨＴＭＬ等で記載された「テニスコート希望日選択」のアプリケーションを取得する。取得したアプリケーションは、ＨＴＭＬ表示・処理部３が取得したアプリケーションに基づいて、ディスプレイ２０に「テニスコート希望日」を選択する希望日選択画面５０２を表示させる。ここで、ＵＲＬ文字列３１７は、施設予約の初期画面５０１で操作が行われた結果、次に表示する画面５０２のＵＲＬ「yoyaku.cgi」に文字列「?」及び「テニスコート」を選択したことを示す文字列「sel=1」を加えた形となっている。

【００４６】

希望日選択画面５０２はテニスコートの予約希望日を選択するアプリケーションウィンドウの一例である。この希望日選択画面５０２では１月のカレンダーが記載されている。ここで利用者がタッチパネル２１により希望日２５日を選択したとする。すると、ＨＴＭＬ表示・処理部３は、ＵＲＬ文字列３１８にリンクされている「テニスコート１月２５日利用コート・時間帯」を選択する利用時間帯選択画面５０３を表示する。ここで、利用時間帯選択画面５０３の上方のＵＲＬ文字列３１８は、希望日選択画面５０２のＵＲＬ文字列３１７に「１月２５日」を選択したことを示す文字列「date=210125」を付加し、文字列「&」で区切った形となっている。

【００４７】

この利用時間帯選択画面５０３には、１月２５日におけるテニスコートの使用状況を示す表が表示されており、縦の項目（Ａ～Ｅ）がコートの種類、横の項目（７～１５）が時間帯を表している。この表において、テニスコートの予約が可能な場合「○」、予約が不可能な場合「×」というように表示されている。例えば、コートＡかつ利用時間帯１１時を選択したとする。そうすると、ＨＴＭＬ表示・処理部３及び機能ボタン表示・処理部４は、ＵＲＬ文字列３１９にリンクされている利用者ＩＤ入力画面５０４を表示する。ここで、ＵＲＬ文字列３１９は、利用時間帯選択画面５０３のＵＲＬ文字列３１８に「コートＡ・１１時」を選択したことを示す情報の文字列「court=A」及び「time=11」を付加し、

それぞれを文字列「&」で区切った形となっている。

【００４８】

利用者ＩＤ入力画面５０４において、利用者がタッチパネル２１により数字ボタンを操作して利用者ＩＤ、例えば「31416」を入力する。利用者ＩＤの入力後、ＨＴＭＬ表示処理部３及び機能ボタン表示・処理部４は、ＵＲＬ文字列３２０にリンクされているパスワード入力画面５０５を表示する。ここで、ＵＲＬ文字列３２０は、上記利用者ＩＤ入力画面５０４のＵＲＬ文字列３１９に、入力した利用者ＩＤを示す文字列「id=31416」を付加し、文字列「&」で区切った形となっている。

【００４９】

パスワード入力画面５０５において、利用者がタッチパネル２１により数字ボタンを操作してパスワード、例えば「5963」を入力する。パスワードの入力後、ＨＴＭＬ表示・処理部３及び機能ボタン表示・処理部４は上記と同様の処理を行い、ＵＲＬ文字列３０１にリンクされている予約結果確認画面５０６を表示する。ここで、ＵＲＬ文字列３０１は、パスワード入力画面５０５のＵＲＬ文字列３２０に入力したパスワードを示す文字列「pw=5963」を付加し、文字列「&」で区切った形となっている。予約結果確認画面５０６において最初ボタンを選択すると初期画面５０１に戻る。上述した各操作に対応する各ＵＲＬ文字列からなるログ情報について所定の暗号化処理を実施した後、不揮発性記憶装置１５のアクセスログファイル１８に記録する。

【００５０】

上記したＵＲＬ文字列３０１，３１７～３２０のように「××.cgi」を含むＵＲＬは、サーバ１１上に例えばＰｅｒｌと呼ばれるプログラミング言語で記載されたプログラムが保存されており、サーバ１１上でプログラムが実行される。情報処理装置２は、このプログラムの実行により生成されたＨＴＭＬで記載された画面データを受け取り、ディスプレイ２０にアプリケーションウィンドウを表示する。なお、ＵＲＬ文字列「××.cgi」の後の「?」以降の文字列は、そのプログラムに渡す引数にあたる。一般に、ＵＲＬ文字列「××.cgi」の部分は同じであり、引数で番号を指定することによって、異なるアプリケーションウィンドウを表示させたり、日付を指定して特定の月のカレンダーを表示したりする。

【００５１】

次に、情報処理装置２によるログ情報の暗号化処理について説明する。図３（a）に、アクセスログの暗号化処理の手順を示す。ここでは、図２に示した施設予約アプリケーションの予約結果確認画面５０６ＵＲＬ文字列３０１の暗号化処理を例に説明する。ＵＲＬ文字列３０１は、「http://・・・/yoyaku.cgi?&pw=5963&id=31416&court=A&time=11&date=210125&sel=1」となっており、「３１４１６」が利用者を特定するＩＤ（識別情報）を示し、「５９６３」がパスワード部分に相当する。利用者ＩＤ及びパスワードのいずれも機密情報である。

【００５２】

一般に、ＵＲＬはクエリー文字列と称する書式で書かれている。クエリー文字列においては、文字「？」の前までがＵＲＬの本体でサーバ上のファイルの指定を行う文字列を示し、文字「？」の後が引数を示す。引数は名称と値を文字「=」で結んだ項（文字列）を、文字「&」で区切って複数並べる方式が採られている。すなわち、ＵＲＬ文字列３０１内の文字「？」以降に機密情報があると判断できる。

【００５３】

そこで、ＵＲＬ文字列分解部５ではまず、ＵＲＬ文字列中の文字「？」以前の文字列を非機密情報３０４とみなし、文字「？」より後を第一の機密情報３０５とみなしてＵＲＬ文字列３０１の分解を行う。なお、文字「／」などの区切り符号と同一の文字列が複数回出現することが分かっている場合、何個目かの区切り符号の位置で分解処理してもよい。さらに、ＵＲＬの一般的な文法には無くとも、例えば文字列「yoyaku.cgi」等の任意の一文字以上の文字列を指定して、区切り符号として処理してもよい。つまり、ＵＲＬ文字列などのログ情報を構成する文字列に含まれる所定の文字もしくは所定の文字列を基準にし

て目的の文字列を分割する。

【００５４】

ＵＲＬ文字列３０１に第一の機密情報３０５の文字列が含まれる場合、共通鍵方式暗号化部６は揮発性記憶装置１２に記憶された共通鍵１３を用いて、共通鍵暗号方式（第一の暗号化方式）により第一の機密情報３０５を暗号化処理する。そして、共通鍵方式暗号化部６は暗号化した文字列よりなる情報３０６を、記録用合成部８ａに入力する。一方、非機密情報３０４の文字列は平文のまま記録用合成部８ａに入力する。

【００５５】

ここで、利用者ＩＤが調査等において利用者を識別するのに必要な情報である場合について説明する。その場合、利用者ＩＤの部分は、一方向暗号方式（第二の暗号方式）により暗号化することで、実データを秘匿したまま、利用者の識別のみできるようにする、一方向暗号化方式で暗号化処理を行うと、同一の平文であれば同じ文字列に変換してしまう。そのため、同一文字列で推定容易な文字列、例えば「pw=」や「time=」部分を、暗号化対象の範囲（文字列）に含めてしまうと、暗号解読の攻撃に弱くなる。したがって、一方向暗号化部７で暗号化する項目は必要最小限に限ることが望ましい。例えば、ＵＲＬ文字列３０１をさらに分解して、予め指定した項目のみ一方向暗号化方式により暗号化することで、仮に解読されたとしても情報漏洩の被害を最小限に止められる。

【００５６】

機密情報のうち予め指定した項目のみ一方向暗号化方式により暗号化する方法について、具体的に説明する。まず、予め文字「=」の左側にある文字列と比較する文字列を暗号化項目指定テーブル１６に登録して、不揮発性記憶装置１５に記憶しておく。

【００５７】

例えば、暗号化項目指定テーブル１６に、一方向暗号化部７での暗号化処理の対象となる項目（文字列）として、文字列「id」を登録しておいたとする。上記のように、予約結果確認画面５０６のＵＲＬ文字列３０１について、文字「&」を区切り符号とみなして分解すると、次の６つの文字列、「sel=1」、「date=210125」、「time=11」、「court=A」、「id=31416」、「pw=5963」、に分解される。ＵＲＬ文字列分解部５は、暗号化項目指定テーブル１６に登録された項目「id」とＵＲＬ文字列３０１中の「id」が合致すると判断して、文字列「id=31416」の右側の文字列「31416」を、第二の機密情報３０７として取り出す。そして、この第二の機密情報３０７を一方向暗号化部７で一方向暗号化処理し、暗号化された第二の機密情報３０８を記録用合成部８ａに入力する。

【００５８】

この第二の機密情報３０８は、暗号化処理前の文字列と異なる文字列であって暗号化処理前の文字列と一対一に対応する文字列となっている。それにより、暗号化後の文字列から暗号化前の文字列を判別できる。したがって、調査担当者は、特定の利用者ＩＤと他の利用者ＩＤの識別が可能になる。

【００５９】

情報処理装置２のＨＴＭＬ表示・処理部３は、ＵＲＬ文字列をサーバ１１へ送出した際、時計２２から日時情報を文字列として取得する。

【００６０】

ＵＲＬ文字列３０１の分解処理及びその後の暗号化処理と並行してまたは終了後、記録用合成部８ａは、日時情報３０２及び付加情報３０３を入手する。まず、記録用合成部８ａは、ＨＴＭＬ表示・処理部３がＵＲＬ文字列３０１に対応するアプリケーションをサーバ１１から取得したときの日時情報３０２を、時計２２から入手する。この日時情報３０２は、記録用合成部８ａが分解・暗号化された状態のＵＲＬ文字列を入手した日時でもよい。また、ログ情報生成手段を構成するＨＴＭＬ表示・処理部３からＵＬＲ文字列分解部５を介して、ログ情報の内容を表す付加情報３０３を入手する。この例では、ＷＥＢへのアクセス履歴であるから、付加情報３０３は「ＵＲＬ」となっている。

【００６１】

そして、記録用合成部８ａは、日時情報３０２、付加情報３０３、平文の非機密情報３

０４、暗号化された第一の機密情報３０６、暗号化された第二の機密情報３０８を一つに合成して記録用文字列３０９を作成する。このとき、それぞれの情報に対応する文字列の間に区切り符号３１２を付加して合成する。その後、記録用文字列３０９を、不揮発性記憶装置１５のアクセスログファイル１８に追記する。区切り符号３１２の例としては、例えばＡＳＣＩＩ文字コードのデリミタコードが用いられる。もし、デリミタコードと同一のデータ（文字）が存在する場合、デリミタコードを付加して識別するようにしてもよい。

【００６２】

ところで、例えばアプリケーションウィンドウ上の機能ボタンの操作によって生じるアクセスログは、日時情報３０２と付加情報３０３だけで構成され、ＵＲＬ文字列を持たない。例えば、図２の予約結果確認画面５０６で最初ボタンが選択された場合、図３（ｂ）に示すように機能ボタン表示・処理部４から付加情報３０３として「ＨＯＭＥ」という文字列と、時計２２からその操作が行われたときの日時情報３０２が記録用合成部８ｂに入力される。記録用合成部８ｂは、日時情報３０２と付加情報３０３のそれぞれの文字列を合成して一つの記録用文字列（レコード）３１０を作成して、アクセスログファイル１８に追記する。

【００６３】

図４は、テキスト形式で記述されたアクセスログファイル１８の一例である。アクセスログファイル１８の予め決められた所定の位置、例えば一行目に共通鍵方式暗号化部６で機密情報の暗号化に用いられた共通鍵１３記述されている。ただし、上述したように、共通鍵１３は、暗号化用公開鍵１７を用いて公開鍵方式暗号化部１０で暗号化されて、テキストデータとしてアクセルログファイル１８に記述される。２行目には、記録用合成部８ａで生成された記録用文字列３０９が記述されている。また、三行目には、機能ボタン操作をした際に生成される日時情報３０２と付加情報３０３を合成した記録用文字列３１０が記述される。

【００６４】

なお、図４に示すアクセルログファイル１８の例では、記録用文字列３０９，３１０のみ記述されているが、実際には各ログ情報に対応する記録用文字列が、ログ情報の取得順（日時順）などの所定順で記述される。例えば、図２に示すアプリケーション操作の例でいうと、ＵＲＬ文字列３１６～３２０，３０１がユーザ操作の順番にアクセスログファイル１８に記述されていく。

【００６５】

次に、本実施形態の端末装置１００によって暗号化されたアクセスログファイル１８を閲覧する閲覧装置について説明する。図５は本発明の暗号化処理によって暗号化されたアクセスログファイル１８を閲覧する閲覧装置２００の構成例である。この閲覧装置２００は、一例として閲覧処理装置２３と、揮発性記憶装置２１２と、不揮発性記憶装置２１５と、ディスプレイ２２０から構成することができる。ここでは、閲覧装置２００に、アクセスログファイル１８が保存されたリムーバブルメディア１９が、図示しないインターフェースを介して閲覧装置２００に接続されている。本実施形態に係る閲覧装置２００としては、例えば表示装置を備えたパーソナルコンピュータ等の端末装置を利用することができる。

【００６６】

閲覧装置２００の本体部分を構成する閲覧処理装置２３は、ログ切り出し部２４と、共通鍵方式復号部２５と、合成部２６と、公開鍵方式復号部２７から構成される。なお、閲覧処理装置２３をコンピュータシステムにより構成するものとして各部の機能をプログラム言語で記述したソフトウェアで実現してもよいし、専用の装置により構成するものとして各部の機能をハードウェアで実現するようにしてもよい。ソフトウェアのプログラムは、閲覧処理装置２３内のＲＯＭ（図示略）、あるいは不揮発性記憶装置２１５に記録しておいてもよい。

【００６７】

公開鍵方式復号部２７は、リムーバブルメディア１９にコピーして持ち運んだアクセスログファイル１８の所定位置（図４の例では１行目）に暗号化して記録された共通鍵１３を不揮発性記憶装置２１５に記憶されている復号用秘密鍵２８を用いて復号し、共通鍵１３を生成する機能を有する。

【００６８】

ログ切り出し部２４はアクセスログファイル１８の第二レコード（２行目）以降に記録されているアクセスログのレコード（文字列）を平文の非機密情報と暗号化された機密情報とに分解し、平文の非機密情報は合成部２６に、暗号化された機密情報は、共通鍵方式復号部２５に送信する機能を備えている。

【００６９】

共通鍵方式復号部２５は、共通鍵１３を用いて暗号化された機密情報の復号を行い、復号された機密情報を合成部２６へ送る機能を有している。

【００７０】

合成部２６は、ログ切り出し部２４で切り出して得られた平文の非機密情報と、共通鍵方式復号部２５で復号された機密情報を適宜合成し、ディスプレイ２２０に送信する機能を備えている。

【００７１】

図６は、本発明の暗号化方式で暗号化したアクセスログの復号手順を示す図である。この図６に示すアクセスログの復号手順について、図５を参照して説明する。まず、閲覧処理装置２３は、アクセスログファイル１８から復号するアクセスログ（記録用文字列）３０９を１レコードずつ取り出し、ログ切り出し部２４に送る。次に、ログ切り出し部２４では、区切り符号３１２を利用し、アクセスログ（記録用文字列）３０９を平文の非機密情報３１３，３０４と、第一の暗号化方式で暗号化された機密情報３０６と、第二の暗号化方式で暗号化された機密情報３０８に分解する。

【００７２】

ここで、ログ切り出し部２４は、非機密情報３１３，３０４を合成部２６に送るとともに、第一の暗号化方式で暗号化された機密情報３０６を共通鍵方式復号部２７へ送る。一方、第二の暗号化方式で暗号化された機密情報３０８は、本実施形態では第一の暗号化方式で暗号化された機密情報３０６の中に重複して含まれる情報なので読み捨てる。すなわち削除する。

【００７３】

そして、共通鍵方式復号部２５では、第一の暗号化方式で暗号化された機密情報３０６を、共通鍵１３を用いて平文の機密情報３０５に復号し、合成部２６に送る。最後に、合成部２６は、非機密情報３１３，３０４及び復号した機密情報３０５を合成して、記録用文字列３０９を暗号化前のＵＲＬ文字列３０１を作成し、ディスプレイ２２０に表示する。これにより、調査担当者等が暗号化されていたアクセスログをディスプレイ２２０で閲覧することができる。

【００７４】

図７は、機能ボタン操作により作成されたアクセスログを復号する手順を示す。まず、アクセスログファイル１８に記録された、機能ボタン操作によるアクセスログ（ＵＲＬ文字列）３０１をログ切り出し部２４に入力する。ログ切り出し部２４は、機能ボタン操作のアクセスログ３１０が暗号化された情報を持たないので、合成部２６に送る。そして、合成部２６は入力された機能ボタン操作のアクセスログ３１０をそのままディスプレイ２２０に出力し、画面に表示する。

【００７５】

図８、は本発明によって暗号化されたアクセスログファイルの非機密情報と一方向暗号化された機密情報部分のみを閲覧するための閲覧装置の構成例である。この例では、一方向暗号化された機密情報部分を復号する必要がない。そのため閲覧装置２１０は、図５に示す閲覧装置２００から、鍵を保存する揮発性記憶装置２１２及び不揮発性記憶装置２１５、復号を行う共通鍵方式復号部２５及び公開鍵方式復号部２７を除いた構成となってい

る。

【００７６】

図９は、本発明の暗号化方式で暗号化したアクセスログの機密情報を秘匿した読み出し手順を示す図である。この図９のアクセスログの読み出し手順について、図８を参照して説明する。このような読み出し手順を行う際、閲覧処理装置２３は、アクセスログファイル１８からアクセスログ（記録用文字列）を１レコード（１行）ずつ取り出し、閲覧処理装置２３のログ切り出し部２４に送る。そして、ログ切り出し部２４では、区切り符号３１２を利用し、取り出したアクセスログ（記録用文字列）３０９を平文の非機密情報３１３，３０４と、第一の暗号化方式で暗号化された機密情報３０６、及び第二の暗号化方式で暗号化された機密情報３０８に分解する。

【００７７】

そして、ログ切り出し部２４は、非機密情報３１３，３０４を合成部２６に送るとともに、機密情報３０８を合成部２６へ送る。機密情報３０６の部分は読み捨てる。合成部２６では、平文の非機密情報３１３，３０４と第二の暗号化方式で暗号化された機密情報３０８を合成して、ＵＲＬ文字列３１１を作成し、ディスプレイ２２０に出力する。これにより、調査担当者等が暗号化されていたアクセスログをディスプレイ２２０で閲覧することができる。

【００７８】

合成部２６で合成したＵＲＬ文字列３１１がディスプレイ２２０に表示できる文字コードでないコード（文字、記号等）を含む場合は、１６進数を表す文字コードに変換して表示するなどの処理を行ってから表示すればよい。なお、本実施形態ではアクセスログをディスプレイ２２０に表示して調査担当者が閲覧する例としたので、ディスプレイ２２０に表示できないコードを１６進数を表す文字コードに変換する処理が必要になる場合がある。しかし、他のアプリケーションソフトウェアの入力用にその文字コードを使用する場合などには当業者が、適宜にコードの変換を実施すればよい。

【００７９】

上記構成の閲覧装置２１０によれば、機密情報３０６が含まれないＵＲＬ文字列３１１（図９参照）は元のＵＲＬ文字列３０１（図３参照）の情報の全てを持ってはいないが、障害の原因解析などの特定の用途に対しては有用な情報となる。

【００８０】

なお、閲覧装置２１０は、図５に示した閲覧装置２００の共通鍵方式復号部２５がログ切り出し部２４から送られる機密情報に施された暗号化方式に応じて、合成部２６に出力する機密情報を切り換えるようにした構成としてもよい。

【００８１】

上述した本発明の実施形態によれば、アクセスログファイル１８に記録する情報（例えば、ＵＲＬ文字列）を、一般的なＵＲＬの書式の区切り文字を利用して、自動的に機密情報３０５と非機密情報３０４に分解する。そして、非機密情報３０４は平文で記録し、機密情報３０５は暗号化してアクセスログファイル１８に記録することで、暗号化演算を行うデータ量を減少させて高速化を図る。さらに、アクセスログの生成時に共通暗号鍵方式の鍵を生成し、共通暗号鍵方式の鍵を公開鍵暗号方式により暗号化（以下、第一の暗号化方式）する。これにより、復号が困難となり、アクセスログファイル１８を保存したハードディスクなどの不揮発性記憶装置の盗難の際にも暗号化に使用する鍵が容易に判明することがない。また、暗号化前の実データを秘匿したまま利用者の識別にのみ必要な機密情報（利用者ＩＤ等）については、同一平文であれば同一暗号文に変換する暗号化（以下、第二の暗号方式）手法を用い、さらに使用した暗号鍵は破棄することで当該一方向暗号化を行うことにより、復号を困難にする。

【００８２】

また、上述したように、第１の暗号化方法によれば、所定のルール、例えばＵＲＬクエリー文字列と称するルールに従っていることを利用して、文字「?」以前を非機密情報部、文字「?」以降を機密情報部とみなしＵＲＬ文字列を分解して暗号化を行っている。そ

れにより、ＷＥＢブラウザの製作業者の意図に関係なく、任意の製作業者が作成したアプリケーションプログラムのＵＲＬ文字列であっても対応できるという効果が得られる。

【００８３】

また、アクセスログファイルを格納した不揮発性記憶装置の盗難や通信回線を介した不正アクセスによるアクセスログファイルの盗難等によって、機密情報を含むログ情報が流出した際の危険を減少させることができる。また、ログ情報に含まれる機密情報が端末装置を過去に利用した利用者の識別にのみ必要とする場合、その利用者の識別に利用される機密情報が復号困難な形態で暗号化されているため、故意または過失による情報漏洩の危険を減少させることができる。さらに、機密情報を含んだアクセスログファイル等を暗号化する際、非機密情報については暗号化しないので、暗号化処理の高速化が実現できる。

【００８４】

なお、アクセスログファイル１８利用者ＩＤ等の利用者識別に使用される機密情報部分を必要としない用途の場合には、図１の端末装置１００において、一方向暗号化部７を持たない構成としてもよい。その場合は、揮発性記憶装置１２に記憶されている一方向鍵１４も不要となる。なお、図５に示した閲覧装置２００の構成は同一である。しかし、閲覧装置２００は、図６に記載した記録用文字列３０９において第二の暗号化方式で暗号化された機密情報部分３０８は無いものとする処理を実行する。

【００８５】

また、第一の機密情報の一部に識別に必要な情報つまり第二の機密情報は存在するが、第一の機密情報の全てを記録する必要のない用途の場合には、図１の端末装置において、共通鍵方式暗号化部６を持たない構成としてもよい。その場合、共通鍵１３、公開鍵方式暗号化部１０、暗号化用公開鍵１７も不要となる。また、図３において、ＵＲＬ文字列３０１から第一の機密情報３０５が抽出されるものの、暗号化は行われる、記録用合成部８ａで合成されることもない。

【００８６】

また、端末装置１００、閲覧装置２００，２１０において、上述した実施形態の機能を実現するソフトウェアのプログラムコード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等の制御装置）が記録媒体に格納されたプログラムコードを読み出し実行することによっても、達成されることは言うまでもない。

【００８７】

さらに、上述した実施の形態では、ログ情報生成手段をＨＴＭＬ表示・処理部３及び機能ボタン表示・処理部４に適用した例について説明したが、物体の有無または動きを検知し、検知結果に基づくログ情報を生成する物体検知センサに適用してもよい。あるいは、例えばキャッシュカードのような接触式磁気カードや電車定期券などに用いられている非接触式磁気カードに記録されたデータの読み込み及び当該データへの書き込みを行い、このデータに対する読み書きの内容及び履歴を示すログ情報を生成するリーダライタ等に適用してもよい。

【図面の簡単な説明】

【００８８】

【図１】本発明の一実施形態に係る端末装置の全体構造図である。

【図２】本発明の一実施形態に係る施設予約のアプリケーション処理に基づく画面遷移を示した図である。

【図３】本発明の一実施形態に係るアクセスログの暗号化処理の手順を示す図である。

【図４】本発明の一実施形態に係るテキスト形式で表記されたアクセスログファイルの一例である。

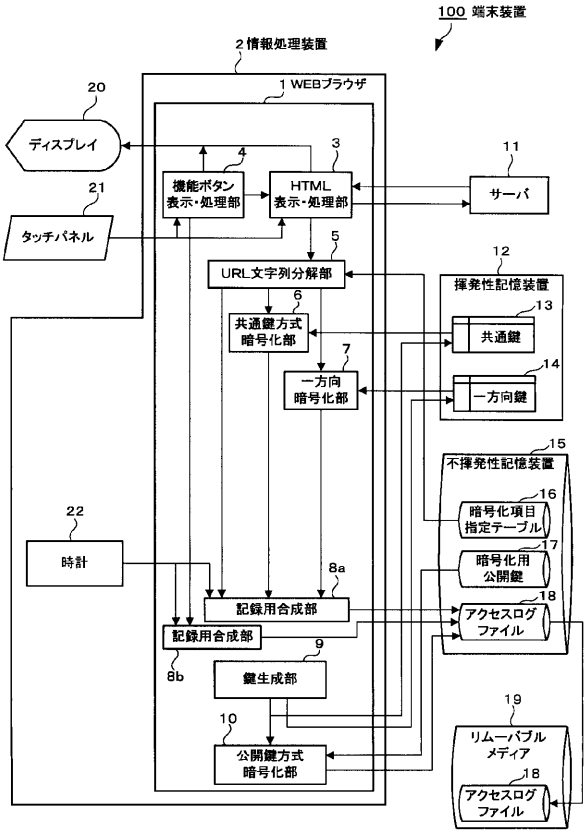
【図５】本発明の一実施形態に係る閲覧装置の構成例である。

【図６】本発明の一実施形態に係る暗号化したアクセスログの復号処理の手順を示す図である。

【図７】本発明の一実施形態に係る閲覧装置の構成例である。

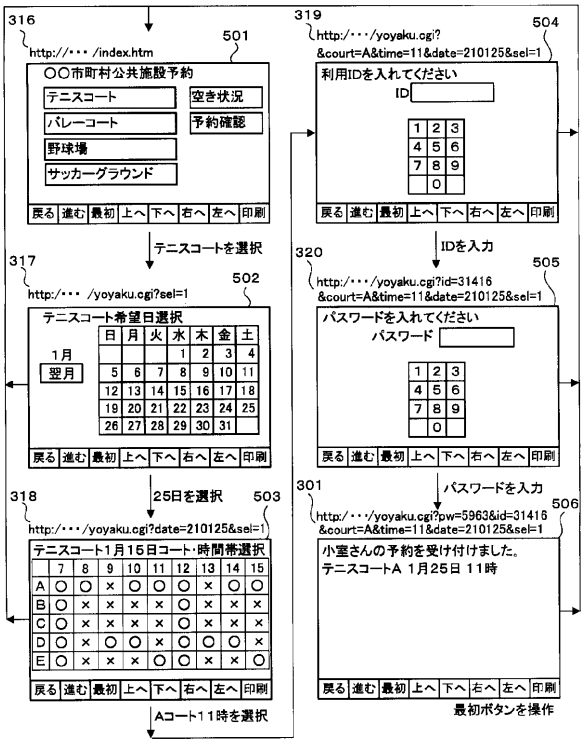
【図８】本発明の一実施形態に係る閲覧装置のアクセスログの復号手順を示す図である。
【図９】本発明の一実施形態に係る暗号化したアクセスログの機密情報を秘匿した読み出し手順を示す図である。
【符号の説明】
【００８９】
１…ＷＥＢブラウザ、２…情報処理装置、３…ＨＴＭＬ表示・処理部、４…機能ボタン表示・処理部、５…ＵＲＬ文字列分解部、６…共通鍵方式暗号化部、７…一方向暗号化部、８…記録用合成部、９…鍵生成部、１０…公開鍵方式暗号化部、１２…揮発性記憶装置、１３…共通鍵、１４…一方向鍵、１５…不揮発性記憶装置、１６…暗号化項目指定テーブル、１７…暗号化用公開鍵、１８…アクセスログファイル、２０…ディスプレイ、２１…タッチパネル、２２…時計、２３…閲覧処理装置、２４…ログ切り出し部、２５…共通鍵方式復号部、２６…合成部、２７…公開鍵方式復号部、２８…復号用秘密鍵、２２０…閲覧装置、２１２…揮発性記憶装置、３０１…ＵＲＬ文字列、３０２…日時情報、３０３…付加情報、３０４…非機密情報、３０５…第一の機密情報、３０６…暗号化された第一の機密情報、３０７…第二の機密情報、３０８…一方向暗号化された第二の機密情報、３０９…記録用文字列、３１０…記録用文字列、３１２…区切り記号、３１５…暗号化した共通鍵

【図１】



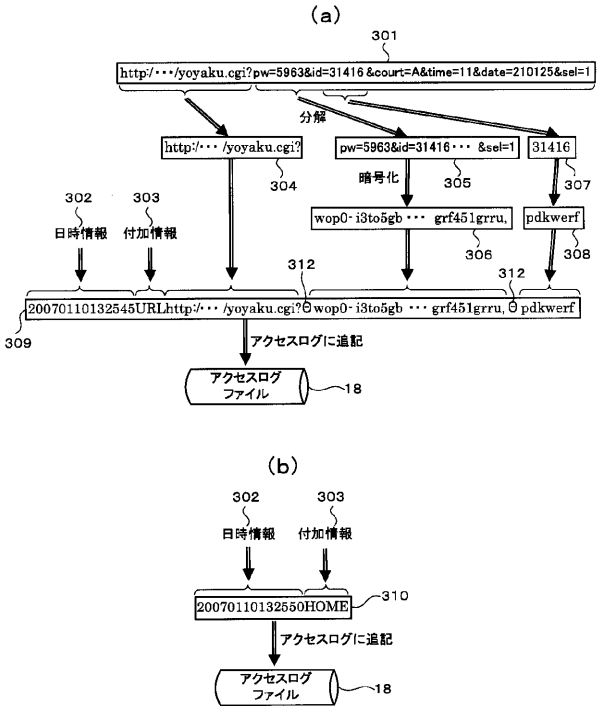
端末装置の構成例

【図２】



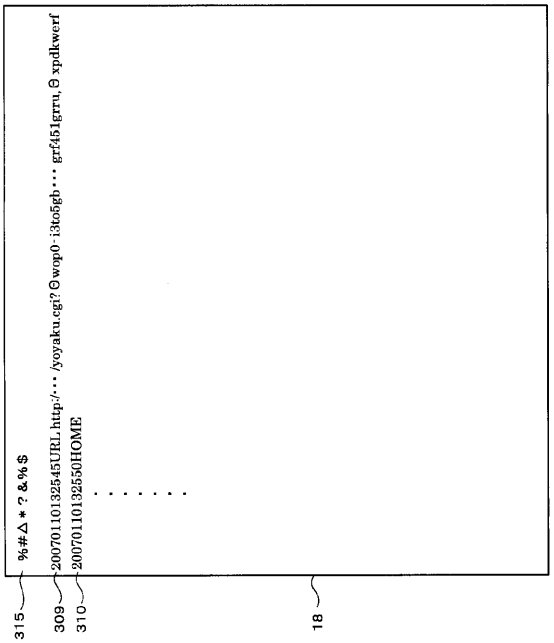
施設予約アプリケーションの画面遷移例

【図３】

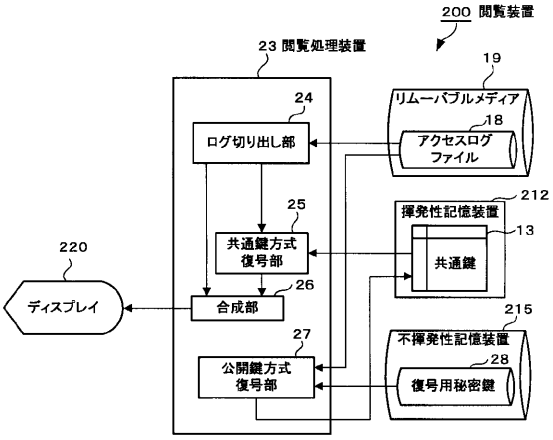


アクセスログの暗号化手順例

【図４】

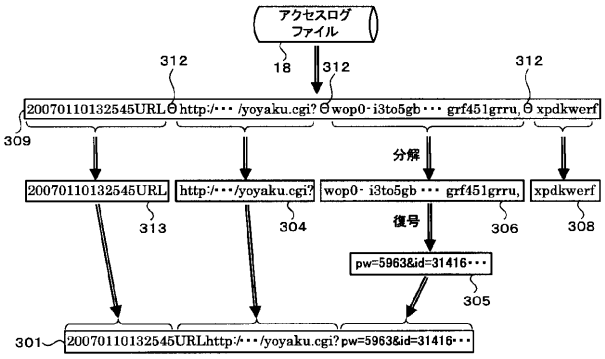


【図５】



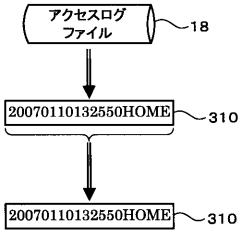
アクセスログファイル閲覧装置の構成例

【図６】



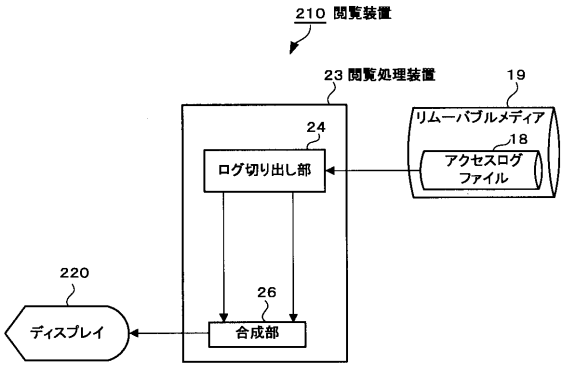
暗号化されたアクセスログの復号手順例

【図７】



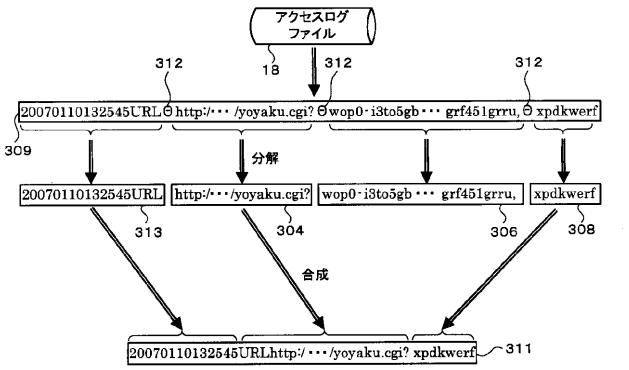
暗号化されたアクセスログの復号手順例

【図８】



アクセスログファイル閲覧装置の構成例

【図９】



アクセスログの読み出し手順例