(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2012-124787
(P2012-124787A)
(43)公開日　平成24年6月28日(2012.6.28)

(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)	H04L	9/00	601E	5J104
		G06F	12/14	540C	
		G06F	12/14	560A	

審査請求 未請求　請求項の数 3　OL　（全 10 頁）

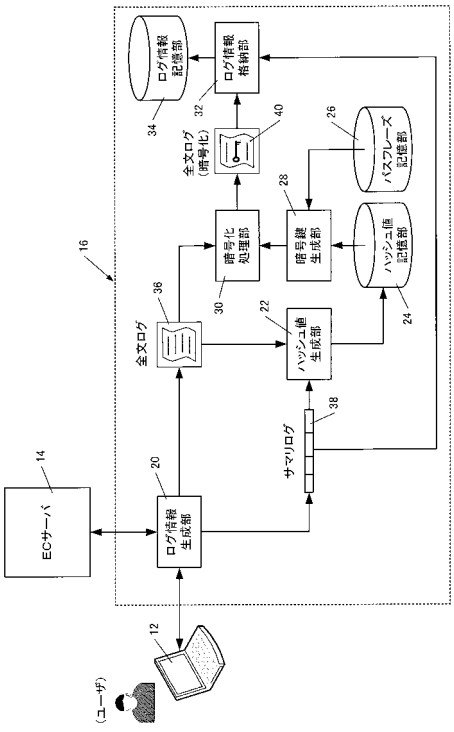
(21)出願番号　特願2010-275130 (P2010-275130)
(22)出願日　平成22年12月9日 (2010.12.9)

(71)出願人　000155469
株式会社野村総合研究所
東京都千代田区丸の内一丁目６番５号
(74)代理人　100096002
弁理士　奥田　弘之
(74)代理人　100091650
弁理士　奥田　規之
(72)発明者　橋本　淳
東京都千代田区丸の内一丁目６番５号　株式会社野村総合研究所内

Fターム(参考)　5B017 AA03 BA05 BA07 CA16
5J104 AA12 AA16 EA04 EA08 EA09 EA15 EA16 JA03 NA02 NA12 NA37 PA14

(54)【発明の名称】アクセス管理システム

(57)【要約】
【課題】ログ情報の秘匿性を確保しつつも、暗号鍵を保管する必要のないアクセス管理システムを実現する。
【解決手段】アクセス管理サーバ16は、クライアント端末12とECサーバ14間の操作履歴を記述した全文ログと、インデックスであるサマリログを生成するログ情報生成手段20と、全文ログ及びサマリログの各ハッシュ値を生成するハッシュ値生成部22と、各ハッシュ値及びパスフレーズに基づいて暗号鍵を生成する暗号鍵生成部28と、暗号鍵を用いて全文ログを暗号化すると共に、暗号鍵をメモリ上から削除する暗号化処理部30と、暗号化全文ログとサマリログをログ情報記憶部34に格納するログ情報格納部32を備える。管理端末17から全文ログの閲覧リクエストが入力された際、暗号鍵生成部28は対応する全文ログ及びサマリログの各ハッシュ値、パスフレーズに基づいて暗号鍵を再生成し、これを用いて復号処理部44が全文ログを復号すると共に、暗号鍵をメモリ上から削除する。
【選択図】図２



【特許請求の範囲】
【請求項１】
クライアント端末とサーバ間に介装されるアクセス管理システムであって、
クライアント端末とサーバ間の操作履歴を記述した全文ログと、当該全文ログのインデックスであるサマリログをセッション単位で生成する手段と、
上記全文ログの記述内容に基づいて所定ビット数のハッシュ値を生成すると共に、上記サマリログの記述内容に基づいて所定ビット数のハッシュ値を生成し、ハッシュ値記憶手段に格納するハッシュ値生成手段と、
少なくとも上記全文ログのハッシュ値及びサマリログのハッシュ値に基づいて、所定ビット数の暗号鍵を生成する第１の暗号鍵生成手段と、
この暗号鍵を用いて上記全文ログを暗号化する手段と、
上記暗号鍵をメモリ上から削除する手段と、
上記暗号化された全文ログをログ情報記憶手段に格納する手段と、
管理者の操作する管理端末から、特定のセッションに係るログ情報の閲覧リクエストが入力された際に、上記ハッシュ値記憶手段から対応する全文ログのハッシュ値及びサマリログのハッシュ値を取得する手段と、
少なくとも当該全文ログのハッシュ値及びサマリログのハッシュ値に基づいて、上記と同一の暗号鍵を生成する第２の暗号鍵生成手段と、
この暗号鍵を用いて上記暗号化された全文ログを復号する手段と、
上記暗号鍵をメモリ上から削除する手段と、
復号された全文ログを上記管理端末に送信する手段と、
を備えたことを特徴とするアクセス管理システム。
【請求項２】
所定の文字列からなるパスフレーズを格納しておくパスフレーズ記憶手段を備えており、
上記第１の暗号鍵生成手段及び第２の暗号鍵生成手段は、上記全文ログのハッシュ値及びサマリログのハッシュ値の他に、上記パスフレーズを用いて上記の暗号鍵を生成することを特徴とする請求項１に記載のアクセス管理システム。
【請求項３】
上記パスフレーズが、２名以上の管理者のパスワードに基づいて生成された文字列よりなることを特徴とする請求項２に記載のアクセス管理システム。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明はアクセス管理システムに係り、特に、クライアント端末とサーバ間におけるデータのやり取りを、ログ情報として外部記憶装置に蓄積する機能を備えたアクセス管理システムに関する。
【背景技術】
【０００２】
セキュリティの確保や内部統制の実現等の観点から、クライアント端末とサーバ間におけるデータのやり取りを、外部記憶装置に逐一記録しておくことが推奨されており、これを実現するための装置やサービスが既に実用化されている。
【０００３】
図７は、従来のアクセス管理システムの利用形態を示すブロック図であり、ユーザが操作するクライアント端末12と、ユーザが利用するEC（Electronic Commerce）サーバ14との間にアクセス管理サーバ60が介装されている様子が描かれている。アクセス管理サーバ60は、クライアント端末12とECサーバ14間において生じたデータのやり取りを、ログ情報としてハードディスク等の外部記憶装置に逐一記録する機能を備えている。
このようなログ情報には、IDやパスワード、クレジットカード番号のように重要な個人情報が含まれているため、暗号化した上で外部記憶装置に格納することが望ましい。

【０００４】
例えば、システムに何らかの障害が発生した場合に、保守担当者は保守端末18からアクセス管理サーバ60に接続し、システムの現状確認や復旧を試みる。この際、必要に応じて外部記憶装置にもアクセスする場面も生じるが、ログ情報が予め暗号化されていれば、権限外の保守担当者がログの内容を認識することを有効に防止できる。
【０００５】
これに対し、このアクセス管理サーバ60の管理者にはログ情報を閲覧する権限が与えられているため、管理端末17からアクセス管理サーバ60にログインし、外部記憶装置に格納された特定のログ情報を指定すると、アクセス管理サーバ60内の暗号処理システムによって当該ログ情報が復号された後、管理端末17に送信される。この結果、管理者はいつでもログ情報を確認することが可能となる。
【０００６】
ところで、ログ情報を暗号化するに際しては、暗号化アルゴリズムを制御するための秘密データとして所謂「暗号鍵」が用いられることになるが、この暗号鍵が外部に流出すると悪意の第三者に暗号文が解読される危険性が生じるため、通常はアクセス管理サーバ60内に保管することなく、外部の暗号鍵管理システム62に付託されている（非特許文献１参照）。
【非特許文献１】暗号鍵管理システム「KeyMeister（キーマイスター）」　インターネットURL：http://jp.fujitsu.com/group/fip/services/safeport/keymeister/　検索日：２０１０年１１月２６日
【発明の開示】
【発明が解決しようとする課題】
【０００７】
このように、暗号鍵の保管を外部の暗号鍵管理システム62に付託することにより、確かにログ情報の秘匿性は担保されることになるが、その分、暗号鍵管理システム62の運用コストやライセンス料等の余計なコストが嵩むことになる。
この発明は、このような現状に鑑みて案出されたものであり、ログ情報の秘匿性を確保しつつも、暗号鍵を保管する必要のないアクセス管理システムを実現することを目的としている。
【課題を解決するための手段】
【０００８】
上記の目的を達成するため、請求項１に記載したアクセス管理システムは、クライアント端末とサーバ間に介装されるアクセス管理システムであって、 クライアントとサーバ間でやり取りされる操作ログの全文を記述した全文ログと、当該全文ログのインデックスであるサマリログとをセッション単位で生成する手段と、上記全文ログの記述内容に基づいて所定ビット数のハッシュ値を生成すると共に、上記サマリログの記述内容に基づいて所定ビット数のハッシュ値を生成し、ハッシュ値記憶手段に格納するハッシュ値生成手段と、少なくとも上記全文ログのハッシュ値及びサマリログのハッシュ値に基づいて、所定ビット数の暗号鍵を生成する第１の暗号鍵生成手段と、この暗号鍵を用いて上記全文ログを暗号化する手段と、上記暗号鍵をメモリ上から削除する手段と、上記暗号化された全文ログをログ情報記憶手段に格納する手段と、管理者の操作する管理端末から、特定のセッションに係るログ情報の閲覧リクエストが入力された際に、上記ハッシュ値記憶手段から対応する全文ログのハッシュ値及びサマリログのハッシュ値を取得する手段と、少なくとも当該全文ログのハッシュ値及びサマリログのハッシュ値に基づいて、上記と同一の暗号鍵を生成する第２の暗号鍵生成手段と、この暗号鍵を用いて上記暗号化された全文ログを復号する手段と、上記暗号鍵をメモリ上から削除する手段と、復号された全文ログを上記管理端末に送信する手段とを備えたことを特徴としている。
上記第１の暗号鍵生成手段及び第２の暗号鍵生成手段は、同一の暗号鍵生成アルゴリズムを備えている。また、上記第２の暗号鍵生成手段の処理を、上記第１の暗号鍵生成手段が兼務するように構成してもよい。

【０００９】
請求項２に記載したアクセス管理システムは、請求項１のシステムを前提とし、さらに所定の文字列からなるパスフレーズを格納しておくパスフレーズ記憶手段を備えており、上記第１の暗号鍵生成手段及び第２の暗号鍵生成手段は、上記全文ログのハッシュ値及びサマリログのハッシュ値の他に、上記パスフレーズを用いて上記の暗号鍵を生成することを特徴としている。
【００１０】
請求項３に記載したアクセス管理システムは、請求項２のシステムを前提とし、さらに上記パスフレーズが、２名以上の管理者のパスワードに基づいて生成された文字列よりなることを特徴としている。
【発明の効果】
【００１１】
請求項１に記載のアクセス管理システムによれば、全文ログを暗号化する際に、当該全文ログから生成したハッシュ値と、当該全文ログに係るアクセスログから生成したハッシュ値に基づき、当該セッションに固有の暗号鍵がその場で生成され、暗号化が完了した時点でメモリ上から削除される仕組みであり、外部記憶装置に保存されることがない。また、各全文ログを復号する際には、当該全文ログのハッシュ値と、当該全文ログに係るアクセスログのハッシュ値、及びパスフレーズに基づき、当該セッションに固有の暗号鍵がその場で再生成され、復号が完了した時点でメモリ上から削除される仕組みであり、やはり外部記憶装置に保存されることがない。このため、暗号鍵の保管や管理自体を不要とすることができる。
【００１２】
請求項２に記載のアクセス管理システムによれば、暗号鍵の生成に際して、全文ログのハッシュ値及びサマリログのハッシュ値の他に、任意のパスフレーズを必須の構成要素として条件付けることができるため、暗号鍵の探知をより困難化することが可能となる。
【００１３】
請求項３に記載のアクセス管理システムによれば、暗号鍵の生成に際して、全文ログのハッシュ値及びサマリログのハッシュ値の他に、２名以上の管理者のパスワードに基づいて生成された文字列よりなるパスフレーズを必須の構成要素として条件付けることができるため、「クレジットカード情報が混入しているログ情報を閲覧するに際しては、２名以上の管理者の認証を必要とすべきである」ことを規定する、PCI DSS（Payment Card Industry Data Security Standard／クレジットカード業界におけるグローバルセキュリティ基準）をクリア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】
【００１４】
図１は、この発明に係るアクセス管理システムの利用形態を示すブロック図であり、ユーザが操作するクライアント端末12と、ユーザが利用するEC（Electronic Commerce）サーバ14との間に、アクセス管理システムを具現化するためのアクセス管理サーバ16が介装されている様子が描かれている。
アクセス管理サーバ16には、システム管理者が操作する管理端末17と、保守担当者が操作する保守端末18も、通信ネットワークを介して接続される。
【００１５】
アクセス管理サーバ16は、クライアント端末12とECサーバ14間において生じたデータのやり取りを、ログ情報として逐一記録する機能を備えている。
このログ情報自体は単純なテキスト形式のデータよりなるが、これにはIDやパスワード、クレジットカード番号のように重要な個人情報が含まれているため、アクセス管理サーバ16は、ログ情報を暗号化した上で所定の記憶手段に格納する機能を備えている。
【００１６】
図２は、ログ情報を暗号化して記憶手段に格納する場面におけるアクセス管理サーバ16の機能構成を示すブロック図であり、ログ情報生成部20と、ハッシュ値生成部22と、ハッ

シュ値記憶部24と、パスフレーズ記憶部26と、暗号鍵生成部28と、暗号化処理部30と、ログ情報格納部32と、ログ情報記憶部34とを備えている。

【００１７】

これらの機能構成要素の中、ログ情報生成部20、ハッシュ値生成部22、暗号鍵生成部28、暗号化処理部30及びログ情報格納部32は、アクセス管理サーバ16のCPUが、OS及びアプリケーションプログラムに従って所定の処理を実行することで実現される。

また、ハッシュ値記憶部24、パスフレーズ記憶部26及びログ情報記憶部34は、アクセス管理サーバ16のハードディスク内に設けられている。

ログ情報生成部20には、通信ネットワークを介して、ユーザの操作するクライアント端末12とECサーバ14とが接続されている。

【００１８】

つぎに、図３のフローチャートに従い、当該場面におけるアクセス管理サーバ16の処理手順について説明する。

まず、ログ情報生成部20は、クライアント端末12とECサーバ14との間において通信が開始されると、双方間で交わされたデータを逐一取得し、セッション単位でログ情報を生成する（Ｓ10）。

【００１９】

ログ情報生成部20によって生成されるログ情報としては、双方間における全データがテキスト形式で記述された全文ログ（操作ログ）36と、当該セッションのインデックス情報として利用されるサマリログ38とがある。

サマリログ38は、例えば、当該セッションに係るアクセス開始日時、アクセス終了日時、ユーザアカウント、接続元クライアント、ポート番号、接続先サーバ、流出データ（byte）、流入データ（byte）、接続時間（秒）等のデータ項目を備えている（図６参照）。

【００２０】

つぎに、ハッシュ値生成部22が全文ログ36の文字列データを所定のハッシュ関数に投入することにより、所定ビット長（例えば128ビット）のハッシュ値を生成し、当該セッションを特定するユニークなIDに関連付けてハッシュ値記憶部24に格納する（Ｓ12）。

同時にハッシュ値生成部22は、サマリログ38の文字列データを所定のハッシュ関数に投入することにより、所定ビット長（例えば128ビット）のハッシュ値を生成し、上記IDに関連付けてハッシュ値記憶部24に格納する（Ｓ14）。

【００２１】

つぎに暗号鍵生成部28が起動し、ハッシュ値記憶部24に格納された全文ログのハッシュ値と、サマリログのハッシュ値、及びパスフレーズ記憶部26に予め格納されたパスフレーズを所定の暗号鍵生成アルゴリズムに投入することにより、所定ビット長（例えば128ビット）の暗号鍵を生成する（Ｓ16）。

上記パスフレーズとしては、例えば２名以上のシステム管理者のログインパスワードに対して、所定の演算処理を施すことによって生成された所定桁数の文字列が該当するが、他の文字列であってもよい。

【００２２】

つぎに暗号化処理部30が起動し、暗号鍵生成部28から渡された暗号鍵を用い、所定の暗号化アルゴリズムを適用することにより、全文ログ36を暗号化する（Ｓ18）。暗号化処理部30は、この暗号化処理が完了した後、暗号鍵をメモリ上から消去する（Ｓ20）。

【００２３】

最後に、ログ情報格納部32により、暗号化された全文ログ40と、平文のままのサマリログ38とが、当該セッションに関連付けてログ情報記憶部34に格納される（Ｓ22）。

【００２４】

図４は、ログ情報を復号して管理端末17に表示させる場面におけるアクセス管理サーバ16の機能構成を示すブロック図であり、ログ情報提示部42と、ログ情報記憶部34と、暗号鍵生成部28と、ハッシュ値記憶部24と、パスフレーズ記憶部26と、復号処理部44とを備えている。

【００２５】
これらの機能構成要素の中、ログ情報記憶部34、暗号鍵生成部28、ハッシュ値記憶部24及びパスフレーズ記憶部26は、図２に示されたものと同じものである。また、ログ情報提示部42及び復号処理部44は、アクセス管理サーバ16のCPUが、OS及びアプリケーションプログラムに従って所定の処理を実行することで実現される。
ログ情報提示部42には、通信ネットワークを介して、管理者の操作する管理端末17が接続されている。
【００２６】
つぎに、図５のフローチャートに従い、当該場面におけるアクセス管理サーバ16の処理手順について説明する。
まず、ログ情報提示部42は、管理端末17からログ情報の閲覧リクエストを受信すると（Ｓ30）、ログ情報記憶部34から複数のサマリログ38を取り出してログ情報の一覧画面を生成し、管理端末17に送信する（Ｓ32）。
【００２７】
図６は、この一覧画面の表示内容を示すものであり、各セッションのサマリログに対応した「アクセス開始日時」、「アクセス終了日時」、「ユーザアカウント」、「接続元クライアント」、「ポート番号」、「接続先サーバ」、「流出データ（byte）」、「流入データ（byte）」、「接続時間（秒）」の表示項目の他に、「全文ログダウンロード」の表示項目を備えている。
【００２８】
「全文ログダウンロード」の表示項目には、暗号化された全文ログの存在を象徴するアイコンが表示されており、管理者が任意のセッションに係るアイコンにマウスポインタを翳してクリックすると、管理端末17からアクセス管理サーバ16に対して当該セッションに係る全文ログの閲覧リクエストが送信される。
【００２９】
これを受信したログ情報提示部42は（Ｓ34）、暗号鍵生成部28に対して暗号鍵の生成を依頼し、暗号鍵生成部28は、当該セッションに係る全文ログのハッシュ値及びサマリログのハッシュ値をハッシュ値記憶部24から取得する（Ｓ36）。
【００３０】
つぎに暗号鍵生成部28は、これら全文ログのハッシュ値及びサマリログのハッシュ値と、パスフレーズ記憶部26に格納された上記のパスフレーズとを、上記と同様の暗号鍵生成アルゴリズムに投入することにより、当該全文ログの暗号化時に用いたのと同一の暗号鍵を生成する（Ｓ38）。
【００３１】
つぎに復号処理部44が起動し、暗号鍵生成部28から渡された暗号鍵を用い、上記の暗号化アルゴリズムに対応した復号アルゴリズムに基づいて、暗号化全文ログを復号する（Ｓ40）。復号処理部44は、この復号処理が完了した後、暗号鍵をメモリ上から消去する（Ｓ42）。
【００３２】
最後に、ログ情報提示部42が復号された全文ログ40の表示画面を生成し、管理端末17に送信する（Ｓ44）。
この結果、管理端末17のディスプレイ上には、特定のセッションに係る全文ログ40の記述内容が表示される（図示省略）。
【００３３】
このアクセス管理システムによれば、各全文ログを暗号化する際に、当該全文ログから生成したハッシュ値と、当該全文ログに係るアクセスログから生成したハッシュ値、及びパスフレーズに基づき、当該セッションに固有の暗号鍵がその場で生成され、この暗号鍵は暗号化が完了した時点でメモリ上から削除される仕組みであり、外部記憶装置に保存されることがない。また、各全文ログを復号する際にも、当該全文ログのハッシュ値と、当該全文ログに係るアクセスログのハッシュ値、及びパスフレーズに基づき、当該セッショ

ンに固有の暗号鍵がその場で再生成され、この暗号鍵は復号が完了した時点でメモリ上から削除される仕組みであり、やはり外部記憶装置に保存されることがない。このため、暗号鍵の管理自体が不要となる。

【００３４】

保守担当者は、保守端末18からこのアクセス管理サーバ16にアクセスすることが可能であるが、例えログ情報記憶部34に格納された全文ログを閲覧したとしても、これらのデータは暗号化されているため、内容を理解することができない。

【００３５】

同様に、保守担当者がハッシュ値記憶部24に格納されたハッシュ値を閲覧できたとしても、ハッシュ値には一方向性（不可逆性）があるため、基になった全文ログを再現することはできない。

【００３６】

さらに、各ハッシュ値や暗号化された全文ログのデータに対して万一改竄がなされた場合には、当該ハッシュ値等に基づいて生成された暗号鍵を用いて暗号化全文ログを復号することができない事態が生じ、その時点で改竄の事実を検知することが可能となる。

【００３７】

上記のように、２名以上の管理者のログインパスワードに基づいて生成された文字列をパスフレーズとして用いることにより、PCI DSSの基準に適合させることが可能となるが、パスフレーズはこれに限定されるものではなく、他の文字列をパスフレーズとして利用することもできる。

また、暗号鍵の生成に際してパスフレーズの利用は必須ではなく、全文ログのハッシュ値とサマリログのハッシュ値のみに基づいて暗号鍵を生成するようにしてもよい。

【図面の簡単な説明】

【００３８】

【図１】この発明に係るアクセス管理システムの利用形態を示すブロック図である。

【図２】ログ情報を暗号化して記憶手段に格納する場面におけるアクセス管理サーバの機能構成を示すブロック図である。

【図３】ログ情報を暗号化して記憶手段に格納する場面におけるアクセス管理サーバの処理手順を示すフローチャートである。

【図４】ログ情報を復号して管理端末に表示させる場面におけるアクセス管理サーバの機能構成を示すブロック図である。

【図５】ログ情報を復号して管理端末に表示させる場面におけるアクセス管理サーバの処理手順を示すフローチャートである。

【図６】管理端末のディスプレイに表示されたログ情報の一覧画面を例示する図である。

【図７】従来のアクセス管理システムの利用形態を示すブロック図である。

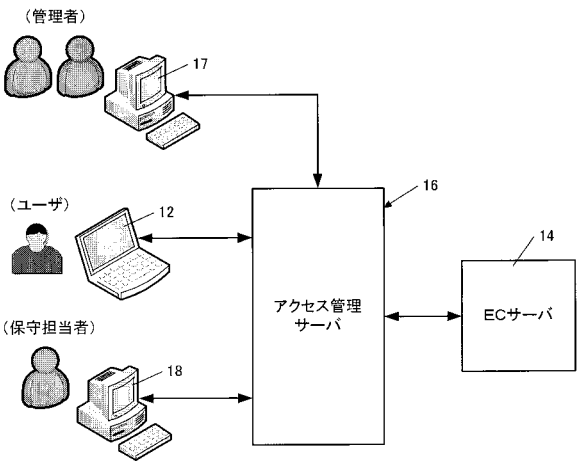
【符号の説明】

【００３９】

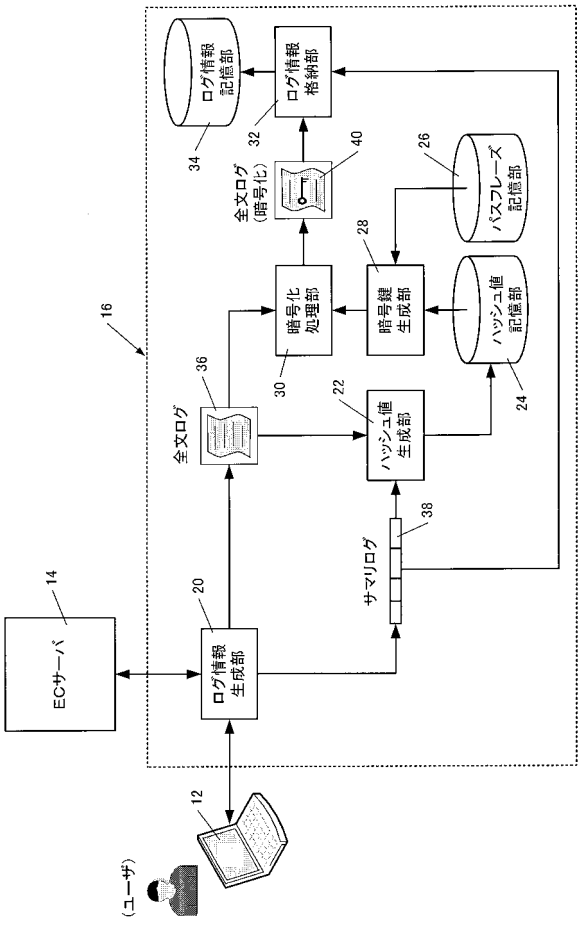
12　クライアント端末
14　ECサーバ
16　アクセス管理サーバ
17　管理端末
18　保守端末
20　ログ情報生成部
22　ハッシュ値生成部
24　ハッシュ値記憶部
26　パスフレーズ記憶部
28　暗号鍵生成部
30　暗号化処理部
32　ログ情報格納部
34　ログ情報記憶部

36　全文ログ
38　サマリログ
40　暗号化された全文ログ
42　ログ情報提示部
44　復号処理部

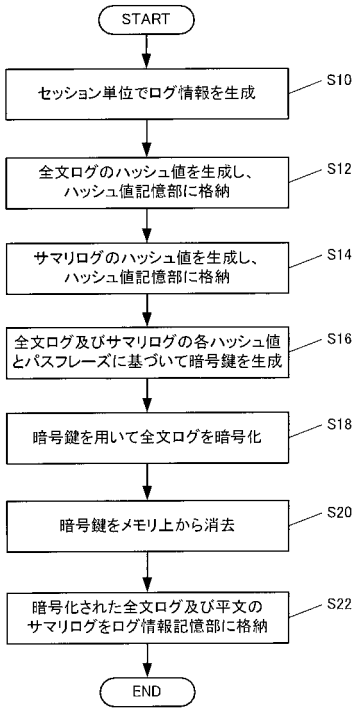
【図１】



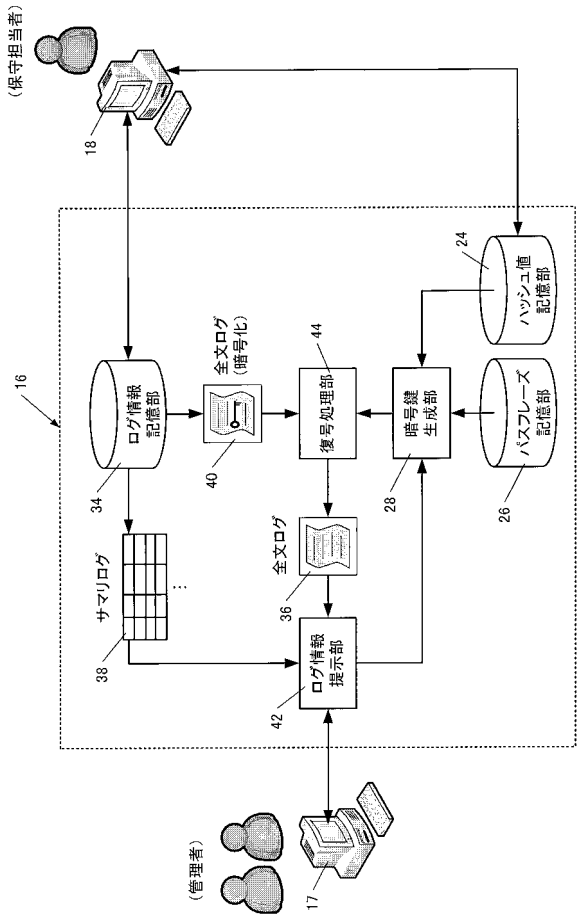
【図２】



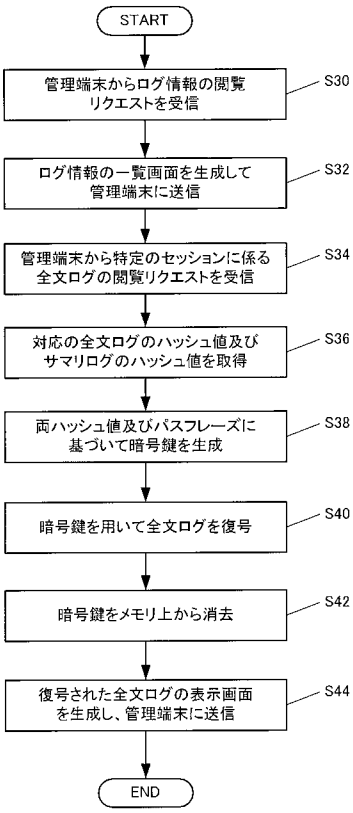
【図３】


START
セッション単位でログ情報を生成
S10
全文ログのハッシュ値を生成し、ハッシュ値記憶部に格納
S12
サマリログのハッシュ値を生成し、ハッシュ値記憶部に格納
S14
全文ログ及びサマリログの各ハッシュ値とパスフレーズに基づいて暗号鍵を生成
S16
暗号鍵を用いて全文ログを暗号化
S18
暗号鍵をメモリ上から消去
S20
暗号化された全文ログ及び平文のサマリログをログ情報記憶部に格納
S22
END

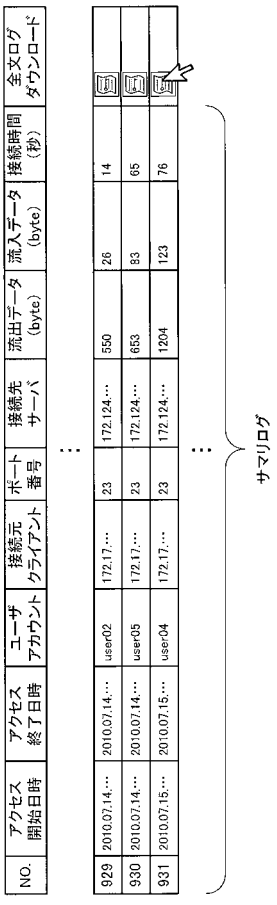
【図４】


（保守担当者）
18
16
ログ情報記憶部
34
全文ログ（暗号化）
40
復号処理部
44
暗号鍵生成部
28
ハッシュ値記憶部
24
パスフレーズ記憶部
26
サマリログ
38
全文ログ
36
ログ情報提示部
42
（管理者）
17

【図５】


START
管理端末からログ情報の閲覧リクエストを受信
S30
ログ情報の一覧画面を生成して管理端末に送信
S32
管理端末から特定のセッションに係る全文ログの閲覧リクエストを受信
S34
対応の全文ログのハッシュ値及びサマリログのハッシュ値を取得
S36
両ハッシュ値及びパスフレーズに基づいて暗号鍵を生成
S38
暗号鍵を用いて全文ログを復号
S40
暗号鍵をメモリ上から消去
S42
復号された全文ログの表示画面を生成し、管理端末に送信
S44
END

【図６】


NO.
アクセス開始日時
アクセス終了日時
ユーザアカウント
接続元クライアント
ポート番号
接続先サーバ
流出データ (byte)
流入データ (byte)
接続時間 (秒)
全文ログダウンロード
929
2010.07.14.…
2010.07.14.…
user02
172.17.…
23
172.124.…
550
26
14
930
2010.07.14.…
2010.07.14.…
user05
172.17.…
23
172.124.…
653
83
65
931
2010.07.15.…
2010.07.15.…
user04
172.17.…
23
172.124.…
1204
123
76
サマリログ

【図７】