(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4801059号
(P4801059)
(45)発行日　平成23年10月26日(2011.10.26)　(24)登録日　平成23年8月12日(2011.8.12)

(51)Int.Cl.		F I		
H04L 9/08	(2006.01)	H04L	9/00	601C
G06F 21/20	(2006.01)	G06F	15/00	330A
G06F 21/24	(2006.01)	H04L	9/00	601E
		G06F	12/14	540P

請求項の数 58　(全 17 頁)

(21)出願番号　特願2007-519590 (P2007-519590)
(86)(22)出願日　平成17年6月30日 (2005.6.30)
(65)公表番号　特表2008-505571 (P2008-505571A)
(43)公表日　平成20年2月21日 (2008.2.21)
(86)国際出願番号　PCT/CH2005/000363
(87)国際公開番号　WO2006/002564
(87)国際公開日　平成18年1月12日 (2006.1.12)
審査請求日　平成20年4月23日 (2008.4.23)
(31)優先権主張番号　04015475.9
(32)優先日　平成16年7月1日 (2004.7.1)
(33)優先権主張国　欧州特許庁 (EP)

(73)特許権者　506333347
テクノストア　アクチエンゲゼルシャフト
Tecnostore AG
スイス国　ルツェルン　ハルデンシュトラーセ　5
Haldenstrasse 5, CH-6006 Luzern, Switzerland
(74)代理人　100061815
弁理士　矢野　敏雄
(74)代理人　100099483
弁理士　久野　琢也
(74)代理人　100114890
弁理士　アインゼル・フェリックス＝ラインハルト

最終頁に続く

(54)【発明の名称】キー断片化による自動的な暗号化と復号化を伴うデータアーカイビングのための方法、システム及びセキュリティ手段

(57)【特許請求の範囲】

【請求項１】

自動的な暗号化と復号化を伴うデータアーカイビングのための方法であって、

データ（９，１０）の記憶処理において複数のデータがクライアントステーション（１）からセキュリティ手段（２）へ転送され、それらのデータがセキュリティ手段によって暗号化されてアーカイブステーション（４）に転送され、

さらにデータ（９，１０）の検索処理においては複数のデータがアーカイブステーション（４）からセキュリティ手段（２）へ転送され、それらのデータがセキュリティ手段によって復号化されてクライアントステーション（１）に転送される方法において、

データ（９，１０）の暗号化と復号化に対して、各ケース毎にファーストキー（６）とセカンドキー（７）とサードキー（８）とが用いられ、

そのうちのセカンドキー（７）は暗号化と復号化の間で少なくとも一時的にスワップアウトされ、さらにセキュリティ手段（２）において局所的に消去され、ここで、前記セカンドキー（７）のスワップアウトは、アーカイブステーション（４）への転送と、そこでの記憶と、そこからの再度のフィードバック転送によって行われるものであり、

サードキー（８）は暗号化と復号化の間で少なくとも一時的にスワップアウトされ、さらにセキュリティ手段（２）において局所的に消去され、ここで、前記サードキー（８）のスワップアウトは、クライアントステーション（１）への転送と、そこでの記憶と、そこからの再度のフィードバック転送によって行われるものであり、

クライアントステーション（１）からアーカイブステーション（４）との間の接続が適

正な場合に、スワップアウトされる前記セカンドキー（７）とスワップアウトされる前記サードキーとが用いられる
ことを特徴とする方法。
【請求項２】
前記セカンドキー（７）は、データ（９，１０）と共にアーカイブステーション（４）へ転送され、及び／又は、データ（９，１０）と共にセキュリティ手段（２）にフィードバック転送される、請求項１記載の方法。
【請求項３】
組合わせキー（５）が前記ファーストキーとセカンドキー並びにサードキー（６，７，８）とから形成され、暗号化と復号化が各ケース毎に当該組合わせキー（５）を用いて実行される、請求項１または２記載の方法。
【請求項４】
対称性の暗号化アルゴリズムが暗号化と復号化において使用され、３ＤＥＳ、ＩＤＥＡ、ｂｌｏｗｆｉｓｈ方式のアルゴリズムが用いられる、請求項１から３いずれか１項記載の方法。
【請求項５】
前記ファーストキー（６）及び／又はセカンドキー（７）及び／又はサードキー（８）が、各ケースにおいて少なくとも１００ビットの長さを有している、請求項１から４いずれか１項記載の方法。
【請求項６】
前記ファーストキー（６）及び／又はセカンドキー（７）及び／又はサードキー（８）は、各ケースにおいて少なくとも１０２４ビット、２０４８ビット及び／又は４０９６ビットの長さを有している、請求項１から５いずれか１項記載の方法。
【請求項７】
前記ファーストキー（６）は、セキュリティ手段（２）の生成動作若しくは初期動作の間に乱数発生器を用いて生成され記憶される、請求項１から６いずれか１項記載の方法。
【請求項８】
セキュリティ手段（２）は、ファーストキー（６）が他のユニットに対して転送不可能でかつ読み出し不可能であるように設計されている、請求項１から７いずれか１項記載の方法。
【請求項９】
データ（９，１０）の記憶前に、各ケースにおいてセカンドキー（７）及び／又はサードキー（８）が新たに生成され、この場合乱数発生器が用いられている、請求項１から８いずれか１項記載の方法。
【請求項１０】
前記セカンドキー（７）及び／又はサードキー（８）が、セキュリティ手段（２）によって生成されている、請求項１から９いずれか１項記載の方法。
【請求項１１】
前記クライアントステーション（１）とセキュリティ手段（２）の間の通信は、ネットワーク（１８）を介して行われている、請求項１から１０いずれか１項記載の方法。
【請求項１２】
前記セキュリティ手段（２）とアーカイブステーション（４）の間の通信は、ネットワーク（３）を介して行われている、請求項１から１１いずれか１項記載の方法。
【請求項１３】
前記ネットワーク（３）はイーサーネット規格に準拠するものであり、及び／又は仮想プライベートネットワーク及び／又はリモートアクセスサービスＲＡＳによるリモートアクセス用に設計されている、請求項１２記載の方法。
【請求項１４】
前記セキュリティ手段（２）は、物理的ユニットである請求項１から１３いずれか１項記載の方法。

【請求項１５】
前記セキュリティ手段（２）は、ＰＣカード若しくはＵＳＢデバイスである請求項１から１３いずれか１項記載の方法。
【請求項１６】
データ（９，１０）は１つ又は複数のファイルの形態で転送されて記憶される、請求項１から１５いずれか１項記載の方法。
【請求項１７】
前記セカンドキー（７）は複数のファイルのヘッダ部分で、又は複数のファイルのうちの１つのヘッダ部分でアーカイブステーション（４）に転送される、請求項１６記載の方法。
【請求項１８】
別個のセカンドキー（７）と一緒に転送された複数のファイルの各々毎若しくは複数のファイルの各グループ毎に、及び／又は、別個のサードキー（８）が生成される、請求項１６または１７記載の方法。
【請求項１９】
さらに複数のクライアントステーション（１）が設けられている、請求項１から１８いずれか１項記載の方法。
【請求項２０】
データ（９，１０）がアーカイブステーション（４）からクライアントステーション（１）へ転送される前に、クライアントステーション（１）がデータ（９，１０）の受信に対して認証されているかどうかがチェックされ、クライアントステーション（１）が認証されている場合にのみ転送が実行される、請求項１から１９いずれか１項記載の方法。
【請求項２１】
クライアントステーション（１）がデータ（９，１０）の受信に対して認証されているかどうかのチェックの際にデータリクエスト送信側のＩＳＤＮナンバー及び／又はＩＰアドレスがチェックされる、請求項２０記載の方法。
【請求項２２】
アーカイブステーション（４）からのデータ（９，１０）検索に対する認証が、必要に応じてリモートアクセスからのアーカイブステーション（４）上のデータ（９，１０）に所属するセカンドキー（７）の引き抜きによって不能にされる、請求項１から２１いずれか１項記載の方法。
【請求項２３】
アーカイブステーション（４）からのデータ（９，１０）検索に対する認証が、必要に応じてリモートアクセスからのアーカイブステーション（４）上のデータ（９，１０）に所属するセカンドキー（７）の消去か又はスワップアウトと消去によって不能にされる、請求項１から２１いずれか１項記載の方法。
【請求項２４】
前記アーカイブステーション（４）が第１及び第２のサーバーコンピュータで構成され、この場合第１のサーバーコンピュータはデータ（９，１０）の記憶のために設けられ、第２のサーバーコンピュータは１つ又は複数のセカンドキーの記憶のために設けられている、請求項１から２３いずれか１項記載の方法。
【請求項２５】
１つのセカンドキー又は複数のセカンドキーが、アーカイブステーション（４）上に記憶されて暗号化され、及び／又はハードウエアモジュール若しくはアダプターに記憶される、請求項１から２４いずれか１項記載の方法。
【請求項２６】
アーカイブステーション（４）のデータ（９，１０）及び／又は１つのセカンドキー又は複数のセカンドキー（７）が、データバックアップのためにストレージユニット（１４）にコピーされる、請求項１から２５いずれか１項記載の方法。
【請求項２７】

アーカイブステーション（４）のデータ（９，１０）及び／又は１つの又は複数のセカンドキー（７）が、データバックアップのために、テープデッキやＣＤ、ＤＶＤ、ディスクアレイにコピーされる、請求項１から２５いずれか１項記載の方法。

【請求項２８】

前記アーカイブステーション（４）は機密保護された空間に配設される、請求項１から２７いずれか１項記載の方法。

【請求項２９】

前記アーカイブステーション（４）はバンカーや地下シェルターに配設される、請求項１から２７いずれか１項記載の方法。

【請求項３０】

自動的な暗号化と復号化を伴うデータアーカイビングのためのシステムであって、

データ（９，１０）の記憶処理において複数のデータがシステムの少なくとも１つのクライアントステーション（１）からシステムのセキュリティ手段（２）へ転送され、それらのデータが当該セキュリティ手段によって暗号化されてシステムのアーカイブステーション（４）に転送され、

さらにデータ（９，１０）の検索処理においては複数のデータがアーカイブステーション（４）からセキュリティ手段（２）へ転送され、それらのデータがセキュリティ手段によって復号化されてクライアントステーション（１）に転送されるシステムにおいて、

データ（９，１０）の暗号化と復号化に対して、各ケース毎にファーストキー（６）とセカンドキー（７）とサードキー（８）とが用いられ、

そのうちのセカンドキー（７）は暗号化と復号化の間で少なくとも一時的にスワップアウトされ、さらにセキュリティ手段（２）において局所的に消去され、ここで、前記セカンドキー（７）のスワップアウトは、アーカイブステーション（４）への転送と、そこでの記憶と、そこからの再度のフィードバック転送によって行われるものであり、

サードキー（８）は暗号化と復号化の間で少なくとも一時的にスワップアウトされ、さらにセキュリティ手段（２）において局所的に消去され、ここで、前記サードキー（８）のスワップアウトは、クライアントステーション（１）への転送と、そこでの記憶と、そこからの再度のフィードバック転送によって行われるものであり、

クライアントステーション（１）からアーカイブステーション（４）との間の接続が適正な場合に、スワップアウトされる前記セカンドキー（７）とスワップアウトされる前記サードキーとが用いられる

ことを特徴とするシステム。

【請求項３１】

前記セカンドキー（７）は、データ（９，１０）と共にアーカイブステーション（４）へ転送され、及び／又は、データ（９，１０）と共にセキュリティ手段（２）にフィードバック転送される、請求項３０記載のシステム。

【請求項３２】

組合わせキー（５）が前記ファーストキーとセカンドキー並びにサードキー（６，７，８）とから形成され、暗号化と復号化が各ケース毎に当該組合わせキー（５）を用いて実行される、請求項３０または３１記載のシステム。

【請求項３３】

対称性の暗号化アルゴリズムが暗号化と復号化において使用され、３ＤＥＳ、ＩＤＥＡ、ｂｌｏｗｆｉｓｈ方式のアルゴリズムが用いられる、請求項３０から３２いずれか１項記載のシステム。

【請求項３４】

前記ファーストキー（６）及び／又はセカンドキー（７）及び／又はサードキー（８）が、各ケースにおいて少なくとも１００ビットの長さを有している、請求項３０から３３いずれか１項記載のシステム。

【請求項３５】

前記ファーストキー（６）及び／又はセカンドキー（７）及び／又はサードキー（８）

は、各ケースにおいて少なくとも１０２４ビット、２０４８ビット及び／又は４０９６ビットの長さを有している、請求項３０から３４いずれか１項記載のシステム。

【請求項３６】

前記ファーストキー（６）は、セキュリティ手段（２）の生成動作若しくは初期動作の間に乱数発生器を用いて生成され記憶される、請求項３０から３５いずれか１項記載のシステム。

【請求項３７】

セキュリティ手段（２）は、ファーストキー（６）が他のユニットに対して転送不可能でかつ読み出し不可能であるように設計されている、請求項３０から３６いずれか１項記載のシステム。

【請求項３８】

データ（９，１０）の記憶前に、各ケースにおいてセカンドキー（７）及び／又はサードキー（８）が新たに生成され、この場合乱数発生器が用いられている、請求項３０から３７いずれか１項記載のシステム。

【請求項３９】

前記セカンドキー（７）及び／又はサードキー（８）が、セキュリティ手段（２）によって生成されている、請求項３０から３８いずれか１項記載のシステム。

【請求項４０】

前記クライアントステーション（１）とセキュリティ手段（２）の間の通信は、ネットワーク（１８）を介して行われている、請求項３０から３９いずれか１項記載のシステム。

【請求項４１】

前記セキュリティ手段（２）とアーカイブステーション（４）の間の通信は、ネットワーク（３）を介して行われている、請求項３０から４０いずれか１項記載のシステム。

【請求項４２】

前記ネットワーク（３）はイーサーネット規格に準拠するものであり、及び／又は、仮想プライベートネットワーク及び／又はリモートアクセスサービスＲＡＳによるリモートアクセス用に設計されている、請求項４１記載のシステム。

【請求項４３】

前記セキュリティ手段（２）は、物理的ユニットである請求項３０から４２いずれか１項記載のシステム。

【請求項４４】

前記セキュリティ手段（２）は、ＰＣカード若しくはＵＳＢデバイスである請求項３０から４２いずれか１項記載のシステム。

【請求項４５】

データ（９，１０）は１つ又は複数のファイルの形態で転送されて記憶される、請求項３０から４４いずれか１項記載のシステム。

【請求項４６】

前記セカンドキー（７）は複数のファイルのヘッダ部分で、又は複数のファイルのうちの１つのヘッダ部分でアーカイブステーション（４）に転送される、請求項４５記載のシステム。

【請求項４７】

別個のセカンドキー（７）と一緒に転送された複数のファイルの各々毎若しくは複数のファイルの各グループ毎に、及び／又は、別個のサードキー（８）が生成される、請求項４５または４６記載のシステム。

【請求項４８】

さらに複数のクライアントステーション（１）が設けられている、請求項３０から４７いずれか１項記載のシステム。

【請求項４９】

データ（９，１０）がアーカイブステーション（４）からクライアントステーション（

１）へ転送される前に、クライアントステーション（１）がデータ（９，１０）の受信に対して認証されているかどうかがチェックされ、クライアントステーション（１）が認証されている場合にのみ転送が実行される、請求項３０から４８いずれか１項記載のシステム。

【請求項５０】

クライアントステーション（１）がデータ（９，１０）の受信に対して認証されているかどうかのチェックの際にデータリクエスト送信側のＩＳＤＮナンバー及び／又はＩＰアドレスがチェックされる、請求項４９記載のシステム。

【請求項５１】

アーカイブステーション（４）からのデータ（９，１０）検索に対する認証が、必要に応じてリモートアクセスからのアーカイブステーション（４）上のデータ（９，１０）に所属するセカンドキー（７）の引き抜きによって不能にされる、請求項３０から５０いずれか１項記載のシステム。

【請求項５２】

アーカイブステーション（４）からのデータ（９，１０）検索に対する認証が、必要に応じてリモートアクセスからのアーカイブステーション（４）上のデータ（９，１０）に所属するセカンドキー（７）の消去か又はスワップアウトと消去によって不能にされる、請求項３０から５０いずれか１項記載のシステム。

【請求項５３】

前記アーカイブステーション（４）が第１及び第２のサーバーコンピュータで構成され、この場合第１のサーバーコンピュータはデータ（９，１０）の記憶のために設けられ、第２のサーバーコンピュータは１つ又は複数のセカンドキーの記憶のために設けられている、請求項３０から５２いずれか１項記載のシステム。

【請求項５４】

１つのセカンドキー又は複数のセカンドキーが、アーカイブステーション（４）上に記憶されて暗号化され、及び／又はハードウエアモジュール若しくはアダプターに記憶される、請求項３０から５３いずれか１項記載のシステム。

【請求項５５】

アーカイブステーション（４）のデータ（９，１０）及び／又は１つのセカンドキー又は複数のセカンドキー（７）が、データバックアップのためにストレージユニット（１４）にコピーされる、請求項３０から５４いずれか１項記載のシステム。

【請求項５６】

アーカイブステーション（４）のデータ（９，１０）及び／又は１つ又は複数のセカンドキー（７）が、データバックアップのためにテープデッキやＣＤ、ＤＶＤ、ディスクアレイにコピーされる、請求項３０から５４いずれか１項記載のシステム。

【請求項５７】

前記アーカイブステーション（４）は機密保護された空間に配設される、請求項３０から５６いずれか１項記載のシステム。

【請求項５８】

前記アーカイブステーション（４）はバンカーや地下シェルターに配設される、請求項３０から５６いずれか１項記載のシステム。

【発明の詳細な説明】

【技術分野】

【０００１】

関連出願の相互参照

本件出願は２００４年７月１日付で出願された欧州特許出願 04 015 475.9 号明細書の優先権を主張するものであり、ここではこの出願の開示内容が参照として組み込まれている。

【０００２】

本発明は独立請求項の上位概念による自動暗号化及び復号化を伴うデータアーカイビン

グのための方法に関している。また本発明は独立請求項上位概念による自動暗号化及び復号化を伴うデータアーカイビングのためのシステム及びセキュリティ手段に関している。

【０００３】

本願発明において用語"アーカイビング"とは、アーカイブにおける記憶もアーカイブからの検索（回復）も含むものと理解されたい。

【０００４】

背景技術

この種の方法及びシステムは、アーカイブステーション上の１つ又は複数のクライアントステーションのデータアーカイビングの役に立つ。中央アーカイブステーション上のデータのアーカイビングは、データ紛失やデータ盗聴に関するセキュリティ向上の利点を有している。このアーカイブステーションは、クライアントステーションやワークステーションにおいて常に実行可能ではない特別に保護されたルーム内に設置され得る。さらに標準ベースのアーカイブステーションの記憶データのバックアップコピーは複数のクライアントステーションの場合よりも容易である。

【０００５】

しかしながら集中的なアーカイビングは、クライアントステーションとアーカイブステーションの間のデータの転送と、異なる顧客若しくはユーザーのアーカイブステーション占有の要求が伴う。このことは特別なセキュリティの準備を要求する。この目的のために、クライアントステーションのデータをアーカイブステーションへの転送前に暗号化し、そしてアーカイブステーションからの返送の後で再び復号化することが公知である。例えばスマートカードに対する暗号化、いわゆる"トークン"では、キーが記憶されてパスワードで保護されて使用される。

【０００６】

パスワードはそれらが忘れられたり、ユーザーによって書き換えられるか書き留められ、盗まれたりする危険性がある。同じようなことは暗号化のハードウエアやソフトウエアにも当てはまる。また少なくとも再現のために必要な文書が盗まれる可能性もある。
それゆえハッカーにとってはしばしばアーカイブデータへのアクセスが比較的容易となる。さらなる弱点はクライアントステーションやアーカイブステーションである。なぜならそれらは基本的に複数のセキュリティホールを有しているからである。さらに周知のシステムでは導入と利用、すなわち特にデータのアーカイビングに対してしばしば多数のユーザーインタラクションを要し、このことは作業時間の浪費と障害頻度を高めてしまう。ユーザーにとっての使い易さと信頼性及び安全性の要求は、周知のシステムでは不完全か若しくは偏った形でしか達成することができない。

【０００７】

国際特許出願公開パンフレット第２００４/０４６８９９号明細書にはパソコン上でＭＰ３プレイヤの音楽データを記憶するための方法が開示されている。このドキュメントはデータヘッダ内のシードの利用と、データの識別に用いられるヘッダ内に記憶されている、キーではない数字の利用とに言及している。データとシードの別個の記憶動作は行われない。ソースと最終ロケーションには暗号化データは含まれず、そのため暗号化は転送のためにだけ使用される。キーは各転送毎に新たに生成され、データと平行して記憶される。キーは定数と変数の２つの部分を有している。変数は転送毎に生成され、データのヘッダ内で転送されるが、キーは転送されない。受信機はヘッダから変数を受取り、この変数と定数からキーを生成する。データが最終ロケーションに到達した場合には、それらは暗号化されず複数回の使用が可能である。クライアント局から物理的に離れている暗号化のための別個の手段は存在せず、プレイヤが盗まれた場合の保存データを保護する方法はドキュメントによって定められていない。欠陥のある若しくは盗まれたデバイスを置換えるためのすべを示している手法はない。

【０００８】

米国特許出願 US 5 940 507 A 明細書には、ソースが非暗号化データを含み宛先は暗号化データを含んでいる方法が開示されている。ソースのトランスミッタは、それ自体が暗

号化されているキーを用いてデータを暗号化する。安全な場所で暗号化されたデータと暗号化されたキーは平行して記憶される。第三者がこの安全な場所から記憶されているデータの読み出しを望む場合には、トランスミッタによってしか与えられない認証キーを必要とする。この特別なキーを用いることによって最初に暗号化されたキーが復号化され、その後でこのキーを用いてデータが復号化される。しかしながらここでは第３のキーもなければ安全な場所からの最初のキーの読み出しに対する防護策も存在していない。

【０００９】

発明の開示

発明が解決しようとする課題

それゆえに本発明の課題は前述してきた従来技術の欠点に鑑みこれを解消すべく改善を行うことである。

【００１０】

課題を解決するための手段

前記課題は独立請求項の特徴部分に記載された本発明によって解決される。

【００１１】

本発明による解決手段では従来のようなパスワードの要求がなされないという利点を有している。セキュリティ手段が盗難された場合の記憶データへの不正なアクセスは、セカンドキーのスワップアウトを阻止することによって防御される。

【００１２】

発明を実施するための最良の形態

本発明による方法及びシステムでは、ソース（クライアント）は暗号化されていないデータを含み、最終ロケーション（サーバー）は暗号化されたデータだけを含む。データはソース（クライアント）から最終ロケーション（サーバー）への転送過程で暗号化されまたその逆方向でも暗号化される。セキュリティ手段、有利には別個の物理ユニットがキーのハンドリングを要する。最初のステップ（システムコンフィグレーション）ではユーザーはパスワード若しくは保護証明を入力する。このパスワード若しくは保護証明はセキュリティデバイス又はセキュリティ手段によって少なくとも２つ、有利には３つの、パートないしフラグメントないしキーへの断片化がなされる。これらのフラグメントの分析ではパスワードないし保護照明のみを導き出すことはできない。フラグメント自体は、単独の機能要素ではなく従って古典的な意味での"鍵"ではなく、単独では使用できない。それにもかかわらず暗号化処理としてのいわゆる"キー"ないし"キーフラグメント"の表現は、複数のパーツないしフラグメントに対しても同じように使われる。フラグメント自体は暗号化可能である。ソースは最終ロケーションに接続されキーフラグメントがディスパッチされる。１つのフラグメントは最終ロケーションに平行して記憶され、１つのフラグメントはソースと平行して記憶され、さらに任意に第３のフラグメントがセキュリティ手段ないしセキュリティボックスのセキュリティ部分にそれぞれ記憶される。断片化は結果としてソースから最終ロケーションへの適正な接続がなされた場合にしかディスパッチされたフラグメントが読み出せないようにしている。本来のものではないコネクション、あるいは不正操作によるコネクションはそのつど検出され、フラグメントの読み出しがブロックされる。ソース及び／又は最終ロケーションがセキュリティ手段によって到達できなかった場合には、フラグメントの読み出しは不可能である。その場合にはセキュリティ手段はサービスを拒絶する。セキュリティデバイスないしはセキュリティ手段に任意に記憶されている第３のフラグメントは、盗難にあった時はそれぞれ一方においてはセキュリティ手段の不正操作に対する保護のために用いられ、さらに最終ロケーションへのソースの適正なコネクションのさらなるコントロールのためにも使用される。本発明による方法及びシステムの通常のサービス期間の間は複数のデータがソースから最終ロケーションへセキュリティ手段を介して転送され、それによって暗号化され、さらに反対方向に復号化される。この暗号化／復号化に要するキーは、それらのフラグメントの異なるロケーションから、複数のフラグメントと共に予めフラグメントの形態で集められる。このことはデータの各転送毎に（すなわちソースから最終ロケーション及び最終ロケーションからソース）毎回

改められて行われる。ソースのデータは最終ロケーションへの転送の後で消去され、それによって最終ロケーション内で暗号化されたデータだけが、ソースから最終ロケーションへのコネクションが適正に確立された場合にアクセス可能となり、アウトソーシングないしディスパッチされたフラグメントが共に再び適正で完全なキーを形成する。

【００１３】

従来技術と比較して本発明及びその有利な実施例は次のようなセキュリティ手段、有利には物理的に独立したボックスとして、ソースから最終ロケーションへのデータ転送に必要なセキュリティ手段を提供している。このセキュリティ手段はそれを通過するデータの暗号化と復号化を実施する。セキュリティ手段はパスワード/証明書を断片化し、フラグメントをディスパッチ／アウトソーシングする（ソース及び最終ロケーション内並びに任意にセキュリティ手段自身で）。セキュリティ手段は、ソースと最終ロケーションのコネクションの妥当性と安全性をディスパッチ／アウトソーシングされたフラグメントのチェックによって検査する。セキュリティ手段は任意にそこに記憶されている第３のフラグメントによって自身の妥当性も検査する。複数の単独フラグメント自体は高度なセキュリティを達成するのに機能的ではなくまた全てのフラグメントの所有すら暗号化／復号化のために十分ではないので、セキュリティ手段は複数のフラグメントからのリフラグメンテーションと機能キーの形成を求める。データヘッドに記憶されるキーのパートは存在しない。

【００１４】

本発明による方法及びシステム並びにセキュリティ手段とそれらの有利な実施例はセキュリティとコントロールの利点を有している。ソースと最終ロケーションの間のパスは保護されている。セキュリティ手段の盗難と別の物理的な場所での操作が検出されるとそれは拒絶できる。フラグメントのディスパッチ／アウトソーシングによってユーザーはソースと最終ロケーションのどちら側でも各フラグメントのブロックないしは分離によっていつでも操作を中断することができる。２つから３つのフラグメントの完全な復元によってしか適正なキーは得られない。セキュリティボックス内のフラグメントはセキュリティ手段内部の"インテリジェンス度"を検査する。本発明においては、暗号化に対して任意のアルゴリズムを用いることが可能である。キーは任意の長さを有することができ、また任意の長さのパスワードも処理することができる。

【００１５】

図面の説明

本発明のさらなる構成および利点は、従属請求項並びに図面を参照した以下の詳細な説明から明らかとなる。これらの図面において

図１は、本発明による方法に基づいたデータアーカイビングのためのシステムの有利な実施例のブロック回路図であり、

図２ａは図１のシステムにおいて実行されるデータ記憶のための方法のフローチャートであり、

図２ｂは図１のシステムにおいて実行されるデータの検索のための方法のフローチャートであり、

図３は、本発明による方法に基づいたデータアーカイビングのためのシステムの別の有利な実施例のブロック回路図であり、

図４ａは図３のシステムにおいて実行されるデータ記憶のための方法のフローチャートであり、

図４ｂは図３のシステムにおいて実行されるデータ検索のための方法のフローチャートである。

【実施例】

【００１６】

図１は、本発明の方法に基づいたデータ９，１０のアーカイビングのためのシステムの有利な実施例のブロック回路図である。種々の、ここでは例として２つのクライアントステーション１が設けられている。これらのクライアントステーション１には、プレーンデ

ータ、すなわちまだ暗号化されていないデータ９が記憶されている。さらに各クライアントステーション１毎にセキュリティ手段２が設けられている。このセキュリティ手段２はデータ９，１０の暗号化と復号化に使用される。このことのためにセキュリティ手段は少なくともファーストキー６と一時的なセカンドキー７若しくはフラグメント６，７を含んでいる。セキュリティ手段２はアーカイブステーション４とネットワーク３を介して通信される。アーカイブステーション４には暗号化されたデータ１０がデータストレージ１１に記憶されている。さらに個々のケースにおいて暗号化されたデータ１０に帰属する複数のセカンドキー７がキーストレージ１２に記憶されている。

【００１７】

データ９．１０はプレーンデータ９ないし暗号化されたデータ１０として実行され、それぞれ記憶されるか及び／又は転送される。本願明細書において用語「データ」が、「プレーン」や「暗号化」等の属性を伴わずに使われた場合には、データの情報内容が暗号化状態にかかわらないことを意味する。個々のプレーンデータ９に属する暗号化されたデータ１０は、この解釈に従って同じデータ９，１０を指示する。参照番号９と１０の組合わせは、個々の状況においてどちらか一方のみが表記されたとしてもこれらのデータ９，１０がプレーンと暗号化の両方で実行可能であることを包括的に意味するものと理解されたい。

【００１８】

以下では例えば共に連続的に実行される本発明によるデータアーカイビング方法の実施例を図２ａと図２ｂに基づいて説明する。この実施例では２つのキー６と７を用いた暗号化がベースになっている。

【００１９】

図２ａには、図１のシステムにおいて実行されるデータ９，１０の記憶方法がフローチャートで表されている。アーカイビング期間中最初にプレーンデータ９はクライアントステーション１からセキュリティ手段２に転送される。セキュリティ手段２は、その後で新たなセカンドキーを生成する（若しくは先行する時点で既に生成されている）。プレーンデータ９はセキュリティ手段２によって暗号化され、少なくともファーストキー６ないしフラグメント６とセカンドキー７を用いてそれぞれ暗号化され、その後で暗号化されたデータ１０としてアーカイブステーション４（最終ロケーション）に転送される。セカンドキー７ないしフラグメント７はそれぞれアーカイブステーション４に転送され、局所的に消去される（例えばセキュリティ手段内で）。セカンドキー７の転送は例えばファイルのヘッダ内で、暗号化されたデータ１０と共に実施されてもよい。

【００２０】

図２ｂは図１のシステムにおいて実行されるデータ９，１０の検索のための方法のフローチャートを示している。最初にクライアントステーション１が最終ロケーションの代わりにソースを受け取るアーカイブステーション２にデータ９，１０を要求する。要求されたデータ９，１０は暗号化されたデータ１０としてアーカイブステーション４によってそれらに属するセカンドキー７と共にセキュリティ手段２へ転送され、セキュリティ手段２はそれらをファーストキー６とセカンドキー７を用いて復号化し、その後でプレーンデータ９としてクライアントステーション１へ転送する。その後でセカンドキー７は再びセキュリティ手段２において消去される。

【００２１】

図３は、本発明による方法に基づいたデータ９，１０のアーカイビングのためのシステムのさらに有利な実施例のブロック回路図である。ここでは図１のシステムとは対称的にサードキー８が設けられている。各ケース毎に、暗号化と復号化の間ではこのサードキー８がクライアントステーション１との間で交換される。この目的のためにクライアントステーション１は有利にはキー記憶装置１３を含んでいる。さらに例えば３つの異なるコネクション構成１５，１６，１７が、クライアントステーション１とそれに属するセキュリティ手段２毎に示されている。第１の構成１５は図１の解決手段に相当する。セキュリティ手段２はクライアントステーション１とアーカイブステーション４の間に接続されてい

る。第２の構成１６ではクライアントステーション１が直接ネットワーク３に接続されている。セキュリティ手段２はクライアントステーション１に接続され、それを介してアーカイブステーション４と間接的に通信している。第３の構成１７ではクライアントステーション１がセキュリティ手段２とローカルネットワーク３を介して接続されている。

【００２２】

以下の明細書で図４ａと図４ｂに基づき説明される方法は共に（すなわち連続的に実行されるべく）本発明によるデータアーカイビングのための方法のさらなる実施例をなしている。この実施例は３つのキー６，７，８を用いた暗号化をベースにしている。

【００２３】

図４ａは図３のシステムにおいて実行されるデータ９，１０の記憶のための方法のフローチャートを示している。アーカイビングにおいてはプレーンデータ９がクライアントステーション１からセキュリティ手段２へ転送される。セキュリティ手段２は、その後で新たなセカンドキー７と新たなサードキー８を生成する（若しくは既に先行する時点において生成されている）。セキュリティ手段２は、プレーンデータ９を少なくともファーストキー６とセカンドキー７とサードキー８を用いて暗号化し、それらをアーカイブステーション４に転送する。つまりセカンドキー７もアーカイブステーション４に転送される。サードキー８はクライアントステーション１に転送される。その後でセキュリティ手段２におけるセカンドキー７並びにサードキー８が局所的に消去される。セカンドキー７の転送は例えばファイルのヘッダ内でデータ９，１０と一緒に実行されてもよい。

【００２４】

図４ｂは図３のシステムにおいて実行されるデータ９，１０の検索のための方法のフローチャートを示している。クライアントステーション１はサードキー８をセキュリティ手段２に転送する。その後で若しくは同時にアーカイブステーションにてデータ９，１０が要求される。

要求されたデータ９，１０は暗号化されたデータ１０としてアーカイブステーション４からセキュリティ手段２へそれらに属するセカンドキー７と共に転送され、セキュリティ手段２はそれらを３つのキー６，７，８を用いて復号化し、その後でそれらをプレーンデータ９としてクライアントステーション１へ転送する。その後でセキュリティ手段２においてセカンドキー７及びサードキー８が消去される。

【００２５】

本発明による方法の可能な実施例全体に係る以下に記載する変化実施例と補足説明は、特に図１、図２ａ、図２ｂによる２つのキーを用いた実施例のみでなく、図３、図４ａ、図４ｂによる３つのキーを用いた実施例にも当てはまる。

【００２６】

暗号化に対しては有利には対称的暗号化アルゴリズム、例えば"３ＤＥＳ"，"ＩＤＥＡ"，"blowfish"方式のアルゴリズムが使用されている。複数のキーを用いた暗号化に対しては多重方式の暗号化が実施されるか若しくは複数のキーが組み合わされた相応の長さの組み合わせキー５を用いた暗号化が実施される。

キー６，７（場合によっては８も）の長さは例えば１０２４/２０４８/４０９６ビットであってもよい。各キー６，７（場合によっては８も）毎の機密保護機能に対しては少なくとも１００ビットの長さを持たせる。

【００２７】

ファーストキー６は有利には定数であり、有利には乱数発生器を用いて生成され、セキュリティ手段２の製造中若しくは初期動作中に記憶される。ファーストキー６のコピーは、システムの外部で例えばアーカイブステーションの操作者によって安全に保管することも可能である。これはセキュリティ手段２が破損や故障した場合の交換デバイスと共に量産できるようにするためである。セキュリティ手段２は有利には次のように設計される。すなわちファーストキー６が記憶は可能であるが、検索は不可能か若しくは一度だけしか検索できないように設計仕様される。それは一種の"デバイスキー"か"プライベートキー"であるがしかしながらその意味ではそれに対する相応の"公開鍵"は存在しない。

【００２８】
セカンドキー７は有利には、各データがアーカイビングされる前に有利にはセキュリティ手段２において乱数発生器を用いて生成される。そのような中で、一度のアーカイビングで転送されたすなわちほぼ一緒に転送された全てのデータないしファイルは、同じセカンドキー７を用いて暗号化される。しかしながら各ケースに応じて、各ファイル毎若しくはファイルグループ毎に、使用後のスワップアウトのために新たなセカンドキー７を生成することも可能である。さらに例えばアーカイブステーションに対してスワップアウトされ、各々のケースにおいてセキュリティ手段２に転送される、ただ１つの一定のセカンドキー７を設けることも可能である。図１及び図３の実施例においてはセカンドキー７がアーカイブステーション４に対してスワップアウトされてそこに転送され、さらにそこから暗号化されたデータ１０と共にフィードバックされている。この状況においてセカンドキー７はその機能に基づいていわゆる"データ附属キー"と称される。

【００２９】
サードキー８には、有利には各データのアーカイビング前に乱数発生器を用いてセキュリティ手段２内で新たに生成されるキーが使用される。このプロセスでは、一緒に転送された各ファイル毎若しくは各ファイルグループ毎に新たなサードキー８がそれぞれのケースにおいて生成されてもよい。図３の実施例ではサードキー８がクライアントステーション１に対してスワップアウトされる。アーカイブからのデータの検索のために、このサードキー８はセキュリティ手段２にフィードバックされる。この状況においてはその機能に基づいてこれはいわゆる"データ検索キー"とも称される。

【００３０】
データが複数回アーカイブされ、さらにセカンドキー７と場合によってはサードキー８がそれぞれのケースにおいて新たに生成される。ここでは複数のセカンドキー７と場合によってはサードキー８が存在する。

【００３１】
セキュリティ手段２と、場合によってはクライアントステーション１並びにアーカイブステーション４との間の通信は有利にはネットワーク３を介して行われる。このネットワークは特に"リモートデータアーカイビング"が可能なワイドエリアネットワーク、すなわちＷＡＮである。ネットワーク３は有利には公共のデータネットワーク、例えばインターネットであってもよい。さらにそれはイーサーネット規格に準拠するものであってもよいし、及び／又は仮想プライベートネットワーク及び／又はリモートアクセスサービスＲＡＳによるリモートアクセスに合わせて設計されたものであってもよい。

【００３２】
クライアントステーション１とセキュリティ手段２の間の通信、及びセキュリティ手段２とアーカイブステーション４の間の通信は、有利な実施例によれば同じネットワークを介して行われる。

【００３３】
セキュリティ手段２は有利には物理的ユニットである。またそれはネットワーク及び／又はコンピュータに対するコネクタを備えた"ボックス"であってもよい。例えばそれはＰＣカード、すなわちＰＣＭＣＩＡ（personal computer memory card international association）ソケットを備えたコンピュータ用のクレジットカードサイズの拡張ボードか若しくはＵＳＢデバイス、すなわちＵＳＢ（universal serial bus）規格に準拠したデバイスであってもよい。

【００３４】
クライアントステーション１上のブランクデータ９は有利には１つのファイルの形態であってもよいし複数のファイルの形態であってもよい。

【００３５】
クライアントステーション１は通常はクライアントコンピュータである。しかしながらそれはサーバーコンピュータ若しくは組み込まれたシステムであってもよい。本発明による方法は、１つのクライアントステーション１のみで実行可能であるが、しかしながら多

くのケースでは複数のクライアントステーション１が設けられている。クライアントステーション１はハードウエアとソフトウエアに関して異なっていてもよい。本発明の有利な実施例によれば、クライアントステーション１とアーカイブステーション４が同じコンピュータである。特にクライアントステーション１が複数存在する場合には、クライアントステーション１若しくはそのセキュリティ手段２がリクエストデータと所属のセカンドキー７の受信に対して認証されているかどうかをアーカイブステーション４によってチェックすることが重要である。転送はそのような認証が行われている場合に限って実行される。このプロセスではとりわけデータ要求側の送信アドレス、すなわちＩＳＤＮナンバー、IPアドレス及び／又はクライアントステーション１の署名及び／又は所属するセキュリティ手段２の署名などがチェックされる。

【００３６】

アーカイブステーション４は通常は１つのサーバーか又は複数のサーバーからなり、詳細にはサービスを提供するコンピュータである。具体的に例えば第１のサーバーと第２のサーバーが設けられている場合には、第１のサーバーには暗号化されたデータ１０が記憶され、それに所属するセカンドキー７は第２のサーバーに記憶される。しかしながらセカンドキー７は、１つ若しくは複数の特定のハードウエアモジュール、詳細にはＰＣＩアダプターに記憶させることも可能である。このオプションでは、アーカイブステーション４上の暗号化データのブロッキングに対して単にハードウエアモジュールを外すだけでよいという簡素な利点を有する。さらにセカンドキー７は暗号化してアーカイブステーション４に記憶させてもよい。更に付加的にアーカイブステーション４は有利には記憶されたデータ、すなわち暗号化されたデータ１０及び／又はセカンドキー７のバックアップのために冗長的なデータ記憶のためのストレージユニット１４、すなわちバックアップシステム、詳細にはテープデッキやディスクアレイあるいはＣＤ/ＤＶＤライターを含み得る。アーカイブステーション４に記憶されているデータは有利には規則的な間隔で（例えば毎日）ストレージユニット１４にセーブされる。このアーカイブステーション４は有利には機密保護された空間、例えばバンカーや地下シェルターに配設される。

【００３７】

例えばセキュリティ手段２が盗まれてしまった場合には、この盗難したセキュリティ手段２を介したアーカイブステーション４の暗号化データ１０へのアクセスは阻止されなければならない。そのような暗号化データ１０への不正アクセスの阻止は有利には１つ又は複数のセカンドキー７をシステムから分離することで実行できる。例えば前述したようにハードウエアモジュールとして記憶されているキーの取り外しやデータ担体へのセカンドキー７のコピーと同時にアーカイブステーション４からの消去によって実行できる。これにより暗号化データ１０は検索はできるがそれを復号化することはできない。セカンドキー７の保護解除に対してはそれをアーカイブステーション４に再びコピーし直すことでできる。この一連の手順は数ある中でもデータへの不正アクセスの阻止と解除がオペレーティングシステムの専用の機能を使うことなく容易にできる利点を有している（システムのセキュリティ機能は大抵の場合認証ができない）。

【００３８】

３つのキー６，７，８を有している本発明の実施例においては、暗号化されたデータ１０への不正アクセスの阻止が代替的にアーカイブステーション４内のセカンドキー７の消去若しくはクライアントステーション１内のサードキー８の消去あるいはその両方の実行によってできる。

【００３９】

システムからのキーの消去若しくは分離が前述したように実施された場合には、それはデータが実際に物理的に消去されたことを意味し、一時ファイルや復元ファイルの形では残らない。さらに転送パスはメモリを有さない、すなわち中継局やネットワークノードに例えばバッファリングのために記憶された情報は転送後に消去され得る。

【００４０】

図２ａ、図２ｂ及び図４ａ、図４ｂに基づいて説明してきた前記実施例では、セキュリ

ティ手段２による信号の受信、暗号化/復号化及び転送が例示的に別個の形で順次連続した方法ステップで説明されている。しかしながら当該分野の当業者にとってはこれらのステップが同時にまた実行可能であることはあきらかである。その場合にはこれらのデータはデータストリームとして処理される。そのような実施例の利点は一方では高速になることであり、他方では同じキーセットに所属する全てのデータ９，１０がセキュリティ手段２に同時にバッファされなくてもよいことである。

【００４１】

本発明による前述の実施例では、各ケース毎に少なくともファーストキー６とセカンドキー７が設けられ、そのうちのファーストキー６は"デバイスキー"若しくは"プライベートキー"であってスワップアウトされない。従ってこのファーストキー６は、セキュリティアルゴリズム、あるいは秘匿パラメータによって変調されたアルゴリズムがその代替として使用される場合には省略できる。

【００４２】

本発明による方法を実行するためのシステムは有利には次のように構成される。すなわちデータの暗号化がバックグラウンドにおいて全て自動で実施され、ユーザー入力、とりわけパスワード入力は不要となるように構成される。

【図面の簡単な説明】

【００４３】

【図１】本発明による方法に基づいたデータアーカイビングのためのシステムの有利な実施例のブロック回路図

【図２ａ】図１のシステムにおいて実行されるデータ記憶のための方法のフローチャート

【図２ｂ】図１のシステムにおいて実行されるデータ検索のための方法のフローチャート

【図３】本発明による方法に基づいたデータアーカイビングのためのシステムの有利な実施例のブロック回路図

【図４ａ】図３のシステムにおいて実行されるデータ記憶のための方法のフローチャート

【図４ｂ】図３のシステムにおいて実行されるデータ検索のための方法のフローチャート

【図１】

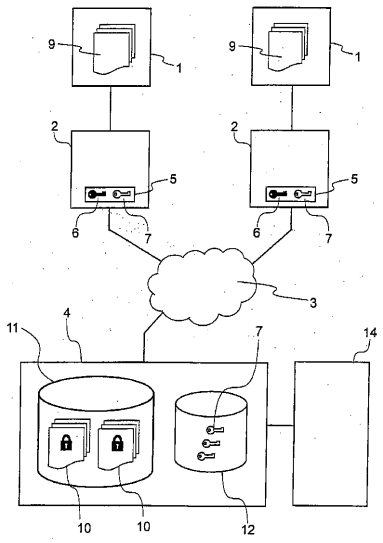
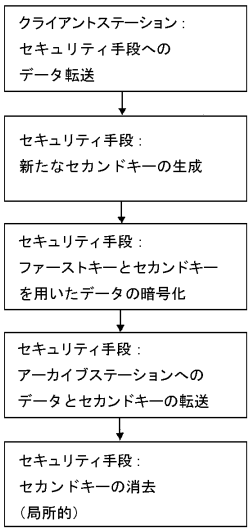
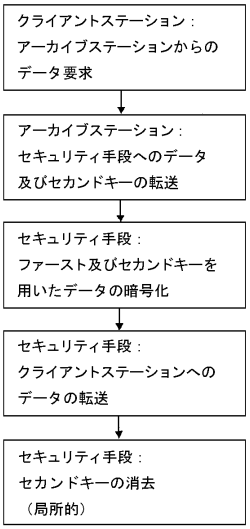


Fig. 1

【図２ａ】



【図２ｂ】



【図３】

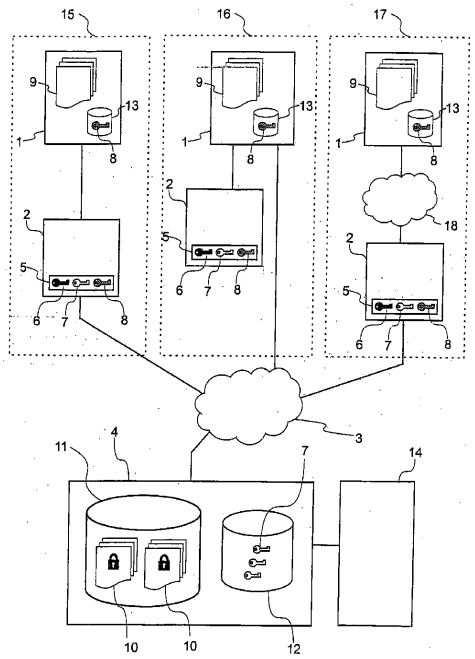
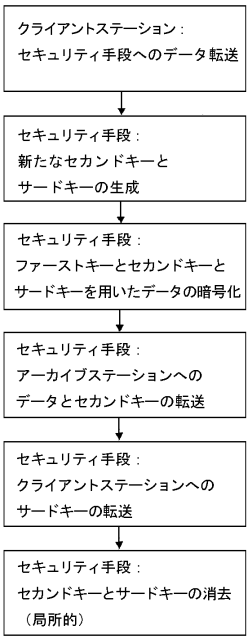
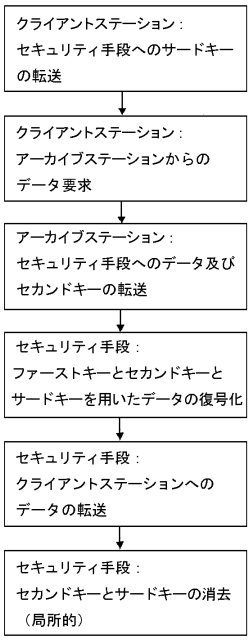


Fig. 3

【図４ａ】


クライアントステーション：
セキュリティ手段へのデータ転送
セキュリティ手段：
新たなセカンドキーと
サードキーの生成
セキュリティ手段：
ファーストキーとセカンドキーと
サードキーを用いたデータの暗号化
セキュリティ手段：
アーカイブステーションへの
データとセカンドキーの転送
セキュリティ手段：
クライアントステーションへの
サードキーの転送
セキュリティ手段：
セカンドキーとサードキーの消去
（局所的）

【図４ｂ】


クライアントステーション：
セキュリティ手段へのサードキー
の転送
クライアントステーション：
アーカイブステーションからの
データ要求
アーカイブステーション：
セキュリティ手段へのデータ及び
セカンドキーの転送
セキュリティ手段：
ファーストキーとセカンドキーと
サードキーを用いたデータの復号化
セキュリティ手段：
クライアントステーションへの
データの転送
セキュリティ手段：
セカンドキーとサードキーの消去
（局所的）

フロントページの続き

(72)発明者　ブルーノ　ルドルフ　ケーツマン
スイス国　シュタインハウゼン　マッテンシュトラーセ　４８

審査官　青木　重徳

(56)参考文献　国際公開第２００４／０４６８９９（WO，Ａ１）
特表２００１－５０８６２７（ＪＰ，Ａ）
特開平０２－１１０４９１（ＪＰ，Ａ）
特開２００２－１５７１６７（ＪＰ，Ａ）
特表２００１－５１４８３４（ＪＰ，Ａ）
特開平１０－２７１１０４（ＪＰ，Ａ）
特開２００２－１８５４４３（ＪＰ，Ａ）
特開平０３－２６１９８７（ＪＰ，Ａ）
柴田陽一，中村逸一，曽我正和，田窪昭夫，西垣正勝，“メカニズムベースＰＫＩ”，コンピュータセキュリティシンポジウム２００３，日本，社団法人情報処理学会，２００３年１０月２９日，第２００３巻，第１５号，ｐ．１８１－１８６

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L　9/08
G06F　21/20
G06F　21/24