【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成22年3月11日(2010.3.11)

【公表番号】特表2009-524153(P2009-524153A)
【公表日】平成21年6月25日(2009.6.25)
【年通号数】公開・登録公報2009-025
【出願番号】特願2008-551455(P2008-551455)
【国際特許分類】
Ｇ０６Ｆ　21/24　　(2006.01)
Ｇ０９Ｃ　 1/00　　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　12/14　　５６０Ａ
Ｇ０６Ｆ　12/14　　５４０Ａ
Ｇ０９Ｃ　 1/00　　６６０Ｄ

【手続補正書】
【提出日】平成22年1月18日(2010.1.18)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
アーカイブ・セッションを構成するデータ・セグメントがアーカイブ・アプリケーションとアーカイブ装置との間でストリームされる、多数のセキュリティ保護されたデータ・アクセスを受けるデータをアーカイビングするための方法であって、
ａ）所定のアーカイブ・セッション・ストリームから所定のアクセス制御群の識別子を抽出する
ステップを含み、前記所定のアクセス制御群は予め定義された暗号化キーの組を各々が含む複数の識別可能なアクセス制御群の１つであり、前記識別子は前記アーカイブ・アプリケーション及び前記アーカイブ装置に関して機能的に透明な前記所定のアーカイブ・セッション・ストリームに埋め込まれており、
ｂ）前記所定のアクセス制御群にアクセスして、前記所定のアクセス制御群内に含まれる所定の暗号化キーを取得し、
ｃ）前記所定の暗号化キーを前記アーカイブ・アプリケーションと前記アーカイブ装置との間に与えられる暗号化エンジンに適用し、
ｄ）前記所定のアーカイブ・セッション・ストリームを前記暗号化エンジンにより処理する、
ステップを含むことを特徴とする方法。
【請求項２】
前記アクセスするステップは、前記所定のアクセス制御群に含まれる前記予め定義された暗号化キーの組を評価して、前記所定の暗号化キーの選択を安全に有効にするステップを含むことを特徴とする請求項１に記載の方法。
【請求項３】
前記処理するステップは、前記所定のアーカイブ・セッション・ストリームの所定の暗号化データ・セグメントに関して、前記所定の暗号化キーを用いて、前記暗号化データ・セグメントからのセグメント暗号化キーを暗号化解除する第１のステップと、前記セグメント暗号化キーを用いて、前記暗号化データ・セグメントからのセグメント・データを暗

号化解除する第２のステップとを含むことを特徴とする請求項２に記載の方法。
【請求項４】
前記処理するステップは、前記所定のアーカイブ・セッション・ストリームの所定のクリアテキスト・データ・セグメントに関して、
ａ）所定のセグメント暗号化キーを用いて、前記所定のクリアテキスト・データ・セグメントを暗号化して、所定の暗号化データ・セグメントを生成し、
ｂ）前記所定の暗号化キーを用いて、前記所定のセグメント暗号化キーを、前記所定のアーカイブ・セッション・ストリームにおける前記所定の暗号化データ・セグメントと関連付ける、
ステップを含むことを特徴とする請求項２に記載の方法。
【請求項５】
持続性格納媒体に連結されたセキュリティ保護された格納サーバ・コンピュータ上のシステム・コンポーネントの実行により実施されるセキュリティ保護されたデータ・アーカイビング・システムであって、
ａ）アーカイブ・セッションを制御するアーカイビング・アプリケーション
を含み、アーカイブ・データ・ストリームがアーカイブ装置と前記アーカイビング・アプリケーションとの間で転送され、前記アーカイビング・アプリケーションは、前記アーカイブ・セッションの一部としてセッション補助データの持続的な格納のために与えられるものであり、
ｂ）前記アーカイブ・データ・ストリームに関して、前記アーカイビング・アプリケーションと前記アーカイブ装置との間に置かれたデータ・セキュリティ・ドライバ
を含み、前記データ・セキュリティ・ドライバは、前記アーカイブ・データ・ストリームからの前記セッション補助データの回復、及び、前記アーカイブ・データ・ストリーム内で転送されるデータ・セグメントの選択的な暗号化処理を与えるデータ・プロセッサを含んでおり、
ｃ）前記データ・セキュリティ・ドライバに連結されて、前記セッション補助データを受信し、これに応答して、所定のポリシー管理制御に選択的に依存して、セッション暗号化キーを前記データ・セキュリティ・ドライバに与えるポリシー管理コントローラ、
を含むことを特徴とするセキュリティ保護されたデータ・アーカイビング・システム。
【請求項６】
前記セッション補助データは、前記アーカイビング・アプリケーションに関して非機能データであり、前記補助データは前記ポリシー管理コントローラにより処理されて、前記データストリーム内で転送された所定のデータ・セグメントに適用可能な暗号化キーのポリシー群を機能的に識別することを特徴とする請求項５に記載のセキュリティ保護されたアーカイビング・システム。
【請求項７】
複数の暗号化キーのポリシー群の持続的な格納を与えるセキュリティ保護されたリポジトリをさらに含み、前記複数のポリシー群の各々は、前記補助データの処理に応じて、前記ポリシー管理コントローラにより独特に識別可能であることを特徴とする請求項６に記載のセキュリティ保護されたアーカイビング・システム。
【請求項８】
前記ポリシー管理コントローラは、認証された識別子を取得するように動作し、前記認証識別子に応じて、さらに、所定の暗号化キーを前記セッション暗号化キーとして前記暗号化キーのポリシー群から選択するように動作し、前記セッション暗号化キーを前記データ・セキュリティ・ドライバに与え、前記データ・セキュリティ・ドライバは、前記セッション暗号化キーに関して、前記所定のデータ・セグメントの選択的な暗号化処理を可能にするように動作することを特徴とする請求項７に記載のセキュリティ保護されたアーカイビング・システム。
【請求項９】
前記データ・セキュリティ・ドライバは、前記セッション暗号化キーを前記所定のデー

タ・セグメントに適用することにより、前記所定のデータ・セグメントからのセグメント暗号化キーを暗号化解除するように動作することを特徴とする請求項８に記載のセキュリティ保護されたアーカイビング・システム。
【請求項１０】
前記データ・セキュリティ・ドライバは、セグメント暗号化キーを用いて、前記所定のデータ・セグメントを暗号化するように動作し、前記データ・セキュリティ・ドライバは、さらに、前記所定のセッション暗号化キーを用いて暗号化し、暗号化されたように、前記セグメント暗号化キーを前記所定のデータ・セグメントに取り付けるように動作することを特徴とする請求項８に記載のセキュリティ保護されたアーカイビング・システム。
【請求項１１】
データ・アーカイブに対するアクセスを選択的に制御するためのシステムであって、
ａ）媒体サーバ・コンピュータ・システムによりホストされ、アーカイブ・セッションとして論理的に組織化されたデータの持続的な格納を与えるアーカイブ
を含み、所定のアーカイブ・セッションは、セッション・メタデータと、第１の複数のアーカイブ・メタデータ・セグメントと、第２の複数のアーカイブ・データ・セグメントとを含み、前記アーカイブ・データ・セグメントは暗号化され、所与のアーカイブ・データ・セグメントに対して、データ・セグメント暗号化キーは、前記所与のアーカイブ・データ・セグメントに対して定められた対応を有する所与のアーカイブ・メタデータ・セグメントにおいてエンコードされ、
ｂ）暗号化キーの組を格納するセキュリティ保護されたリポジトリ・サーバ
を含み、前記セキュリティ保護されたリポジトリ・サーバは、前記暗号化キーの組の対応する１つの選択に対するポリシー識別子に応答し、
ｃ）クライアント・コンピュータ・システムによりホストされ、前記所定のアーカイブ・セッションに対するアクセスのために、前記媒体サーバ・コンピュータ・システムに連結可能なアーカイブ・データ・リーダ
を含み、前記アーカイブ・データ・リーダは、前記セッション・メタデータから取得された認証トークン及び前記ポリシー識別子を、前記セキュリティ保護されたリポジトリ・サーバに提示して、前記暗号化キーの組の前記対応する１つにアクセスし、前記アーカイブ・データ・リーダは、前記暗号化キーの組の前記対応する１つが与えられると、前記所与のアーカイブ・メタデータ・セグメントからの前記データ・セグメント暗号化キーをデコードして、前記所与のアーカイブ・データ・セグメントを暗号化解除するように動作する、
ことを特徴とするシステム。
【請求項１２】
前記アーカイブ・リーダは、前記認証トークン及び前記ポリシー識別子に基づいて、所定の暗号化キーを前記暗号化キーの組の前記対応する１つから検索するように動作し、前記ポリシー・コントローラは、さらに、所定の使用制御を受ける前記所定の暗号化キーを過渡的に維持するように動作することを特徴とする請求項１１に記載のシステム。
【請求項１３】
前記ポリシー・コントローラは、前記所定の暗号化キーを、アーカイブ・データ読み取りセッションの持続時間だけ過渡的に維持することを特徴とする請求項１２に記載のシステム。
【請求項１４】
前記ポリシー・コントローラは、前記所定の暗号化キーを、所定の時間期間だけ過渡的に維持することを特徴とする請求項１２に記載のシステム。
【請求項１５】
前記ポリシー・コントローラは、前記所定の暗号化キーを、所定のアーカイブ・データ読み取りセッション数の持続期間だけ過渡的に維持することを特徴とする請求項１２に記載のシステム。
【請求項１６】

前記セキュリティ保護されたリポジトリ・サーバは、前記セキュリティ保護されたリポジトリ・サーバと等価に実行することができる複数のセキュリティ保護されたリポジトリ・サーバの１つであることを特徴とする請求項１２に記載のシステム。

【請求項１７】

前記複数のセキュリティ保護されたリポジトリ・サーバは、通信ネットワークにより前記アーカイブ・データ・リーダに連結可能であることを特徴とする請求項１６に記載のシステム。

【請求項１８】

前記アーカイブ・データ・リーダは、前記アーカイブ・データ・リーダと等価に実行することができる複数のアーカイブ・データ・リーダの１つであり、前記複数のアーカイブ・データ・リーダは、前記通信ネットワークにより前記媒体サーバ・システムに連結可能であることを特徴とする請求項１７に記載のシステム。