【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７部門第３区分
【発行日】平成17年10月13日(2005.10.13)

【公開番号】特開2004-15527(P2004-15527A)
【公開日】平成16年1月15日(2004.1.15)
【年通号数】公開・登録公報2004-002
【出願番号】特願2002-167480(P2002-167480)
【国際特許分類第７版】
　Ｈ０４Ｌ　 9/32
　Ｇ０６Ｆ　15/00
　Ｈ０４Ｌ　 9/08
【ＦＩ】
　Ｈ０４Ｌ　 9/00　　６７５Ｂ
　Ｇ０６Ｆ　15/00　　３３０Ｚ
　Ｈ０４Ｌ　 9/00　　６０１Ａ
　Ｈ０４Ｌ　 9/00　　６０１Ｅ
　Ｈ０４Ｌ　 9/00　　６７５Ｄ

【手続補正書】
【提出日】平成17年6月6日(2005.6.6)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
　サービスプロバイダの提供するサービスを実行するユーザデバイスにおけるデータ処理権限を管理するデータ処理権限管理システムであり、
　サービスプロバイダは、
　暗号化処理のなされたデータ処理実行命令を含む暗号化実行命令と、該暗号化実行命令の復号処理に適用する登録鍵のユーザデバイス内メモリの格納領域を示すアドレス（Ａｄ）情報とを格納データとして有する実行属性証明書をサービス受領デバイスであるユーザデバイスに対して提供し、
　ユーザデバイスは、
　前記実行属性証明書に格納されたアドレス（Ａｄ）情報に従って、該ユーザデバイスのメモリから取得した登録鍵を適用して、該実行属性証明書に格納された暗号化実行命令の復号を行ない、復号結果に基づくデータ処理を実行する構成としたことを特徴とするデータ処理権限管理システム。
【請求項２】
　データ処理を実行する情報処理装置であり、
　暗号化データの復号処理に適用する登録鍵を格納するメモリ部と、
　暗号化処理のなされたデータ処理実行命令を含む暗号化実行命令と、該暗号化実行命令の復号処理に適用する登録鍵の情報処理装置内のメモリにおける格納領域を示すアドレス（Ａｄ）情報とを格納データとして有し、発行者署名のなされた実行属性証明書を入力し、署名検証処理を実行するとともに、署名検証の成立を条件として、前記アドレス（Ａｄ）情報に従って、前記メモリ部から取得した登録鍵を適用して前記暗号化実行命令を復号する暗号処理部と、
　前記暗号処理部において復号された実行命令を実行するデータ処理部と、

を有することを特徴とする情報処理装置。
【請求項３】
前記データ処理部は、
前記登録鍵格納領域を指定したアドレス（Ａｄ）に対応するメモリ領域に、リセット鍵データを書き込むことにより登録鍵の破棄処理を実行する構成であることを特徴とする請求項２に記載の情報処理装置。
【請求項４】
前記実行属性証明書に格納された暗号化実行命令には、
実行命令の適用可能回数識別値が格納され、
前記データ処理部は、
実行命令の実行に応じて前記適用可能回数識別値を更新して、更新された適用可能回数識別値を含む新たな実行属性証明書の生成を行なう構成であることを特徴とする請求項２に記載の情報処理装置。
【請求項５】
前記実行属性証明書に格納された暗号化実行命令には、
実行命令の適用可能回数識別値が格納され、
前記データ処理部は、
実行命令の実行に応じて前記適用可能回数識別値を更新して、更新された適用可能回数識別値が０となった場合に、前記登録鍵格納領域を指定したアドレス（Ａｄ）に対応するメモリ領域に、リセット鍵データを書き込むことにより登録鍵の破棄処理を実行する構成であることを特徴とする請求項２に記載の情報処理装置。
【請求項６】
前記実行属性証明書に格納された暗号化実行命令は、
他デバイスへの譲渡用実行属性証明書の生成処理命令を含み、
前記データ処理部は、
前記譲渡用実行属性証明書の生成処理命令に従い、
新たな譲渡用実行属性証明書の生成処理を実行し、他デバイスへの提供処理を実行する構成であることを特徴とする請求項２に記載の情報処理装置。
【請求項７】
前記実行属性証明書に格納された暗号化実行命令には、
他デバイスの属性を証明する証明書としての審査代行属性証明書の発行処理命令、および該審査代行属性証明書の生成に必要とする署名生成用鍵を含み、
前記データ処理部は、
前記審査代行属性証明書の発行処理命令に従い、
前記署名生成用鍵を適用して署名を実行した審査代行属性証明書の生成処理を実行する構成であることを特徴とする請求項２に記載の情報処理装置。
【請求項８】
前記実行属性証明書に格納された暗号化実行命令には、
他デバイスの属性を証明する証明書としての代理署名属性証明書の発行処理命令、および該代理署名属性証明書の生成に必要とする署名生成用鍵を含み、
前記データ処理部は、
前記代理署名属性証明書の発行処理命令に従い、
該代理署名属性証明書の検証を実行する検証デバイスから受領した検証用乱数（Ｒａ）を格納データとして含み、前記署名生成用鍵を適用した署名を有する代理署名属性証明書の生成処理を実行する構成であることを特徴とする請求項２に記載の情報処理装置。
【請求項９】
サービスプロバイダの提供するサービスを実行するユーザデバイスにおけるデータ処理権限を管理するデータ処理権限管理方法であり、
サービスプロバイダにおける実行ステップとして、
暗号化処理のなされたデータ処理実行命令を含む暗号化実行命令と、該暗号化実行命令

の復号処理に適用する登録鍵のユーザデバイス内メモリの格納領域を示すアドレス（Ａｄ）情報とを格納データとして有する実行属性証明書をサービス受領デバイスであるユーザデバイスに対して提供するステップを有し、
ユーザデバイスにおける実行ステップとして、
前記実行属性証明書に格納されたアドレス（Ａｄ）情報に従って、該ユーザデバイスのメモリから登録鍵を取得するステップと、
取得した登録鍵を適用して、該実行属性証明書に格納された暗号化実行命令の復号を実行するステップと、
復号結果に基づくデータ処理を実行するステップと、
を有することを特徴とするデータ処理権限管理方法。
【請求項１０】
データ処理を実行する情報処理装置における情報処理方法であり、
暗号化処理のなされたデータ処理実行命令を含む暗号化実行命令と、該暗号化実行命令の復号処理に適用する登録鍵の情報処理装置内のメモリにおける格納領域を示すアドレス（Ａｄ）情報とを格納データとして有し発行者署名のなされた実行属性証明書を入力するステップと、
署名検証処理を実行するとともに、署名検証の成立を条件として、前記アドレス（Ａｄ）情報に従って、前記メモリから登録鍵を取得するステップと、
取得した登録鍵を適用して前記暗号化実行命令を復号するステップと、
復号された実行命令を実行するデータ処理ステップと、
を有することを特徴とする情報処理方法。
【請求項１１】
データ処理を実行する情報処理装置における情報処理を実行せしめるコンピュータ・プログラムであって、
暗号化処理のなされたデータ処理実行命令を含む暗号化実行命令と、該暗号化実行命令の復号処理に適用する登録鍵の情報処理装置内のメモリにおける格納領域を示すアドレス（Ａｄ）情報とを格納データとして有し発行者署名のなされた実行属性証明書を入力するステップと、
署名検証処理を実行するとともに、署名検証の成立を条件として、前記アドレス（Ａｄ）情報に従って、前記メモリから登録鍵を取得するステップと、
取得した登録鍵を適用して前記暗号化実行命令を復号するステップと、
復号された実行命令を実行するデータ処理ステップと、
を有することを特徴とするコンピュータ・プログラム。