【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26年2月27日(2014.2.27)

【公開番号】特開2010-140470(P2010-140470A)
【公開日】平成22年6月24日(2010.6.24)
【年通号数】公開・登録公報2010-025
【出願番号】特願2009-242567(P2009-242567)
【国際特許分類】
Ｇ０６Ｆ　21/60　(2013.01)
Ｇ０６Ｆ　21/12　(2013.01)
Ｇ０６Ｆ　21/62　(2013.01)
Ｈ０４Ｌ　 9/10　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　12/14　５６０Ａ
Ｇ０６Ｆ　 9/06　６６０Ｌ
Ｇ０６Ｆ　12/14　５４０Ｐ
Ｇ０６Ｆ　12/14　５６０Ｄ
Ｈ０４Ｌ　 9/00　６２１Ｚ

【誤訳訂正書】
【提出日】平成26年1月8日(2014.1.8)
【誤訳訂正１】
【訂正対象書類名】特許請求の範囲
【訂正対象項目名】全文
【訂正方法】変更
【訂正の内容】
【特許請求の範囲】
【請求項１】
グラフィックプロセッサ、ビデオプロセッサ及びオーディオプロセッサの少なくとも１つのプロセッサと、
第２エンティティのプログラムを処理するために前記プロセッサ上で具現化される第１エンティティの少なくとも１つのセキュアなバーチャルマシンと、
第３エンティティのコンテンツを出力用に処理するためにコンピュータ読み取り可能な媒体上で実施される少なくとも１つのプログラムと、
を備え、
第１エンティティは、セキュアなバーチャルマシンを備えたエンティティである場合を含み、
第２エンティティは、ソフトウェアを認可するエンティティである場合を含み、
第３エンティティは、コンテンツを認可するエンティティである場合を含み、
前記少なくとも１つのセキュアなバーチャルマシンは、当該少なくとも１つのセキュアなバーチャルマシン内で第２エンティティのプログラムにより第３エンティティのコンテンツを処理する、
装置。
【請求項２】
残留する機密プログラム情報、処理されている情報、及び前記少なくとも１つのバーチャルマシンの各々により生成されるエフェメラル変数は、処理後に削除される、請求項１に記載の装置。
【請求項３】
個々のコンテクスト内において前記プロセッサ上で複数のセキュアなバーチャルマシン

が具現化される、請求項１に記載の装置。
【請求項４】
前記複数のセキュアなバーチャルマシン間での情報の共有が制限される、請求項３に記載の装置。
【請求項５】
エフェメラル情報の形式、及び前記複数のセキュアなバーチャルマシンにより処理されている情報の記憶が制限される、請求項４に記載の装置。
【請求項６】
前記情報は、保護されたコンテンツの解読に使用されるキー及び中間暗号値を含む、請求項４に記載の装置。
【請求項７】
クライアント供給プログラムを実行して前記保護されたコンテンツを処理するために前記少なくとも１つのバーチャルマシンが設けられる、請求項１に記載の装置。
【請求項８】
前記クライアント供給プログラムは、第３エンティティのコンテンツを処理する際に前記クライアント供給プログラムによって使用されるアルゴリズム詳細、シークレット及びキーの機密性を保証するために第２エンティティにより暗号化される、請求項７に記載の装置。
【請求項９】
前記クライアント供給プログラムは、更に、そのクライアント供給プログラムの完全性を検証できるように第２エンティティにより署名されると共に、そのクライアント供給プログラムのソースの真正性を検証できるようにする証明書を含む、請求項８に記載の装置。
【請求項１０】
第３エンティティのコンテンツは、前記少なくとも１つのバーチャルマシンにより処理される前に第３エンティティにより別々に暗号化される、請求項７に記載の装置。
【請求項１１】
前記クライアント供給プログラム、機密アルゴリズム及びシークレットは、前記少なくとも１つのバーチャルマシン内での実行を許す前に、含まれた署名及び証明書を検証することで、解読され認証される、請求項１０に記載の装置。
【請求項１２】
前記クライアント供給プログラムの処理は、第３エンティティのコンテンツを解読することを含む、請求項１０に記載の装置。
【請求項１３】
前記処理は、更に、第３エンティティのコンテンツ又は第３エンティティのコンテンツ内のストリームの１つ以上の部分のうちの少なくとも１つを再暗号化することを含む、請求項１２に記載の装置。
【請求項１４】
前記再暗号化は、第３エンティティのコンテンツが前記少なくとも１つのバーチャルマシンから退出する前に行われる、請求項１３に記載の装置。
【請求項１５】
前記再暗号化は、第３エンティティのコンテンツが前記プロセッサから出力された後に行われる、請求項１３に記載の装置。
【請求項１６】
前記クライアント供給プログラムは、アプリケーションから受け取られ、前記クライアント供給プログラムは、前記プロセッサとアプリケーションとの間にセキュアな通信チャンネルを確立する、請求項７に記載の装置。
【請求項１７】
前記プロセッサとアプリケーションとの間の前記通信チャンネルは、前記プロセッサにおいて導出された暗号値及び少なくとも１つの証明書を使用してセキュア化される、請求

項１６に記載の装置。
【請求項１８】
前記少なくとも１つのバーチャルマシンは、アプリケーションによって供給される保護コンテンツ処理プログラムのインタープリターとして働く、請求項１に記載の装置。
【請求項１９】
前記プロセッサは、少なくとも１つのセキュリティプロセッサを含み、そして処理されたコンテンツを、グラフィックプロセッサ、ビデオプロセッサ又はオーディオプロセッサの少なくとも１つに与えるように構成される、請求項１に記載の装置。
【請求項２０】
前記プロセッサは、パッケージから解かれたコンテンツキー、及びプログラム実行中に導出される中間暗号値のためのセキュアな機密記憶部を含む、請求項１に記載の装置。
【請求項２１】
前記プロセッサの少なくとも１つのバーチャルマシン内で第２エンティティのプログラムにより第３エンティティのコンテンツを処理するのに、前記プロセッサが、認可されたシークレットを含むことも、以前に実施された認可アルゴリズムを有することも要求されない、請求項１に記載の装置。
【請求項２２】
前記少なくとも１つのバーチャルマシンの設計、及び前記少なくとも１つのバーチャルマシン内の第２エンティティのプログラムによる第３エンティティのコンテンツの処理は、認可応諾及び頑健性ルールに関して第２エンティティにより再検討され、これにより、第３エンティティのコンテンツに対する適合性を決定できる、請求項１に記載の装置。
【誤訳訂正２】
【訂正対象書類名】明細書
【訂正対象項目名】００１８
【訂正方法】変更
【訂正の内容】
【００１８】
[0029]例えば、プログラム２０６は、ベンダー２０４のＣＰＵにより生成され、次いで、暗号化されることでセキュア化されてもよい。一実施形態では、プログラム２０６は、プロセッサ２５０がコンテンツを受け取れるようにするアプリケーション（例えば、コンテンツプレーヤ、等）によって使用される。この場合に、プログラム２０６は、アプリケーションによりセキュア化することができる。従って、プログラム２０６は、コンテンツに基づき、アプリケーションによってメモリ２２８から検索されてもよい。