【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21年7月9日(2009.7.9)

【公開番号】特開2008-5156(P2008-5156A)
【公開日】平成20年1月10日(2008.1.10)
【年通号数】公開・登録公報2008-001
【出願番号】特願2006-171727(P2006-171727)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ｂ

【手続補正書】
【提出日】平成21年5月25日(2009.5.25)
【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】
サービス提供装置からサービスの提供を受ける情報処理端末であって、
前記サービス提供装置からサービスの提供を受けるプログラムであるサービスクライアントを含む、複数のプログラムを格納する格納手段と、
前記複数のプログラムのうち１以上のプログラムをそれぞれ実行する複数の実行環境を提供する実行環境提供手段と、
前記複数のプログラムのうち、実行されているプログラムを示す情報であるエントリを記憶する記憶手段と、
複数の記憶領域を備え、前記複数の実行環境それぞれごとに当該実行環境で実行されているプログラムを示すエントリに所定の演算を施すことで、前記実行環境において実行されている１以上のプログラムの実行状態を示す蓄積情報を前記複数の実行環境それぞれについて生成し、生成した累積情報のそれぞれを前記蓄積情報が対応する実行環境ごとに異なる記憶領域に記憶するモジュールと、
前記複数の記憶領域のうち前記サービスクライアントが実行されている実行環境に対応する記憶領域から読み出した蓄積情報を前記サービス提供装置へ送信して、前記サービスクライアントを含む実行環境で実行されているプログラムの検証を前記サービス提供装置に要求する検証要求手段と、
を備えることを特徴とする情報処理端末。
【請求項２】
前記複数の実行環境のうち、少なくとも１つは仮想実行環境であることを特徴とする請求項１に記載の情報処理端末。
【請求項３】
前記モジュールは、前記仮想実行環境について、当該仮想実行環境が実現されている実行環境において実行されているプログラムを示すエントリ、および、前記仮想実行環境で実行されているプログラムを示すエントリから、前記蓄積情報を生成する、
ことを特徴とする請求項２に記載の情報処理端末。
【請求項４】
サービス提供装置からサービスクライアントを用いてサービスの提供を受ける情報処理端末であって、

システムを構成する１以上のプログラムと、前記サービスクライアントを含む１以上のアプリケーションプログラムとから構成される複数のプログラムを格納する格納手段と、
前記複数のプログラムのうち１以上のプログラムをそれぞれ実行する実行手段と、
前記複数のプログラムのうち、実行されているプログラムを示す情報であるエントリを記憶する記憶手段と、
前記システムを構成するプログラムを示すエントリに所定の演算を施すことで、前記システムを構成するプログラムのうち実行されているプログラムの実行状態を示すシステム蓄積情報を生成して、第１記憶領域に記憶し、
前記アプリケーションのプログラムのうち、少なくとも前記サービスクライアントを示すエントリに所定の演算を施すことで、前記アプリケーションのプログラムのうち実行されているプログラムの実行状態を示すアプリケーション蓄積情報を生成して、前記第１記憶領域とは異なる第２記憶領域に記憶するモジュールと、
前記システム蓄積情報と、前記アプリケーション蓄積情報とを前記サービス提供装置へ送信して、前記情報処理端末で動作しているプログラムの検証を前記サービス提供装置に要求する検証要求手段と
を備えることを特徴とする情報処理端末。
【請求項５】
前記情報端末は、更に、
前記アプリケーションのプログラムを示すエントリのそれぞれについて、前記サービス提供装置に通知することが許可されるか否かを判定する公開有無判定手段と、
前記通知が許可されなかったエントリに隠蔽処理を行う隠蔽手段とを備え、
前記モジュールは、前記通知が許可されたエントリについては前記エントリを、前記通知が許可されなかったエントリについては隠蔽処理後のエントリを用いて、前記所定の演算を行うことにより、前記アプリケーション蓄積情報を生成する
ことを特徴とする請求項４に記載の情報処理端末。
【請求項６】
前記情報端末は、更に、
前記システムを構成するプログラムを示すエントリを収集したシステムログと、
前記アプリケーションのプログラムを示すエントリのうち、前記通知が許可されたエントリについては前記エントリを、前記通知が許可されなかったエントリについては隠蔽処理後のエントリを収集したアプリケーションログとを生成するログ構成手段とを備え、
前記検証要求手段は、さらに、前記システムログと前記アプリケーションログとを前記サービス提供装置に送信する
ことを特徴とする請求項５に記載の情報処理端末。
【請求項７】
前記モジュールは、
前記システムを構成するプログラムを示すエントリのそれぞれについて、前記エントリそれぞれのハッシュ値を演算して前記第１記憶領域に格納されているシステム蓄積情報と連結し、連結して得られた情報のハッシュ値を演算して前記第１記憶領域に格納されているシステム蓄積情報を更新する処理を、前記エントリに対応するプログラムが実行された順序で行うことで、前記サービス提供装置へ送信されるシステム蓄積情報を生成し、
前記アプリケーションのプログラムを示すエントリのそれぞれについて、前記エントリの通知が許可されている場合には前記エントリのハッシュ値を演算し、前記エントリの通知が許可されていない場合には前記隠蔽処理後のエントリのハッシュ値を演算して、前記第２記憶領域に格納されているアプリケーション蓄積情報と連結し、連結して得られた情報のハッシュの値を演算して前記第２記憶領域に格納されているアプリケーション蓄積情報を更新する処理を、前記エントリに対応するプログラムが実行された順序で行うことで、前記サービス提供装置へ送信されるシステム蓄積情報を生成する
ことを特徴とする請求項５に記載の情報処理端末。
【請求項８】

前記情報処理端末は、更に、前記サービス提供装置と異なる第２サービス提供装置からサービスの提供を受け、
前記モジュールは、さらに、前記アプリケーションのプログラムのうち、少なくとも前記第２サービス提供装置からサービスの提供を受けるサービスクライアントを示すエントリに所定の演算を施すことで、第２アプリケーション蓄積情報を生成し、
前記モジュールは、
前記アプリケーション蓄積情報と前記第２アプリケーション蓄積情報とが同じ値になる場合には、前記第２記憶領域に、一つの情報として格納し、
前記アプリケーション蓄積情報と前記第２アプリケーション蓄積情報とが異なる値になる場合には、前記第２記憶領域とは異なる第３記憶領域に、前記第２アプリケーション蓄積情報を格納し、
前記検証手段は、更に、前記システム蓄積情報と、前記第２アプリケーション蓄積情報とを前記第２サービス提供装置へ送信することで、前記情報処理端末で動作しているプログラムの検証を前記第２サービス提供装置に要求する、
ことを特徴とする請求項５に記載の情報処理端末。
【請求項９】
前記情報処理端末は、更に、前記サービス提供装置と異なる第２サービス提供装置からサービスの提供を受け、
前記モジュールは、さらに、前記アプリケーションのプログラムのうち、少なくとも前記第２サービス提供装置からサービスの提供を受けるサービスクライアントを示すエントリに所定の演算を施すことで、第２アプリケーション蓄積情報を生成し、
前記モジュールは、
前記アプリケーションのプログラムが実行されるごとに、前記アプリケーション蓄積情報と前記第２アプリケーション蓄積情報とを更新し、
前記アプリケーション蓄積情報と前記第２アプリケーション蓄積情報とが同一の値であり、かつ前記アプリケーション蓄積情報と前記第２アプリケーション蓄積情報について同じ更新を行う場合には、前記アプリケーション蓄積情報と前記第２アプリケーション蓄積情報の一方を更新して、更新した結果を他方にコピーにすることで、前記アプリケーション蓄積情報と前記第２アプリケーション蓄積情報の両方を更新し、
前記検証手段は、更に、前記システム蓄積情報と、前記第２アプリケーション蓄積情報とを前記第２サービス提供装置へ送信することで、前記情報処理端末で動作しているプログラムの検証を前記第２サービス提供装置に要求する
ことを特徴とする請求項５に記載の情報処理端末。
【請求項１０】
前記エントリには、前記エントリそれぞれを識別するエントリＩＤが付され、
前記隠蔽手段は、マスターキーを保持し、前記エントリＩＤを前記マスターキーにより暗号化したものから暗号鍵を生成し、エントリを前記暗号鍵で暗号化することで前記エントリの隠蔽処理を行う
ことを特徴とする請求項５に記載の情報処理端末。
【請求項１１】
前記隠蔽手段は、暗号鍵をランダムに生成し、前記エントリを前記暗号鍵で暗号化することで前記エントリの隠蔽処理を行い、
前記検証要求手段は、更に、前記暗号鍵を前記サービス提供装置へ送信する
ことを特徴とする請求項５に記載の情報処理端末。
【請求項１２】
前記隠蔽手段は、前記エントリの内容の一部または全部を削除することで前記エントリの隠蔽処理を行う
ことを特徴とする請求項５に記載の情報処理端末。
【請求項１３】
前記情報処理端末は、

前記サービス提供装置から隠蔽処理の施されたエントリの開示を要求された際に、前記隠蔽処理を解除する情報を取得ないしは生成し、要求してきた相手に開示してよいか判断し、開示してよいと判断した場合に、前記隠蔽を解除する情報または解除したエントリを前記サービス提供装置に提供するログ開示判定手段と、
をさらに備えた請求項５に記載の情報処理端末。
【請求項１４】
前記ログ開示判定手段は、開示してよいかを判断する際に、隠蔽を解除したエントリを利用者に提示し、前記利用者に前記エントリを開示してよいか指定させる
ことを特徴とする請求項１３に記載の情報処理端末。
【請求項１５】
システムを構成する１以上のプログラムと、サービスの提供を受けるプログラムであるサービスクライアントとを含む１以上のアプリケーションのプログラムとから構成される複数のプログラムを格納し、前記複数のプログラムのうち１以上のプログラムをそれぞれ実行する情報処理端末に接続されるセキュアデバイスであって、
前記情報処理端末から、前記情報処理端末で前記複数のプログラムのうちいずれかが実行される毎に、実行されたプログラムを示す情報であるエントリを受信する受信手段と、
前記システムを構成するプログラムを示すエントリに所定の演算を施すことで、前記システムを構成するプログラムのうち前記情報処理端末で実行されているプログラムの実行状態を示すシステム蓄積情報を生成して、第１記憶領域に記憶し、
前記アプリケーションのプログラムのうち、少なくとも前記サービスクライアントを示すエントリに所定の演算を施すことで、前記アプリケーションのプログラムのうち実行されているプログラムの実行状態を示すアプリケーション蓄積情報を生成して、前記第１記憶領域とは異なる第２記憶領域に記憶するモジュールと、
前記システム蓄積情報と前記アプリケーション蓄積情報とを用いて前記情報処理端末で実行されているプログラムの実行状態を検証する検証手段と、
検証に成功した場合に前記サービスを前記サービスクライアントに提供するサーバと、
を備えることを特徴とするセキュアデバイス。
【請求項１６】
前記モジュールは、前記システム蓄積情報と前記アプリケーション蓄積情報とを前記セキュアデバイスの内部インターフェイスを介して前記検証手段へ送信する
ことを特徴とする請求項１５に記載のセキュアデバイス。
【請求項１７】
サービス提供装置からサービスクライアントを用いてサービスの提供を受ける情報処理端末で用いられる情報処理方法であって、
前記情報処理端末は、システムを構成する１以上のプログラムと、前記サービスクライアントを含む１以上のアプリケーションのプログラムとから構成される複数のプログラムを格納し、
前記情報処理方法は、
前記複数のプログラムのうち１以上のプログラムをそれぞれ実行する実行ステップと、
前記複数のプログラムのうち、実行されているプログラムを示す情報であるエントリを記憶する記憶ステップと、
前記システムを構成するプログラムを示すエントリに所定の演算を施すことで、前記システムを構成するプログラムのうち実行されているプログラムの実行状態を示すシステム蓄積情報を生成して、第１記憶領域に記憶し、
前記アプリケーションのプログラムのうち、少なくとも前記サービスクライアントを示すエントリに所定の演算を施すことで、前記アプリケーションのプログラムのうち実行されているプログラムの実行状態を示すアプリケーション蓄積情報を生成して、前記第１記憶領域とは異なる第２記憶領域に記憶する蓄積情報記憶ステップと、
前記システム蓄積情報と、前記アプリケーション蓄積情報とを前記サービス提供装置へ送信して、前記情報処理端末で動作しているプログラムの検証を前記サービス提供装置に

要求する検証要求ステップと
を備えることを特徴とする情報処理方法。