

【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20年7月31日(2008.7.31)

【公表番号】特表2008-503014(P2008-503014A)

【公表日】平成20年1月31日(2008.1.31)

【年通号数】公開・登録公報2008-004

【出願番号】特願2007-527785(P2007-527785)

【国際特許分類】

G 06 F 21/22 (2006.01)

G 09 C 1/00 (2006.01)

G 06 F 21/24 (2006.01)

【F I】

G 06 F 9/06 6 6 0 L

G 09 C 1/00 6 6 0 D

G 06 F 12/14 5 6 0 C

【手続補正書】

【提出日】平成20年6月10日(2008.6.10)

【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】

ソフトウェア改ざんを抑止するための方法であって、

難読化された保護ダイナミックリンクライブラリをコンピューティングマシンにロードする前に、前記難読化された保護ダイナミックリンクライブラリの第1のチェックサムを計算することと、

ソフトウェア改ざんを抑止するためのセキュリティエラー対策を講じるべきか否かを判定するために、前記難読化された保護ダイナミックリンクライブラリのソフトウェアイメージのオリジナル性を検証することと

を備えることを特徴とする方法。

【請求項2】

システムファイルに含まれるカタログファイルのリストを得ることと、

前記カタログファイルのリスト内のカタログファイルに含まれる第2のチェックサムを検索することと

をさらに備えることを特徴とする請求項1に記載の方法。

【請求項3】

前記第1のチェックサムと前記第2のチェックサムとが一致しない場合、前記検証することは、前記ソフトウェアイメージが、オリジナルの難読化された保護ダイナミックリンクライブラリではないと判定するこ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】

前記難読化された保護ダイナミックリンクライブラリと、前記第2のチェックサムを含む前記カタログファイルとが信用できるか否かを判定するために、信用チェック用(trust-checking)アプリケーションプログラミングインターフェースのセットを呼び出すことをさらに備え、

前記信用チェック用アプリケーションプログラミングインターフェースのセットは、状態データを返す

ことを特徴とする請求項 3 に記載の方法。

【請求項 5】

前記信用チェック用アプリケーションプログラミングインターフェースのセットを呼び出し、前記状態データを使用して信用できるプロバイダ情報 (trust provider information) を検索すること

をさらに備えることを特徴とする請求項 4 に記載の方法。

【請求項 6】

前記信用チェック用アプリケーションプログラミングインターフェースのセットを呼び出し、前記信用できるプロバイダ情報を使用してベースサイナ (base signer) を検索すること

をさらに備えることを特徴とする請求項 5 に記載の方法。

【請求項 7】

前記信用チェック用アプリケーションプログラミングインターフェースのセットを呼び出し、前記ベースサイナのコンテキストを使用して証明書チェーン (certificate chain) 内の最後の要素を妥当性検査すること

をさらに備えることを特徴とする請求項 6 に記載の方法。

【請求項 8】

前記最後の要素が、前記ソフトウェアイメージのメーカーからの正しい公開キーを含む場合、前記検証することは、前記ソフトウェアイメージがオリジナルであるとの結論を下すことを含むことを特徴とする請求項 7 に記載の方法。

【請求項 9】

ソフトウェア改ざんを抑止するために、

難読化された保護ダイナミックリンクライブラリをコンピューティングマシンにロードする前に、前記難読化された保護ダイナミックリンクライブラリの第 1 のチェックサムを計算する手順と、

ソフトウェア改ざんを抑止するためのセキュリティエラー対策を講じるべきか否かを判定するために、前記難読化された保護ダイナミックリンクライブラリのソフトウェアイメージのオリジナル性を検証する手順と

をコンピュータに実行させるためのコンピュータ実行可能命令を記憶したことを特徴とするコンピュータ読み取り可能な記憶媒体。

【請求項 10】

システムファイルに含まれるカタログファイルのリストを得る手順と、

前記カタログファイルのリスト内のカタログファイルに含まれる第 2 のチェックサムを検索する手順と

をさらにコンピュータに実行させるためのコンピュータ実行可能命令を記憶したことを特徴とする請求項 9 に記載のコンピュータ読み取り可能な記憶媒体。

【請求項 11】

前記第 1 のチェックサムと前記第 2 のチェックサムとが一致しない場合、前記検証する手順は、前記ソフトウェアイメージが、オリジナルの難読化された保護ダイナミックリンクライブラリではないと判定する手順を含むことを特徴とする請求項 10 に記載のコンピュータ読み取り可能な記憶媒体。

【請求項 12】

前記難読化された保護ダイナミックリンクライブラリと、前記第 2 のチェックサムを含む前記カタログファイルとが信用できるか否かを判定するために、信用チェック用アプリケーションプログラミングインターフェースのセットを呼び出す手順

をさらにコンピュータに実行させるためのコンピュータ実行可能命令を記憶し、

前記信用チェック用アプリケーションプログラミングインターフェースのセットは、状態データを返すことを特徴とする請求項 11 に記載のコンピュータ読み取り可能な記憶媒体。

【請求項 13】

前記信用チェック用アプリケーションプログラミングインターフェースのセットを呼び出し、前記状態データを使用して信用できるプロバイダ情報を検索する手順

をさらにコンピュータに実行させるためのコンピュータ実行可能命令を記憶したこととを特徴とする請求項12に記載のコンピュータ読取り可能な記憶媒体。

【請求項14】

前記信用チェック用アプリケーションプログラミングインターフェースのセットを呼び出し、前記信用できるプロバイダ情報を使用してベースサイナを検索する手順

をさらにコンピュータに実行させるためのコンピュータ実行可能命令を記憶したこととを特徴とする請求項13に記載のコンピュータ読取り可能な記憶媒体。

【請求項15】

前記信用チェック用アプリケーションプログラミングインターフェースのセットを呼び出し、前記ベースサイナのコンテキストを使用して証明書チェーン内の最後の要素を妥当性検査する手順

をさらにコンピュータに実行させるためのコンピュータ実行可能命令を記憶したこととを特徴とする請求項14に記載のコンピュータ読取り可能な記憶媒体。

【請求項16】

前記最後の要素が、前記ソフトウェアイメージのメーカーからの正しい公開キーを含む場合、前記検証する手順は、前記ソフトウェアイメージがオリジナルであるとの結論を下す手順を含むことを特徴とする請求項15に記載のコンピュータ読取り可能な媒体。

【請求項17】

ソフトウェア改ざんを抑止するためのシステムであって、

難読化された保護ダイナミックリンクライブラリをコンピューティングマシンにロードする前に、前記難読化された保護ダイナミックリンクライブラリの第1のチェックサムを計算する手段と、

ソフトウェア改ざんを抑止するためのセキュリティエラー対策を講じるべきか否かを判定するために、前記難読化された保護ダイナミックリンクライブラリのソフトウェアイメージのオリジナル性を検証する手段と

を備えたことを特徴とするシステム。

【請求項18】

システムファイルに含まれるカタログファイルのリストを得る手段と、

前記カタログファイルのリスト内のカタログファイルに含まれる第2のチェックサムを検索する手段と

をさらに備えたことを特徴とする請求項17に記載のシステム。

【請求項19】

前記第1のチェックサムと前記第2のチェックサムとが一致しない場合、前記検証する手段は、前記ソフトウェアイメージが、オリジナルの難読化された保護ダイナミックリンクライブラリではないと判定することを特徴とする請求項18に記載のシステム。

【請求項20】

前記難読化された保護ダイナミックリンクライブラリと、前記第2のチェックサムを含む前記カタログファイルとが信用できるか否かを判定するために、信用チェック用アプリケーションプログラミングインターフェースのセットを呼び出す手段

をさらに備え、

前記信用チェック用アプリケーションプログラミングインターフェースのセットは、状態データを返すこととする請求項19に記載のシステム。