【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】令和1年12月26日(2019.12.26)

【公開番号】特開2019-20872(P2019-20872A)
【公開日】平成31年2月7日(2019.2.7)
【年通号数】公開・登録公報2019-005
【出願番号】特願2017-136725(P2017-136725)
【国際特許分類】
Ｇ０６Ｆ　21/12　(2013.01)
Ｈ０４Ｌ　 9/32　(2006.01)
Ｇ０９Ｃ　 1/00　(2006.01)
Ｇ０６Ｆ　21/64　(2013.01)
【ＦＩ】
Ｇ０６Ｆ　21/12
Ｈ０４Ｌ　 9/00　６７５Ａ
Ｇ０９Ｃ　 1/00　６４０Ｄ
Ｇ０６Ｆ　21/64

【手続補正書】
【提出日】令和1年11月12日(2019.11.12)
【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】
プログラムを分割したｍ個の分割プログラム、および検証用認証子を記憶する記憶部（１１、１５）と、
暗号演算により前記ｍ個の分割プログラムそれぞれのｍ個の部分認証子を生成する暗号演算部（１２、１３、３０、２２４）と、
１乃至ｎ－１番目の部分認証子を用いた論理演算を行って生成されたｎ－１番目の演算認証子と、ｎ番目の部分認証子とを用いた論理演算を行って、ｎ番目の演算認証子を生成する認証子演算部（１４、３０、２２４）、と、
前記ｎ番目の演算認証子を保存する認証子保存部（２２）と、
ｎ＋１番目の部分認証子を生成する分割プログラムを特定する情報を保存する次回生成対象保存部（２１）と、
前記検証用認証子とｍ番目の演算認証子とが一致するか否かによって前記プログラムの改ざんを検証する検証部（３０、２２４）と、
を有する電子制御装置。
【請求項２】
前記暗号演算部は、前記認証子演算部が前記ｎ－１番目の演算認証子を生成した後に、前記ｎ番目の部分認証子を生成し、
前記認証子演算部は、前記認証子保存部に保存された前記ｎ－１番目の演算認証子と、前記ｎ番目の部分認証子とを用いた論理演算を行って、前記ｎ番目の演算認証子を生成し、
前記認証子保存部は、前記ｎ－１番目の演算認証子に前記ｎ番目の演算認証子を上書きして保存する、
請求項１に記載の電子制御装置。

【請求項３】
前記記憶部（１１）に記憶されている前記検証用認証子が一つであり、
前記認証子演算部が、すべての前記部分認証子を用いた論理演算を行って一つの演算認証子を生成し、
前記検証部は、前記一つの検証用認証子と前記一つの演算認証子とが一致するか否かによって前記プログラムの改ざんを検証する、
請求項１または２に記載の電子制御装置。
【請求項４】
前記認証子演算部が行う前記論理演算が、排他的論理和（ＸＯＲ演算）または排他的論理和の否定（ＸＮＯＲ演算）である、
請求項１乃至３のいずれか１項に記載の電子制御装置。
【請求項５】
プログラムを分割したｍ個の分割プログラムそれぞれのｍ個の部分認証子を生成する暗号演算ステップ（Ｓ２０、Ｓ５０）と、
前記暗号演算ステップ（Ｓ２０、Ｓ５０）により得られた１乃至ｎ－１番目の部分認証子を用いた論理演算を行って生成されたｎ－１番目の演算認証子と、ｎ番目の部分認証子とを用いた論理演算を行って、ｎ番目の演算認証子を生成する認証子演算ステップ（Ｓ６０）と、
前記ｎ番目の演算認証子を保存する保存ステップ（Ｓ７０）と、
ｎ＋１番目の部分認証子を生成する分割プログラムを特定する情報を保存する保存ステップ（Ｓ４０）と、
前記演算認証子と、あらかじめ求めた検証用認証子とが一致するか否かを判定する検証ステップ（Ｓ９０、Ｓ１００）と、
を有するプログラム改ざん検知方法。
【請求項６】
電子制御装置が起動する際に前記各ステップを実行する、
請求項５に記載のプログラム改ざん検知方法。
【請求項７】
電子制御装置の低消費電力モードから通常モードに移行する際に前記各ステップを実行する、
請求項５に記載のプログラム改ざん検知方法。
【請求項８】
プログラムを分割したｍ個の分割プログラムそれぞれのｍ個の部分認証子を生成する暗号演算ステップ（Ｓ２０、Ｓ５０）と、
前記暗号演算ステップ（Ｓ２０、Ｓ５０）により得られた１乃至ｎ－１番目の部分認証子を用いた論理演算を行って生成されたｎ－１番目の演算認証子と、ｎ番目の部分認証子とを用いた論理演算を行って、ｎ番目の演算認証子を生成する認証子演算ステップ（Ｓ６０）と、
前記ｎ番目の演算認証子を保存する保存ステップ（Ｓ７０）と、
ｎ＋１番目の部分認証子を生成する分割プログラムを特定する情報を保存する保存ステップ（Ｓ４０）と、
前記演算認証子と、あらかじめ求めた検証用認証子とが一致するか否かを判定する検証ステップ（Ｓ９０、Ｓ１００）と、
を有するプログラム改ざん検知方法、をコンピュータに実行させるプログラム。
【請求項９】
プログラムを分割したｍ個の分割プログラムそれぞれのｍ個の部分認証子を生成する暗号演算ステップ（Ｓ２０、Ｓ５０）と、
前記暗号演算ステップ（Ｓ２０、Ｓ５０）により得られた１乃至ｎ－１番目の部分認証子を用いた論理演算を行って生成されたｎ－１番目の演算認証子と、ｎ番目の部分認証子とを用いた論理演算を行って、ｎ番目の演算認証子を生成する認証子演算ステップ（Ｓ６

０）と、
前記ｎ番目の演算認証子を保存する保存ステップ（Ｓ７０）と、
ｎ＋１番目の部分認証子を生成する分割プログラムを特定する情報を保存する保存ステップ（Ｓ４０）と、
前記演算認証子と、あらかじめ求めた検証用認証子とが一致するか否かを判定する検証ステップ（Ｓ９０、Ｓ１００）と、
を有するプログラム改ざん検知方法、を電子制御装置が起動する際にコンピュータに実行させるプログラム。
【請求項１０】
プログラムを分割したｍ個の分割プログラムそれぞれのｍ個の部分認証子を生成する暗号演算ステップ（Ｓ２０、Ｓ５０）と、
前記暗号演算ステップ（Ｓ２０、Ｓ５０）により得られた１乃至ｎ－１番目の部分認証子を用いた論理演算を行って生成されたｎ－１番目の演算認証子と、ｎ番目の部分認証子とを用いた論理演算を行って、ｎ番目の演算認証子を生成する認証子演算ステップ（Ｓ６０）と、
前記ｎ番目の演算認証子を保存する保存ステップ（Ｓ７０）と、
ｎ＋１番目の部分認証子を生成する分割プログラムを特定する情報を保存する保存ステップ（Ｓ４０）と、
前記演算認証子と、あらかじめ求めた検証用認証子とが一致するか否かを判定する検証ステップ（Ｓ９０、Ｓ１００）と、
を有するプログラム改ざん検知方法、を電子制御装置の低消費電力モードから通常モードに移行する際にコンピュータに実行させるプログラム。

【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】０００８
【補正方法】変更
【補正の内容】
【０００８】
上記課題を解決するために、本発明の電子制御装置（１００、２００）は、
プログラムを分割したｍ個の分割プログラム、および検証用認証子を記憶する記憶部（１１、１５）と、
暗号演算により前記ｍ個の分割プログラムそれぞれのｍ個の部分認証子を生成する暗号演算部（１２、１３、３０、２２４）と、
１乃至ｎ－１番目の部分認証子を用いた論理演算を行って生成されたｎ－１番目の演算認証子と、ｎ番目の部分認証子とを用いた論理演算を行って、ｎ番目の演算認証子を生成する認証子演算部（１４、３０、２２４）、と、
前記ｎ番目の演算認証子を保存する認証子保存部（２２）と、
ｎ＋１番目の部分認証子を生成する分割プログラムを特定する情報を保存する次回生成対象保存部（２１）と、
前記検証用認証子と前記演算認証子とが一致するか否かによって前記プログラムの改ざんを検証する検証部（３０、２２４）と、
を有する。