【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4年4月13日(2022.4.13)

【公開番号】特開2020-181540(P2020-181540A)
【公開日】令和2年11月5日(2020.11.5)
【年通号数】公開・登録公報2020-045
【出願番号】特願2019-86270(P2019-86270)
【国際特許分類】
*Ｇ０６Ｆ 12/14(2006.01)*
*Ｇ０６Ｆ 21/57(2013.01)*
【ＦＩ】
Ｇ０６Ｆ 12/14 ５１０Ｄ
Ｇ０６Ｆ 21/57 ３５０

【手続補正書】
【提出日】令和4年3月31日(2022.3.31)
【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】
情報処理装置であって、
ＢＩＯＳプログラムの先頭アドレスを開始アドレスとして記憶し、かつ、前記先頭アドレスから前記ＢＩＯＳプログラムを記憶しているメモリと、
リセットが解除されると前記メモリの前記開始アドレスを参照し、前記ＢＩＯＳプログラムの前記先頭アドレスを読み出し、前記読み出された先頭アドレスから前記ＢＩＯＳプログラムを読み出して実行する第１のプロセッサと、
前記情報処理装置に電源が供給されることに従って、前記情報処理装置の起動処理を開始するブートプログラムを実行する第２のプロセッサと、を有し、
前記第２のプロセッサは、
前記ブートプログラムを実行することによって、
前記メモリに記憶されている前記ＢＩＯＳプログラムおよび前記メモリの前記開始アドレスに記憶されている前記先頭アドレスに基づくデータが、正当であるか否かを検証することを特徴とする情報処理装置。
【請求項２】
前記第２のプロセッサは、前記データが正真であると判定した場合に、前記第１のプロセッサのリセットを解除することを特徴とする請求項１に記載の情報処理装置。
【請求項３】
前記データは、前記開始アドレスから前記ＢＩＯＳプログラムの終了アドレスまでの連続したアドレスに記憶されたデータに基づくデータであることを特徴とする請求項１又は２に記載の情報処理装置。
【請求項４】
前記メモリの前記開始アドレスは、前記第１のプロセッサのリセットベクタであることを特徴とする請求項１乃至３のいずれか１項に記載の情報処理装置。
【請求項５】
前記メモリは、前記ＢＩＯＳプログラムおよび前記先頭アドレスに基づくデータを記憶し、

前記ＢＩＯＳプログラムおよび前記先頭アドレスに基づくデータは、前記ＢＩＯＳプログラムおよび前記先頭アドレスを少なくとも含む署名であることを特徴とする請求項１乃至４のいずれか１項に記載の情報処理装置。
【請求項６】
前記第２のプロセッサは、
前記署名を計算する計算手段を有し、
前記メモリから読み出した署名と前記計算された署名とが一致しているか否かに基づいて、前記検証を行うことを特徴とする請求項５に記載の情報処理装置。
【請求項７】
前記メモリは、前記署名を秘密鍵で暗号化された状態で記憶し、
前記第２のプロセッサは、
前記暗号化された状態の前記署名を前記秘密鍵と対になる公開鍵で復号化する復号化手段を有し、
前記メモリから読み出して復号化された署名と、前記計算された署名とが一致しているか否かに基づいて、前記検証を行うことを特徴とする請求項６に記載の情報処理装置。
【請求項８】
前記メモリは、
前記開始アドレスから前記ＢＩＯＳプログラムの終了アドレスまで連続したアドレスに記憶されたデータを記憶し、
前記前記開始アドレスから前記ＢＩＯＳプログラムの終了アドレスまで連続したアドレスに記憶されたデータに基づくデータは、前記開始アドレスから前記ＢＩＯＳプログラムの終了アドレスまで連続したアドレスに記憶されたデータに基づく署名であることを特徴とする請求項１乃至７のいずれか１項に記載の情報処理装置。
【請求項９】
前記署名とは、ハッシュ値であることを特徴とする請求項５乃至８のいずれか１項に記載の情報処理装置。
【請求項１０】
前記第１のプロセッサは、前記第２のプロセッサが前記ブートプログラムによって前記検証を行った後、前記ＢＩＯＳプログラムを実行することを特徴とする請求項９に記載の情報処理装置。
【請求項１１】
前記第２のプロセッサは、前記検証を行なった後、前記第１のプロセッサをリセットおよび該リセットの解除を行い、
前記第１のプロセッサは、前記第２のプロセッサによってリセットが解除されると、前記ＢＩＯＳプログラムを実行することを特徴とする請求項１０に記載の情報処理装置。
【請求項１２】
ＢＩＯＳプログラムの先頭アドレスを開始アドレスとして記憶し、かつ、前記先頭アドレスから前記ＢＩＯＳプログラムを記憶しているメモリと、リセットが解除されると前記メモリの前記開始アドレスを参照し、前記ＢＩＯＳプログラムの前記先頭アドレスを読み出し、前記読み出された先頭アドレスから前記ＢＩＯＳプログラムを読み出して実行する第１のプロセッサと、装置に電源が供給されることに従って、前記装置の起動処理を開始するブートプログラムを実行する第２のプロセッサと、を有する装置のデータ検証方法であって、
前記第２のプロセッサが前記ブートプログラムを実行する工程と、
前記メモリに記憶されている前記ＢＩＯＳプログラムおよび前記メモリの前記開始アドレスに記憶されている前記先頭アドレスに基づくデータが、正当であるか否かを検証する工程を有することを特徴とするデータ検証方法。
【請求項１３】
前記検証によって前記データが正真であると判定した場合に、前記第１のプロセッサのリセットを解除する工程を有することを特徴とする請求項１２に記載のデータ検証方法。

【請求項１４】
前記検証されるデータは、前記開始アドレスから前記ＢＩＯＳプログラムの終了アドレスまで連続したアドレスに記憶されたデータに基づくデータであることを特徴とする請求項１２又は１３に記載のデータ検証方法。
【請求項１５】
前記メモリの前記開始アドレスは、前記第１のプロセッサのリセットベクタであることを特徴とする請求項１２乃至１４のいずれか１項に記載のデータ検証方法。
【請求項１６】
前記メモリは、
前記ＢＩＯＳプログラムおよび前記先頭アドレスに基づくデータを記憶し、
前記ＢＩＯＳプログラムおよび前記先頭アドレスに基づくデータは、前記ＢＩＯＳプログラムおよび前記先頭アドレスを少なくとも含む署名であることを特徴とする請求項１２乃至１５のいずれか１項に記載のデータ検証方法。
【請求項１７】
前記第２のプロセッサは、
前記署名を計算する計算手段を有し、
前記メモリから読み出した署名と前記計算された署名とが一致しているか否かに基づいて、前記検証を行うことを特徴とする請求項１６に記載のデータ検証方法。
【請求項１８】
前記メモリは、
前記開始アドレスから前記ＢＩＯＳプログラムの終了アドレスまで連続したアドレスに記憶されたデータを記憶し、
前記前記開始アドレスから前記ＢＩＯＳプログラムの終了アドレスまで連続したアドレスに記憶されたデータに基づくデータは、前記開始アドレスから前記ＢＩＯＳプログラムの終了アドレスまで連続したアドレスに記憶されたデータに基づく署名であることを特徴とする請求項１２乃至１７のいずれか１項に記載のデータ判定方法。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】０００７
【補正方法】変更
【補正の内容】
【０００７】
本発明の情報処理装置は、ＢＩＯＳプログラムの先頭アドレスを開始アドレスとして記憶し、かつ、前記先頭アドレスから前記ＢＩＯＳプログラムを記憶しているメモリと、リセットが解除されると前記メモリの前記開始アドレスを参照し、前記ＢＩＯＳプログラムの前記先頭アドレスを読み出し、前記読み出された先頭アドレスから前記ＢＩＯＳプログラムを読み出して実行する第１のプロセッサと、前記情報処理装置に電源が供給されることに従って、前記情報処理装置の起動処理を開始するブートプログラムを実行する第２のプロセッサと、を有し、前記第２のプロセッサは、前記ブートプログラムを実行することによって、ＢＩＯＳプログラムおよび前記メモリの前記開始アドレスに記憶されている前記先頭アドレスに基づくデータが、正当であるか否かを検証することを特徴とする情報処理装置。