【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30年10月4日(2018.10.4)

【公開番号】特開2016-81517(P2016-81517A)
【公開日】平成28年5月16日(2016.5.16)
【年通号数】公開・登録公報2016-029
【出願番号】特願2015-159129(P2015-159129)
【国際特許分類】
Ｇ０６Ｆ　21/57　　(2013.01)
【ＦＩ】
Ｇ０６Ｆ　21/57

【手続補正書】
【提出日】平成30年8月20日(2018.8.20)
【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】
通常のプログラム実行モードであるノーマルモードと、予め定めた最低限のソフトウェアモジュールを実行するセーフモードとのいずれかのモードで動作する情報処理装置であって、
起動モードがセーフモードとノーマルモードのいずれであるかを検知する検知手段と、
前記情報処理装置のセキュリティを管理するセキュリティ管理手段とを有し、
前記セキュリティ管理手段は、前記検知手段により検知したモードに応じて、前記情報処理装置を監視する複数の手段のいずれかを利用することを特徴とする情報処理装置。
【請求項２】
前記セキュリティ管理手段による監視の対象は、デバイスの接続の可否を含み、前記セキュリティ管理手段は、前記検知手段により検知したモードに応じて、前記デバイスの接続を監視する複数の手段のいずれかを利用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】
前記セキュリティ管理手段による監視の対象は、ネットワークアクセスの可否を含み、前記セキュリティ管理手段は、前記検知手段により検知したモードに応じて、前記ネットワークアクセスを監視する複数の手段のいずれかを利用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４】
前記セキュリティ管理手段による監視の対象は、プロセスの起動の可否を含み、前記セキュリティ管理手段は、前記検知手段により検知したモードに応じて、前記プロセスの起動を監視する複数の手段のいずれかを利用する
を特徴とする請求項１に記載の情報処理装置。
【請求項５】
前記セキュリティ管理手段による監視の対象は、ログインの可否を含み、前記セキュリティ管理手段は、前記検知手段により検知したモードに応じて、前記ログインを監視する複数の手段のいずれかを利用する
を特徴とする請求項１に記載の情報処理装置。
【請求項６】

前記セキュリティ管理手段による監視の対象は、ファイル共有の可否を含み、前記セキュリティ管理手段は、前記検知手段により検知したモードに応じて、前記ファイル共有を監視する複数の手段のいずれかを利用する
を特徴とする請求項１に記載の情報処理装置。
【請求項７】
前記セキュリティ管理手段は、前記監視する手段にて監視されたネットワークアクセスを記録することを特徴とする請求項３に記載の情報処理装置。
【請求項８】
前記セキュリティ管理手段は、前記セーフモードの場合にはデバイスの接続を示すメッセージを監視することでデバイスの接続を監視することを特徴とする請求項２に記載の情報処理装置。
【請求項９】
前記セキュリティ管理手段は、接続を検知したデバイスの使用が禁止されている場合、前記セーフモードであれば当該デバイスを使用不可の状態にすることで当該デバイスの使用を禁止することを特徴とする請求項２または８に記載の情報処理装置。
【請求項１０】
前記セキュリティ管理手段は、接続を検知したデバイスの使用が禁止されている場合、前記セーフモードであれば当該デバイスに対する入出力を遮断することで当該デバイスの使用を禁止することを特徴とする請求項２または８に記載の情報処理装置。
【請求項１１】
前記セキュリティ管理手段は、接続を検知したデバイスの使用が禁止されている場合、前記セーフモードであれば、さらに当該デバイスの使用が禁止されていることを示すメッセージをユーザに通知することを特徴とする請求項９または１０に記載の情報処理装置。
【請求項１２】
前記セキュリティ管理手段は、前記デバイスに対する入出力を遮断した後、当該デバイスが前記情報処理装置から取り外されたならば遮断を解除することを特徴とする請求項１１に記載の情報処理装置。
【請求項１３】
前記セキュリティ管理手段は、前記デバイスに対する入出力を遮断した後、所定時間内に当該デバイスが前記情報処理装置から取り外されないならば、ログイン中のユーザをログオフするか、あるいは前記情報処理装置をシャットダウンすることを特徴とする請求項１１または１２に記載の情報処理装置。
【請求項１４】
通常のプログラム実行モードであるノーマルモードと、予め定めた最低限のソフトウェアモジュールを実行するセーフモードとのいずれかのモードで動作する情報処理装置におけるセキュリティ管理方法であって、
検知手段が、起動モードがセーフモードとノーマルモードのいずれであるかを検知する検知工程と、
セキュリティ管理手段が、前記情報処理装置のセキュリティを管理するセキュリティ管理工程とを有し、
前記セキュリティ管理工程では、前記検知工程により検知したモードに応じて、前記情報処理装置を監視する複数の手段のいずれかを利用することを特徴とするセキュリティ管理方法。
【請求項１５】
通常のプログラム実行モードであるノーマルモードと、予め定めた最低限のソフトウェアモジュールを実行するセーフモードとのいずれかのモードで動作する情報処理システムであって、
起動モードがセーフモードとノーマルモードのいずれであるかを検知する検知手段と、
前記情報処理システムのセキュリティを管理するセキュリティ管理手段とを有し、
前記セキュリティ管理手段は、前記検知手段により検知したモードに応じて、前記情報

処理システムを監視する複数の手段のいずれかを利用することを特徴とする情報処理システム。
【請求項１６】
通常のプログラム実行モードであるノーマルモードと、予め定めた最低限のソフトウェアモジュールを実行するセーフモードとのいずれかのモードで動作するコンピュータを、
起動モードがセーフモードとノーマルモードのいずれであるかを検知する検知手段と、
前記コンピュータのセキュリティを管理するセキュリティ管理手段として機能させるためのプログラムであって、
前記セキュリティ管理手段は、前記検知手段により検知したモードに応じて、前記コンピュータを監視する複数の手段のいずれかを利用することを特徴とするプログラム。
【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】
上記目的を達成するために本発明は以下の構成を有する。すなわち、
通常のプログラム実行モードであるノーマルモードと、予め定めた最低限のソフトウェアモジュールを実行するセーフモードとのいずれかのモードで動作する情報処理装置であって、
起動モードがセーフモードとノーマルモードのいずれであるかを検知する検知手段と、
前記情報処理装置のセキュリティを管理するセキュリティ管理手段とを有し、
前記セキュリティ管理手段は、前記検知手段により検知したモードに応じて、前記情報処理装置を監視する複数の手段のいずれかを利用することを特徴とする。