【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28年3月17日(2016.3.17)

【公開番号】特開2013-178764(P2013-178764A)
【公開日】平成25年9月9日(2013.9.9)
【年通号数】公開・登録公報2013-049
【出願番号】特願2013-26487(P2013-26487)
【国際特許分類】
Ｇ０６Ｆ　21/57　(2013.01)
Ｇ０６Ｆ　13/10　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　21/00　１５７Ａ
Ｇ０６Ｆ　13/10　３４０Ａ

【手続補正書】
【提出日】平成28年1月28日(2016.1.28)
【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】
コンピュータシステムにおいて、
アプリケーションを実行するように構成されている第１のハードウェアプロセッサを備える第１のハードウェアサブシステムと、
セキュリティファームウェアを実行するように構成されている第２の別個のハードウェアプロセッサを備える第２のハードウェアサブシステムと、
前記第２のハードウェアサブシステムに接続されている周辺機器と、ここにおいて、前記アプリケーションによる前記接続されている周辺機器へのアクセスは、前記第１のハードウェアサブシステムの対応する周辺接続をエミュレートする、前記第２のハードウェアプロセッサ上で実行している前記セキュリティファームウェアにより選択的に妨げられる、
を具備し、
前記周辺機器は、ビデオディスプレイを備え、
前記コンピュータシステムは、前記第１のハードウェアサブシステムに接続される第１の入力と、前記第２のハードウェアサブシステムに接続される第２の入力と、前記ビデオディスプレイに接続される出力とを有するビデオマルチプレクサをさらに具備し、
前記出力を導出するための、前記第１の入力および前記第２の入力からのコンテンツの選択は、前記第２のハードウェアプロセッサ上で実行している前記セキュリティファームウェアにより制御される、コンピュータシステム。
【請求項２】
前記周辺機器は、キーボードをさらに備え、前記セキュリティファームウェアは、スタートアップシーケンスを含み、前記キーボード、および、前記ビデオディスプレイのための前記出力は、前記第２のハードウェアプロセッサにより排他的に制御され、前記第１のハードウェアプロセッサによる前記キーボードおよびビデオディスプレイへのアクセスは妨げられる請求項１記載のコンピュータシステム。
【請求項３】
前記周辺機器は、前記第１のハードウェアサブシステムのためのオペレーティングシス

テムおよびアプリケーションソフトウェアを含むディスクドライブを備え、
前記システムは、前記セキュリティファームウェアにより維持されるエミュレートされたディスクドライブをさらに具備し、
前記第１のハードウェアプロセッサによる、前記ディスクドライブ上の前記オペレーティングシステムおよびアプリケーションソフトウェアへのアクセスは、前記エミュレートされたディスクドライブを介して制御される請求項１記載のコンピュータシステム。
【請求項４】
前記セキュリティファームウェアは、前記エミュレートされたディスクドライブの１つ以上の時間特有な画像を維持する請求項３記載のコンピュータシステム。
【請求項５】
前記ディスクドライブは、ソリッドステートディスクドライブを含む請求項３記載のコンピュータシステム。
【請求項６】
前記セキュリティファームウェアは、前記ディスクドライブ上のすべてのデータを暗号化し、前記暗号化のためのキーは、前記セキュリティファームウェアにより排他的に維持される請求項３記載のコンピュータシステム。
【請求項７】
前記周辺機器は、ネットワーク接続を備え、前記セキュリティファームウェアは、前記第１のハードウェアサブシステムによる外部ネットワークへのアクセスを制御する請求項１記載のコンピュータシステム。
【請求項８】
前記第１のハードウェアサブシステムと前記外部ネットワークとの間のすべての通信のために、前記セキュリティファームウェアにより維持されているＶＰＮトンネルをさらに具備する請求項７記載のコンピュータシステム。
【請求項９】
コンピュータシステムを守る方法において、
アプリケーションを実行する第１のハードウェアプロセッサを備える、前記コンピュータシステムの第１のハードウェアサブシステムを構成することと、
セキュリティファームウェアを実行する第２の別個のハードウェアプロセッサを備える、前記コンピュータシステムの第２のハードウェアサブシステムを構成することと、
周辺機器を前記第２のハードウェアサブシステムに接続することと、
前記第１のハードウェアサブシステムの対応する周辺接続をエミュレートする、前記第２のハードウェアプロセッサ上で実行している前記セキュリティファームウェアを使用して、前記アプリケーションによる前記接続されている周辺機器へのアクセスを選択的に妨げることと、
含み、
前記周辺機器は、ビデオディスプレイを備え、
前記方法は、
ビデオマルチプレクサを前記コンピュータシステム中に提供することと、
前記ビデオマルチプレクサの第１の入力を前記第１のハードウェアサブシステムに接続することと、
前記ビデオマルチプレクサの接続されている第２の入力を前記第２のハードウェアサブシステムに接続することと、
前記ビデオマルチプレクサの出力を前記ビデオディスプレイに接続することと、
前記第２のハードウェアプロセッサ上で実行している前記セキュリティファームウェアを使用して、前記出力を導出するための、前記第１の入力および前記第２の入力からのコンテンツの選択を制御することとをさらに含む、方法。
【請求項１０】
前記周辺機器は、キーボードをさらに備え、
前記方法は、前記セキュリティファームウェアにより実行されるスタートアップシーケ

ンスをさらに含み、
前記キーボード、および、前記ビデオディスプレイのための前記出力は、前記第２のハードウェアプロセッサにより排他的に制御され、前記第１のハードウェアプロセッサによる、前記キーボードおよびビデオディスプレイへのアクセスは妨げられる請求項９記載の方法。
【請求項１１】
前記周辺機器は、前記第１のハードウェアサブシステムのためのオペレーティングシステムおよびアプリケーションソフトウェアを含むディスクドライブを備え、
前記方法は、前記セキュリティファームウェアを使用して、エミュレートされたディスクドライブを維持することをさらに含み、
前記第１のハードウェアプロセッサによる、前記ディスクドライブ上の前記オペレーティングシステムおよびアプリケーションソフトウェアへのアクセスは、前記エミュレートされたディスクドライブを介して制御される請求項９記載の方法。
【請求項１２】
前記セキュリティファームウェアを使用して、前記エミュレートされたディスクドライブの１つ以上の時間特有な画像を維持することをさらに含む請求項１１記載の方法。
【請求項１３】
前記ディスクドライブは、ソリッドステートディスクドライブを含む請求項１１記載の方法。
【請求項１４】
前記セキュリティファームウェアを使用して、前記ディスクドライブ上のすべてのデータを暗号化することと、
前記暗号化のためのキーを、前記セキュリティファームウェアにより排他的に維持することとをさらに含む請求項１１記載の方法。
【請求項１５】
前記周辺機器は、ネットワーク接続を備え、
前記方法は、前記セキュリティファームウェアを使用して、前記第１のハードウェアサブシステムによる外部ネットワークへのすべてのアクセスを制御することをさらに含む請求項９記載の方法。
【請求項１６】
前記セキュリティファームウェアを使用して、前記第１のハードウェアサブシステムと前記外部ネットワークとの間のすべての通信のために、ＶＰＮトンネルを維持することをさらに含む請求項１５記載の方法。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００６６
【補正方法】変更
【補正の内容】
【００６６】
本発明は、その好ましい実施形態を参照して、特に記述されているが、本発明の精神および範囲から逸脱することなく、形式および詳細における変更および修正を行うことができることは当業者にとって容易に明らかであるべきである。付随の特許請求の範囲は、このような変更および修正を含むことが意図されている。
以下に、本願出願当初の特許請求の範囲に記載された発明を付記する。
［Ｃ１］
コンピュータシステムにおいて、
アプリケーションを実行するように構成されている第１のプロセッサを備える第１のサブシステムと、
セキュリティファームウェアを実行するように構成されている第２の別個のプロセッサを備える第２のサブシステムと、

前記第２のサブシステムに接続されている周辺機器とを具備し、
前記アプリケーションによる前記周辺機器へのアクセスは、前記第１のサブシステムの対応する周辺接続をエミュレートする、前記第２のプロセッサ上で実行している前記セキュリティファームウェアにより制御されるコンピュータシステム。
［Ｃ２］
前記周辺機器は、ビデオディスプレイを備え、
前記コンピュータシステムは、前記第１のサブシステムに接続される第１の入力と、前記第２のサブシステムに接続される第２の入力と、前記ビデオディスプレイに接続される出力とを有するビデオマルチプレクサをさらに具備し、
前記出力を導出するための、前記第１の入力および前記第２の入力からのコンテンツの選択は、前記第２のプロセッサ上で実行している前記セキュリティファームウェアにより制御される［Ｃ１］記載のコンピュータシステム。
［Ｃ３］
前記周辺機器は、キーボードをさらに備え、前記セキュリティファームウェアは、スタートアップシーケンスを含み、前記キーボード、および、前記ビデオディスプレイのための前記出力は、前記第２のプロセッサにより排他的に制御され、前記第１のプロセッサによる前記キーボードおよびビデオディスプレイへのアクセスは妨げられる［Ｃ２］記載のコンピュータシステム。
［Ｃ４］
前記周辺機器は、前記第１のプロセッササブシステムのためのオペレーティングシステムおよびアプリケーションソフトウェアを含むディスクドライブを備え、
前記システムは、前記セキュリティファームウェアにより維持されるエミュレートされたディスクドライブをさらに具備し、
前記第１のプロセッサによる、前記ディスクドライブ上の前記オペレーティングシステムおよびアプリケーションソフトウェアへのアクセスは、前記エミュレートされたディスクドライブを介して制御される［Ｃ１］記載のコンピュータシステム。
［Ｃ５］
前記セキュリティファームウェアは、前記エミュレートされたディスクドライブの１つ以上の時間特有な画像を維持する［Ｃ４］記載のコンピュータシステム。
［Ｃ６］
前記ディスクドライブは、ソリッドステートディスクドライブを含む［Ｃ４］記載のコンピュータシステム。
［Ｃ７］
前記セキュリティファームウェアは、前記ディスクドライブ上のすべてのデータを暗号化し、前記暗号化のためのキーは、前記セキュリティファームウェアにより排他的に維持される［Ｃ４］記載のコンピュータシステム。
［Ｃ８］
前記周辺機器は、ネットワーク接続を備え、前記セキュリティファームウェアは、前記第１のサブシステムによる外部ネットワークへのアクセスを制御する［Ｃ１］記載のコンピュータシステム。
［Ｃ９］
前記第１のサブシステムと前記外部ネットワークとの間のすべての通信のために、前記セキュリティファームウェアにより維持されているＶＰＮトンネルをさらに具備する［Ｃ８］記載のコンピュータシステム。
［Ｃ１０］
コンピュータシステムを守る方法において、
アプリケーションを実行する第１のプロセッサを備える、前記コンピュータシステムの第１のサブシステムを構成することと、
セキュリティファームウェアを実行する第２の別個のプロセッサを備える、前記コンピュータシステムの第２のサブシステムを構成することと、

周辺機器を前記第２のサブシステムに接続することと、
前記第１のサブシステムの対応する周辺接続をエミュレートする、前記第２のプロセッサ上で実行している前記セキュリティファームウェアを使用して、前記アプリケーションによる前記周辺機器へのアクセスを制御することとを含む方法。
［Ｃ１１］
前記周辺機器は、ビデオディスプレイを備え、
前記方法は、
ビデオマルチプレクサを前記コンピュータシステム中に提供することと、
前記ビデオマルチプレクサの第１の入力を前記第１のサブシステムに接続することと、
前記ビデオマルチプレクサの接続されている第２の入力を前記第２のサブシステムに接続することと、
前記ビデオディスプレイの出力を前記ビデオディスプレイに接続することと、
前記第２のプロセッサ上で実行している前記セキュリティファームウェアを使用して、前記出力を導出するための、前記第１の入力および前記第２の入力からのコンテンツの選択を制御することとをさらに含む［Ｃ１０］記載の方法。
［Ｃ１２］
前記周辺機器は、キーボードをさらに備え、
前記方法は、前記セキュリティファームウェアにより実行されるスタートアップシーケンスをさらに含み、
前記キーボード、および、前記ビデオディスプレイのための前記出力は、前記第２のプロセッサにより排他的に制御され、前記第１のプロセッサによる、前記キーボードおよびビデオディスプレイへのアクセスは妨げられる［Ｃ１１］記載の方法。
［Ｃ１３］
前記周辺機器は、前記第１のプロセッササブシステムのためのオペレーティングシステムおよびアプリケーションソフトウェアを含むディスクドライブを備え、
前記方法は、前記セキュリティファームウェアを使用して、エミュレートされたディスクドライブを維持することをさらに含み、
前記第１のプロセッサによる、前記ディスクドライブ上の前記オペレーティングシステムおよびアプリケーションソフトウェアへのアクセスは、前記エミュレートされたディスクドライブを介して制御される［Ｃ１０］記載の方法。
［Ｃ１４］
前記セキュリティファームウェアを使用して、前記エミュレートされたディスクドライブの１つ以上の時間特有な画像を維持することをさらに含む［Ｃ１３］記載の方法。
［Ｃ１５］
前記ディスクドライブは、ソリッドステートディスクドライブを含む［Ｃ１３］記載の方法。
［Ｃ１６］
前記セキュリティファームウェアを使用して、前記ディスクドライブ上のすべてのデータを暗号化することと、
前記暗号化のためのキーを、前記セキュリティファームウェアにより排他的に維持することとをさらに含む［Ｃ１３］記載の方法。
［Ｃ１７］
前記周辺機器は、ネットワーク接続を備え、
前記方法は、前記セキュリティファームウェアを使用して、前記第１のサブシステムによる外部ネットワークへのすべてのアクセスを制御することをさらに含む［Ｃ１０］記載の方法。
［Ｃ１８］
前記セキュリティファームウェアを使用して、前記第１のサブシステムと前記外部ネットワークとの間のすべての通信のために、ＶＰＮトンネルを維持することをさらに含む［Ｃ１７］記載の方法。

［Ｃ１９］
システムにおいて、
独立型コンピュータシステムと、
前記独立型コンピュータシステムを制御する組織によりホストされた安全なイントラネットとを具備し、
前記独立型コンピュータシステムは、
アプリケーションを実行するように構成されている第１のプロセッサを備える第１のサブシステムと、
セキュリティファームウェアを実行するように構成されている第２の別個のプロセッサを備える第２のサブシステムとを備え、
前記アプリケーションによる前記安全なイントラネットへのアクセスは、前記第１のサブシステムの対応する周辺ネットワーク接続をエミュレートする、前記第２のプロセッサ上で実行している前記セキュリティファームウェアにより制御されるシステム。
［Ｃ２０］
前記独立型コンピュータシステムは、ノートブックコンピュータを含む［Ｃ１９］記載のシステム。