【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17年8月25日(2005.8.25)

【公開番号】特開2003-16403(P2003-16403A)
【公開日】平成15年1月17日(2003.1.17)
【出願番号】特願2001-194748(P2001-194748)
【国際特許分類第７版】
　Ｇ０６Ｋ　19/07
　Ｂ４２Ｄ　15/10
　Ｇ０６Ｆ　 1/00
　Ｇ０６Ｆ　12/00
　Ｇ０６Ｆ　12/14
【ＦＩ】
　Ｇ０６Ｋ　19/00　　Ｎ
　Ｂ４２Ｄ　15/10　　５２１
　Ｇ０６Ｆ　12/00　　５２０Ｐ
　Ｇ０６Ｆ　12/00　　５３７Ｍ
　Ｇ０６Ｆ　12/14　　３２０Ｃ
　Ｇ０６Ｆ　 9/06　　６６０Ｄ

【手続補正書】
【提出日】平成17年2月22日(2005.2.22)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
　メモリ領域と、
　前記メモリ領域を各アプリケーションに割り当てるメモリ割当手段と、
　前記メモリ領域に割り当てられた各アプリケーションに対して、アクセス権を制御するための暗証コードを設定する暗証コード設定手段と、
　前記メモリ領域に割り当てられた各アプリケーションのアクセス可否状態を管理するアクセス可否状態管理手段とを備え、
　前記アクセス可否状態管理手段は、暗証コードが設定されたアプリケーションをデフォルトではアクセス不可状態とし、ユーザから入力された暗証コードが一致したことに応答して該当するアプリケーションをアクセス許可状態に設定する、
ことを特徴とする集積回路装置。
【請求項２】
　前記メモリ割当手段は、ディレクトリを用いて階層的にアプリケーションにメモリ領域を割り当て、
　前記暗証コード設定手段は、各アプリケーション及びディレクトリに対して、アクセス権を制御するための暗証コードを設定し、
　前記アクセス可否状態管理手段は、暗証コードが設定されたアプリケーション及びディレクトリをデフォルトではアクセス不可状態とし、ユーザから入力された暗証コードが一致したことに応答して該当するアプリケーション又はディレクトリをアクセス許可状態に設定する、
ことを特徴とする請求項１に記載の集積回路装置。

【請求項３】
前記アクセス可否状態管理手段は、ユーザから入力された暗証コードがディレクトリに設定された暗証コードと一致したことに応答して、該ディレクトリ以下のすべてのアプリケーション及びサブディレクトリをアクセス許可状態にする、
ことを特徴とする請求項２に記載の集積回路装置。
【請求項４】
前記メモリ領域に割り当てられた各アプリケーションに対して、認証用の秘密鍵を設定する秘密鍵設定手段をさらに備え、
前記アクセス可否状態管理手段は、所定の認証局との間で秘密鍵を用いた相互認証を経て、アクセス不可状態のアプリケーションをアクセス許可状態に設定する、
ことを特徴とする請求項１に記載の集積回路装置。
【請求項５】
前記メモリ領域に割り当てられた各アプリケーション及びディレクトリに対して、認証用の秘密鍵を設定する秘密鍵設定手段をさらに備え、
前記アクセス可否状態管理手段は、所定の認証局との間で秘密鍵を用いた相互認証を経て、アクセス不可状態のアプリケーション又はディレクトリをアクセス許可状態に設定する、
ことを特徴とする請求項２に記載の集積回路装置。
【請求項６】
当該装置への電源が遮断されたことに応答してアクセス許可状態のアプリケーションをアクセス不可状態に戻す、アクセス禁止手段をさらに備える、
ことを特徴とする請求項１に記載の集積回路装置。
【請求項７】
当該装置への電源が遮断されたことに応答してアクセス許可状態のアプリケーション並びにディレクトリをアクセス不可状態に戻すアクセス禁止手段をさらに備える、
ことを特徴とする請求項２に記載の集積回路装置。
【請求項８】
前記メモリ領域に割り当てられた各アプリケーションに対する暗証コードの入力失敗回数を保持する入力失敗回数保持手段と、
前記メモリ領域に割り当てられた各アプリケーションに対する暗証コードの最大許容入力失敗回数を設定する最大許容入力失敗回数設定手段とをさらに備え、
前記アクセス可否状態管理手段は、入力失敗回数が最大許容入力回数に到達したアプリケーションをアクセス不可状態に設定する、
ことを特徴とする請求項１に記載の集積回路装置。
【請求項９】
前記メモリ領域に割り当てられた各アプリケーション及びディレクトリに対する暗証コードの入力失敗回数を保持する入力失敗回数保持手段と、
前記メモリ領域に割り当てられた各アプリケーション及びディレクトリに対する暗証コードの最大許容入力失敗回数を設定する最大許容入力失敗回数設定手段とをさらに備え、
前記アクセス可否状態管理手段は、入力失敗回数が最大許容入力回数に到達したアプリケーション又はディレクトリをアクセス不可状態に設定する、
ことを特徴とする請求項２に記載の集積回路装置。
【請求項１０】
所定の認証局との相互認証処理を経た管理者によって前記入力失敗回数保持手段に保持された入力失敗回数をクリアする入力失敗回数初期化手段をさらに備える、
ことを特徴とする請求項８又は９のいずれかに記載の集積回路装置。
【請求項１１】
請求項１に記載の集積回路装置を搭載することを特徴とする情報処理装置。
【請求項１２】
前記情報処理装置は情報記憶媒体であ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】
前記情報記憶媒体はＩＣカード型の記憶媒体であることを特徴とする請求項１２に記載の情報処理装置。
【請求項１４】
情報記憶装置のメモリ管理方法であって、
前記メモリ領域を各アプリケーションに割り当てるメモリ割当ステップと、
前記メモリ領域に割り当てられた各アプリケーションに対して、アクセス権を制御するための暗証コードを設定する暗証コード設定ステップと、
前記メモリ領域に割り当てられた各アプリケーションのアクセス可否状態を管理するアクセス可否状態管理ステップと、
を備え、
前記アクセス可否状態管理ステップでは、暗証コードが設定されたアプリケーションをデフォルトではアクセス不可状態とし、ユーザから入力された暗証コードが一致したことに応答して該当するアプリケーションをアクセス許可状態に設定する、
ことを特徴とする情報記憶装置のメモリ管理方法。
【請求項１５】
前記メモリ割当ステップでは、ディレクトリを用いて階層的にアプリケーションにメモリ領域を割り当て、
前記暗証コード設定ステップでは、各アプリケーション及びディレクトリに対して、アクセス権を制御するための暗証コードを設定し、
前記アクセス可否状態管理ステップでは、暗証コードが設定されたアプリケーション及びディレクトリをデフォルトではアクセス不可状態とし、ユーザから入力された暗証コードが一致したことに応答して該当するアプリケーション又はディレクトリをアクセス許可状態に設定する、
ことを特徴とする請求項１４に記載の情報記憶装置のメモリ管理方法。
【請求項１６】
前記アクセス可否状態管理ステップでは、ユーザから入力された暗証コードがディレクトリに設定された暗証コードと一致したことに応答して、該ディレクトリ以下のすべてのアプリケーション及びサブディレクトリをアクセス許可状態にする、
ことを特徴とする請求項１５に記載の情報記憶装置のメモリ管理方法。
【請求項１７】
前記メモリ領域に割り当てられた各アプリケーションに対して、認証用の秘密鍵を設定する秘密鍵設定ステップをさらに備え、
前記アクセス可否状態管理ステップでは、所定の認証局との間で秘密鍵を用いた相互認証を経て、アクセス不可状態のアプリケーションをアクセス許可状態に設定する、
ことを特徴とする請求項１４に記載の情報記憶装置のメモリ管理方法。
【請求項１８】
前記メモリ領域に割り当てられた各アプリケーション及びディレクトリに対して、認証用の秘密鍵を設定する秘密鍵設定ステップをさらに備え、
前記アクセス可否状態管理ステップでは、所定の認証局との間で秘密鍵を用いた相互認証を経て、アクセス不可状態のアプリケーション又はディレクトリをアクセス許可状態に設定する、
ことを特徴とする請求項１５に記載の情報記憶装置のメモリ管理方法。
【請求項１９】
前記情報記憶装置への電源が遮断されたことに応答してアクセス許可状態のアプリケーションをアクセス不可状態に戻すアクセス禁止ステップをさらに備える、
ことを特徴とする請求項１４に記載の情報記憶装置のメモリ管理方法。
【請求項２０】
前記情報記憶装置への電源が遮断されたことに応答してアクセス許可状態のアプリケー

ション並びにディレクトリをアクセス不可状態に戻すアクセス禁止ステップをさらに備える、
ことを特徴とする請求項１５に記載の情報記憶装置のメモリ管理方法。
【請求項２１】
前記メモリ領域に割り当てられた各アプリケーションに対する暗証コードの入力失敗回数を保持する入力失敗回数保持ステップと、
前記メモリ領域に割り当てられた各アプリケーションに対する暗証コードの最大許容入力失敗回数を設定する最大許容入力失敗回数設定ステップとを備え、
前記アクセス可否状態管理ステップでは、入力失敗回数が最大許容入力回数に到達したアプリケーションをアクセス不可状態に設定する、
ことを特徴とする請求項１４に記載の情報記憶装置のメモリ管理方法。
【請求項２２】
前記メモリ領域に割り当てられた各アプリケーション及びディレクトリに対する暗証コードの入力失敗回数を保持する入力失敗回数保持ステップと、
前記メモリ領域に割り当てられた各アプリケーション及びディレクトリに対する暗証コードの最大許容入力失敗回数を設定する最大許容入力失敗回数設定ステップとをさらに備え、
前記アクセス可否状態管理ステップでは、入力失敗回数が最大許容入力回数に到達したアプリケーション又はディレクトリをアクセス不可状態に設定する、
ことを特徴とする請求項１５に記載の情報記憶装置のメモリ管理方法。
【請求項２３】
所定の認証局との相互認証処理を経た管理者によって前記入力失敗回数保持ステップにより保持された入力失敗回数をクリアする入力失敗回数初期化ステップをさらに備える、
ことを特徴とする請求項１４又は１５のいずれかに記載の情報記憶装置のメモリ管理方法。