(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5490114号
(P5490114)

(45)発行日　平成26年5月14日(2014.5.14)　(24)登録日　平成26年3月7日(2014.3.7)

(51)Int.Cl.		F I		
G06F 21/60	(2013.01)	G06F	21/24	160B
G01R 31/28	(2006.01)	G01R	31/28	V
G06F 21/62	(2013.01)	G06F	21/24	165A

請求項の数 7　(全 13 頁)

(21)出願番号	特願2011-517840 (P2011-517840)
(86)(22)出願日	平成21年6月22日 (2009.6.22)
(65)公表番号	特表2011-528144 (P2011-528144A)
(43)公表日	平成23年11月10日 (2011.11.10)
(86)国際出願番号	PCT/EP2009/057717
(87)国際公開番号	WO2010/006879
(87)国際公開日	平成22年1月21日 (2010.1.21)
審査請求日	平成24年6月7日 (2012.6.7)
(31)優先権主張番号	61/080,414
(32)優先日	平成20年7月14日 (2008.7.14)
(33)優先権主張国	米国(US)
(31)優先権主張番号	08172216.7
(32)優先日	平成20年12月18日 (2008.12.18)
(33)優先権主張国	欧州特許庁(EP)

(73)特許権者　598036300
テレフオンアクチーボラゲット　エル　エム　エリクソン(パブル)
スウェーデン国　ストックホルム　エス－１６４　８３
(74)代理人　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(74)代理人　100130409
弁理士　下山　治

最終頁に続く

(54)【発明の名称】集積回路、方法および電子機器

(57)【特許請求の範囲】

【請求項１】

ユーティリティ動作に対して構成されている第１のセキュリティ動作状態と、テスト動作に対して構成されている第２のセキュリティ動作状態とを有する集積回路に対する方法であって、

前記第２のセキュリティ動作状態で動作している場合に、

第１のオブジェクトのセットと第２のオブジェクトのセットを利用可にするステップと、

第３のオブジェクトのセットを利用不可にするステップとを備え、

前記第１のセキュリティ動作状態で動作している場合に、

前記第１のセキュリティ動作状態のセキュリティメカニズムによる認可に応じて、前記第３のオブジェクトのセットを利用可にするステップとを備え、

前記第１のセキュリティ動作状態で動作している場合に、

前記セキュリティメカニズムによって、前記第２のオブジェクトのセットを利用不可にし、かつ前記セキュリティメカニズムによる認可に応じて、前記第１のオブジェクトのセットを利用可にするステップとを備え、

前記第２のセキュリティ動作状態で動作している場合に、前記第３のオブジェクトのセットを利用不可にするステップは、前記集積回路のロジック回路によって実行され、かつ、前記ロジック回路によって前記第２のセキュリティ動作状態で動作している場合に、前記第３のオブジェクトのセットを備える前記集積回路の一部を制限する動作を制御するこ

とを含み、
前記オブジェクトは、機能、情報、及び信号の少なくとも１つであり、
前記方法は、更に、
前記第２のセキュリティ動作状態に入る場合に、極秘情報あるいは機密情報を削除するステップと、
前記第２のセキュリティ動作状態を終了する場合に、更なる実行に影響を与える状態を削除し、そして、前記第１のセキュリティ動作状態の前記セキュリティメカニズムをバイパスすることを防止するために前記第１のセキュリティ動作状態へ戻るステップとを備える
ことを特徴とする方法。
【請求項２】
前記第１のセキュリティ動作状態の場合と前記第２のセキュリティ動作状態の場合との両方で、第４のオブジェクトのセットを利用可にするステップを更に備える
ことを特徴とする請求項１に記載の方法。
【請求項３】
テストリクエストを受信するステップと、
前記テストリクエストの受信に応じて、前記第２のセキュリティ動作状態に入るステップと
を更に備えることを特徴とする請求項１または２に記載の方法。
【請求項４】
前記テストリクエストを受信するステップは、テストポートへの信号を受信すること、あるいは前記集積回路の１つ以上の電気コネクタでの特定の電気状態を検出することを含んでいる
ことを特徴とする請求項３に記載の方法。
【請求項５】
ユーティリティ動作に対して構成されている第１のセキュリティ動作状態と、テスト動作に対して構成されている第２のセキュリティ動作状態とを有する集積回路であって、
請求項１乃至４のいずれか１項に記載の方法を実行するように構成されている
ことを特徴とする集積回路。
【請求項６】
請求項５に記載の集積回路を備える電子機器。
【請求項７】
セルラー電話である通信装置である
ことを特徴とする請求項６に記載の電子機器。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ユーティリティ動作に構成されている第１のセキュリティ動作状態と、テスト動作に対して構成されている第２のセキュリティ動作状態とを有する集積回路に関するものである。本発明は、更に、方法および電子機器に関するものである。
【背景技術】
【０００２】
通信機器、例えば、移動電話の集積回路のような組込デバイスは、任意のソフトウェアおよびハードウェアの再構成設定を防止する機能を必要とすることがしばしばある。
【０００３】
あるリソースを保護するための要件は、規格、例えば、移動体与信モジュール、３ＧＰＰ（第３世代パートナシッププロジェクト）や、商業的要件、例えば、ＤＲＭ（デジタル著作権管理）、ＳＩＭ（加入者アイデンティティモジュール）ロックからきている。更なる別の要件定義は、信頼性盗用抑止機能を実現すること、例えば、盗難電話を無効にするために使用されるＩＭＥＩ（国際移動体機器アイデンティティ）番号ロッキングを実現す

ることである。この保護は、破壊、例えば、未認可改造に対抗することができる、あるいは、機密漏洩、例えば、未認可アクセスに対抗することができる。

【０００４】

通常に使用される方法には、ハードウェアスタートアップからソフトウェアに通じる信頼済経路を持たせることである。この信頼済経路は、チップがリセットされる場合に開始し、必要であれば、ソフトウェアの実行を通じて継続する。

【０００５】

例えば、移動電話では、基地局に提示されるＩＭＥＩ番号は、与えられるデバイスを固有に識別するべきである。ＩＭＥＩ番号は、とりわけ、盗難届けのあったサービス受信用のデバイスを保護するために使用される。ＩＭＥＩを保護するために、ＩＭＥＩと、基地局と通信するソフトウェアの記憶は、改竄行為から保護されなければならない。基本要件は、少なくとも改竄されたデバイスは、電話として使用できるようにしてはならないことである。

【０００６】

別の例には、ＤＲＭ保護化媒体をアンロックするために使用されるキー群とアイデンティティ群がある。これらは、抽出されることから保護されなければならない。

【０００７】

集積回路の製造中では、様々な製造段階での一連のテストを実行することが共通している。これらのテストは、期待通りに動作しないデバイスの個々のデバイスを識別するために動作する。このテストは、通常は、集積回路のすべての態様を通常検証することができないが、合理的なサブセットを検証することができる。テストによって検証されない部分でのエラーに起因して、仕分けの際に、いくつかの不良チップが抜け落ちることになる。

【０００８】

デバイスの製造を低下させず、かつコストを増加させないためには、製造テストは高速になされる必要がある。

【０００９】

多くのデバイスでエラーが発生すると、生産量が低下して、コストが増加する。更に悪いことは、多くのチップに影響を与えるが、テストには引っかからないエラーがあることである。これらのチップは、最終敵には、製品に組み込まれることになるが、動作不良あるいは全く動作しない可能性がある。この製品製造者は、解析のために、このような不良デバイスを返品されることになる。

【００１０】

故障返品（field return）の解析の間において、第１の方針は、できる限り精密に不良の原因を判定することである。当初の製造テストは、手順が、そのデバイスの当初の製造テストからそのデバイスが展開されている既知のものであるかどうかを確認するために戻ることができる。

【００１１】

不良の原因が既存の製造テストによるものでなかった場合、第２の方針は、製造テスト中の手順を検出できる新規のテストを展開することである。そして、この新規に展開されるテストは、標準の製造テストに含めることができる。新規のテストが実際に手順を把握することを検証するために、製造テストが、不良のデバイス上で動作させられる。デバイスが不良としてフラグが立てられると、新規のテストは有効となる。

【００１２】

製造時でのテストを実行することを可能とし、かつ故障返品におけるテストに戻すことを可能にするための要件は、システムのある部分へのアクセスを防止するための要件と衝突する。様々な方法が、これらの要件を調整するために利用可能である。

【００１３】

デバイスは、しばしば、セキュリティがまだ適用されておらず、かつあらゆるテスタビリティ（testability）メカニズムが実現可能な状況で製造される。これは、テスト時の柔軟性を最大にすることを可能にする一方で、テスト時間を最小にし、コストをより抑え

、更に、可能な限りの最大テスト許容範囲を実現する。
【００１４】
製造時の後半の段階で、デバイスは、セキュリティ対策を実現可能にするために改造される。これは、例えば、パッケージの段階での物理的な変更であり得る。このパッケージの段階とは、デバイス内部の電気的属性を変更することによって、重要な電気接続が利用不能にされる、あるいはより微妙にされる段階である。これは、チップ上にヒューズ／アンチヒューズをプログラミングすることによって、永続的なメモリセル群に書き込むことによって、あるいは他の対策によって達成され得る。この状態では、デバイスに対する完全なテストをこれ以上動作させることはできない。
【００１５】
故障返品の解析を可能にするために、テストの方法を再度実現可能にすることが必要とされる。これには、いくつかの共通の方法がある。
【００１６】
シークレットメカニズムを使用することは、すなわち、「バックドア（back door）」である。これは、隠蔽（undocumented）ピン、あるいは保護を無効にする電気入力の状態群の組み合わせを隠蔽したものであっても良い。これは、例えば、リバースエンジニアリングのリスクによって、あるいは、バックドアがどのように作動するかについての秘密が漏洩することによって、セキュリティを低下させる。
【００１７】
スタートされる前にその信頼性が検証されなければならないソフトウェアが、セキュリティのすべてあるいは一部を無効にするためのリクエストを承認し、かつ認可することができる程度に、デバイスをスタートアップさせることを許容することができる。例えば、ブートＲＯＭ（リードオンリーメモリ）は、リクエストを受信して、暗号署名を解析し、その有効性に基づいて、特定のデバイスにアクセスすることを可能にする。この場合の、ブートＲＯＭは黙示的に認証される。これは、チップ自身に記憶されているからである。
【００１８】
ハードウェアは、ハードウェアリクエストの強力な認証に基づいている。これは、上述のソフトウェアの方法に類似しているが、但し、ハードウェアで実現される。ハードウェアは、ミッションモードでハードウェアを共有してもしてなくも良い。例えば、ＪＴＡＧ（ジョイントタグアクショングループ）、即ち、ＩＥＥＥ１１４９．１を介するリクエストは、特定のデバイスへのアクセスを選択的に可能にするために、ハードウェアモジュールによって解析される暗号署名を含んでいる。
【発明の概要】
【発明が解決しようとする課題】
【００１９】
後者の２つは、いくつかの認証メカニズムを要求する。１つの方法は、国際公開２００６／００４７５４号公報に示されている。これには、セキュアデータを記憶している集積回路のようなデバイスのハードウェアセキュリティが保証されている。しかしながら、このような方法は、テスターを認証するための、無視できない量の回路とロジックを要求する。また、認証の管理は、テストを複雑にする。
【００２０】
本発明の目的は、上述の問題を少なくとも解決することである。本発明は、機能群の動作が制限されている別々のセキュリティ動作状態を提供することによって、複雑な認証をすることなく、テスト動作を実現可能にするという理解に基づいている。それどころか、この制限されている動作は、テスト動作中に、機密の機能群あるいは機密の情報がアクセスされない、使用されない、あるいは変更されないことを保証する。
【課題を解決するための手段】
【００２１】
第１の構成に従えば、ユーティリティ動作に対して構成されている第１のセキュリティ動作状態と、テスト動作に対して構成されている第２のセキュリティ動作状態とを有する

集積回路に対する方法が提供される。この方法は、前記第２のセキュリティ動作状態で動作している場合に、第１のオブジェクトのセットと第２のオブジェクトのセットを利用可にするステップと、第３のオブジェクトのセットを利用不可にするステップとを備え、前記第１のセキュリティ動作状態で動作している場合に、前記第１のセキュリティ動作状態のセキュリティメカニズムによる認可に応じて、前記第３のオブジェクトのセットを利用可にするステップとを備える。前記第２のセキュリティ動作状態で動作している場合に、前記第３のオブジェクトのセットを利用不可にするステップは、前記集積回路のロジック回路によって実行される。前記第２のセキュリティ動作状態で動作している場合に、前記第３のオブジェクトのセットを利用不可にするステップは、前記ロジック回路によって前記第２のセキュリティ動作状態で動作している場合に、前記第３のオブジェクトのセットを備える前記集積回路の一部を制限する動作を制御することを含んでいる。

【００２２】

ここで、「ユーティリティ動作」は、例えば、電子デバイスで使用される場合の集積回路の用途に従う動作であり、また、「テスト動作」とは異なる動作として解釈されるべきものである。

【００２３】

第１のセキュリティ動作状態と第２のセキュリティ動作状態は、相互に排他的であっても良い。即ち、集積回路は、第１のセキュリティ動作状態あるいは第２のセキュリティ動作状態のいずれかで動作するように構成されているが、両方の状態で動作するように構成されていない。

【００２４】

この方法は、前記第１のセキュリティ動作状態で動作している場合に、前記セキュリティメカニズムによる認可に応じて、前記第１のオブジェクトのセットを利用可にするステップを更に備えても良い。この方法は、前記第１のセキュリティ動作状態で動作している場合に、前記セキュリティメカニズムによって、前記第２のオブジェクトのセットを利用不可にするステップを更に備えても良い。この方法は、前記第１のセキュリティ動作状態の場合と前記第２のセキュリティ動作状態の場合との両方で、第４のオブジェクトのセットを利用可にするステップを更に備えても良い。

【００２５】

この方法は、テストリクエストを受信するステップと、前記テストリクエストの受信に応じて、前記第２のセキュリティ動作状態に入るステップとを更に備えても良い。前記テストリクエストを受信するステップは、テストポートへの信号を受信することを含んでいても良い。前記テストリクエストを受信するステップは、前記集積回路の１つ以上の電気コネクタでの特定の電気状態を検出することを含んでいても良い。前記特定の電気状態は、時系列の副次電気状態を備えていても良い。

【００２６】

この方法は、前記第２のセキュリティ動作状態に入る場合に、極秘情報及び機密情報の少なくとも一方を削除するステップを更に備えても良い。

【００２７】

この方法は、前記第２のセキュリティ動作状態から出る場合に、更なる実行に影響を与える状態を削除し、前記第１のセキュリティ動作状態の前記セキュリティメカニズムをバイパスすることを防止するために前記第１のセキュリティ動作状態へ戻るステップとを更に備えても良い。

【００２８】

第２の構成に従えば、ユーティリティ動作に対して構成されている第１のセキュリティ動作状態と、テスト動作に対して構成されている第２のセキュリティ動作状態とを有する集積回路が提供される。この集積回路は、第１の構成に従う方法を実行するように構成されている。

【００２９】

つまり、第２のセキュリティ動作状態では、第１のオブジェクトのセットと第２のオブ

ジェクトのセットが利用可であり、第３のオブジェクトのセットが利用不可である。第１のセキュリティ動作状態では、第３のオブジェクトのセットが、第１のセキュリティ動作状態のセキュリティメカニズムによる認可を伴って利用可である。第３のオブジェクトのセットは、第２のセキュリティ動作状態で動作している場合に、集積回路のロジック回路によって利用不可となる。ロジック回路は、第２のセキュリティ動作状態で動作している場合に、第３のオブジェクトのセットを備える集積回路の一部を制限する動作を制御するように構成されている。

【００３０】

ここで、「ユーティリティ動作」は、例えば、電子デバイスで使用される場合の集積回路の用途に従う動作であり、また、「テスト動作」とは異なる動作として解釈されるべきものである。

【００３１】

第１のセキュリティ動作状態と第２のセキュリティ動作状態は、相互に排他的であっても良い。即ち、集積回路は、第１のセキュリティ動作状態あるいは第２のセキュリティ動作状態のいずれかで動作するように構成されているが、両方の状態で動作するように構成されていない。

【００３２】

前記第１のオブジェクトのセットは、前記第１のセキュリティ動作状態で動作している場合に、前記セキュリティメカニズムによる認可に応じて、利用可にされても良い。前記第１のセキュリティ動作状態の前記セキュリティメカニズムは、前記第１のセキュリティ動作状態で動作している場合に、前記第２のオブジェクトのセットを利用不可にするように構成されていても良い。第４のオブジェクトのセットが、前記第１のセキュリティ動作状態と前記第２のセキュリティ動作状態との両方で利用可にされても良い。

【００３３】

ロジック回路は、テストリクエストの検出に応じて、前記集積回路の一部の前記第２のセキュリティ動作状態の動作を制限する制御を実行するように構成されていても良い。前記テストリクエストは、テストポートへの信号の入力を含んでいてもよい。前記テストリクエストは、前記集積回路の１つ以上の電気コネクタでの特定の電気状態を検出することを含んでいてもよい。前記特定の電気状態は、時系列の副次電気状態を備えていても良い。

【００３４】

前記集積回路は、前記第２のセキュリティ動作状態に入る場合に、極秘情報及び機密情報の少なくとも一方を削除するように構成されているメカニズムを更に備えても良い。これによって、前記第２のセキュリティ動作状態からデータ及びキーの抽出を防止することができる。

【００３５】

前記集積回路は、前記第２のセキュリティ動作状態から出る場合に、更なる実行に影響を与えるオブジェクト削除し、かつ前記第１のセキュリティ動作状態の前記セキュリティメカニズムをバイパスすることを防止するために前記第１のセキュリティ動作状態へ戻すように構成されているメカニズムを更に備えても良い。ここで、オブジェクトは、第２のセキュリティ動作状態中に発生する、登録コンテンツ、内部スイッチ設定、他の情報の部分等であり得る。

【００３６】

第３のオブジェクトのセットを備える集積回路の一部は、第３のオブジェクトのセットが実現される、１つ以上の物理的に保護された回路エリアを備えていても良い。これは、ロジック回路によって第３のオブジェクトのセットを無効にすることを容易にする。物理的に保護された回路エリアは、更に、ロジック回路を備えていても良い。これは、第２のセキュリティ動作状態である場合になされる任意のセキュリティ攻撃から保護する。

【００３７】

第３のオブジェクトのセットは、デジタル著作権管理キー群、加入者アイデンティティ

モジュール機能群、国際移動機器アイデンティティ記憶装置、無線周波数生成回路、セキュリティキー群、安全化メモリエリア、クロック信号ジェネレータ、スキャンチェーンジェネレータ、あるいはリセットメカニズム、あるいはそれらの任意の組み合わせの任意のものを備えていても良い。

【００３８】

第３の構成に従えば、第２の構成に従う集積回路を備える電子機器が提供される。この電子機器は、通信装置、例えば、セルラー電話であっても良い。

【００３９】

本発明の実施形態の利点は、第２のセキュリティ動作状態での動作を通じて、第１のセキュリティ動作状態のセキュリティメカニズムをバイパスすることが無効にされることである。

【図面の簡単な説明】

【００４０】

【図１】実施形態に従う集積回路のセキュリティ動作状態を示す図である。

【図２】実施形態に従う集積回路を示す図である。

【図３】実施形態に従う、状態間の遷移での動作に伴う、集積回路のセキュリティ動作状態を示す図である。

【図４】実施形態に従うセキュリティ動作状態におけるオブジェクトのセットの可用性を示す図である。

【発明を実施するための形態】

【００４１】

図１は、実施形態に従う集積回路のセキュリティ動作状態を示している。この例では、第１のセキュリティ動作状態１００と、第２のセキュリティ動作状態１０２、それに加えて、オプションのスタート状態１０４が示されている。スタート状態１０４は、どのように実施形態が動作するかの理解を高めるための状態であり得り、また、これは、機能については本質的ではない。集積回路のスタートアップで、あるいは、実用上では、集積回路を備える装置のスタートアップで、スタート状態１０４に入る。ここでは、テストインタフェースがアクセスされているかどうか、すなわち、テストリクエストにおける表示が存在するかどうか、例えば、信号がテストポートに入力されているかどうかが判定される。テストインタフェースは、ハードウェアインタフェースでもソフトウェアインタフェースであっても良い。ハードウェアインタフェースは、集積回路の１つ以上のピンに接続される電気信号であり得る。特定の電気状態を、この集積回路へのこれらのピン群あるいはコネクタ群で検出することができる。ここで、この電気状態は、時間非依存の電気状態、あるいは時系列の副次電気状態であり得る。１つ以上のピンは、専用のテストピン群、あるいは集積回路で利用可能な適切な他のピン群のセットであり得る。ソフトウェアインタフェースは、テスト動作が実行されるべきかどうかを判定するために、集積回路によって復号される信号群であり得る。この例では、ＩＥＥＥ１１４９．１としても知られているジョイントテストアクショングループに従うリクエストである。実行されるべきテスト動作がないと判定される場合、集積回路は、第１のセキュリティ動作状態１００に入る。ここでは、スタートアップ動作が、集積回路の第１のセキュリティ動作状態１００の通常の動作手順とセキュリティメカニズムに従って実行される。第１のセキュリティ動作状態１００は、集積回路を備える電気デバイスのアプリケーション用、すなわち、電子デバイス製品で使用することが意図されているアプリケーション用のユーティリティ動作に対して向けられている。テスト動作が実行されるべきであると判定される場合、集積回路は、第２のセキュリティ動作状態１０２に入る。第２のセキュリティ動作状態１０２は、例えば、集積回路を備える電子デバイスにおけるテスト動作、すなわち、そのアプリケーションで、集積回路の機能及び動作の解析に対して向けられている。第２のセキュリティ動作状態１０２に入ると、集積回路のある部分の動作を制限するための、さらに、好ましくは、集積回路によって制御されるいくつかの機能を制限するための制御ロジックがアクティベートされる。同様に、第１のセキュリティ動作状態で動作していて、かつ上述の任意のテス

ト動作リクエストが検出される場合にも、同様の方法で、第２のセキュリティ動作状態に入る。

【００４２】

できる限り簡単に改竄を防止することを可能にするために、動作の制限がなされることが好ましい。これは、集積回路内の１つ以上のスイッチであり得る。この集積回路は、その内部でのみ制御され、かつ第２のセキュリティ動作状態１０２で保護されるべき部分あるいは機能を無効にするあるいは切断する。無効にすることができるあるいは切断することができる機能あるいは部分は、一定のメモリエリア、クロック信号、例えば、モジュレータ／デモジュレータのような無線周波数信号ジェネレータの制御及び実現、通信インタフェース、スキャンチェーン（scan chain）であり得る。ここで、スキャンチェーンの制御は、通常のスキャンチェーンの無効にすること、及び通常のスキャンチェーンを代替のスキャンチェーンへ置換することを含むことができる。別の方法は、一定の機能群を無効にするために、あるいは一定の情報へアクセスするために、集積回路の少なくとも一部を継続的なリセット状態にすることである。ここで、アクセスとは、情報の読出を行うための能力、あるいは情報の追加／変更／削除を行うための能力の一方を意味し得る。例えば、移動端末では、国際移動機器アイデンティティは、変更可能にされるべきではない。他の例には、一定のキー群が、メッセージ認証コードキー、デジタル著作権管理キー、あるいは他の暗号または認証キー群、あるいは、加入者アイデンティティモジュール機能群が、読取可能にされるべきでないことである。

【００４３】

つまり、機能群、情報及び信号群は、各セキュリティ動作状態１００、１０２に対して利用可能な構造が与えられるオブジェクトとして見なすことができる。この構造は、第２のセキュリティ動作状態では、第１のオブジェクトのセットと第２のオブジェクトのセットが利用可能であり、一方で、第３のオブジェクトのセットが利用不可であり、第１のセキュリティ動作状態では、第３のオブジェクトのセットが第１のセキュリティ動作状態のセキュリティメカニズムによる認証を用いて利用可能であり、また、第２のセキュリティ動作状態で動作する場合には、集積回路のロジック回路によって、第３のオブジェクトのセットが利用不可にされる。ここで、このロジック回路は、第２のセキュリティ動作状態で動作する場合には、第３のオブジェクトのセットを備える集積回路の一部の動作を制限する制御を行うように構成されている。つまり、第３のオブジェクトのセットは、動作の制限を提供する、テスト動作中に利用不可にされる。第１のオブジェクトのセットは、第１のセキュリティ動作状態で動作する場合にセキュリティメカニズムによる認可を利用可能にすることができ、一方で、第１のセキュリティ動作状態のセキュリティメカニズムは、第１のセキュリティ動作状態で動作する場合に第２のオブジェクトのセットを利用不可にするように構成することができる。これは、電子デバイスのユーティリティ動作中に、オブジェクトの改竄あるいは未認可アクセスを回避するためのセキュリティメカニズム機能群の一部となる。第１のセキュリティ動作状態１００、第２のセキュリティ動作状態１０２の両方で利用可能となる第４のオブジェクトのセットも存在することができる。

【００４４】

テスト動作が実行されていて、かつ第２のセキュリティ動作状態１０２から出る場合、ユーティリティ動作へ戻るために第１のセキュリティ動作状態への遷移が行われる、あるいは、例えば、リスタートあるいは終了するためにオプションのスタート状態１０４への遷移が行われる。第２のセキュリティ動作状態１０２から出る場合、更なる実行に影響を与える任意のオブジェクトを、第１のセキュリティ動作状態へ入る場合にこれらのオブジェクトがセキュリティメカニズムを漏らすことを防止するために削除することができる。ここで、オブジェクトは、第２のセキュリティ動作状態中に発生する、登録コンテンツ、内部スイッチ設定、他の情報の部分等であり得る。例えば、テスト動作中に実行される動作に依存して、このようなオブジェクトが存在しない場合、あるいは残っていない場合、もちろん、この削除は必要ない。このような任意のオブジェクトの削除は、集積回路のセットとして実行され得る。

【００４５】
図２は、実施形態に従う集積回路２００を示している。集積回路２００は、保護エリア２０２、即ち、外部からアクセスできないあるいは操作できず、かつ集積回路の内部でのみ制御されるエリアを備える。この保護エリアは、１つのエリアである必要はなく機能的なものであると解釈されるべきである。そして、この保護エリアは、機密情報と機能群を備えることができる。これには、例えば、一定のメモリエリア、クロック信号制御、例えば、無線周波数電力増幅器あるいはモジュレータ／デモジュレータの制御及び実行許可、通信インタフェース制御、スキャンチェーン制御等がある。保護エリア２０２では、上述のように、第１のセキュリティ動作状態のセキュリティメカニズムを介してのみアクセス可能とするべき情報を記憶することができる。ここで、アクセスとは、情報の読出を行うための能力、あるいは情報の追加／変更／削除を行うための能力を意味することができる。例えば、移動端末では、国際移動機器アイデンティティは変更可能とされるべきでない。他の例では、あるキー群２０４は、読出可能とするべきでない。これには、例えば、メッセージ認証コードキー群、デジタル著作権管理キー群、あるいは他の暗号化あるいは認証キー群、加入者アイデンティティモジュール機能群がある。保護エリアは、セキュリティ実現ロジック２０６によって隠蔽が維持され、このセキュリティ実現ロジック２０６は、動作の制限を保証するロジック回路によって実現することができる。これは、改竄を防止するためにできる限り単純に実行されることが好ましい。これは、例えば、集積回路内の１つ以上のスイッチとすることができ、これは、集積回路内でのみ内部的に制御され、また、第２のセキュリティ動作状態で保護されるべき部分あるいは機能群を無効にするあるいは切断する。セキュリティ実現ロジック２０６は、上述のように、テスト動作に対するリクエストが検出されるとすぐにアクティベートされる。

【００４６】
図３は、実施形態に従う、状態間の遷移での動作とともに、集積回路のセキュリティ動作状態群を示す図である。図では、第１のセキュリティ動作状態３００と第２のセキュリティ動作状態３０２、オプションのスタート／オフ状態３０４が示されている。スタート／オフ状態３０４は、どのようにして実施形態が動作するかの理解を高めるための状態であり得り、また、これは、機能について本質的ではない。集積回路のスタートアップで、あるいは、実用上では、集積回路を備える装置のスタートアップで、手順は、スタート／オフ状態３０４を開始する。チェッキングステップ３０６では、テストインタフェースがアクセスされているかどうかがチェックされる。図１を参照して説明されるように、テストインタフェースは、ハードウェアインタフェースでもソフトウェアインタフェースでもあっても良く、また、図１を参照して説明される機能群と同様の機能群を有する。実行されるべきテスト動作がないと判定される場合、集積回路は第１のセキュリティ動作状態３００に入る。ここでは、スタートアップ動作が、集積回路の第１のセキュリティ動作状態３００の通常の動作手順とセキュリティメカニズムに従って実行される。テスト動作が実行されるべきと判定される場合、集積回路は第２のセキュリティ動作状態３０２に入る。第２のセキュリティ動作状態３０２に入ると、極秘情報及び機密情報の少なくとも一方、例えば、ユーザ情報、一定のセキュリティキー群、プロファイル等が、極秘／機密情報削除ステップ３０８で削除され得る。集積回路の一定の部分の動作を制限するために、また、好ましくは、集積回路によって制御されるいくつかの機能群を制限するために、制御ロジックアクティベーションステップ３１０で、制御ロジックがアクティベートされる。制御ロジックアクティベーションステップ３１０は、１つ以上のサブステップを備えることができ、これには、例えば、セキュアメモリエリアを無効にするステップ、クロック信号を無効にするステップ、無線周波数信号ジェネレータを無効にするステップ、回路を短絡するあるいはスキャンチェーンを変更するステップ、集積回路の一部を継続的なリセット状態にするステップ等がある。同様に、上述のように、第１のセキュリティ動作状態で動作していて、かつ任意のテスト動作リクエストが検出される場合、極秘／機密削除ステップ３０８と制御ロジックアクティベーションステップ３１０を介して、同様の方法で、第２のセキュリティ動作状態に入る。動作の制限は、図１を参照して説明されるように実行

されることが好ましい。

【００４７】

テスト動作が実行されていて、かつ第２のセキュリティ動作状態３０２から出る場合、更なる実行に影響を与える任意のオブジェクトが、第１のセキュリティ動作状態に入る場合にこれらのオブジェクトがセキュリティメカニズムを漏らすことを防止するためにオブジェクト削除ステップ３１２で削除され得る。ここで、オブジェクトは、第２のセキュリティ動作状態中に発生する、登録コンテンツ、内部スイッチ設定、他の情報の部分等であり得る。例えば、テスト動作中に実行される動作に依存して、このようなオブジェクトが存在しない場合、もちろん、この削除は必要ない。このような任意のオブジェクトの削除は、集積回路のリセットとして実行され得る。その後、ユーティリティ動作に戻るために第１のセキュリティ動作状態３００への遷移が行われる、あるいは、例えば、リスタートあるいは終了のためにスタート／オフ状態３０４への遷移が行われる。

【００４８】

集積回路は、電子機器で利用することができる。この電子機器は、テスト動作及びセキュリティ動作の提供による恩恵を受ける任意の装置とすることができる。テスト動作の恩恵は、あらゆる電気機器に適用する。セキュリティ動作の恩恵は、例えば、セルラー電話、メディアプレーヤ、デジタルカメラ、パーソナルデジタルアシスタント、あるいは汎用デジタルコンピュータに適用することができる。これらの内の任意のもので、キー群、著作権管理メカニズム群、盗難保護メカニズム、コンテンツ等が存在することができ。そして、これらは、関心のあるユーザ、ネットワークオペレータ、あるいは未認可アクセスあるいは改竄から保護するためのコミュニティ自身内に存在する。

【００４９】

図４は、実施形態に従うセキュリティ動作状態でのオブジェクトのセット群の可用性を示す図である。セキュリティ動作状態の観点からは、各セキュリティ動作状態は、異なるオブジェクトのセットの可用性について異なる基準を有する。異なるオブジェクトのセットは、上述のように定義され、そして、各セットの共通の機能は、この状況では、可用性の観点からどのように取り扱われるかである。

【００５０】

第１のセキュリティ動作状態では、上述のように、第１のオブジェクトのセットが利用可とされ、好ましくは、第１のセキュリティ動作状態のセキュリティメカニズムによって管理される認可を伴う。一方、第２のオブジェクトのセットは利用不可となる。第３のオブジェクトのセットは、第２のセキュリティメカニズムによって管理される認可を伴って利用可となり、認可を伴うことなく、利用可となる第４のオブジェクトのセットも存在し得る。第１のセットのオブジェクトの例は、ＪＴＡＧベースのデバッグであり、これは、例えば、第１のセキュリティ動作状態での正規の信用証明が提示された後、ブートＲＯＭソフトウェアによって認可される。第２のセットのオブジェクトの例は、ＪＴＡＧを介するレジスタスキャンチップテストアクセスである。第３のセットのオブジェクトの例は、無線機能の実現であり、これは、例えば、署名済コードを正しく提示した後、ブートＲＯＭソフトウェアによって認可される。第４のセットのオブジェクトの例は、セキュリティが何等関与しないものであり、これには、例えば、タイマー、ユニバーサル非同期受信機／送信機等がある。

【００５１】

第２のセキュリティ動作状態では、上述のように、第１のオブジェクトのセットと第２のオブジェクトのセットが利用可となり、一方、第３のオブジェクトのセットは利用不可となる。利用可となる第４のオブジェクトのセットも存在し得る。好ましくは、第２のセキュリティ動作状態では、認可用のセキュリティメカニズムは存在しない。このことは、テスト動作をより容易にする。これは、テスト動作用の任意のアクセスコード群、キー群等の配信が必要とされないからである。代わりに、第２のセキュリティ動作状態で利用不可となる所定のセットの構造を、セキュリティ用に提供する。また、上述のように、セキュリティ動作状態間の遷移がなされる場合に、セキュリティの改竄を防止するためのメカ

ニズムを存在させることができる。

【００５２】

オブジェクトの観点からは、各オブジェクトは、オブジェクトのセットによって定義される任意のカテゴリに割り当てることができる。ここで、第２のセキュリティ動作状態で利用不可となるオブジェクトの定義は最も重要な改善点である。上述のように、ロジック回路によって実現されるための特定のメカニズムが提供される。

【図１】

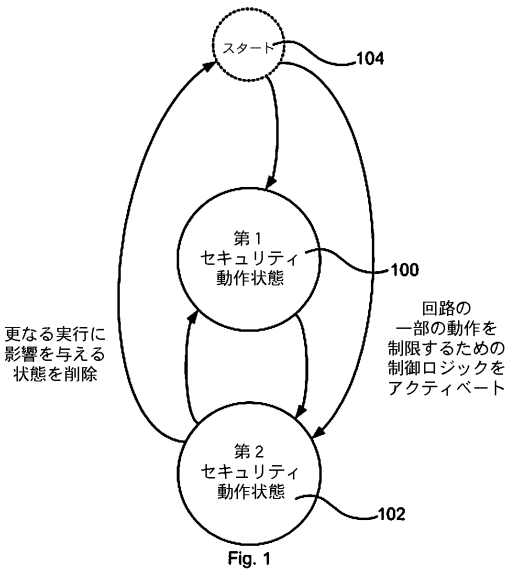

Fig. 1

【図２】

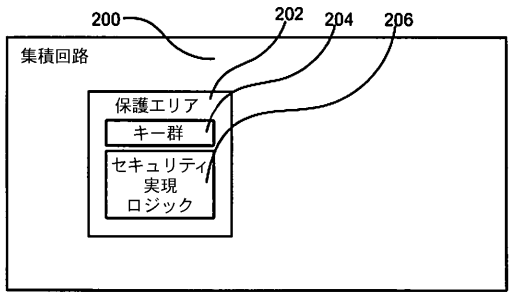

Fig. 2

【図３】

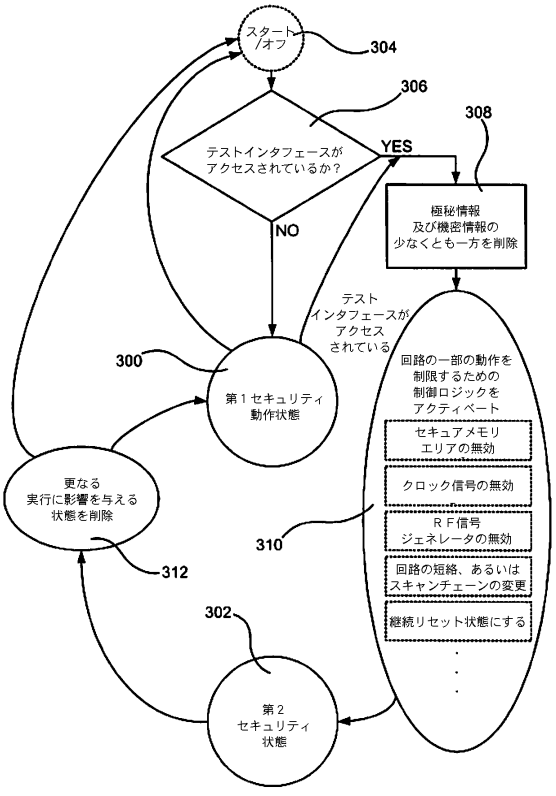

Fig. 3

【図４】

	オブジェクトセット1	オブジェクトセット2	オブジェクトセット3	オブジェクトセット4
第１ セキュリティ状態	認可による利用可	利用不可	認可による利用可	利用可
第２ セキュリティ状態	利用可	利用可	利用不可	利用可

Fig. 4

フロントページの続き

(31)優先権主張番号 61/153,493
(32)優先日 平成21年2月18日(2009.2.18)
(33)優先権主張国 米国(US)

(72)発明者 スヴェンソン, ペテル
スウェーデン国 ルンド エス－２２６ ５７, ユリーヴェーゲン １５
(72)発明者 ロステッド, ミカエル
スウェーデン国 グルムスレブ エス－２６１ ６２, クングスヘグスヴェーゲン １２

審査官 久慈 渉

(56)参考文献 特開平０９－１９８３１６（ＪＰ，Ａ）
特表２００６－５０５７９８（ＪＰ，Ａ）
特開２００５－３１６７３４（ＪＰ，Ａ）
特開２００６－０５３８０８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl., ＤＢ名)
Ｇ０６Ｆ ２１／６０
Ｇ０１Ｒ ３１／２８
Ｇ０６Ｆ ２１／６２