(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2007-503797
(P2007-503797A)
(43)公表日　平成19年2月22日(2007.2.22)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/10	(2006.01)	H04L	9/00	621Z	5B017
G06F 21/24	(2006.01)	G06F	12/14	530D	5J104
G06F 21/06	(2006.01)	G06F	12/14	540A	
		G06F	12/14	560E	

審査請求 有　予備審査請求 未請求　（全 14 頁）

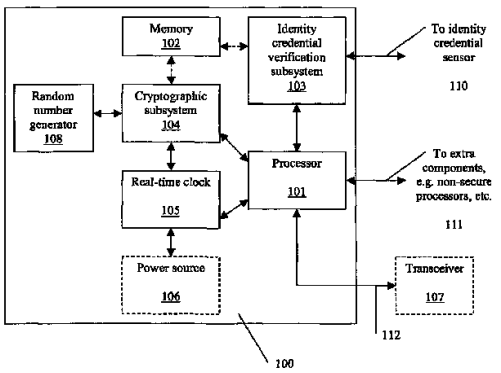
(21)出願番号　特願2006-533548 (P2006-533548)
(86)(22)出願日　平成16年6月1日 (2004.6.1)
(85)翻訳文提出日　平成17年11月15日 (2005.11.15)
(86)国際出願番号　PCT/US2004/017272
(87)国際公開番号　WO2004/109455
(87)国際公開日　平成16年12月16日 (2004.12.16)
(31)優先権主張番号　60/474,750
(32)優先日　平成15年5月30日 (2003.5.30)
(33)優先権主張国　米国 (US)

(71)出願人　505015864
プリヴァリス・インコーポレーテッド
アメリカ合衆国バージニア州２２９１１，シャーロッツヴィル，ピーター・ジェファーソン・パークウェイ　６７５，スイート　１５０
(74)代理人　100089705
弁理士　社本　一夫
(74)代理人　100140109
弁理士　小野　新次郎
(74)代理人　100075270
弁理士　小林　泰
(74)代理人　100080137
弁理士　千葉　昭男

最終頁に続く

(54)【発明の名称】機密データへのアクセス及び使用を制御するための回路内セキュリティ・システム及び方法

(57)【要約】
本明細書に開示された発明は、電子デバイス用の回路内セキュリティ・システム（１００）である。回路内セキュリティ・システム（１００）は、識別信用証明検証（１０３）と、セキュアなデータ及び命令のストレージと、セキュアなデータ伝送機能と、を組み込む。単一の半導体チップを備え、酸素反応層の追加などの情報の不正改ざん又は盗聴を防ぐための業界実施機構を使用して、機密保護される。本発明は、回路内セキュリティ・システム（１００）及び登録された個人用に、セキュリティ設定と、プロファイルと、応答とを確立するための手段も、組み込む。回路内セキュリティ・システム（１００）は、様々な電子デバイス内で使用することができ、それらは、ハンドヘルド・コンピュータと、セキュアな設備キーと、車両オペレーション／イグニッション・システムと、デジタル権管理と、を含む。



【特許請求の範囲】
【請求項１】
電子デバイス用の回路内セキュリティ・システムであって、
プロセッサと、
前記プロセッサに結合されたメモリと、
前記プロセッサに結合されたリアルタイム・クロックと、
前記プロセッサ及び前記リアルタイム・クロックに結合された、暗号化サブシステムと、
前記暗号化サブシステムに結合された乱数発生器と、
前記プロセッサに結合された識別信用証明検証サブシステムと、
少なくとも３つの入力／出力インターフェースと、
を備え、
前記プロセッサは、命令及び関連するデータのロード及び実行のための手段を提供し、
前記メモリは、セキュリティ設定及びプロファイルを含む命令及びデータを格納するための手段を提供し、
前記リアルタイム・クロックは、正確な時間を生成するための手段を提供し、
前記暗号化サブシステムは、暗号化と、復号と、デジタル署名と、デジタル署名検証とを実行するための手段を提供し、
前記乱数発生器は、所定のレベルを満たすのに十分な統計的ランダム性を備えた数をランダムに生成するための手段を提供し、
前記識別信用証明検証サブシステムは、識別信用証明の取得と、分析と、格納と、突合せとのための手段を提供し、
第１の入力／出力インターフェースは、前記識別信用証明検証サブシステムと外部識別信用証明センサとの間の接続に使用され、
第２の入力／出力インターフェースは、リモート接続デバイスとの間のデータの送信及び受信に使用され、
第３の入力／出力ラインは、少なくとも１つの周辺デバイスへの接続に使用される、
回路内セキュリティ・システム。
【請求項２】
請求項１に記載の回路内セキュリティ・システムであって、リモート接続デバイスとの間のデータの送信及び受信用の前記入力／出力インターフェースは、前記プロセッサをトランシーバに接続する、回路内セキュリティ・システム。
【請求項３】
請求項２に記載の回路内セキュリティ・システムであって、前記トランシーバは、無線通信トランシーバである、回路内セキュリティ・システム。
【請求項４】
請求項２に記載の回路内セキュリティ・システムであって、前記トランシーバからアンテナへの接続を、更に備える回路内セキュリティ・システム。
【請求項５】
請求項２に記載の回路内セキュリティ・システムであって、前記トランシーバは、ＲＦＩＤ通信に使用される、回路内セキュリティ・システム。
【請求項６】
請求項２に記載の回路内セキュリティ・システムであって、前記トランシーバは、Ｂｌｕｅｔｏｏｔｈ通信に使用される、回路内セキュリティ・システム。
【請求項７】
請求項２に記載の回路内セキュリティ・システムであって、前記トランシーバは、赤外線通信に使用される、回路内セキュリティ・システム。
【請求項８】
請求項１に記載の回路内セキュリティ・システムであって、リモート接続デバイスとの間のデータの送信及び受信用の前記入力／出力インターフェースは、前記プロセッサを、

有線通信に使用されるトランシーバに接続する、回路内セキュリティ・システム。
【請求項９】
請求項８に記載の回路内セキュリティ・システムであって、前記トランシーバは、シリアル通信に使用される、回路内セキュリティ・システム。
【請求項１０】
請求項８に記載の回路内セキュリティ・システムであって、前記トランシーバは、ＵＳＢ通信に使用される、回路内セキュリティ・システム。
【請求項１１】
請求項１に記載の回路内セキュリティ・システムであって、前記識別信用証明検証サブシステムは、生物測定認証を使用する、回路内セキュリティ・システム。
【請求項１２】
請求項１に記載の回路内セキュリティ・システムであって、内部電源を、更に備える回路内セキュリティ・システム。
【請求項１３】
回路内セキュリティ・システムを有する電子デバイスへのアクセスを制御するための方法であって、
ａ．識別信用証明検証サブシステム内の個人識別信用証明の登録を必要とする工程と、
ｂ．前記個人識別信用証明を少なくとも１つのセキュリティ特権に関連付ける工程と、
ｃ．アクセス要求時に、個人識別信用証明サンプルを前記識別信用証明検証サブシステムに提供するよう要求する工程と、
ｄ．前記個人識別信用証明サンプルを、前記識別信用証明検証サブシステム内の少なくとも１つの登録済み個人識別信用証明と比較する工程と、
ｅ．前記個人識別信用証明サンプルと登録済み個人識別信用証明との間の一致の有無を判定する工程と、
ｆ．前記個人識別信用証明サンプルに関連付けられたすべてのセキュリティ特権を決定する工程と、
ｇ．前記判定された一致の有無又は前記決定されたセキュリティ特権のうちの少なくとも１つに基づいて、アクセス許可を決定する工程と、
ｈ．前記アクセス許可に基づいてアクセスを認可又は拒否する工程と、
ｉ．セキュリティ設定によって規定されたように、前記アクセスの認可又は拒否に必要な任意のアクションを実行する工程と、
を備える方法。
【請求項１４】
請求項１３に記載の方法であって、前記要求されるアクセスは、格納されたデータへのアクセスである、方法。
【請求項１５】
請求項１３に記載の方法であって、前記要求されるアクセスは、構成要素を選択的に使用不可にすることである、方法。
【請求項１６】
請求項１３に記載の方法であって、前記要求されるアクセスは、使用不可にされた構成要素を選択的に使用可能にすることである、方法。
【請求項１７】
請求項１３に記載の方法であって、前記要求されるアクセスは、構成要素を選択的に破棄することである、方法。
【発明の詳細な説明】
【技術分野】
【０００１】
（関連米国出願データ）
本出願は、参照によりその全文が組み込まれた「Ｓｅｃｕｒｅ　Ｂｉｏｍｅｔｒｉｃ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　Ｄｅｖｉｃｅｓ　ａｎｄ　Ｓｙｓｔｅｍｓ　ｆｏｒ　Ｖ

ａｒｉｏｕｓ　Ａｐｐｌｉｃａｔｉｏｎｓ」という名称の仮特許出願第６０／４７４７５０号の優先権をＵＳＣ　１１９（ｅ）に基づいて主張する。

【０００２】

（発明の分野）

本明細書で開示される本発明は、電子回路を使用して格納、処理、及び配布される機密データのセキュリティに関する。より具体的に言えば、本発明は、データへのアクセス／使用に先立つ個人の識別、及び、前記データへのアクセス／使用の未許可の試行に対するセキュリティ制御の実行に関する。

【背景技術】

【０００３】

近年、個人が機密データの格納及び伝送のために使用できる電子デバイスが、急増してきた。セキュリティの低い例では、Ｐａｌｍ（商標）又はＢｌａｃｋＢｅｒｒｙハンドヘルド・コンピュータなどのポータブル・デバイスは、通常、電子メール用のソフトウェア、並びに、クレジット・カードと、スケジュールと、他のデータとを格納するためのオプションを含んでいる。ほとんどの人々は、この情報を保護することを望んでいるが、ほとんどのハンドヘルド・デバイスは、データの機密保護をそれらのオペレーティング・システムに依拠している。残念ながら、これらハンドヘルド・コンピュータ用のほとんどの一般的なオペレーティング・システムは、主な目標としてセキュリティを備えた設計とはなっておらず、後付けの基本セキュリティ・メカニズムは、不出来なものであった。

【０００４】

増加しつつあるスマート・カードなどの電子デバイスは、特に公開鍵インフラストラクチャを使用してユーザを識別及び認証することが意図されており、これには秘密鍵のセキュアな格納が必要である。これらのデバイスは、たとえば、設備にアクセスするための適切な許可を得た個人にスマート・カード及び非対称鍵ペアが割り当てられるという、セキュリティを構築する際には、一般的である。証明機関が、公開鍵用のデジタル証明を生成し、これがスマート・カード内に格納される。秘密鍵も、スマート・カード上に格納される。個人が、設備のアクセス・ポイントにある読み取り機内に自分のスマート・カードを置くと、カードは、そのデジタル証明を伝送し、読み取り機は、与えられた文字列を個人の秘密鍵で暗号化するようカードに喚起する。読み取り機は、デジタル証明から公開鍵を取得し、秘密鍵で暗号化された文字列を復号して、鍵が関連していることを検証する。これには、秘密鍵を使用する個人がスマート・カードの割り当てられた所有者であるという保証がないことから、固有の問題がある。更に、熟練した攻撃者であれば、カード上に格納された鍵へのアクセス権を取得するのは、いとも簡単である。

【０００５】

ＨｅｗｌｅｔｔＰａｃｋａｒｄのｉＰＡＱ　ＰｏｃｋｅｔＰＣ　ｈ５４５０などの幾つかのハンドヘルド・デバイスは、機密データにアクセスできるようにする前の改良型個人識別用のバイオメトリクス・センサを含む。このデバイスを所有する個人は、１つ又は複数の自分の指紋をデバイスのソフトウェアに登録するように、指示される。登録された指紋は、唯一のパスワードとして、又は、入力されるパスワードの代わりとして使用することができる。バイオメトリクスは、１人の個人に決定的に関係付けることが可能であるため、この種のデバイスは、従来のデータ・アクセス方法への大幅な改良とすることができる。しかしながら、機密データがセキュアでない形で格納又は伝送された場合、バイオメトリクス認証では、攻撃者がメモリを調べてこれを漏洩するのを実質的に防げない。

【０００６】

これらの懸案事項は、「セキュア・メモリ」又は「セキュア・プロセッサ」として宣伝される製品のマーケティングに寄与してきた。これらの製品は、通常、様々なセキュリティ・レベルで構築され、レベルの低いものの１つは、「不正改ざん発見可能（ｔａｍｐｅｒ－ｅｖｉｄｅｎｔ）」であるとみなされ、未熟な観察者でも、誰かが悪意をもってセキュア・データにアクセスしようと試みたことがわかる。レベルの高いものの１つは、「不正改ざん防止可能（ｔａｍｐｅｒ－ｒｅｓｉｓｔａｎｔ）」であり、自己破壊機構、ポリ

マー・ベース・コーティング又は他のいわゆる「絶縁保護コーティング」などの機密データを格納している構成要素をコーティングする不浸透性物質、或いは、何らかの他の工程を使用することによって、製品が実際に不正改ざんを防ぐ。更にこれらの製品は、入力／出力ラインを暗号化すること、部品に違うラベル表示をすること、及び、他の種類の不明瞭化（ｏｂｆｕｓｃａｔｉｏｎ）を実行することが可能である。

【０００７】

（関連技術の考察）

Ｆｏｒｃｅ等への米国特許第５，５３３，１２３号は、プログラム可能分散型個人セキュリティの発明を開示する。この特許は、「ＳＰＵチップ」を備えた「機密保護処理ユニット（ＳＰＵ／Ｓｅｃｕｒｅｄ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）」及びセキュアなデータ処理用に特別に設計されたマイクロプロセッサを開示する。この発明は、鍵、暗号化及び復号エンジン、並びにアルゴリズムを、発明のＳＰＵ内に統合する。その称するところによれば、セキュリティ工程は、移植可能であり、物理的境界線をまたいで容易に分散される。この発明は、３つの相互に依存したサブシステムに基づく。この発明の第１のサブシステムは、ＳＰＵに対してセキュリティ攻撃の存在及び特徴を喚起する検出器サブシステムである。第２のサブシステムは、複数の検出器からのデータを相関させ、その後、その秘密データ及びＳＰＵそれ自体の設計の両方のＳＰＵの整合性に対するリスクへの攻撃の重大度を査定する、フィルタ・サブシステムである。第３のサブシステムは、検出された攻撃に対処するためにその環境下で最も適切となるようにフィルタによって算出された、応答又は対抗手段を生成するための、応答サブシステムである。Ｆｏｒｃｅは、ＳＰＵ内での識別信用証明検証（ｉｄｅｎｔｉｔｙ　ｃｒｅｄｅｎｔｉａｌ　ｖｅｒｉｆｉｃａｔｉｏｎ）を開示していない。

【０００８】

Ｔａｋａｈａｓｈｉへの米国特許第５，８２５，８７８号は、マイクロプロセッサ用のセキュアな埋め込み型メモリ管理ユニットを開示する。マイクロプロセッサ・メモリ管理装置は、暗号化された命令及びデータの外部メモリからの転送に使用される。物理的なセキュリティは、同じチップ上に、マイクロプロセッサ・コアと、内部メモリと、暗号化／復号論理と共に直接メモリ・アクセス制御装置を埋め込むことによって得られる。外部メモリから及び外部メモリへのデータ転送は、外部メモリとメモリ管理ユニットのメモリ制御装置との間で行われる。外部メモリへの及び外部メモリからのすべてのファームウェアは、ページごとに処理される。処理のすべてがチップ内部のバス上で実行されるため、明白な暗号化されていない命令及びデータの検出が防止される。Ｔａｋａｈａｓｈｉは、管理ユニット上又はマイクロプロセッサ・コア内に識別信用証明検証を含めるための何れの機能、予想、意図、又は提案も開示していない。

【０００９】

Ｌｉｔｔｌｅ等への米国特許第５，８３２，２０７号は、マイクロプロセッサ及びコプロセッサを含むセキュア・モジュールを教示する。電子モジュールには、単一の集積回路内に配置された少なくとも１つのマイクロプロセッサ及びコプロセッサが提供される。電子モジュールは、小型のフォーム・ファクタ・ハウジングに収容することができる。電子モジュールは、データ・バスを介してセキュアな双方向データ通信を提供する。電子モジュールは、主としてＲＳＡ計算向けの１，０２４ビットのモジュロ数学を処理するように適合されたマイクロプロセッサ及びコプロセッサを含む、集積回路を含むことができる。電子モジュールは、好ましくは小型トークン・サイズの金属容器に収容される。モジュールは、好ましくは１ワイヤ・プロトコルを使用して単線のデータ・バスを介して通信する。Ｌｉｔｔｌｅ等は、個人識別システムを開示していない。

【００１０】

Ｔｈｉｒｅｉｔへの米国特許第５，８９４，５５０号は、マイクロプロセッサ・カード内のセキュア・プログラム及びセキュア・プログラムを含むマイクロプロセッサ・カードの実施方法を開示する。この発明は、ＣＰＵに関してプログラムをセキュアにできることを主張する。この発明は、ＣＰＵによって直接実行可能な所定のアドレス機能を第１のメ

モリ・ゾーンに格納することによって、これを実施する。その後第１のメモリ・ゾーンは、書き込み保護され、その後プログラムは、第２のメモリ・ゾーン内で実行可能であるか、又は第１のメモリ・ゾーンに含まれる機能を活動化する、一連の命令の形で第２のメモリ・ゾーンに格納される。

【００１１】

Ｒｕｓｓｅｌｌへの米国特許第５，４８１，２６５号と、第５，７２９，２２０号と、第６，２０１，４８４号と、第６，４４１，７７０号とは、人の認証に使用されるハンドヘルド・デバイス及びそのデバイス対リモート・コンピュータ・システムについて詳述する。更にこの発明は、コンピュータ・システムがリモートでハンドヘルド・デバイスを使用不能にすること、及び他のエミッションを制限することを可能にする、「ｋｉｌｌスイッチ」又は「ｋｉｌｌ信号」を含む。しかしながら、このシステムは、主としてローカル・エリア・ネットワーク・アプリケーションを対象としており、広範なアプリケーションを予想又は提案するものではない。

【発明の開示】

【課題を解決するための手段】

【００１２】

（発明の簡単な概要）

本明細書に開示された発明は、電子デバイス用の回路内セキュリティ・システムである。回路内セキュリティ・システムは、識別信用証明検証と、セキュアなデータ及び命令のストレージと、セキュアなデータ伝送機能と、を組み込む。構成要素のコストを下げ、ボード・スペースを削減する、単一の半導体チップを備える。回路内セキュリティ・システム・チップは、酸素反応層の追加などの情報の不正改ざん又は盗聴を防ぐための機構を使用して、機密保護される。本発明は、回路内セキュリティ・システム及び登録された個人用にセキュリティ設定及びプロファイルを確立するための手段も、組み込む。回路内セキュリティ・システムは、様々な電子デバイス内で使用することができ、それらは、ハンドヘルド・コンピュータと、セキュアな設備キーと、車両オペレーション／イグニッション・システムと、デジタル権管理と、を含む。

【発明を実施するための最良の形態】

【００１３】

本明細書に記載された発明は、回路内セキュリティ・システムであり、これにより、完全に監視及び保護されている環境で、事前登録された個人が、機密データにアクセスするか又は機密データに関するアクションを実行することができる。回路内セキュリティ・システムは、個人の完全な認証を必要とし、事前に設定された認証標準に合致しない場合は様々なプログラミング済みの応答を実行することができる。回路内セキュリティ・システムは、リモート・デバイスへの機密データのセキュアな伝送を含む。

【００１４】

回路内セキュリティ・システムは、単一のセキュア・チップにセキュアに合体された、幾つかの構成要素を備える。図１に示されるように、回路内セキュリティ・システム１００の第１の実施形態は、プロセッサ１０１と、メモリ１０２と、リアルタイム・クロック１０５と、乱数発生器１０８と、を備える。回路内セキュリティ・システム１００は、暗号化サブシステム１０４及び識別信用証明サブシステム１０３も、含む。これらのサブシステムは、論理的、物理的、又はこれらの何らかの組み合わせとすることが可能であり、以下で、更に詳細に説明する。典型的な実施形態では、回路内セキュリティ・システム１００は、リアルタイム・クロック１０５への電力を維持するためにバッテリなどの電源１０６も、含むことになる。回路内セキュリティ・システム１００は、製造時に、読み取りは可能であるが変更又は除去が不可能な固有のワンタイム・プログラム可能電子識別コードを受け取る。好ましくは、回路内セキュリティ・システム１００は、トランシーバ１０７、アンテナ、識別信用センサ、非セキュア・プロセッサなどのオプションの内部／外部構成要素に接続するための、複数の入力／出力インターフェース１１０～１１２も、提供する。

【００１５】
プロセッサ１０１は、主制御構成要素であり、チップの様々な構成要素を制御するための命令のロード及び実行、並びにユーザ要求タスクの実行に関する責務を負う。メモリ１０２は、プロセッサ１０１に結合される。これは、揮発性及び不揮発性の両方の構成要素を備え、セキュリティ設定又はプロファイル及び暗号化鍵などの命令又はデータを格納するために、使用することができる。これらのセキュリティ設定の応用例について、以下で論じる。リアルタイム・クロック１０５も、プロセッサ１０１に結合され、暗号化署名、監査記録、又は他のトランザクションで使用可能な正確な時間を維持するために、使用される。リアルタイム・クロック１０５を電源１０６に接続して、絶えず時間を維持することができる。回路内セキュリティ・システム１００が、電源１０６を含まない場合、リアルタイム・クロック１０５は、電源切断を認識しなければならず、これは、もはや正確な時間が提供できないことを意味する。

【００１６】
回路内セキュリティ・システム１００の第４の構成要素は、乱数発生器１０８である。乱数発生器１０８は、暗号化アルゴリズムのシーディング（ｓｅｅｄｉｎｇ）に使用され、また、十分なランダム性を保証するために何れかの確立された方法を使用することができる。乱数発生器１０８は、暗号化サブシステム１０４の一部として含まれるか、又は、サブシステム１０４に結合されたスタンドアロン型構成要素とすることができる。暗号化サブシステム１０４は、暗号化及び復号と、デジタル署名と、デジタル署名検証と、を実行するための専用システムである。一実施形態では、サブシステム１０４は、それ専用のメモリに暗号化鍵を格納する責務を負い、他の実施形態では、サブシステムは、回路内セキュリティ・システム１００の主メモリ１０２に結合され、これを使用する。加えて、本発明の第１の一実施形態は、暗号化サブシステム１０４として、暗号化加速チップ又は構成要素を使用する。代替実施形態は、主プロセッサ１０１に結合され、暗号化エンジンとして、これを使用する。

【００１７】
識別信用証明検証サブシステム１０３は、回路内セキュリティ・システム１００の使用を試みる個人の識別を判定し、その人物に関連するセキュリティ特権を識別するために、使用される。識別信用証明検証サブシステム１０３は、識別信用証明の取得と、分析と、格納と、突合せと、を実行する。本発明の第１の実施形態では、識別信用証明検証サブシステム１０３は、識別信用証明として、指紋のデジタル表現を使用する。この実施形態では、識別信用証明検証サブシステム１０３は、指紋画像の獲得と、テンプレートの生成、格納及び突合せと、を実行する。識別信用証明検証サブシステム１０３は、信用証明の処理作業に回路内セキュリティ・システム１００の主プロセッサ１０１を使用するか、又はそれ専用の特殊なプロセッサを使用することができる。同様に、信用証明の格納用にそれ専用のメモリを使用するか、又は、回路内セキュリティ・システム１００の主メモリ１０２を使用することができる。回路内セキュリティ・システム１００は、指紋センサなどの信用証明感知用の外部構成要素への１つ又は複数の接続１１０を、提供する。

【００１８】
回路内セキュリティ・システム１００は、プロセッサ１０１に結合された、トランシーバ１０７、アンテナ、電線、又は他のリモート通信デバイスへのインターフェース１１２を組み込む。この構成要素は、デバイス間でのデータの伝送に、使用される。回路内セキュリティ・システム１００から伝送されることになるすべての機密データは、暗号化サブシステム１０４を使用して暗号化可能であるため、トランシーバ１０７を、回路内セキュリティ・システム１００のセキュアな境界内に配置する必要がない。しかしながら、幾つかの実施形態では、トランシーバ１０７を、チップに組み込めば便利であることが証明できる。これらの実施形態では、インターフェース１１２は、トランシーバから、アンテナ、電線、又は他の通信デバイスまでとなる。本発明の第１の実施形態では、伝送技術は、ＩＳＯ　１４４４３　Ａ／Ｂ又は１５６９３標準などの無線周波識別（ＲＦＩＤ）である。他の実施形態では、回路内セキュリティ・システム１００は、Ｂｌｕｅｔｏｏｔｈ又は

赤外線技術を使用する。他の実施形態は、これらの技術又は他の技術の組み合わせを提供する。代替実施形態では、シリアル又はＵＳＢ接続などのワイヤード技術の使用が、有用な場合がある。回路内セキュリティ・システム１００は、好ましくは、必須のコネクタ、ケーブル、又はアンテナ用の外部接続１１２を提供する。

【００１９】

個人の認証により、回路内セキュリティ・システム１００は、個人をシステム内の特定のセキュリティ特権に関連付けることができる。たとえば、一方のユーザは、システム１００をリセットする機能を持たない典型的なユーザとして登録及び識別され、他方のユーザは、その機能を有する管理者として識別されることが可能である。更に、回路内セキュリティ・システム１００は、セキュリティ・イベントに対して、一時的及び永続的の両方の様々な応答を実行するようにプログラムすることができる。たとえば、特定の時間間隔内に指定数のアクセス拒否があれば、登録された管理者がリセットするまで、回路内セキュリティ・システム１００に、すべてのアクションを中断させるか、又は、リアルタイム・クロック１０５を停止させることができる。別の方法として、チップ・ハウジングのケースをこじ開けようと試みると、回路内セキュリティ・システム１００は、メモリ１０２の永続的消去又は他の構成要素の消滅を発生させることができる。回路内セキュリティ・システム１００は、登録された個人が構成要素を直接使用不可又は破棄できるように、プログラムすることも可能である。

【００２０】

前述のように、回路内セキュリティ・システム１００は、指紋センサなどの信用証明感知機構へのインターフェースと、非セキュア・プロセッサ又はユーザ・インターフェース・デバイスなどの周辺構成要素へのインターフェースと、リモート通信用のトランシーバ又はアンテナへのインターフェースとの、３つの主要なインターフェースを備えた１つのセキュア・チップに合体される。他のインターフェースは、厳重に阻止される。このチップは、１つ又は複数の物理的なセキュリティ手段を使用して、情報の盗聴を防止することができる。これらの不明瞭化技法は、「ポッティング（ｐｏｔｔｉｎｇ）」と、酸素反応層と、光センサと、ホール効果センサと、クロック周波数及び／又はリセット周波数を監視する回路との使用を含む。

【００２１】

加えてシステム１００は、インターフェース・トラフィックのアルゴリズム分析を実行することもできる。たとえば、指紋センサから受け取った指紋画像を識別信用証明検証サブシステム１０３によって分析することが可能であり、識別信用証明検証サブシステム１０３が、指紋のまったく同一のビット・パターン表現を繰り返し受け取った場合、何者かが、そのビット・パターンをインターフェース上に故意に置いている可能性がある。同様に、識別信用証明検証サブシステム１０３が、以前に受け取った画像の正確な回転又は他の並べ替えであるビット・パターンを受け取った場合も、何者かが、インターフェースのコンテンツを改変している可能性がある。

【００２２】

回路内セキュリティ・システムは、セキュリティ・アプリケーション用のスタンドアロン型構成要素として、又は、電子デバイス内の複数の構成要素のうちの１つとして、使用することができる。本発明の用法の１つでは、図２に示されるように、ハンドヘルド・コンピュータに、回路内セキュリティ・システム１００が装備される。更にこのコンピュータは、ディスプレイ２１３と、キーパッド２１４と、非セキュア・プロセッサ２０１及びメモリ２０２と、指紋センサ２０３と、を備える。更に、実施形態において、回路内セキュリティ・システム１００が、セルラ式無線技術を使用するトランシーバ１０７を含む場合、ハンドヘルド・コンピュータは、アンテナ２０４も組み込む。

【００２３】

ハンドヘルド・コンピュータの主要なユーザは、指紋と、デジタル証明と、関連する秘密鍵とを、回路内セキュリティ・システム１００に登録する。指紋は、識別信用証明検証サブシステム１０３に格納され、デジタル証明に関連付けられた秘密鍵の使用を許可する

ために使用される。デジタル証明は、回路内セキュリティ・システム１００の暗号化サブシステム１０４又は主メモリ１０２に格納することができる。

【００２４】

個人は、通常、ハンドヘルド・コンピュータを使用して、電子メールを送受信する。自分の電子メールにデジタル署名するためには、その個人は、回路内セキュリティ・システム１００を必要とし、自分の指紋に関連付けられた格納済みの秘密鍵にアクセスする必要がある。その個人は、自分の電子メール・プログラムを選択し、キーパッド２１４を使用して伝送する電子メールをタイプ入力する。キーパッド２１４は、プロセッサ２０１に結合され、これがデータを受け取り、伝送のために適切なメッセージ・パケットを作成する。メッセージ・パケットが作成されると、更に処理するために回路内セキュリティ・システム１００に送られる。

【００２５】

回路内セキュリティ・システム１００のプロセッサ１０１は、このメッセージ・パケットを受け取り、電子メール伝送用に確立されたセキュリティ設定を分析する。回路内セキュリティ・システム１００は、伝送に先立つ電子メールのデジタル署名を必要とするように構成されるため、個人は、第１に自分の指紋を識別信用証明検証サブシステム１０３に認証させなければならない。生物測定認証は、未許可のユーザが自分のものでない秘密鍵を使用して電子メールを暗号化するのを防止するために必要である。プロセッサ１０１は、新しい指紋サンプルを待つようにという信号を指紋センサ２０３から識別信用証明検証サブシステム１０３に対して発信し、ユーザへの可視プロンプトをディスプレイ２１３上に提供するようにという信号を非セキュア・プロセッサ２０１に対して発信する。ユーザが、指紋センサ２０３上に自分の指を置くと、このセンサは、この新しい指紋画像を識別信用証明検証サブシステム１０３に送る。識別信用証明検証サブシステム１０３は、画像を分析し、テンプレートを生成し、これを登録済みの指紋テンプレートと比較する。この２つが一致した場合、識別信用証明検証サブシステム１０３は、その個人が格納済みの秘密鍵を使用する権限を与えられている旨の信号をプロセッサ１０１に送る。

【００２６】

次にプロセッサ１０１は、暗号化サブシステム１０４に電子メール・メッセージを送り、このメッセージに署名するよう暗号化サブシステム１０４に指示する。これには、通常、メッセージのハッシュの生成及び秘密鍵での暗号化が含まれる。暗号化サブシステム１０４は、ハッシュに先立つ、リアルタイム・クロックによって生成されたタイムスタンプ、固有のデバイス識別子、又は他のデータを含むこともできる。次に暗号化サブシステム１０４は、署名済みの電子メール・メッセージをプロセッサ１０１に送り返す。次にプロセッサ１０１は、この署名済み電子メールを、リモート受信者への伝送のためにセルラ式トランシーバ１０７に送る。

【００２７】

本発明の第２の実施形態では、回路内セキュリティ・システム１００は、セキュアな設備へのアクセスを制御するために使用される電子ドア・ロック機構に、埋め込まれる。図３に示されるように、システムは、電子ドア・ロック３１４への有線接続と、指紋センサ２０３と、ユーザに可視フィードバックを提供するために使用される一連の発光ダイオード（ＬＥＤ）３１３とを有する、回路内セキュリティ・システム１００を備える。個人は、回路内セキュリティ・システム１００で自分の指紋登録を明示することによって、セキュアな設備にアクセスする。回路内セキュリティ・システム１００のセキュリティ設定は、事前に指定されたタイム・スパン内に事前に指定された回数の試行失敗があると、ロッキング機構全体をシャット・ダウンするように構成される。これは、メモリ１０２内に格納されるセキュリティ・パラメータ及び設定の例である。

【００２８】

登録された個人が、設備へ入ることを望むとする。１つのＬＥＤ３１３が、指紋センサ３０３の準備ができていることを示す緑色に光る。この個人が、自分の指をセンサ２０３上に置くと、このセンサが、指紋画像を生成し、これを識別信用証明検証サブシステム１

０３に送る。識別信用証明検証サブシステム１０３は、指紋テンプレートを生成し、これを登録された指紋と比較する。新しい指紋テンプレートが、既存のテンプレートと一致するため、識別信用証明検証サブシステム１０３は、この個人の固有の識別子をプロセッサ１０１に送る。プロセッサ１０１は、登録された個人に関連付けられたセキュリティ特権を格納するメモリ１０２にアクセスする。現時点で認証されている個人は、セキュアな設備に単独で入ることを許可されるため、プロセッサ１０１は、解除のためにロック３１４をトリガするようにという信号をトランシーバ１０７に送る。

【００２９】

次に、識別信用証明検証サブシステム１０３に事前に登録されていない個人が、セキュアな設備に入ることを試みるとする。この個人は、自分の指を指紋センサ２０３上に置くと、このセンサ２０３は、指紋の画像を識別信用証明検証サブシステム１０３に送り返す。この指紋がすべての登録済みの指紋と比較され、この個人は登録されていないため、一致は見つからない。識別信用証明検証サブシステム１０３は、失敗したアクセス試行の日付、時間、及び他の必須の特徴を記録し、アクセスが拒否されたことを示すように赤色のＬＥＤ３１３をフラッシュさせる。識別信用証明検証サブシステム１０３は、アクセス失敗が発生した旨を、プロセッサ１０１内の適切なプロセスにも通知する。

【００３０】

次に、個人は、別の登録されていない指を試そうとする。識別信用証明検証サブシステム１０３は、その後の失敗を記録し、別の失敗があった旨をプロセッサ１０１に通知する。失敗した試行回数が、事前に設定された限界に達した場合、識別信用証明検証サブシステム１０３は、失敗が発生した旨を再度プロセッサ１０１に通知する。この時点で、プロセッサ１０１は、セキュリティ設定を適用し、電子ロック機構３１４を認可機関がリセットしない限りロック解除できない状態に置き、第１の実施形態では、これは「フェイルセキュア（ｆａｉｌ－ｓｅｃｕｒｅ）」ロックを使用して実施され、電源の切断を含むことになる。必要に応じてロック３１４をこの状態にするために、代替アクションを実行することもできる。プロセッサ１０１は、識別信用証明検証サブシステム１０３を、新しい指紋の受け入れ、画像の作成、又は突合せの実行を実行しない状態にすることもできる。セキュアな設備の調節装置の所望に応じて、プロセッサ１０１は、識別信用証明検証サブシステム１０３に対して任意の登録済み指紋画像を削除するよう指示することができる。これらはすべて、プログラム可能セキュリティ設定の例である。

【図面の簡単な説明】

【００３１】

【図１】回路内セキュリティ・システムの例示的実施形態を示す概略図である。

【図２】回路内セキュリティ・システムを使用する例示的なハンドヘルド・コンピュータの構成要素を示す概略図である。

【図３】回路内セキュリティ・システムを使用する電子ロック機構の構成要素を示す概略図である。

【符号の説明】

【００３２】

図１：回路内セキュリティ・システム構成要素の例示的実施形態

１００　回路内セキュリティ・システム
１０１　プロセッサ
１０２　メモリ
１０３　識別信用証明検証サブシステム
１０４　暗号化サブシステム
１０５　リアルタイム・クロック
１０６　電源（オプション）
１０７　トランシーバ（オプション）
１０８　乱数発生器
１１０　識別信用証明センサへの接続

１１１　　周辺構成要素への接続
１１２　　アンテナ又はケーブルへの接続
図２：回路内セキュリティ・システムを備えたハンドヘルド・コンピュータ
１００　　回路内セキュリティ・システム
２０１　　非セキュア・プロセッサ
２０２　　非セキュア・メモリ
２０３　　指紋センサ
２０４　　アンテナ
２１３　　ディスプレイ
２１４　　キーパッド
図３：回路内セキュリティ・システムを備えた電子ロック機構
１００　　回路内セキュリティ・システム
３１３　　ＬＥＤ
３１４　　電子ロック機構

【図１】

DRAWINGS

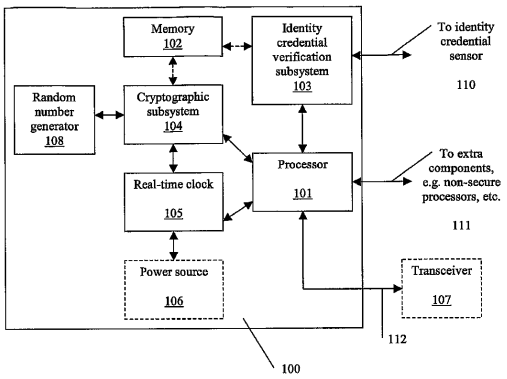


FIGURE 1

【図２】

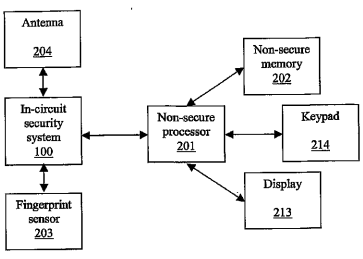


FIGURE 2

【図３】

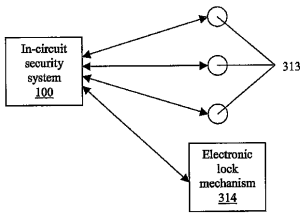


FIGURE 3

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/17272

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : H04L 9/00, 9/32; G06F 12/14
US CL : 713/150, 168, 175, 176, 182-186, 200-202
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/150, 168, 175, 176, 182-186, 200-202

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,173,400 B1 (PERLMAN et al) 09 January 2001, see column 2, lines 8-13; column 4, lines 38-64; column 5, lines 5-10, 18-21, & 35-45; column 6, lines 19-33; and column 11, line 38 through column 12, line 23	1-17

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 November 2004 (13.11.2004)	06 DEC 2004
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703) 305-3230	Authorized officer Ayaz Sheikh for James R. Matthews Telephone No. 703-305-3900

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/17272

Continuation of B. FIELDS SEARCHED Item 3:
BRS (files: USPAT, DERWENT, JPO, EPO, IBM TDB, US PGPUB)

search terms: clock, password, passcode, biometric, encrypt, encryption, encrypted, encrypted, random, number, identity, identifier, identification, identified, credential

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IT,LU,MC,NL,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NA,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

（特許庁注：以下のものは登録商標）
１．Ｂｌｕｅｔｏｏｔｈ

(74)代理人 100096013
弁理士 富田 博行
(74)代理人 100120558
弁理士 住吉 勝彦
(72)発明者 ジョンソン，バリー・ダブリュー
アメリカ合衆国バージニア州２２９１１，シャーロッツヴィル，ティークウッド・コーヴ １４１３
(72)発明者 ティラック，ジョナサン・エイ
アメリカ合衆国バージニア州２２９０２，シャーロッツヴィル，ウッド・ダック・プレイス １１５，ナンバー ４０４
(72)発明者 オルヴェラ，クリステン・アール
アメリカ合衆国バージニア州２２９０３，シャーロッツヴィル，センター・アベニュー １６４２
(72)発明者 ラッセル，デーヴィッド・アール
アメリカ合衆国バージニア州２３４５１－０９１３，バージニア・ビーチ，ピー・オー・ボックス ９１３

Ｆターム(参考) 5B017 AA01 BA05 BA07 CA05
5J104 NA37 NA38 NA39 NA41 PA01 PA07