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

特許第5776927号
(P5776927)

(45)発行日　平成27年9月9日(2015.9.9)　(24)登録日　平成27年7月17日(2015.7.17)

(51)Int.Cl.		F I		
G06F 21/75	(2013.01)	G06F	21/75	
G06F 21/86	(2013.01)	G06F	21/86	
G06K 19/073	(2006.01)	G06K	19/073	063

請求項の数 8　(全 30 頁)

(21)出願番号　特願2011-69925(P2011-69925)
(22)出願日　平成23年3月28日(2011.3.28)
(65)公開番号　特開2012-203800(P2012-203800A)
(43)公開日　平成24年10月22日(2012.10.22)
審査請求日　平成26年3月3日(2014.3.3)

(73)特許権者　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100082131
弁理士　稲本　義雄
(74)代理人　100121131
弁理士　西川　孝
(72)発明者　吉見　英朗
東京都港区港南１丁目７番１号　ソニー株式会社内

審査官　児玉　崇晶

最終頁に続く

(54)【発明の名称】情報処理装置及び方法、並びにプログラム

(57)【特許請求の範囲】
【請求項１】
攻撃を検出する攻撃検出部と、
前記攻撃検出部により攻撃が検出される毎に、セキュリティ対策の強度を段階的に上げるために、重要処理を所定の回数だけ実行し、前記所定の回数分の前記重要処理の結果を比較して一致するか否かを判断する検算処理における前記所定の回数をインクリメントし、所定の条件が満たされる毎に、前記セキュリティ対策の強度を段階的に下げるために前記検算処理における前記所定の回数をデクリメントする強度調整部と
を備える情報処理装置。
【請求項２】
前記強度調整部は、前記セキュリティ対策の強度を上げるために、さらに、タイミングジッタの挿入量の増加、ダミー演算の挿入、通常モードに戻るまでの時間の増加、または規定処理の成功回数の増加のうち、少なくとも１つを行う
請求項１に記載の情報処理装置。
【請求項３】
前記強度調整部は、前記所定の条件として、前記攻撃検出部により攻撃が検出されてから所定時間が経過したという条件、または規定処理の実行が成功したという条件の少なくとも一方が満たされた場合、前記検算の回数をデクリメントする
請求項１または２に記載の情報処理装置。
【請求項４】

前記攻撃検出部による攻撃の検出後にコンデンサを充電する充放電部と、
前記充放電部により放電されつつある前記コンデンサの電荷量と、所定の閾値とを比較する電荷量検出部と
をさらに備え、
前記所定時間は、電荷量が前記所定の閾値となるまでの前記コンデンサの放電時間である
請求項３に記載の情報処理装置。
【請求項５】
前記強度調整部は、前記セキュリティ対策の強度を上げる対象を、前記攻撃検出部により攻撃が検出された関数とする
請求項１から４のいずれかに記載の情報処理装置。
【請求項６】
前記強度調整部は、前記セキュリティ対策の強度を上げる対象を、前記攻撃検出部により攻撃が検出された関数が実行されている前記情報処理装置の構成要素が実行するすべての関数とする
請求項１から５のいずれかに記載の情報処理装置。
【請求項７】
攻撃を検出する攻撃検出ステップと、
前記攻撃検出ステップの処理により攻撃が検出される毎に、セキュリティ対策の強度を段階的に上げるために、重要処理を所定の回数だけ実行し、前記所定の回数分の前記重要処理の結果を比較して一致するか否かを判断する検算処理における前記所定の回数をインクリメントするインクリメントステップと、
所定の条件が満たされる毎に、前記セキュリティ対策の強度を段階的に下げるために前記検算処理における前記所定の回数をデクリメントするデクリメントステップと
を含む情報処理方法。
【請求項８】
攻撃を検出する攻撃検出ステップと、
前記攻撃検出ステップの処理により攻撃が検出される毎に、セキュリティ対策の強度を段階的に上げるために、重要処理を所定の回数だけ実行し、前記所定の回数分の前記重要処理の結果を比較して一致するか否かを判断する検算処理における前記所定の回数をインクリメントするインクリメントステップと、
所定の条件が満たされる毎に、前記セキュリティ対策の強度を段階的に下げるために前記検算処理における前記所定の回数をデクリメントするデクリメントステップと
を含む制御処理をコンピュータに実行させるプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本技術は、情報処理装置及び方法、並びにプログラムに関し、特に、処理速度を維持したまま、セキュリティレベルを向上させることができる、情報処理装置及び方法、並びにプログラムに関する。
【背景技術】
【０００２】
近年、IC(Integrated Circuit)カードに含まれるICチップに対する能動攻撃が脅威となっている。能動攻撃とは、悪意のある第三者が、ICカードにレーザー光を照射させる等して、本来の通常動作とは異なる動作を人為的かつ強制的にICチップに実行させ、秘密情報を入手しようとすることをいう。
【０００３】
このような能動攻撃の代表的な１つとして、DFA(Differential Fault Analysis)攻撃が存在する。DFAとは、悪意のある第三者が、本来の通常動作とは異なる動作を人為的かつ強制的にICチップに実行させ、その結果得られる異常な演算結果と、予め入手しておいた

通常動作による正常な演算結果とを比較することによって、秘密情報を入手しようとすることをいう。

【０００４】

このようなDFA等の能動攻撃に対して秘密情報を保護する従来の手法としては、暗号演算等の重要な処理を検算することで、通常動作とは異なる動作（すなわち、能動攻撃による異常動作）を検出する手法が存在する（特許文献１参照）。

【先行技術文献】

【特許文献】

【０００５】

【特許文献１】特開平１０－１５４９７６号公報

【発明の概要】

【発明が解決しようとする課題】

【０００６】

しかしながら、近年では、強いレーザー光を短周期で照射できる装置が製品化されている。このような装置による能動攻撃に対して、従来の手法を適用して秘密情報を守るためには、検算回数やセキュリティチェックをさらに増す等してセキュリティレベルを向上させる必要がある。一方、セキュリティレベルの向上は、ICチップの処理速度の低下を招く。このように、従来の手法を適用すると、セキュリティレベルと、ICチップの処理速度との間にトレードオフの関係が生じてしまい、ICチップの処理速度を維持したまま、セキュリティレベルを向上させることは非常に困難である。

【０００７】

本技術は、このような状況に鑑みてなされたものであり、処理速度を維持したまま、セキュリティレベルを向上させることができるようにしたものである。

【課題を解決するための手段】

【０００８】

本技術の一側面の情報処理装置は、攻撃を検出する攻撃検出部と、前記攻撃検出部により攻撃が検出される毎に、セキュリティ対策の強度を段階的に上げるために、重要処理を所定の回数だけ実行し、前記所定の回数分の前記重要処理の結果を比較して一致するか否かを判断する検算処理における前記所定の回数をインクリメントし、所定の条件が満たされる毎に、前記セキュリティ対策の強度を段階的に下げるために前記検算処理における前記所定の回数をデクリメントする強度調整部とを備える。

【００１０】

前記強度調整部は、前記セキュリティ対策の強度を上げるために、さらに、タイミングジッタの挿入量の増加、ダミー演算の挿入、通常モードに戻るまでの時間の増加、または規定処理の成功回数の増加のうち、少なくとも１つを行うことができる。

【００１１】

前記強度調整部は、前記所定の条件として、前記攻撃検出部により攻撃が検出されてから所定時間が経過したという条件、または規定処理の実行が成功したという条件の少なくとも一方が満たされた場合、前記検算の回数をデクリメントすることができる。

【００１３】

前記攻撃検出部による攻撃の検出後にコンデンサを充電する充放電部と、前記充放電部により放電されつつある前記コンデンサの電荷量と、所定の閾値とを比較する電荷量検出部とをさらに備え、前記所定時間は、電荷量が前記所定の閾値となるまでの前記コンデンサの放電時間とすることができる。

【００１４】

前記強度調整部は、前記セキュリティ対策の強度を上げる対象を、前記攻撃検出部により攻撃が検出された関数とすることができる。

【００１５】

前記強度調整部は、前記セキュリティ対策の強度を上げる対象を、前記攻撃検出部により攻撃が検出された関数が実行されている前記情報処理装置の構成要素が実行するすべて

の関数とすることができる。
【００１６】
本技術の一側面の情報処理方法及びプログラムは、上述した本技術の一側面の情報処理装置に対応する方法及びプログラムである。
【００１７】
本技術の一側面においては、攻撃が検出され、攻撃が検出される毎に、セキュリティ対策の強度を段階的に上げるために、重要処理を所定の回数だけ実行し、前記所定の回数分の前記重要処理の結果を比較して一致するか否かを判断する検算処理における前記所定の回数がインクリメントされ、また、所定の条件が満たされる毎に、前記セキュリティ対策の強度を段階的に下げるために前記検算処理における前記所定の回数がデクリメントされる。
【発明の効果】
【００１８】
以上のごとく、本技術によれば、処理速度を維持したまま、セキュリティレベルを向上させることができる。
【図面の簡単な説明】
【００１９】
【図１】ICチップの構成例を示すブロック図である
【図２】検算回数を段階的に増やす例について説明する図である。
【図３】ICカードに搭載された充放電回路の原理について説明する図である。
【図４】等価回路のコンデンサＣの充放電時の電荷量のタイミングチャートである。
【図５】CPUの機能的構成例を示すブロック図である。
【図６】第１のセキュリティ対策強度調整処理が開始される状態を示す図である。
【図７】第１のセキュリティ対策強度調整処理の流れを説明するフローチャートである。
【図８】第２のセキュリティ対策強度調整処理の流れを説明するフローチャートである。
【図９】セキュリティ対策の種類と強度の関係について説明する図である。
【図１０】第３のセキュリティ対策強度調整処理の流れを説明するフローチャートである。
【図１１】第４のセキュリティ対策強度調整処理の流れを説明するフローチャートである。
【図１２】第５のセキュリティ対策強度調整処理の流れを説明するフローチャートである。
【図１３】関数Ａの攻撃検出処理の流れを説明するフローチャートである。
【図１４】関数Ｂの攻撃検出処理の流れを説明するフローチャートである。
【図１５】本技術が適用される情報処理装置のハードウエアの構成例を示すブロック図である。
【発明を実施するための形態】
【００２０】
[本技術の概要]
はじめに、本技術の理解を容易なものとすべく、その概略について説明する。
【００２１】
本技術に属するICカードは、能動攻撃（以下、攻撃と略称する）を検出する毎に、セキュリティレベル（以下、セキュリティ対策の強度とも称する）を段階的に上げる。例えば、セキュリティ対策として暗号演算の検算が採用されているICカードは、攻撃を検出する毎に、検算回数を１回ずつ増やしていく。すると、攻撃者がICカードに対する攻撃を試みる毎に、当該ICカードのセキュリティ対策の強度は加速度的に上がるので、当該ICカードに対する攻撃の成功率は飛躍的に低下していく。
【００２２】
一方、セキュリティ対策の強度を上げたままでは、処理速度が低下して、ユーザビリティが損なわれるおそれがある。したがって、本技術に属するICカードは、ユーザビリティ

を維持するために、攻撃検出後に所定の条件が満たされると、セキュリティ対策の強度を段階的に下げる。例えば、攻撃検出後に所定時間が経過した場合や、既定処理の実行に成功した場合、当該ICカードは、検算回数を１回ずつ減らしていく。すると、所定の条件が満たされる毎に処理速度はもとの速度に近づくので、ユーザビリティが維持される。

【００２３】

このように、ICカードにつき、セキュリティ対策の強度を段階的に調整することにより、処理速度を維持したまま、セキュリティレベルを向上させることができる。

【００２４】

以下、本技術の４つの実施形態（以下、それぞれ第１実施形態乃至第４実施形態と称する）について、次の順序で説明する。

１．第１実施形態（セキュリティ対策として検算回数を段階的に調整する例）
２．第２実施形態（複数のセキュリティ対策の強度を段階的に調整する例）
３．第３実施形態（セキュリティ対策の強度を段階的に調整する関数を限定する例）
４．第４実施形態（セキュリティ対策の強度を段階的に調整する箇所を限定する例）

【００２５】

＜１．第１実施形態＞

[ICカードの構成例]

図１は、ICカードに含まれるICチップの構成例を示すブロック図である。

【００２６】

ICチップ１１は、センサ２１、RAM（Random Access Memory）２２、EEPROM（Electrically Erasable and Programmable Read Only Memory）２３、ROM（Read Only Memory）２４、暗号エンジン２５、乱数発生器２６、I/O（Input/Output）２７、およびCPU(Central Processing Unit)２８が、内部バス２９により相互に接続されることにより構成される。

【００２７】

センサ２１は、ICチップ１１への供給電圧、クロック周波数、温度や光といった外部条件等を検出し、検出結果が、予め設定された正常な範囲内にあるか否かを監視する。

【００２８】

RAM２２は、CPU２８が各種の処理を実行する上で必要な各種データなどを適宜記憶する。

【００２９】

EEPROM２３、ROM２４は、各種プログラムを記憶する。

【００３０】

暗号エンジン２５は、乱数発生器２６が発生した乱数を用いて、リーダライタ等の他の装置とICカードとの間で送受信されるデータ、EEPROM２３に記憶されたデータ等の各種データをAES(Advanced Encryption Standard)方式で暗号化または復号化する。また、暗号エンジン２５は、暗号化又は復号化に際し、鍵の生成、および相互認証等を行う。

【００３１】

乱数発生器２６は、暗号エンジン２５で用いる乱数を発生させ、内部バス２９を介して暗号エンジン２５に供給する。

【００３２】

I/O２７は、他の装置とデータの送受信を行う。I/O２７は、例えば、リーダライタと電磁波を利用して非接触でデータの送受信を行い、CPU２８から内部バス２９を介して供給されるデータをリーダライタに送信したり、リーダライタからのデータを受信して内部バス２９を介してCPU２８等に供給する。

【００３３】

CPU２８は、EEPROM２３またはROM２４に記録されているプログラムに従って各種の処理を実行する。または、CPU２８は、RAM２２にロードされたプログラムに従って各種の処理を実行する。RAM２２にはまた、CPU２８が各種の処理を実行する上で必要なデータなども適宜記憶される。

【００３４】
図１に示されるICチップ１１は、攻撃を検出する検出手法として、例えば、次の３通りの検出手法を採用することができる。
【００３５】
第１の検出手法は、センサ２１が外部条件等から攻撃を検出する手法である。上述したように、センサ２１は、ICチップ１１への供給電圧、クロック周波数、温度や光などの外部条件等を検出し、その検出結果が、予め設定された正常な範囲内にあるか否かを監視する。そして、センサ２１は、これらの外部条件等の検出値が異常値を示した場合には、ICチップ１１が攻撃を受けたと判断する。
【００３６】
第２の検出手法は、CPU２８が重要な処理の検算結果から攻撃を検出する手法である。CPU２８は、重要な処理に対しては検算を行い、通常の演算結果と検算の演算結果が一致するかを検証する。そして、CPU２８は、通常の演算結果と検算の演算結果が一致しなかった場合には、ICチップ１１が攻撃を受けたと判断する。
【００３７】
第３の検出手法は、CPU２８が関数の戻り値から攻撃を検出する手法である。CPU２８は、予め設定された関数の戻り値が正常であるかを検証する。そして、CPU２８は、戻り値が異常な値を示した場合には、ICチップ１１が攻撃を受けたと判断する。
【００３８】
なお、第１乃至第３の検出手法は、個別に単体で用いてもよいし、任意の種類の任意の個数の検出手法を組み合わせて用いてもよい。さらに、ここでは説明しない別の検出手法を、単体で、又は、第１乃至第３の検出手法を含む他の検出手法のうち、任意の種類の任意の個数の検出手法と組み合せてもよい。要するに、ICチップ１１が攻撃を検出する手法は、ICチップ１１に対する攻撃を検出できる手法であれば足り、１以上の任意の種類の任意の個数の手法を適宜組み合わせて用いることができる。
【００３９】
ICチップ１１は、これらの手法により攻撃を検出した場合、攻撃を検出する毎に重要な処理の検算回数のカウント値を１ずつインクリメントすることによって、攻撃が成功してしまう難易度を上げる。以下、検算回数が増やされる重要な処理として、暗号演算が採用された場合を例に説明する。
【００４０】
[検算回数を段階的に増やす例]
図２は、暗号演算の検算回数を段階的に増やす例について説明する図である。
【００４１】
図２の左側の図に示されるように、セキュリティレベル１の時、すなわち攻撃が検出されていない通常時には、ICチップ１１は、第１暗号演算を実行した後で、その検算を目的として、第１暗号演算と同様の第２暗号演算を実行する。したがって、セキュリティレベル１の場合、検算回数は１回となる。ICチップ１１は、第１暗号演算と第２暗号演算の２つの演算結果を比較する比較処理を実行し、演算結果が一致した場合には攻撃を受けていないと判断し、一致しない場合には攻撃を受けたと判断する。
【００４２】
換言すると、攻撃者にとってすれは、第１暗号演算と第２暗号演算の両方を攻撃して同一エラーを発生させることができれば、比較処理の結果が一致してしまうので、ICチップ１１に攻撃を受けていないと判断させることができる。この場合、ICチップ１１に気付かれないうちに秘密情報が攻撃者に入手されてしまう。しかしながら、１回の攻撃のみで、連続して２回の同一エラーを発生させることは困難であるし、また、１回のエラー結果のみから秘密情報が漏洩してしまうことは非常にまれである。このため、通常、攻撃者は、ICチップ１１に何度も攻撃を検出されながらも、複数回にわたって攻撃を執拗に繰り返すことになる。
【００４３】

そこで、セキュリティレベル１の状態で攻撃が１度検出されると、ICチップ１１は、図２の中央の図に示されるように、セキュリティレベルを２にあげて、暗号演算の検算回数を２回に増やす。すなわち、ICチップ１１は、第１暗号演算を実行した後で、その検算として、第２暗号演算及び第３暗号演算を行う。そして、ICチップ１１は、第１暗号演算乃至第３暗号演算の３つの演算結果を比較する比較処理を実行し、３つの演算結果が全て一致した場合には攻撃を受けていないと判断し、３つの演算結果から選択された２つの演算結果の組み合わせのうち、１つの組み合わせでも一致しない場合には攻撃を受けたと判断する。

【００４４】

換言すると、攻撃者にとっては、ICチップ１１に攻撃を受けていないと判断させるためには、セキュリティレベル１では、連続して同一エラーを発生させる回数は２回必要があったところ、セキュリティレベル２になると、当該回数は３回に増えることになる。このように、セキュリティレベル１からセキュリティレベル２になると、検算回数が２回から３回に増加し、その結果、攻撃の難易度（すなわち、秘密情報の入手に失敗する確率）が高くなる。

【００４５】

さらに、セキュリティレベル２の状態で攻撃が検出されると、ICチップ１１は、図２の右側に示されるように、セキュリティレベルを３にあげて、暗号演算の検算回数を３回に増やす。すなわち、ICチップ１１は、第１暗号演算を実行した後で、その検算として、第２暗号演算乃至第４暗号演算を行う。そして、ICチップ１１は、第１暗号演算乃至第４暗号演算の４つの演算結果を比較する比較処理を実行し、４つの演算結果が全て一致した場合には攻撃を受けていないと判断し、４つの演算結果から選択された２つの演算結果の組み合わせのうち、１つの組み合わせでも一致しない場合には攻撃を受けたと判断する。

【００４６】

換言すると、攻撃者にとっては、ICチップ１１に攻撃を受けていないと判断させるためには、セキュリティレベル２では、連続して同一エラーを発生させる回数は３回必要があったところ、セキュリティレベル３になると、当該回数は４回に増えることになる。このように、セキュリティレベル２からセキュリティレベル３になると、検算回数が３回から４回に増加し、その結果、攻撃の難易度（すなわち、秘密情報の入手に失敗する確率）が高くなる。

【００４７】

このように、攻撃が検出される毎に、セキュリティレベルが上がり、その分だけ検算回数が増加していくので、その結果、攻撃の難易度が向上し、攻撃者が秘密情報を入手できる確率は低下していく。

【００４８】

なお、当然のことながら、セキュリティの上昇毎に増加させる検算回数は１回ずつに限定されず、任意の回数を採用することができる。

【００４９】

一方、検算回数が増加すると、その分だけ、ICチップ１１の処理速度が低下する。したがって、ICチップ１１は、所定の条件が満たされた場合には検算回数を減らすことで、自己の処理速度の低下を抑制する。ここで、所定の条件として、例えば、次の２通りの条件のうち一方または両者の組み合わせを採用することができる。

【００５０】

第１の条件として、攻撃検出から所定時間が経過したことという条件を採用することができる。すなわち、攻撃検出から所定時間、例えば３０分が経過する毎に、第１の条件が満たされたとして検算回数が１回ずつ減らされる。

【００５１】

第２の条件として、既定処理の実行が成功したことという条件を採用することができる。すなわち、規定処理、例えば相互認証処理における相互認証コマンドに従った処理の実行が成功した場合、条件が満たされたとして検算回数が１回減らされる。なお、既定処理

としては、相互認証コマンドの実行に限定されず、例えば、検算回数初期化コマンドに従った処理等、その他ICチップ１１が行う各種各様の処理を実行することができる。

【００５２】

このように、第１の条件や第２の条件といったように、所定の条件が満たされた場合に検算回数を減らすことで、ICチップ１１の処理速度の低下を抑制することができる。なお、所定の条件は、上述の第１及び第２の条件に限定されない。

【００５３】

以下、さらに、このような第１の条件と第２の条件のうち、第１の条件の詳細について説明する。

【００５４】

電力が常時供給される装置であれば、当該装置内に搭載されたクロックカウンタに基づいて、所定時間を計時することは容易である。しかしながら、従来のICカードは、リーダライタ等に接近している時にしか電力が供給されないので、所定時間を計測するのは非常に困難であった。

【００５５】

そこで、本実施形態のICチップ１１を搭載したICカードは、内蔵するコンデンサの充放電時間を用いて所定時間を計測することで、第１の条件が採用可能に構成されている。

【００５６】

本実施形態のICカードには、所定時間の計測が可能となるように設計された充放電回路が搭載されている。このような充放電回路を用いた所定時間の計測について図３と図４を用いて説明する。

【００５７】

[所定時間の計測について]

図３は、本実施形態のICカードに搭載された充放電回路の原理について説明する図である。

【００５８】

図３Ａは、リーダライタ等が接近してコンデンサが充電する場合の充放電回路４１の等価回路図である。

【００５９】

充放電回路４１は、コンデンサＣ、及び抵抗Ｒ１，Ｒ２により構成されるＣＲ回路である。即ち、コンデンサＣと抵抗Ｒ２との並列接続のうち、一端が接地され、他端には、入力端が接続される。ICカードがリーダライタ等に接近すると、入力端に電源Ｅｒが接続され、当該入力端と抵抗Ｒ１の一端とが接続された状態、換言すると、入力端と抵抗Ｒ１を介して出力端とを結ぶ仮想スイッチ４２がオン状態になったのと等価な状態になる。この場合、リーダライタ等から供給される電力（等価回路上は電源Ｅｒから供給される電力）は、コンデンサＣの充電に用いられ、その結果、所定の電荷量Ｑの電荷が蓄えられる。

【００６０】

図３Ｂは、リーダライタ等が離間してコンデンサが放電する場合の充放電回路４１の等価回路図である。

【００６１】

リーダライタ等がICカードから離間すると、図３Ｂに示すように、入力端と抵抗Ｒ１を介して出力端とを結ぶ仮想スイッチ４２がオフ状態になったのと等価な状態になる。この場合、コンデンサＣに蓄積された所定の電荷量Ｑの電荷は、出力端側に放電される。

【００６２】

図４は、図３の等価回路のコンデンサＣの充放電時の電荷量のタイミングチャートである。

【００６３】

図４において、縦軸はコンデンサＣの電荷量を示し、横軸は時間を示している。

【００６４】

ICカードがリーダライタ等に接近して、仮想スイッチがオン状態に切り替えられた時刻

、即ちコンデンサＣへの充電が開始した時刻が、基準時刻０とされている。

【００６５】

図４に示すように、基準時刻０にコンデンサＣへの充電が開始されると、その後電荷量は即座に上昇し、電荷量Ｑmaxまで到達する。この段階で、ICカードがリーダライタから離間すると、放電が開始され、電荷量は降下していく。

【００６６】

そこで、本実施形態では、放電開始（充電時間は非常に短いので無視すれば時刻０）から電荷量が所定の閾値Ｌよりも小さくなる時刻ｔ１までの時間Ｔｒが、上述した所定時間、例えば３０分となるように、充放電回路４１が設計される。例えば、充放電回路４１はＣＲ回路であるため、コンデンサＣの放電の応答特性は一次遅れとみなすことができ、所定の閾値Ｌを電荷量Ｑmaxの63%の電荷量とすると、当該閾値Ｌに到達するまでの時間Ｔｒが時定数となるため、時間Ｔｒは、コンデンサＣの静電容量と抵抗Ｒ２の抵抗値の積によって容易に求めることができる。換言すると、設計者は、時間Ｔｒが所定時間（例えば３０分）となるように、充放電回路４１のコンデンサＣの静電容量と抵抗Ｒ２の抵抗値とを容易に設計することができる。なお、このような閾値Ｌと所定時間は、例示に過ぎない。

【００６７】

本実施形態のICカードは、このように所定時間を計測可能な充放電回路４１を搭載しているので、攻撃が終了した後の検算回数を減らすための第１の条件を採用することができる。即ち、本実施形態のICカードは、充放電回路４１により攻撃検出から所定時間が計測されると、第１の条件が満たされたとして、検算回数を１回減らす。

【００６８】

[CPUの機能的構成例]

図５は、図１のCPU２８が有する機能のうち、セキュリティ対策の強度を段階的に調整するための各種機能を実現させるための機能的構成例を示すブロック図である。

【００６９】

CPU２８は、電源起動部６１、強度判定部６２、メイン処理部６３、攻撃検出部６４、強度調整部６５、充放電部６６、動作停止部６７、電荷量検出部６８、規定処理部６９、および規定処理監視部７０を有している。

【００７０】

電源起動部６１は、ICカードがリーダライタ等に接近すると、仮想的に電源を起動させ、ICカードがリーダライタ等から離間すると、仮想的に電源を落とす。ここで、仮想的に電源を起動するとは、充放電回路４１を図３Ａに示す等価回路として機能させることを意味する。一方、仮想的に電源を落とすとは、充放電回路４１を図３Ｂに示す等価回路として機能させることを意味する。

【００７１】

強度判定部６２は、現在のICカードに設定されているセキュリティ対策の強度として、検算回数を判定する。

【００７２】

メイン処理部６３は、ICチップ１１が実行すべき処理のコマンドを受信して実行する。

【００７３】

攻撃検出部６４は、ICチップ１１に対する攻撃を検出する。すなわち、攻撃検出部６４は、上述した攻撃を検出する第１乃至第３の検出手法のうちの少なくとも１つの検出手法に従って、ICチップ１１に対する攻撃を検出する。

【００７４】

強度調整部６５は、セキュリティ対策の強度の設定の調整、すなわち、検算回数の増減の調整を行う。

【００７５】

充放電部６６は、図３の充放電回路４１に相当し、電源起動部６１により仮想的に電源が起動されるとコンデンサＣの充電を開始し、電源起動部６１により仮想的に電源が落とされるとコンデンサＣの放電を開始する。

【００７６】
動作停止部６７は、CPU２８の動作、特にメイン処理部６３の動作を停止させる制御を実行する。
【００７７】
電荷量検出部６８は、充放電部６６（すなわち、図３の充放電回路４１）のコンデンサＣの電荷量を検出し、所定の閾値Ｌと比較することによって、検算回数を減らすための第１の条件が満たされたか否かを判定する。すなわち、電荷量検出部６８は、コンデンサの電荷量が所定の閾値Ｌよりも小さくなったことを検出したとき、第１の条件が満たされて所定時間が経過したと判断する。
【００７８】
規定処理部６９は、検算回数を減らすための第２の条件として採用される規定処理を実行する。このような規定処理としては、例えば、相互認証コマンドや検算回数初期化コマンドの実行等の処理を採用することができる。
【００７９】
規定処理監視部７０は、規定処理部６９による規定処理の実行が成功したかを監視する。
【００８０】
次に、検算回数を減らす所定の条件として、第１の条件、すなわち攻撃検出から所定時間の経過が採用された場合のCPU２８が実行する処理（以下、第１のセキュリティ対策強度調整処理と称する）について説明する。
【００８１】
[第１のセキュリティ対策強度調整処理]
図６は、第１のセキュリティ対策強度調整処理が開始される状態を示す図である。
【００８２】
ICチップ１１を含む非接触型のICカード８１は、リーダライタ８２に接近すると、電磁誘導によってリーダライタ８２から電力の供給を受ける。すると、図７に示される第１のセキュリティ対策強度調整処理が開始される。
【００８３】
図７は、第１のセキュリティ対策強度調整処理の流れを説明するフローチャートである。
【００８４】
ステップＳ１１において、電源起動部６１は、リーダライタ８２から供給された電力により仮想的に電源を起動する。
【００８５】
ステップＳ１２において、強度判定部６２は、検算回数が初期値であるかを判定する。なお、検算回数の初期値は、図２を用いて上述したセキュリティレベル１の検算回数である１回が採用されている。
【００８６】
検算回数が初期値の１回でない場合、ステップＳ１２においてＮＯであると判定されて、処理はステップＳ２０に進む。なお、ステップＳ２０以降の処理については後述する。
【００８７】
これに対して、検算回数が初期値の１回である場合、ステップＳ１２においてＹＥＳであると判定されて、処理はステップＳ１３に進む。すなわち、今までに一度も攻撃が検出されていないか、または攻撃が検出された後に、後述するステップＳ２１で検算回数が初期値に戻された後に攻撃が再検出されていない場合、ステップＳ１２においてＹＥＳであると判定されて、処理はステップＳ１３に進む。
【００８８】
ステップＳ１３において、メイン処理部６３は、コマンド待ち受け状態にする。すなわち、メイン処理部６３は、リーダライタ８２からコマンドが送信されるのを待つ。
【００８９】

ステップＳ１４において、メイン処理部６３は、コマンドを受信したかを判定する。

【００９０】

コマンドが受信されない場合、ステップＳ１４においてＮＯであると判定され、処理はステップＳ１３に戻され、それ以降の処理が繰り返される。すなわち、コマンドを受信するまでの間、ステップＳ１３，Ｓ１４のループ処理が繰り返される。

【００９１】

その後、コマンドを受信した場合、ステップＳ１４においてＹＥＳであると判定されて、処理はステップＳ１５に進む。

【００９２】

ステップＳ１５において、メイン処理部６３は、受信したコマンドを実行する。

【００９３】

ステップＳ１６において、攻撃検出部６４は、攻撃を検出したかを判定する。すなわち、攻撃検出部６４は、上述した第１乃至第３の検出手法等により、ICチップ１１に対する攻撃の検出を試みる。

【００９４】

攻撃が検出されていない場合、ステップＳ１６においてＮＯであると判定され、処理はステップＳ１３に戻され、それ以降の処理が繰り返される。すなわち、攻撃を検出するまでの間、ステップＳ１３乃至Ｓ１６のループ処理が繰り返される。

【００９５】

その後、攻撃が検出された場合、ステップＳ１６においてＹＥＳであると判定されて、処理はステップＳ１７に進む。

【００９６】

ステップＳ１７において、強度調整部６５は、検算回数を１回増やす。すなわち、強度調整部６５は、検算回数を初期値の１回から２回に増やし、セキュリティ対策の強度を上げる。

【００９７】

ステップＳ１８において、充放電部６６は、コンデンサを充電する。すなわち、充放電部６６は、攻撃検出からの所定時間の経過を計測するために、コンデンサを充電する

【００９８】

ステップＳ１９において、動作停止部６７は、ＩＣチップ１１の動作を停止する。

【００９９】

これにより、第１のセキュリティ対策強度調整処理は終了する。

【０１００】

一方、ステップＳ１２において検算回数が初期値でない場合、ＮＯであると判定されて、処理はステップＳ２０に進む。すなわち、攻撃が検出されて検算回数が増やされた後に、ICカードがリーダライタ等に接近されると、再度第１のセキュリティ対策強度調整処理が開始するので、このような場合検算回数は初期値の１回ではないと判定され、即ちステップＳ１２においてＮＯであると判定されて、処理はステップＳ２０に進む。

【０１０１】

ステップＳ２０において、電荷量検出部６８は、コンデンサの電荷量が閾値Ｌより小さいかを判定する。すなわち、電荷量検出部６８は、攻撃検出から所定時間が経過したかを判定する。

【０１０２】

コンデンサの電荷量が閾値Ｌをまだ下回っていない場合、すなわち、前回の攻撃検出から所定時間が経過していない場合、ステップＳ２０においてＮＯであると判定されて、処理はステップＳ１３に進む。すなわち、検算回数は減らされないまま、メイン処理が開始される。

【０１０３】

これに対して、コンデンサの電荷量が閾値Ｌを下回っている場合、すなわち、前回の攻撃検出から所定時間が経過している場合、ステップＳ２０においてＹＥＳであると判定さ

れて、処理はステップＳ２１に進む。
【０１０４】
ステップＳ２１において、強度調整部６５は、検算回数を１回減らす。例えば、強度調整部６５は、ステップＳ１２の時点で検算回数が３回であった場合には、検算回数を３回から２回に減らす。また例えば、強度調整部６５は、ステップＳ１２の時点で検算回数が２回であった場合には、検算回数を２回から１回に減らす。
【０１０５】
ステップＳ２２において、強度判定部６２は、検算回数が初期値に戻っているかを判定する。
【０１０６】
検算回数が初期値である１回に戻っている場合、ステップＳ２２においてＹＥＳであると判定されて、処理はステップＳ１３に進む。
【０１０７】
これに対して、検算回数が初期値である１回に戻っていない場合、ステップＳ２２においてＮＯであると判定されて、処理はステップＳ２３に進む。例えば、ステップＳ１２の時点で検算回数が３回であった場合には、ステップＳ２１の処理で検算回数が２回になるため、強度判定部６２は、ステップＳ２２で検算回数が初期値に戻っていないと判定する。
【０１０８】
ステップＳ２３において、充放電部６６は、コンデンサを充電する。すなわち、充放電部６６は、所定時間の経過の計測をリセットするために、コンデンサを再度充電する。
【０１０９】
その後、処理はステップＳ１３に進む。ステップＳ１３乃至ステップＳ１６の処理については繰り返しになるので、その説明を省略する。
【０１１０】
ステップＳ１７において、強度調整部６５は、検算回数を増やす。すなわち、ステップＳ２３の処理でコンデンサが充電され、所定時間の経過が計測されている間に攻撃が検出された場合にも、検算回数は増やされる。
【０１１１】
ステップＳ１８において、充放電部６６は、コンデンサを充電する。すなわち、充放電部６６は、所定時間の経過が計測されている間に攻撃が検出された場合、再度攻撃検出からの所定時間の経過を計測するために、コンデンサを充電する。
【０１１２】
ステップＳ１９において、動作停止部６７は、ＩＣチップ１１の動作を停止する。
【０１１３】
これにより、第１のセキュリティ対策強度調整処理は終了する。
【０１１４】
なお、ステップＳ１８のコンデンサを充電する処理は、ステップＳ１５のコマンドの実行中に実行されてもよい。これにより、攻撃者によってコンデンサの充電中に電力の供給が停止され、所定時間を待たずに検算回数が初期値に戻されることを回避することができる。
【０１１５】
次に、検算回数を減らす所定の条件として、第２の条件、すなわち既定処理の実行が成功したことという条件が採用された場合のCPU２８が実行する処理（以下、第２のセキュリティ対策強度調整処理と称する）について図８を用いて説明する。
【０１１６】
[第２のセキュリティ対策強度調整処理]
図８は、第２のセキュリティ対策強度調整処理の流れを説明するフローチャートである。
【０１１７】

ICチップ１１を含む非接触型のICカード８１は、リーダライタ８２に接近すると、電磁誘導によってリーダライタ８２から電力の供給を受ける。すると、図８に示される第２のセキュリティ対策強度調整処理が開始される。

【０１１８】

ICカード８１がリーダライタ８２に接近すると、第２のセキュリティ対策強度調整処理が開始される。

【０１１９】

ステップＳ３１において、電源起動部６１は、リーダライタ８２から供給された電力により仮想的に電源を起動する。

【０１２０】

ステップＳ３２において、メイン処理部６３は、コマンド待ち受け状態にする。すなわち、メイン処理部６３は、リーダライタ８２からコマンドが送信されるのを待つ。

【０１２１】

ステップＳ３３において、メイン処理部６３は、コマンドを受信したかを判定する。

【０１２２】

コマンドが受信されない場合、ステップＳ３３においてＮＯであると判定され、処理はステップＳ３２に戻され、それ以降の処理が繰り返される。すなわち、コマンドを受信するまでの間、ステップＳ３２，Ｓ３３のループ処理が繰り返される。

【０１２３】

その後、コマンドを受信した場合、ステップＳ３３においてＹＥＳであると判定されて、処理はステップＳ３４に進む。

【０１２４】

ステップＳ３４において、メイン処理部６３は、受信したコマンドが規定処理のコマンドであるかを判定する。

【０１２５】

受信したコマンドが規定処理のコマンドではない場合、ステップＳ３４においてＮＯであると判定されて、処理はステップＳ３５に進む。

【０１２６】

ステップＳ３５において、メイン処理部６３は、受信したコマンドを実行する。その後、処理はステップＳ３９に進む。なお、ステップＳ３９以降の処理については後述する。

【０１２７】

これに対して、ステップＳ３４において、受信したコマンドが規定処理のコマンドである場合、ＹＥＳであると判定されて、処理はステップＳ３６に進む。

【０１２８】

ステップＳ３６において、規定処理部６９は、規定処理のコマンドを実行する。

【０１２９】

ステップＳ３７において、規定処理監視部７０は、規定処理の実行に成功したかを判定する。

【０１３０】

規定処理の実行に成功した場合、ステップＳ３７においてＹＥＳであると判定されて、処理はステップＳ３８に進む。

【０１３１】

ステップＳ３８において、強度調整部６５は、検算回数を初期値の１回に戻す。その後、処理はステップＳ３２に戻され、それ以降の処理が繰り返される。すなわち、規定処理の実行に成功しなくなるまでの間、ステップＳ３２乃至Ｓ３８のループ処理が繰り返される。

【０１３２】

その後、規定処理の実行に成功しなかった場合、処理はステップＳ３７においてＮＯであると判定されて、処理はステップＳ３９に進む。

【０１３３】

ステップＳ３９において、攻撃検出部６４は、攻撃を検出したかを判定する。すなわち、攻撃検出部６４は、上述した第１乃至第３の検出手法等により、ICチップ１１に対する攻撃の検出を試みる。

【０１３４】

攻撃が検出されていない場合、ステップＳ３９においてＮＯであると判定されて、処理はステップＳ３２に戻され、それ以降の処理が繰り返される。すなわち、攻撃を検出するまでの間、ステップＳ３２乃至Ｓ３９のループ処理が繰り返される。

【０１３５】

その後、攻撃が検出された場合、ステップＳ３９においてＹＥＳであると判定されて、処理はステップＳ４０に進む。

【０１３６】

ステップＳ４０において、強度調整部６５は、検算回数を１回増やす。すなわち、強度調整部６５は、検算回数を１回増やし、セキュリティ対策の強度を上げる。

【０１３７】

ステップＳ４１において、動作停止部６７は、ＩＣチップ１１の動作を停止する。

【０１３８】

これにより、第２のセキュリティ対策強度調整処理は終了する。

【０１３９】

以上、説明したように、第１実施形態においては、攻撃が検出される毎に検算回数が増えるので、セキュリティレベルが上がり、攻撃の難易度が向上して攻撃者が秘密情報を入手できる確率は低下していく。また、所定の条件が満たされた場合、検算回数が減るので処理速度を維持することができる。

【０１４０】

＜２．第２実施形態＞

第１実施形態においては、セキュリティ対策として重要な処理の検算が採用され、セキュリティ対策の強度を上げる場合、重要な処理の検算回数が増やされた。しかしながら、セキュリティ対策は、重要な処理の検算のみに限定されず、その他のセキュリティ対策を採用することも、また、それらと組み合わせて採用することもできる。これにより、セキュリティ対策が重要な処理の検算のみの場合と比較して、より一段とセキュリティ対策強度が上がる。

【０１４１】

[セキュリティ対策の種類と強度]

図９は、セキュリティ対策の種類と強度の関係について説明する図である。

【０１４２】

図９に示されるように、セキュリティ対策の種類として、重要な処理の検算、タイミングジッタの挿入、ダミー演算、セキュリティ対策の強度を下げるまでの時間、および規定処理の成功回数を採用することができる。

【０１４３】

検算は、ICチップ１１が行う所定の演算と同じ演算を行い、両者の演算結果の比較処理の結果が一致することを確認する。検算回数を増やすことで、比較処理の結果を一致させることを困難にすることができる。したがって、セキュリティ対策の強度を上げる場合、重要な処理の検算回数を増やすことで、比較処理の結果を一致させて気付かれないうちに秘密情報を入手する攻撃を、より困難にすることができる。

【０１４４】

タイミングジッタは、イベントタイミングのゆらぎであり、タイミングジッタを挿入することで、処理時間をランダム化することができる。したがって、セキュリティ対策の強度を上げる場合、タイミングジッタの挿入量を増やすことにより、クリティカルポイントを狙った攻撃をより困難にすることができる。

【０１４５】

ダミー演算は、ICチップ１１が本来行うべき所定の演算とは異なる演算であり、ランダ

ムに挿入することで、本来行うべき演算のタイミングを推定しにくくすることができる。したがって、セキュリティ対策強度を上げる場合、ダミー演算を挿入することにより、演算が実行される時間を測定して秘密情報を入手する攻撃をより困難にすることができる。

【０１４６】

セキュリティ対策の強度を下げるまでの時間は、第１実施形態で、セキュリティ対策の強度を段階的に下げる場合に第１の条件として採用された「所定時間の経過」における所定時間のことである。すなわち、充放電回路４１のコンデンサＣの電荷量が所定の閾値Ｌよりも小さくなるまでの時間が所定時間となるように、静電容量Ｃと抵抗Ｒの抵抗値の積が設計される。セキュリティ対策の強度を下げるまでの時間を長くすることで、より長くセキュリティ対策の強度が高い状態を保つことができる。したがって、セキュリティ対策の強度を上げる場合、セキュリティ対策の強度を下げるまでの時間を長くすることで、攻撃がより困難である時間を長くすることができる。

【０１４７】

規定処理の成功回数は、第１実施形態で、セキュリティ対策の強度を段階的に下げる場合に第２の条件として採用された「既定処理の実行の成功」の回数のことである。規定処理の成功回数を増やすことで、セキュリティ対策の強度を下げる条件を厳しくすることができる。したがって、セキュリティ対策の強度を上げる場合、規定処理の成功回数を増やすことで、攻撃がより困難である状態を保つことができる。

【０１４８】

以上、説明した複数のセキュリティ対策の強度が、単独または複数組合わされて、攻撃が検出される毎に段階的に調整される。

【０１４９】

例えば、図９に示されるように、セキュリティレベル１（すなわち、攻撃が検出されていない通常時）においては、検算回数を１回、タイミングジッタの挿入量を１０％、ダミー演算の挿入は無、セキュリティ対策の強度を下げるまでの時間を１０分、規定処理の成功回数を１回とする。

【０１５０】

セキュリティレベル２（すなわち、攻撃の累積検出回数が１回）においては、検算回数を２回、タイミングジッタの挿入量を２０％、ダミー演算の挿入は無、セキュリティ対策の強度を下げるまでの時間を３０分、規定処理の成功回数を２回とする。

【０１５１】

セキュリティレベル３（すなわち、攻撃の累積検出回数が２回）においては、検算回数を３回、タイミングジッタの挿入量を３０％、ダミー演算の挿入は有、セキュリティ対策の強度を下げるまでの時間を６０分、規定処理の成功回数を３回とする。

【０１５２】

次に、このように複数のセキュリティ対策を組み合わせた場合におけるセキュリティレベルを下げる条件として、第１の条件（すなわち、攻撃検出から所定時間が経過したことという条件）が採用された場合の処理（以下、第３のセキュリティ対策強度調整処理）について図１０を用いて説明する。

【０１５３】

そして、このように複数のセキュリティ対策を組み合わせた場合におけるセキュリティレベルを下げる条件として、第２の条件（すなわち、既定処理の実行が成功したことという条件）が採用された場合の処理（以下、第４のセキュリティ対策強度調整処理）について図１１を用いて説明する。

【０１５４】

はじめに、セキュリティレベルを下げる条件として、第１の条件、すなわち攻撃検出から所定時間が経過したことという条件が採用された場合の第３のセキュリティ対策強度調整処理について図１０を用いて説明する。

【０１５５】

[第３のセキュリティ対策強度調整処理]

図１０は、第３のセキュリティ対策強度調整処理の流れを説明するフローチャートである。

【０１５６】

第３のセキュリティ対策強度調整処理の各処理は、図７の第１のセキュリティ対策強度調整処理の各処理と基本的に同様の処理である。したがって、同様の処理の説明は繰り返しになるので省略し、異なる処理についてのみ説明する。

【０１５７】

ステップＳ５１において、電源起動部６１は、リーダライタ８２から供給された電力により仮想的に電源を起動する。

【０１５８】

ステップＳ５２において、強度判定部６２は、セキュリティレベルが初期値であるかを判定する。なお、セキュリティレベルの初期値は１であるとする。

【０１５９】

セキュリティレベルが初期値の１でない場合、ステップＳ５２においてＮＯであると判定されて、処理はステップＳ６０に進む。なお、ステップＳ６０以降の処理については後述する。

【０１６０】

これに対して、セキュリティレベルが初期値の１である場合、ステップＳ５２においてＹＥＳであると判定されて、処理はステップＳ５３に進む。

【０１６１】

ステップＳ５３において、メイン処理部６３は、コマンド待ち受け状態にする。その後のステップＳ５４乃至Ｓ５６の処理については、図７のステップＳ１４乃至Ｓ１６の処理と同様であり、繰り返しになるのでその説明を省略する。

【０１６２】

ステップＳ５６において攻撃検出部６４が攻撃を検出した場合、ステップＳ５７において、強度調整部６５は、セキュリティレベルを１上げる。すなわち、強度調整部６５は、セキュリティレベルを１から２に上げて、検算回数を２回、タイミングジッタの挿入量を２０％、ダミー演算の挿入を無とする。

【０１６３】

ステップＳ５８以降の処理は、図７のステップＳ１８以降の処理と同様であり、繰り返しになるのでその説明を省略する。

【０１６４】

一方、ステップＳ５２においてセキュリティレベルが初期値の１でない場合、ＮＯであると判定されて、処理はステップＳ６０に進む。すなわち、攻撃が検出されてセキュリティレベルが上げられた後に、ICカード８１がリーダライタ８２等に接近されると、再度第３のセキュリティ対策強度調整処理が開始する。このような場合、セキュリティレベルは初期値の１ではないと判定され、即ちステップＳ５２においてＮＯであると判定されて、処理はステップＳ６０に進む。

【０１６５】

ステップ６１において、電荷量検出部６８は、コンデンサの電荷量が閾値Ｌより小さいかを判定する。

【０１６６】

コンデンサの電荷量が閾値Ｌをまだ下回っていない場合、ステップＳ６０においてＮＯであると判定されて、処理はステップＳ５３に進む。

【０１６７】

これに対して、コンデンサの電荷量が閾値Ｌを下回っている場合、ステップＳ６０においてＹＥＳであると判定されて、処理はステップＳ６０に進む。

【０１６８】

ステップＳ６１において、強度調整部６５は、セキュリティレベルを１下げる。例えば、強度調整部６５は、ステップＳ５２の時点でセキュリティレベルが３であった場合には

、セキュリティレベルを３から２に下げる。また例えば、強度調整部６５は、ステップＳ５２の時点でセキュリティレベルが２であった場合には、セキュリティレベルを２から１に下げる。

【０１６９】

ステップＳ６２において、強度判定部６２は、セキュリティレベルが初期値に戻っているかを判定する。

【０１７０】

セキュリティレベルが初期値である１に戻っている場合、ステップＳ６１においてＹＥＳであると判定されて、処理はステップＳ５３に進む。

【０１７１】

これに対して、セキュリティレベルが初期値である１に戻っていない場合、ステップＳ６１においてＮＯであると判定されて、処理はステップＳ６２に進む。例えば、ステップＳ５２の時点でセキュリティレベルが３であった場合には、ステップＳ６０の処理でセキュリティレベルが２になるため、強度判定部６２は、ステップＳ６２でセキュリティレベルが初期値に戻っていないと判定する。

【０１７２】

ステップＳ６３以降の処理の説明は、繰り返しになるので省略する。

【０１７３】

第３のセキュリティ対策強度調整処理は、以上のように実行される。

【０１７４】

次に、セキュリティレベルを下げる条件として、第２の条件、すなわち既定処理の実行が成功したことという条件が採用された場合の第４のセキュリティ対策強度調整処理について図１１を用いて説明する。

【０１７５】

[第４のセキュリティ対策強度調整処理]

図１１は、第４のセキュリティ対策強度調整処理の流れを説明するフローチャートである。

【０１７６】

第４のセキュリティ対策強度調整処理の各処理は、図８の第２のセキュリティ対策強度調整処理の各処理と基本的に同様の処理である。したがって、同様の処理の説明は繰り返しになるので省略し、異なる処理についてのみ説明する。

【０１７７】

ステップＳ７１において、電源起動部６１が、リーダライタ８２から供給された電力により仮想的に電源を起動すると、ステップＳ７２において、メイン処理部６３は、コマンド待ち受け状態にする。

【０１７８】

その後のステップＳ７２乃至Ｓ７５の処理については、図８のステップＳ３２乃至Ｓ３５の処理と同様であり、繰り返しになるのでその説明を省略する。

【０１７９】

ステップＳ７４においてメイン処理部６３が規定処理のコマンドを受信した場合、ステップＳ７６において、規定処理部６９は、規定処理のコマンドを既定の回数実行する。すなわち、セキュリティレベルが２の場合には２回、セキュリティレベルが３の場合には３回、既定の処理を実行する。

【０１８０】

ステップＳ７７において、規定処理監視部７０は、規定処理の実行に規定の回数成功したかを判定する。

【０１８１】

規定処理の実行に規定の回数成功した場合、ステップＳ７７においてＹＥＳであると判定されて、処理はステップＳ７８に進む。

【０１８２】

ステップＳ７８において、強度調整部６５は、セキュリティレベルを初期値の１に戻す。その後、処理はステップＳ７２に戻され、それ以降の処理が繰り返される。すなわち、規定処理の実行に規定の回数成功しなくなるまでの間、ステップＳ７２乃至Ｓ７８のループ処理が繰り返される。

【０１８３】

その後、規定処理の実行に規定の回数成功しなかった場合、処理はステップＳ７７においてＮＯであると判定されて、処理はステップＳ７９に進む。

【０１８４】

ステップＳ７９において、攻撃検出部６４は、攻撃を検出したかを判定する。すなわち、攻撃検出部６４は、上述した第１乃至第３の検出手法により、ICチップ１１に対する攻撃の検出を試みる。

【０１８５】

攻撃が検出されていない場合、ステップＳ７９においてＮＯであると判定されて、処理はステップＳ７２に戻され、それ以降の処理が繰り返される。すなわち、攻撃を検出するまでの間、ステップＳ７２乃至Ｓ７９のループ処理が繰り返される。

【０１８６】

その後、攻撃が検出された場合、ステップＳ７９においてＹＥＳであると判定されて、処理はステップＳ８０に進む。

【０１８７】

ステップＳ８０において、強度調整部６５は、セキュリティレベルを１上げる。

【０１８８】

ステップＳ８１において、動作停止部６７は、ＩＣチップ１１の動作を停止する。

【０１８９】

これにより、第４のセキュリティ対策強度調整処理は終了する。

【０１９０】

なお、セキュリティ対策は上述の例に限定されず、さらに、その組み合わせも、セキュリティレベルの増減数も上述の例に限定されない。

【０１９１】

以上、説明したように、第２実施形態においては、複数のセキュリティ対策を組み合わせて採用することができるので、１つのセキュリティ対策を採用するよりもさらにセキュリティ対策強度が上がる。

【０１９２】

＜３．第３実施形態＞

第１及び第２実施形態においては、攻撃が検出される毎、及び所定の条件が満たされる毎にセキュリティ対策強度が段階的に調整された。しかしながら、セキュリティ対策強度の調整は、ICチップ１１が実行する全ての関数に対して行われずに、攻撃が検出された関数のみに行われてもよい。

【０１９３】

例えば、暗号化処理を行っている関数Ａと認証処理を行っている関数Ｂがある場合、それぞれの関数に、重要な処理の検算回数を決定するセキュリティレベルパラメータが保持される。そして、攻撃が検出された関数が保持するセキュリティレベルパラメータの値のみが１増やされる。例えば、関数Ａにのみ攻撃が検出された場合、関数Ａが保持するセキュリティレベルパラメータ（Security_Level_A）の値のみが１増やされる。また例えば、関数Ｂにのみ攻撃が検出された場合、関数Ｂが保持するセキュリティレベルパラメータ（Security_Level_B）の値のみが１増やされる。関数Ａと関数Ｂの両方に攻撃が検出された場合には、両方の関数が保持するセキュリティパラメータの値がそれぞれ１増やされる。

【０１９４】

これにより、検算回数が増える関数は限定される。したがって、ICチップ１１の処理速度が低下するのを抑制し、ユーザビリティを維持することができる。以下、検算回数が増やされる重要な処理を暗号演算として説明する。

【０１９５】
このように、攻撃を検出した関数にのみセキュリティ対策強度の調整を行う場合に、CPU２８が実行する処理（以下、第５のセキュリティ対策強度調整処理と称する）について図１２を用いて説明する。
【０１９６】
[第５のセキュリティ対策強度調整処理]
図１２は、第５のセキュリティ対策強度調整処理の流れを説明するフローチャートである。
【０１９７】
なお、ICチップ１１が実行する全ての関数を、関数Ａ，関数Ｂとする。
【０１９８】
ICチップ１１を含む非接触型のICカード８１は、リーダライタ８２に接近すると、電磁誘導によってリーダライタ８２から電力の供給を受ける。すると、図１２に示される第５のセキュリティ対策強度調整処理が開始される。
【０１９９】
ステップＳ９１において、電源起動部６１は、リーダライタ８２から供給された電力により仮想的に電源を起動する。
【０２００】
ステップＳ９２において、強度判定部６２は、全ての関数のセキュリティレベルパラメータの値が初期値であるかを判定する。すなわち、強度判定部６２は、関数Ａと関数Ｂのセキュリティパラメータである Security_Level_A と Security_Level_B の値が両方とも初期値であるかを判定する。なお、セキュリティレベルパラメータの初期値は１とする。
【０２０１】
Security_Level_A と Security_Level_B のうちのどちらか一方、または両方の値が初期値の１でない場合、ステップＳ９２においてＮＯであると判定されて、処理はステップＳ１０２に進む。なお、ステップＳ１０２以降の処理については後述する。
【０２０２】
これに対して、Security_Level_A と Security_Level_B の両方の値が初期値の１である場合、ステップＳ９２においてＹＥＳであると判定されて、処理はステップＳ９３に進む。すなわち、今までに一度も関数Ａと関数Ｂの両方に攻撃が検出されていないか、または攻撃が検出された関数が、その後、後述するステップＳ１０３でセキュリティレベルパラメータが初期値に戻された後に攻撃が再検出されていない場合、ステップＳ９２においてＹＥＳであると判定されて、処理はステップＳ９３に進む。
【０２０３】
ステップＳ９３において、メイン処理部６３は、コマンド待ち受け状態にする。すなわち、メイン処理部６３は、リーダライタ８２から関数Ａと関数Ｂを実行するためのコマンドが送信されるのを待つ。
【０２０４】
ステップＳ９４において、メイン処理部６３は、コマンドを受信したかを判定する。
【０２０５】
コマンドが受信されない場合、ステップＳ９４においてＮＯであると判定され、処理はステップＳ９３に戻され、それ以降の処理が繰り返される。すなわち、コマンドを受信するまでの間、ステップＳ９３，Ｓ９４のループ処理が繰り返される。
【０２０６】
その後、コマンドを受信した場合、ステップＳ９４においてＹＥＳであると判定されて、処理はステップＳ９５に進む。
【０２０７】
ステップＳ９５において、メイン処理部６３は、受信したコマンドを実行する。すなわち、メイン処理部６３は、受信したコマンドにより関数Ａと関数Ｂの処理を実行する。
【０２０８】

ステップＳ９６において、攻撃検出部６４は、関数Ａの攻撃検出処理を実行する。なお、関数Ａの攻撃検出処理については、図１３を用いて後述する。

【０２０９】

ステップＳ９７において、攻撃検出部６４は、関数Ｂの攻撃検出処理を実行する。なお、関数Ｂの攻撃検出処理については、図１４を用いて後述する。

【０２１０】

なお、ステップＳ９６とステップＳ９７の処理は並行して行われる。

【０２１１】

図１３は、関数Ａの攻撃検出処理の流れを説明するフローチャートである。

【０２１２】

ステップＳ１２１において、攻撃検出部６４は、Security_Level_Aの値が１であるかを判定する。

【０２１３】

Security_Level_Aの値が１でない場合、ステップＳ１２１においてＮＯであると判定されて、処理はステップＳ１２８に進む。なお、ステップＳ１２８以降の処理については後述する。

【０２１４】

Security_Level_Aの値が１である場合、ステップＳ１２１においてＹＥＳであると判定されて、処理はステップＳ１２２に進む。

【０２１５】

ステップＳ１２２において、攻撃検出部６４は、第１暗号演算を実行する。

【０２１６】

ステップＳ１２３において、攻撃検出部６４は、第２暗号演算を実行する。すなわち、規定処理部６９は、第１暗号演算を実行した後で、その検算を目的として、第１暗号演算と同様の第２暗号演算を実行する。

【０２１７】

ステップＳ１２４において、攻撃検出部６４は、比較処理を実行する。すなわち、規定処理監視部７０は、第１暗号演算と第２暗号演算の２つの演算結果を比較する比較処理を実行する。

【０２１８】

ステップＳ１２５において、攻撃検出部６４は、全ての演算結果が一致するかを判定する。

【０２１９】

全ての演算結果が一致する場合、すなわち第１暗号演算と第２暗号演算の２つの演算結果が一致する場合、ステップＳ１２５においてＹＥＳであると判定されて、処理はステップＳ１２６に進む。すなわち、関数Ａは攻撃を受けていないと判断される。

【０２２０】

ステップＳ１２６において、攻撃検出部６４は、正常な戻り値を第５のセキュリティ対策強度調整処理に戻す。

【０２２１】

これにより、関数Ａの攻撃検出処理は終了する。すなわち、図１２のステップＳ９６の処理が終了し、処理はステップＳ９７に進む。

【０２２２】

これに対して、全ての演算結果が一致しない場合、すなわち第１暗号演算と第２暗号演算の２つの演算結果が一致せず、攻撃を受けたと判断された場合、ステップＳ１２５においてＮＯであると判定されて、処理はステップＳ１２７に進む。

【０２２３】

ステップＳ１２７において、攻撃検出部６４は、攻撃検出の戻り値を第５のセキュリティ対策強度調整処理に戻す。

【０２２４】

これにより、関数Ａの攻撃検出処理は終了する。すなわち、図１２のステップＳ９６の処理が終了し、処理はステップＳ９７に進む。

【０２２５】

一方、ステップＳ１２１において、Security_Level_Aの値が１でない場合、ステップＳ１２１においてＮＯであると判定されて、処理はステップＳ１２８に進む。

【０２２６】

ステップＳ１２８において、攻撃検出部６４は、Security_Level_Aの値が２であるかを判定する。

【０２２７】

Security_Level_Aの値が２でない場合、ステップＳ１２８においてＮＯであると判定されて、処理はステップＳ１３４に進む。なお、ステップＳ１３４以降の処理については後述する。

【０２２８】

Security_Level_Aの値が２である場合、ステップＳ１２８においてＹＥＳであると判定されて、処理はステップＳ１２９に進む。

【０２２９】

ステップＳ１２９において、攻撃検出部６４は、第１暗号演算を実行する。

【０２３０】

ステップＳ１３０において、攻撃検出部６４は、第２暗号演算を実行する。すなわち、規定処理部６９は、第１暗号演算を実行した後で、その検算を目的として、第１暗号演算と同様の第２暗号演算を実行する。

【０２３１】

ステップＳ１３１において、攻撃検出部６４は、第３暗号演算を実行する。すなわち、規定処理部６９は、第１暗号演算と同様の第３暗号演算を実行し再度検算を行う。

【０２３２】

ステップＳ１３２において、攻撃検出部６４は、比較処理を実行する。すなわち、規定処理監視部７０は、第１暗号演算乃至第３暗号演算の３つの演算結果を比較する比較処理を実行する。

【０２３３】

ステップＳ１３３において、攻撃検出部６４は、全ての演算結果が一致するかを判定する。

【０２３４】

全ての演算結果が一致する場合、すなわち第１暗号演算乃至第３暗号演算の３つの演算結果が一致する場合、ステップＳ１３３においてＹＥＳであると判定されて、処理はステップＳ１２６に進む。すなわち、関数Ａは攻撃を受けていないと判断される。

【０２３５】

ステップＳ１２６において、攻撃検出部６４は、正常な戻り値を第５のセキュリティ対策強度調整処理に戻す。

【０２３６】

これにより、関数Ａの攻撃検出処理は終了する。すなわち、図１２のステップＳ９６の処理が終了し、処理はステップＳ９７に進む。

【０２３７】

これに対して、全ての演算結果が一致しない場合、すなわち第１暗号演算乃至第３暗号演算の３つの演算結果が全て一致せず、攻撃を受けたと判断された場合、ステップＳ１３３においてＮＯであると判定されて、処理はステップＳ１２７に進む。

【０２３８】

ステップＳ１２７において、攻撃検出部６４は、攻撃検出の戻り値を第５のセキュリティ対策強度調整処理に戻す。

【０２３９】

これにより、関数Ａの攻撃検出処理は終了する。すなわち、図１２のステップＳ９６の

処理が終了し、処理はステップＳ９７に進む。
【０２４０】
一方、ステップＳ１２８において、Security_Level_Aの値が２でない場合、すなわち３以上である場合、ステップＳ１２８においてＮＯであると判定されて、処理はステップＳ１３４に進む。
【０２４１】
ステップＳ１３４において、攻撃検出部６４は、第１暗号演算を実行する。
【０２４２】
ステップＳ１３５において、攻撃検出部６４は、第２暗号演算を実行する。すなわち、規定処理部６９は、第１暗号演算を実行した後で、その検算を目的として、第１暗号演算と同様の第２暗号演算を実行する。
【０２４３】
ステップＳ１３６において、攻撃検出部６４は、第３暗号演算を実行する。すなわち、規定処理部６９は、第１暗号演算と同様の第３暗号演算を実行し再度検算を行う。
【０２４４】
ステップＳ１３７において、攻撃検出部６４は、第４暗号演算を実行する。すなわち、規定処理部６９は、第１暗号演算と同様の第４暗号演算を実行し再度検算を行う。
【０２４５】
ステップＳ１３８において、攻撃検出部６４は、比較処理を実行する。すなわち、規定処理監視部７０は、第１暗号演算乃至第４暗号演算の４つの演算結果を比較する比較処理を実行する。
【０２４６】
ステップＳ１３９において、攻撃検出部６４は、全ての演算結果が一致するかを判定する。
【０２４７】
全ての演算結果が一致する場合、すなわち第１暗号演算乃至第４暗号演算の４つの演算結果が全て一致する場合、ステップＳ１３９においてＹＥＳであると判定されて、処理はステップＳ１２６に進む。すなわち、関数Ａは攻撃を受けていないと判断される。
【０２４８】
ステップＳ１２６において、攻撃検出部６４は、正常な戻り値を第５のセキュリティ対策強度調整処理に戻す。
【０２４９】
これにより、関数Ａの攻撃検出処理は終了する。すなわち、図１２のステップＳ９６の処理が終了し、処理はステップＳ９７に進む。
【０２５０】
これに対して、全ての演算結果が一致しない場合、すなわち第１暗号演算乃至第４暗号演算の４つの演算結果が全て一致せず、攻撃を受けたと判断された場合、ステップＳ１３９においてＮＯであると判定されて、処理はステップＳ１２７に進む。
【０２５１】
ステップＳ１２７において、攻撃検出部６４は、攻撃検出の戻り値を第５のセキュリティ対策強度調整処理に戻す。
【０２５２】
これにより、関数Ａの攻撃検出処理は終了する。すなわち、図１２のステップＳ９６の処理が終了し、処理はステップＳ９７に進む。
【０２５３】
ステップＳ９７において、攻撃検出部６４は、関数Ｂの攻撃検出処理を実行する。
【０２５４】
図１４は、関数Ｂの攻撃検出処理の流れを説明するフローチャートである。
【０２５５】
関数Ｂの攻撃検出処理の各処理は、図１３の関数Ａの攻撃検出処理の各処理と基本的に

同様の処理である。図１３の関数Ａの攻撃検出処理においては、関数Ａが保持するセキュリティレベルパラメータ（Security_Level_A）の値に応じて処理が実行された。これに対して、図１４の関数Ｂの攻撃検出処理においては、関数Ｂが保持するセキュリティレベルパラメータ（Security_Level_B）の値に応じて処理が実行される。したがって、関数Ｂの攻撃検出処理の説明は繰り返しになるので省略する。

【０２５６】

関数Ｂの攻撃検出処理、すなわち図１２のステップＳ９７の処理が終了すると、処理はステップＳ９８に進む。

【０２５７】

ステップＳ９８において、攻撃検出部６４は、関数Ａ、Ｂの両方から正常な戻り値を受け取ったかを判定する。

【０２５８】

関数Ａ、Ｂの両方から正常な戻り値を受け取った場合、すなわち、関数Ａ、Ｂの両方の関数が攻撃を受けていないと判断された場合、ステップＳ９８においてＹＥＳであると判定され、処理はステップＳ９３に戻され、それ以降の処理が繰り返される。すなわち、関数Ａ、Ｂの両方から正常な戻り値を受け取らなくなるまでの間、ステップＳ９３乃至Ｓ９８のループ処理が繰り返される。

【０２５９】

その後、関数Ａ、Ｂの両方から正常な戻り値を受け取らなくなった場合、すなわち、関数Ａ、Ｂのうちの一方、または両方の関数が攻撃を受けたと判断された場合、ステップＳ９８においてＮＯであると判定されて、処理はステップＳ９９に進む。

【０２６０】

ステップＳ９９において、強度調整部６５は、攻撃検出の戻り値を受け取った関数のセキュリティパラメータの値を１増やす。すなわち、強度調整部６５は、関数Ａ、Ｂのうち、攻撃検出の戻り値を受け取った方の関数のセキュリティパラメータの値を１増やす。

【０２６１】

ステップＳ１００において、充放電部６６は、コンデンサを充電する。すなわち、充放電部６６は、攻撃検出からの所定時間の経過を計測するために、コンデンサを充電する。

【０２６２】

ステップＳ１０１において、動作停止部６７は、ＩＣチップ１１の動作を停止する。

【０２６３】

これにより、第５のセキュリティ対策強度調整処理は終了する。

【０２６４】

なお、第５のセキュリティ対策強度調整処理の説明では、検算回数を減らす所定の条件として、第１の条件が採用された場合について説明した。しかしながら、検算回数を減らす所定の条件は上述の例に限定されず、例えば、第２の条件が採用されてもよい。

【０２６５】

以上、説明したように、第３実施形態においては、セキュリティ対策強度が調整される関数が限定されるので、ICチップ１１の処理速度が低下するのを抑制し、ユーザビリティが損なわれることを抑制することができる。

【０２６６】

＜４．第４実施形態＞

第３実施形態においては、攻撃が検出された関数のセキュリティ対策強度のみが調整された。しかしながら、セキュリティ対策強度の調整は、攻撃が検出された関数を実行している、ICチップ１１を構成する構成要素が実行する全ての関数に対して行われてもよい。すなわち、攻撃が検出された関数を実行している、ICチップ１１を構成する構成要素に対してのみセキュリティ対策強度が調整される。ICチップ１１を構成する構成要素とは、図１においてブロックで示されるセンサ２１乃至内部バス２９の各構成要素である。

【０２６７】

この場合、ICチップ１１は、全ての関数がどの構成要素で実行されているのかを表すマ

ッピングテーブルを所持する。そして、所定の関数に対する攻撃を検出した場合、マッピングテーブルを参照して、攻撃を検出した所定の関数を実行しているICチップ１１の構成要素を特定する。そして、当該構成要素が実行している全ての関数に対してセキュリティ対策強度の調整を実行する。なお、セキュリティ対策強度の調整の手法は特に限定されず、例えば、第１乃至第３実施形態において用いられた手法を採用することができる。

【０２６８】

これにより、第４実施形態においては、セキュリティ対策強度が調整される場所が限定されるので、ICチップ１１の処理速度が低下するのを抑制し、ユーザビリティが維持される。

【０２６９】

[本技術のプログラムへの適用]

上述した一連の処理は、ハードウエアにより実行させることもできるし、ソフトウェアにより実行させることもできる。

【０２７０】

この場合、上述した情報処理装置の少なくとも一部として、例えば、図１５に示されるパーソナルコンピュータを採用してもよい。

【０２７１】

図１５において、CPU１０１は、ROM１０２に記録されているプログラムに従って各種の処理を実行する。または記憶部１０８からRAM１０３にロードされたプログラムに従って各種の処理を実行する。RAM１０３にはまた、CPU１０１が各種の処理を実行する上において必要なデータなども適宜記憶される。

【０２７２】

CPU１０１、ROM１０２、及びRAM１０３は、バス１０４を介して相互に接続されている。このバス１０４にはまた、入出力インタフェース１０５も接続されている。

【０２７３】

入出力インタフェース１０５には、キーボード、マウスなどよりなる入力部１０６、ディスプレイなどよりなる出力部１０７が接続されている。また、ハードディスクなどより構成される記憶部１０８、及び、モデム、ターミナルアダプタなどより構成される通信部１０９が接続されている。通信部１０９は、インターネットを含むネットワークを介して他の装置（図示せず）との間で行う通信を制御する。

【０２７４】

入出力インタフェース１０５にはまた、必要に応じてドライブ１１０が接続され、磁気ディスク、光ディスク、光磁気ディスク、或いは半導体メモリなどよりなるリムーバブルメディア１１１が適宜装着される。そして、それらから読み出されたコンピュータプログラムが、必要に応じて記憶部１０８にインストールされる。

【０２７５】

一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウエアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、ネットワークや記録媒体からインストールされる。

【０２７６】

このようなプログラムを含む記録媒体は、図１５に示されるように、装置本体とは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク（フロッピディスクを含む）、光ディスク（CD-ROM(Compact Disk-Read Only Memory),DVD(Digital Versatile Disk)を含む）、光磁気ディスク（MD（Mini-Disk）を含む）、もしくは半導体メモリなどよりなるリムーバブルメディア（パッケージメディア）２１１により構成されるだけでなく、装置本体に予め組み込まれた状態でユーザに提供される、プログラムが記録されているROM１０２や、記憶部１０８に含まれるハードディスクなどで構成される。

【０２７７】

なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、その順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【０２７８】

本技術の実施の形態は、上述した実施の形態に限定されるものではなく、本技術の要旨を逸脱しない範囲において種々の変更が可能である。

【０２８０】

本技術は、非接触ICカードに適用することができる。

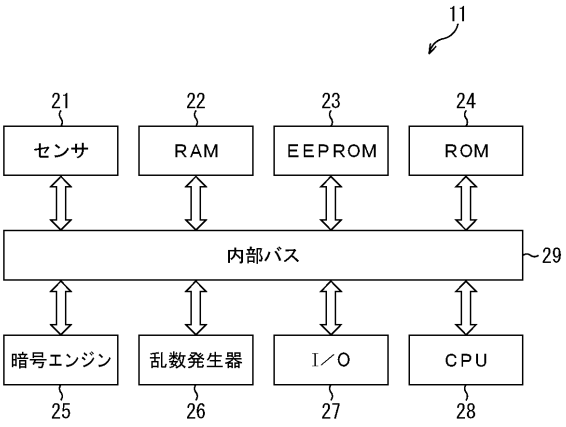
【符号の説明】

【０２８１】

１１　ICチップ，　２１　センサ，　２８　CPU，　４１　充放電回路，　６１　電源起動部，　６２　強度判定部，　６３　メイン処理部，　６４　攻撃検出部，　６５　強度調整部，　６６　充放電部，　６７　動作停止部，　６８　電荷量検出部，　６９　規定処理部，　７０　規定処理監視部

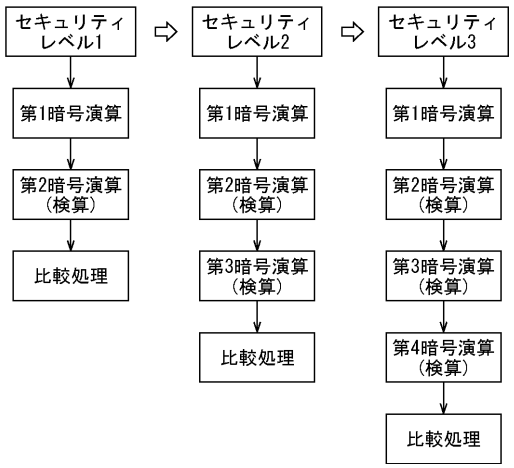
【図１】

図1

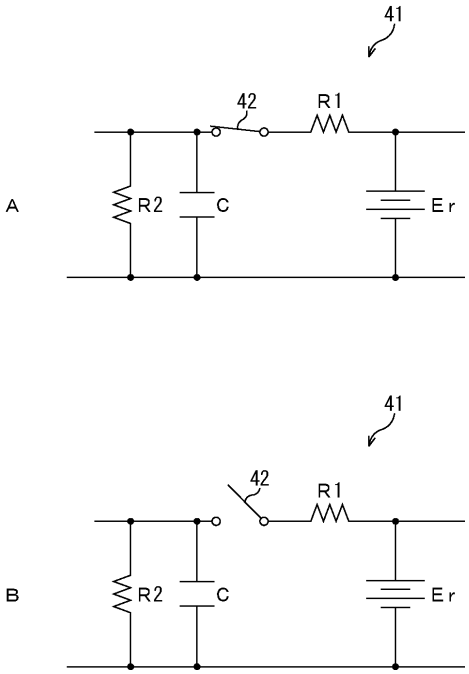


【図２】

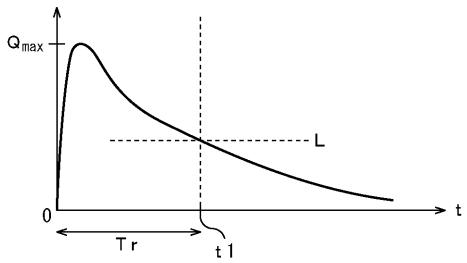
図2



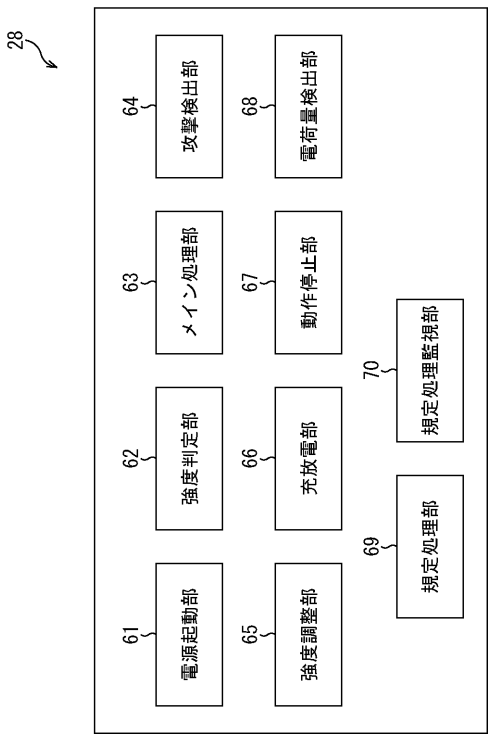
【図３】
図3



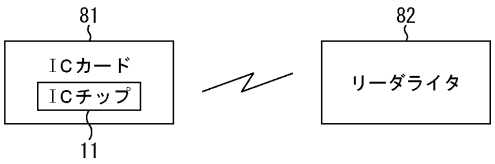
【図４】
図4



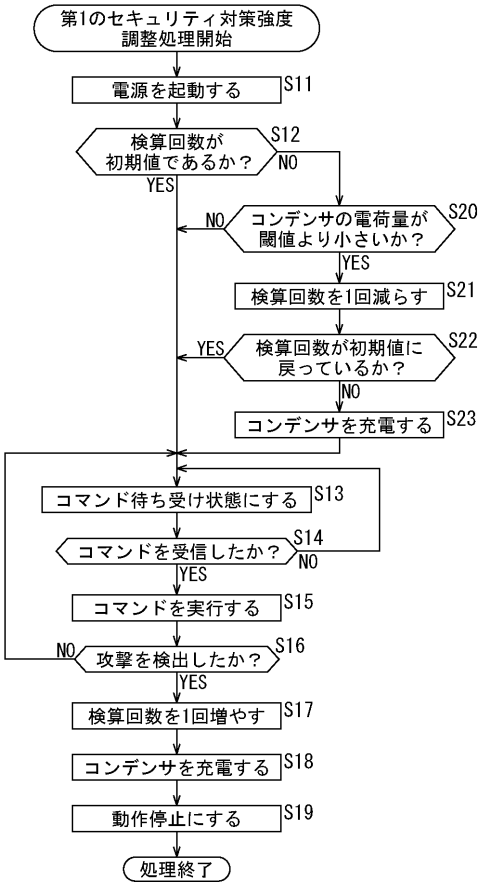
【図５】
図5



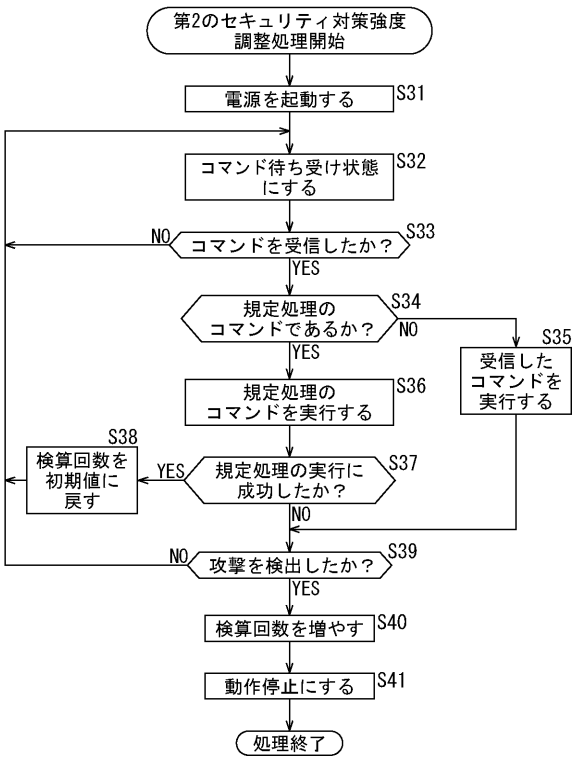
【図６】
図6



【図７】
図7



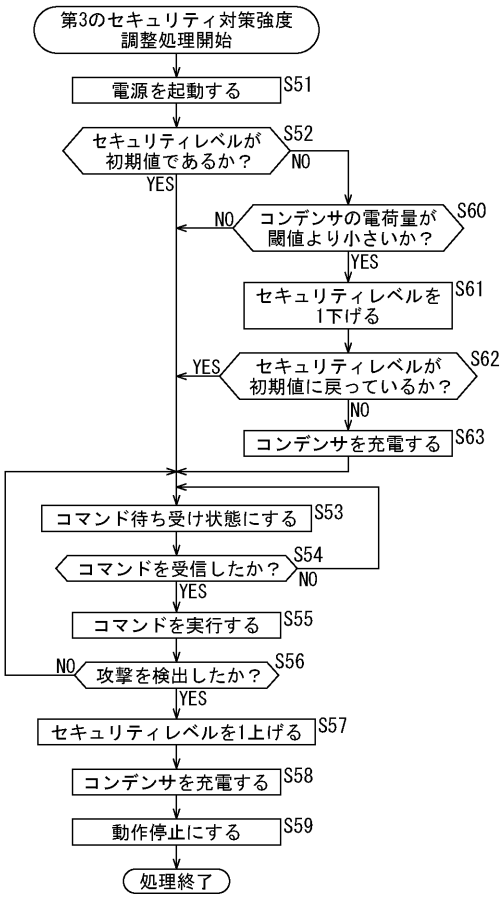
【図８】
図8



【図９】
図9

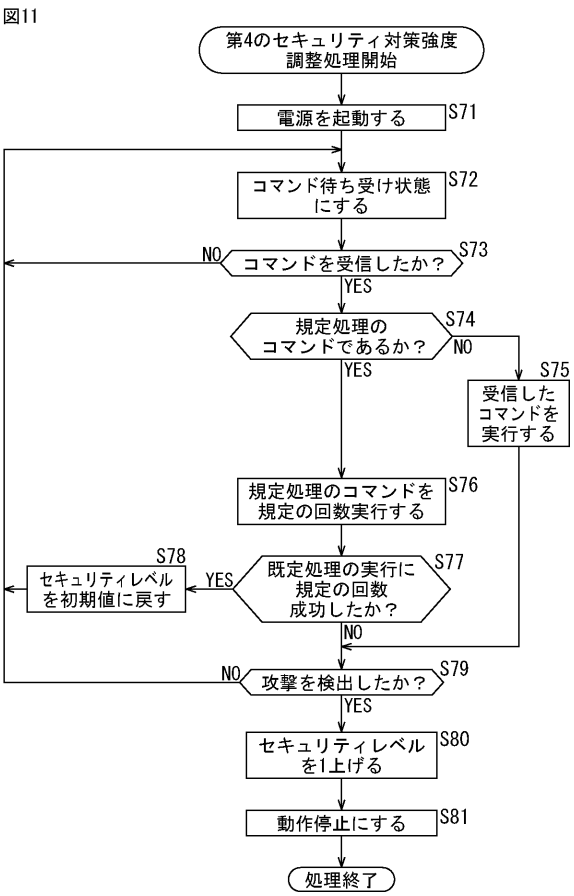
		セキュリティレベル1	セキュリティレベル2	セキュリティレベル3
セキュリティ対策の種類	重要処理の検算	1回	2回	3回
	タイミングジッタの挿入	10%	20%	30%
	ダミー演算	無	無	有
	セキュリティ対策の強度を下げるまでの時間	10分	30分	60分
	規定処理の成功回数	1回	2回	3回

【図１０】
図10



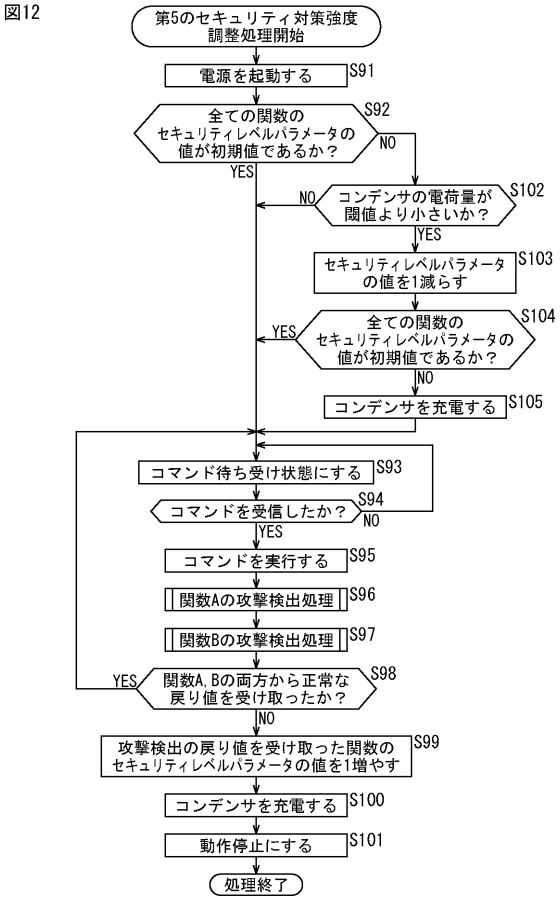
【図１１】

図11



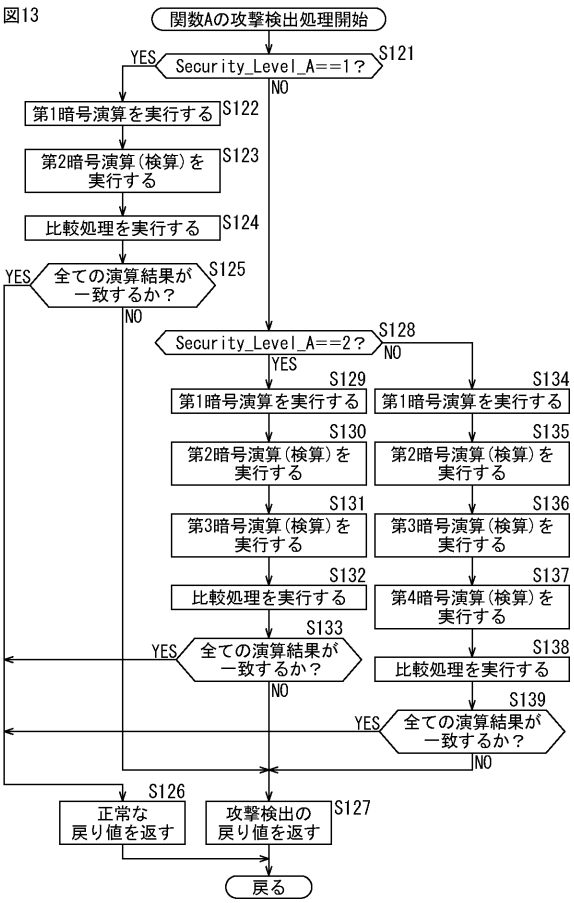
【図１２】

図12



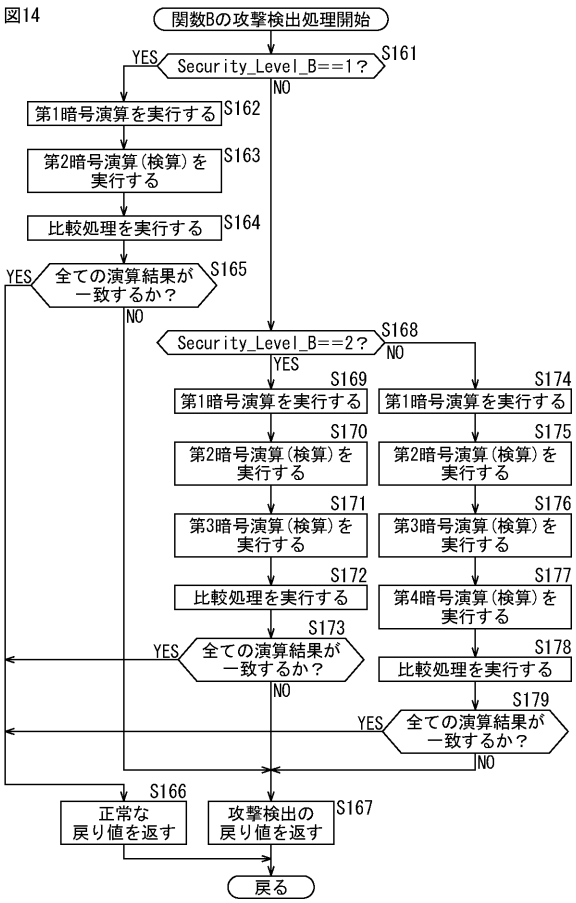
【図１３】

図13

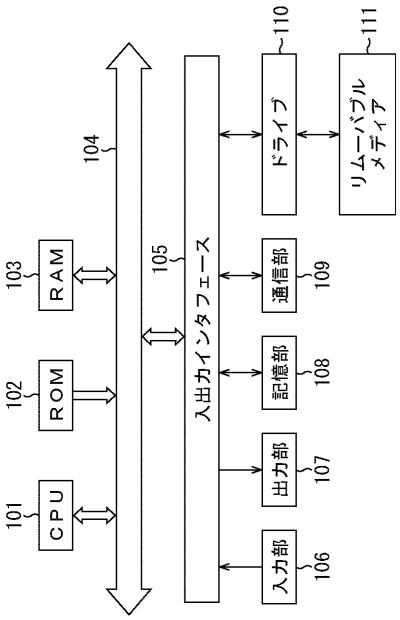


【図１４】

図14



【図１５】
図15


CPU
101
ROM
102
RAM
103
104
105
入出カインタフェース
入力部
106
出力部
107
記憶部
108
通信部
109
ドライブ
110
リムーバブル
メディア
111

フロントページの続き

(56)参考文献 特開平１０－１５４９７６（ＪＰ，Ａ）
国際公開第２００９／１１９０４９（WO，Ａ１）
特開２００９－２８９０１７（ＪＰ，Ａ）
特開２００３－０８５１３９（ＪＰ，Ａ）
特表２０１０－５１５１８７（ＪＰ，Ａ）
特表２００５－５２２９１２（ＪＰ，Ａ）
米国特許第０７５９０８８０（ＵＳ，Ｂ１）
米国特許出願公開第２００８／０１０２７９７（ＵＳ，Ａ１）
特開２００４－３４３８５５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／７５
Ｇ０６Ｆ　２１／８６
Ｇ０６Ｋ　１９／０７３