

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2006-31416

(P2006-31416A)

(43) 公開日 平成18年2月2日(2006.2.2)

(51) Int.Cl.

G06F 21/20 (2006.01)

F I

G06F 15/00 330B

テーマコード (参考)

5B085

審査請求 未請求 請求項の数 6 O L (全 20 頁)

(21) 出願番号 特願2004-209480 (P2004-209480)
 (22) 出願日 平成16年7月16日 (2004.7.16)

(71) 出願人 000002897
 大日本印刷株式会社
 東京都新宿区市谷加賀町一丁目1番1号
 (74) 代理人 100091476
 弁理士 志村 浩
 (72) 発明者 深谷 宗志
 東京都新宿区市谷加賀町一丁目1番1号
 大日本印刷株式会社内
 (72) 発明者 入澤 和義
 東京都新宿区市谷加賀町一丁目1番1号
 大日本印刷株式会社内
 (72) 発明者 金子 太一
 東京都新宿区市谷加賀町一丁目1番1号
 大日本印刷株式会社内

最終頁に続く

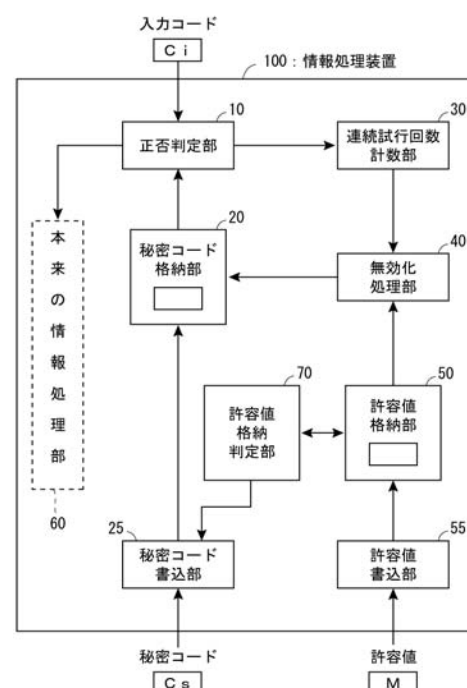
(54) 【発明の名称】 認証機能を備えた情報処理装置およびその発行方法

(57) 【要約】

【課題】 連続試行回数の許容値の書込処理に失敗しても、十分なセキュリティを確保する。

【解決手段】 秘密コード格納部20内の秘密コードCsと外部から入力された入力コードCiとが一致しているか否かを、正否判定部10によって判定して認証を行う。認証が失敗した連続試行回数は連続試行回数計数部30で計数され、計数値が許容値格納部50内の許容値Mを越えると、無効化処理部40による無効化が行われる。秘密コードCsおよび許容値Mは、情報処理装置100の発行時に、秘密コード書込部25および許容値書込部55に所定の指示を与えることにより書き込まれる。秘密コード書込部25は、許容値格納判定部70によって、許容値Mが書込済である判定がなされることを条件として、秘密コードCsの書き込みを実行するので、許容値Mの書込処理が失敗した場合、秘密コードCsの書込処理も中止される。

【選択図】 図3



【特許請求の範囲】

【請求項 1】

所定の秘密コードを格納するための秘密コード格納部と、
外部から所定の入力コードを伴うアクセスがあったときに、前記秘密コードを用いて前記入力コードの正否を判定する正否判定部と、

前記正否判定部により連続して否定的判定が行われた回数を計数する連続試行回数計数部と、

連続試行回数の許容値を格納するための許容値格納部と、

前記連続試行回数計数部の計数値が前記許容値を越えた場合に、前記秘密コードを無効化する無効化処理部と、

外部からの指示に基づいて、前記秘密コード格納部に所定の秘密コードを書き込む処理を行う秘密コード書込部と、

外部からの指示に基づいて、前記許容値格納部に所定の許容値を書き込む処理を行う許容値書込部と、

を備える情報処理装置において、

前記許容値格納部に許容値が格納されているか否かを判定する許容値格納判定部を更に設け、この許容値格納判定部により許容値が格納されていると判定された場合にのみ、秘密コード書込部による秘密コードの書込処理が実行されるようにしたことを特徴とする認証機能を備えた情報処理装置。

10

【請求項 2】

請求項 1 に記載の情報処理装置において、

許容値格納判定部が、許容値がとるべき有効範囲を予め記憶しており、許容値格納部に記憶されているデータが前記有効範囲内のデータであった場合に、許容値が格納されている旨の判定を行うことを特徴とする認証機能を備えた情報処理装置。

20

【請求項 3】

請求項 1 に記載の情報処理装置において、

第 1 の論理状態と第 2 の論理状態とのいずれか一方を示す機能を有し、当初は前記第 1 の論理状態を示しているフラグ領域を備え、

許容値書込部が、許容値を書き込む処理を行ったときに、前記フラグ領域を前記第 2 の論理状態に変更する機能を有し、

許容値格納判定部が、前記フラグ領域が前記第 2 の論理状態を示している場合に、許容値が格納されている旨の判定を行うことを特徴とする認証機能を備えた情報処理装置。

30

【請求項 4】

請求項 1 ～ 3 のいずれかに記載の情報処理装置において、

正否判定部が、外部から与えられた入力コードと、秘密コード格納部に格納されている秘密コードとを照合し、両者が一致した場合に、前記入力コードが正しい旨の判定を行うことを特徴とする認証機能を備えた情報処理装置。

【請求項 5】

請求項 1 ～ 3 のいずれかに記載の情報処理装置において、

正否判定部が、外部から与えられた入力コードと秘密コード格納部に格納されている秘密コードとについて、一方のコードに基づいて所定の演算を実行した結果が他方のコードに一致した場合に、もしくは、両方のコードに基づいてそれぞれ所定の演算を実行した結果が一致した場合に、前記入力コードが正しい旨の判定を行うことを特徴とする認証機能を備えた情報処理装置。

40

【請求項 6】

所定の秘密コードを格納するための秘密コード格納部と、

外部から所定の入力コードを伴うアクセスがあったときに、前記秘密コードを用いて前記入力コードの正否を判定する正否判定部と、

前記正否判定部により連続して否定的判定が行われた回数を計数する連続試行回数計数部と、

50

連続試行回数の許容値を格納するための許容値格納部と、
前記連続試行回数計数部の計数値が前記許容値を越えた場合に、前記秘密コードを無効化する無効化処理部と、
外部からの指示に基づいて、前記秘密コード格納部に所定の秘密コードを書き込む処理を行う秘密コード書込部と、
外部からの指示に基づいて、前記許容値格納部に所定の許容値を書き込む処理を行う許容値書込部と、
を備える情報処理装置について、所望の秘密コードおよび所望の許容値を書き込むことにより、当該情報処理装置を特定のユーザのために発行する発行方法において、
前記情報処理装置を準備する処理装置準備段階と、
前記許容値書込部に指示を与えることにより、前記許容値格納部にデフォルト許容値を書き込む処理を行う発行準備段階と、
前記発行準備段階を実行した後に、前記秘密コード書込部に指示を与えることにより、前記秘密コード格納部に前記所望の秘密コードを書き込む処理と、前記許容値書込部に指示を与えることにより、前記許容値格納部に前記所望の許容値を書き込む処理と、を行う発行処理段階と、
を有することを特徴とする認証機能を備えた情報処理装置の発行方法。

10

【発明の詳細な説明】

【技術分野】

【0001】

20

本発明は、認証機能を備えた情報処理装置およびその発行方法に関し、特に、認証処理の連続試行回数を制限することによりセキュリティを高める方式をとる情報処理装置およびその発行方法に関する。

【背景技術】

【0002】

情報処理装置に関するセキュリティ対策として、外部からアクセスがあった場合に、当該アクセスが正当な権限をもったアクセスであることを確認する認証処理は非常に重要である。特に、ＩＣカードをはじめとする携帯型情報処理装置の場合、紛失や盗難というリスクが高いため、外部からアクセスを行う際の認証処理機能は不可欠である。このような認証処理を行うためには、通常、装置内部に予め所定の秘密コードを書き込んでおく手法が採られる。たとえば、秘密コードとして、正規のユーザのみが知りうるパスワードを書き込んでおき、アクセス時には、当該パスワードの入力を要求し、パスワードが一致することを確認することにすれば、正規のユーザからのアクセスであることを認証することができる。あるいは、秘密コードとして、正規のユーザのみが保有する暗号化鍵を書き込んでおき、当該暗号化鍵を用いて外部で暗号化された所定のデータを、装置内部で復号化して、元のデータに一致することを確認する手法が採られる場合もある。たとえば、下記の特許文献１には、このような暗号化の手法を用いたＩＣカードについての認証方法が開示されている。

30

【0003】

また、上述のような認証処理におけるセキュリティを更に向上させるために、通常は、認証処理の連続試行回数を制限する手法が付加される。これは、試行錯誤を繰り返す不正なアクセスにより、偶然、パスワードなどが一致してしまう危険性を低減させる上で有用である。具体的には、パスワード不一致などによる認証失敗の回数を計数するようにし、連続して認証に失敗した回数が所定の許容値を越えた場合には、認証用の秘密コードを無効化してしまう処理を行えばよい。たとえば、許容値を５回に設定した場合、５回までは誤ったパスワードを入力することができるが、６回目に誤ったパスワードを入力すると、当該パスワード認証に用いられる秘密コードが無効化されてしまい、もはや通常の方法でのアクセスはすべて拒絶されることになる。このような措置を講じておけば、不正アクセスが成功する確率を著しく低減させることができる。また、下記の特許文献２には、単位時間あたりのパスワード入力回数を制限する手法が開示されている。

40

50

【特許文献 1】特開平 5－290225 号公報

【特許文献 2】特開平 9－212458 号公報

【発明の開示】

【発明が解決しようとする課題】

【0004】

近年、ＩＣカードをはじめとする携帯型情報処理装置の需要が高まってきており、クレジットカードや携帯電話など、その用途も様々である。したがって、このような情報処理装置に要求される認証機能も多様化してきており、パスワードなどの秘密コードの構成や連続試行回数の許容値なども、用途に応じて様々な設定がなされている。たとえば、同じクレジットカード用ＩＣカードであっても、発行元の信販会社によって、パスワードの構成（数字のみか、文字も含むか、あるいは、総桁数をいくつにするかなど）や、連続試行回数の許容値は、それぞれ異なる。 10

【0005】

このような事情から、たとえば、ＩＣカードの場合、基本機能を備えたＩＣカードを提供するＩＣカードの提供業者は、固有の秘密コードや連続試行回数の許容値などのデータが書き込まれていない状態のＩＣカードを、信販会社などのサービス提供業者に納入し、サービス提供業者が個々のユーザに対してＩＣカードを発行する段階で、所望の構成をもった秘密コードおよび所望の許容値を書き込む処理を行っているのが実情である。

【0006】

もちろん、このＩＣカードの発行処理を行う段階で、秘密コードおよび許容値を正しく書き込む処理が行われれば問題はないが、何らかのトラブルで、許容値が正しく書き込まれていないと、連続試行回数を制限する機能が正しく動作せず、試行錯誤を繰り返す不正なアクセスによる攻撃に無防備な状態になってしまう。このような許容値の書込エラーは、様々な要因で起こりうるが、最近では、通信環境のトラブルに起因したエラーの発生が無視できなくなっている。これは、ＩＣカードなどの発行処理を、種々の通信網やネットワークを介して遠隔地から行う事例が増えると思われるからである。たとえば、携帯電話に装着するタイプのＩＣカードの場合、携帯電話の通信機能を利用して外部と通信することができるので、信販会社のサーバにオンライン接続した状態で、クレジットカードとしての発行処理を受けることも可能である。この場合、秘密コードや許容値の書込処理も、オンラインで行われることになるので、通信トラブルの発生により、許容値の書き込みが正しく行われない事態も十分に予想できる。 20 30

【0007】

ここで、秘密コードの書込処理は成功し、許容値の書込処理に失敗したような事態を考えると、正規の方法による認証処理は実行可能であるので、あたかもＩＣカードの発行プロセスは何ら異常なく終了したように見え、当該ＩＣカードが実用に供されてしまう可能性がある。しかしながら、このようなＩＣカードは、上述したとおり、試行錯誤を繰り返す不正なアクセスによる攻撃に無防備な状態であり、セキュリティの点において重大な脆弱性を抱えていることになる。

【0008】

そこで本発明は、連続試行回数の許容値の書込処理に異常が生じてても、十分なセキュリティを確保することが可能な認証機能を備えた情報処理装置を提供することを目的とし、また、そのような情報処理装置の発行方法を提供することを目的とする。 40

【課題を解決するための手段】

【0009】

(1) 本発明の第 1 の態様は、
所定の秘密コードを格納するための秘密コード格納部と、
外部から所定の入力コードを伴うアクセスがあったときに、秘密コードを用いて入力コードの正否を判定する正否判定部と、
この正否判定部により連続して否定的判定が行われた回数を計数する連続試行回数計数部と、

連続試行回数の許容値を格納するための許容値格納部と、
連続試行回数計数部の計数値が許容値を越えた場合に、秘密コードを無効化する無効化処理部と、

外部からの指示に基づいて、秘密コード格納部に所定の秘密コードを書き込む処理を行う秘密コード書込部と、

外部からの指示に基づいて、許容値格納部に所定の許容値を書き込む処理を行う許容値書込部と、

を備える情報処理装置において、

許容値格納部に許容値が格納されているか否かを判定する許容値格納判定部を更に設け、この許容値格納判定部により許容値が格納されていると判定された場合にのみ、秘密コード書込部による秘密コードの書込処理が実行されるようにしたものである。 10

【0010】

(2) 本発明の第2の態様は、上述の第1の態様に係る認証機能を備えた情報処理装置において、

許容値格納判定部が、許容値がとるべき有効範囲を予め記憶しており、許容値格納部に記憶されているデータが有効範囲内のデータであった場合に、許容値が格納されている旨の判定を行うようにしたものである。

【0011】

(3) 本発明の第3の態様は、上述の第1の態様に係る認証機能を備えた情報処理装置において、 20

第1の論理状態と第2の論理状態とのいずれか一方を示す機能を有し、当初は第1の論理状態を示しているフラグ領域を用意し、

許容値書込部に、許容値を書き込む処理を行ったときに、フラグ領域を第2の論理状態に変更する機能をもたせ、

許容値格納判定部が、フラグ領域が第2の論理状態を示している場合に、許容値が格納されている旨の判定を行うようにしたものである。

【0012】

(4) 本発明の第4の態様は、上述の第1～3の態様に係る認証機能を備えた情報処理装置において、

正否判定部が、外部から与えられた入力コードと、秘密コード格納部に格納されている秘密コードとを照合し、両者が一致した場合に、入力コードが正しい旨の判定を行うようにしたものである。 30

【0013】

(5) 本発明の第5の態様は、上述の第1～3の態様に係る認証機能を備えた情報処理装置において、

正否判定部が、外部から与えられた入力コードと秘密コード格納部に格納されている秘密コードとについて、一方のコードに基づいて所定の演算を実行した結果が他方のコードに一致した場合に、もしくは、両方のコードに基づいてそれぞれ所定の演算を実行した結果が一致した場合に、入力コードが正しい旨の判定を行うようにしたものである。

【0014】

(6) 本発明の第6の態様は、 40

所定の秘密コードを格納するための秘密コード格納部と、

外部から所定の入力コードを伴うアクセスがあったときに、秘密コードを用いて入力コードの正否を判定する正否判定部と、

正否判定部により連続して否定的判定が行われた回数を計数する連続試行回数計数部と、

連続試行回数の許容値を格納するための許容値格納部と、

連続試行回数計数部の計数値が許容値を越えた場合に、秘密コードを無効化する無効化処理部と、

外部からの指示に基づいて、秘密コード格納部に所定の秘密コードを書き込む処理を行 50

う秘密コード書込部と、

外部からの指示に基づいて、許容値格納部に所定の許容値を書き込む処理を行う許容値書込部と、

を備える情報処理装置について、所望の秘密コードおよび所望の許容値を書き込むことにより、当該情報処理装置を特定のユーザのために発行する発行方法において、

上述した構成をもった情報処理装置を準備する処理装置準備段階と、

許容値書込部に指示を与えることにより、許容値格納部にデフォルト許容値を書き込む処理を行う発行準備段階と、

発行準備段階を実行した後に、秘密コード書込部に指示を与えることにより、秘密コード格納部に所望の秘密コードを書き込む処理と、許容値書込部に指示を与えることにより、許容値格納部に所望の許容値を書き込む処理と、を行う発行処理段階と、
を行うようにしたものである。

10

【発明の効果】

【0015】

本発明に係る認証機能を備えた情報処理装置によれば、許容値格納判定部によって、連続試行回数の許容値の書き込みが正しく行われているか否かを判定し、正しく書き込まれている場合にのみ、秘密コードの書込処理を実行するようにしたため、許容値の書込処理に異常が生じた場合には、秘密コードの書き込みも実行されないことになる。したがって、許容値の書込処理に異常が生じた場合には、当該情報処理装置がそのまま実用に供されることはなく、この点に関する十分なセキュリティ確保が可能になる。

20

【0016】

また、本発明に係る情報処理装置の発行方法によれば、まず、発行準備段階において、連続試行回数に関するデフォルト許容値が書き込まれ、その後の発行処理段階において、所望の秘密コードを書き込む処理と、所望の許容値を書き込む処理（デフォルト許容値を書き換える処理）とが行われるので、万一、所望の許容値を書き込む処理が正しく行われなかったとしても、デフォルト許容値をもった情報処理装置として機能するので、セキュリティ上、重大な支障は生じない。

【発明を実施するための最良の形態】

【0017】

以下、本発明を図示する実施形態に基づいて説明する。

30

【0018】

<<< § 1. 一般的な認証機能を備えた情報処理装置 >>>

図1は、従来から一般的に利用されている認証機能を備えた情報処理装置100の基本構成を示すブロック図である。図示のとおり、この情報処理装置100には、正否判定部10、秘密コード格納部20、連続試行回数計数部30、無効化処理部40、許容値格納部50なる構成要素が組み込まれている。これらの各構成要素は、いずれも外部からのアクセスがあった場合に、当該アクセスが正規のアクセスであることを認証する処理を実行するための要素である。

【0019】

なお、図に破線で示す本来の情報処理部60は、この情報処理装置100が行うべき本来の情報処理を実行する部分を示しており、その具体的な内容は、情報処理装置100の種類や用途に応じて様々である。たとえば、情報処理装置100が、クレジットカードとしての機能をもったICカードである場合には、本来の情報処理部60は、クレジットカード会員としての会員情報や決済情報を記憶する機能をもち、クレジットカードによる決済を行う際には、決済に必要な種々の処理を実行する機能を有する。したがって、この本来の情報処理部60の部分は、情報処理装置100の主たる構成部分というべきものであるが、本発明は、情報処理装置100の認証機能に関する技術であるので、本来の情報処理部60自身についての詳細な説明は省略する。

40

【0020】

正否判定部10は、情報処理装置100における認証処理を行うための最も重要な構成

50

要素であり、外部から所定の入力コード C i を伴うアクセスがあったときに、この入力コード C i の正否を判定する機能を有する。この正否判定部 10 における判定結果は、本来の情報処理部 60 へと伝えられる。本来の情報処理部 60 は、正否判定部 10 により肯定的判定が行われた場合には、当該アクセスに応じて正規の処理を実行するが、正否判定部 10 により否定的判定が行われた場合には、当該アクセスを拒絶する。

【0021】

正否判定部 10 における正否判定は、秘密コード格納部 20 内に格納されている秘密コード C s を利用して行われる。最も単純な正否判定の方法は、外部から与えられた入力コード C i と、秘密コード格納部 20 に格納されている秘密コード C s とを照合し、両者が一致した場合に、当該入力コード C i が正しい旨の判定を行う方法である。この場合、秘密コード格納部 20 に格納されている秘密コード C s は、正規のユーザのみが知りうるパスワードとして機能することになり、アクセス時に、この秘密コード C s と同一のパスワードを入力コード C i として入力することにより、認証は成功する。すなわち、正否判定部 10 は、外部から入力された入力コード C i が秘密コード C s と一致した場合に、肯定的判定を行うことになる。

10

【0022】

もっとも、秘密コード C s を利用した正否判定は、入力コード C i との一致を判定する方法に限定されるわけではない。別な方法としては、外部から与えられた入力コード C i と秘密コード格納部 20 に格納されている秘密コード C s とについて、一方のコードに基づいて所定の演算を実行した結果が他方のコードに一致した場合に、入力コード C i が正しい旨の判定を行うこともできる。たとえば、所定のアルゴリズムに基づく暗号化処理に用いる暗号化鍵を秘密コード C s として、秘密コード格納部 20 内に用意しておいた場合を考える。ここで、外部において、たとえば、この情報処理装置 100 に付与されたシリアル番号に対して、上記暗号化鍵（秘密コード C s ）を用いた所定のアルゴリズムによる暗号化処理を施して暗号化し、暗号化したシリアル番号を入力コード C i として入力したとする。この場合、正否判定部 10 は、情報処理装置 100 の内部に記憶されているシリアル番号に対して、秘密コード格納部 20 内に格納されている秘密コード C s を暗号化鍵として上述と同一のアルゴリズムによる暗号化処理を施して暗号化する処理を行い、その結果が入力コード C i と一致した場合に肯定的な判定を行えばよい。もちろん、暗号化の対象は、情報処理装置 100 のシリアル番号に限定されるものではなく、たとえば、情報処理装置 100 のユーザ名や日時の情報などを用いてもかまわない。また、外部から与えられた入力コード C i と秘密コード格納部 20 に格納されている秘密コード C s との両方に基づいてそれぞれ所定の演算を実行し、両演算結果が一致した場合に、入力コード C i が正しい旨の判定を行うこともできる。

20

30

【0023】

この他にも、秘密コード C s を利用した正否判定方法は種々存在するが、正否判定部 10 が行う具体的な正否判定方法それ自身は本発明の主題ではないので、ここではこれ以上詳しい説明は省略する。

【0024】

このように、正否判定部 10 が、秘密コード C s を利用した正否判定を行う以上、試行錯誤を繰り返す不正なアクセスにより、偶然、肯定的判定がなされてしまう可能性は排除できない。そこで、既に述べたとおり、通常は、認証処理の連続試行回数を制限する対策がとられる。図示の連続試行回数計数部 30、無効化処理部 40、許容値格納部 50 は、このような対策を施すための構成要素である。

40

【0025】

すなわち、連続試行回数計数部 30 は、正否判定部 10 により連続して否定的判定が行われた回数を計数する機能をもった構成要素であり、許容値格納部 50 は、連続試行回数の許容値 M を格納するための構成要素であり、無効化処理部 40 は、連続試行回数計数部 30 の計数値が許容値 M を越えた場合に、秘密コード C s を無効化するための構成要素である。

50

【0026】

正否判定部10は、外部から入力コードCiを伴うアクセスがあると、前述した手法により、当該入力コードCiの正否判定を行い、その結果を連続試行回数計数部30へと伝達する。連続試行回数計数部30は、肯定的判定が伝達された場合には、これまでの計数値を0にクリアするが、否定的判定が伝達された場合には、これまでの計数値を1だけ増加させる処理を行う。その結果、正否判定部10により連続して否定的判定が行われると、その合計回数が連続試行回数計数部30によって計数されることになる。

【0027】

無効化処理部40は、この連続試行回数計数部30による計数値が許容値格納部50に格納されている許容値Mを越えた場合に、秘密コード格納部20内の秘密コードCsを無効化する処理を行う。たとえば、許容値格納部50内に格納されている許容値Mが5であった場合、正否判定部10が連続して6回、否定的判定を行った時点で、無効化処理部40による無効化が行われることになり、以後は、通常の方法でのアクセスはすべて拒絶されることになる。具体的な無効化の方法は、秘密コードCsの値を予め定められた「無効を示す値」に書き換える方法をとってもよいし、無効であることを示すフラグを立て、正否判定部10に当該秘密コードCsが無効であることを示すようにしてもよい。

【0028】

このような各構成要素の連携作用により、試行錯誤を繰り返す不正なアクセスに対する防護力を高めることが可能になる。たとえば上述の例の場合、6回までの試行錯誤によって、偶然、肯定的判定が得られてしまう可能性はあるものの、それ以後の試行は無効化により阻止されることになる。

【0029】

<<< §2. 発行処理時の書込機能を備えた情報処理装置 >>>

図1では、秘密コード格納部20内に所定の秘密コードCsが既に設定されており、許容値格納部50内に所定の許容値Mが既に設定されている例を示した。しかしながら、前述したとおり、これらの各設定内容は、情報処理装置100の用途に応じて様々であり、実際には、情報処理装置100を特定のユーザ向けに発行する段階で書き込むケースが多い。一般的には、情報処理装置100の発行時には、本来の情報処理部60内に特定のユーザ向けの個人情報などを書き込む処理が行われ、同時に、秘密コードCsや許容値Mを書き込む処理が行われる。

【0030】

図2は、図1に示す情報処理装置100に、更に、秘密コード書込部25および許容値書込部55を付加した構成例を示すブロック図である。ここで、秘密コード書込部25は、外部からの指示に基づいて、秘密コード格納部20に所定の秘密コードCsを書き込む処理を行う構成要素であり、同様に、許容値書込部55は、外部からの指示に基づいて、許容値格納部50に所定の許容値Mを書き込む処理を行う構成要素である。なお、本来の情報処理部60内にも、同様に、発行時に必要な情報を書き込む構成要素が含まれているが、ここでは説明は省略する。

【0031】

このような発行処理時の書込機能を備えた情報処理装置100を利用すれば、当該情報処理装置100を用いて種々のサービスを提供する業者が、当該情報処理装置100を個々のユーザ向けに発行する際に、それぞれ所望の秘密コードCsおよび所望の許容値Mを書き込むことが可能になる。しかしながら、この発行時のプロセスにおいて、秘密コードの書込処理は成功したのに、許容値の書込処理に失敗した場合、試行錯誤を繰り返す不正なアクセスによる攻撃に無防備な状態となり、セキュリティの点において重大な問題が生じることは既に述べたとおりである。

【0032】

たとえば、図示の例の場合、秘密コード格納部20内に秘密コードCsが書き込まれていれば、正否判定部10は、正常にその機能を果たすことができ、認証機能それ自身には何ら支障は生じない。したがって、この観点からは、発行プロセスは何ら異常なく終了し

10

20

30

40

50

たように見える。しかしながら、許容値格納部 50 内に許容値 M が書き込まれていない状態であると、不正アクセスがあった場合でも、無効化処理部 40 による無効化機能は正常に動作しない可能性が高い。たとえば、許容値格納部 50 として、EEPROM などの不揮発性メモリを用いており、その初期値が 16 進数での「FF」であったような場合、許容値 M の書き込みに失敗すると、許容値格納部 50 内は初期値の「FF」となっているため、無効化処理部 40 による無効化処理が実行されるのは、連続試行回数計数部 30 の計数値が 256 に達した時点ということになる。これは、試行錯誤による 256 通りもの不正アクセスを許す結果となり、セキュリティ上、重大な問題である。

【0033】

本願発明者は、許容値 M の書き込みに失敗するケースが、今後は増える傾向にあるであろうと予測している。その理由は、先にも述べたとおり、情報処理装置 100 の発行処理をオンラインで行うケースが益々増加するであろうと思われるからである。実際、携帯電話に装着するタイプの IC カードの場合、携帯電話の通信機能を利用して外部と通信し、データやプログラムをダウンロードする機能が既に備わっている。したがって、今後は、携帯電話装着型の IC カードなどからなる情報処理装置 100 を、特定の信販会社用のクレジットカードとして利用できるようにするために、当該信販会社のサーバと情報処理装置 100 とをオンライン接続し、その状態でクレジットカードの発行処理を行うような形態が一般化すると考えられる。このようなケースでは、発行処理プロセスにおける通信環境のトラブルにより、許容値 M の書込処理が失敗する可能性も十分にありうる。

【0034】

本発明は、このように、連続試行回数の許容値の書込処理に異常が生じて、十分なセキュリティを確保することを可能にする新たな技術を提案するものである。この技術は、大別して 2 つのアプローチにより構成される。第 1 のアプローチは、情報処理装置 100 内に付加的な構成要素を追加し、当該付加的構成要素の機能により課題を解決するものであり、その実施形態を § 3 で述べることにする。一方、第 2 のアプローチは、情報処理装置 100 の発行処理を工夫することにより同じ課題を解決するものであり、その実施形態を § 4 で述べることにする。

【0035】

<<< § 3. 本発明の第 1 のアプローチに基づく実施形態 >>>

図 3 は、本発明の第 1 のアプローチに基づく実施形態に係る情報処理装置 100 の基本構成を示すブロック図である。図 2 に示す従来装置との相違は、新たな構成要素として許容値格納判定部 70 が付加されている点と、秘密コード書込部 25 が、この許容値格納判定部 70 の判定結果に依存して書込処理の実行を行う点である。すなわち、許容値格納判定部 70 は、許容値格納部 50 に許容値が格納されているか否かを判定する機能を有し、秘密コード書込部 25 は、許容値格納判定部 70 により許容値が格納されていると判定された場合にのみ、秘密コードの書込処理を実行するように構成されている。

【0036】

したがって、この情報処理装置 100 に対して、所望の秘密コード Cs を書き込む処理を行う際には、その前に、所望の許容値 M を書き込む処理を実行しておく必要がある。許容値 M についての書込処理を行う前に、秘密コード Cs についての書込処理を行ったとしても、許容値格納判定部 70 により、許容値格納部 50 内にはまだ許容値が格納されていない旨の判定がなされ、秘密コード書込部 25 は、秘密コード Cs についての書込指示を拒絶することになる。

【0037】

結局、図 3 に示す情報処理装置 100 では、特定のユーザ向けに発行する発行処理プロセスに関しては、「必ず許容値 M を先に書き込み、その後で秘密コード Cs を書き込む」という書込順序についての制約は生じるものの、それ以外の点では、特に不都合は生じない。しかも、この図 3 に示す情報処理装置 100 によれば、許容値の書込処理に異常が生じて、十分なセキュリティが確保される、というメリットが得られる。たとえば、オンライン接続を介して、許容値 M および秘密コード Cs の書込処理（情報処理装置 100 の発

行処理)を実行中に通信エラーが生じ、許容値Mの書き込みに失敗したとすると、その後に行われる秘密コードCsの書込処理は、許容値格納判定部70の否定的な判定結果に基づいて、秘密コード書込部25により拒絶されることになる。結果的に、当該情報処理装置100に対する発行処理自体が失敗に終わることになるので、少なくとも許容値が書き込まれていない状態の情報処理装置100が、実用に供されることはなくなる。

【0038】

もちろん、通常は、このように発行処理自体が失敗に終わった場合、再度の発行処理が実行されることになる。この再度の発行処理において、許容値Mが正しく書き込まれれば、今度は許容値格納判定部70による肯定的な判定結果に基づいて、秘密コード書込部25による秘密コードCsの書き込みが行われることになる。

10

【0039】

以上、本発明の第1のアプローチに基づく実施形態の基本概念を説明したが、続いて、許容値格納判定部70の行う具体的な判定方法を、2つの実例に即して説明する。図4は、第1の実例を示すためのブロック図であり、図5は第2の実例を示すためのブロック図である。

【0040】

上述したように、許容値格納判定部70は、許容値格納部50に許容値が格納されているか否かを判定する構成要素であるが、実際には、許容値格納部50は、EEPROMなどのメモリの1領域からなる構成要素であり、そこには何らかのデータが書き込まれていることになる。たとえば、許容値格納部50を1バイト分のメモリ領域によって構成した場合を考える。この場合、当該メモリ領域は、16進数の「00」～「FF」までのいずれか1つの数値を示すことになる。これは、許容値書込部55による書込処理が行われているがいまいが同じである。もし、このメモリ領域の初期値が16進数の「FF」であった場合、許容値書込部55による書込処理が行われていない場合であっても、許容値格納部50には「FF」なるデータが格納されていることになる。

20

【0041】

このように、許容値格納部50内には、いつの時点であっても、常に何らかのデータが格納された状態になっているので、許容値格納判定部70は、何らかの基準に基づいて、許容値格納判定部70に格納されているデータが許容値を示すデータであるのか否かを判定する必要がある。

30

【0042】

図4に示す実例は、この基準として、許容値がとるべき有効範囲を定めた例である。図示の例では、許容値格納判定部70内に有効範囲設定部71が設けられており、ここに、「1～10」なる有効範囲が設定されている。このように、許容値格納判定部70に、許容値がとるべき有効範囲を予め記憶させておけば、許容値格納部50に記憶されているデータがこの有効範囲内のデータであった場合に、許容値が格納されている旨の判定を行うことができる。図示の例の場合、許容値格納部50に格納されているデータが、有効範囲1～10の範囲内の値であった場合に、許容値格納判定部70は、肯定的判定を下すことになる。

【0043】

40

許容値格納部50に格納すべき許容値は、誤った入力コードCiを連続して入力可能な回数の最大値を示すものであり、一般的には、せいぜい1～10程度の値に設定すべき値である。このように、有効範囲設定部71には、許容値がとるべき有効範囲としてある程度妥当と判断可能な範囲を設定しておけばよい。そうすれば、もし、許容値の書込処理に失敗して、許容値格納部50内のデータが初期値「FF」を示していた場合は、許容値格納判定部70によって否定的な判定がなされ、秘密コード書込部25による秘密コードCsの書込処理は拒絶されることになる。

【0044】

なお、許容値の書込処理に失敗したものの、許容値格納部50内のデータが有効範囲設定部71に設定されている有効範囲内のものになってしまった場合は、許容値格納判定部

50

70は肯定的な判定を下すことになるが、この場合、そもそも許容値格納部50内のデータが有効範囲内に収まっているのであるから、許容値格納判定部70による肯定的な判定がなされたとしても大きな問題は生じない。たとえば、許容値Mとして「5」を書き込むように許容値書込部55に対して指示を与えたのにもかかわらず、書込処理に失敗して、許容値Mとして「10」が書き込まれてしまった場合、許容値Mの書込処理自体は失敗したことになるが、許容値格納部50に書き込まれた許容値「10」は、許容値がとるべき有効範囲としてある程度妥当と判断可能な値であるので、許容値格納判定部70により肯定的な判定がなされ、秘密コードCsの書込処理が実行され、当該情報処理装置100が実用に供されたとしても、セキュリティ上の重大な支障には至らない。

【0045】

10

一方、図5に示す実例は、許容値書込部55による正常な書込処理が完了したことを、フラグとして記録に残すようにしたものである。すなわち、図示のフラグ領域72は、第1の論理状態と第2の論理状態とのいずれか一方を示す機能を有し、当初は第1の論理状態を示している記憶領域によって構成されており、許容値書込部55は、許容値を書き込む処理を行ったときに、このフラグ領域72を第2の論理状態に変更する機能を有する。この場合、許容値格納判定部70は、フラグ領域72が第2の論理状態を示している場合に、許容値が格納されている旨の判定を行えばよいことになる。

【0046】

たとえば、フラグ領域72として、初期状態では「1」を示している1ビットからなるメモリを用いたものとしよう。この場合、許容値書込部55は、許容値の書込処理を完了した時点で、当該ビットを「0」に書き換える処理を行うようにすればよい。許容値格納判定部70は、フラグ領域72のビットが「0」なら肯定的な判定を下し、「1」なら否定的な判定を下すことになる。

20

【0047】

<<< §4. 本発明の第2のアプローチに基づく実施形態 >>>

続いて、第2のアプローチに基づく実施形態を述べる。この実施形態は、情報処理装置100の発行処理を工夫することにより課題解決を図るものであり、用いる情報処理装置100としては、図2に示す従来の情報処理装置でかまわない（許容値格納判定部70を設ける必要はない）。

【0048】

30

図6は、この第2のアプローチに基づく実施形態に係る情報処理装置の発行方法の手順を示す流れ図である。図示のとおり、この発行方法は、処理装置準備段階（ステップS1）、発行準備段階（ステップS2）、発行処理段階（ステップS3）の3つの段階から構成されている。ステップS1の処理装置準備段階は、図2に示す情報処理装置100を準備する段階であり、この情報処理装置100の構成に関しては、既に§1および§2で述べたとおりである。

【0049】

続く、ステップS2の発行準備段階は、この情報処理装置100内の許容値格納部50にデフォルト許容値Dを書き込む段階である。具体的には、許容値書込部55に指示を与えることにより、所定のデフォルト許容値Dが許容値格納部50に書き込まれるようにすればよい。デフォルト許容値Dとしては、許容値がとるべき有効範囲としてある程度妥当と判断可能な値であれば、どのような値を設定してもかまわないが、一般的には、発行処理を行う多くの業者にとって標準的な許容値を、デフォルト許容値Dとして設定しておくのが好ましい。

40

【0050】

ステップS3の発行処理段階は、こうして用意された情報処理装置100について、所望の秘密コードおよび所望の許容値を書き込むことにより、当該情報処理装置100を特定のユーザのために発行するための処理であり、ステップS2の発行準備段階を実行した後に行われる。この発行処理段階では、秘密コード書込部25に指示を与えることにより、秘密コード格納部20に所望の秘密コードCsを書き込む処理と、許容値書込部55に

50

指示を与えることにより、許容値格納部 50 に所望の許容値 M を書き込む処理と、が実行される。両書込処理の順序は不問である。なお、許容値格納部 50 内には、既にステップ S 2 において、デフォルト許容値 D が書き込まれているので、ステップ S 3 で行われる所望の許容値 M を書き込む処理は、デフォルト許容値 D を所望の許容値 M に書き換える処理ということになる。

【0051】

このような手順で情報処理装置 100 の発行を行うようにすれば、ステップ S 3 において、所望の許容値 M を書き込む処理が失敗したとしても、許容値格納部 50 には、ステップ S 2 で書き込んだデフォルト許容値 D が格納されているので、セキュリティ上、重大な支障は生じない。

10

【0052】

なお、ここで留意すべき点は、ステップ S 2 の発行準備段階までは、情報処理装置 100 を提供する提供者において行うことができる、という点である。この点を、携帯電話装着型の IC カードを情報処理装置 100 として用いた例について、もう少し詳しく説明しよう。

【0053】

いま、IC カードの提供者 X が、携帯電話サービス提供者 Y から受注した携帯電話装着型の IC カード上に、Y 社と 3 つの信販会社 A, B, C からクレジット機能の追加を受注し、Y 社に納入するものとする。この場合、許容値格納部 50 に設定すべき許容値 M の値は、A 社、B 社、C 社でそれぞれ異なり、また、同じ A 社が発行するクレジットカードであっても、その種類によって、許容値 M の値にバリエーションをもたせる可能性もあるので、提供者 X が IC カードを各社に納品した時点では、許容値格納部 50 内に本来の許容値 M を書き込んでおくことはできない。また、秘密コード Cs は、通常、個々のユーザごとに異なるので、秘密コード格納部 20 内にも、秘密コード Cs を書き込んでおくことはできない。いずれも、各信販会社 A, B, C が、特定の顧客に向けて、各 IC カードを発行する処理（ステップ S 3 の処理）を行う時点で書き込むべき情報ということになる。

20

【0054】

ただ、この § 4 で述べる手法では、提供者 X が、各信販会社 A, B, C による発行処理（ステップ S 3）が実行される前の段階（ステップ S 2）で、各 IC カード内の許容値格納部 50 に、デフォルト許容値 D を書き込む処理を行うようにする。このデフォルト許容値 D は、A 社、B 社、C 社ごとに異ならせることも可能であるが、実用上は、各社共通の同一値でかまわない。たとえば、デフォルト許容値 D = 5 に設定した場合、すべての IC カードの許容値格納部 50 内に、デフォルト許容値 5 を書き込む処理が実行されることになる。このステップ S 2 で行われる書込処理は、IC カードが提供者 X の管理下にある時点で行われるので、通信エラーなどが生じるおそれが少ない安定した環境下で実行することができ、デフォルト許容値 D の書き込みに失敗した製品が出荷される可能性は極めて小さい。

30

【0055】

こうして、デフォルト許容値 D が書き込まれた IC カードは、提供者 X の手元を離れ、一般の流通経路を経て、ユーザの手元に到達する。携帯電話装着型の IC カードの場合、携帯電話の付属品としてユーザに提供されるケースが多い。ここで、ユーザが、当該 IC カードを携帯電話に装着し、携帯電話の通信機能を利用して、所望の信販会社のサーバにオンライン接続すれば、当該サーバからの遠隔発行処理（ステップ S 3）を受けることができ、当該 IC カードにクレジットカードとしての機能をもたせることができる。たとえば、信販会社 A が、許容値 M = 4 なる設定を行っていた場合、デフォルト許容値 D = 5 は許容値 M = 4 に書き換えられる。

40

【0056】

この遠隔発行処理のプロセスにおいて、通信エラーが生じると、許容値 M の書き込みに失敗するおそれがあることは既に述べたとおりである。しかしながら、ステップ S 3 にお

50

いて、許容値Mの書き込みに失敗しても、許容値格納部50内には、ステップS2において書き込まれたデフォルト許容値Dが格納されているため、セキュリティ上の重大な支障には至らない。上述の例の場合、許容値格納部50内には、本来は許容値4が格納されているべきであるが、書き込みが失敗した場合は、デフォルト許容値5が格納されている状態になり、厳密には、信販会社Aの意図どおりにはならないが、重大な支障にはならない。

【0057】

以上、本発明を図示する実施形態に基づいて説明したが、本発明はこれらの実施形態に限定されるものではなく、この他にも種々の態様で実施可能である。特に、図1～図5にブロックとして示した各構成要素は、情報処理装置100の特定の処理機能を1つの構成要素として抽出したものであり、実際には、情報処理装置100を構成するCPUやメモリなどのハードウェアと、情報処理装置100に組み込まれた種々のプログラムなどのソフトウェアとの組み合わせによって実現される要素である。

【図面の簡単な説明】

【0058】

【図1】従来から一般的に利用されている認証機能を備えた情報処理装置の基本構成を示すブロック図である。

【図2】図1に示す情報処理装置100に、更に、秘密コード書込部25および許容値書込部55を付加した構成例を示すブロック図である。

【図3】本発明の第1のアプローチに基づく実施形態に係る情報処理装置の基本構成を示すブロック図である。

【図4】図3に示す実施形態のより具体的な第1の実例を示すブロック図である。

【図5】図3に示す実施形態のより具体的な第2の実例を示すブロック図である。

【図6】本発明の第2のアプローチに基づく実施形態に係る情報処理装置の発行方法の手順を示す流れ図である。

【符号の説明】

【0059】

10…正否判定部
 20…秘密コード格納部
 25…秘密コード書込部
 30…連続試行回数計数部
 40…無効化処理部
 50…許容値格納部
 55…許容値書込部
 60…本来の情報処理部
 70…許容値格納判定部
 71…有効範囲設定部
 72…フラグ領域
 100…情報処理装置
 Ci…入力コード
 Cs…秘密コード
 D…デフォルト許容値
 M…許容値
 S1～S3…流れ図の各ステップ

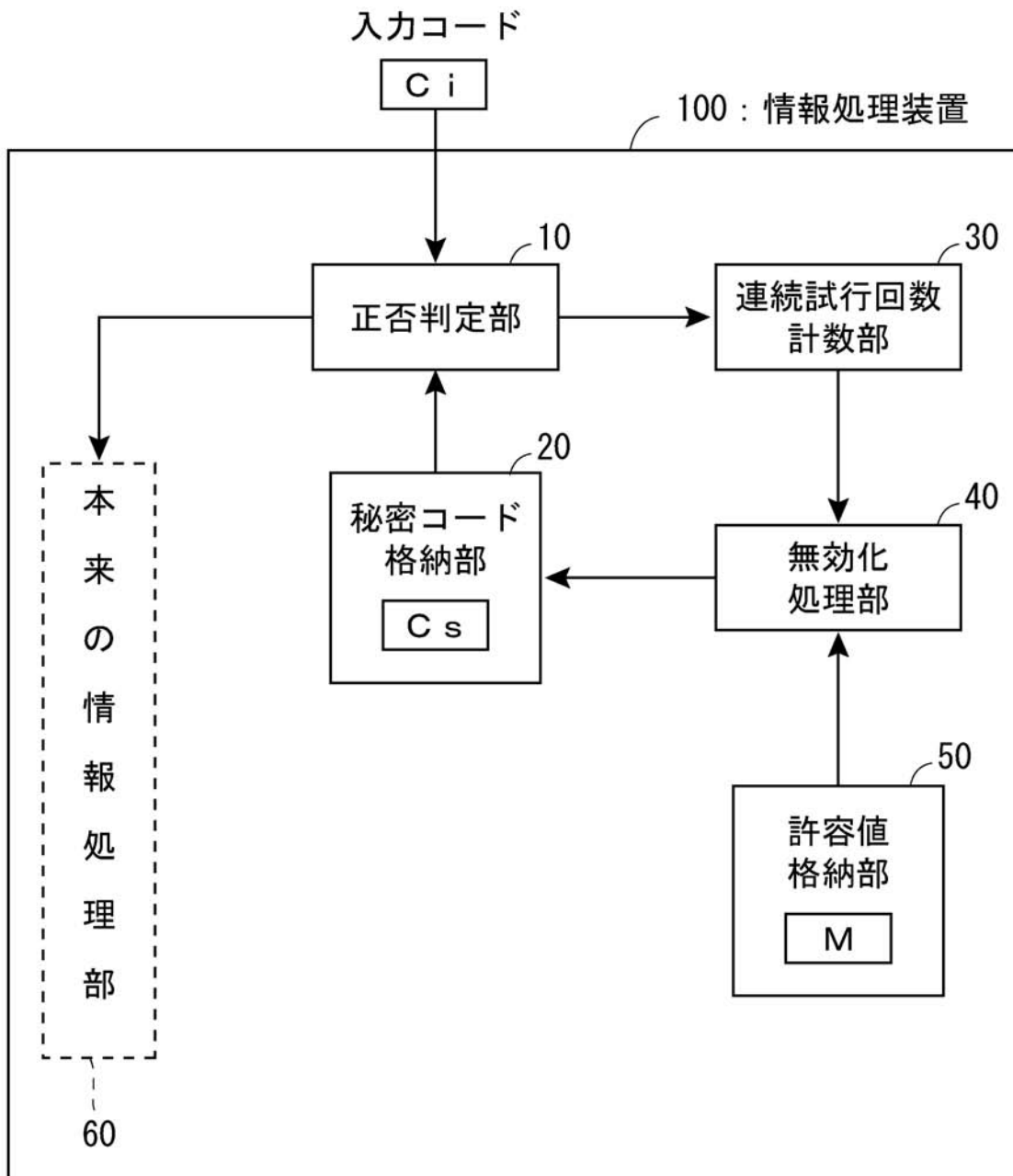
10

20

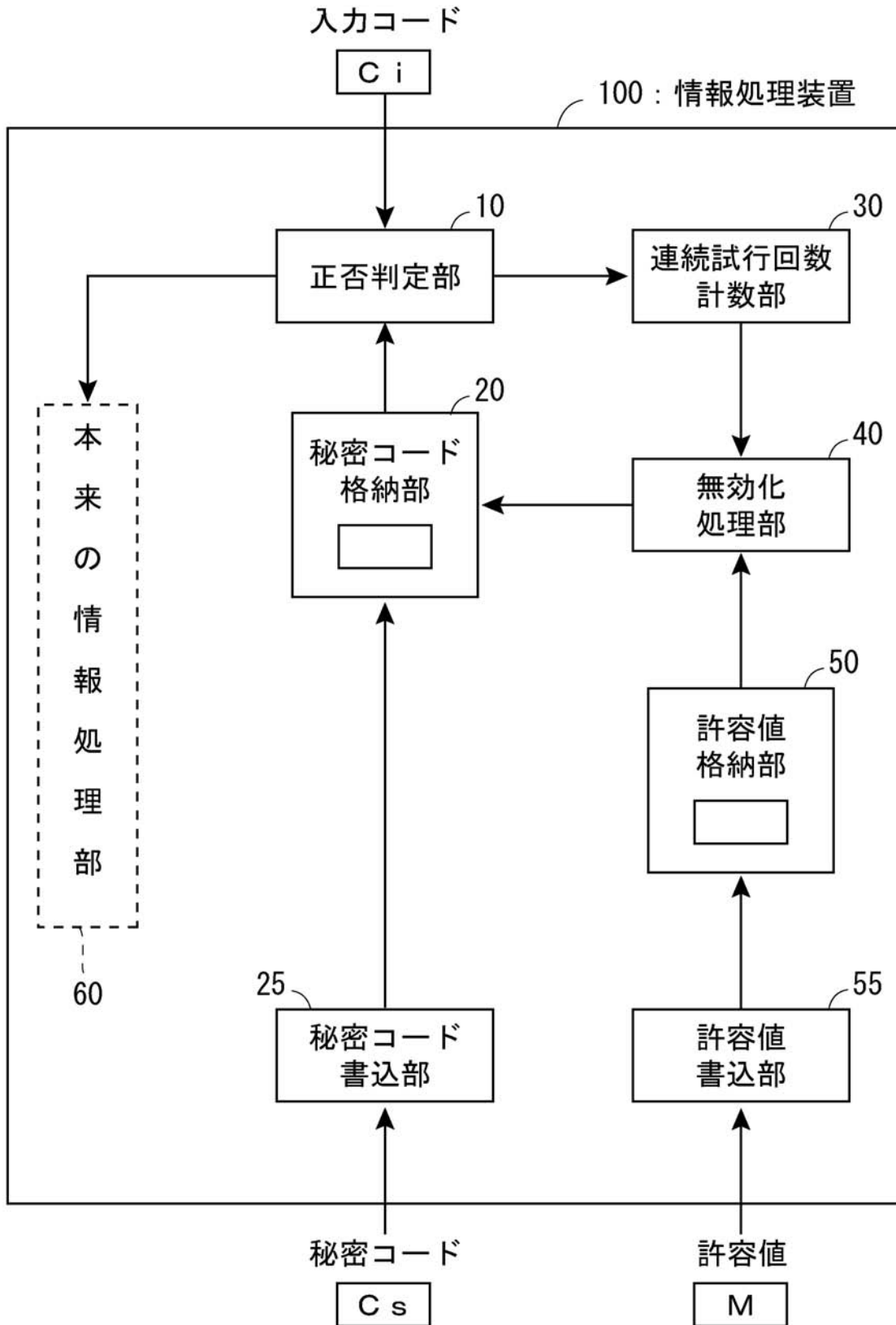
30

40

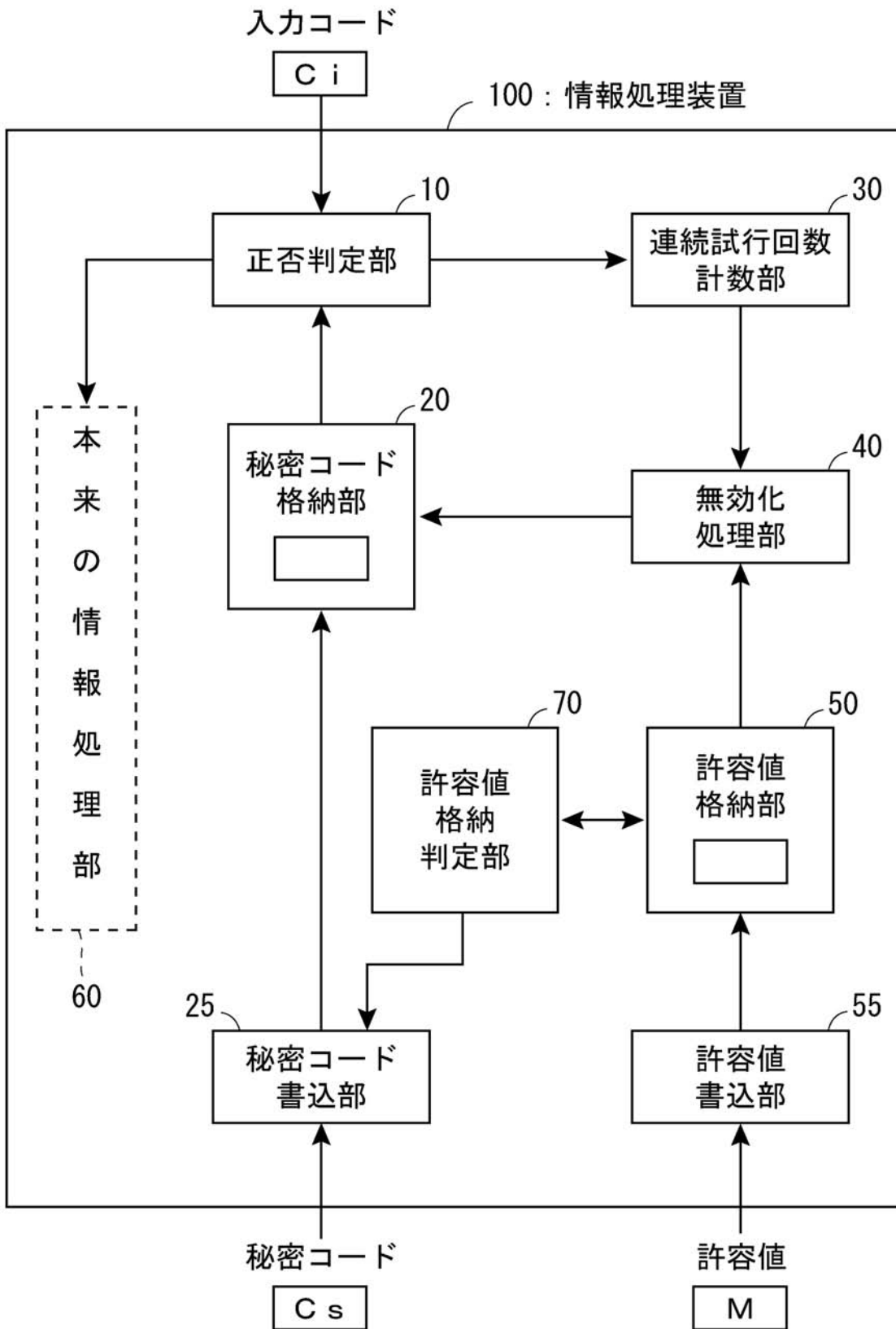
【図 1】



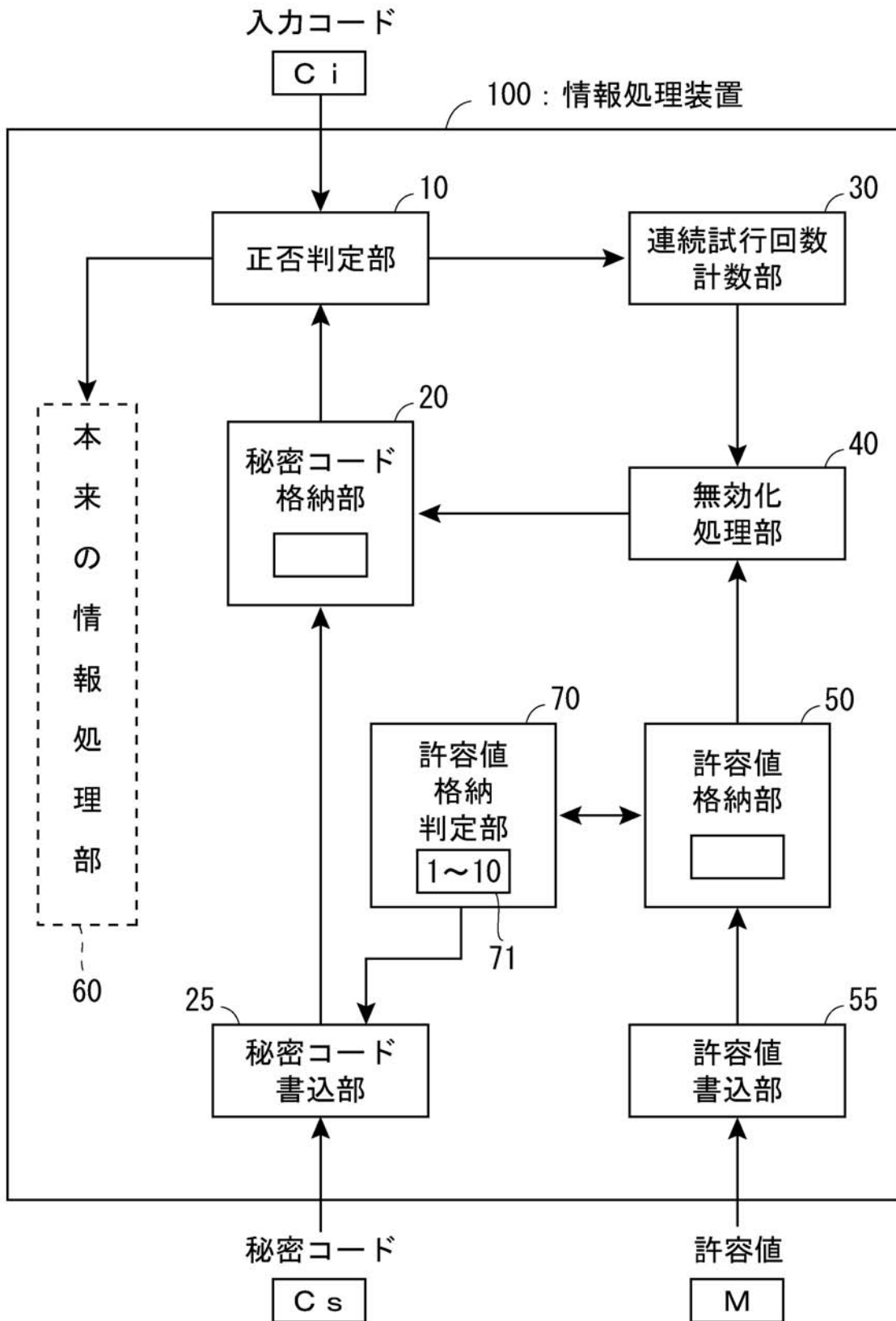
【図 2】



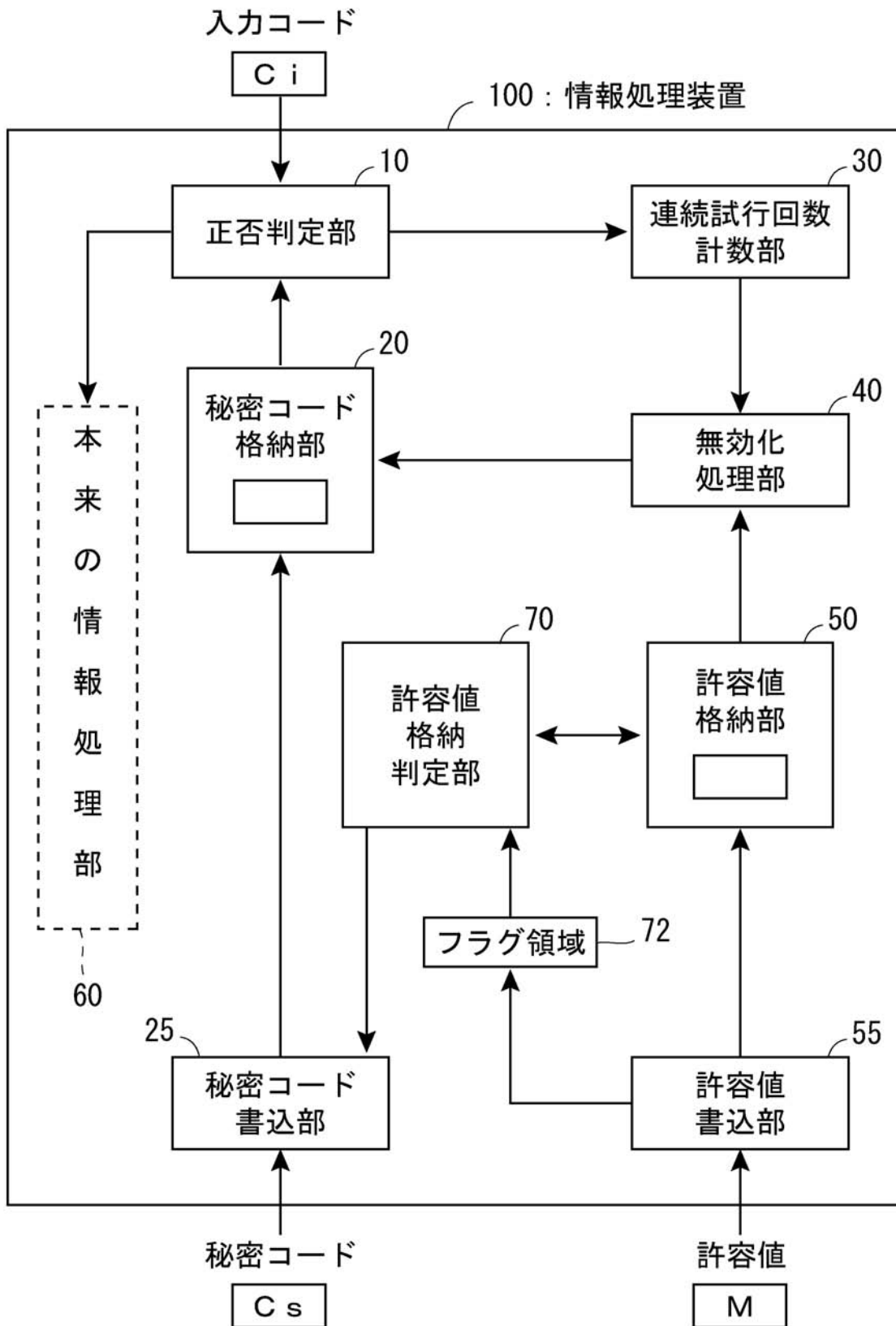
【図 3】



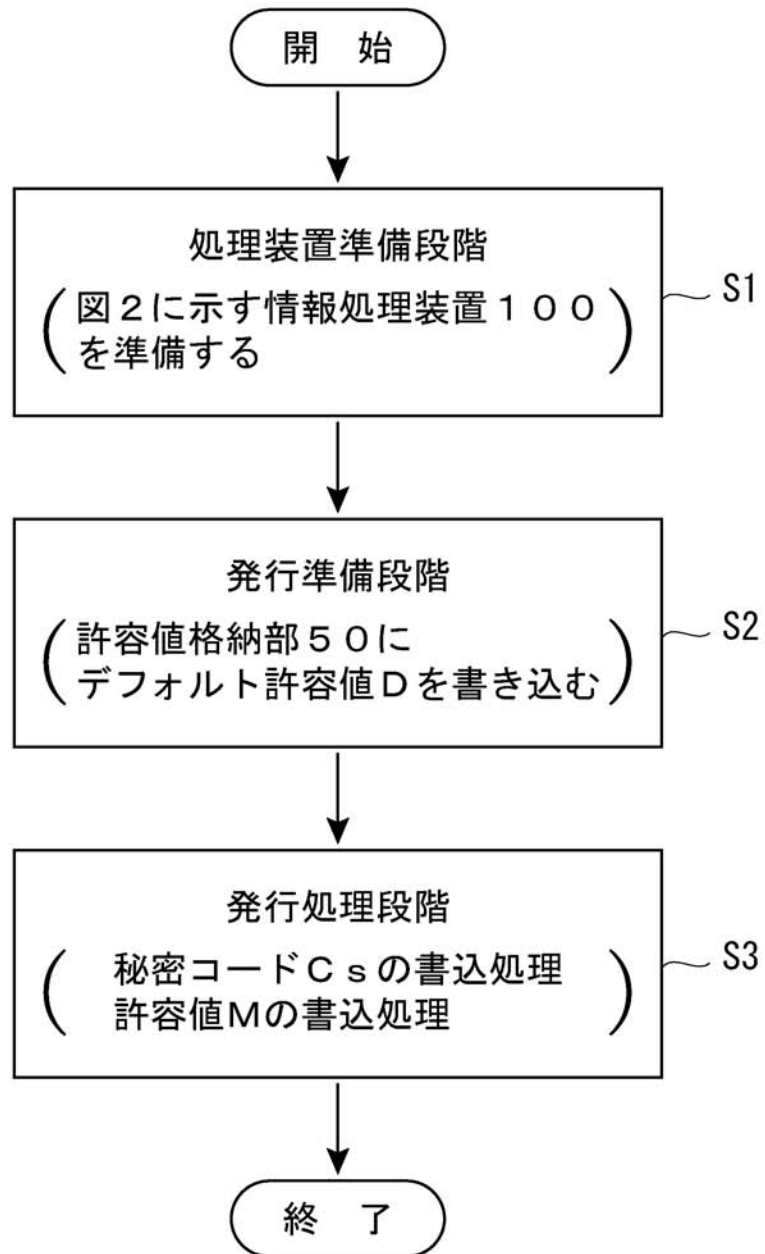
【図 4】



【図 5】



【図 6】



フロントページの続き

(72)発明者 加藤 純代

東京都新宿区市谷加賀町一丁目1番1号 大日本印刷株式会社内

Fターム(参考) 5B085 AE02 AE03