(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7569119号
(P7569119)

(45)発行日　令和6年10月17日(2024.10.17)

(24)登録日　令和6年10月8日(2024.10.8)

(51)国際特許分類
G06F 21/45 (2013.01)

FI
G06F 21/45

請求項の数　14　（全23頁）

(21)出願番号　特願2023-513794(P2023-513794)
(86)(22)出願日　令和3年12月16日(2021.12.16)
(65)公表番号　特表2023-539502(P2023-539502A)
(43)公表日　令和5年9月14日(2023.9.14)
(86)国際出願番号　PCT/CN2021/138583
(87)国際公開番号　WO2022/174665
(87)国際公開日　令和4年8月25日(2022.8.25)
審査請求日　令和5年2月24日(2023.2.24)
(31)優先権主張番号　202110182503.5
(32)優先日　令和3年2月16日(2021.2.16)
(33)優先権主張国・地域又は機関
中国(CN)

(73)特許権者　523066598
蒋 雲帆
中華人民共和国 江蘇省常州市北環南村１４－丁－４０１
(74)代理人　100130111
弁理士　新保 斉
(72)発明者　蒋 雲帆
中華人民共和国 江蘇省常州市北環南村１４－丁－４０１
審査官　三森 雄介

最終頁に続く

(54)【発明の名称】　スマート暗号の実現方法、装置、電子機器、およびコンピュータ可読媒体

(57)【特許請求の範囲】

【請求項１】

暗号センターサーバーに適用されるスマート暗号の実現方法であって、

ユーザー端末によって送信された管理要求情報を取得する、その中に暗号変更要求、暗号変更モジュール設定、および暗号変更頻度設定を含むステップと、

前記暗号変更モジュール設定、暗号変更要求、または暗号変更頻度に応じて変更対象暗号を生成する変更対象暗号、暗号変更要求、または暗号変更頻度に応じて、対象デバイス／施設の変更対象情報を生成するステップと、

変更対象情報により対象デバイス／施設の暗号変更を実行する、または変更対象情報により対象デバイス／施設に保留中の変更情報を提供するステップと、

変更フィードバック情報を生成する、または前記対象デバイス／施設によって送信される変更フィードバック情報を取得する、前記変更フィードバック情報に変更結果が含まれているステップと、

前記変更フィードバック情報を前記ユーザー端末に送信するステップとを含み、

前記暗号センターサーバーが複数あり、複数の暗号センターサーバーは独自の暗号センター識別コードを持ち、複数の暗号センターサーバー間でデータ同期と情報プッシュが実行される、信頼できる暗号センターサーバーは別の暗号センターサーバーに管理されている対象のデバイス／施設にワンクリックログインを実現できる

ことを特徴とするスマート暗号の実現方法。

【請求項２】

対象デバイス／施設の登録依頼情報を取得する、
前記対象デバイス／施設の確認依頼情報をユーザー端末に送信する、
前記ユーザー端末からフィードバックされる登録確認情報を取得する、ことを含む
請求項１に記載のスマート暗号の実現方法。
【請求項３】
前記対象デバイス／施設は、ローカルデバイス／施設、遠隔デバイス／施設、または前記ローカルデバイス／施設、遠隔デバイス／施設、関連する関連デバイス／施設を含む
請求項１または２に記載のスマート暗号の実現方法。
【請求項４】
前記対象デバイス／施設は、必要に応じて、暗号検証、傍受および結合、および要件に応じたアプリケーションスプライシングの後に、対象デバイス／施設の暗号を自動的に変更する
請求項１に記載のスマート暗号の実現方法。
【請求項５】
前記暗号には、静的暗号、暗号で保護された質問と回答、デジタル証明書、デジタル資産、非公開アクセスパスのポート、コミュニティストリング、およびアプリケーションコンテキストが含まれる
請求項１に記載のスマート暗号の実現方法。
【請求項６】
前記管理要求情報には、暗号センターサーバーの管理、対象デバイス／施設の管理、または対象デバイス／施設の管理を他のユーザーに許可するために使用される制御命令が含まれ、前記対象デバイス／施設の管理方法には、即時のシャットダウン、ログインの禁止または許可、強制ログアウト、サービスおよびアプリケーションの開始と停止が含まれる
請求項１に記載のスマート暗号の実現方法。
【請求項７】
ユーザー端末に適用されるスマート暗号の実現方法を含み、
管理要求情報を暗号センターサーバーに送信する、前記管理要求情報には、暗号変更要求、暗号変更モジュール設定、および暗号変更頻度設定が含まれ、暗号変更モジュール、暗号変更要求、または暗号変更頻度が使用される、変更対象の暗号が前記暗号センターサーバーで生成され、前記変更対象の暗号、暗号変更要求、または暗号変更頻度が暗号センターサーバーによって使用され、対象デバイス／施設の変更対象の情報が生成される、前記変更対象の情報は、暗号センターサーバーによって使用される対象デバイス／施設の暗号変更操作を実行し、変更フィードバック情報を生成する、または、対象デバイス／施設が暗号センターサーバーから暗号を取得した後、暗号変更操作を実行し、変更フィードバック情報を暗号センターサーバーに送信する、前記変更フィードバック情報には変更結果を含む
請求項１に記載のスマート暗号の実現方法。
【請求項８】
対象デバイス／施設に適用されるスマート暗号の実現方法を含み、
暗号センターサーバーによって提供される変更対象の情報を取得する、前記変更対象の情報は、対象デバイス／施設を暗号センターサーバーにポーリングすることによって取得されるか、暗号センターサーバーによって送信される、変更対象の情報には変更対象の暗号、暗号変更要求または暗号変更頻度を含む、前記変更対象の暗号は、暗号変更モジュール、暗号変更要求または暗号変更頻度によって生成する、前記暗号変更モジュール、暗号変更要求または暗号変更頻度がユーザー端末から暗号センターサーバーに送信する、
変更対象情報に従って、暗号変更操作を実行する、
変更フィードバック情報を前記暗号センターサーバーに送信する、前記変更フィードバック情報は、暗号センターサーバーによって使用されるユーザー端末に送信する、変更フィードバック情報は変更結果を含む、ことを含む
請求項１に記載のスマート暗号の実現方法。

【請求項９】
暗号センターサーバーに適用されるスマート暗号の実現装置であって、
管理要求情報取得モジュール、ユーザー端末によって送信された管理要求情報を取得するに使用される、前記管理要求情報が、暗号変更要求、暗号変更モジュール設定、および暗号変更頻度設定を含む；
変更対象情報生成モジュール、前記暗号変更モジュール設定、暗号変更要求、または暗号変更頻度に応じて変更対象暗号を生成し、前記変更対象暗号、暗号変更要求または暗号変更頻度に応じて対象デバイス／設備変更情報を生成する、
暗号変更実行モジュール、変更対象情報に従って対象デバイス／施設の暗号変更操作を実行する、または対象デバイス／施設が暗号を実行するために変更対象情報を対象デバイス／施設に提供する、
サーバーフィードバック取得モジュール、変更フィードバック情報を生成するため、または前記対象デバイス／施設から送信された変更フィードバック情報を取得するために使用される、前記変更フィードバック情報は変更結果を含む、
サーバーフィードバック送信モジュール、前記変更フィードバック情報を前記ユーザー端末に送信するために使用される、ことを含み、
前記暗号センターサーバーが複数あり、複数の暗号センターサーバーは独自の暗号センター識別コードを持ち、複数の暗号センターサーバー間でデータ同期と情報プッシュが実行される、信頼できる暗号センターサーバーは別の暗号センターサーバーに管理されている対象のデバイス／施設にワンクリックログインを実現できる
ことを特徴とするスマート暗号の実現装置。
【請求項１０】
請求項９に記載のスマート暗号の実現装置及びユーザー端末に適用されるスマート暗号の実現装置を含み、
当該ユーザー端末に適用されるスマート暗号の実現装置は、
管理要求情報送信モジュール、管理要求情報を暗号センターサーバーに送信するために使用される、前記管理要求情報は、暗号変更要求、暗号変更モジュール設定、および暗号変更頻度設定を含む、前記暗号変更モジュール設定、暗号変更要求または暗号変更頻度は、変更対象暗号を生成するために前記暗号センターサーバーによって使用される、変更対象暗号、暗号変更要求または暗号変更頻度は、暗号センターサーバーによって対象デバイス／施設を生成するために使用される、または対象デバイス／施設が暗号変更操作を実行する上に、変更フィードバック情報を暗号センターサーバーに送信する、前記変更フィードバック情報は変更結果を含む、
端末フィードバック取得モジュール、前記暗号センターサーバーによって送信された変更フィードバック情報を取得するために使用される
ことを特徴とするスマート暗号の実現システム。
【請求項１１】
請求項９に記載のスマート暗号の実現装置及び対象デバイス／施設に適用されるスマート暗号の実現装置を含み、
当該対象デバイス／施設に適用されるスマート暗号の実現装置は、
変更対象情報取得モジュール、暗号センターサーバーによって提供される変更情報を取得するために使用される、前記変更情報は、対象デバイス／施設を暗号センターサーバーにポーリングすることによって取得される、または暗号センターサーバーによって送信される、変更対象情報は変更対象暗号、暗号変更要求または暗号変更頻度を含む、前記変更対象暗号は、暗号変更モジュール、暗号変更要求または暗号変更頻度、および暗号変更モジュールに従って、暗号センターサーバーによって生成される、前記暗号変更モジュール、暗号変更要求または暗号変更頻度はユーザー端末によって、暗号センターサーバーに送信する、
変更実行モジュール、変更対象情報に従って暗号変更操作を実行するために使用される、
デバイスフィードバック送信モジュール、変更フィードバック情報は前記暗号センター

サーバーによってユーザー端末に送信するために使用される、変更フィードバック情報は変更結果を含む
ことを特徴とするスマート暗号の実現システム。
【請求項１２】
スマート暗号の実現システムであって、
暗号センターサーバー、前記暗号センターサーバーに接続されたユーザー端末、および前記暗号センターサーバーに接続された対象デバイス／施設を含む、
前記暗号センターサーバーは、請求項９に記載のスマート暗号変更の実現装置、前記ユーザー端末は、請求項１０に記載のスマート暗号変更の実現装置、前記対象デバイス／施設は請求項１１に記載のスマート暗号変更の実現装置、を含む
ことを特徴とするスマート暗号の実現システム。
【請求項１３】
電子デバイスであって、
少なくとも１つのプロセッサ；
少なくとも１つのコンピュータプログラムを記憶するための記憶手段；
少なくとも１つの前記コンピュータプログラムが少なくとも１つの前記プロセッサによって実行されるとき、少なくとも１つのプロセッサは、請求項１ないし８のいずれかに記載の方法を実施する
ことを特徴とする電子デバイス。
【請求項１４】
コンピュータプログラムが格納されたコンピュータ可読媒体であって、
前記コンピュータプログラムは、プロセッサによって実行され、請求項１ないし８のいずれかに記載の方法を実施する
ことを特徴とするコンピュータ可読媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報セキュリティの分野に関し、特に、スマート暗号の実現方法、装置、電子機器、及びコンピュータ可読媒体に関する。
【背景技術】
【０００２】
今の時代は、情報化が発展の一般的な傾向であり、先進的な生産性を代表し、人類は工業化の時代から情報化の時代に突入している。情報セキュリティの重要性が高まるにつれて、多数のセキュリティ技術と標準が生まれている。
【０００３】
関連技術では、情報システムの暗号は依然として主に手動で変更される、これは主観性、ランダム性、コンプライアンスの難しさなどの特徴がある。
【０００４】
実践の過程で、本発明者は、この技術には少なくとも次のような問題が存在することを発見した：
今の情報システムは複雑であるため、コンプライアンスに従って暗号を変更することは困難である。また、個人も組織も大量の暗号を記憶する必要がある。皆が暗号を紙に記録するか、電子文書に記録している。これらは紛失や漏洩しやすく、さまざまな隠れた危険を引き起こす。暗号を保護するための質問はほとんど変更されない。また、暗号をなくしたり忘れたりする現象も時折発生する。その際、時間と手間のかかる様々なリセットや訴えが必要となる。中規模の情報システムでは、本番データベースの暗号を変更するのに数時間かかる場合があり、更に、甲の情報システム管理者、甲の業務システムのリーダー、データベース管理者、システムの運用保守担当者、および業務システムの実装メンバーの立会いが必要になる可能性もある。暗号管理は、情報システムのセキュリティにおける明らかな弱点になっている。

【発明の概要】
【発明が解決しようとする課題】
【０００５】
暗号が紛失、忘れ、漏洩しやすく、変更に時間や手間がかかり、およびそれに伴う変更の問題を解決するために、本発明は、スマート暗号の実現する方法、装置、電子機器、およびコンピュータ可読媒体を提供する。
【課題を解決するための手段】
【０００６】
第１態様において、本発明はスマート暗号の実現方法を提供する、次の技術的解決策を採用する。
暗号センターサーバーに適用されるスマート暗号の実現方法は、
ユーザ端末によって送信された管理要求情報を取得する、その中に前記暗号変更要求、暗号変更モジュール設定、および暗号変更頻度設定を含むステップと、
前記暗号変更モジュール、暗号変更要求、または暗号変更頻度に応じて変更対象暗号が生成され、前記変更対象暗号、暗号変更要求、または暗号変更頻度に応じて、対象デバイス／施設の変更対象情報を生成するステップと、
変更対象情報により対象デバイス／施設の暗号変更を実行する、または変更対象情報により対象デバイス／施設に保留中の変更情報を提供するステップと、
変更フィードバック情報を生成する、または前記対象デバイス／施設によって送信される変更フィードバック情報を取得する。その中、前記変更フィードバック情報に変更結果が含まれているステップと、
前記変更フィードバック情報を前記ユーザー端末に送信するステップと、を含む。
【０００７】
いくつかの実施形態では、
対象デバイス／施設の登録依頼情報を取得するステップと、
前記対象デバイス／施設の確認依頼情報をユーザー端末に送信するステップと、
前記ユーザー端末からフィードバックされる登録確認情報を取得するステップと、を含む。
【０００８】
上記の技術的解決策を採用することにより、前記対象デバイス／施設を暗号センターサーバーに登録することができる。
いくつかの実施形態では、前記対象デバイス／施設は、ローカルデバイス／施設、リモートデバイス／施設、または前記ローカルデバイス／施設、リモートデバイス／施設に関連付けられた関連デバイス／施設を含む。
【０００９】
上記の技術的解決策を採用することにより、ローカルおよびリモートのデバイス／施設で暗号変更管理を実行する上、関連するデバイス／施設で同時に同期変更管理を実行することもできる。
【００１０】
いくつかの実施形態では、前記暗号センターサーバーが複数あり、複数の暗号センターサーバーは独自の暗号センター識別コードを持ち、複数の暗号センターサーバー間でデータ同期と情報プッシュが実行される。信頼できる暗号センターサーバーは別の暗号センターサーバーに管理されている対象のデバイス／施設にワンクリックログインを実現できる。
【００１１】
上記の技術的解決策を採用することにより、複数の暗号センターサーバーをデータ共有または災害復旧に使用できる。信頼できるサーバーは、他の暗号センター識別コードを持つサーバーとデータを同期して、データの冗長性を実現し、スマートアカウント管理とワンクリックログインなどを提供できる。ユーザーがより便利に利用できる。
【００１２】
いくつかの実施形態では、前記対象デバイス／施設は、必要に応じで、暗号検証、傍受

および結合、および要件に応じたアプリケーションスプライシングの後に、対象デバイス／施設の暗号を自動的に変更する。

【００１３】

いくつかの実施形態では、前記暗号には、静的暗号、暗号保護に関する質問と回答、デジタル証明書、デジタル資産、非公開アクセスパスのポート、コミュニティストリング、およびアプリケーションコンテキストが含まれるが、これらに限定されない。

【００１４】

上記の技術的解決策を採用することにより、前記対象のデバイス／施設が変更できる暗号には、上記の複数の種類が含まれるが、これらに限定されない； 暗号センターサーバーは、従来の静的暗号を管理するだけでなく、他のさまざまな情報、ポートなどに変更保護も可能である。セキュリティを大幅に強化する。

【００１５】

いくつかの実施形態では、前記管理要求情報には、暗号センターサーバーの管理、対象デバイス／施設の管理、または対象デバイス／施設の管理を他のユーザーに許可するために使用される制御命令が含まれる。前記対象デバイス／施設の管理方法には、即時のシャットダウン、ログインの禁止または許可、強制ログアウト、サービスおよびアプリケーションの開始と停止などが含まれるが、これらに限定されない。暗号センターサーバーの管理には、ユーザーが暗号を使用する時間枠の調整、暗号センター （またはその一部） 機能の使用の許可または禁止などが含まれるが、これらに限定されない。

【００１６】

上記の技術的解決策を採用することにより、制御命令を通じて暗号センターサーバーと対象デバイス／施設に対して特別な制御を実行することができる、より完全な管理を実現する。

【００１７】

第２態様において、本発明はスマート暗号を実現するための方法を提供する、次の技術的解決策を採用する。

【００１８】

ユーザー端末に適用されるスマート暗号の実現方法は、

管理要求情報を暗号センターサーバーに送信するステップであって、前記管理要求情報には、暗号変更要求、暗号変更モジュール設定、および暗号変更頻度設定が含まれ、前記暗号変更モジュール、暗号変更要求、または暗号変更頻度は、前記暗号センターサーバーに使用する、変更対象の暗号が生成され、前記変更対象の暗号、暗号変更要求、または暗号変更頻度が暗号センターサーバーによって使用され、対象デバイス／施設の変更対象の情報が生成され、前記変更対象の情報は、暗号センターサーバーによって使用される対象デバイス／施設の暗号変更操作を実行し、変更フィードバック情報が生成され、または、対象デバイス／施設が暗号センターサーバーから暗号を取得した後、暗号変更操作を実行し、変更フィードバック情報を暗号センターサーバーに送信する、前記変更フィードバック情報には変更結果を含む、

【００１９】

暗号センターサーバーから送信された変更フィードバック情報を取得するステップと、を含む。

【００２０】

第３態様において、本発明はスマート暗号の実現方法を提供する。次の技術的解決策を採用する。

対象デバイス／施設に適用されるスマート暗号の実現方法は、

暗号センターサーバーによって提供される変更対象の情報を取得するステップであって、前記変更対象の情報は、対象デバイス／施設を暗号センターサーバーにポーリングすることによって取得されるか、暗号センターサーバーによって送信され、変更対象の情報には変更対象の暗号、暗号変更要求または暗号変更頻度を含む、前記変更対象の暗号は、暗号変更モジュール、暗号変更要求または暗号変更頻度によって生成する、前記暗号変更モ

ジュール、暗号変更要求または暗号変更頻度がユーザー端末から暗号センターサーバーに送信するステップと、を含む。

【００２１】

変更対象情報に従って、暗号変更操作を実行する。

変更フィードバック情報を前記暗号センターサーバーに送信する。前記変更フィードバック情報は、暗号センターサーバーによって使用されるユーザー端末に送信する、変更フィードバック情報は変更結果を含む。

【００２２】

第４態様において 、本発明は、スマート暗号変更を実現するための装置を提供する。次の技術的解決策を採用する。

暗号センターサーバーに適用されるスマート暗号を実現するための装置は、

管理要求情報取得モジュール、ユーザ端末によって送信された管理要求情報を取得するに使用される。前記管理要求情報が、暗号変更要求、暗号変更モジュール設定、および暗号変更頻度設定を含む、

変更対象情報生成モジュール、前記暗号変更モジュール、暗号変更要求、または暗号変更頻度に応じて変更対象暗号を生成し、前記変更対象暗号、暗号変更要求または暗号変更頻度に応じて対象デバイス／設備変更情報を生成する、

暗号変更実行モジュール、変更対象情報に従って対象デバイス／施設の暗号変更操作を実行する、または対象デバイス／施設が暗号を実行するために変更対象情報を対象デバイス／施設に提供する、

サーバーフィードバック取得モジュール、変更フィードバック情報を生成するため、または前記対象デバイス／施設から送信された変更フィードバック情報を取得するために使用される、前記変更フィードバック情報は変更結果を含む、

サーバーフィードバック送信モジュール、前記変更フィードバック情報を前記ユーザー端末に送信するために使用される、を含む。

【００２３】

第５態様において、本発明は、スマート暗号変更を実現するための装置を提供する。次の技術的解決策を採用する。

ユーザー端末に適用されるスマート暗号を実現するための装置は、

管理要求情報送信モジュール、管理要求情報を暗号センターサーバーに送信するために使用される、前記管理要求情報は、暗号変更要求、暗号変更モジュール設定、および暗号変更頻度設定を含み、前記暗号変更モジュール、暗号変更要求または暗号変更頻度は、変更対象暗号を生成するために前記暗号センターサーバーによって使用され、前記変更対象暗号、暗号変更要求または暗号変更頻度は、暗号センターサーバーによって対象デバイス／施設の変更対象情報を生成するために使用され、前記変更対象情報は暗号センターサーバーが対象デバイス／施設の暗号変更操作を実行する変更フィードバック情報を生成するために使用され、または対象デバイス／施設が暗号センタサーバから取得する暗号変更操作を実行して暗号センタサーバに変更フィードバック情報を送信、変更フィードバック情報は変更結果を含む、

端末フィードバック取得モジュール、暗号センターサーバーによって送信された変更フィードバック情報を取得するために使用される、を含む。

【００２４】

第６態様において、本発明は、スマート暗号変更を実現するための装置を提供する、次の技術的解決策を採用する。

対象デバイス／施設に適用されるスマート暗号を実現するための装置は、

変更対象情報取得モジュール、暗号センターサーバーによって提供される変更情報を取得するために使用され、前記変更情報は、対象デバイス／施設を暗号センターサーバーにポーリングすることによって取得される、または暗号センターサーバーによって送信される。変更対象情報は変更対象暗号、暗号変更要求または暗号変更頻度を含み、前記変更対象暗号は、暗号変更モジュール、暗号変更要求または暗号変更頻度、および暗号変更モジ

ュールに従って、暗号センターサーバーによって生成され、前記暗号変更モジュール、暗号変更要求または暗号変更頻度はユーザー端末によって、暗号センターサーバーに送信する、

変更実行モジュール、変更対象情報に従って暗号変更操作を実行するために使用される、

デバイスフィードバック送信モジュール、変更フィードバック情報は前記暗号センターサーバーによってユーザ端末に送信するために使用され、変更フィードバック情報は変更結果を含む、を含む。

【００２５】

第７態様において 、本発明は、スマート暗号変更を実現するための装置を提供する、次の技術的解決策を採用する。

スマート暗号を実現するためのシステム、暗号センターサーバー、前記暗号センターサーバーに接続されたユーザー端末、および前記暗号センターサーバーに接続された対象デバイス／施設を含む、

前記暗号センターサーバーは、スマート暗号を実現するための上記のデバイスを含む、前記ユーザー端末は、スマート暗号変更を実現するための上記のデバイスを含む、前記対象デバイス／施設は、スマート暗号変更を実現するための上記のデバイスを含む。

【００２６】

第８態様において、本発明は、電子機器を提供する、以下の技術を採用する：

電子機器は、

少なくとも １ つのプロセッサ、

少なくとも１つのコンピュータプログラムを記憶するための記憶装置、

少なくとも１つの前記コンピュータプログラムが少なくとも１つの前記プロセッサによって実行されるとき、少なくとも１つの前記プロセッサは、スマート暗号変更を実施するための上記の実施方法、を含む。

【００２７】

第９態様において、本発明は、コンピュータ可読媒体を提供する。以下の技術的解決策を採用する：

コンピュータ可読媒体、コンピュータプログラムが格納され、前記コンピュータプログラムがプロセッサによって実行されると、スマート暗号を実現するための上記の実現方法。

【発明の効果】

【００２８】

本発明の技術案によれば、本発明は、以下の有益な技術的効果の少なくとも１つを含む：

１．本方法は、ユーザー主導のインテリジェントな暗号管理モードを採用し、暗号が簡単に紛失、忘れ、漏洩し、規制に従って暗号が生成および変更されるなどのさまざまな問題を解決する。

２．設定された暗号変更モジュールと暗号変更頻度に従って暗号が変更され、暗号管理のコンプライアンスが確保される。

３．ユーザーが暗号を変更するには、時間がかかり、労働集約的で、主観的であり、常に準拠しているとは限らないという欠点を解決する。特に、エンタープライズレベルのユーザーの情報システムなどのデバイス／施設の暗号管理を促進して、さまざまなセキュリティ基準に準拠する。

４．従来の静的な暗号インテリジェンスの実現に加えて、暗号で保護されたさまざまな質問と回答、デジタル証明書、デジタルアセット、非パブリックアクセスパスのポート、コミュニティストリング、およびアプリケーションコンテキストを変更および管理することも可能である。従来の暗号にはない、自動変更と通知、および制御命令の実行という利点がある。

５．利用者自身の対象デバイス／設備の管理ができる、対象デバイス／設備の管理権限を他人に与えることもできる、特定のデバイス／設備を管理する同時に、関連するデバイス／設備を管理することができる。

６．ユーザー端末と同じデバイスに暗号センターサーバーを設置してワンクリックログ

インを実現し、複雑な暗号の使用を大幅に容易にし、各暗号センターサーバー間のセッション情報をプッシュすることでシングルサインオンとシングルログアウトを実現する。

【図面の簡単な説明】

【００２９】

【図１】本発明の一実施形態によって提供される暗号センターサーバー構造模式図である。

【図２】本発明の一実施形態によって提供されるスマート暗号を実現するための方法のフローチャートである。

【図３】本発明の一実施形態によって提供される暗号センターサーバーに適用されるスマート暗号実装デバイスの構造フレーム図である。

【図４】本発明の一実施形態によって提供されるユーザ端末に適用されるスマート暗号を実現するためのデバイスの構造フレームワーク図である。

【図５】本発明の一実施形態によって提供される対象デバイス／施設に適用されるスマート暗号を実現するための装置の構造フレームワーク図である。

【図６】本発明の一実施形態によって提供される電子機器の概略ブロック図である。

【発明を実施するための形態】

【００３０】

以下、図面を参照しながら本発明の例示的な実施例を詳細に説明する。

本発明の実施例は、スマート暗号を実現するための方法および装置を開示する。暗号センターサーバー（すなわち、スマート暗号センター）およびその汎クライアントの実現を通じて、人々は手動の方法を使用して暗号を変更する必要がない。暗号生成・変更プログラム、暗号モジュール・変更頻度管理プログラム、メッセージサービスプログラムからなる暗号は、暗号管理のインテリジェントコアを構成し、暗号モジュール・変更頻度管理プログラムは、施設所有者によって発行された暗号モジュール／変更頻度要求； 暗号生成および変更プログラムは、設定された時間枠内で指定された暗号モジュール／変更頻度に従って新しい暗号を生成し、暗号変更操作を自動的に実行する。ローカルデバイス／施設暗号および関連デバイス／施設暗号を含む。対象のデバイス／施設でクライアントプログラムを実行し、暗号センターサーバーへの登録申請を行う。登録認可後、指定したノード施設アカウントの暗号を取得し、希望の時間枠で施設暗号または関連施設暗号を期間内に変更することができる。ローカル変更またはリモート変更の結果に関係なく、暗号／施設アカウントの所有者はメッセージ サービス プログラムを通じて通知され、暗号／施設アカウントの所有者は暗号モジュールと変更頻度を照会および調整できる。

【００３１】

スマート暗号の実装は、暗号の生成、保存、使用、変更、および破棄の革新という点で従来の暗号とは異なり、従来の暗号にはない自動変更、通知、および制御命令がある。システムが従来の暗号を制限しない限り、暗号の使用 （暗号の複雑さと変更サイクル） は、暗号所有者の主観に依存する。一部のアプリケーションシステムでは、暗号に特定の複雑さと変更サイクルを持たせる必要があるが、最終的には暗号所有者が変更する必要がある。従来の暗号の記憶は、暗号の所有者に完全に依存している。記憶に依存することに加えて， それはどこかに書かれている （紙やコンピュータや携帯電話のファイルに）。前者は忘れやすい、後者は紛失・漏洩しやすい。記録媒体の忘れ紛失も多い。現在、暗号忘れ・暗号再設定のアプリはさまざまで、最も利用されているのは携帯電話・メール。前者は十分に安全ではない、後者には暗号が含まれる； セキュリティの質問と回答は比較的安全だが、明らかにより多くのメモリが必要になる； 一般的に使用される携帯電話の確認コードログイン方法は一時的な場合に使用され、携帯電話が交換または紛失した時に予期しない問題に直面することがよくある。もちろん、スマート暗号方式は、従来の暗号方式を完全に置き換えることを意図したものではない。スマート暗号と従来の暗号は共存でき、交換できる。たとえば、スマート暗号を有効にして、従来の暗号を自動的に更新できる。スマート暗号を無効にするには、手動で変更して、従来の暗号の使用を復元できる、必要の時に、スマート暗号に切り替える。

【００３２】

本発明の実施例による、制御命令は、暗号化センターサーバを管理する、対象デバイス／施設を管理する、または対象デバイス／施設を管理することを他者に許可するために使用され、また、暗号センターサーバーの時間枠およびソースアドレスを管理することができる。対象デバイス／施設の管理方法としては、即時シャットダウン、ログイン（暗号ログイン、無暗号ログインを含む）の禁止または許可、強制ログアウト、サービスやアプリケーションの起動・停止などがある。対象デバイス／施設の時間枠は、暗号センターサーバーによって設定され、ユーザーの設定を受け入れる。具体的には、許可された時間範囲内で暗号変更または一部の管理コマンドの実行または実行を禁止することを含む。これは、デバイス／設備がサーバー側ではなく、常にオンにすることを保証できないため。時間調整のみに依存する場合、いくつかのタスクを見逃す可能性がある。もちろん、一部のデバイス／施設が重要なプロセスを実行している場合、それらを妨害することはできないため、時間枠が使用されるデバイス／施設の本業の安全を確保する。結局、スマート暗号システムはあくまでも付加機能、デバイス／施設本来の機能を無視することはできない。暗号センターサーバー自体の時間枠は、セキュリティを確保するために、システム管理者が特定のユーザーまたは一部のユーザー設定を指定して、自分のアカウントが特定の時間枠でのみスマート暗号機能を要求できるように指定できる。

【００３３】

本発明の実施例による、暗号を変更する必要がある対象の／施設は、ノード、施設、およびアカウントとして具体的に定義されている。スマート暗号センターによって生成する暗号を自動的に適用する必要がある場合、そのノードは、ＩＰアドレスとネットワーク到達可能なデバイス、または物理リンクを持つ通信可能なデバイスが必要である。たとえばルーター／スイッチ、 ＮＡＳ／ＳＡＳ、ＰＣ／サーバーなど。組み込みデバイス、産業用制御デバイスなどの特定のノード設備に対して、 ＡＰＩインターフェースを備えている必要がある。その施設は、さまざまなビジネスシステム、オペレーティングシステム自体、データベース、アプリケーション サーバーを参照できる。その他のシステムサービス、およびそのアカウントは、通常、ログイン／アクセシビリティの特性を備えているため、通常のアカウントに加えて、ＩＴ システム固有のポートおよびネットワーク固有のポートも含む。コミュニティストリング、アプリケーションコンテキストの業務システムなどノード、施設、アカウントとそれらの所有者、つまりユーザー管理の間には多対多の関係があり、上位レベルのユーザーが下位レベルのユーザーの施設を管理できるように、ユーザー管理の間に一定のレベル差がある。

【００３４】

本発明の実施例による、非パブリック アクセスパスのポートは、通常、２２ ｓｓｈデフォルトリモートアクセスポート、３３８９ｗｉｎｄｏｗｓリモートデスクトップアクセスポートを含む、コミュニティ／グループ文字列ｃｏｍｍｕｎｉｔｙ ｓｔｒｉｎｇは、ＳＮＭＰ の単純なネットワークプロトコルアクセスによってＭＩＢ 管理情報ベースと組み合わせて、オブジェクトに関する多くの情報は取得できる。アプリケーションコンテキストｃｏｎｔｅｘｔ、例えばアプリケーションサーバー ｗｅｂｌｏｇｉｃ のコンソールコンテキストｃｏｎｓｏｌｅなど。これらの情報は通常に公開する必要はないが、許可された人だけがアクセスできるようにすることが重要であり、そのダイナミゼーションを実現することで、不正な検出とアクセスを効果的に回避できる。この情報は通常、構成ファイル （ Ｗｉｎｄｏｗｓ ではレジストリを使用するものもある） に保存され、特定のプログラムを作成することで変更できる。このプログラムは、事前設定された変更頻度ウィンドウ内でスマート暗号生成プログラムによってトリガーされ、変更結果が次の変更時間とともにメッセージシステムによって管理者に知らせる、管理者のメンテナンス作業が妨げられず、必要なアクセス情報は外部から隠されている。さらに、スマート暗号システムは関連する変更もトリガーする、情報にアクセスする必要があるシステム／アプリケーションは同時にアクセス構成を変更できる、必要な情報を確実に取得することを確保する。最も代表的なものは運用・保守システムだ。ポートモジュールには、システム内の他のプログラムによって使用されないポートを選択すべき、それは値の範囲も必要がある。

たとえば、ポート　２２　は　４００００　～　４９９９９　を使用できる。１時間ごとに変更する場合、モジュールは　４＋０　から　９９９９　までの乱数または　４％ｍ％ｄ％ｈで、１０　か月間繰り返されないように保証できる　（４１１２３　４１１５３　４１１８３）。コミュニティ／グループ文字列とアプリケーションコンテキストは、いくつかの特殊な記号がモジュール定義から除外されている限り、より広い範囲を持つことができる。

【００３５】

本発明の実施例による、暗号モジュール／変更頻度基本修飾詞ＹｙｍｄＨＭｗＳ　（年、月、日、時、週、四半期）は、実際の必要性に従って調整することができ、符号化ビット数／長さは、それに従って決定することができる。システムのライフサイクルに合わせて、適切な修飾詞を選択する。このうち、Ｙ　は　１　文字で表される相対的な年、ｙ　は　２　文字の年、ｍｄＨｗｓ　は　全て１　文字で表示する、修飾詞の前に　％　を追加して、順序が固定された正確なモジュールを形成する。入力の解析中にランダムな順序で生成される。８　桁などの最小長に満たないランダムに挿入された文字または記号に加えて、ユーザー管理の固有文字シーケンスにより、（全員）　毎回異なる暗号モジュールが作成される。変更の頻度は暗号モジュールと一致する必要がある。　例えばＹｗ，　ｗ１．８：ｗ３　（コンマの前は準定義の暗号モジュール、コンマの後ろは変更頻度）　、暗号が　３　週間ごとの最初の月曜日の　８：００　に変更することを示す。年と週はモジュールで使用され、生成されたモジュールには　％Ｙ　と　％ｗ　を含む。もちろん、順序はランダムに決定されるため、ユーザー管理　（ｙｕｎｆａｎ　など）　が特定のモジュールを生成する、Ｆ　％ｗ＃ｕｎ％Ｙｙ　＆　，　拡張修飾子　％ｒ　を使用しない場合、モジュールの更新ごとの暗号は、年と週を除いて同じだ。％ｒ　を追加すると、毎回生成される暗号が再び乱れ、推測できなくなる。暗号モジュール／変更頻度以外に、暗号保護の質問と回答、リンク変更スクリプト名、地域／ネットワークアドレスと時間保護などの拡張情報を同時に入力できる。もちろん、上記の入力方法はシステム実装における最も基本的なものに過ぎない。より実用的なのは、　ＷＥＢサーバーに面したｈｔｔｐｓリンクの形のショートカットモジュールである。例えば、「クリックで３週間ごど暗号変更モジュールを生成する」　、　「クリックで３ヶ月ごと暗号変更モジュールを生成する」など。また、少なくとも下記３種がある：Ｗｅｂプログラムによる実現する、モバイルアプリによる実現する、音声による実現する。その中で、モバイル　ＡＰＰ　は、モバイルデバイス　（システムとアプリケーション）　の暗号変更を同時に実現し、細かい管理を実現し、優れたユーザー　エクスペリエンスを実現できる。　ショートカット　テンプレートは、基本的な修飾詞に基づく正確なテンプレートとして、システムによってランダムに決定される。同時に、ショートカットモジュール　（またはシステム　カスタム　モジュール）　をユーザーが手動で入力して、バカ式操作を実現する。ユーザーの選択によって、２　か月以内に暗号を変更するなど。カスタムモジュールは、　ただｙｍかもしれない、ランダムに生成された少なくとも８つの数字の正確なモジュールが保存され、１分の終わりに、暗号センターサーバーがこれに基づいて新しい暗号を生成し、次の変更時間と同時にユーザー端末に送信する。

【００３６】

図１に示されるように、本発明の実施例による、スマート暗号センターは、センターデータベース２００および暗号生成変更プログラム２０１を含む（２つは、ローカルエリアネットワーク内の同じホスト上または異なるホスト上にあってもよい。すべてのホストはファイアウォールを開き、対応するセキュリティポリシーを有効にする必要がある。リンク１０２　は、クリアコードまたはデータベースによって暗号化できる）、暗号センターＷＥＢ　サービスプログラム２０２で実行される暗号モジュール／変更頻度管理プログラム（リンク　１０１　は、ファイアウォールまたはゲートキーパーを追加する）、受け入れる暗号センターインスタントメッセージング　サービス　プログラム　２０３　に通知メッセージを送信する　（リンク　１０３　はユーザー管理に通知するために使用され、リンク　１０８　はインスタントメッセージングサーバーによる暗号化通信を提供し、リンク　１０４　は暗号センターデータベース　２００　に直接アクセスする内部インスタントメッセージングサーバー、外部インスタントメッセージングサーバーを採用する場合、暗号センタ

ーインスタントメッセージングサービスプログラム　２０３　は、暗号センター　ＷＥＢ　サービス　プログラム　２０２　に統合される。特定の変更を実行するクライアント　プログラム　２０４　（リンク　１０６　は一般に　ｈｔｔｐｓ　暗号化でアクセスされ、その通信内容はセキュリティを確保するために暗号センター専用の　２　層暗号化プロトコルを持っている）　は、暗号を変更する必要があるノード上で実行される。または、リモートの到達可能なノード機能の暗号を変更するために使用される　（ｓｓｈ　証明書の信頼を設定するなど）。後者は、現代の複雑な　ＩＴ　環境のニーズにより適している。リンク　１０５　は、暗号センター　ＷＥＢ　サービス　プログラム　２０２　からユーザー管理へのメッセージ通知を実現する。リンク　１０７　は、ユーザーが　ＷＥＢ　モードで暗号モジュールを管理することを可能にするが、必須ではない。リンク　１０９　は、ユーザーがモバイルＡＰＰ　を介して暗号モジュールをより細かく管理することを可能にするが、大規模な環境でない限り必要がない。

【００３７】

本発明の実施例による、ユーザー管理はクライアントプログラム　２０４　またはモバイルＡＰＰ　２０６　を使用して登録要求を開始し、暗号を変更する必要があるノード上の施設とアカウントを指定する。スマート暗号センターは要求に応答し、インスタントメッセージングクライアントまたはモバイルＡＰＰ　２０６　で確認した後、登録は成功し、ユーザー管理はユーザー端末　２０５またはモバイルＡＰＰ　２０６　を介して暗号モジュール／変更頻度を設定し、ユーザーは独自の正確な固定モジュールを設定することができる、またはシステムの事前定義されたモジュールと機能に基づく可変モジュールを採用するように設定し、同時に変更頻度を設定することができる。スマート暗号センターが受け入れ後、ユーザーの特定のニーズを分析して、決定された暗号モジュールを生成し、頻度と拡張情報を変更し、入力を確認するためにユーザーに返信する。正確なモジュールが明確に指定されていない限り，　毎回確定されたモジュールが違う、暗号生成プログラムが即時に採用された暗号モジュールと頻度、および次回の暗号変更時間をユーザー管理に通知する。ユーザー管理は、すべてのノード、施設、およびアカウントの暗号を照会できる、またユーザーレベルに応じる、暗号モジュールと変更頻度、および次回の変更時間を含む。

【００３８】

本発明の実施例による、対象デバイス／施設の以下の登録手順を実装することができる：

暗号センターサーバーは対象デバイス／設備の登録依頼情報を取得し、ここでの登録依頼情報は対象デバイス／施設の所有者より送信することができる（既存の対象デバイス／施設一覧表をお持ちの方はこちらの手順をスキップして直接次の　２　つの手順を実行して登録する）　、

暗号センターサーバーは、対象デバイス／施設の確認要求情報をユーザー端末に送信する、

ユーザ端末は、登録確認情報を暗号センターサーバにフィードバックする。

【００３９】

本発明の実施例による、対象施設の自動登録処理：暗号センターのデータベースが施設所有者のアカウントを有することを前提とし、施設自体の管理システムが施設所有者の正当性を保証するもの、例えば、退社した者は、以下の業務を継続することができない。施設の所有者は、インスタントメッセージング　ロボットにクエスチョン　マークなどの指示を送信してスマート　暗号を有効にするだけでよく、スマート　暗号　システム　サービスプログラムは、メッセージを受信した後、暗号　モジュールと頻度を生成するリンク　オプションに応答する。施設所有者がクリックすると、スマート暗号システムサービスプログラムがアカウントを使用して、この人の登録記録があるかどうかを判断し、そうでない場合は、暗号モジュールと頻度を自動的に作成して生成し、新しい暗号を施設所有者に送信する。同時に、元の施設管理システムで所有者の施設暗号を更新する。施設の所有者は、スマート　暗号を有効にした後、クリア　暗号　モジュール／変更頻度コマンドをインスタント　メッセージング　ロボットに送信することもできる。操作は上記よりも複雑で、明確なセマンティクスを知る必要がある。クライアントレス　対象デバイスの自動登録は上記

と同じである。
【００４０】
本発明の実施例による、管理ユーザとノード、施設、およびアカウントと多対多の関係を有し、ノード、施設、およびアカウントは関連付けることができ、またはセンター間でさえ関連付けることができる。
【００４１】
本発明の実施例による、暗号センターの暗号生成プログラムは時限タスクであり、ユーザーが設定した暗号　モジュールに従ってセンターデータベースに記録された有効なノード、施設、およびアカウントの暗号を生成し、次の値を計算。変更頻度に応じて変更時期を設定し、送信利用者は、暗号変更前にノード、施設、アカウントの管理者に通知するなど、必要なリマインダー情報を送信し、手動での介入が必要な場合に変更に備える。暗号生成プログラムには、ローカル施設およびローカルに到達可能なノードと施設の暗号を変更する機能があり、指定された時間枠でローカル施設の暗号とリモートで到達可能な　（たとえば、配置済みの　ｓｓｈ　証明書信頼）　ノードおよび施設の暗号をネットワーク内で直接変更できる。
【００４２】
本発明の実施例による、前記暗号変更モジュール、暗号変更頻度、変更される暗号、および現在の暗号は、前記ユーザー端末または許可された対象デバイス／施設によって照会されるか、または前記暗号センターサーバーが積極的にリマインダを送信する。関連情報は、ユーザー端末または対象デバイス／施設によってアクティブに照会できる。または、変更の時間枠に入ると、暗号センターサーバーは、所有者の事前定義／システムデフォルトの方法に従って、ユーザー端末または対象デバイス／施設に送信し、変更予定または変更済みの状況を知らせる。
【００４３】
暗号センターのＷＥＢサーバーにポーリングし続けるクライアントは、暗号変更時間帯に入ると暗号変更を実行し、その結果を暗号センターとユーザー管理に知らせる、ログにも書き込める。需要が高くセキュリティの高いシステム　（ノード、施設）　に対して、複数の暗号化センターをポーリングして、暗号検証、暗号合成、および暗号スプライシングを実現できる。通知時には、さまざまな通知方法と通知対象を使用し、セキュリティを確保できる。同時に、受信した情報の長期的な可視性を回避するために、読み取り後書き込みモードをオンにすることをクライアントに通知する。
【００４４】
スマート暗号センターは、暗号所有者の介入なしに暗号変更を実現し、暗号に関する情報システムのセキュリティ要件を満たす。エイリアスなどの階層的なコンテンツ通知と複数の通知方法の混合使用により、セキュリティを確保する。たとえば、メッセージの返信は　４　つのレベルに分けている（施設アカウントはエイリアスを使用でき、別のメッセージチャネルを介して送信することもできる）。
【００４５】
最初のレベルは現在の暗号のみを返信する、
第　２　レベルは現在の暗号　＋　有効期限を返信する、
第　３　レベルは、現在の暗号　＋　有効期限　＋　暗号モジュール　＋　変更頻度を返信する、
第　４　レベルは、現在の暗号＋　有効期限　＋　暗号モジュール　＋　変更頻度　＋　特定の　ＡＰＩ　パラメータを返信する。
エイリアス制：　実際の施設とアカウントはエイリアスに置き換えられ、メッセージ返信の最初の　２　レベルに反映される。
【００４６】
本発明の実施例による、マルチチャネルメッセージ応答方法を採用することができ、メッセージチャネル、電子メール、インスタントメッセージング（プライベート、パブリック）、ショートメッセージ、音声通話、およびその他の方法の組み合わせを使用することができる。

【００４７】
スマート暗号センターの暗号モジュールを決定するには２つの方法がある、１、所有者が頻度を含む正確な暗号モジュールを入力する、２、頻度に応じて最終的な暗号モジュールをランダムに生成する。最終的に３種類の暗号がある。１　種は暗号モジュールを使用せず、ランダムな暗号を直接生成する、残り２種の暗号は暗号モジュールに基づいている。１　つは暗号モジュールに従って同じ形式の最終暗号を生成する。もう一つは前述の最終暗号の文字順番を乱す。
【００４８】
対象デバイス／施設が２つの暗号センターから変更暗号を取得する必要がある場合、検証が必要な場合は、２つの暗号センターに同じ正確なモジュールと変更頻度を設定する必要がある。スプライシングで取得した変更暗号なら、任意のモジュールを設定できる。対象デバイス／施設クライアントプログラムアプリケーションの暗号変更は、クライアントプログラム内で実行できる。一部の施設では、暗号を変更するために別のプログラムが必要である。クライアントプログラムは、暗号を変更するために他のプログラム／スクリプトの変更暗号を出力できる。
【００４９】
ユーザー管理は、暗号センターのインスタントメッセージング　サーバーとやり取りして、暗号モジュールと変更頻度を設定および照会し、ＷＥＢ　サーバー管理プログラムまたはモバイルＡＰＰ　クライアントを通じて管理することもできる；　クライアントと暗号センター間のやり取り少なくとも　２　層の対称暗号化通信を採用し、内側層には、暗号モジュール、変更頻度、現在の暗号、経過時間などを含む、ノード施設の特定の通信コンテンツを含む。外側層には、タイムスタンプ、ユーザー管理アカウント、通信タイプ（登録／ポーリング／プッシュ／ワンキー　ログインなどの使用）　、内部の暗号化された文字列を含む。
【００５０】
典型的な　２　層暗号化では、外側層の暗号化は一般に暗号化センターの特定のキーを採用し、内側層の暗号化はノード、施設、アカウント固有のキー、または暗号化の特定のキーと組み合わせたものです。また、通信要件は、永久トークン、時間トークン　（時間または日で置き換えられる）、および分トークン　（１　分ごとに置き換えられ、数分間有効）　の　３　つのカテゴリに分けることができる。上記対象デバイス／施設をプッシュ通信対象とする特定鍵トークンは、対象デバイス／施設から発行される。
【００５１】
完全な情報が低レベルで表示されないことを除いて、情報を簡素化し、適切に機密に保つために、ノード、施設、およびアカウントにエイリアスを設定できる。
【００５２】
既存の情報システムにおけるスマート暗号センターとユーザー／暗号管理の関係：　共存し、相互に切り替えることができる。アプリケーションシステムを例にとると、スマート暗号センターを介して暗号をリセットすると、新しい暗号がリセットされる　（指定された暗号　モジュールを押すたびに、変更後の暗号　（変更頻度）　がシステムに更新され、システム内の独自の暗号変更機能を介して暗号を変更した後、スマート暗号内の施設の暗号変更機能センターは無効になり、スマート暗号は引き続きいつでも使用できる。センターの暗号をリセットする。他のアプリケーションシステムでも同じ効果が得られるが、必要に応じて関連するインターフェイスをカスタマイズする必要がある。
【００５３】
携帯電話、タブレット、個人の　ＰＣ　などの個人および家族のミニデバイスのみが使用できるほど小さい場合もあれば、あらゆる規模の組織／企業で使用する場合もある。ルーターやＮＡＳサーバー、専用サーバー上での運用も可能で、各種クラスタ、ディザスタリカバリ、マルチセンターモードでの構成も可能スマート暗号センターは利用可能自作の通信プラットフォーム　（インスタント　メッセージングまたは　ＳＭＳ）、またはパブリックＡＰＩ　機能を備えたインスタントメッセージング　プラットフォームの場合、必要に応

じてＷｅｂ　サーバーを構成するかどうかを決定する。通常、既存のシステムを適切に拡張すれば、スマート暗号センターの特性を持ち、対応する方法でサービスを提供できる。

【００５４】

暗号センターサーバーが信頼されている場合、たとえば、ユーザー端末が属するデバイスがローカル暗号センター　（つまり、ローカルサーバー）　を持っている場合、ユーザー端末に適用されたスマート暗号実現する方法は、ローカルによって実行できる。暗号センターを作成し、結果とログを後で参照できるように記録し、対象デバイス／施設へのワンクリックログインを実現できる。

【００５５】

暗号センターサーバーを利用者端末と同一上に設置することで、ユニット・組織・グループ・エリアネットワーク内の対象デバイス／施設全てを管理する全利用者向けの暗号センターとデータを同期し、個人のスマートアカウントセンター、および対象のデバイス／施設へのワンクリック　ログインを実現する。操作に関しては、通常の操作は、最初にリモート暗号センターに送信されるだけでなく、ローカル暗号センター　（つまり、ローカルサーバー）　にも保存され、その後、ローカル　暗号センターを選択してプッシュすることができる。編集および更新のための以前の設定を確認または呼び出すための情報、および同時に受信した通知は、ローカルの暗号センターにも保持される。ローカル暗号センターは、リモート暗号センター、対象／施設を追加するか、既存の暗号センターをクリックして対象デバイス／施設を追加することができる；　リモート暗号センターの信頼レベルを表示し、その関連情報を表示することができる。たとえば、コンピューターまたは自宅の暗号センターの同期ステータスが携帯電話に表示される。

【００５６】

対象デバイス／施設が属する機器に暗号センターを構築すると、対象の・設備に適用されたスマート暗号実装方式を暗号センターで実行し、結果やログを記録して今後の参考にすることができる。

【００５７】

本発明の実施例の実施プロセスは以下の通りである。

１）　既存環境の評価、暗号センターの仕様の決定、既存のデータベースを使用するか、新しい独立したデータベースを作成するかの決定、暗号センターで使用される暗号モジュールの仕様、暗号の変更頻度の仕様、および管理者との通信の仕様の決定ユーザーとクライアントを確認し、暗号センターキーを決定する。

２）　安全性と標準化の計画と対策を評価する、実装プロセス全体でリスク要因を評価する、実装プロセス全体で計画と対策を決定する、実装されたシステムが強力で効果的であることを確認する。例えば、機器のダウンタイム／シャットダウン、デバイスの時差、サービスのシャットダウン／異常、ネットワークの変動と切断、人間の不適切な操作による暗号変更の失敗、さまざまな偽造や攻撃の可能性などを考える。重要なシステムでは、暗号の変更がシステムの通常の運用に影響を与えないように、リスク評価と開発仕様を特に強調する必要がありる。変更の頻度を評価することにより、３　つの時間枠と１　つの拡張情報入力制限が許可される。指定された時間枠で暗号を変更し、指定された時間枠で暗号センターにアクセスし、指定された時間枠で暗号を使用し、指定されていない地域／ネットワークアドレスからの暗号センターおよび指定ノード施設へのアクセスを制限する。

３）　暗号センターのデータベースを作成する。ルーターや　ＮＡＳ　などの小規模な設備を使用する必要がある場合を除き、既存のデータベースを使用することをお勧めする。少なくとも、ユーザー管理テーブル　（既存のユーザー辞書テーブルを使用して、既製の階層と権限定義を使用することをお勧めする）、暗号モジュール／変更頻度テーブル、および暗号変更ログテーブルを含む。

４）　暗号生成および変更プログラムを作成する、暗号センター　データベース内の有効なレコードをトラバースし、各レコードの暗号モジュール／頻度に従って次の変更時間を計算する　（仕様のデバッグと変更には長い時間がかかる）。時間枠に入ったときに新しい暗号を生成し、暗号モジュール／頻度テーブルと暗号変更ログテーブルを更新する、ユ

ーザー管理に、ローカルノード施設とリモートアクセス施設　（異なるタイプのノード）の暗号を直接変更できることを知らせる。異なる施設では、異なる変更方法が必要になる）。

５）入力、クエリ応答、および通知を実現するため、暗号センター管理プログラムを作成する、ノード、ファシリティ、アカウント、およびそれらの暗号テンプレート／変更頻度の設定をユーザー管理に許可する、変更の頻度は個別に変更できるが、暗号テンプレートとの互換性が必要である。例えば、年月によるモジュールの変更頻度に、時刻修飾詞が出現しても意味がない、管理プログラムは、情を受信の　２　層の復号化と情報送信の　２　層の暗号化が含まれる、ノードキーと暗号化センターキーをそれぞれ使用する。

６）　クライアントプログラムを作成する、独自のクライアントノードキーを生成し、ノード登録要求、暗号クエリ、暗号更新を実現し、複数の暗号センターに対して暗号比較、暗号マージ／スプライシングなどの機能も備えている。クライアントコードは、暗号センターの通信プロトコルと一致している。オペレーティングシステムが異なれば、クライアントの実装方法も異なる。たとえば、Ｗｉｎｄｏｗｓ　では、使いやすさと互換性を確保するためにＣ　＋＋　プログラミングを使用すること、ｏｐｅｎｓｓｌ／ｃｕｒｌ　などのライブラリを直接コンパイルすること、および暗号の変更は、暗号のリセットではなくｃｈａｎｇｅ　を使用することをお勧めする。Ｗｉｎｄｏｗｓ　以外のシステムと異なり、開発仕様で決定されるが、暗号センターとの通信は、同じ暗号化／復号化仕様に準拠する必要がある。暗号変更をクライアントプログラムから直接実行するか、外部プログラムを呼び出して実行するかは、施設の種類によって異なる。たとえば、通常、オペレーティングシステムは、クライアントプログラムから直接暗号変更を実行する。汎クライアントと呼ばれる理由は、機能の複雑さがさまざまな種類のノードを作成するため。　機能にはさまざまなクライアント　コードと変更方法が必要だが、変更暗号を取得するプロセスは同じである。

７）　インスタントメッセージングサーバーサービスプログラムを作成する、ｘｍｐｐロボットなどのプライベートプログラム、オープンソース　ＳＭＳ　サーバー、ＡＰＩ　インターフェイスを備えたパブリック　インスタント　メッセージング　サービスを使用するために登録する。

８）　共同デバッグ　テスト、対象デバイス／設備が正常に登録されていること、暗号モジュール／暗号変更頻度の設定が正常であること、暗号の生成と変更が正常であること、ユーザー端末のクエリと受信通知が正常であること、および対象デバイスが正常であることを確認する。　／ｆａｃｉｌｉｔｙ暗号は正常に自動的に変更される。つまり、最初の目的は達成された。その後、連携の変更とマルチセンター機能を追加し、それらを　１　つずつテストし、さまざまな施設、アプリケーション、サービスなどに徐々に拡張できる。一般化を達成する。

９）　セキュリティテスト、異常入力、脆弱性スキャン、および侵入テストを含むがこれらに限定されない；　冒頭で述べたリスク評価で考えられるさまざまな異常状況への適応性を含むがこれらに限定されない。

１０）　縮小と拡張、連携変更の典型的なケース：　データベース接続、データベースバックアップ、データベース監視、データベース　クラスタ、およびデータベースとアプリケーション　サーバーでの災害復旧　データベース　ユーザーの暗号が変更された場合、後者の　３　つの暗号に関連する暗号を変更する必要がある。クラスターおよびディザスター　リカバリー環境での暗号の変更は、より複雑である。

【００５８】

図２に示されるように、本発明の実施例では、スマート暗号を実現するための方法を提供する、以下の手順で実施できる：

【００５９】

３０１、ユーザ端末は、管理要求情報を暗号センターサーバに送信する。ここで、管理要求情報は、暗号変更要求、暗号変更モジュール設定、および暗号変更頻度設定を含む。

管理要求は　２　つのカテゴリに分類できる。１　つは暗号のモジュールと頻度に直接関

連するもので、もう　１　つは次のような暗号の使用制御です。アドレスと指定された時間の使用）、これらの　２　つの機能は、データベースなどの／施設管理の協力を必要とし、達成するためにアカウントをロックおよびロック解除することができる；　２）　リモートコントロールを要求する。指定されたアドレスを開閉できるリモート制御、これにはリモート制御ソフトウェアのサポートが必要だ、この形式は　％Ｒ１９２．１６８．１００．１００：５１２３４　の可能性がありる；　３）　現在の暗号ロックと同様に、指定された／設備の暗号を管理する権限を他のユーザーに付与する；　４）　組織の上位者は、下位の特定の／設備を管理できる。タイムアラインメントやタイムウィンドウなどの従来の管理要求は上記の最初のカテゴリに属し、たとえば次のような記述「％ｒ　は毎回生成される暗号を再び乱れ、推測できないようにする」など；　５）　有効化／非暗号　ログインを無効に。現在、非暗号ログイン　（指紋／虹彩／スワイプ　フェイス、関連付けられたログイン／シングル　サインオンなど）　は、暗号ログインと制限関係を持たない可能性がある。暗号センターは制限関係を追加できる。追加のセキュリティを確保し、必要に応じて機会に会う。時間枠と組み合わせることで、セキュリティはより高くなる。このスマート暗号システムによって制限関係を実現する利点は、ユーザーが特定の施設に触れる必要がない。

【００６０】

　３０２、前記暗号センターサーバーは、前記暗号変更モジュール、暗号変更要求、または暗号変更頻度に従って、変更される暗号を生成し、暗号センターサーバーは、前記変更される暗号、暗号変更要求に従って、対象のデバイス／施設を生成する、または暗号の変更頻度暗号センターサーバーは、ユーザーの要求に従って意味分析を実行し、あいまい入力用の特定の暗号モジュールを生成し、モジュールのセマンティクスを満たす正確な暗号モジュールを直接入力するために利用可能な暗号モジュールを決定する、ランダムな暗号の場合は直接生成され、残りの場合、変更される暗号は、暗号変更モジュールに従って暗号生成プログラムによって生成される。

【００６１】

　３０３、前記暗号センターサーバーは、変更される情報に従って前記対象のデバイス／施設の暗号変更操作を実行するか、または暗号センターサーバーが変更される情報を対象デバイス／施設に提供し、対象デバイス／施設が変更を実行する。変更される情報に応じた暗号変更操作；一部の対象デバイス／施設は、リセット操作の代わりに変更操作を確実に実行できるようにするために、登録時に保存された元の暗号を解読する必要もある。いくつかの実施形態では、前記変更される情報の提供する方法には、前記対象デバイス／施設が暗号　セントラル　サーバーをポーリングして変更する情報を取得するか、暗号セントラルサーバーが変更する情報を対象デバイス／施設に送信する、を含む。

【００６２】

　複数の前記暗号センターサーバーがあり、それぞれが固有の暗号センター識別コードを持ち、複数の暗号センターサーバー間でデータの同期と情報プッシュが実行される。暗号センター　サーバーは、単一のサーバーまたはサーバー　クラスターである場合がある。サーバー　クラスターの場合、各サーバー　クラスターには独自の暗号センター識別コードがあり、複数のサーバー　クラスターがデータの同期と情報のプッシュを実行する.

【００６３】

　複数の暗号センター　サーバーをデータ共有や災害復旧に使用でき、各暗号センターサーバーは暗号センター信頼テーブルを維持し、信頼できる暗号センターサーバー　（ローカル　サーバーなど）　はリモートの暗号センターサーバーとデータを同期できる。スマートアカウント管理やワンキーログインなど、ユーザーにとってより便利な機能を提供する。たとえば、アカウントと暗号を複数のブラウザーに保存する必要はなく、アカウントと暗号を直接送信することができる　（スマート　暗号を使用してシステムによって生成される暗号は、特に一般的に使用されるいくつかの暗号を除いて、基本的に非常に複雑です）。それらのほとんどはライブで覚えておくべきではない。現時点ではワンキー　ログインが非常に必要である。ワンキー　ログインのもう　１　つの意味は、暗号センター間のセッション共有を通じてシングル　サインオンを実現すること）。暗号を直接。また、同一端

末に暗号センターを搭載した利用者端末を紛失・盗難にあった場合、破壊プログラムを起動し、暗号センター情報のセキュリティを確保することができる。

【００６４】

２　つの暗号センター間で変更する情報をプッシュすることの特別な意味：　１　つの暗号センターが、変更する情報を対象　デバイス／機能にプッシュする．　対象　デバイス／機能にも暗号センターがある場合、３　つの状況がある。当事者の暗号センターが直接変更を実行し、変更された暗号は暗号化された暗号にすることができる；　２つ目は、変更情報が対象のデバイス／施設の暗号センターに入りるが、変更されない。　３つ目は、プッシュされた変更情報に暗号モジュールと変更頻度を含む、対象デバイス／施設の暗号センターに入る。初めてプッシュされると、対象　デバイス／施設の暗号センターが変更をトリガーする。プッシュ結果は検証と更新として使用され、データ共有と増分災害復旧の効果を実現する。３　つの状況は、信頼の程度の明らかな違いを反映している。最初の状況はまったく信頼していない。３　番目の状況は完全な信頼だ。暗号変更要求は、ユーザーが暗号変更頻度に従わずに直接変更を要求する状況である可能性があるが、この時点でも頻度はスマート暗号の特性を反映するために関連する役割を果たすことができる。例えば交換のリマインダーに使用するなど。

【００６５】

対象デバイス／設備は暗号センターサーバー上で変更する情報をポーリングにより取得し、暗号センターサーバーはプッシュにより対象デバイス／設備にプッシュすることもできる。これらの　２　つの形式は、信頼の程度と統合の難しさに依存する．　暗号センターに完全な信頼がある、統合が便利な場合、それはサーバーに属する、特に同じ人によって開発および管理されている場合は、暗号センターが直接実行するのは比較的簡単だ、対象デバイス／施設のポーリングは、クロスプラットフォーム、クロスデバイス／施設タイプ、クロスネットワークなど、より優れた柔軟性を備えているか、生成された暗号またはニーズに対するさらなる処理要件を備えている。管理コマンドを実行するため、またはサーバーとして使用する必要がない。暗号センターが直接実施する場合でも、マザーボード上のＵＥＦＩ　ＢＩＯＳの暗号変更など、対象デバイス／施設の条件によっては非常に煩雑になる場合があり、暗号センターにこの要件がある場合、具体的な変更実施は、また、特別なインターフェイス　プログラムを介して実行される。また、暗号センターが大量の変更タスクを実行する場合は、キュー　メカニズムを有効にして、処理用に別のキュー　ハンドラを用意する必要がある場合がある。また、実際にポーリングやプッシュをどのように選択するかは、セキュリティの境界にも関係しており、たとえば、暗号センターは変更情報を大規模なソーシャル、メディア、その他のプラットフォームにプッシュが、これはまったく異なるセキュリティ分野だ。

【００６６】

３０４、前記暗号化センターサーバーが変更フィードバック情報を生成するか、または前記対象デバイス／施設が変更フィードバック情報を暗号化センターサーバーに送信する。前記変更フィードバック情報は変更結果を含む。

【００６７】

３０５、暗号化センターサーバーは、前記変更フィードバック情報を前記ユーザー端末に送信する。

【００６８】

図３に示すように、本発明の実施例で提供されるスマート暗号実現装置は、暗号セントラルサーバーに適用され、

管理要求情報取得モジュール４０１は、ユーザー端末１０から送信された管理要求情報を取得するように構成され、前記管理要求情報には、暗号変更要求、暗号変更モジュール設定、および暗号変更頻度設定が含まれる、

変更情報生成モジュール４０２は、前記暗号変更モジュール、暗号変更要求、または暗号変更頻度に従って、変更される暗号を生成し、前記変更される暗号、暗号変更要求、または暗号変更頻度に従って、対象デバイス／施設の変更される情報を生成する、

暗号変更実行モジュール４０３は、変更される情報に従って対象の装置／施設の暗号変更動作を実行するか、または対象の装置／施設が暗号変更操作を実行するための保留中の変更情報を対象デバイス／施設に提供する、
サーバフィードバック取得モジュール４０４は、変更フィードバック情報を生成するため、または前記対象デバイス／施設から送信された変更フィードバック情報を取得するために使用される、前記変更フィードバック情報は変更結果を含む、
サーバフィードバック送信モジュール４０５は、前記変更フィードバック情報を前記ユーザ端末に送信するように使用される、を含む。

【００６９】

図４に示すように、本発明の実施形態で提供されるスマート暗号実装デバイスは、ユーザー端末に適用され、
管理要求情報送信モジュール５０１は、前記管理要求情報を暗号センターサーバーに送信するように構成され、管理要求情報は、暗号変更要求、暗号変更モジュール設定、および暗号変更頻度設定を含み、暗号変更モジュール、暗号、変更要求または暗号変更頻度は、変更する暗号を生成するために暗号　セントラル　サーバーによって使用され、変更される暗号、暗号変更要求または暗号変更頻度は、暗号　セントラル　サーバーによって使用され、対象のデバイス／機能を生成。変更される情報、変更される情報は、暗号センターサーバーによって、対象のデバイス／施設の暗号変更操作を実行し、変更フィードバック情報を生成するために、または対象のデバイス／施設が暗号変更操作を実行し、変更を送信するために使用される。暗号センターサーバーから情報を取得した後、暗号センターサーバーへのフィードバック情報　変更フィードバック情報には、変更結果が含まれる、
端末フィードバック取得モジュール５０２は、前記暗号化センターサーバーによって送信された変更フィードバック情報を取得するために使用される、を含む。

【００７０】

図５に示すように、本発明の実施形態で提供されるスマート暗号実装デバイスは、対象／施設に適用され、
変更情報取得モジュール６０１は、暗号センターサーバーによって提供される変更情報を取得するために使用され、変更情報は、暗号センターサーバーから対象デバイス／設備をポーリングすることによって取得されるか、暗号センターによって送信される。暗号の変更、暗号変更要求、または暗号変更頻度、変更される暗号は、暗号変更モジュール、暗号変更要求、または暗号変更に従って、暗号センターサーバーによって生成される。ユーザー端末から暗号センターサーバーに送信される頻度、暗号変更モジュール、暗号変更要求、または暗号変更頻度、
変更実行モジュール６０２は、変更対象情報に従って暗号変更操作を実行するように使用される、
デバイスフィードバック送信モジュール６０３は、変更フィードバック情報は、前記ユーザー端末に送信するために暗号化センター　サーバーによって使用され、変更フィードバック情報は変更結果を含む、を含む。

【００７１】

図６に示すように、いくつかの可能な実装方法では、本発明の実装方法による電子デバイス７０は、少なくとも１つのプロセッサ７０１および少なくとも１つの記憶装置７０２を含む。前記記憶装置７０２は、少なくとも１つのコンピュータプログラム７０３を格納し、前記コンピュータプログラム７０３が前記プロセッサ７０１によって実行されると、前記プロセッサ７０１は、本明細書の上記の技術的解決法に記載された本願による様々なプログラムを実行する。

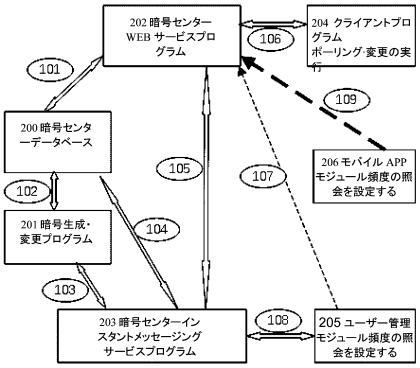
【００７２】

いくつかの可能な実施形態では、本発明の様々な態様は、コンピュータプログラムが格納されたコンピュータ可読媒体として実装することもでき、前記コンピュータプログラムが電子デバイスのプロセッサによって実行されると、それを使用して実現する本願の様々な具体的な実装による技術的解決策に記載された方法における上述の手順である。

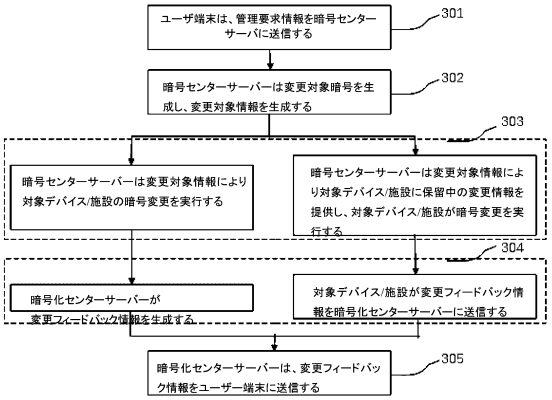
【００７３】
説明したいのは、上記の媒体は、読み取り可能な信号媒体または読み取り可能な記憶媒体であってもよい。可読記憶媒体は、例えば、電気、磁気、光学、電磁気、赤外線、または半導体システム、デバイス、またはデバイス、またはそれらの任意の組み合わせであり得るが、これらに限定されない。読み取り可能な記憶媒体のより具体的な例（非網羅的なリスト）には、１つまたは複数の導体との電気的接続、ポータブル ディスク、ハード ディスク、ランダム アクセス メモリ （ＲＡＭ）、読み取り専用メモリ （ＲＯＭ）、消去可能なプログラム可能な読み取り専用メモリ （ ＥＰＲＯＭ またはフラッシュメモリ）、光ファイバ、ポータブル コンパクト ディスク読み取り専用メモリ （ＣＤ－ＲＯＭ）、光記憶装置、磁気記憶装置、または上記の任意の適切な組み合わせ。
【００７４】
可読信号媒体は、可読プログラムコードをベースバンドで、または搬送波の一部として搬送するデータ信号を含むことができる。そのような伝播データ信号は、電磁信号、光信号、または前述の任意の適切な組み合わせを含むがこれらに限定されない多くの形態をとることができる。読み取り可能な信号媒体は、命令実行システム、装置、またはデバイスによって、またはこれらと組み合わせて使用するためのプログラムを送信、伝搬、または転送できる読み取り可能な記憶媒体以外の任意の読み取り可能な媒体であってもよい。
【００７５】
可読媒体に具現化されたプログラムコードは任意の適切な媒体によって送信できる。
無線、有線、光ケーブル、ＲＦなど、または上記の任意の適切な組み合わせを含むがこれらに限定されない。
【００７６】
本発明の動作を実行するためのプログラムコードは、Ｊａｖａ、Ｃ＋＋などのオブジェクト指向プログラミング言語、および従来の手続き型プログラミング言語を含む、１つまたは複数のプログラミング言語の任意の組み合わせで記述され得る。 「Ｃ」または同様のプログラミング言語など。プログラムコードは、完全にユーザ電子デバイス上で、部分的にユーザ電子デバイス上で部分的にリモート電子デバイス上で、または完全にリモート電子デバイスまたはサーバ上で実行することができる。リモート電子デバイスが関与する場合、リモート電子デバイスは、ローカルエリアネットワーク （ＬＡＮ） またはワイドエリア ネットワーク （ＷＡＮ） を含む任意の種類のネットワークを介してユーザー電子デバイスまたは外部電子デバイスに接続することができる。 （インターネット接続を介してインターネット サービス プロバイダーを使用するなど）。
【００７７】
当業者は、本発明の様々な態様がシステム、方法、またはプログラム製品として実施できることを理解することができる。したがって、本発明のさまざまな態様は、具体的には次の形式で実装できる。つまり、完全なハードウェア実装、完全なソフトウェア実装（ファームウェア、マイクロコードなどを含む）、またはハードウェアとソフトウェアの組み合わせ。本明細書では「回路」 、 「モジュール」 、または「システム」と呼ばれる。
【００７８】
上記具体的な実施形態は、本発明の保護範囲を限定するものではない。したがって、本発明の構造、形状、および原理に従って精神および原則内で行われる任意の修正、均等置換および改良等は、いずれも本発明の保護範囲に含まれる。

【図面】

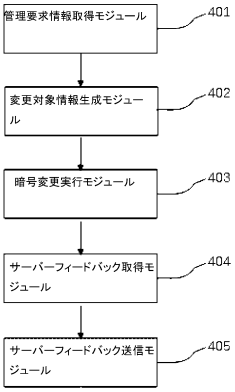
【図１】


202 暗号センター WEB サービスプログラム
204 クライアントプログラム ポーリング·変更の実行
106
101
109
200 暗号センターデータベース
206 モバイル APP モジュール·頻度の照会を設定する
105
107
102
201 暗号生成·変更プログラム
104
103
203 暗号センターインスタントメッセージングサービスプログラム
108
205 ユーザー管理モジュール·頻度の照会を設定する

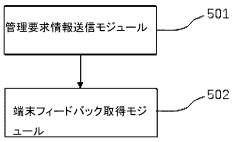
【図２】


ユーザ端末は、管理要求情報を暗号センターサーバに送信する
301
暗号センターサーバーは変更対象暗号を生成し、変更対象情報を生成する
302
303
暗号センターサーバーは変更対象情報により対象デバイス/施設の暗号変更を実行する
暗号センターサーバーは変更対象情報により対象デバイス/施設に保留中の変更情報を提供し、対象デバイス/施設が暗号変更を実行する
304
暗号化センターサーバーが変更フィードバック情報を生成する
対象デバイス/施設が変更フィードバック情報を暗号化センターサーバーに送信する
暗号化センターサーバーは、変更フィードバック情報をユーザー端末に送信する
305

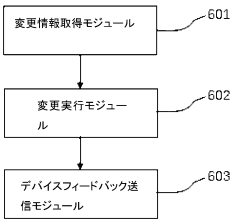
【図３】


管理要求情報取得モジュール
401
変更対象情報生成モジュール
402
暗号変更実行モジュール
403
サーバーフィードバック取得モジュール
404
サーバーフィードバック送信モジュール
405

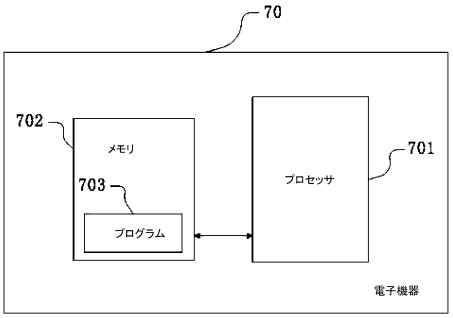
【図４】


管理要求情報送信モジュール
501
端末フィードバック取得モジュール
502

【図５】


変更情報取得モジュール
601
変更実行モジュール
602
デバイスフィードバック送信モジュール
603

【図６】


70
702
メモリ
703
プログラム
プロセッサ
701
電子機器

フロントページの続き

(56)参考文献　特表２０１９－５０５９４１（ＪＰ，Ａ）
特開平０９－２３１１７４（ＪＰ，Ａ）
特開２００５－１０７８０１（ＪＰ，Ａ）
特開２０１０－０９２１３４（ＪＰ，Ａ）
特開２０１７－１１１８０９（ＪＰ，Ａ）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／００，２１／３０－２１／４６