(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7559178号
(P7559178)

(45)発行日　令和6年10月1日(2024.10.1)

(24)登録日　令和6年9月20日(2024.9.20)

(51)国際特許分類

Ｈ０４Ｌ　9/32　(2006.01)	Ｈ０４Ｌ	9/32	１００Ｅ
Ｇ０６Ｆ　21/32　(2013.01)	Ｈ０４Ｌ	9/32	２００Ｚ
Ｇ０６Ｆ　21/44　(2013.01)	Ｇ０６Ｆ	21/32	
Ｇ０６Ｆ　21/60　(2013.01)	Ｇ０６Ｆ	21/44	３５０
Ｇ０６Ｆ　21/64　(2013.01)	Ｇ０６Ｆ	21/60	３６０

ＦＩ

請求項の数　3　（全14頁）　最終頁に続く

(21)出願番号　特願2023-179920(P2023-179920)
(22)出願日　令和5年10月19日(2023.10.19)
(62)分割の表示　特願2021-193218(P2021-193218)の分割
原出願日　令和3年11月29日(2021.11.29)
(65)公開番号　特開2023-176034(P2023-176034A)
(43)公開日　令和5年12月12日(2023.12.12)
審査請求日　令和5年10月19日(2023.10.19)

(73)特許権者　509185516
エイエスディ株式会社
東京都品川区東五反田１丁目１０番地７号
(73)特許権者　522465488
株式会社フィードバックコーポレイション
広島県広島市中区上八丁堀５番２５号
(74)代理人　100083884
弁理士　田中 昭雄
(72)発明者　清本 尚一
東京都品川区東五反田１丁目１０番地７号エイエスディ株式会社内
審査官　青木 重徳

最終頁に続く

(54)【発明の名称】　ブロックチェーンを利用したネットワークの認証システムとこれを使用した認証方法

(57)【特許請求の範囲】

【請求項１】

インターネットのエンドポイントにアクセスする際の利用者の本人認証を指紋認証付きICカードを用いた指紋認証により実施すると同時に、そのバックグラウンドでの認証処理として、利用者の直近のアクセス履歴をトランザクションとして管理、保管するブロックチェーンネットワークを設置し、前記エンドポイントの入口に認証エージェントを実装し、前記指紋認証付きICカードとブロックチェーンに夫々記録された直近のアクセス履歴を前記認証エージェント上で照合することによりサービスや業務システムへのアクセスを制御するようにしたことを特徴とする認証システムにおける

指紋認証付きICカードと認証エージェントとの間での安全なデータの送受信を可能にするための暗号化・復号化に利用する共通鍵を前記指紋認証付きICカード内部のメモリと前記認証エージェントに接続された個人情報データベースとに記録すると共に、利用者のアクセス履歴が書き込まれたトランザクションを複数のブロックチェーンネットワークの複数のノードに前記認証エージェントから配信する際、トランザクションの配信元の認証と配信の転送路上でのデータの改竄が無かったことを検証するために必用な公開鍵暗号化方式の秘密鍵を指紋認証付きICカード内部のメモリに、またそのペアとなる公開鍵を前記認証エージェントに接続された個人情報データベースに記録して新規利用者の登録と指紋認証付きICカードの発給を実施して利用者のアクセス権の正当性とエンドポイントの真正性との相互認証を指紋認証付きICカードと認証エージェントとの間で検証することを特徴する認証システム方法において、

ステップ１では指紋認証付きICカードの指紋認証により、カード外部との通信を許可し、認証エージェントにアクセスし、
ステップ２では、認証エージェントは個人情報データベースより共通鍵を得、この共通鍵をベースとして指紋認証付きICカードと認証エージェントとの真正性を相互に認証すると共に、テンポラリーにセッションキーを生成し、通信上でのセキュリティを確保し、
ステップ３では指紋認証付きICカードに記録された秘密鍵及びアクセス履歴を夫々セッションキーにより暗号化して認証エージェントに送信し、認証エージェント側で復元する方法でデータを受渡しし、
ステップ４では認証エージェントにおいて指紋認証付きICカードから受信したアクセス履歴ハッシュ値の一半分（１／２）と個人情報データベースから得たアクセス履歴ハッシュ値の他の一半分と（２／２）を結合したトランザクションハッシュを用いて、ブロックチェーンより、トランザクション・レコードを得、このレコードに記録されたアクセス履歴のハッシュ値が前記ステップ３のアクセス履歴のハッシュ値に一致することを確認し、
ステップ５では認証エージェントが利用者のアクセス権の正当性を認めた事を新たなアクセス履歴としてトランザクションをブロックチェーンに配信し、他のノードの合意形成後に確定したトランザクションハッシュ値を用いて、新たなアクセス履歴ハッシュ値を得て、
ステップ６では新たに獲得したトランザクションハッシュ値の一半分を含む新たなアクセス履歴を次回のアクセス時の認証用として指紋認証付きICカードに送信し、指紋認証付きICカード内では、アクセス履歴を更新した後に保管の完了を認証エージェントに通知し、認証エージェントがそれを確認して、個人情報データベースの記録の中の直近のアクセス履歴のトランザクションハッシュ値の残りの一半分を更新した後に利用者に対してリモートからの作業が許可され、利用者によるサービスや業務システム204に対する作業が開始される認証方法。
【請求項２】
複数の業務システムのうち、特に重要な業務システムだけを他の業務システムと切り離してエンドポイントとし、その業務システムの入口に認証エージェントを設けて認証の制御を行う方式や、作業効率を高めるために関連する複数の業務システムをひとつのグループとし、このグループを一つのエンドポイントとして認証エージェントを設けてグループ内の業務システムを一括して認証を行う方式も実現可能なことを特徴とする請求項１記載の認証方法。
【請求項３】
利用者の真正性の認証と厳正なアクセス履歴の管理により保護されたブロックチェーンのトランザクションに、業務に係る契約書のドキュメント情報を当該トランザクションのデータ・レコードに追加して保管することによりハイセキュリティな署名付きタイムスタンプ機能を実現可能にすることを特徴とする請求項１記載の認証方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ブロックチェーンを利用したネットワークの認証システムとこれを使用した認証方法に関するものである。
【背景技術】
【０００２】
クラウドサービスの利用とテレワークの拡大により、企業のファイアーウォールの内側と外側の環境境界をデバイスが行き来することから、企業のIT環境において今や安全な場所はなくなりつつある。
【０００３】
実際、テレワークの間に流出した企業の暗証番号が、世界で900社（国内で38社）分、犯罪サイトに挙げられていることが2020年に8月に公表されており、またIPA（情報処理推進機構）「情報セキュリティ10大脅威2021」によると、企業における脅威としては、外部からのサイバー攻撃の他に内部不正による情報漏洩が上位にランクされている。

【０００４】
そこで、既に始まっている欧米での「取引先に対するセキュリティ対策の義務化」の流れを受け、「サプライチェーン管理」、「一般データ保護規則」等に対応する社内システムの見直しは、大企業に限らず中小企業にも待ったなしの課題となっており、業務システムにアクセスする際の厳格な認証が求められている。
【０００５】
一方、テレワークにおいて企業の業務サイトをアクセスする場合や、ネットワーク経由で電子取引を行うサイトなどのネットワークのエンドポイント（様々なインターネットのアクセス先の総称）が、犯罪者によって用意された偽のサイトであるといったフィッシング詐欺の脅威にも対策が求められている。
【０００６】
すなわち、ネットワークのエンドポイントの正当性の認証にも配慮した新しい相互認証のサイバーセキュリティが求められている。
【０００７】
図２に示したように従来の認証プロセスにおいては、利用者が社内システム200にリモートでアクセスするためのアプリS400を介してアクセスしS401、社内システム200から認証要求S402を受信し、自ら「ID・パスワード」を入力しS403、ログインS404し、社内システムのID管理データベース410を検索の上、入力されたID・パスワードの照合S407が実施され、OKの判定後に業務開始が許可されS408、利用者は作業を開始S409することが可能となる。
【先行技術文献】
【特許文献】
【０００８】
【文献】特開２０２０－１９０８６８
【文献】特開２０１９－８７５３
【発明の概要】
【発明が解決しようとする課題】
【０００９】
現在、社内の業務システムにアクセスする際や、ネットワーク経由で電子取引を行う場合に用意されているセキュリティ・ソリューションの本人認証手段は、ID・パスワードに依拠するものが殆どである（特許文献１，２）。
【００１０】
しかしながら、近時コンピュータの高速化に伴いID・パスワードにも際限なく複雑さが要求されており、ID・パスワードによるセキュリティ対策としての有効性は疑問視される状態にある。
【００１１】
しかも、ID・パスワードを記憶する面倒や、失念による人的ミスの誘発、更には、第三者による盗聴、流用など、絶えず「ハッキング」や「なりすまし」の脅威を意識させられるID・パスワードによる認証は破綻した状態にあると言わざるを得ない。
【００１２】
一方、身分証や金融系、交通系カードとして用いられる従来のICカードは、オフライン端末であり、内部データに対する秘匿性、機密性が高いし、内部データに対する外部からの攻撃による改竄、漏洩に対して堅牢な情報端末であるが、カード内の持主の登録済み指紋情報との照合によってのみ、ICカードとしての機能を発揮するように調整されている指紋認証付きICカードは、「スキミング」や「なりすまし」の心配も無くなり、セキュリティ上の安全対策としては有力な手段となる。
【００１３】
しかし、前出の指紋認証付きICカードを用いてネットワークのエンドポイントにアクセスする場合においても、繰返し同一のID・パスワードの入力が求められている以上、盗聴などの脅威に対して完全なセキュリティ対策になってはいない。

【００１４】
しかも、ネットワークのエンドポイントの正当性、真正性の確認は全く手付かずなため、偽のエンドポイントに誘導されてID・パスワードを盗まれる「フィッシング詐欺」などの犯罪を防止できない。
【００１５】
そこで、本願発明は上記の課題に鑑みてなされたものであり、ネットワークのエンドポイントへのアクセスに際して、ID・パスワードの入力を必要とせず、本人認証の正当性をアクセス先に保証すると共に、アクセス先のエンドポイントの真正性を保証する相互認証を実現する完全なサイバーセキュリティ対策を提供することを目的とする。
【課題を解決するための手段】
【００１６】
本発明は、ネットワーク上の様々なサービスや業務システム等のインターネットのエンドポイントにアクセスする際の利用者の本人認証を指紋認証付きICカード（Secure Finger ID card）（SFID）を用いた指紋認証により実施すると同時に、そのバックグラウンドでの認証処理として、前記利用者の直近のアクセス履歴をトランザクション（Tx）として管理、保管するブロックチェーンネットワークを設置し、当該エンドポイントの入口に認証エージェント（Authentication Provider Interface ）（API）を実装し、SFIDとブロックチェーンに夫々記録された直近のアクセス履歴をAPI上で照合することにより業務システムへのアクセスを制御するようにした認証システムにおいて、
SFIDとAPIとの間での安全なデータの送受信を可能にするための暗号化・復号化に利用する共通鍵を前記SFID内部のメモリと前記APIに接続された個人情報データベースとに記録すると共に、利用者のアクセス履歴が書き込まれたトランザクション（Tx）を複数のブロックチェーンネットワークの複数のノードに前記APIから配信する際、トランザクション（Tx）の配信元の認証と配信の転送路上でのデータの改竄が無かったことを検証するために必用な公開鍵暗号化方式の秘密鍵をSFID内部のメモリに、またそのペアとなる公開鍵を前記認証エージェントに接続された個人情報データベースに記録して、新規利用者の登録とSFIDの発給を実施して利用者のアクセス権の正当性とエンドポイントの真正性との相互認証をSFIDとAPIとの間で検証する認証システムとこれを使用した認証方法を提案するものである。
【００１７】
本発明ではSFIDが、ID・パスワードに代わり、利用者の業務システムへのアクセス権を認証する役割を果たす為に、SFIDの内部には、氏名または社員コードのような個人を特定するデータと共に、個人に紐付けされる固有の暗号鍵等、本人にも知らされない情報を予め記録、保存した状態で本人に発給され、その後にSFIDカードへの正確な指紋の登録に必要な操作方法の指示を対面またはリモートで受けながら指紋登録を実施する。
【００１８】
指紋が未登録のSFIDカードの発給後、本人の指紋を登録完了した事象が、社内システムに設置された「個人情報データベース」の当該利用者のレコードに「利用者の登録日」として記録され、同時に最初の「アクセス履歴」として当該ブロックチェーンの起点となる記録データ（一つのトランザクションに相当）が生成され、以後、当該ブロックチェーンに記録された「アクセス履歴」とSFIDに記録された「認証履歴情報」の照合により。利用者の当該業務システムへのアクセスが検証されることになる。
【００１９】
すなわち、本発明では、正当な利用者であることの本人確認のためにSFIDカードを付与し、当該利用者のネットワークのエンドポイントへのアクセス履歴を「トランザクション（Tx）」として記録、管理するブロックチェーンネットワークと、前記ICカードSFIDとブロックチェーンネットワークとの連携を仲介するAPIを当該エンドポイントに配備し、利用者によるエンドポイントへのアクセス履歴情報をAPIにおいて暗号化、復号化、集配信および検証を実施し、利用者のリモートワーク等のネットワークからのアクセスを認証および制御するものである。

【００２０】
さらに、本発明では当該最新のアクセス履歴情報を当該利用者のアクセスとその認証の実施の度に更新して、前記SFID およびブロックチェーンネットワークに秘匿し、それぞれAPIからの要求により集配信し、検証を行うことにより利用者およびエンドポイントの真正性の相互認証を実現するサイバーセキュリティの新たなインフラとなる。
【００２１】
本発明ではSFID、APIおよびブロックチェーン技術により利用者自身の指紋認証とエンドポイントへのアクセス履歴を用いた認証基盤（Finger Identity as a Service認証基盤）（以下FIDaaS認証基盤）が形成され、これにより利用者の正当性とネットワークのアクセスサイトの真正性とを相互に認証可能となる。
【００２２】
また、本発明によればネットワークのエンドポイントへのアクセスの際にパスワードの入力を必要とせずに上記の認証が行われるため、利用者がID・パスワードを記憶する面倒や、失念による人的ミスの誘発、更には、盗聴等による「ハッキング」や「なりすまし」を防止し、外部からのサイバー攻撃のみならず内部不正による情報漏洩に対する防御が可能となる。
【００２３】
なお、本発明では複数の業務システムのうち、特に重要な業務システム、例えばサイバー攻撃を受けた場合に事業に深刻な影響が及ぶような基幹システムだけを他の業務システムと切り離して独立したエンドポイントとし、APIを設けて認証を行うようにすることもできる。
【００２４】
また、本発明によれば作業効率を高めるために関連する複数の業務システムをひとつのグループとし、このグループを一つのポータルとしてのエンドポイントに対し認証エージェントを設けてグループ内の複数の業務システムを一括して一度だけの認証を行うようにするシングルサインオンと呼ばれるサービス形態を実現することもできる。
【発明の効果】
【００２５】
本発明によれば利用者の正当性とエンドポイントの真正性とを相互に認証でき、サイバー空間における厳正な認証インフラが実現可能となる。
【００２６】
また、本発明によれば、利用者の真正性の認証と厳正なアクセス履歴の管理により保護された当該ブロックチェーンのトランザクションは、完全な署名付きタイムスタンプとしての機能要件を満たす。そこで、業務に係る契約書等のドキュメント情報を当該トランザクションのデータ・レコードに追加して保管する等の付加価値の高いカスタマイズが提供可能となる。例えば、本FIDaaS認証基盤に接続し制御する業務アプリが、社内システムの中の資材管理システムの場合、受発注に係る契約のエビデンスをトランザクションに記録として残すことにより、受発注書データの改竄や削除の心配の無い安全な保管が可能となる。
【００２７】
更に、本発明ではSFIDにより利用者の真正性が認証され、またSFIDに書き込まれたアクセス履歴は、書き換えが不可能となり、欠損も起きないブロックチェーンのトランザクションに記載された内容と照合するため、業務システムサイトの真正性が認証され、利用者の真正性と業務システムサイトの真正性とを相互に認証でき、厳正な認証が可能となる。
【図面の簡単な説明】
【００２８】
【図１】この発明に係るFIDaaS認証基盤の構成を模式的に説明する図
【図２】この発明に係る従来の認証プロセスのシーケンスを説明する図
【図３】この発明に係るFIDaaS認証基盤における認証プロセスのシーケンスを説明する図
【図４】この発明に係るSCP01に従いSFIDカードとAPIとの相互認証方式を説明する図
【図５】この発明に係るFIDaaS認証基盤の仕組みと各データの相関を模式的に説明する図

【図６】この発明に係るFIDaaS認証基盤のブロックチェーンのデータ構造を示す図
【発明を実施するための形態】
【００２９】
以下、本発明に係るネットワーク上の様々なWEBサービスや業務システムのサイト等のインターネットのエンドポイントにアクセスする際の利用者の本人認証をSFIDの指紋認証を用いて実施すると同時に、利用者のアクセス履歴をトランザクションとして管理、保管するブロックチェーンネットワークを配備し、当該エンドポイントの前段に認証エージェント（API）を実装し、SFIDとブロックチェーンに夫々記録された直近のアクセス履歴を照合することにより業務システムへのアクセス権をチェックするようにしたサイバー・フィジカル・セキュリティを実施するための好適な実施形態について説明する。
【００３０】
図１は、FIDaaS認証基盤の一つの構成例を模式的に示したものである。
【実施例１】
【００３１】
図１に示されるように業務システム等のインターネットのエンドポイントにアクセスする際の利用者の本人認証を指紋認証付きICカード（SFID）を用いた指紋認証により実施すると同時に、そのバックグラウンドでの認証処理として、前記利用者の直近のアクセス履歴をトランザクションとして管理、保管するブロックチェーンネットワークを設置し、当該エンドポイントの入口に認証エージェント（API）を実装し、認証エージェント（API）に個人情報データベースを接続し、SFIDとブロックチェーンに夫々記録された直近のアクセス履歴をAPI上で照合、検証することにより業務システムへのアクセスを制御するようにしたことを特徴とする認証システムにおいて、SFIDにはAPIとのに共通鍵、前記ブロックチェーンネットワークで用いられる公開鍵暗号化方式の秘密鍵および当該利用者の直近のアクセス履歴を含むブロックチェーンのトランザクションのハッシュIDの前半分とアクセス履歴を記録し、個人情報データベースには前記共通鍵、秘密鍵を複合する公開鍵および前記トランザクションハッシュIDの後半分が記録されている。（図5参照）
【００３２】
上記認証システムについて、SFID110を身分証明書（例えば、社員証）として保有する利用者100（例えば、一部の選ばれた社員または取引先の社員）が、作業環境として用意された業務システム（例えば、社内システム200の中の製造システム204）にアクセスする場合を例にして、FIDaaS認証基盤の実施形態について図に沿って説明する。
【００３３】
従来の認証プロセスと異なる方式を採用したFIDaaS認証基盤における認証手順を、図１の製造システム204をエンドポイントとして、外部からのアクセスに対するセキュリティのために具備された認証エージェントソフトウェアであるAPI220とリモートで業務を実行しようとする利用者100の保有するSFID110との認証過程を図３に示す。
【００３４】
その認証工程はステップ１では、当該業務システムへのハッシュ値で表記されたアクセス履歴が書き込まれた指紋認証付きICカードの指紋認証により、カード外部との通信を許可して認証エージェントにアクセスし、ステップ２では、認証エージェントは個人情報データベースより共通鍵を得、この共通鍵をベースとして指紋認証付きICカードと認証エージェントとの真正性を相互に認証すると共に、テンポラリーにセッションキーを生成し、通信上でのセキュリティを確保し、
ステップ３では指紋認証付きICカード内に記録された秘密鍵及びアクセス履歴を夫々セッションキーにより暗号化して認証エージェントに送信し、認証エージェント側で復元する方法でデータを受渡しし、
ステップ４では認証エージェントにおいて指紋認証付きICカードから受信したアクセス履歴ハッシュ値の前半分（１／２）と個人情報データベースから得たアクセス履歴ハッシュ値の後半分と（２／２）を結合したトランザクションハッシュを用いて、ブロックチェーンより、当該トランザクション・レコードを得、このレコードに記録されたアクセス履歴

のハッシュ値が前記ステップ３のアクセス履歴のハッシュ値に一致することを確認し、ステップ５では認証エージェントが利用者のアクセス権の正当性を認めた事を新たなアクセス履歴としてトランザクションをブロックチェーンに配信し、他のノードの合意形成後に確定したトランザクションハッシュ値を用いて、新たなアクセス履歴ハッシュ値を得る。ステップ６では新たに獲得したトランザクションハッシュ値の前半分を含む新たなアクセス履歴を次回のアクセス時の認証用としてSFIDに送信し、SFID内では、アクセス履歴を更新した後に保管の完了をAPIに通知し、APIがそれを確認して、個人情報データベースの記録の中の直近のアクセス履歴のトランザクションハッシュ値の残りの一半分を更新した後に、利用者に対してリモートからの作業が許可され、以下、それぞれのステップを詳細に説明する。

【００３５】

ステップ１

図3の利用者100は、製造システム204に対するリモートでの作業を実施するためのアプリケーション・ソフトウェアを起動S150し、「STEP1」S10に記載されたSFID110の上に実装された指紋センサーを用いて指紋認証を実施することにより、カード外部との通信およびSFID110内部に保管されているデータの送受信を可能ならしめ、例えば社員コード（個人情報データベース260の262または図5のSFID110内のメモリ111に記録される個人情報112に含まれる）を送信する方式でAPIをアクセスする。

【００３６】

ステップ２

図3の「STEP2」S11は、SFID110とAPI220との相互の真正性の認証と、その後の相互のデータ通信上におけるセキュリティを確保するための処理を示す。

【００３７】

SFID110には、利用者100の個人情報と共に「共通鍵K0（図5のSFID110内のメモリ111に記録される113）」が、予め記録されて発行される。このSFID110と、個人情報データベース260より共通鍵K0265を読取るAPI220とが、この共通鍵をベースとして相互の真正性を検証すると共に、通信を実施する度毎に生成され、しかも一度きりの使い捨ての「セッションキーKS 」を用いることにより、通信上でのセキュリティを確保する。

【００３８】

SCPの説明

共通鍵をベースとした相互認証方式としては、ICカードの安全性管理システムの世界標準化組織である「globalplatform.org」で規定するSCP(Secure Channel Protocol) 01をベースとした認証スキームがあるが、以下、このスキームを利用する場合を例に説明する。

【００３９】

この認証方式の例を図4に示す。SFID110とAPI220とは、夫々共通鍵K0を保有S501し、認証を開始する際に夫々が16B（バイト）の乱数RapiとRsfidを生成し、例えば共通鍵K0で暗号化し、相手に送信するS502。両者は互いに受け取った乱数を４B単位に区切り、S503の配置規則に従い組み替えてテスト用の暗号文CRMを算出する。このCRMを共通鍵K0で暗号化してセッションキーKS とするS504。このKSを暗号鍵として乱数Rapi、Rsfidを暗号化して暗号文Capi、Csfidを算出し、相互に送信し、復号化することにより元の乱数に戻ることを確認する方法で、互いの真正性を検証すると同時に、SFID110とAPI220とは、このセッションキーKSを用いてデータの送受信を安全に実施することが可能となる。

【００４０】

ステップ３

図3の「STEP3」S12は、図５のSFID内のメモリ111に記録されたアクセス履歴を意味する｛TSi、TxHi(1/2)｝116、117および秘密鍵KB114を夫々セッションキーKS により、暗号化（各通信データをXで代表して記す。図５の10を参照のこと）し、API220に送信し、API側で復元する方法でデータを安全に送受信する。以下の数式（１）および（２

）にTSiの処理の例を示す。
（例） SFID ： Xi ＝ E (TSi 、KS) ・・・（１）
API ： TSi ＝E -1(X i 、KS) ・・・（２）
ここで添え字“ i ”は、利用者100の製造システム204のAPI220への直近の“ i番目 ”のアクセスであることを意味する。
【００４１】
前記数式（１）および（２）では、関数「暗号文＝E (平文、暗号鍵)」を意味する記号としてE、E の逆関数「平文＝E -1(暗号文、暗号鍵)」を意味する記号としてE -1を用いた。
【００４２】
ステップ４
図3の「STEP4」S221では、SFIDから受信したTxHi(1/2) 117と個人情報データベース260に記録されたTxHi(2/2) 266を連結して生成されるトランザクションハッシュTxHi12を用いて、ブロックチェーン・データベース351より、図５のトランザクション・レコードTxi13を得て、その中に記録されている当該利用者100すなわち社員コード122と当該SFID110の前回のアクセス履歴のハッシュ値H(TSi)を取り出して、「STEP3」S12で受信したデータTSiのハッシュ値を計算した結果との照合を実施する。すなわち、両者が一致すれば指紋認証で本人確認されたSFID110の正当な保有者は、真正性の認証を受けた製造システム204へのアクセス権の保有者であることが検証される。
【００４３】
ここで、記号H(X)は、データXを引数とするハッシュ関数を表し、その計算結果の値が「ハッシュ値」に他ならない。
【００４４】
前出の「TxHi(1/2) 117と個人情報データベース260に記録されたTxHi(2/2) 266を連結し生成する」ことの具体例を以下の数式（３）、（４）、（５）および（６）に示す。
TxHi ＝TxHi(1/2) ＋ TxHi(2/2) ・・・（３）
TxHi(1/2) ＝“ 6b88c87243aa29yfhhtdfh1d4rws2jb1 ” ・・・（４）
TxHi(2/2) ＝“ 2b67gg32hhjrvud3343421987wev4f32 ” ・・・（５）
TxHi ＝“ 6b88c87243aa29yfhhtdfh1d4rws2jb12b67gg32hhjrvud3343421987wev4f32 ” ・・・（６）
例えば、（４）および（５）のそれぞれ32Bのデータを結合して、（６）のように64BのTxHi12データとすることを意味する。
【００４５】
ステップ５
図3の「STEP5」S222では、前出の［００３９］に記載の「STEP4」S221の検証の結果、利用者100が正当なアクセス権の保有者であることが認められ、リモートでの作業が許可されるが、この事実は、この利用者100の次回のアクセスの際に検証用に必要となるアクセス履歴として記録を残さなければならない。そのために、図１に示したブロックチェーンネットワーク300に現在時刻に相当するアクセス履歴TSi+1のハッシュ値を含むトランザクションTxi+1（図５の15を参照）に、そのハッシュ値を公開鍵暗号方式により秘密鍵KBを用いて暗号化して得られるデジタル署名を付帯して配信する。複数のブロックチェーン・ノード（図１の351～353に当る）への「ブロードキャスト」とも呼ばれる。
【００４６】
トランザクションTxi+115を受けたブロックチェーン・ノードでは、受信したデジタル署名を秘密鍵KBに対応する公開鍵PKB（図５の個人情報データベース260の社員コード262）によって復号化し、TxHi+1のハッシュ値との一致を検証することにより、トランザクションの配信元が、公開鍵のペアとなる秘密鍵を有する者からの送信であることを認証し、ハッシュ値の一致から伝送路上でのデータの改竄が無かったことを検証する。
【００４７】
ブロックチェーンネットワークの説明
図１に示されているようにブロックチェーンネットワーク300におけるデータは、分散型

ネットワークを構成する複数のノード351～353に同期して記録される。ブロックチェーンを構成するデータ構造は、図６に示されるようにデータの送受信に係る出来事を一つの単位である「トランザクションTx13」として、更に、そのハッシュ値を「トランザクションハッシュID、TxH12」として付加し、一定期間に生起した複数のトランザクションTx13が集められ（図６の例では、8個のTxとしてD1～ID8を示す）、ブロックチェーンのプロトコルに従い暗号化してブロックの単位310（320、330および340も同様）にまとめられ、ノード間で、そのブロックの正当性を検証し合いながら記録をチェーン（鎖）のようにつないで蓄積する。図６の例では、「j+1」番目のブロック310のハッシュ値311が、「j」番目の情報から生成されるハッシュ値312を内包することがチェーン（鎖）構造の所以に当る。このチェーン構造により、トランザクション・データの改竄や削除は困難とされている。同時に、複数のノードで同期してデータが記録されることからデータのバックアップの機能も果たすことになる。

【００４８】

また、各ブロックのハッシュ値の計算にノンスと呼ばれる値をパラメータとして加えて、この値を調節することにより決められた条件に合致したハッシュ値を見出し、更に他のノードでの計算によっても当該ハッシュ値の結果が再現されることを追試することによって当該ブロックの正当性が合意形成されたとし、新たにTxHi+1を確定する。

【００４９】

即ち、前述の通り他のノードによりトランザクションTxi+1（図５の15）の正当性が追認されて初めて図６のブロック310の8個のトランザクションの一つとしてブロックチェーン・データベースに蓄積され、改めてTxHi+1（図５の14を参照）が検索可能となる。

【００５０】

なお、ブロックの蓄積が許可される従来の方式（例えば、仮想通貨ビットコインのブロックチェーンの場合）に対して、プライベート・ブロックチェーンの場合は、ハッシュ値の制限を緩め、条件に合致するパラメータ（ノンス）を高速且つ容易に発見出来る方式を採用することも出来る。

【００５１】

ステップ６

図3の「STEP6」S13では、新たに確定したTxHi+1の前半分(1/2)を含むアクセス履歴｛TSi+1、TxHi+1(1/2)｝115を次回のアクセス時の認証用としてSFIDに送信し、SFID内では、アクセス履歴115を更新した後に保管の完了をAPIに通知し、APIがそれを確認して、個人情報データベース260の記録の中の直近のアクセス履歴のトランザクションハッシュ値の残りの一半分266を更新した後に、リモートからの作業が許可され、利用者100による製造システム204に対する作業が開始S151される。

【００５２】

以上、この発明において特に留意すべきことは、図３に示された一連の認証処理のシーケンスにおいて、「STEP1」S10における指紋認証のみが利用者100が実際に行わねばならない行為であって、それ以降のリモート作業開始S151の許可が発行され、作業を開始するまでのプロセスは利用者の感知しないバックグラウンドにおいて、SFIDとAPIと当該ブロックチェーンネットワークとの間で自動的に処理が遂行されるという点である。すなわち、利用者100にとって負担となっていたID・パスワードの入力の手間はもちろん、それを記憶する負荷、失念や操作ミス、更には盗聴の心配も無くなる。

【実施例２】

【００５３】

図1に沿って説明した実施例１では、社内システムのうち、重要な業務システム、例えばサイバー攻撃を受けた場合に事業に深刻な影響が及ぶような基幹システム（例えば、図1の「製造システム」204）だけを他の業務システムと切り離してこの発明に係る認証基盤で管理する形態について説明した。

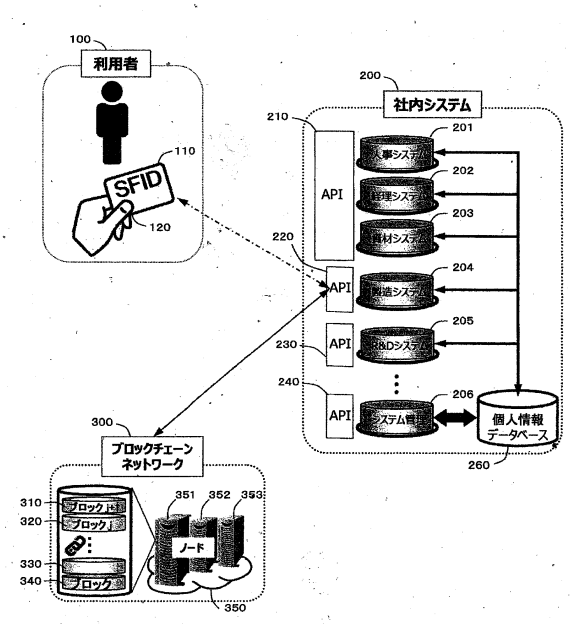
【００５４】

この場合は、特定システムへのアクセスを選ばれた社員のみにSFID（指紋認証付きICカー

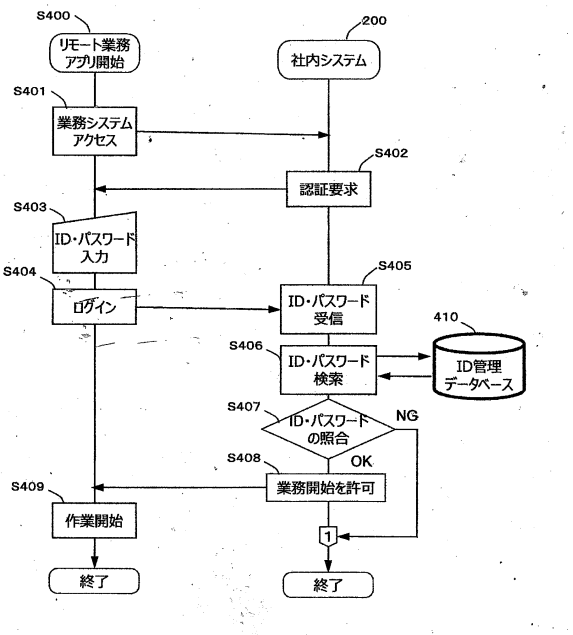
ド）110が発行、配布されて利用される。
【００５５】
上記と異なり、社内のシステムにおける作業効率を高めるために関連する複数の業務システムを一つのグループとし、そのグループに対してポータルとして統一した一つのアクセスポイントを定め、一つのAPI（認証エージェント）を実装することにより、グループ内のシングルサインオン（SSO）機能を構成、提供することができる。例えば、図１の人事システム201、経理システム202、資材システム203では、共通のAPI210によりアクセスの認証を管理する形態をとっている。すなわち、利用者100は、従来、別々のID・パスワードで管理される3つの異なるサービスを、SFIDカードを用いた一度の指紋認証により横断的な使用が許可される。
【産業上の利用可能性】
【００５６】
以上要するに、本発明によれば業務システム等のネットワークへのアクセスに際し、完全なセキュリティ対策が施され、且つ厳格な認証が行われるようなエンドポイントでの認証システムを提供できる。
【符号の説明】
【００５７】
１００　本FIDaaS認証基盤の利用者であり、社内システムの中の製造システムにリモートでアクセスする業務アプリの利用者
１１０　利用者の保有するSFIDカード（指紋認証付きICカード）
１１１　SFIDカード内のメモリ
１１２　SFID内のメモリに記録された、利用者の氏名、連絡先等の一般的な個人情報
１１３　SFID内のメモリに記録された、SFIDカードと業務システムのAPIとの間でデータを安全に通信するための共通鍵データ
１１４　SFID内のメモリに記録された、本発明のFIDaaS認証基盤で用いられる公開鍵暗号方式に必要な秘密鍵データ。社員コードに用いられる公開鍵と対になる。
１１５　SFID内のメモリに記録された、このSFIDの保有者が、業務システムをアクセスした直近のアクセス履歴
１１６　SFID内のメモリに記録された、このSFIDの保有者が、業務システムをアクセスした直近のアクセス時刻データ
１１７　SFID内のメモリに記録された、ブロックチェーン・データベースに記録された業務システムへの直近のアクセス履歴が書かれたトランザクションのトランザクションハッシュIDの前半のデータ
１２０　指紋照合を実施する指
２００　リモートアクセスを認める複数の業務システムを含む社内システムの全体
２０１　社内システムの中、リモートアクセスを認める人事システム
２０２　社内システムの中、リモートアクセスを認める経理システム
２０３　社内システムの中、リモートアクセスを認める資材システム
２０４　社内システムの中、リモートアクセスを認める製造システム
２０５　社内システムの中、リモートアクセスを認めるR&Dシステム
２０６　社内システムの中、リモートアクセスを認めるシステム管理業務を意味する。
２１０　社内システムの中、人事システム、経理システム、資材システムを一つの合同アクセスポイントとして扱い、アクセスを制御する認証エージェントソフトウェア（API：Authentication Provider Interface）
２２０　社内システムの中、製造システムへのアクセスを制御する認証エージェントソフトウェア（API）。本発明の実施形態の説明において例として言及
２３０　社内システムの中、R&Dシステムへのアクセスを制御する認証エージェントソフトウェア（API）。
２４０　社内システムの中、システム管理業務へのアクセスを制御する認証エージェントソフトウェア（API）。

２６０　社内システムにアクセスする全ての利用者の個人情報を記録、管理するデータベース
２６１　「個人情報データベース」の中、利用者の氏名、連絡先等の一般的な個人データ・レコード
２６２　「個人情報データベース」の中、社員コードを記録するレコードで、本発明のFIDaaS認証基盤で用いられる公開鍵暗号方式に必要なSFID内に秘匿される秘密鍵と対になる公開鍵を社員コードとして使用
２６３、２６７　「個人情報データベース」の予備のデータ・レコード
２６４　「個人情報データベース」の中、利用者のSFIDカードへの指紋登録を完了した時刻または利用者に業務システムへのアクセス権を登録した時刻のデータ・レコード
２６５　「個人情報データベース」の中、利用者のSFIDカードと業務システムのAPIとの間でデータを安全に通信するための共通鍵を記録するデータ・レコード。
２６６　「個人情報データベース」の中、ブロックチェーン・データベースに記録された業務システムへの直近のアクセス履歴が書かれたトランザクションのトランザクションハッシュIDの後半のデータが記録されるデータ・レコード
３００　ブロックチェーンネットワーク
３１０　ノードの一つに相当するブロックチェーン・データベース中の「Ｊ＋１」番目のブロック。ブロックは、番号の若い順から昇順に蓄積される。
３１１　ブロックチェーン・データベース中の「Ｊ＋１」番目のブロックを代表するハッシュ値
３１２ ブロックチェーン・データベース中の「Ｊ」番目のブロックを代表するハッシュ値
３１３、３１４　ブロックチェーン・データベース中の「Ｊ＋１」番目のブロックを構成する８個のトランザクション・データから成るハッシュ木（マークル木）とそのルートを示す。
３２０　ブロックチェーン・データベース中の「Ｊ」番目のブロック。
３４０　ブロックチェーン・データベース中の「新規利用者の登録時刻」または「SFIDカードへの指紋の登録完了時刻」を起点とするアクセス履歴が記録されるブロック。
３５０　ブロックチェーンのノード３５１、３５２、３５２が配置されたクラウド
Ｓ４００～Ｓ４０９　リモートアクセスの従来の認証プロセスのフローチャートの各処理工程を示す。
４１０　リモートアクセスの従来の認証プロセスに用いられるID管理データベース
Ｓ１５０　本発明の実施形態の例として、製造システムのAPIをリモートでアクセスする為のアプリケーション・ソフトウェア
Ｓ１５１　本発明の実施形態の例として、APIの認証を得て製造システムへのリモートワークを開始、実施工程を意味する。
Ｓ１０～Ｓ１３　本発明の実施形態の例として、製造システムのリモートワークを実施する際に要求される利用者のアクセス権とエンドポイントの相互認証をSFIDとAPI間で検証するプロセスの各処理工程を示す。
Ｓ２２１～Ｓ２２２　本発明の実施形態の例として、製造システムのリモートワークを実施する際に要求される利用者のアクセス権とエンドポイントの相互認証に必要なデータのAPIとブロックチェーン・データベースとの間の読込み、書込みの各処理工程を示す
Ｓ５００～Ｓ５０５　ICカードの安全性管理システムの世界標準化組織で規定する認証スキームSCP01をベースとしたSFIDカードとAPIとの相互認証プロセスのフローチャートの各処理工程を示す。
１０　認証スキームSCP01をベースとして、認証の度毎に再計算されるセッションキーを使って、SFIDからAPIに送られる暗号化されたデータ
１１　認証スキームSCP01をベースとして、認証の度毎に再計算されるセッションキーを使って、APIからSFIDに送られる暗号化されたデータ
１２　ブロックチェーン・データベースに記録された業務システムへの直近のアクセス履歴が書かれたトランザクションのトランザクションハッシュID

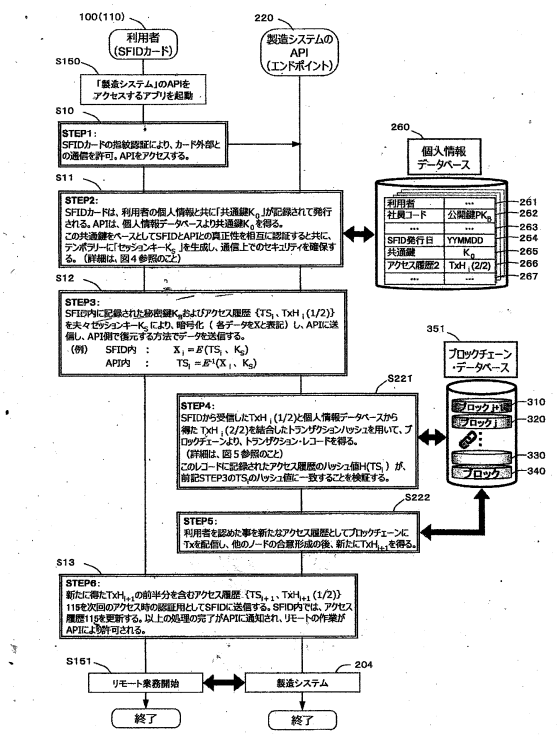
１３　ブロックチェーン・データベースに記録された業務システムへの直近のアクセス履歴が書かれたトランザクション・レコード
１２２　業務システムへの直近のアクセス履歴が書かれたトランザクション・データに含まれる利用者を示す社員コード。本発明のFIDaaS認証基盤で用いられる公開鍵暗号方式に必要なSFID内に秘匿される秘密鍵と対になる公開鍵
１２３　業務システムへの直近のアクセス履歴が書かれたトランザクション・データに含まれる業務システムへの直近のアクセス時刻データ
１２４　業務システムへの直近のアクセス履歴が書かれたトランザクション・データに含まれる予備のレコード
１２５　業務システムへの直近のアクセス履歴が書かれたトランザクション・データに含まれるカスタマイズに使用される予備のレコード
１４　業務システムへのアクセス権が認証完了した直後のアクセス履歴データが含まれたトランザクション・レコードのトランザクションハッシュID
１５　業務システムへのアクセス権が認証完了した直後のアクセス履歴データが含まれたトランザクション・レコード
【図面】
【図１】



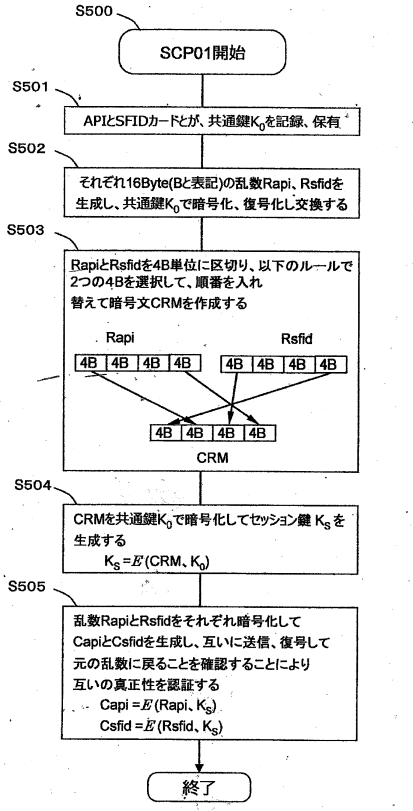
【図２】



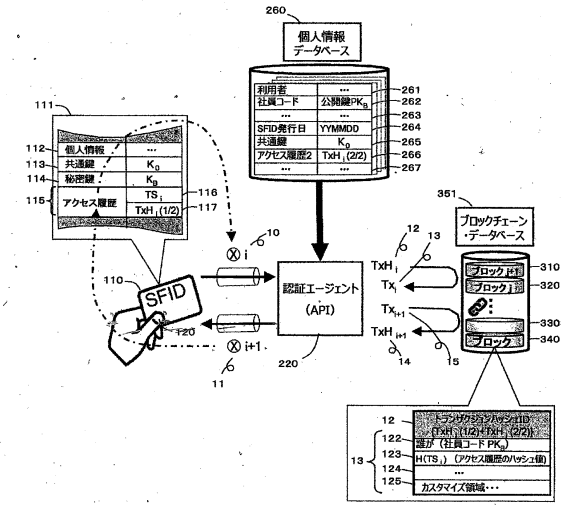
【図３】


100(110)
利用者
(SFIDカード)
220
製造システムの
API
(エンドポイント)
S150
「製造システム」のAPIを
アクセスするアプリを起動
S10
STEP1:
SFIDカードの指紋認証により、カード外部と
の通信を許可、APIをアクセスする。
S11
STEP2:
SFIDカードは、利用者の個人情報と共に「共通鍵K_0」が記録されて発行
される。APIは、個人情報データベースより共通鍵K_0を得る。
この共通鍵をベースとしてSFIDとAPIとの真正性を相互に認証すると共に、
テンポラリーに「セッションキーK_S」を生成し、通信上でのセキュリティを確保す
る。(詳細は、図４参照のこと)
S12
STEP3:
SFID内に記録された秘密鍵K_Bおよびアクセス履歴{TS_i、$TxH_i(1/2)$}
を夫々セッションキーK_Sにより、暗号化（各データをXと表記）し、APIに送
信し、API側で復元する方法でデータを送信する。
(例) SFID内 : $X_i = E(TS_i, K_S)$
API内 : $TS_i = E^{-1}(X_i, K_S)$
260
個人情報
データベース
利用者
社員コード
公開鍵PK_B
SFID発行日
YYMMDD
共通鍵
K_0
アクセス履歴2
$TxH_i(2/2)$
261
262
263
264
265
266
267
351
ブロックチェーン
・データベース
ブロック[i+1]
ブロック[i]
ブロック
310
320
330
340
S221
STEP4:
SFIDから受信したTxH$_i$(1/2)と個人情報データベースから
得たTxH$_i$(2/2)を結合したトランザクションハッシュを用いて、ブ
ロックチェーンより、トランザクション・レコードを得る。
(詳細は、図５参照のこと)
このレコードに記録されたアクセス履歴のハッシュ値H(TS_i)が、
前記STEP3のTS_iのハッシュ値に一致することを検証する。
S222
STEP5:
利用者を認めた事を新たなアクセス履歴として「ブロックチェーン」に
Txを転記し、他のノードの合意形成の後、新たにTxH$_{i+1}$を得る。
S13
STEP6:
新たに得たTxH$_{i+1}$の前半分を含むアクセス履歴{TS_{i+1}、$TxH_{i+1}(1/2)$}
115を次回のアクセス時の認証用としてSFIDに送信する。SFID内では、アクセス
履歴115を更新する。以上の処理の完了がAPIに通知され、リモートの作業が
APIにより許可される。
S151
リモート業務開始
204
製造システム
終了
終了

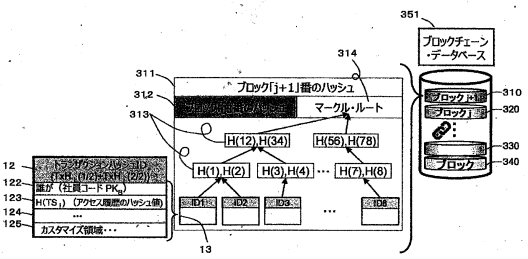
【図４】


S500
SCP01開始
S501
APIとSFIDカードとが、共通鍵K_0を記録、保有
S502
それぞれ16Byte(Bと表記)の乱数Rapi、Rsfidを
生成し、共通鍵K_0で暗号化、復号化し交換する
S503
RapiとRsfidを4B単位に区切り、以下のルールで
2つの4Bを選択して、順番を入れ
替えて暗号文CRMを作成する
Rapi
Rsfid
4B 4B 4B 4B
4B 4B 4B 4B
4B 4B 4B 4B
CRM
S504
CRMを共通鍵K_0で暗号化してセッション鍵 K_Sを
生成する
$K_S = E(CRM, K_0)$
S505
乱数RapiとRsfidをそれぞれ暗号化して
CapiとCsfidを生成し、互いに送信、復号して
元の乱数に戻ることを確認することにより
互いの真正性を認証する
Capi = E(Rapi、K_S)
Csfid = E(Rsfid、K_S)
終了

【図５】


260
個人情報
データベース
利用者
社員コード
公開鍵PK_B
SFID発行日
YYMMDD
共通鍵
K_0
アクセス履歴2
$TxH_i(2/2)$
261
262
263
264
265
266
267
111
個人情報
共通鍵
秘密鍵
アクセス履歴
K_0
K_B
TS_i
$TxH_i(1/2)$
112
113
114
115
116
117
351
ブロックチェーン
・データベース
ブロック[i+1]
ブロック[i]
ブロック
310
320
330
340
SFID
110
120
認証エージェント
(API)
220
10
11
12
13
14
15
トランザクションハッシュID
($TxH_i(1/2)$+$TxH_i(2/2)$)
鍵ア（社員コードPK_B）
$H(TS_i)$（アクセス履歴のハッシュ値）
カスタマイズ領域・・・
122
123
124
125

【図６】


351
ブロックチェーン
・データベース
ブロック[i+1]
ブロック[i]
ブロック
310
320
330
340
314
311
312
313
ブロック[j+1]番のハッシュ
マークル・ルート
H(12),H(34)
H(56),H(78)
H(1),H(2)
H(3),H(4)
H(7),H(8)
ID1
ID2
ID3
ID8
12
122
123
124
125
13

フロントページの続き

(51)国際特許分類　　ＦＩ
　　Ｇ０６Ｆ　　21/64

(56)参考文献　　特許第６５３２５８１（ＪＰ，Ｂ１）
　　米国特許出願公開第２０２０／０１４５２１９（ＵＳ，Ａ１）
　　中国特許出願公開第１０６８４５２１０（ＣＮ，Ａ）

(58)調査した分野　(Int.Cl.，ＤＢ名)
　　Ｈ０４Ｌ　　９／３２
　　Ｇ０６Ｆ　２１／３２
　　Ｇ０６Ｆ　２１／４４
　　Ｇ０６Ｆ　２１／６０
　　Ｇ０６Ｆ　２１／６４