

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2016年7月28日(28.07.2016)



(10) 国際公開番号

WO 2016/117500 A1

- (51) 国際特許分類:
G06F 21/31 (2013.01) G06F 21/12 (2013.01)
- (21) 国際出願番号: PCT/JP2016/051268
- (22) 国際出願日: 2016年1月18日(18.01.2016)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2015-008162 2015年1月19日(19.01.2015) JP
- (71) 出願人: 日本電気株式会社(NEC CORPORATION)
[JP/JP]; 〒1088001 東京都港区芝五丁目7番1号
Tokyo (JP). 国立大学法人東京大学(THE UNIVERSITY OF TOKYO)
[JP/JP]; 〒1138654 東京都文京区本郷七丁目3番1号 Tokyo (JP).
- (72) 発明者: 坂本 静生(SAKAMOTO, Shizuo); 〒1088001 東京都港区芝五丁目7番1号 日本電気株式会社内 Tokyo (JP). 山口 利恵(YAMAGUCHI, Rie); 〒1138654 東京都文京区本郷七丁目3番1号 国立大学法人東京大学内 Tokyo (JP). 鈴

木 宏哉(SUSUKI, Hiroya); 〒1138654 東京都文京区本郷七丁目3番1号 国立大学法人東京大学内 Tokyo (JP).

(74) 代理人: 加藤 朝道(KATO, Asamichi); 〒2220033 神奈川県横浜市港北区新横浜3丁目20番12号加藤内外特許事務所内 Kanagawa (JP).

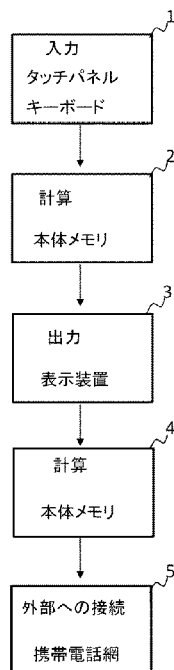
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユー

[続葉有]

(54) Title: AUTHENTICATION APPARATUS, METHOD, SYSTEM AND PROGRAM, AND SERVER APPARATUS

(54) 発明の名称: 認証装置、方法、システムとプログラム並びにサーバ装置



- 1 Input: Touch panel keyboard
2, 4 Calculation: Internal memory
3 Output: Display apparatus
5 Connection to outside: Cellular phone network

(57) Abstract: The present invention provides an apparatus, a system, a method, and a program changeable to authentication corresponding to a security environment. A scenario consisting of a combination of procedures of multi-factor authentication needed for a communicating/connecting terminal to receive the provision of a service is associated with said service and stored and managed, and the probability of each procedure's success is stored and managed by associating the scenario with each procedure. The success probability through the service scenario is calculated on the basis of the probability for each procedure, at least one of security and usability is assessed on the basis of the success probability, and the service is controlled with respect to the terminal in accordance with the assessment results.

(57) 要約: 本発明は、セキュリティ環境に応じた認証に変更可能な装置、システム、方法、プログラムを提供する。通信接続する端末がサービスの提供を受けるために必要とされる多要素認証の手順の組み合わせからなるシナリオを、前記サービスに対応させて記憶管理するとともに、前記各手順に対応させて、前記手順が成功する確率を記憶管理し、前記手順に関する前記確率に基づき、前記サービスのシナリオを通しての成功確率を算出し、前記成功確率に基づきセキュリティ及びユーザビリティの少なくとも一方を評価し、前記評価結果にしたがって、前記端末に対する前記サービスを制御する。



ロシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨー
ロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE,
ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,
MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK,
SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ,
GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告 (条約第 21 条(3))

明 細 書

発明の名称：

認証装置、方法、システムとプログラム並びにサーバ装置

技術分野

[0001] （関連出願についての記載）

本発明は、日本国特許出願：特願２０１５－００８１６２号（２０１５年１月１９日出願）の優先権主張に基づくものであり、同出願の全記載内容は引用をもって本書に組み込み記載されているものとする。

本発明は、認証装置、方法、システムとプログラム並びにサーバ装置に関する。

背景技術

[0002] スマートフォン等の高機能携帯端末の普及により、複数のセンサやアプリケーションの常時アップデートを利用することで、より安全かつ現実的に多要素認証（Multi-Factor Authentication）が可能となるに到っている。例えばスマートフォンやタブレットＰＣ（Personal Computer）等のスマートデバイスを利用する際のセキュリティを向上するための認証サービスを行うクラウドサービスでは、ソフトウェア証明書を用いた２要素認証が採用されている。この場合、例えばスマートデバイスからＩＤ（Identity:識別情報）／パスワードを入力することで、許可されたデバイスと利用者が識別され、当該スマートデバイスから例えば業務アプリケーション等へのアクセスが可能となる。

[0003] 多要素認証手法は各種提案されているが、それぞれの認証精度について一定の評価軸が未だ提供されていないというのが実情である。

[0004] ＥＣ（Electronic Commerce：電子商取引）サイトのログインにおける認証には、ほとんどのサイトで、ＩＤとパスワードが利用されている（例えば非特許文献１参照）。しかしながら、ＩＤとパスワードだけの認証では、セキュリティ上の問題があると言われている。例えばパスワードリスト攻撃と呼

ばれる攻撃が多発する等、IDとパスワードだけでは、ログイン認証におけるセキュリティを十分に担保することができない、という状態になっている（例えば非特許文献2参照）。

[0005] スマートデバイスには、複数のセンサやセキュアエレメントを予め実装したものが製造、販売されている。特に、端末そのものに、生体認証機能を実装したものや、SIM（Subscriber Identity Module）のセキュアエレメントを利用した端末認証を利用した決済等が利用され始めている。すなわち、IDやパスワードは、ユーザの記憶と入力によるが、ユーザの記憶と入力だけによらない認証が利用され始めている。

[0006] また、通常のアクセス元と異なるIP（Internet Protocol）でのログイン時に不正の可能性を指摘することや、過去のショッピングやWeb閲覧の履歴を活用することで、本人らしさについて検討する方法等、行動に基づく認証方式の可能性も広がってきている。例えば、通常日本でログインしているユーザが海外でのログインを行った際に、パスワードのアラートが出るような仕組みも提案されている（例えば非特許文献4参照）。

先行技術文献

非特許文献

[0007] 非特許文献1：株式会社シマンテック／日本ベリサイン株式会社，「個人・企業のパスワード管理」に関する意識調査結果のご報告，2013. 10，[2014. 12. 15検索]，インターネット<URL: https://www.jp.websecurity.symantec.com/welcome/pdf/password_management_survey.pdf>

非特許文献2：IPA，オンライン本人認証方式の実態調査，2014. 8，[2014. 12. 15検索]，インターネット<URL: <https://www.ipa.go.jp/security/fy26/reports/ninsho/>>

非特許文献3：ゆうちょ銀行，リスクベース認証（画像・合い言葉）について，[2014. 12. 15検索]，インターネット <URL: http://www.jp-bank.japanpost.jp/direct/pc/security/dr_pc_sc_riskbase.html>

非特許文献4：Google，前回のアカウント アクティビティ，[2014. 1

2. 15検索], インターネット <URL: <https://support.google.com/mail/answer/45938?hl=ja>>

非特許文献5: 内閣官房, オンライン手続におけるリスク評価及び電子署名・認証ガイドライン, 2010. 8, [2014. 12. 15検索], インターネット <URL: http://www.kantei.go.jp/jp/singi/it2/guide/guide_line/guideline100831.pdf>

発明の概要

発明が解決しようとする課題

[0008] 以下に関連技術の分析を与える。

[0009] 認証方式の多くは、一つの認証要素によって認証の成功失敗を判断するような方式である。また、複数の認証要素を組み合わせた多要素認証も、例えばID・パスワードと例えば乱数表の提示のような、事前に設定された要素を利用したものである。

[0010] また、リスクベース認証のように、利用者の振る舞いが「通常と異なる」時にだけ、認証要素を追加する等（例えば非特許文献3参照）、常に同じ形式での認証要求を行わないようなサービスも増えてきている。リスクベース認証は、例えばいつもと同じユーザ情報等でのアクセスに対しては、例えば固定のパスワード等で認証し、いつもと異なるユーザ情報等でアクセスがあった場合、例えばパスワード等のユーザ情報が盗まれたリスクが高いとして、事前に登録しておいた追加の質問に回答させる等の追加認証を行う。

[0011] また近年は特にスマートフォンの高機能端末の普及によって、新しいアプリケーションの導入と、該端末に実装された各種センサ等の活用によって、手順の頻繁な変更を可能とする環境も整いつつある、ともいえる。

[0012] このように、多様かつ可変な認証要素の組み合わせをダイナミックに変更して利用するためには、認証全体に対する評価方式が必要である。また、この評価方式は、例えば、実際にサービスがスタートしたときに、別の認証方式への変更が可能となるような、柔軟で利便性の高い方式が望まれている。

[0013] 本発明は、上記課題に鑑みて創案されたものであって、その目的は、認証

要素の組み合わせをダイナミックに変更して利用可能とする装置、方法、システムとプログラム並びにサーバ装置を提供することにある。

課題を解決するための手段

[0014] 本発明の1つの側面によれば、端末と通信接続し、多要素認証を行う装置であって、端末がサービスの提供を受けるために必要とされる多要素認証の手順の組み合わせからなるシナリオを、前記サービスに対応させて記憶するとともに、前記各手順に対応させて、前記手順が成功する確率を記憶する記憶部と、

前記手順に関する前記確率に基づき、前記サービスのシナリオを通しての成功確率を算出し、前記成功確率に基づきセキュリティ及びユーザビリティの少なくとも一方を評価する評価手段（評価部）と、

前記評価結果にしたがって、前記端末に対する前記サービスを制御する制御手段（制御部）と、

を備えた多要素認証装置が提供される。

[0015] 本発明によれば、端末と、上記多要素認証装置を備えた認証システムが提供される。

[0016] 本発明の別の側面によれば、上記多要素認証装置を備えたサーバ装置が提供される。

[0017] 本発明のさらに別の側面によれば、通信接続する端末がサービスの提供を受けるために必要とされる多要素認証の手順の組み合わせからなるシナリオを前記サービスに対応させて記憶部で記憶するとともに、前記各手順に対応させて、前記手順が成功する確率を前記記憶部で記憶し、

前記手順に関する前記確率に基づき、前記サービスのシナリオを通しての成功確率を算出し、前記成功確率に基づきセキュリティ及びユーザビリティの少なくとも一方を評価し、

前記評価結果にしたがって、前記端末に対する前記サービスを制御する多要素認証方法が提供される。

[0018] 本発明のさらに別の側面によれば、端末に通信接続し、多要素認証を行う

コンピュータに、通信接続する端末がサービスの提供を受けるために必要とされる多要素認証の手順の組み合わせからなるシナリオを前記サービスに対応させて記憶部で記憶するとともに、前記各手順に対応させて、前記手順が成功する確率を前記記憶部で記憶する処理、

前記手順に関する前記確率に基づき、前記サービスのシナリオを通しての成功確率を算出し、前記成功確率に基づきセキュリティ及びユーザビリティの少なくとも一方を評価する処理、及び、

前記評価結果にしたがって、前記端末に対する前記サービスを制御する処理、を実行させるプログラムが提供される。

[0019] 本発明によれば、上記プログラムを記録したコンピュータ読み出し可能な記録媒体（半導体メモリ、磁気／光・記録媒体等）が提供される。

発明の効果

[0020] 本発明によれば、認証要素の組み合わせをダイナミックに変更して利用可能としている。

図面の簡単な説明

[0021] [図1]多要素認証における要素の一例を説明する図である。

[図2]（A）乃至（D）は直列手順と並列手順とそれらの組み合わせを説明する図である。

[図3]（A）はスマートフォン機能を表形式で示す図、（B）は手順と確率の関係を表形式で示す図である。

[図4]（A）は、コストとセキュリティパラメータの関係を表形式で示す図、（B）はシナリオと攻撃確率、ユーザの失敗確率の関係を表形式で示す図である。

[図5]実施形態のシステムの構成例を例示する図である。

[図6]各サービスに対するシナリオ選択の例を説明する図である。

発明を実施するための形態

[0022] はじめに本発明の概要について説明したあと、実施形態について説明する。以下では、

(A) スマートフォン等における多要素認証に利用可能な手段について複数のシナリオを検討することの必要性について説明する。

(B) サービスの提供に複数のシナリオがある場合、それぞれの確率モデルを利用したセキュリティ評価が必要である。そこで、セキュリティ評価の更新についても説明する。

(C) さらに、セキュリティ評価だけでなく、ユーザの利便性についても、同様の評価をし、双方を含めた評価結果を更新しつづけることで、実際のサービスにおいてどのようにシナリオ選択を行うのか等について説明する。

[0023] スマートフォンにおける機能の一例を列挙し、認証手段として複数の要素を組み合わせる多要素認証が現実的に適用可能となりつつある点を分析する。また、多要素認証方式をセキュリティ評価するための枠組みとしてどのようなモデルがよいのかについて検討する。また、このモデルの活用方法について説明する。

[0024] スマートフォンは、インターネット接続機能を備え、アプリケーションはインターネット機能を活用して様々なサービスを提供する。インターネットを介したサービスの多くは、認証を必要としており、ユーザの「本人性」を確かめる必要性がある。「本人性」を確かめるために有効な認証手段として、セキュアエレメントがある。また、ユーザの記憶に頼る情報を入力するための手段や、複数のセンサを内蔵している。スマートフォンがもつ機能の一例について列挙し、今後スマートフォンにおいて、どのような認証のシナリオが考えられるかについて検討する。

[0025] スマートフォンがもつユーザとインタラクション可能な機能について説明する。ここでは複数の機能が列挙されているが、各機能それぞれが入力等だけに限定された機能ではない場合もある。主にどちらに利用されているのかについて説明する。

[0026] ユーザがスマートフォンに対して何らかの操作を行う際、スマートフォンがもつ入力機器を通してスマートフォンへの要求を伝える。市販されている機器において考えられる入力、図3(A)の「入力機器」列のとおりであ

る。特に制限されないが、この例のスマートフォンでは、入力機器として、タッチパネル、マイク、ボタン、カメラ、指紋センサ等がある。

[0027] センサのうちジャイロセンサ（加速度センサ）は、スマートフォンを手にしたユーザのとり動作（ジェスチャ）を検出する。GPS（Global Positioning System）センサはスマートフォンの位置を検出する。光センサは例えば環境光（照度）を検出する。ガイガーカウンタは、例えばスマートフォン接続型の放射線検出器である。スマートフォンが接続する外部接続対象は、基地局を介して携帯電話網、Bluetooth（Bluetooth SIG, Incの登録商標）、NFC（Near Field Communication：近接距離通信）、WiFi（Wireless Fidelity：WiFiはWiFi Allianceの登録商標）、USB（Universal Serial Bus）、CTIA（Cellular Telephone Industries Association）等がある。出力は、スマートフォンの表示装置、スピーカ、ライト、バイブレータによる振動、メモリ、SDカード等がある。セキュアエレメントは、秘密情報を管理するためのセキュアな領域である。キャリアSIM、TPM（Trusted Platform Module）、Felica（ソニー株式会社の登録商標）、ソフトウェアSIM、クラウドSIM等がある。

[0028] なお、耐タンパ装置であっても複数の攻撃をよって安全性が脅かされる危険性もあるので、ある時間軸の中で安全性を考慮する必要性がある。

[0029] スマートフォンにおいて、単体の認証として既に利用されているものや、複数の認証を組み合わせることで多要素認証として既に実現されているものが存在する。スマートフォンの機能の1つ1つを要素とし、要素を組み合わせることで、各手順が実現される。

[0030] 例えば、IDの入力とパスワードの入力を行う場合、図1のように、スマートフォンの機能を組み合わせることで、IDパスワード認証という手順を実現している。このような手順を組み合わせることで、例えば、以下のような多要素認証を実現することができる。

[0031] ・SIMを生体認証で該当する機能を活性化し、ログイン（指紋、声、入力パターン等の入力）；

- ・ウェアブル端末によって該当する機能を活性化し、端末IDを利用してログイン；
- ・非接触カードによって該当する機能を活性化し、端末IDを利用してログイン；

[0032] このように、複数の要素（機能）を組み合わせた多要素認証が実現可能となってきた。しかしながら、多要素認証は、専用トークン（例えばハードウェア等で生成されるワイタイムトークン）や事前に渡した乱数表の利用を前提としたシステムでの限定的な利用に限られている。このため、複数要素の統一的な評価軸を設けることは必要とされていない。また、システムやユーザの負荷、特にユーザビリティについても、セキュリティとの対比や分析は行われていない。

[0033] 例えば、複数のセンサやセキュアエレメントの実装等、多要素認証に適用可能な機能を具備しているスマートフォンが利用されている。また、アプリケーションの頻繁な更新（アップデート）が可能となる枠組みもシステム化されていることから、要素の柔軟な変更も必要である。一方で、一旦、始めたサービスの提供をやめることは難しい。したがって、継続性の観点も検討しなければならない。

[0034] このように、統一的で柔軟、継続可能なサービス実現に向けた多要素認証の安全性をダイナミックに評価する枠組みが求められている。

[0035] 本発明は、多要素認証の評価基準（評価軸）を、シナリオごとのセキュリティとユーザビリティの確率モデルを利用することで構成し、継続的なサービスを提供可能としながら、例えばセキュリティ環境の変化等に応じた認証手法を、ダイナミックに変更可能とする枠組みを提案する。

[0036] 以下では、本発明による多要素認証についてより詳細に説明する。

[0037] <認証>

「認証」とは、ある行為の「実行主体」と、当該主体が行った「登録情報」との同一性を、ネットワークを介した状態で検証することによって、「実行主体」が登録された人物（あるいは装置）であることの信用を確立するプ

ロセスをいう（例えば非特許文献5参照）。

[0038] 以下、ある行為の実行主体を、ユーザ $u \in U$ とする。ここで、 U は、ユーザ全体の集合を表している。また、認証が求められる場面では、あるサービス $s r v c$ をユーザが受ける際、あるトランザクション $t r a$ においてサービスを受ける権限があるか否かについて、サービス提供者が権限を確認する。

[0039] 権限の確認が必要な場面として想定しているのは、誰に対しても行うことができるようなサービスにおいては、認証は必要ない。一方、権限のある人だけが受けられるサービスに対しては認証が必要である。権限があるユーザ u は、ある意図を持って、サービス $s r v c$ の提供を受けているとする。

[0040] また、トランザクション $t r a$ は、オンライン経由で行うこととする。オンラインでのサービスとして、例えばWebショッピングサイトやオークションのようなEC(Electronic Commerce)サイト、SNS(Social Networking Service)といったコミュニケーションを目的としたサイトを想定する。これらのサイトは、ユーザ u に利用の意思がある場合、ユーザ u はサービスの提供を求める（システム登録時等に、一度の設定のみでユーザ u が継続的にはアクセスしないサービスではない）。このため、システムはサービスの提供を求めるユーザ u に対して、たびたび、認証を求める。このようなサービスを受ける際、ユーザは、直接ネットワークに接続することではなく、ユーザの持つ端末（スマートフォンやPC）等を介して、インターネットに接続する。なお、端末等を通じたサービス提供であっても、ユーザ u がサービスを受けているものとして説明する。

[0041] 生体認証においては、ユーザ u が正しい生体情報の入力を試みたにもかかわらず、入力時に、例えば指紋の接地に失敗する等して、情報が正しく取得されない場合がある。また、ユーザ u とは別の人の入力ユーザ u の入力と認識される誤検知が発生する場合もある。以下では、生体認証において各要素の認証結果が一意に決まるものとし、その値が正しいか間違っているかについて、後からの追跡が可能である場合において、検知されるものとする。

[0042] まず、ユーザ u があるサービス $s\ r\ v\ c$ をうける際、IDやパスワードのような記憶や乱数表の活用等、複数の要素を利用して、ログインするものとする。また、ユーザ u になりすまそうとする攻撃者 $\alpha \in A$ の存在（ A は攻撃者の集合）を想定する。

[0043] ユーザ u があるサービスを受ける際、多要素認証が行われる。スマートフォン等のように複数の認証要素（タッチパネルやセンサ等）がある場合には、どの認証要素を選択し組み合わせるかについては、サービスごとに、異なるものとする。

[0044] また、サービスによっては、複数の認証要素の組み合わせを選択できるものとする。

[0045] <シナリオ>

このような認証要素の組み合わせのことを「シナリオ」という。

[0046] <手順（ファクタ）>

$$s' = ((f_1), (f_2), \dots, (f_n)) \quad (n \in N)$$

認証要素の組み合わせにおいて、シナリオ S の複数の手順（ファクタ） $f \in F$ （ F は手順の集合）を、ある定められた順番で配置することが可能であるとする（次式（1））。ここで手順（ファクタ） $f \in F$ とは、例えばIDとパスワードという記憶による認証要素や、指紋認証を指す。

[0047] <シナリオと手順>

$$s = ((f_1, 1), (f_2, 2), \dots, (f_n, n)) \quad (n \in N)$$

・・・(1)

[0048] また、手順 f の順番を定めずを示すこともできる。その場合、シナリオは次式（2）で与えられるものとする。

[0049] ・・・(2)

[0050] <エレメント>

また、各手順は複数のエレメント $e \in E$ （ E はエレメント集合）によって構成される。

[0051] ここで、エレメントとは手順 f ごとに必要な行動である。

[0052] <手順とエレメント>

手順 f は、例えば次式 (3) のように、1 又は複数のエレメントからなる。

$$f = ((e_1, 1), (e_2, 2), \dots, (e_n, n)) \quad (n \in N) \quad \dots (3)$$

[0053] 例えば、ID とパスワードと指紋認証を組み合わせたようなシナリオ S を選択するとする。シナリオ S は例えば次式 (4) で表される。

$$S = ((f_1, 1), (f_2, 2)) = (((e_1, 1), \dots), ((e_2, 1), \dots)) \quad \dots (4)$$

[0055] ここで、 S は、ID パスワード認証と指紋認証からなる。 f_1 が ID パスワード認証要素、 f_2 が指紋認証要素である。

[0056] $((e_1, 1), \dots), ((e_2, 1), \dots)$ の各 $(e_1, 1)$ 、 $(e_2, 1)$ は、図 1 のような一つ一つのエレメント（入力、計算等）とする。

[0057] 各 f は、認証結果として、認証が正しいとされた場合は 1、認証が正しいとされなかった場合は、0 の二値 (0、1) を返す。

[0058] ユーザ u に対して、サービスを提供するにあたり、認証要素の組み合わせであるシナリオ S は一つとは限らない。複数の認証要素の選択が可能である、ということは、複数のシナリオの組み合わせも可能である。すなわち、複数のシナリオが存在し、その選択が可能とされる。これによって、ユーザ u に対して、一つのシナリオ（ある認証要素の組み合わせ）が利用できなくなった際、他のシナリオ（認証要素の別の組み合わせ）の選択を可能とすることで、ユーザ u に対して、継続的なサービス提供を図ることが可能となる。

[0059] 多要素認証を実施するに当たり、それぞれの要素がどのように関係していくのかについて、説明する。多要素認証は、直列手順、並列手順の二つのパターンのシナリオが考えられる。

[0060] <直列手順>

認証は、段階的に手順が進む。例えば、ID とパスワードの入力を求めた

後、乱数表からの入力を求めることは、直列手順にあたる。

[0061] 図2（A）のように、ある手順 f_1 を行ったあと、次の手順である f_2 の要求が行われ、次に手順 f_3 という具合に、一つ一つの認証を多段階でつなげることがある。この手順を直列手順と呼ぶ。この場合、シナリオ S は次式（5）で表される。

$$[0062] \quad S = ((f_1, 1), (f_2, 2), \dots, (f_n, n)) \quad (n \in N) \quad \dots (5)$$

[0063] 式（5）において、手順 $(f_1, 1)$ 、 $(f_2, 2)$ 、 $\dots$ 、 (f_n, n) の順番は、多段階の認証の順番としての意味をもつ。

[0064] <並列手順>

認証は、並列に評価を行う。例えば、IDとパスワードの入力と並行して、スマートフォンがもつSIMカードのIDを確認している場合がこれにあたる。例えば図2（B）に示すように、ある手順 f_{i+1} と別の手順 f_{i+2} を並列に確認することを「並列手順」という。この場合、シナリオ S は次式（6）で表される。

$$[0065] \quad S = ((f_1, 1), (f_2, 2), \dots, (f_n, n)) \quad (n \in N) \quad \dots (6)$$

[0066] 式（6）において、手順 $(f_1, 1)$ 、 $(f_2, 2)$ 、 $\dots$ 、 (f_n, n) の順番は、意味をもたない。このため、次式（7）のように表記する。

$$[0067] \quad S' = ((f_1), (f_2), \dots, (f_n)) \quad (n \in N) \quad \dots (7)$$

[0068] 直列手順と並列手順とを組み合わせるシステムを構成することもある。図2（C）は、直列手順のシナリオ S_1 、 S_2 、 S_4 と並列手順のシナリオ S_3' を直列に組み合わせたものである。図2（D）は、並列手順のシナリオ S_3' を展開して示した図であり、次式（8）と表される。

$$[0069] \quad S_{all} = (S_1, S_2, S_3', S_4) \\ = (S_1, S_2, (f_{3-1}, f_{3-2}, f_{3-3}), S_4)$$

．．．(8)

[0070] 次に、本実施形態における直列認証と成功確率について説明する。

[0071] <手順ごとの成功確率>

各手順ごとに成功する確率について図3 (B) を利用して説明する。認証の手順を、 $f \in F$ としたとき、手順 f は、成功した場合、1を返し、失敗した場合、0を返す。

[0072] f という手順を利用した際、ユーザ u のIDによって手順を行う場合には、 $f(u)$ と表記する。また、1が返る手順を f^+ 、0が返る手順を f^- とする。

[0073] ユーザ u が、 u というIDを利用して、手順 f を行い、1が返る手順を $f^+(u)$ とし、確率を $p(f^+(u) | u)$ とする。また、 u になりすまして成功しようとする攻撃者 a が成功する確率を $p(f^+(u) | a)$ とする。

[0074] 次に、 u が手順 f を失敗した場合、その失敗した場合の確率を $p(f^-(u) | u)$ とする。次式(9)、(10)が成り立つ(図3 (B) 参照)。

$$[0075] \quad p(f^+(u) | u) + p(f^-(u) | u) = 1$$

．．．(9)

$$[0076] \quad p(f^+(u) | a) + p(f^-(u) | a) = 1$$

．．．(10)

[0077] あるシナリオ S が1つの手順 f だけ含む場合、確率 $p(f^+(u) | u)$ が、 S の成功確率となる。

[0078] 知識を利用している場合、成功確率が、一定の間、100%になりうることもある。これは、本来、ユーザ u が記憶しているべき内容(IDに対応するパスワード)等について、ブラウザ等のアプリケーションが記憶することで、その役割を果たすことがあるためである。

[0079] この場合、ユーザは失敗のしようがなく、必ず、確率 $p(f^+(u) | u)$ は、 $p = 1$ 、すなわち成功する。

[0080] 一方、生体認証の場合、ユーザの入力時に、ゆれ等が生じるので、成功確率が1にはなりえない。つまり、 $p < 1$ にしかなりえない。

[0081] <シナリオごとの多要素認証の成功確率>

ユーザ u が、認証要素の組み合わせとして、シナリオ S を選択し、複数の手順 $f_1 \sim f_n$ を行ったものとする。

$$[0082] \quad S = (f_1(u), \dots, f_n(u)) \quad (n \in N) \quad \dots (11)$$

[0083] ここで、ユーザ u が u という ID で手順 f を成功する確率を $p(f^+ | u)$ と表記する。

[0084] また、ユーザ u がシナリオ S を通して成功する確率を $p(S^+ | u)$ で表す。

[0085] ここで、ユーザ u が認証する場合のシナリオを並列手順と直列手順で確率で下記のように定める。

[0086] <並列手順の成功確率>

シナリオ S の中で手順 f が全て並列であるとする。並列の場合、各手順と他の手順の成功確率は独立であるとする、シナリオ S を通して成功する確率 $p(S^+(u) | u)$ は、次式 (12) のように表される。

$$[0087] \quad p(S^+(u) | u) = p(f_1^+(u) | u) \times p(f_2^+(u) | u) \times \dots \times p(f_n^+(u) | u) \quad \dots (12)$$

[0088] また、攻撃者 a がユーザ u になりすまして試行を行った場合、シナリオ S を通して成功する確率 $p(S^+(u) | a)$ は、次式 (13) のように表される。

$$[0089] \quad p(S^+(u) | a) = p(f_1^+(u) | a) \times p(f_2^+(u) | a) \times \dots \times p(f_n^+(u) | a) \quad \dots (13)$$

[0090] <直列手順と事前確率>

直列手順が組み合わされたシナリオ S :

$$S = (f_1(u), \dots, f_n(u)) \quad (n \in N) \quad \dots (14)$$

をユーザ u が成功する確率 $p(S^+(u) | u)$ は以下ようになる。

[0091] 直列の場合、手順 f_i ($i \in \mathbb{N}$) が行われる前に $f_1, \dots, f_{i-1}$ が行われたことによって、事象の発生確率が相関がある場合において変化する。ここで、事前確率を考慮して次式 (15) で与えられる。

$$\begin{aligned}
 [0092] \quad p(S^+(u)|u) &= p(f_1^+(u)|u) \times p(f_2^+(u)|uf_1^+(u)) \times \\
 &\quad p(f_3^+(u)|uf_1^+(u)f_2^+(u)) \times \\
 &\quad \dots \times p\left(f_n^+(u)|u \prod_{i=1}^{n-1} f_i^+(u)\right) \\
 &\quad \dots (15)
 \end{aligned}$$

[0093] また、攻撃者 a が式 (14) のシナリオ S を成功する確率 $p(S^+(u)|a)$ は次式 (16) で与えられる。

$$\begin{aligned}
 [0094] \quad p(S^+(u)|a) &= p(f_1^+(u)|a) \times p(f_2^+(u)|af_1^+(u)) \times \\
 &\quad p(f_3^+(u)|af_1^+(u)f_2^+(u)) \times \\
 &\quad \dots \times p\left(f_n^+(u)|a \prod_{i=1}^{n-1} f_i^+(u)\right) \\
 &\quad \dots (16)
 \end{aligned}$$

[0095] <並列手順と直列手順の組み合わせの確率計算>

並列手順と直列手順が組み合わさったシナリオ S をユーザ u が成功する確率 $p(S^+(u)|a)$ は次式 (17) で与えられる。

$$\begin{aligned}
 p(S^+(u)|u) &= p(f_1^+(u)|u) \times p(f_2^+(u)|uf_1^+(u)) \times \\
 &\quad p(f_3^+(u)|uf_1^+(u)f_2^+(u)) \times \\
 &\quad \dots \times p\left(S_n^+(u)|u \prod_{i=1}^{n-1} f_i^+(u)\right) \\
 &\quad \dots (17)
 \end{aligned}$$

[0096] 式 (17) において、並列確率は事前確率が存在しないとして計算し、直列手順に一般化できる。

[0097] <多要素認証確率の適用例>

次に、実施形態における多要素認証確率の適用例について説明する。

[0098] スマートフォン等、複数の認証方式を活用するようなサービスがある。このようなサービスを継続的、かつ動的にセキュリティ評価を行っていく手法

への適用例について説明する。本実施形態では、サービスを評価するにあたり、セキュリティパラメータとユーザビリティパラメータについて説明する。

[0099] 複数の要素の認証を行う上でのセキュリティ評価が重要となる。認証においては、各手順に対して、常にユーザ u が成功し、攻撃者 a が成功しない状況が望ましい。言換すれば、攻撃者 a が成功する確率は 0 が望ましい。攻撃者 a_1 、 $\dots$ 、 a_n がいるとき、ある手順 1 が成功する確率は、

$$p(S^+(u) \mid a_i) = 0 \quad \dots (18)$$

が望ましい。

[0100] しかしながら、各手順は、ある時点 t_0 にサービスをリリースする際に、攻撃者の成功確率を完全に 0 としておくことはできない。このためセキュリティ評価が必要となる。ここでセキュリティ評価として検討されることは、総当たり攻撃のようなスキルレベルの高くない攻撃が行われている場合には、セキュリティパラメータ k を超えることがないようにセキュリティ評価を設定する。

[0101] そこでセキュリティパラメータ k について、

$$p(S^+(u) \mid a) < k \quad \dots (19)$$

として、サービス s_{svc} をスタートする。

[0102] また、攻撃者 a がユーザ u に対して行った攻撃を行った結果、セキュリティの評価が、セキュリティパラメータ k 以上となったときに、何らかの対策が必要である、といえる。

[0103] ユーザ u にとっては、いくらセキュリティが高かったとしても、いつも自身の入力拒否されるような仕組みであっては、使い勝手はよくない。例えば、ユーザビリティのみに重点を置き、各手順において、常にユーザの入力が成功するように設定するためには、

$$p(S^+(u) \mid u) = 1$$

．．．(20)

となるようなシステムの構築を目指す必要がある。

[0104] また、ユーザの入力ミスや生体認証における入力のゆらぎのように、常に一定の入力がないこと等が予想されるため、常にユーザの入力が成功するシステムを構築することは現実的でない。

[0105] そのため、ユーザビリティパラメータ u_b について、

$$p(S^+(u) | u) > u_b$$

．．．(21)

として、サービス s_{svc} をスタートする。

[0106] また、選択されたシナリオ S の流れが、ユーザに利用しやすいか否かに関するユーザビリティについても考慮する必要性がある。例えばシナリオ S そのもののユーザビリティパラメータ u_b' について、ある一定の水準をみたしたもののについて、サービス s_{svc} をスタートする。以後は、ユーザビリティパラメータ u_b' について、ユーザビリティパラメータ u_b に含まれているものとみなす。

[0107] セキュリティパラメータ k やユーザビリティパラメータ u_b の値は、一意とは限らない。例えば、銀行振り込みで、過去に何度も入金しているところへ、少ない金額を振り込む場合には、高めのセキュリティパラメータ k を選択し、一度も振り込んでいない口座番号へ高額を振り込む場合には、低めのセキュリティパラメータ k を選択する等、柔軟な対応が考えられる。

[0108] このように、提供するサービスに合わせたセキュリティパラメータ k の選択や、逆に、あわせたサービス提供についても、検討の必要がある。同様に、セキュリティパラメータ k によって、シナリオが選択されたり、逆に、シナリオによってセキュリティパラメータ k を設定する構成としてもよい。

[0109] ユーザビリティパラメータ u_b によって、サービスが変更されることも多くある。例えば、一般にセキュリティが高いシステムが望まれるが、セキュリティ過剰なシステム構築がサービス上適切なこととは限らない。ここは、セキュリティとユーザの使い勝手等に配慮した、サービス全体の質に対する

考慮が必要なところであり、判断が難しい。

[0110] そこで、図4 (A) のように、各サービス $s r v c 1$ 、 $s r v c 2$ 、 $s r v c 3 \cdots$ に対して、各パラメータを設定可能とすることが重要である。各サービスに対して、セキュリティパラメータ、ユーザビリティパラメータが設定されている。コスト欄は各サービスのコストである。

[0111] <多要素認証における更新>

次に、本実施形態における多要素認証における値の更新について説明する。

[0112] シナリオにおける各手順の安全性は、サービスのスタート時に設定された通りになるとは限らない。常に、各手順に対しての攻撃も提案される可能性があり、設定時とは異なるコンピュータ性能の向上等からシステムの危殆化（何らかの作為や状況の変化により、対象が保安上の危険にさらされること）等も考えられる。また、例えば、ある特定の日付に攻撃が多発するような、ある期間で急激に攻撃が増えることによる安全性の低下等も考慮しなければならない。

[0113] システムだけでは見つけることができないような攻撃が流行ることによって、ある手順の安全性を急に下げる必要が生じる場合もある。つまり、各要素ごとの成功確率は、様々な要素によって変化する（下がる）ことが考えられる。一方、サービスは継続的に提供され続ける必要がある。攻撃の流行った日のサービスをやめるということよりも、対策を施しながらのサービス継続性を重視する必要がある。

[0114] ユーザにとっては、その都度新しい認証方式を強要されるよりは、今利用している認証方式を利用しつつ、他の方式と両立したり、ある程度準備されていた他の方式への変更等、柔軟性や利便性が、重要である。

[0115] そこで、過去の経験や予測による反映や、急に流行っている攻撃への対応、徐々に増えてきた攻撃によって代わった確率の反映等を行うために、「値の更新」が必要となる。

[0116] 成功確率をある時間 t_i ($i \in \mathbb{N}$ 、 N は1以上の正整数) までの成功確率を

時間 t_{i-1} までの成功確率で、評価し続けるとする。この場合、サービス s_{rv} c が行われあるシナリオ S_i ($i \in N$) が行われている限り、成功確率 $p(S^+_i(u) | a)$ の値は変化し続ける可能性がある。

[0117] また、攻撃が起こる等の事象に対しても、ユーザや攻撃者の成功確率の頻度を正確に更新し続けることによって、システムのリスクを正確に見積もることが可能になる。

[0118] サービスを行う上で、システムは、システム管理者等によって管理されているものであるため、攻撃があるとされた場合は、急に成功確率が変化することを予想すること、別のユーザにおいて攻撃が増えたと判断して対応すること、急激に p の値が変化しうると判断して対応する場合がある。

[0119] 特に、サービスに対して、レベルの高い攻撃が行われることが予測されたり、サービスに対して何かレベルの高い攻撃が行われたことが散見された場合、対策を行う必要性がある。レベルの高い攻撃とは、IDパスワードの場合のパスワードリスト攻撃や、生体認証への攻撃は例えばグミ指、ウルフ攻撃も含む。

[0120] ある時間に攻撃が急速に増える等の予測によって、時刻 $t_i \in T$ にある攻撃が多々増える場合への対応：時刻 t_i に、管理者が決めた成功確率 $p(S^+_i(u) | a)$ の値を事前に設定されていたセキュリティパラメータ k' の値に入れ替える。この場合、全てのユーザの $p(S^+_i(u) | a)$ が変更される。セキュリティパラメータ k' の値は、一意とは限らない。攻撃のレベルによって多様な値に変化する場合がある。

[0121] 成功確率 $p(S^+_i(u) | a)$ はユーザ u_i ごとだけが計測されているだけでなく、複数のユーザの値も観測されている。あるサービス S ごとに、ユーザ $u \in U$ (U はユーザ集合) のうち、事前に決められた人数 j 人のユーザの $p(S^+ | a)$ がセキュリティパラメータ k を超えた時、 j に含まれていない他のユーザの $p(S^+ | a)$ をセキュリティパラメータ k' に入れ替えるようにしてもよい。

[0122] 例えばパスワードリストの漏洩等、他によっておきた攻撃によって、サー

ビスにも攻撃が来ることも予想される。そのような予測がされた場合、ある時点（時刻） t_i に、管理者が決めた $p(S^+_i | a)$ の値を、事前に設定されたセキュリティパラメータ k' の値に入れ替えるようにしてもよい。

[0123] <多要素認証確率の変化とシナリオの変更>

シナリオ S の攻撃者の成功確率 $p(S^+ | a)$ がセキュリティパラメータ k を超えた際、サービスの手順の変更が必要である。この場合、例えば、このシナリオの変更や、サービス s_{rvc} の拒否が行われる。ある時間 t に成功確率 $p(S^+ | a)$ がセキュリティパラメータ k を超えた場合、シナリオ S の変更等の対策が施される。以下では、いくつかの対策について説明する。サービス s_{rvc} が行われている際、シナリオごとにセキュリティパラメータ k が計算されている。 $p(S^+(u_j) | a)$ はセキュリティの観点での評価となり、また、 $p(S^+(u_j) | u)$ は、ユーザビリティの観点となる。

[0124] 図4（B）に示すように、シナリオごとに攻撃の成功だけでなく各シナリオのユーザがどの程度失敗したのか等についても評価に含めることで、より利用しやすいシステムの構築が可能となる。

[0125] ユーザ u_j へのサービスの提供にあたり、以下の条件：

$$p(S^+(u_j) | a) < k \quad \dots (22)$$

$$p(S^+(u_j) | u) > ub \quad \dots (23)$$

を満たすようにして、サービス s_{rvc} をスタートする。

[0126] シナリオ S_i において、ユーザ u_j に対する $p(S^+(u_j) | a)$ がセキュリティパラメータ k を超えた際、シナリオ S を通したサービス提供を止め、 $p(S^+(u_j) | a) < k$ となるようなシナリオ S によるサービス s_{rvc} を受け付けるようにしてもよい。

[0127] シナリオの変更は、ユーザビリティの評価やサービスへの影響も含めて検討する必要がある。どのシナリオを次に受け付けるかについては、シナリオ S ごとに、表4を利用して、ユーザの失敗率とユーザビリティパラメータ

u_b の関係を考慮し、次のシナリオを提示する必要がある。 $p(S^+(u_j) | a)$ の値だけでは、シナリオの順番は評価できない。

[0128] 本実施形態では、各シナリオでの評価を行ったあと、全く新しいシナリオを設定する場合もある。サービスを行うにあたり、セキュリティ対策の上で、サービスそのものを変更する場合もある。例えば、銀行振り込みの上限金額を一時的に下げたり、チャージできる金額を下げる等である。この場合、図4(A)と図4(B)を見比べながら、適切なサービスの選択を行う必要がある。

[0129] また、サービス s_{svc} が取り得る全てのシナリオにおいて、 $p(S^+ | a) > k$ となると、サービス提供者は、サービス s_{svc} を停止する。また、シナリオ S のユーザビリティ u_b を考慮して、著しくユーザの利便性が下がる場合も、サービス s_{svc} を停止する。

[0130] <作用効果>

本実施形態によれば、スマートフォン等高機能型携帯端末の普及によって、多要素認証におけるシナリオを、サービス開始後に変更可能としている。多要素認証をダイナミックに評価し続ける統一的な仕組みの実装を可能としている。認証方式の選択は、サービス開始時に定めたような認証のセキュリティ評価だけでは不十分である場合に対して、シナリオ変更等の対策、例えば、シナリオごとの成功確率の更新が行われる。

[0131] <システム構成例>

次に、上記した多要素認証システムの例を説明する。図5は、本実施形態のシステム構成の一例を示す図である。図5を参照すると、ネットワーク30を介して接続されたサーバ装置等からなる多要素認証装置20を備えている。ネットワーク30は、例えば無線アクセス網、モバイル通信網、インターネット網等を含む。サーバ装置からなる多要素認証装置20は、クライアントにサービスを提供するサーバ装置内に実装してもよいし、クライアントにサービスを提供するサーバ装置とは別のサーバ装置として構成してもよい。

[0132] 多要素認証装置 20 は、サービスの提供を受けるために必要とされる多要素認証の手順 f の組み合わせからなるシナリオ S を、前記サービスに対応させて、記憶する（例えば図 6 参照）とともに、前記各手順 f に対応して、前記手順が成功する確率（図 3（B）参照）を記憶する記憶部 21 と、前記手順に関する前記確率に基づき、前記サービスのシナリオ S を通しての成功確率を算出し、成功確率に基づき、セキュリティ及びユーザビリティの少なくとも一方を評価する評価手段（評価部）23 と、評価手段 23 による評価結果にしたがって、提供するサービスを制御する制御手段（制御部）24 と、を備える。セキュリティパラメータ k 及びユーザビリティパラメータ u_b は、当該サービスに対応して記憶部 21 で記憶管理される（図 4（A）参照）。管理手段（管理部）22 は、記憶部 21 に記憶されるシナリオに対応する手順 f 、手順 f が成功する確率、サービスに対するセキュリティパラメータ k 及びユーザビリティパラメータ u_b の設定、保持、あるいは変更等の更新管理を行う。これら各手段（各部）の少なくとも 1 つ又は全ては、サーバ装置 20 のコンピュータ（プロセッサ、CPU（Central Processing Unit））で実行されるプログラムによりその機能を実現するようにしてもよい。該プログラムはコンピュータで読み出し可能なメモリ（例えば半導体ストレージ、磁気／光記録媒体等の媒体）に記憶保持される。

[0133] 本実施形態において、制御手段 24 は、評価手段 23 による評価結果に基づき、サービスのスタート、継続、又は、停止を制御するようにしてもよい。

[0134] 本実施形態において、評価手段 23 は、サービス（ svc ）のシナリオ S を通してのユーザ u （サービスを受ける利用者）の成功確率 $p(S^+ | u)$ 、及び、攻撃者 a （利用した攻撃者）による成功確率 $p(S^+ | u | a)$ を算出し、攻撃者による成功確率 $p(S^+ | u | a)$ と比較されるセキュリティパラメータ k 、及び、ユーザの成功確率 $p(S^+ | u)$ と比較されるユーザビリティパラメータ u_b の値をそれぞれ評価する。

[0135] 本実施形態において、制御手段 24 は、サービス（ svc ）のシナリオ

Sを通した攻撃者 a による成功確率 $p(S^+(u) | a)$ が前記セキュリティパラメータ k より小であり（式（22））、前記サービス（ srv ）のシナリオ S を通した前記ユーザ u の成功確率 $p(S^+(u) | u)$ が前記ユーザビリティパラメータ ub よりも大である（式（23））という条件で、前記シナリオ S を通した前記サービス（ srv ）をスタート又は継続する。

[0136] 本実施形態において、制御手段 24 は、前記サービス（ srv ）のシナリオ S を通した前記攻撃者 a による成功確率 $p(S^+(u) | a)$ が前記セキュリティパラメータ k を超えた場合、前記シナリオ S を通したサービス（ srv ）の提供を止め、前記サービス（ srv ）のシナリオ S を通した前記攻撃者 a による成功確率が前記セキュリティパラメータ k よりも小であるシナリオ S' に変更し、シナリオ S' による前記サービス（ srv ）を提供するようにしてもよい。

[0137] 本実施形態において、前記各手順（ f ）は、前記手順（ f ）が成功すると 1 を返し、失敗すると 0 を返す手順 f として表され、前記確率は、ユーザ u 、攻撃者 a が行った手順 f が成功して 1 が返す確率 $p(f^+(u) |)$ 、 $p(f^+(u) | a)$ を含む。

[0138] 本実施形態において、評価手段 23 において、シナリオ S を構成する手順 f が並列接続、直列接続、又はこれらの組み合わせ、にしたがって前記サービス（ srv ）のシナリオ S を通してのユーザの成功確率、前記攻撃者による成功確率を計算する（上式（15）～（17）参照）。

[0139] 図 6 は、図 5 の評価手段 23 の処理の例を説明するための図である。図 6 (A) において、各シナリオに対する $p(S^+(u) | a)$ の欄において、記号○は、当該シナリオを通した攻撃者 a による成功確率 $p(S^+(u) | a)$ が、サービス 1 に対して設定されたセキュリティパラメータ k_1 よりも小であることを表し（式（22））、記号×は、該 $p(S^+(u) | a)$ がセキュリティパラメータ k_1 を超えている（以上である）ことを表している。また、 $p(S^+(u) | u)$ の欄において、記号○は、当該シナリオを通したユーザ u による成功確率 $p(S^+(u) | u)$ が、サービス 1 に対して設定された

ユーザビリティパラメータ u_{b1} よりも大であることを表し（式（23））、記号 $\times$ は、 $p(S^+(u) | u)$ がユーザビリティパラメータ u_{b1} 以下であることを表している。

[0140] 図6（A）のサービス1には、シナリオA1～シナリオA5があるとする。評価手段（図5の23／16）は、シナリオA1～シナリオA5のそれぞれについて、当該シナリオを通した攻撃者 a による成功確率 $p(S^+(u) | a)$ がセキュリティパラメータ k_1 より小であり、且つ、ユーザ u の成功確率 $p(S^+(u) | u)$ がユーザビリティパラメータ u_{b1} よりも大であるかという条件を満たすか否かチェックする。図6（A）の例では、シナリオA2だけが、該条件を満たしている。前述したように、シナリオSにおいて、攻撃者 a による成功確率 $p(S^+(u) | a)$ が k を超えた際、シナリオSを通したサービス提供を止め、 $p(S^+(u_j) | a) < k$ となるようなシナリオA2、A5によるサービスを受け付けるようにしてもよい。

[0141] 図6（B）のサービス2には、シナリオB1～シナリオB4があり、該サービス2に対して設定されたセキュリティパラメータ k_2 、ユーザビリティパラメータ u_{b2} が設定されているものとする。評価手段（図5の23／16）は、シナリオB1～シナリオB4のそれぞれについて、当該シナリオを通した攻撃者 a による成功確率 $p(S^+(u) | a)$ がセキュリティパラメータ k_2 より小であり、且つ、ユーザ u の成功確率 $p(S^+(u) | u)$ がユーザビリティパラメータ u_{b2} よりも大であるかという条件を満たすか否かチェックする。図6（B）の例では、シナリオB2、B3だけが、該条件を満たしており、シナリオB1、B4は、セキュリティ、ユーザビリティに関する条件（式（22）、式（23））を満たしていない。

[0142] なお、図6等にした例は、多要素認証の評価例を説明するためのものであり、本発明がかかる構成に制限されるものでないことは勿論である。

[0143] なお、上記の非特許文献の各開示を、本書に引用をもって繰り込むものとする。本発明の全開示（請求の範囲を含む）の枠内において、さらにその基本的技術思想に基づいて、実施形態ないし実施例の変更・調整が可能である

。また、本発明の請求の範囲の枠内において種々の開示要素（各付記の各要素、各実施例の各要素、各図面の各要素等を含む）の多様な組み合わせ乃至選択が可能である。すなわち、本発明は、請求の範囲を含む全開示、技術的思想にしたがって当業者であればなし得るであろう各種変形、修正を含むことは勿論である。

[0144] 上記した実施形態は例えば以下のように付記される（ただし以下に制限されない）。

[0145] （付記１）

端末に通信接続する多要素認証装置であって、

前記端末がサービスの提供を受けるために必要とされる多要素認証の手順の組み合わせからなるシナリオを、前記サービスに対応させて記憶するとともに、前記各手順に対応させて、前記手順が成功する確率を記憶する記憶部と、

前記手順に関する前記確率に基づき、前記サービスのシナリオを通しての成功確率を算出し、前記成功確率に基づきセキュリティ及びユーザビリティの少なくとも一方を評価する評価手段（評価部）と、

前記評価結果にしたがって、前記端末に対する前記サービスを制御する制御手段（制御部）と、

を備えた、ことを特徴とする多要素認証装置。

[0146] （付記２）

前記制御手段（制御部）は、前記評価結果に基づき、前記端末に対する前記サービスのスタート、継続、又は、停止を制御する、ことを特徴とする付記１記載の多要素認証装置。

[0147] （付記３）

前記評価手段（評価部）は、前記サービスのシナリオを通してのユーザの成功確率、及び、攻撃者による成功確率を算出し、

前記攻撃者による成功確率と比較されるセキュリティパラメータ、及び、前記ユーザの成功確率と比較されるユーザビリティパラメータの値をそれぞれ

れ評価し、

前記制御手段（制御部）は、前記サービスのシナリオを通した前記攻撃者による成功確率が前記セキュリティパラメータより小であり、且つ、前記サービスのシナリオを通した前記ユーザの成功確率が前記ユーザビリティパラメータよりも大であるという条件で、前記端末に対する前記サービスの開始又は継続を制御する、ことを特徴とする付記 1 又は 2 記載の多要素認証装置。

[0148] （付記 4）

前記制御手段（制御部）は、前記サービスのシナリオを通した前記攻撃者による成功確率が前記セキュリティパラメータを超えた場合、前記端末に対する前記シナリオを通したサービスの提供を止め、

前記サービスのシナリオを通した前記攻撃者による成功確率が前記セキュリティパラメータよりも小であるシナリオに変更した上で、前記端末に対して前記サービスを提供するように制御する、ことを特徴とする付記 3 記載の多要素認証装置。

[0149] （付記 5）

前記各手順は、前記手順が成功すると 1 を返し、失敗すると 0 を返す手順 f として表され、

前記確率は、ユーザ、攻撃者が行った前記手順 f が成功して 1 が返す確率を含み、

前記評価手段（評価部）において、

前記シナリオを構成する手順が並列接続、直列接続、又はこれらの組み合わせ、にしたがって前記サービスのシナリオを通してのユーザの成功確率、前記攻撃者による成功確率を計算する、ことを特徴とする付記 1 乃至 4 のいずれかに記載の多要素認証装置。

[0150] （付記 6）

前記記憶部に記憶されるシナリオに対する手順、前記手順が成功する確率、前記サービスに対するセキュリティ及びユーザビリティの設定、保持、又

は変更を管理する管理手段（管理部）を備えた、ことを特徴とする付記 1 乃至 5 のいずれかに記載の多要素認証装置。

[0151] （付記 7）

付記 1 乃至 6 のいずれかに記載の多要素認証装置を含むサーバ装置。

[0152] （付記 8）

端末と、付記 1 乃至 6 のいずれかに記載の多要素認証装置とを備えた認証システム。

[0153] （付記 9）

通信接続する端末がサービスの提供を受けるために必要とされる多要素認証の手順の組み合わせからなるシナリオを前記サービスに対応させて記憶部で記憶するとともに、前記各手順に対応させて、前記手順が成功する確率を前記記憶部で記憶し、

前記手順に関する前記確率に基づき、前記サービスのシナリオを通しての成功確率を算出し、前記成功確率に基づきセキュリティ及びユーザビリティの少なくとも一方を評価し、

前記評価結果にしたがって、前記端末に対する前記サービスを制御する、ことを特徴とする多要素認証方法。

[0154] （付記 10）

前記評価結果に基づき、前記端末に対する前記サービスのスタート、継続、又は、停止を制御する、ことを特徴とする付記 9 記載の多要素認証方法。

[0155] （付記 11）

前記評価にあたり、前記サービスのシナリオを通してのユーザの成功確率、及び、攻撃者による成功確率を算出し、前記攻撃者による成功確率と比較されるセキュリティパラメータ、及び、前記ユーザの成功確率と比較されるユーザビリティパラメータの値をそれぞれ評価し、

前記サービスのシナリオを通した前記攻撃者による成功確率が前記セキュリティパラメータより小であり、且つ、前記サービスのシナリオを通した前記ユーザの成功確率が前記ユーザビリティパラメータよりも大であるという

条件で、前記端末に対する前記サービスの開始又は継続を制御する、ことを特徴とする付記 9 又は 10 記載の多要素認証方法。

[0156] (付記 12)

前記サービスのシナリオを通した前記攻撃者による成功確率が前記セキュリティパラメータを超えた場合、前記端末に対する前記シナリオを通したサービスの提供を止め、前記サービスのシナリオを通した前記攻撃者による成功確率が前記セキュリティパラメータよりも小であるシナリオに変更した上で、前記端末に対して前記サービスを提供するように制御する、ことを特徴とする付記 11 記載の多要素認証方法。

[0157] (付記 13)

前記各手順は、前記手順が成功すると 1 を返し、失敗すると 0 を返す手順 f として表され、

前記確率は、ユーザ、攻撃者が行った前記手順 f が成功して 1 が返す確率を含み、

前記評価手段において、前記シナリオを構成する手順が並列接続、直列接続、又はこれらの組み合わせ、にしたがって前記サービスのシナリオを通してのユーザの成功確率、前記攻撃者による成功確率を計算する、ことを特徴とする付記 9 乃至 12 のいずれかに記載の多要素認証方法。

[0158] (付記 14)

通信接続する端末がサービスの提供を受けるために必要とされる多要素認証の手順の組み合わせからなるシナリオを前記サービスに対応させて記憶部で記憶するとともに、前記各手順に対応させて、前記手順が成功する確率を前記記憶部で記憶する処理、

前記手順に関する前記確率に基づき、前記サービスのシナリオを通しての成功確率を算出し、前記成功確率に基づきセキュリティ及びユーザビリティの少なくとも一方を評価する評価処理、及び、

前記評価結果にしたがって、前記端末に対する前記サービスを制御する制御処理、

をコンピュータに実行させるプログラム。

[0159] (付記 15)

前記制御処理は、前記評価結果に基づき、前記端末に対する前記サービスのスタート、継続、又は、停止を制御する、ことを特徴とする付記 14 記載のプログラム。

[0160] (付記 16)

前記評価処理は、前記サービスのシナリオを通してのユーザの成功確率、及び、攻撃者による成功確率を算出し、

前記攻撃者による成功確率と比較されるセキュリティパラメータ、及び、前記ユーザの成功確率と比較されるユーザビリティパラメータの値をそれぞれ評価し、

前記制御処理は、前記サービスのシナリオを通した前記攻撃者による成功確率が前記セキュリティパラメータより小であり、且つ、前記サービスのシナリオを通した前記ユーザの成功確率が前記ユーザビリティパラメータよりも大であるという条件で、前記端末に対する前記サービスの開始又は継続を制御する、ことを特徴とする付記 14 又は 15 記載のプログラム。

[0161] (付記 17)

前記制御処理は、前記サービスのシナリオを通した前記攻撃者による成功確率が前記セキュリティパラメータを超えた場合、前記端末に対する前記シナリオを通したサービスの提供を止め、

前記サービスのシナリオを通した前記攻撃者による成功確率が前記セキュリティパラメータよりも小であるシナリオに変更した上で、前記端末に対して前記サービスを提供するように制御する、ことを特徴とする付記 14 記載のプログラム。

[0162] (付記 18)

前記各手順は、前記手順が成功すると 1 を返し、失敗すると 0 を返す手順 f として表され、

前記確率は、ユーザ、攻撃者が行った前記手順 f が成功して 1 が返す確率

を含み、

前記評価処理において、

前記シナリオを構成する手順が並列接続、直列接続、又はこれらの組み合わせ、にしたがって前記サービスのシナリオを通してのユーザの成功確率、前記攻撃者による成功確率を計算する、ことを特徴とする付記 14 乃至 17 のいずれかに記載のプログラム。

[0163] (付記 19)

前記記憶部に記憶されるシナリオに対する手順、前記手順が成功する確率、前記サービスに対するセキュリティ及びユーザビリティの設定、保持、変更を管理する処理を前記コンピュータに実行させる付記 14 乃至 18 のいずれかに記載のプログラム。

[0164] (付記 20)

付記 14 乃至 19 のいずれかのプログラムを記録したコンピュータ読み出し可能な記憶媒体。

符号の説明

- [0165] 1 入力
2 計算
3 出力
4 計算
5 外部への接続
20 サーバ（多要素認証装置）
21 記憶部
22 管理手段（管理部）
23 評価手段（評価部）
24 制御手段（制御部）

請求の範囲

- [請求項1] 端末に通信接続し、多要素認証を行う装置であって、
- 前記端末がサービスの提供を受けるために必要とされる多要素認証の手順の組み合わせからなるシナリオを、前記サービスに対応させて記憶するとともに、前記各手順に対応させて、前記手順が成功する確率を記憶する記憶部と、
- 前記手順に関する前記確率に基づき、前記サービスのシナリオを通しての成功確率を算出し、前記成功確率に基づきセキュリティ及びユーザビリティの少なくとも一方を評価する評価手段と、
- 前記評価結果にしたがって、前記端末に対する前記サービスを制御する制御手段と、
- を備えた、ことを特徴とする多要素認証装置。
- [請求項2] 前記制御手段は、前記評価結果に基づき、前記端末に対する前記サービスのスタート、継続、又は、停止を制御する、ことを特徴とする請求項1記載の多要素認証装置。
- [請求項3] 前記評価手段は、前記サービスのシナリオを通してのユーザの成功確率、及び、攻撃者による成功確率を算出し、
- 前記攻撃者による成功確率と比較されるセキュリティパラメータ、及び、前記ユーザの成功確率と比較されるユーザビリティパラメータの値をそれぞれ評価し、
- 前記制御手段は、前記サービスのシナリオを通した前記攻撃者による成功確率が前記セキュリティパラメータより小であり、且つ、前記サービスのシナリオを通した前記ユーザの成功確率が前記ユーザビリティパラメータよりも大であるという条件で、前記端末に対する前記サービスの開始又は継続を制御する、ことを特徴とする請求項1又は2記載の多要素認証装置。
- [請求項4] 前記制御手段は、前記サービスのシナリオを通した前記攻撃者による成功確率が前記セキュリティパラメータを超えた場合、前記端末に

対する前記シナリオを通したサービスの提供を止め、

前記サービスのシナリオを通した前記攻撃者による成功確率が前記セキュリティパラメータよりも小であるシナリオに変更した上で、前記端末に対して前記サービスを提供するように制御する、ことを特徴とする請求項3記載の多要素認証装置。

[請求項5] 前記各手順は、前記手順が成功すると1を返し、失敗すると0を返す手順fとして表され、

前記確率は、ユーザ、攻撃者が行った前記手順fが成功して1が返す確率を含み、

前記評価手段において、

前記シナリオを構成する手順が並列接続、直列接続、又はこれらの組み合わせ、にしたがって前記サービスのシナリオを通してのユーザの成功確率、前記攻撃者による成功確率を計算する、ことを特徴とする請求項1乃至4のいずれか1項に記載の多要素認証装置。

[請求項6] 前記記憶部に記憶される前記シナリオに対する手順、前記手順が成功する確率、前記サービスに対するセキュリティ及びユーザビリティの少なくとも一方の設定、保持、又は変更を管理する管理手段を備えた、ことを特徴とする請求項1乃至5のいずれか1項に記載の多要素認証装置。

[請求項7] 請求項1乃至6のいずれか1項に記載の多要素認証装置を含むサーバ装置。

[請求項8] 端末と、請求項1乃至6のいずれか1項に記載の多要素認証装置とを備えた認証システム。

[請求項9] 通信接続する端末がサービスの提供を受けるために必要とされる多要素認証の手順の組み合わせからなるシナリオを前記サービスに対応させて記憶部で記憶するとともに、前記各手順に対応させて、前記手順が成功する確率を前記記憶部で記憶し、

前記手順に関する前記確率に基づき、前記サービスのシナリオを通

しての成功確率を算出し、前記成功確率に基づきセキュリティ及びユーザビリティの少なくとも一方を評価し、

前記評価結果にしたがって、前記端末に対する前記サービスを制御する、ことを特徴とする多要素認証方法。

[請求項10] 前記評価結果に基づき、前記端末に対する前記サービスのスタート、継続、又は、停止を制御する、ことを特徴とする請求項9記載の多要素認証方法。

[請求項11] 前記評価にあたり、前記サービスのシナリオを通してのユーザの成功確率、及び、攻撃者による成功確率を算出し、前記攻撃者による成功確率と比較されるセキュリティパラメータ、及び、前記ユーザの成功確率と比較されるユーザビリティパラメータの値をそれぞれ評価し、

前記サービスのシナリオを通した前記攻撃者による成功確率が前記セキュリティパラメータより小であり、且つ、前記サービスのシナリオを通した前記ユーザの成功確率が前記ユーザビリティパラメータよりも大であるという条件で、前記端末に対する前記サービスの開始又は継続を制御する、ことを特徴とする請求項9又は10記載の多要素認証方法。

[請求項12] 前記サービスのシナリオを通した前記攻撃者による成功確率が前記セキュリティパラメータを超えた場合、前記端末に対する前記シナリオを通したサービスの提供を止め、前記サービスのシナリオを通した前記攻撃者による成功確率が前記セキュリティパラメータよりも小であるシナリオに変更した上で、前記端末に対して前記サービスを提供するように制御する、ことを特徴とする請求項11記載の多要素認証方法。

[請求項13] 前記各手順は、前記手順が成功すると1を返し、失敗すると0を返す手順 f として表され、

前記確率は、ユーザ、攻撃者が行った前記手順 f が成功して1が返

す確率を含み、

前記評価手段において、前記シナリオを構成する手順が並列接続、直列接続、又はこれらの組み合わせ、にしたがって前記サービスのシナリオを通してのユーザの成功確率、前記攻撃者による成功確率を計算する、ことを特徴とする請求項9乃至12のいずれか1項に記載の多要素認証方法。

[請求項14]

端末に通信接続し、多要素認証を行うコンピュータに、

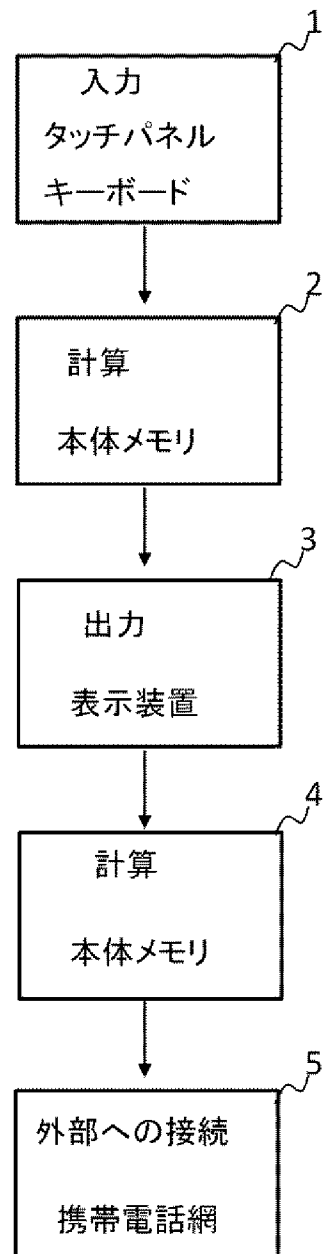
前記端末がサービスの提供を受けるために必要とされる多要素認証の手順の組み合わせからなるシナリオを前記サービスに対応させて記憶部で記憶するとともに、前記各手順に対応させて、前記手順が成功する確率を前記記憶部で記憶する処理、

前記手順に関する前記確率に基づき、前記サービスのシナリオを通しての成功確率を算出し、前記成功確率に基づきセキュリティ及びユーザビリティの少なくとも一方を評価する処理、及び、

前記評価結果にしたがって、前記端末に対する前記サービスを制御する処理、

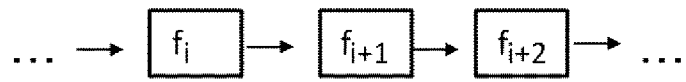
を実行させるプログラム。

[図1]

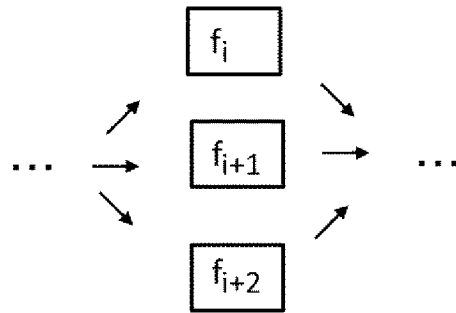


[図2]

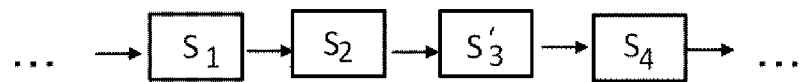
(A)



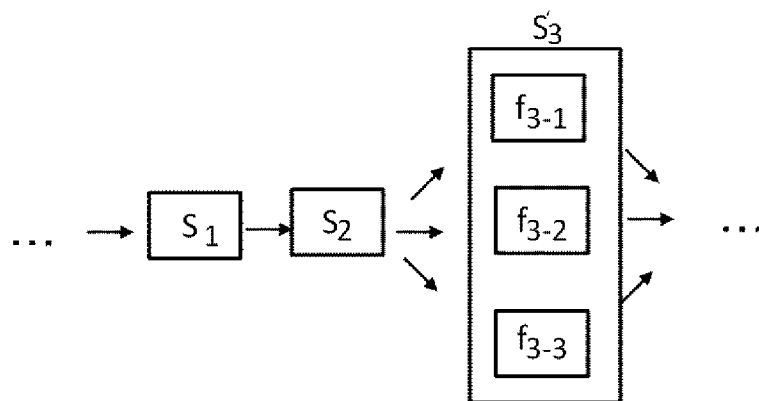
(B)



(C)



(D)



[図3]

(A)

入力機器	センサ	外部接続	出力	セキュアエレメント
タッチパネルキーボード	ジャイロセンサ	携帯電話網	ディスプレイ	キャリアSIM
マイク	GPSセンサ	Bluetooth	スピーカー	TPM
ボタン	温度計・湿度計	NFC	ライト	Felica
カメラ	光センサ	WiFi	バイブレーション	ソフトウェアSIM
指紋センサ	ガイガーカウンタ	USB	本体メモリ	クラウドSIM
		CTIA	SDカード	

(B)

手順	ログイン依頼者	誰のIDを使って ログインするか	成功／失敗	確率
$f(u)$	u	U	1	$p(f(u) u)$
$f(u)$	u	U	0	$p(f(u) u)$
$f(a)$	a	U	1	$p(f(u) a)$
$f(a)$	a	U	0	$p(f(u) a)$

[図4]

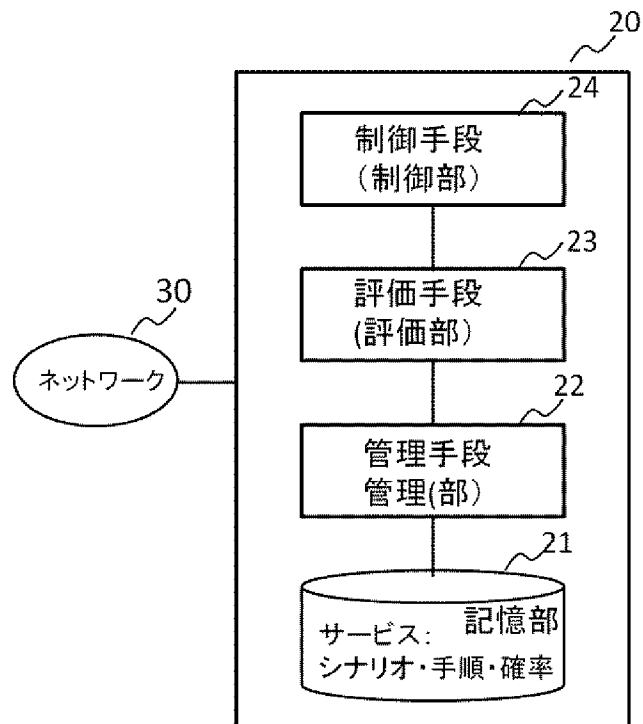
(A)

サービス	コスト	セキュリティ パラメータ	ユーザビリティ パラメータ
$s r v c_1$	$c o s t_1$	k_1	$u b_1$
$s r v c_2$	$c o s t_2$	k_2	$u b_2$
$s r v c_3$	$c o s t_3$	k_3	$u b_3$
.	.	.	.
.	.	.	.
.	.	.	.

(B)

シナリオ	攻撃の成功率	ユーザの失敗率
S_1	$p(S^+_1(u_j) a)$	$p(S^+_1(u_j) u_j)$
S_2	$p(S^+_2(u_j) a)$	$p(S^+_2(u_j) u_j)$
.	.	.
.	.	.
.	.	.
S_n	$p(S^+_n(u_j) a)$	$p(S^+_n(u_j) u_j)$

[図5]



[図6]

(A)

サービス1

	$p(S(u) a)$	$p(S(u) u)$
シナリオSA1	×	×
シナリオSA2	○	○
シナリオSA3	×	×
シナリオSA4	×	○
シナリオSA5	○	×

セキュアパラメータ:k1

ユーザビリティパラメータ:ub1

(B)

サービス2

	$p(S(u) a)$	$p(S(u) u)$
シナリオSB1	×	×
シナリオSB2	○	○
シナリオSB3	○	○
シナリオSB4	×	×

セキュアパラメータ:k2

ユーザビリティパラメータ:ub2

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2016/051268

A. CLASSIFICATION OF SUBJECT MATTER

G06F21/31(2013.01)i, G06F21/12(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F21/31, G06F21/12

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

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2016
Kokai Jitsuyo Shinan Koho	1971-2016	Toroku Jitsuyo Shinan Koho	1994-2016

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2013/0055346 A1 (ALCATEL-LUCENT USA INC.), 28 February 2013 (28.02.2013), paragraphs [0014], [0017] to [0035]; fig. 1 to 3 & WO 2013/028346 A1	1-14
A	Isoo UENO et al., "An Evaluation Method of Combined Authentication Techniques Including Biometric Authentication Techniques", IEICE Technical Report, 13 January 2011 (13.01.2011), vol.110, no.372, pages 1 to 6	1-14
A	JP 2009-175984 A (Nippon Telegraph and Telephone Corp.), 06 August 2009 (06.08.2009), paragraphs [0044] to [0076]; fig. 1 to 6 (Family: none)	1-14

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search
25 March 2016 (25.03.16)

Date of mailing of the international search report
05 April 2016 (05.04.16)

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2016/051268

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2008-250446 A (Nippon Telegraph and Telephone Corp.), 16 October 2008 (16.10.2008), paragraphs [0052] to [0055]; fig. 3 (Family: none)	1-14

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl. G06F21/31(2013.01)i, G06F21/12(2013.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int.Cl. G06F21/31, G06F21/12

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2016年
日本国実用新案登録公報	1996-2016年
日本国登録実用新案公報	1994-2016年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	US 2013/0055346 A1 (ALCATEL-LUCENT USA INC.) 2013.02.28, 段落 [0014]、[0017] - [0035]、FIG. 1-3 & WO 2013/028346 A1	1-14
A	上野 磯生 他, 生体認証を含めた多要素認証の評価方法, 電子情報通信学会技術研究報告, 2011.01.13, Vol. 110 No. 372, p. 1-6	1-14

☒ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

- | | |
|---|---|
| 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの | 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの |
| 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの | 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの |
| 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す） | 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの |
| 「O」 口頭による開示、使用、展示等に言及する文献 | 「&」 同一パテントファミリー文献 |
| 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願 | |

国際調査を完了した日

25.03.2016

国際調査報告の発送日

05.04.2016

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）

青木 重徳

5 S

4229

電話番号 03-3581-1101 内線 3546

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	JP 2009-175984 A (日本電信電話株式会社) 2009. 08. 06, 段落 [0 0 4 4] - [0 0 7 6]、[図 1] - [図 6] (ファミリーなし)	1 - 1 4
A	JP 2008-250446 A (日本電信電話株式会社) 2008. 10. 16, 段落 [0 0 5 2] - [0 0 5 5]、[図 3] (ファミリーなし)	1 - 1 4