(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
2020年1月23日(23.01.2020)

WIPO | PCT

(10) 国際公開番号
WO 2020/016985 A1

(51) 国際特許分類:
G06F 21/31 (2013.01)

(21) 国際出願番号： PCT/JP2018/027067

(22) 国際出願日： 2018年7月19日(19.07.2018)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

(71) 出願人:三菱電機株式会社(**MITSUBISHI ELECTRIC CORPORATION**) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目7番3号 Tokyo (JP).

(72) 発明者: 反町 孝平 (**TAMMACHI, Kohei**); 〒1008310 東京都千代田区丸の内二丁目7番3号 三菱電機株式会社内 Tokyo (JP).

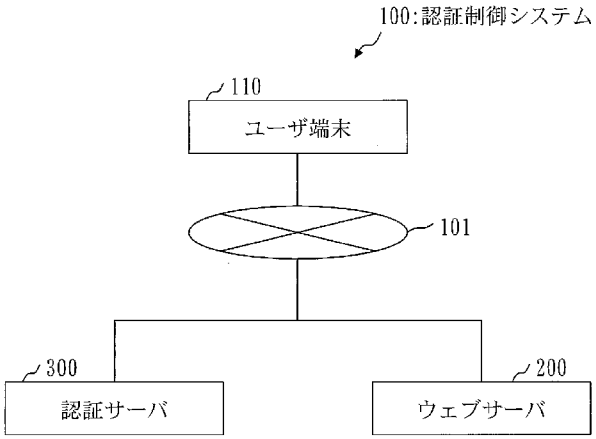
(74) 代理人: 溝井国際特許業務法人(**MIZOI INTERNATIONAL PATENT FIRM**); 〒2470056 神奈川県鎌倉市大船二丁目17番10号3階 Kanagawa (JP).

(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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY,

(54) **Title:** AUTHENTICATION CONTROL SYSTEM AND AUTHENTICATION CONTROL PROGRAM

(54) 発明の名称： 認証制御システムおよび認証制御プログラム

[図1]



100 Authentication control system
110 User terminal
200 Web server
300 Authentication server

(57) **Abstract:** An authentication server (300) determines whether there is a registration identifier that is the same as a login identifier. If there is a registration identifier that is the same as the login identifier, the authentication server determines whether the login password is the correct password. If authentication fails, a web server (200) determines whether the number of failed logins that used a login identifier that is the same as the abovementioned login identifier has reached an upper limit. If the number of failed logins that used a login identifier that is the same as the abovementioned login

WO 2020/016985 A1

[続葉有]

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), ユーラシア (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:

一 国際調査報告(条約第21条(3))

identifier has reached the upper limit, the web server displays an account lock screen regardless of whether or not there is a registration identifier that is the same as the login identifier.

(57) 要約:認証サーバ(３００)は、ログイン識別子と同じ登録識別子が存在するか判定する。前記ログイン識別子と同じ登録識別子が存在する場合、前記認証サーバは、ログインパスワードが正しいパスワードであるか判定する。認証が失敗した場合、ウェブサーバ(２００)は、前記ログイン識別子と同じログイン識別子を用いたログインの失敗回数が上限回数に達しているか判定する。前記ログイン識別子と同じログイン識別子を用いたログインの失敗回数が上限回数に達している場合、前記ウェブサーバは、前記ログイン識別子と同じ登録識別子が存在するか否かに関わらず、アカウントロック画面を表示させる。

明　細　書

発明の名称 ： 認証制御システムおよび認証制御プログラム

技術分野

[0001] 本発明は、ログイン時の認証制御に関するものである。

背景技術

[0002] ウェブアプリケーションのログインにおいて、一般的に、ユーザ識別子とパスワードとを用いた認証が行われる。

このような認証に対して、任意のユーザ識別子に対して複数のパスワードを用いて、有効なアカウントを取得しようとする攻撃が行われる。この攻撃は、ブルートフォース攻撃（ＢＦ攻撃）と呼ばれる。

[0003] ＢＦ攻撃では、ユーザ識別子を固定してパスワードを毎回変更してログインが繰り返し行われる。例えば、総当たり攻撃または辞書攻撃が行われる。総当たり攻撃は、ユーザ閾別子とパスワードとのそれぞれについて、全ての文字列（例えば、数字４桁の場合は００００から９９９９まで）を試す攻撃である。辞書攻撃は、ユーザ識別子とパスワードとのそれぞれについて、よく使用される文字列がリスト化されてリスト内の文字列を試す攻撃である。

[0004] ＢＦ攻撃の一般的な対策として、有効なアカウントに対して一定回数以上のログイン失敗が発生した場合にアカウントロックが行われる。アカウントロックが行われると、そのアカウントが一定時間利用不可能になる。または、アカウントロックが管理者によって解除されるまで、そのアカウントが利用不可能になる。

一般的に、アカウントロックされたことがＢＦ攻撃の実行者に判明しないよう、ウェブアプリケーションは、アカウントロックの有無によって、ログイン試行の応答画面を変更しない。

[0005] 正規ユーザがユーザ識別子とパスワードとを誤って覚えている場合、一定回数以上のログイン失敗が発生し、アカウントロックされてしまう。このとき、ログイン試行の応答画面が変更されないと、正規ユーザがアカウントロ

ックに気付かないことがある。

[0006] 特許文献１において、不要なアカウントロックが発生することを低減させることを目的とした認証方式が提案されている。

この認証方式では、正規ユーザがパスワードを誤って覚えている場合が想定される。一定期間内に有効なユーザ識別子と同じパスワードとの組が使用されてログインが繰り返し失敗した場合、ウェブアプリケーションを介して、ユーザに既に失敗しているパスワードであることが通知される。これにより、アカウントロックのトリガーとなるカウントを増加させないようにすることが可能となる。

しかし、攻撃者が任意のユーザ識別子を使用してログインを２回試行すると、試行されたユーザ識別子が有効なユーザ識別子であると判明してしまう場合がある。具体的には、試行されたユーザ識別子が有効なユーザ識別子である場合、既に失敗しているパスワードが表示される。この場合、試行されたユーザ識別子が有効なユーザ識別子であることが判明してしまう。

また、正規ユーザがユーザ識別子を誤って覚えている場合、入力されたユーザ識別子が有効でないため、ログイン失敗時にウェブアプリケーションの画面に変化がない。そのため、正規ユーザは、入力したユーザ識別子が誤っていることに気付くことができない。

[0007] 特許文献２において、アカウントロックされたユーザがアカウントロックを解除することによってアカウントロック後のユーザの利便性を向上させることを目的とした認証方式が提案されている。

この認証方式では、通常アカウントと解除用アカウントとが生成される。通常アカウントがアカウントロックされた場合、ウェブアプリケーションを介して、解除用アカウントの入力が指示される。ユーザは、解除用アカウントを入力することにより、通常アカウントのアカウントロックを解除することができる。

しかし、攻撃者が任意のユーザ識別子を使用してＢＦ攻撃を実行すると、有効な通常アカウントが判明してしまう場合がある。具体的には、使用され

たユーザ識別子が有効なユーザ識別子である場合、解除用アカウントの入力が表示される。この場合、使用されたユーザ識別子が有効な通常アカウントであることが判明してしまう。

また、正規ユーザが通常アカウントを誤って覚えている場合、入力された通常アカウントが有効なアカウントでないため、ログイン失敗時にウェブアプリケーションの画面に変化がない。そのため、正規ユーザは、入力した通常アカウントが誤っていることに気付くことができない。

先行技術文献

特許文献

[0008] 特許文献1：特開２０１６－１１９０１７号公報

特許文献2：特開２００８－０４６８６７号公報

発明の概要

発明が解決しようとする課題

[0009] 正規ユーザがユーザ識別子またはパスワードを誤って覚えている場合、正規ユーザは、ユーザ識別子とパスワードとの誤った組によってログインを複数回試行する。そして、アカウントロックが発生する。しかし、ウェブアプリケーションの画面にはアカウントロックを示す情報が表示されない。そのため、正規ユーザがさらにログインを試行することとなり、ユーザの利便性を下げてしまう。

また、ウェブアプリケーションの画面にアカウントロックを示す情報が表示される場合、試行されたユーザ識別子が有効なユーザ識別子であることが攻撃者に判明してしまう。そして、そのユーザ識別子が更なる攻撃に利用される可能性がある。

[0010] 本発明は、正規ユーザがユーザ識別子またはパスワードを誤って覚えている場合であっても、セキュリティを保ったまま、正規ユーザの利便性を向上できるようにすることを目的とする。

課題を解決するための手段

[0011] 本発明の認証制御システムは、

ログイン識別子とログインパスワードとを受け付ける受付部と、

１つ以上の登録識別子と１つ以上の登録パスワードとが互いに対応付けられたアカウント管理ファイルに基づいて前記ログイン識別子と同じ登録識別子が存在するか判定する識別子判定部と、

前記ログイン識別子と同じ登録識別子が存在する場合に前記アカウント管理ファイルに基づいて前記ログインパスワードが正しいパスワードであるか判定するパスワード判定部と、

前記ログイン識別子と同じ登録識別子が存在し、且つ、前記ログインパスワードが正しいパスワードでなく、且つ、前記ログイン識別子と同じログイン識別子を用いたログインの失敗回数が上限回数に達している場合に、アカウントロック画面を表示させる実在アカウントロック部と

前記ログイン識別子と同じ登録識別子が存在せず、且つ、前記ログイン識別子と同じログイン識別子を用いたログインの失敗回数が前記上限回数に達している場合に、アカウントロック画面を表示させる仮想アカウントロック部とを備える。

発明の効果

[0012] 本発明によれば、ログイン識別子がアカウント管理ファイル上の登録識別子のいずれかに一致するか否かに関わらず、アカウントロック画面が表示される。

アカウントロック画面が表示されると、正規ユーザは、ログイン識別子またはログインパスワードを誤って覚えていることを知ることができる。そのため、その後に、正規ユーザによる不要なログイン試行が発生しない。また、ログイン識別子がアカウント管理ファイル上の登録識別子と一致するか否かに関わらずアカウントロック画面が表示されるため、攻撃者は、ログイン識別子が有効なユーザ識別子であるか否かを判断することができない。

したがって、セキュリティを保ったまま、正規ユーザの利便性を向上させることが可能である。

図面の簡単な説明

[0013] [図1]実施の形態１における認証制御システム１００の構成図。

[図2]実施の形態１におけるウェブサーバ２００の構成図。

[図3]実施の形態１における認証サーバ３００の構成図。

[図4]実施の形態１における失敗ログイン管理ファイル２９１の構成図。

[図5]実施の形態１におけるログイン試行データ２９２の構成図。

[図6]実施の形態１におけるアカウント管理ファイル３９１の構成図。

[図7]実施の形態１における認証制御方法のフローチャート。

[図8]実施の形態１における認証処理（Ｓ１１０）のフローチャート。

[図9]実施の形態１におけるログイン失敗処理（Ｓ１３０）のフローチャート。

[図10]実施の形態１における実在アカウント処理（Ｓ１３２）のフローチャート。

[図11]実施の形態１における仮想アカウント処理（Ｓ１３３）のフローチャート。

[図12]実施の形態１における応答内容パターンを示す表。

[図13]実施の形態２におけるウェブサーバ２００の構成図。

[図14]実施の形態２におけるアドレステーブル２９３の構成図。

[図15]実施の形態２における認証制御方法のフローチャート。

[図16]実施の形態２におけるアドレス監視処理（Ｓ２１０）のフローチャート。

[図17]実施の形態２におけるアドレス決定処理（Ｓ２５０）のフローチャート。

[図18]実施の形態３におけるウェブサーバ２００の構成図。

[図19]実施の形態３における実在アカウント処理（Ｓ１３２）のフローチャート。

[図20]実施の形態３における仮想アカウント処理（Ｓ１３３）のフローチャート。

[図21]実施の形態３における上限操作処理（Ｓ３００）のフローチャート。

[図22]実施の形態４における認証制御システム１００の構成例を示す図。

[図23]実施の形態におけるウェブサーバ２００のハードウェア構成図。

[図24]実施の形態における認証サーバ３００のハードウェア構成図。

発明を実施するための形態

[0014] 実施の形態および図面において、同じ要素または対応する要素には同じ符号を付している。説明した要素と同じ符号が付された要素の説明は適宜に省略または簡略化する。図中の矢印はデータの流れ又は処理の流れを主に示している。

[0015] 実施の形態１．

認証制御システム１００について、図１から図１２に基づいて説明する。

[0016] ＊＊＊構成の説明＊＊＊

図１に基づいて、認証制御システム１００の構成を説明する。

認証制御システム１００は、ユーザ端末１１０とウェブサーバ２００と認証サーバ３００とを備える。

ユーザ端末１１０は、ウェブアプリケーションを利用するためにユーザ認証を受けるコンピュータである。

ウェブサーバ２００は、ユーザ端末１１０に対するユーザ認証を制御するサーバ装置である。

認証サーバ３００は、ユーザ認証を行うサーバ装置である。

ウェブサーバ２００は、ネットワーク１０１を介して、ユーザ端末１１０と認証サーバ３００と通信する。

[0017] 図２に基づいて、ウェブサーバ２００の構成を説明する。

ウェブサーバ２００は、プロセッサ２０１とメモリ２０２と補助記憶装置２０３と入出力インタフェース２０４といったハードウェアを備えるコンピュータである。これらのハードウェアは、信号線を介して互いに接続されている。

[0018] プロセッサ２０１は、演算処理を行うＩＣ（Ｉｎｔｅｇｒａｔｅｄ　Ｃｉ

ｒｃｕｉｔ）であり、他のハードウェアを制御する。例えば、プロセッサ２０１は、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）、ＤＳＰ（Ｄｉｇｉｔａｌ　Ｓｉｇｎａｌ　Ｐｒｏｃｅｓｓｏｒ）、またはＧＰＵ（Ｇｒａｐｈｉｃｓ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）である。

メモリ２０２は揮発性の記憶装置である。メモリ２０２は、主記憶装置またはメインメモリとも呼ばれる。例えば、メモリ２０２はＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）である。メモリ２０２に記憶されたデータは必要に応じて補助記憶装置２０３に保存される。

補助記憶装置２０３は不揮発性の記憶装置である。例えば、補助記憶装置２０３は、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）、ＨＤＤ（Ｈａｒｄ　Ｄｉｓｋ　Ｄｒｉｖｅ）、またはフラッシュメモリである。補助記憶装置２０３に記憶されたデータは必要に応じてメモリ２０２にロードされる。

入出力インタフェース２０４は入力装置および出力装置が接続されるポートである。例えば、入出力インタフェース２０４はＵＳＢ端子であり、入力装置はキーボード、マウスおよびレシーバであり、出力装置はディスプレイおよびトランスミッタである。ＵＳＢはＵｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓの略称である。

[0019] ウェブサーバ２００は、受付部２１０とログイン判定部２２０とアカウントロック部２３０と応答部２４０といった要素を備える。これらの要素はソフトウェアで実現される。

アカウントロック部２３０は、実在アカウントロック部２３１と仮想アカウントロック部２３２とを含む。

[0020] 補助記憶装置２０３には、受付部２１０とログイン判定部２２０とアカウントロック部２３０と応答部２４０としてコンピュータを機能させるための認証制御プログラムが記憶されている。認証制御プログラムは、メモリ２０２にロードされて、プロセッサ２０１によって実行される。

さらに、補助記憶装置２０３にはＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ）が記憶されている。ＯＳの少なくとも一部は、メモリ２０２にロードさ

れて、プロセッサ２０１によって実行される。

つまり、プロセッサ２０１は、ＯＳを実行しながら、認証制御プログラムを実行する。

認証制御プログラムを実行して得られるデータは、メモリ２０２、補助記憶装置２０３、プロセッサ２０１内のレジスタ、または、プロセッサ２０１内のキャッシュメモリといった記憶装置に記憶される。

[0021] 補助記憶装置２０３は記憶部２９０として機能する。但し、他の記憶装置が、補助記憶装置２０３の代わりに、又は、補助記憶装置２０３と共に、記憶部２９０として機能してもよい。

[0022] ウェブサーバ２００は、プロセッサ２０１を代替する複数のプロセッサを備えてもよい。複数のプロセッサは、プロセッサ２０１の役割を分担する。

[0023] 認証制御プログラムは、光ディスクまたはフラッシュメモリ等の不揮発性の記録媒体にコンピュータ読み取り可能に記録（格納）することができる。

[0024] 図３に基づいて、認証サーバ３００の構成を説明する。

認証サーバ３００は、プロセッサ３０１とメモリ３０２と補助記憶装置３０３と入出力インタフェース３０４といったハードウェアを備えるコンピュータである。これらのハードウェアは、信号線を介して互いに接続されている。

[0025] プロセッサ３０１は、演算処理を行うＩＣであり、他のハードウェアを制御する。例えば、プロセッサ３０１はＣＰＵ、ＤＳＰまたはＧＰＵである。

メモリ３０２は揮発性の記憶装置である。メモリ３０２は、主記憶装置またはメインメモリとも呼ばれる。例えば、メモリ３０２はＲＡＭである。メモリ３０２に記憶されたデータは必要に応じて補助記憶装置３０３に保存される。

補助記憶装置３０３は不揮発性の記憶装置である。例えば、補助記憶装置３０３は、ＲＯＭ、ＨＤＤまたはフラッシュメモリである。補助記憶装置３０３に記憶されたデータは必要に応じてメモリ３０２にロードされる。

入出力インタフェース３０４は入力装置および出力装置が接続されるポー

トである。例えば、入出力インタフェース３０４はＵＳＢ端子であり、入力装置はキーボード、マウスおよびレシーバであり、出力装置はディスプレイおよびトランスミッタである。

[0026] 認証サーバ３００は、認証部３１０を備える。認証部３１０はソフトウェアで実現される。

認証部３１０は、受付部３１１と識別子判定部３１２とロック状態判定部３１３とパスワード判定部３１４と応答部３１５とを含む。

[0027] 補助記憶装置３０３には、認証部３１０としてコンピュータを機能させるための認証プログラムが記憶されている。認証プログラムは、メモリ３０２にロードされて、プロセッサ３０１によって実行される。

さらに、補助記憶装置３０３にはＯＳが記憶されている。ＯＳの少なくとも一部は、メモリ３０２にロードされて、プロセッサ３０１によって実行される。

つまり、プロセッサ３０１は、ＯＳを実行しながら、認証プログラムを実行する。

認証プログラムを実行して得られるデータは、メモリ３０２、補助記憶装置３０３、プロセッサ３０１内のレジスタ、または、プロセッサ３０１内のキャッシュメモリといった記憶装置に記憶される。

[0028] 補助記憶装置３０３は記憶部３９０として機能する。但し、他の記憶装置が、補助記憶装置３０３の代わりに、又は、補助記憶装置３０３と共に、記憶部３９０として機能してもよい。

[0029] 認証サーバ３００は、プロセッサ３０１を代替する複数のプロセッサを備えてもよい。複数のプロセッサは、プロセッサ３０１の役割を分担する。

[0030] 認証プログラムは、光ディスクまたはフラッシュメモリ等の不揮発性の記録媒体にコンピュータ読み取り可能に記録（格納）することができる。

認証プログラムは、認証制御プログラムの一部である。

[0031] 図４に基づいて、失敗ログイン管理ファイル２９１の構成を説明する。失敗ログイン管理ファイル２９１は記憶部２９０に記憶される。

失敗ログイン管理ファイル２９１は、１つ以上の試行識別子と１つ以上の試行回数とを互いに対応付ける。

試行識別子は、ログインの失敗時にログイン識別子として指定されたユーザ識別子である。

試行回数は、ログイン試行識別子を用いたログインの失敗回数である。

例えば、図４の失敗ログイン管理ファイル２９１は、「ＲＥＤ」というユーザ識別子を用いたログインが９回失敗していることを示している。

[0032] 図５に基づいて、ログイン試行データ２９２の構成を説明する。ログイン試行データ２９２は記憶部２９０に記憶される。

ログイン試行データ２９２は、直近の試行識別子とその試行回数とを含む。

[0033] 図６に基づいて、アカウント管理ファイル３９１の構成を説明する。アカウント管理ファイル３９１は記憶部３９０に記憶される。

アカウント管理ファイル３９１は、１つ以上の登録識別子と１つ以上の登録パスワードと１つ以上のロック状態フラグとを互いに対応付ける。

登録識別子は、登録されているユーザ識別子である。つまり、登録識別子は、正規ユーザのユーザ識別子である。

登録パスワードは、登録されているユーザパスワードである。つまり、登録パスワードは、正規ユーザのパスワードである。アスタリスクはパスワードを表している。

登録識別子と登録パスワードとの組をアカウントと呼ぶ。

[0034] ロック状態フラグは、アカウントのロック状態を示す。具体的には、ロック状態フラグは、未ロックまたはロック中を示す。

未ロックは、アカウントがロックされていない状態を意味する。

ロック中は、アカウントがロックされている状態を意味する。

[0035] ＊＊＊動作の説明＊＊＊

認証制御システム１００の動作は認証制御方法に相当する。また、認証制御方法の手順は認証制御プログラムの手順に相当する。

[0036] 図７に基づいて、認証制御方法を説明する。

ステップＳ１０１において、ユーザは、ログイン識別子とログインパスワードとをユーザ端末１１０に入力する。

ログイン識別子は、ログインのために指定されたユーザ識別子である。

ログインパスワードは、ログインのために指定されたユーザパスワードである。

ログイン識別子とログインパスワードとを含んだデータをログインデータという。

[0037] ユーザ端末１１０は、ログインデータをウェブサーバ２００に送信する。

ウェブサーバ２００において、受付部２１０は、ログインデータを受信する。つまり、受付部２１０は、ログインデータを受け付ける。

[0038] ステップＳ１１０において、認証サーバ３００は、ログインデータに基づいて認証処理を行う。

[0039] 図８に基づいて、認証処理（Ｓ１１０）を説明する。

ステップＳ１１１において、ログイン判定部２２０は、ログインデータを認証サーバ３００に送信する。

認証サーバ３００において、受付部３１１は、ログインデータを受信する。つまり、受付部３１１は、ログインデータを受け付ける。つまり、受付部３１１は、ログイン識別子とログインパスワードとを受け付ける。

[0040] ステップＳ１１２において、識別子判定部３１２は、アカウント管理ファイル３９１に基づいて、ログイン識別子と同じ登録識別子が存在するか判定する。

具体的には、識別子判定部３１２は、ログイン識別子と同じ登録識別子がアカウント管理ファイル３９１に含まれるか判定する。ログイン識別子と同じ登録識別子がアカウント管理ファイル３９１に含まれる場合、識別子判定部３１２は、ログイン識別子と同じ登録識別子が存在すると判定する。

ログイン識別子と同じ登録識別子が存在する場合、処理はステップＳ１１３に進む。

ログイン識別子と同じ登録識別子が存在しない場合、処理はステップＳ１１６に進む。

[0041] ステップＳ１１３において、ロック状態判定部３１３は、アカウント管理ファイル３９１に基づいて、ログイン識別子に対応するアカウントのロック状態を判定する。

具体的には、ロック状態判定部３１３は、ログイン識別子と同じ登録識別子に対応付けられたロック状態フラグをアカウント管理ファイル３９１から選択する。そして、ロック状態判定部３１３は、選択されたロック状態フラグに基づいてアカウントのロック状態を判定する。

ログイン識別子に対応するアカウントのロック状態が未ロックである場合、処理はステップＳ１１４に進む。

ログイン識別子に対応するアカウントのロック状態がロック中である場合、処理はステップＳ１１７に進む。

[0042] ステップＳ１１４において、パスワード判定部３１４は、アカウント管理ファイル３９１に基づいて、ログインパスワードが正しいパスワードであるか判定する。

具体的には、パスワード判定部３１４は、ログイン識別子と同じ登録識別子に対応付けられた登録パスワードをアカウント管理ファイル３９１から選択する。そして、パスワード判定部３１４は、ログインパスワードを、選択された登録パスワードと比較する。ログインパスワードが選択された登録パスワードと一致する場合、パスワード判定部３１４は、ログインパスワードが正しいパスワードであると判定する。

ログインパスワードが正しいパスワードである場合、処理はステップＳ１１５に進む。

ログインパスワードが正しいパスワードでない場合、処理はステップＳ１１８に進む。

[0043] ステップＳ１１５において、応答部３１５は、認証結果（認証成功）をウェブサーバ２００に送信する。つまり、応答部３１５は、認証結果（認証成

功）を応答する。

ウェブサーバ２００において、ログイン判定部２２０は、認証結果（認証成功）を受信する。

認証結果（認証成功）は、認証が成功したことを示す認証結果である。

[0044] ステップＳ１１６において、応答部３１５は、認証結果（アカウント無し）をウェブサーバ２００に送信する。つまり、応答部３１５は、認証結果（アカウント無し）を応答する。

ウェブサーバ２００において、ログイン判定部２２０は、認証結果（アカウント無し）を受信する。

認証結果（アカウント無し）は、「アカウント無し」を理由に認証が失敗したことを示す認証結果である。

「アカウント無し」は、ログイン識別子と同じ登録識別子が存在しないこと、つまり、ログイン識別子に対応するアカウントが存在しないことを意味する。

[0045] ステップＳ１１７において、応答部３１５は、認証結果（ロック中）をウェブサーバ２００に送信する。つまり、応答部３１５は、認証結果（ロック中）を応答する。

ウェブサーバ２００において、ログイン判定部２２０は、認証結果（ロック中）を受信する。

認証結果（ロック中）は、「ロック中」を理由に認証が失敗したことを示す認証結果である。

「ロック中」は、ログイン識別子に対応するアカウントのロック状態がロック中であることを意味する。

[0046] ステップＳ１１８において、応答部３１５は、認証結果（パスワード誤り）をウェブサーバ２００に送信する。つまり、応答部３１５は、認証結果（パスワード誤り）を応答する。

ウェブサーバ２００において、ログイン判定部２２０は、認証結果（パスワード誤り）を受信する。

認証結果（パスワード誤り）は、「パスワード誤り」を理由に認証が失敗したことを示す認証結果である。

「パスワード誤り」は、ログインパスワードが正しいパスワードでないことを意味する。

[0047] 図７に戻り、ステップＳ１２１から説明を続ける。

ステップＳ１２１において、ログイン判定部２２０は、認証結果に基づいてログイン許否を判定する。

認証結果が認証成功を示す場合、ログイン判定部２２０はログインを許可する。認証結果が認証失敗を示す場合、ログイン判定部２２０はログインを許可しない。

ログインが許可される場合、処理はステップＳ１２２に進む。

ログインが許可されない場合、処理はステップＳ１３０に進む。

[0048] ステップＳ１２２において、応答部２４０は、ログイン成功を示すログイン結果データをユーザ端末１１０に送信する。つまり、応答部２４０はログイン成功を応答する。

ユーザ端末１１０は、ログイン結果データを受信する。ログイン結果データがログイン成功を示す場合、ユーザ端末１１０は、ログイン後の画面をディスプレイに表示する。

[0049] ステップＳ１３０において、アカウントロック部２３０は、認証結果に基づいてログイン失敗処理を行う。

[0050] 図９に基づいて、ログイン失敗処理（Ｓ１３０）を説明する。

ステップＳ１３１において、ログイン判定部２２０は、認証結果に基づいて、認証失敗の理由を判定する。

認証失敗の理由が「パスワード誤り」である場合、処理はステップＳ１３２に進む。

認証失敗の理由が「アカウント無し」である場合、処理はステップＳ１３３に進む。

認証結果の理由が「ロック中」である場合、処理はステップＳ１３４に進

む。

[0051] ステップＳ１３２において、ウェブサーバ２００は実在アカウント処理を行う。

実在アカウント処理は、アカウント管理ファイル３９１に登録されているアカウント、すなわち、実在するアカウントのための処理である。

実在アカウン処理（Ｓ１３２）の詳細については後述する。

[0052] ステップＳ１３３において、ウェブサーバ２００は仮想アカウント処理を行う。

仮想アカウント処理は、アカウント管理ファイル３９１に登録されていないアカウント、すなわち、実在しないアカウントのための処理である。

仮想アカウント処理（Ｓ１３３）の詳細については後述する。

[0053] ステップＳ１３４において、実在アカウントロック部２３１は、アカウントロック画面をユーザ端末１１０に表示させるために、アカウントロックを応答する。

アカウントロック画面は、アカウントがロックされた状態であることをユーザに知らせるための画面である。

[0054] 具体的には、実在アカウントロック部２３１は、アカウントロックの応答を応答部２４０に指示する。応答部２４０は、アカウントロックを示すログイン結果データをユーザ端末１１０に送信する。ユーザ端末１１０は、ログイン結果データを受信する。ログイン結果データがアカウントロックを示す場合、ユーザ端末１１０は、アカウントロック画面をディスプレイに表示する。

[0055] 図１０に基づいて、実在アカウントロック処理（Ｓ１３２）を説明する。

ステップＳ１３２１において、ログイン判定部２２０は、ログイン識別子の試行回数を取得する。

ログイン識別子の試行回数は、同じログイン識別子を用いたログインの失敗回数である。

[0056] 具体的には、ログイン判定部２２０は、ログイン識別子の試行回数を以下

のように取得する。

ログイン判定部２２０は、ログイン識別子がログイン試行データ２９２の中の試行識別子と同じであるか判定する。

[0057] ログイン識別子がログイン試行データ２９２の中の試行識別子と同じである場合、ログイン判定部２２０は、ログイン試行データ２９２の中の試行回数を１増加させる。そして、ログイン判定部２２０は、ログイン試行データ２９２から試行回数を取得する。

さらに、ログイン判定部２２０は、ログイン識別子と同じ試行識別子を見つけるため、失敗ログイン管理ファイル２９１を検索する。ログイン識別子と同じ試行識別子が失敗ログイン管理ファイル２９１に登録されている場合、ログイン判定部２２０は、ログイン識別子と同じ試行識別子に対応付けられている試行回数を１増加させる。ログイン識別子と同じ試行識別子が失敗ログイン管理ファイル２９１に登録されていない場合、ログイン判定部２２０は、ログイン試行データ２９２の中の試行回数を失敗ログイン管理ファイル２９１の中の最小の試行回数と比較する。ログイン試行データ２９２の中の試行回数が失敗ログイン管理ファイル２９１の中の最小の試行回数より大きい場合、ログイン判定部２２０は、失敗ログイン管理ファイル２９１の中の最小の試行回数に対応付けられた試行識別子をログイン試行データ２９２の中の試行識別子に置き換え、失敗ログイン管理ファイル２９１の中の最小の試行回数をログイン試行データ２９２の中の試行回数に置き換える。

[0058] ログイン識別子がログイン試行データ２９２の中の試行識別子と異なる場合、ログイン判定部２２０は、ログイン試行データ２９２の中の試行識別子をログイン識別子に変更し、ログイン試行データ２９２の中の試行回数を１にリセットする。そして、ログイン判定部２２０は、ログイン試行データ２９２から試行回数を取得する。

[0059] ステップＳ１３２２において、ログイン判定部２２０は、ログイン識別子の試行回数が上限回数に達しているか判定する。上限回数は、試行回数の上限であり、予め決められる。

具体的には、ログイン判定部２２０は、ログイン識別子の試行回数を上限回数と比較する。ログイン識別子の試行回数が上限回数以上である場合、ログイン判定部２２０は、ログイン識別子の試行回数が上限回数に達していると判定する。

ログイン識別子の試行回数が上限回数に達している場合、処理はステップＳ１３２３に進む。

ログイン識別子の試行回数が上限回数に達していない場合、処理はステップＳ１３２５に進む。

[0060] ステップＳ１３２３において、実在アカウントロック部２３１は、認証サーバ３００のアカウント管理ファイル３９１にアクセスし、ログイン識別子と同じ登録識別子をアカウント管理ファイル３９１から選択する。そして、実在アカウントロック部２３１は、選択した登録識別子に対応付けられたロック状態フラグに「ロック中」を設定する。

[0061] ステップＳ１３２４において、実在アカウントロック部２３１は、アカウントロック画面をユーザ端末１１０に表示させるために、アカウントロックを応答する。

ステップＳ１３２４の処理は、ステップＳ１３４の処理と同じである（図９参照）。

[0062] ステップＳ１３２５において、応答部２４０は、認証失敗を示すログイン結果データをユーザ端末１１０に送信する。つまり、応答部２４０は認証失敗を応答する。

ユーザ端末１１０は、ログイン結果データを受信する。ログイン結果データが認証失敗を示す場合、ユーザ端末１１０は、認証失敗画面をディスプレイに表示する。

認証失敗画面は、ユーザが認証されなかったことをユーザに知らせるための画面である。具体的には、認証失敗画面は、ログイン識別子とログインパスワードとの組が正しくないことをユーザに知らせる。

[0063] 図１１に基づいて、仮想アカウント処理（Ｓ１３３）を説明する。

ステップＳ１３３１において、ログイン判定部２２０は、ログイン識別子の試行回数を取得する。

ステップＳ１３３１の処理は、ステップＳ１３２１の処理と同じである（図１０参照）。

[0064] ステップＳ１３３２において、ログイン判定部２２０は、ログイン識別子の試行回数が上限回数に達しているか判定する。

ステップＳ１３３２の処理は、ステップＳ１３２２の処理と同じである（図１０参照）。

ログイン識別子の試行回数が上限回数に達している場合、処理はステップＳ１３３３に進む。

ログイン識別子の試行回数が上限回数に達していない場合、処理はステップＳ１３３４に進む。

[0065] ステップＳ１３３３において、仮想アカウントロック部２３２は、アカウントロック画面をユーザ端末１１０に表示させるために、アカウントロックを応答する。

ステップＳ１３３３の処理は、ステップＳ１３４の処理と同じである（図９参照）。

[0066] ステップＳ１３３４において、応答部２４０は、認証失敗を示すログイン結果データをユーザ端末１１０に送信する。つまり、応答部２４０は認証失敗を応答する。

ステップＳ１３３４の処理は、ステップＳ１３２５の処理と同じである（図１０参照）。

[0067] 図１２に基づいて、認証失敗時の応答内容を説明する。

ログイン識別子の試行回数が上限未満であり、且つ、ログイン識別子に対応するアカウントが無い場合、ロック状態に関わらず、応答内容は認証失敗となる。

ログイン識別子の試行回数が上限未満であり、且つ、ログイン識別子に対応するアカウントが有り、且つ、ロック状態が未ロックである場合、応答内

容は認証失敗となる。

ログイン識別子の試行回数が上限未満であり、且つ、ログイン識別子に対応するアカウントが有り、且つ、ロック状態がロック中である場合、応答内容はアカウントロックとなる。

ログイン識別子の試行回数が上限以上であり、且つ、ログイン識別子に対応するアカウントが無い場合、ロック状態に関わらず、応答内容はアカウントロックとなる。

ログイン識別子の試行回数が上限以上であり、且つ、ログイン識別子に対応するアカウントが有り、且つ、ロック状態が未ロックである場合、応答内容はアカウントロックとなる。また、ロック状態は未ロックからロック中に変わる。

ログイン識別子の試行回数が上限以上であり、且つ、ログイン識別子に対応するアカウントが有り、且つ、ロック状態がロック中である場合、応答内容はアカウントロックとなる。

[0068] ＊＊＊実施の形態１の補足＊＊＊

アカウント（登録識別子および登録パスワード）の変更、追加および削除が、ウェブアプリケーションを介して、または、管理者によって可能であることが望ましい。

アカウントのロック状態の「ロック中」から「未ロック」への変更は、管理者によって可能である。この変更が一般のユーザによって行われないようにすることが望ましい。

失敗ログイン管理ファイル２９１が試行回数が上限回数に満たない試行識別子で埋まることを防ぐ必要がある。例えば、失敗ログイン管理部をウェブサーバ２００に備える。認証が成功した場合、失敗ログイン管理部はログイン識別子と同じ試行識別子を失敗ログイン管理ファイル２９１から削除する。失敗ログイン管理部は、管理者からウェブサーバ２００への指示に従って失敗ログイン管理ファイル２９１を編集してもよいし、失敗ログイン管理ファイル２９１を定期的にリセットしてもよい。

アカウントロック画面は、他のアカウントのユーザ識別子およびパスワードを入力させるためのユーザインタフェースを含んでもよい。

アカウントロック画面は、アカウントのロック状態を解除する方法をユーザに提示するためのメッセージを含んでもよい。例えば、メッセージは、ユーザ識別子およびユーザパスワードを使用する認証ではなく、電子メールまたは電話などの通信方法を利用して正規ユーザのみが知る情報を使用する認証、を実施するようことをユーザに提示する。

[0069] ＊＊＊実施の形態１の効果＊＊＊

正規ユーザが認証情報（ユーザ識別子およびユーザパスワード）を誤って覚えている場合でも、攻撃者に試行識別子に対応するアカウントの有無を判明されることなく、正規ユーザに認証情報が誤っていることを通知することができる。

正規ユーザが認証情報を誤って覚えている場合と正規ユーザがユーザパスワードのみを誤って覚えている場合とのいずれの場合であっても、アカウントロック画面が表示される。そのため、正規ユーザは他の認証方式で認証を受けざるを得ない。したがって、アカウントロック後、正規ユーザは、誤ったユーザ識別子または誤ったユーザパスワードを使用した認証を繰り返すという不要な認証を行わなくてよい。

攻撃者が様々なユーザ識別子を使用するＢＦ攻撃を実施しても、攻撃者には全てユーザ識別子が有効なユーザ識別子であるかのように確認できる。そのため、ＢＦ攻撃を困難にすることができる。

[0070] 実施の形態２.

攻撃者によるログイン試行を検知する形態について、主に実施の形態１と異なる点を図１３から図１７に基づいて説明する。

[0071] ＊＊＊構成の説明＊＊＊

認証制御システム１００の構成は、実施の形態１における構成と同じである（図１参照）。

[0072] 図１３に基づいて、ウェブサーバ２００の構成を説明する。

ウェブサーバ２００は、さらに、攻撃判定部２５０を備える。攻撃判定部２５０は、アドレス監視部２５１とアドレス管理部２５２とアドレス決定部２５３とを備える。

認証制御プログラムは、さらに、攻撃判定部２５０としてコンピュータを機能させる。

[0073] 図１４に基づいて、試行識別子別のアドレステーブル２９３の構成を説明する。試行識別子別のアドレステーブル２９３は、記憶部２９０に記憶される。

アドレステーブル２９３は、認証が失敗したログイン毎に試行元アドレスを示す。

試行識別子は、認証が失敗したログインにおいてログイン識別子として使用されたユーザ識別子である。

試行元アドレスは、認証が失敗したログインにおけるログインデータの送信元アドレスである。具体的には、送信元アドレスの種類はＩＰアドレスである。ＩＰはＩｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌの略称である。

[0074] アドレステーブル２９３Ｒは、「Ｒｅｄ」という試行識別子用のアドレステーブル２９３である。アドレステーブル２９３Ｒは、「Ｒｅｄ」がログイン識別子として使用されたログインが４回失敗したことを示している。また、アドレステーブル２９３Ｒは、失敗したログインそれぞれにおける送信元アドレス（試行元アドレス）を示している。

アドレステーブル２９３Ｙは、「Ｙｅｌｌｏｗ」という試行識別子用のアドレステーブル２９３である。アドレステーブル２９３Ｙは、「Ｙｅｌｌｏｗ」がログイン識別子として使用されたログインが３回失敗したことを示している。また、アドレステーブル２９３Ｙは、失敗したログインそれぞれにおける送信元アドレス（試行元アドレス）を示している。

アドレステーブル２９３Ｘは、「Ｘ」という試行識別子用のアドレステーブル２９３である。アドレステーブル２９３Ｘは、「Ｘ」がログイン識別子として使用されたログインが１回失敗したことを示している。また、アドレ

ステーブル２９３Ｘは、失敗したログインにおける送信元アドレス（試行元アドレス）を示している。

[0075] ＊＊＊動作の説明＊＊＊

図１５に基づいて、認証制御方法を説明する。

ステップＳ２０１において、受付部２１０は、ログインデータを受信する。ログインデータは、ログイン識別子とログインパスワードとを含む。

ステップＳ２０１の処理は、実施の形態１におけるステップＳ１０１の処理と同じである。

[0076] ステップＳ２１０において、アドレス監視部２５１は、アドレス監視処理を行う。

アドレス監視処理（Ｓ２１０）において、アドレス監視部２５１は、受信されたログインデータの送信元アドレスが監視対象アドレスと同じアドレスである場合に攻撃通知を行う。また、アドレス監視部２５１は、受信されたログインデータの送信元アドレスが監視対象アドレスと同じアドレスである場合にアカウントロック画面を表示させる。

[0077] 図１６に基づいて、アドレス監視処理（Ｓ２１０）の手順を説明する。

アドレス監視処理（Ｓ２１０）において、監視対象リストが使用される。

監視対象リストは、１つ以上の監視対象アドレスを示すリストであり、記憶部２９０に記憶される。

監視対象アドレスは、監視の対象となる送信元アドレスである。

[0078] ステップＳ２１１において、監視対象リストに監視対象アドレスが１つも登録されていない場合、アドレス監視処理（Ｓ２１０）は終了する。

監視対象リストに１つ以上の監視対象アドレスが登録されている場合、アドレス監視部２５１は以下のように動作する。

まず、アドレス監視部２５１は、ログインデータのヘッダから送信元アドレスを抽出する。

そして、アドレス監視部２５１は、送信元アドレスをそれぞれの監視対象アドレスと比較することによって、送信元アドレスがいずれかの監視対象ア

ドレスと同じアドレスであるか判定する。

送信元アドレスがいずれかの監視対象アドレスと同じアドレスである場合、処理はステップＳ２１２に進む。

送信元アドレスがいずれの監視対象アドレスとも異なるアドレスである場合、アドレス監視処理（Ｓ２１０）は終了する。

[0079] ステップＳ２１２において、アドレス監視部２５１は、攻撃通知を行う。

攻撃通知は、攻撃の可能性が高いアドレスからのアクセスがあったことを通知することである。言い換えると、攻撃通知は、攻撃者によって試行されたと推定されるログインの発生を通知することである。

具体的には、アドレス監視部２５１は、攻撃通知メッセージを管理者のアドレス宛てに送信する。または、アドレス監視部２５１は、攻撃通知メッセージを監視装置へ送信する。管理者のアドレスおよび監視装置のアドレスは記憶部２９０に予め登録されている。

[0080] ステップＳ２１３において、アドレス監視部２５１は、アカウントロック画面をユーザ端末１１０に表示させるために、アカウントロックを応答する。

ステップＳ２１３の処理は、実施の形態１におけるステップＳ１３４の処理と同じである（図９参照）。

ステップＳ２１３の後、アドレス監視処理（Ｓ２１０）は終了する。

[0081] 図１５に戻り、アドレス監視処理（Ｓ２１０）の後の処理を説明する。

アドレス監視処理（Ｓ２１０）において攻撃通知が行われた場合、処理は終了する。

アドレス監視処理（Ｓ２１０）において攻撃通知が行われなかった場合、処理はステップＳ２２０に進む。

[0082] ステップＳ２２０において、認証サーバ３００は、ログインデータに基づいて認証処理を行う。

認証処理（Ｓ２２０）は、実施の形態１における認証処理（Ｓ１１０）と同じである。

[0083] ステップＳ２３１において、ログイン判定部２２０は、認証結果に基づいてログイン許否を判定する。

ステップＳ２３１の処理は、実施の形態１におけるステップＳ１２１の処理と同じである（図７参照）。

ログインが許可される場合、処理はステップＳ２３２に進む。

ログインが許可されない場合、処理はステップＳ２３３に進む。

[0084] ステップＳ２３２において、応答部２４０は、ログイン成功を応答する。

ステップＳ２３２の処理は、実施の形態１におけるステップＳ１２２の処理と同じである（図７参照）。

[0085] ステップＳ２３３において、アドレス管理部２５２は、ログイン識別子と同じユーザ識別子用のアドレステーブル２９３にログインデータの送信元アドレスを登録する。

[0086] ステップＳ２４０において、アカウントロック部２３０は、認証結果に基づいてログイン失敗処理を行う。

ログイン失敗処理（Ｓ１３０）は、実施の形態１におけるログイン失敗処理（Ｓ１３０）と同じである。

[0087] 但し、ステップＳ２４０において、アドレス監視部２５１は、非攻撃通知を行ってもよい。

非攻撃通知は、攻撃の可能性が低いアドレスからのアクセスがあったことを通知することである。言い換えると、非攻撃通知は、正規ユーザによって試行されたと推定されるログインの発生を通知することである。

非攻撃通知の方法は、ステップＳ２１２における攻撃通知の方法と同じである。

[0088] ステップＳ２５０において、アドレス決定部２５３は、アドレス決定処理を行う。

アドレス決定処理（Ｓ２５０）において、アドレス決定部２５３は次のように動作する。アドレス決定部２５３は、ログイン識別子と同じユーザ識別子を用いたログインの失敗回数が上限回数に達している場合に、ログイン識

別子と同じユーザ識別子用のアドレステーブル２９３に基づいて監視対象アドレスを決定する。

[0089] 図１７に基づいて、アドレス決定処理（Ｓ２５０）の手順を説明する。

ステップＳ２５１において、アドレス決定部２５３は、ログイン失敗処理（図１５のＳ２４０）で行われた応答の種類を判定する。

アカウントロックが応答された場合、処理はステップＳ２５２に進む。

アカウントロックが応答されなかった場合、つまり、認証失敗が応答された場合、アドレス決定処理（Ｓ２５０）は終了する。

[0090] ステップＳ２５２において、アドレス決定部２５３は、ログイン識別子と同じユーザ識別子用のアドレステーブル２９３を記憶部２９０から選択する。

そして、アドレス決定部２５３は、選択したアドレステーブル２９３に基づいて、ログインデータの送信元アドレスが監視条件を満たすか判定する。

例えば、アドレス決定部２５３は、選択したアドレステーブル２９３に含まれる試行元アドレスが全て同じであるか判定する。選択したアドレステーブル２９３に含まれる試行元アドレスが全て同じである場合、ログインデータの送信元アドレスは監視条件を満たす。

例えば、アドレス決定部２５３は、選択したアドレステーブル２９３から、規定回数数以上含まれる試行元アドレスまたは規定割合以上含まれる試行元アドレスを選択する。そして、アドレス決定部２５３は、ログインデータの送信元アドレスが、選択した試行元アドレスと同じであるか判定する。ログインデータの送信元アドレスが、選択した試行元アドレスと同じである場合、ログインデータの送信元アドレスは監視条件を満たす。

ログインデータの送信元アドレスが監視条件を満たす場合、処理はステップＳ２５３に進む。

ログインデータの送信元アドレスが監視条件を満たさない場合、アドレス決定処理（Ｓ２５０）は終了する。

[0091] ステップＳ２５３において、アドレス決定部２５３は、ログインデータの

送信元アドレスを監視対象アドレスとして監視対象リストに登録する。

ステップＳ２５３の後、アドレス決定処理（Ｓ２５０）は終了する。

[0092] ＊＊＊実施の形態２の効果＊＊＊

実施の形態１では、アカウントロック画面が表示されるのみであるため、認証が失敗したときのログインの試行者が正規ユーザと攻撃者とのいずれであるかが不明である。

実施の形態２では、送信元アドレスが固定のＩＰである攻撃者からＢＦ攻撃を行われた場合に、ＢＦ攻撃が行われたことを検知することが可能となる。

[0093] 正規ユーザは自身のユーザ識別子が正しいと認識している。そのため、アカウントロックが発生した場合、正規ユーザは別の認証方法を利用してアカウントロックを解除しようとする、と考えられる。一方、アカウントロックが発生した場合、攻撃者は同じユーザ識別子によるログインの試行が無効であると考えて他のユーザ識別子に対してＢＦ攻撃を行う、と考えられる。

実施の形態２では、アカウントロック後もログインを試みる動作を検知することで、攻撃者と正規ユーザとを区別して攻撃者を検知することができる。

[0094] 実施の形態３．

ログインの失敗回数の上限を動的に変更する形態について、主に実施の形態１と異なる点を図１８から図２１に基づいて説明する。

[0095] ＊＊＊構成の説明＊＊＊

認証制御システム１００の構成は、実施の形態１における構成と同じである（図１参照）。

[0096] 図１８に基づいて、ウェブサーバ２００の構成を説明する。

ウェブサーバ２００は、さらに、上限操作部２６０を備える。上限操作部２６０は、変更判定部２６１と上限変更部２６２とを備える。

認証制御プログラムは、さらに、上限操作部２６０としてコンピュータを機能させる。

[0097] ＊＊＊動作の説明＊＊＊

認証制御方法における処理の流れは、実施の形態１と同じである（図７参照）。

但し、実在アカウント処理（Ｓ１３２）および仮想アカウント処理（Ｓ１３３）において、上限操作処理が実行される。

[0098] 上限操作処理は、ログイン識別子の試行回数の上限（上限回数）を変更するための処理である。

上限操作処理において、変更判定部２６１は、変更条件を満たすか判定する。例えば、変更判定部２６１は、ユーザ識別子毎のログインの失敗回数または単位時間当たりのログインの試行回数に基づいて、変更条件を満たすか判定する。単位時間当たりのログインの試行回数は、単位時間当たりにログインデータ（ログイン識別子およびログインパスワード）が受け付けられた回数に相当する。

変更条件を満たす場合、上限変更部２６２は、ユーザ識別子毎のログインの失敗回数に基づいて、上限回数を変更する。

上限操作処理の詳細については後述する。

[0099] 図１９に基づいて、実在アカウント処理（Ｓ１３２）を説明する。

ステップＳ１３２１において、ログイン判定部２２０は、ログイン識別子の試行回数を取得する。

ステップＳ１３２１は、実施の形態１において説明した通りである（図１０参照）。

[0100] ステップＳ１３２２において、ログイン判定部２２０は、ログイン識別子の試行回数が上限回数に達しているか判定する。

ステップＳ１３２２は、実施の形態１において説明した通りである（図１０参照）。

ログイン識別子の試行回数が上限に達している場合、処理はステップＳ１３２３に進む。

ログイン識別子の試行回数が上限に達していない場合、処理はステップＳ

３００に進む。

[0101] ステップＳ１３２３において、実在アカウントロック部２３１は、ログイン識別子に対応するロック状態フラグに「ロック中」を設定する。

ステップＳ１３２４において、実在アカウントロック部２３１は、アカウントロックを応答する。

ステップＳ１３２３およびステップＳ１３２４は、実施の形態１で説明した通りである（図１０参照）。

[0102] ステップＳ３００において、上限操作部２６０は上限操作処理を行う。

上限操作処理（Ｓ３００）については後述する。

[0103] 上限操作処理（Ｓ３００）において上限回数が変更された場合、処理はステップＳ３１１に進む。

上限操作処理（Ｓ３００）において上限回数が変更されなかった場合、処理はステップＳ１３２５に進む。

[0104] ステップＳ３１１において、ログイン判定部２２０は、ログイン識別子の試行回数が上限回数に達しているか判定する。

ステップＳ３１１の処理は、ステップＳ１３２２の処理と同じである。

ログイン識別子の試行回数が上限に達している場合、処理はステップＳ１３２３に進む。

ログイン識別子の試行回数が上限に達していない場合、処理はステップＳ１３２５に進む。

[0105] ステップＳ１３２５において、応答部２４０は認証失敗を応答する。

ステップＳ１３２５は、実施の形態１において説明した通りである（図１０参照）。

[0106] 図２０に基づいて、仮想アカウント処理（Ｓ１３３）を説明する。

ステップＳ１３３１において、ログイン判定部２２０は、ログイン識別子の試行回数を取得する。

ステップＳ１３３１は、実施の形態１において説明した通りである（図１１参照）。

[0107] ステップＳ１３３２において、ログイン判定部２２０は、ログイン識別子の試行回数が上限回数に達しているか判定する。

ステップＳ１３３２は、実施の形態１において説明した通りである（図１１参照）。

ログイン識別子の試行回数が上限回数に達している場合、処理はステップＳ１３３３に進む。

ログイン識別子の試行回数が上限回数に達していない場合、処理はステップＳ３００に進む。

[0108] ステップＳ３００において、上限操作部２６０は上限操作処理を行う。

上限操作処理（Ｓ３００）については後述する。

[0109] 上限操作処理（Ｓ３００）において上限回数が変更された場合、処理はステップＳ３１２に進む。

上限操作処理（Ｓ３００）において上限回数が変更されなかった場合、処理はステップＳ１３３４に進む。

[0110] ステップＳ３１２において、ログイン判定部２２０は、ログイン識別子の試行回数が上限回数に達しているか判定する。

ステップＳ３１２の処理は、ステップＳ１３３２の処理と同じである。

ログイン識別子の試行回数が上限回数に達している場合、処理はステップＳ１３３３に進む。

ログイン識別子の試行回数が上限回数に達していない場合、処理はステップＳ１３３４に進む。

[0111] ステップＳ１３３４において、応答部２４０は認証失敗を応答する。

ステップＳ１３３４は、実施の形態１において説明した通りである（図１１参照）。

[0112] 図２１に基づいて、上限操作処理（Ｓ３００）を説明する。

ステップＳ３０１において、変更判定部２６１は、変更条件を満たすか判定する。

例えば、変更判定部２６１は、失敗ログイン管理ファイル２９１の中に試

行回数が上限回数に達している試行識別子が存在するか判定する。試行回数が上限回数に達している試行識別子が存在する場合、変更条件を満たす。

[0113] 例えば、変更判定部２６１は、失敗ログイン管理ファイル２９１に基づいて、試行回数が上限回数に達していない試行識別子の数が閾値より多いか判定する。試行回数が上限回数に達していない試行識別子の数が閾値より多い場合、変更条件を満たす。

[0114] 例えば、変更判定部２６１は、単位時間当たりのログインの試行回数が閾値より多いか判定する。単位時間当たりのログインの試行回数が閾値より多い場合、変更条件を満たす。

[0115] 変更条件を満たす場合、処理はステップＳ３０２に進む。

変更条件を満たさない場合、上限回数は変更されず、上限操作処理（Ｓ３００）は終了する。

[0116] ステップＳ３０２において、上限変更部２６２は、新たな上限回数を決定する。

例えば、上限変更部２６２は、ユーザ識別子毎のログインの失敗回数に基づいて、新たな上限回数を決定する。具体的には、上限変更部２６２は、失敗ログイン管理ファイル２９１に登録されている試行回数の平均を算出する。算出される平均が新たな上限回数となる。

[0117] ステップＳ３０３において、上限変更部２６２は、既定の上限回数を新たな上限回数に変更する。

[0118] 上限操作処理（Ｓ３００）について補足する。

上限回数が１回になって頻繁にアクセスロックが発生してしまうことを防ぐためには、上限回数のリセットが必要となる。

例えば、ウェブサーバ２００に管理部を備える。そして、管理部は、認証成功時のログイン識別子を失敗ログイン管理ファイル２９１から削除する。または、管理部は、定期的に、失敗ログイン管理ファイル２９１の中の試行回数をリセットする。管理部は、上限回数をリセットするためのその他の処理を行ってもよい。これらの処理は、人手によって行われてもよい。

[0119] ＊＊＊実施の形態３の効果＊＊＊

実施の形態１および実施の形態２では、攻撃者にアカウントロックの上限回数が判明してしまう恐れがある。アカウントロックの上限回数が判明すると、攻撃者は、上限回数に満たない回数でログイン試行を行うことができる。この場合、管理者は、攻撃されていることに気付かない可能性がある。

実施の形態３では、アカウントロックの上限回数が動的に変更される。これにより、アカウントロックの上限回数が判明し難くなる。そのため、攻撃者は、上限回数に満たない回数でログイン試行を行うことが困難となる。

[0120] ＊＊＊他の構成＊＊＊

実施の形態３において実施の形態２を適用してもよい。つまり、実施の形態３において、ウェブサーバ２００は攻撃判定部２５０を備えてもよい。

[0121] 実施の形態４．

認証制御システム１００の構成例について、主に実施の形態１から実施の形態３と異なる点を図２２に基づいて説明する。

[0122] 認証制御システム１００（図１参照）において、ウェブサーバ２００と認証サーバ３００とは、アプライアンス製品などに適用する場合、１つの筐体の中に搭載されてもよい。

また、認証制御システム１００は、ウェブサーバ２００と認証サーバ３００との組の代わりに、１つの認証制御装置を備えてもよい。

[0123] 認証制御システム１００は、ウェブサーバ２００の代わりに、複数の装置を備えてもよい。

[0124] 図２２に示すように、認証制御システム１００は、ウェブサーバ２００の代わりに、ウェブサーバ４１０と認証制御装置４２０とを備えてもよい。

ウェブサーバ４１０は、ウェブサーバ２００と同様に各種のハードウェアを備えるコンピュータである。

認証制御装置４２０は、ウェブサーバ２００と同様に各種のハードウェアを備えるコンピュータである。

認証サーバ３００は、認証部３１０という要素を備える。認証サーバ３０

０の記憶装置には、アカウント管理ファイル３９１が記憶される。

ウェブサーバ４１０は、受付部２１０とログイン判定部２２０と応答部２４０といった要素を備える。

認証制御装置４２０は、アカウントロック部２３０という要素を備える。認証制御装置４２０の記憶装置には、失敗ログイン管理ファイル２９１およびログイン試行データ２９２などが記憶される。アカウントロック部２３０は、ウェブアプリケーションから切り離すことが可能である。

[0125] ＊＊＊実施の形態の補足＊＊＊

図２３に基づいて、ウェブサーバ２００のハードウェア構成を説明する。

ウェブサーバ２００は処理回路２０９を備える。

処理回路２０９は、受付部２１０とログイン判定部２２０とアカウントロック部２３０と応答部２４０と攻撃判定部２５０と上限操作部２６０とを実現するハードウェアである。

処理回路２０９は、専用のハードウェアであってもよいし、メモリ２０２に格納されるプログラムを実行するプロセッサ２０１であってもよい。

[0126] 処理回路２０９が専用のハードウェアである場合、処理回路２０９は、例えば、単一回路、複合回路、プログラム化したプロセッサ、並列プログラム化したプロセッサ、ＡＳＩＣ、ＦＰＧＡまたはこれらの組み合わせである。

ＡＳＩＣはＡｐｐｌｉｃａｔｉｏｎ Ｓｐｅｃｉｆｉｃ Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔの略称であり、ＦＰＧＡはＦｉｅｌｄ Ｐｒｏｇｒａｍｍａｂｌｅ Ｇａｔｅ Ａｒｒａｙの略称である。

ウェブサーバ２００は、処理回路２０９を代替する複数の処理回路を備えてもよい。複数の処理回路は、処理回路２０９の役割を分担する。

[0127] 処理回路２０９において、一部の機能が専用のハードウェアで実現されて、残りの機能がソフトウェアまたはファームウェアで実現されてもよい。

[0128] このように、処理回路２０９はハードウェア、ソフトウェア、ファームウェアまたはこれらの組み合わせで実現することができる。

[0129] 図２４に基づいて、認証サーバ３００のハードウェア構成を説明する。

認証サーバ３００は処理回路３０９を備える。

処理回路３０９は、認証部３１０を実現するハードウェアである。

処理回路３０９は、専用のハードウェアであってもよいし、メモリ３０２に格納されるプログラムを実行するプロセッサ３０１であってもよい。

[0130] 処理回路３０９が専用のハードウェアである場合、処理回路３０９は、例えば、単一回路、複合回路、プログラム化したプロセッサ、並列プログラム化したプロセッサ、ＡＳＩＣ、ＦＰＧＡまたはこれらの組み合わせである。

認証サーバ３００は、処理回路３０９を代替する複数の処理回路を備えてもよい。複数の処理回路は、処理回路３０９の役割を分担する。

[0131] 処理回路３０９において、一部の機能が専用のハードウェアで実現されて、残りの機能がソフトウェアまたはファームウェアで実現されてもよい。

[0132] このように、処理回路３０９はハードウェア、ソフトウェア、ファームウェアまたはこれらの組み合わせで実現することができる。

[0133] 実施の形態は、好ましい形態の例示であり、本発明の技術的範囲を制限することを意図するものではない。実施の形態は、部分的に実施してもよいし、他の形態と組み合わせて実施してもよい。フローチャート等を用いて説明した手順は、適宜に変更してもよい。

符号の説明

[0134] １００　認証制御システム、１０１　ネットワーク、１１０　ユーザ端末、２００　ウェブサーバ、２０１　プロセッサ、２０２　メモリ、２０３　補助記憶装置、２０４　入出力インタフェース、２０９　処理回路、２１０　受付部、２２０　ログイン判定部、２３０　アカウントロック部、２３１　実在アカウントロック部、２３２　仮想アカウントロック部、２４０　応答部、２５０　攻撃判定部、２５１　アドレス監視部、２５２　アドレス管理部、２５３　アドレス決定部、２６０　上限操作部、２６１　変更判定部、２６２　上限変更部、２９０　記憶部、２９１　失敗ログイン管理ファイル、２９２　ログイン試行データ、２９３　アドレステーブル、３００　認証サーバ、３０１　プロセッサ、３０２　メモリ、３０３　補助記憶装置、

３０４　入出力インタフェース、３０９　処理回路、３１０　認証部、３１１　受付部、３１２　識別子判定部、３１３　ロック状態判定部、３１４　パスワード判定部、３１５　応答部、３９０　記憶部、３９１　アカウント管理ファイル、４１０　ウェブサーバ、４２０　認証制御装置。

請求の範囲

[請求項1] ログイン識別子とログインパスワードとを受け付ける受付部と、

１つ以上の登録識別子と１つ以上の登録パスワードとが互いに対応付けられたアカウント管理ファイルに基づいて前記ログイン識別子と同じ登録識別子が存在するか判定する識別子判定部と、

前記ログイン識別子と同じ登録識別子が存在する場合に前記アカウント管理ファイルに基づいて前記ログインパスワードが正しいパスワードであるか判定するパスワード判定部と、

前記ログイン識別子と同じ登録識別子が存在し、且つ、前記ログインパスワードが正しいパスワードでなく、且つ、前記ログイン識別子と同じログイン識別子を用いたログインの失敗回数が上限回数に達している場合に、アカウントロック画面を表示させる実在アカウントロック部と、

前記ログイン識別子と同じ登録識別子が存在せず、且つ、前記ログイン識別子と同じログイン識別子を用いたログインの失敗回数が前記上限回数に達している場合に、アカウントロック画面を表示させる仮想アカウントロック部と

を備える認証制御システム。

[請求項2] 前記アカウント管理ファイルは、さらに、１つ以上の登録識別子と１つ以上のロック状態フラグとを互いに対応付け、

それぞれのロック状態フラグは、アカウントのロック状態を示し、

前記認証制御システムは、さらに、

前記ログイン識別子と同じ登録識別子が存在する場合に前記アカウント管理ファイルに基づいて前記ログイン識別子に対応するアカウントのロック状態を判定するロック状態判定部を備え、

前記パスワード判定部は、前記ログイン識別子に対応するアカウントのロック状態が未ロックである場合に前記ログインパスワードが正しいユーザパスワードであるか判定し、

前記実在アカウントロック部は、

前記ログイン識別子と同じ登録識別子が存在し、且つ、前記ログイン識別子に対応するアカウントのロック状態がロック中である場合にアカウントロック画面を表示させ、

前記ログイン識別子と同じ登録識別子が存在し、且つ、前記ログイン識別子に対応するアカウントのロック状態が未ロックであり、且つ、前記ログインパスワードが正しいパスワードでなく、且つ、前記ログイン識別子と同じログイン識別子を用いたログインの失敗回数が前記上限回数に達している場合に、アカウントロック画面を表示させる

請求項１に記載の認証制御システム。

[請求項3] 前記認証制御システムは、さらに、アドレス監視部を備え、

前記受付部は、前記ログイン識別子と前記ログインパスワードとを含んだログインデータを受信し、

前記アドレス監視部は、受信されたログインデータの送信元アドレスが監視対象アドレスと同じアドレスである場合に攻撃通知を行う

請求項１または請求項２に記載の認証制御システム。

[請求項4] 前記アドレス監視部は、受信されたログインデータの送信元アドレスが監視対象アドレスと同じアドレスである場合にアカウントロック画面を表示させる

請求項３に記載の認証制御システム。

[請求項5] 前記認証制御システムは、さらに、アドレス監視部を備え、

前記受付部は、前記ログイン識別子と前記ログインパスワードとを含んだログインデータを受信し、

前記アドレス監視部は、前記ログインデータの送信元アドレスが監視対象アドレスと同じアドレスである場合にアカウントロック画面を表示させる

請求項１または請求項２に記載の認証制御システム。

[請求項6] 前記認証制御システムは、さらに、

前記ログイン識別子と同じ登録識別子が存在しない場合と前記ログインパスワードが正しいパスワードでない場合に、前記ログイン識別子と同じユーザ識別子用のアドレステーブルに前記ログインデータの送信元アドレスを登録するアドレス管理部と、

前記ログイン識別子と同じログイン識別子を用いたログインの失敗回数が上限回数に達している場合に、前記ログイン識別子と同じユーザ識別子用のアドレステーブルに基づいて監視対象アドレスを決定するアドレス決定部とを備える

請求項３から請求項５のいずれか１項に記載の認証制御システム。

[請求項7] 変更条件を満たすか判定する変更判定部と、

前記変更条件を満たす場合にユーザ識別子毎のログインの失敗回数に基づいて前記上限回数を変更する上限変更部を備える

請求項１から請求項６のいずれか１項に記載の認証制御システム。

[請求項8] 前記実在アカウントロック部は、前記ログイン識別子と同じ登録識別子が存在し、且つ、前記ログインパスワードが正しいパスワードでない場合に、前記ログイン識別子と同じログイン識別子を用いたログインの失敗回数が前記上限回数に達しているか判定し、

前記変更判定部は、前記ログイン識別子と同じログイン識別子を用いたログインの失敗回数が前記上限回数に達していない場合に、前記変更上限を満たすか判定し、

前記上限変更部は、前記変更条件を満たす場合に前記上限回数を変更し、

前記実在アカウントロック部は、前記上限回数が変更された場合に前記ログイン識別子と同じログイン識別子を用いたログインの失敗回数が前記上限回数に達しているか判定し、前記ログイン識別子と同じログイン識別子を用いたログインの失敗回数が前記上限回数に達している場合にアカウントロック画面を表示させる

請求項７に記載の認証制御システム。

[請求項9] 前記仮想アカウントロック部は、前記ログイン識別子と同じ登録識別子が存在しない場合に、前記ログイン識別子と同じログイン識別子を用いたログインの失敗回数が前記上限回数に達しているか判定し、

前記変更判定部は、前記ログイン識別子と同じログイン識別子を用いたログインの失敗回数が前記上限回数に達していない場合に、前記変更上限を満たすか判定し、

前記上限変更部は、前記変更条件を満たす場合に前記上限回数を変更し、

前記仮想アカウントロック部は、前記上限回数が変更された場合に前記ログイン識別子と同じログイン識別子を用いたログインの失敗回数が前記上限回数に達しているか判定し、前記ログイン識別子と同じログイン識別子を用いたログインの失敗回数が前記上限回数に達している場合にアカウントロック画面を表示させる

請求項７または請求項８に記載の認証制御システム。

[請求項10] ログイン識別子とログインパスワードとを受け付ける受付処理と、

１つ以上の登録識別子と１つ以上の登録パスワードとが互いに対応付けられたアカウント管理ファイルに基づいて前記ログイン識別子と同じ登録識別子が存在するか判定する識別子判定処理と、

前記ログイン識別子と同じ登録識別子が存在する場合に前記アカウント管理ファイルに基づいて前記ログインパスワードが正しいパスワードであるか判定するパスワード判定処理と、

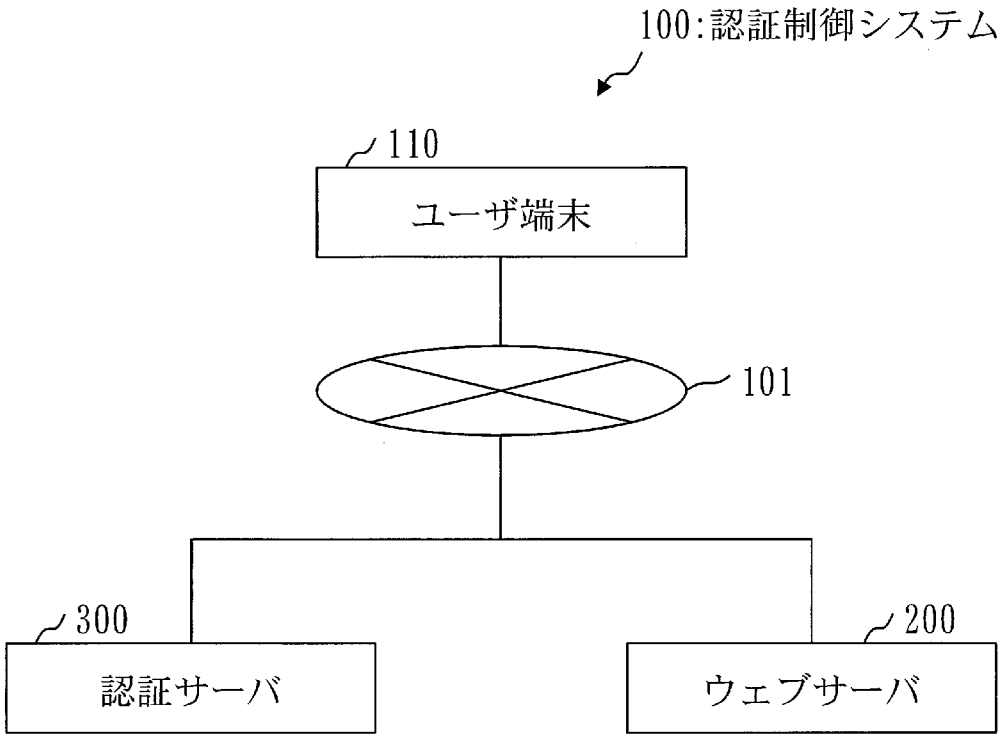
前記ログイン識別子と同じ登録識別子が存在し、且つ、前記ログインパスワードが正しいパスワードでなく、且つ、前記ログイン識別子と同じログイン識別子を用いたログインの失敗回数が上限回数に達している場合に、アカウントロック画面を表示させる実在アカウントロック処理と、

前記ログイン識別子と同じ登録識別子が存在せず、且つ、前記ログイン識別子と同じログイン識別子を用いたログインの失敗回数が前記

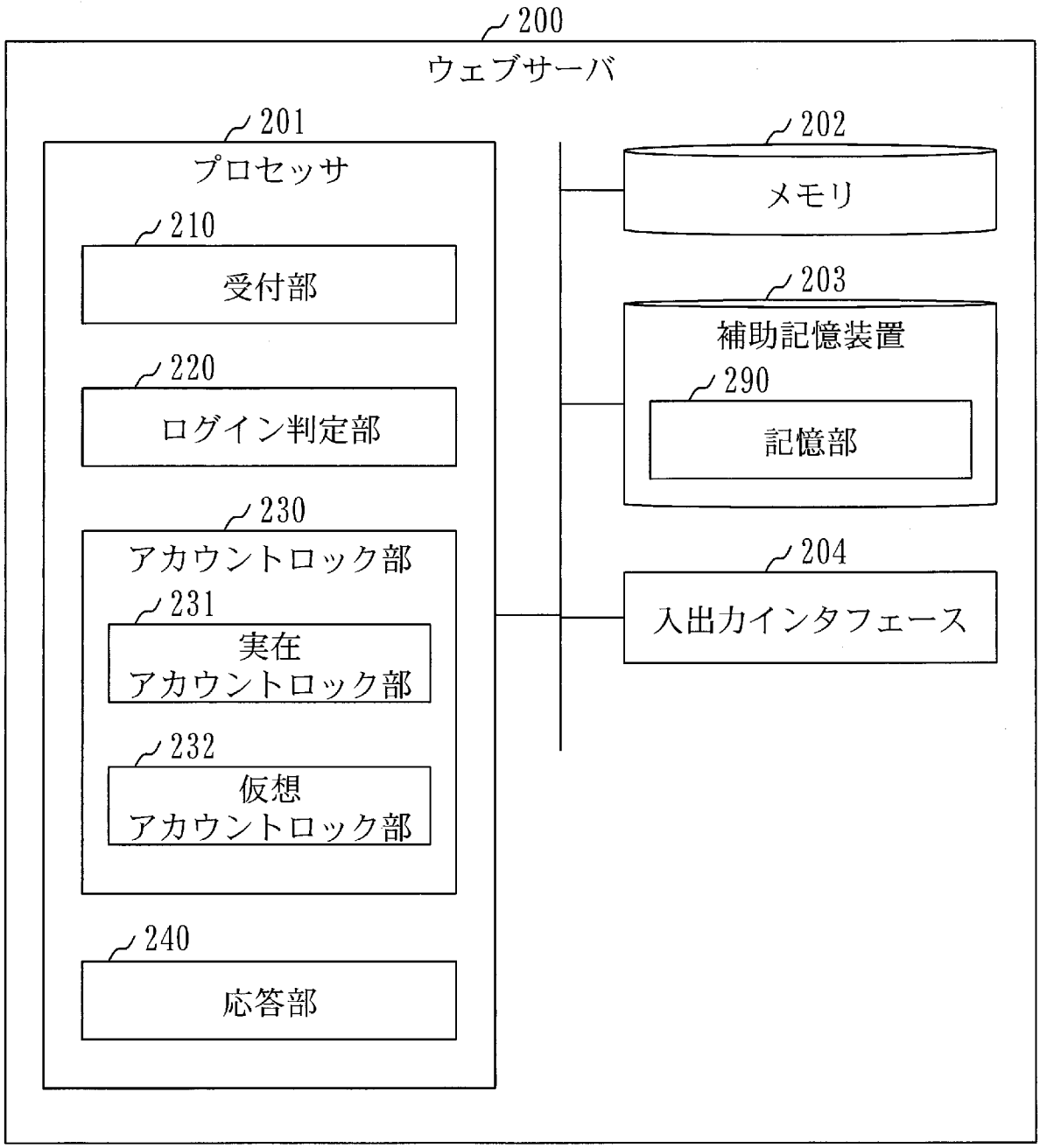
上限回数に達している場合に、アカウントロック画面を表示させる仮想アカウントロック処理と

をコンピュータを実行させるための認証制御プログラム。

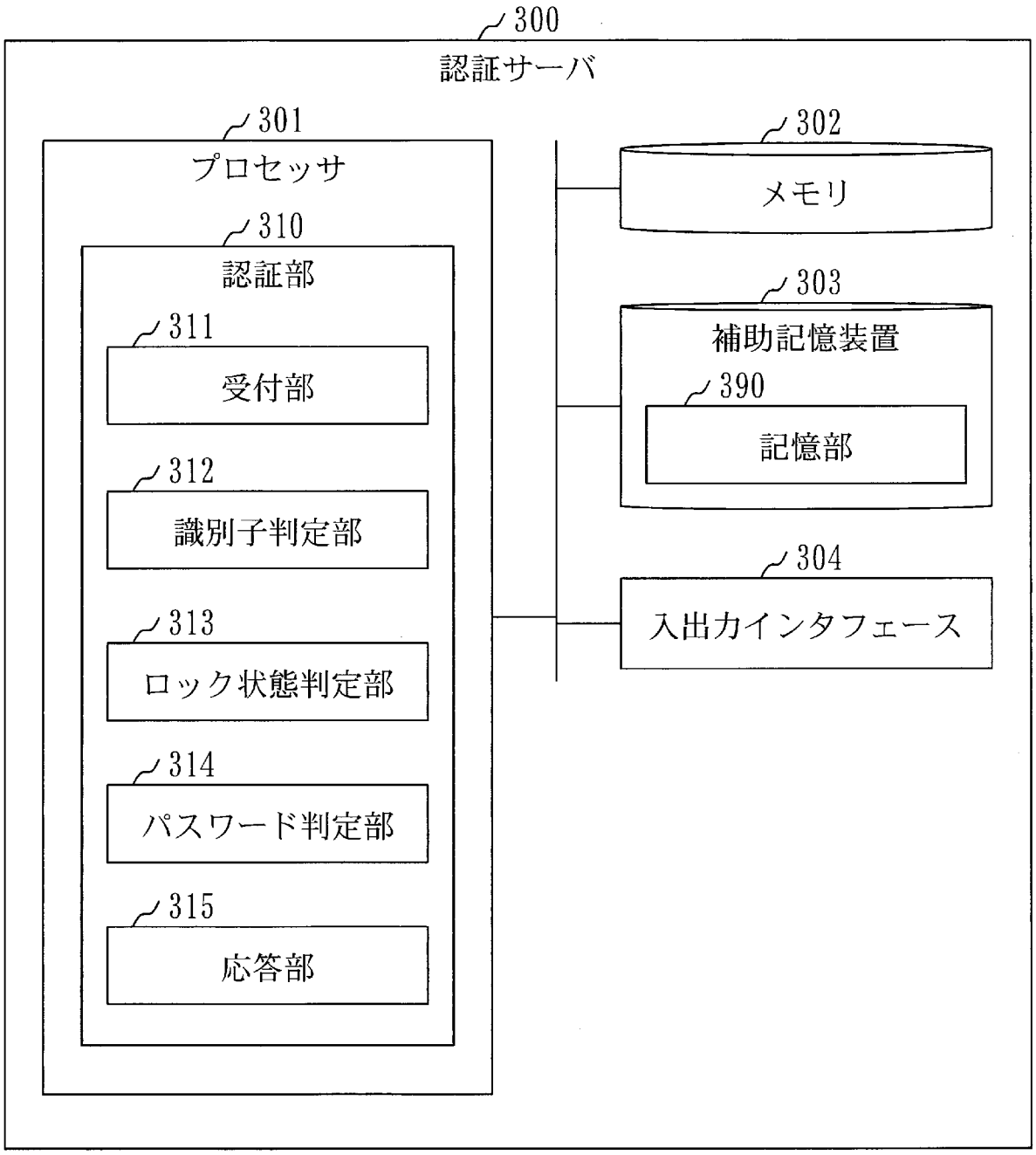
[図1]



[図2]


200
ウェブサーバ
201
プロセッサ
210
受付部
220
ログイン判定部
230
アカウントロック部
231
実在
アカウントロック部
232
仮想
アカウントロック部
240
応答部
202
メモリ
203
補助記憶装置
290
記憶部
204
入出力インタフェース

[図3]


300
認証サーバ
301
プロセッサ
310
認証部
311
受付部
312
識別子判定部
313
ロック状態判定部
314
パスワード判定部
315
応答部
302
メモリ
303
補助記憶装置
390
記憶部
304
入出力インタフェース

[図4]

291:失敗ログイン管理ファイル

項番	試行識別子	試行回数
1	Red	9
2	Yellow	9
3	Blue	7
4	Green	6
5	Pink	6
6	Black	4
7	White	4
・・・	・・・	・・・
N	Gold	1

[図5]

292:ログイン試行データ

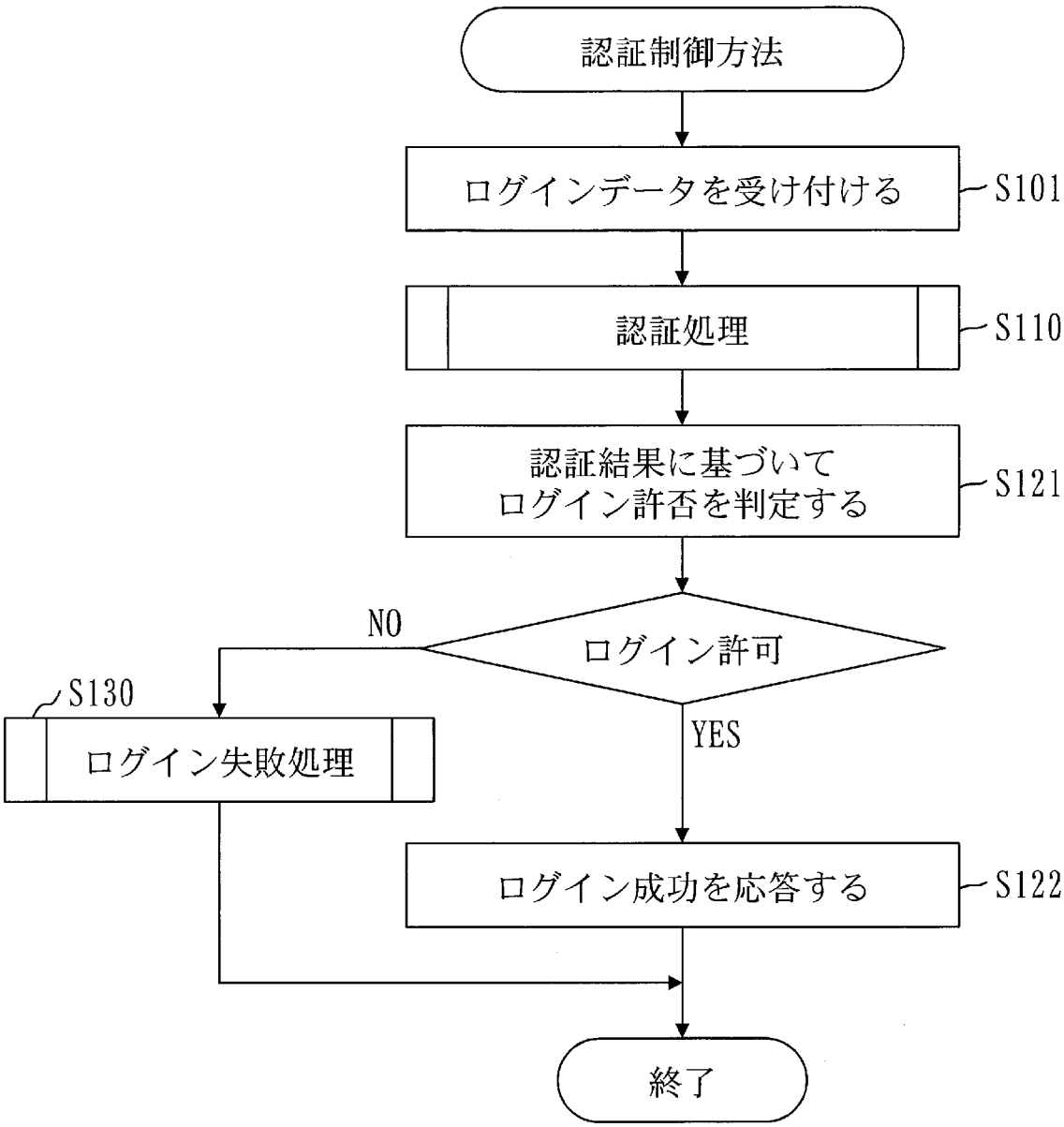
試行識別子	試行回数
Red	9

[図6]

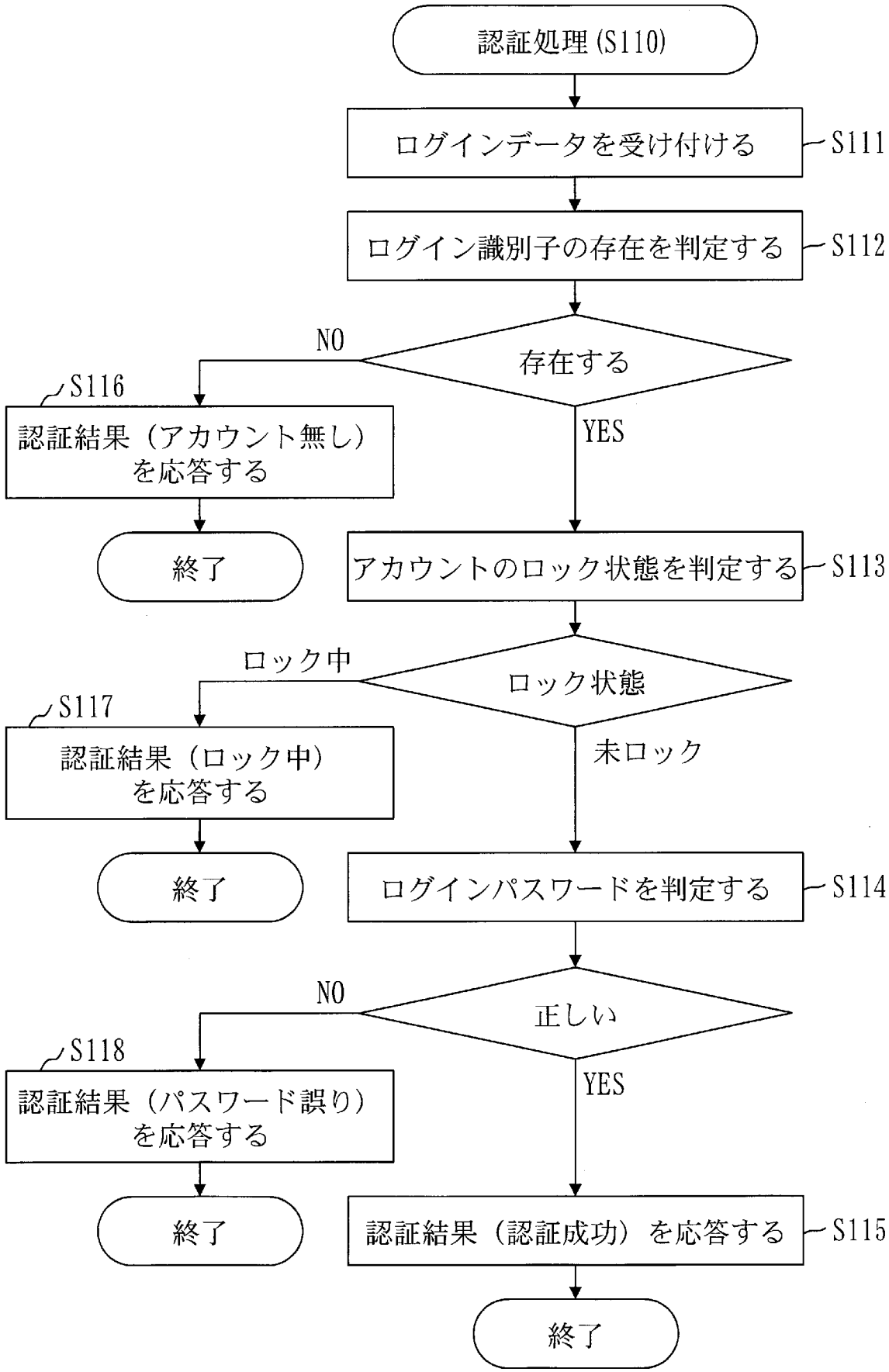
391:アカウント管理ファイル

登録識別子	登録パスワード	ロック状態フラグ
Apple	****	未ロック
Orange	****	未ロック
Strawberry	****	未ロック
Grape	****	未ロック

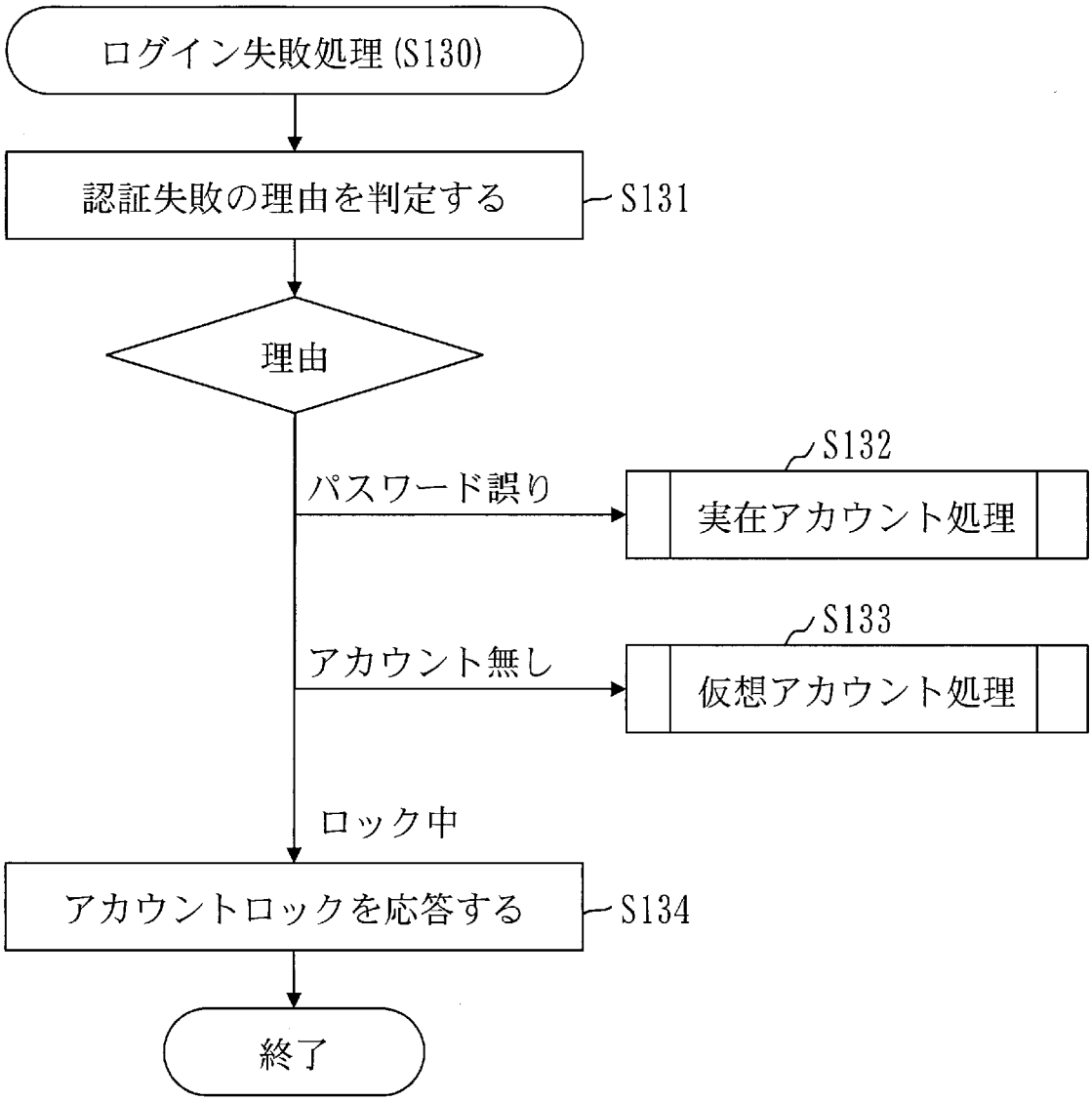
[図7]


認証制御方法
ログインデータを受け付ける
S101
認証処理
S110
認証結果に基づいて
ログイン許否を判定する
S121
ログイン許可
NO
YES
S130
ログイン失敗処理
ログイン成功を応答する
S122
終了

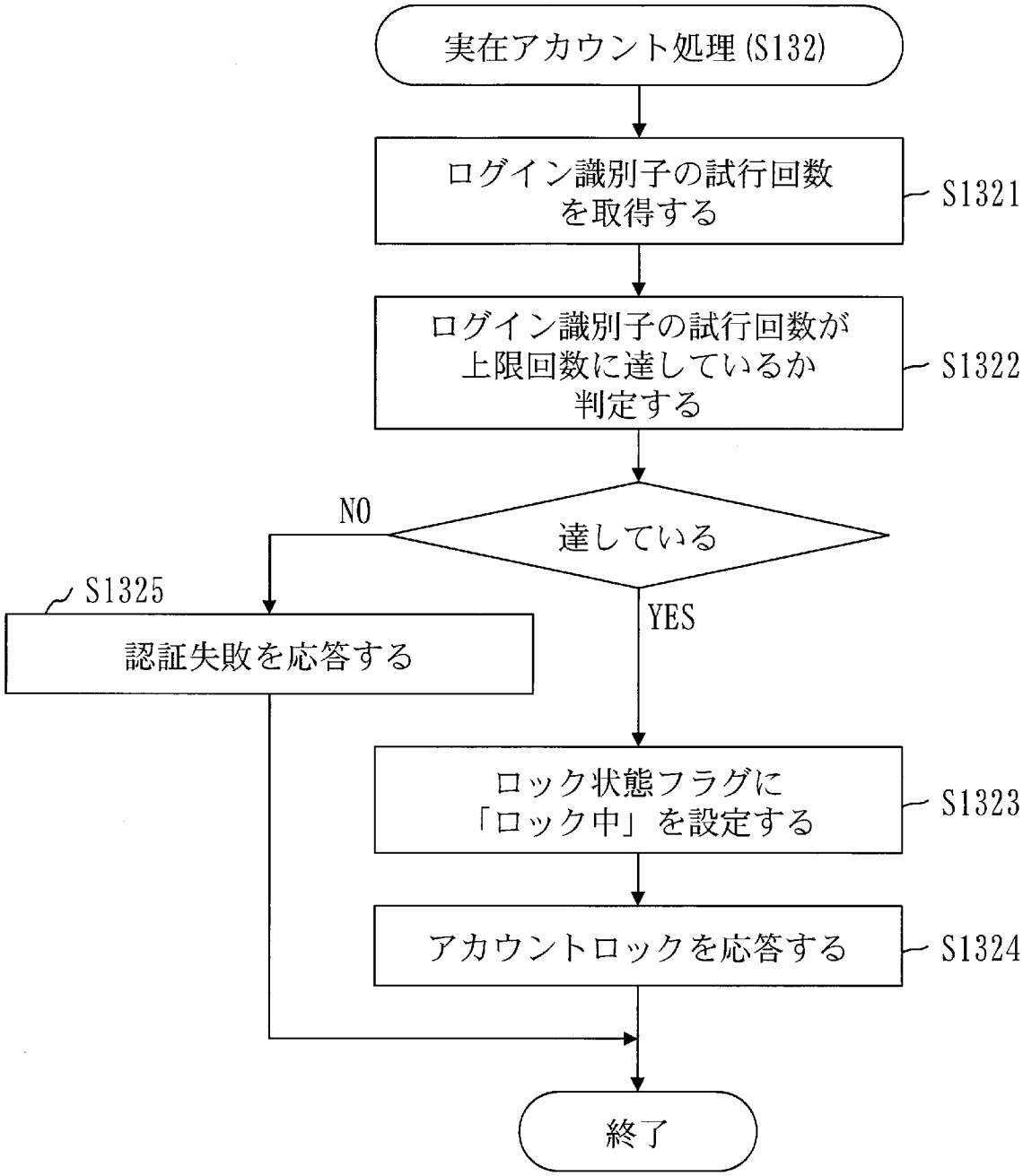
[図8]


認証処理(S110)
ログインデータを受け付ける
S111
ログイン識別子の存在を判定する
S112
存在する
NO
YES
S116
認証結果（アカウント無し）を応答する
終了
アカウントのロック状態を判定する
S113
ロック状態
ロック中
未ロック
S117
認証結果（ロック中）を応答する
終了
ログインパスワードを判定する
S114
正しい
NO
YES
S118
認証結果（パスワード誤り）を応答する
終了
認証結果（認証成功）を応答する
S115
終了

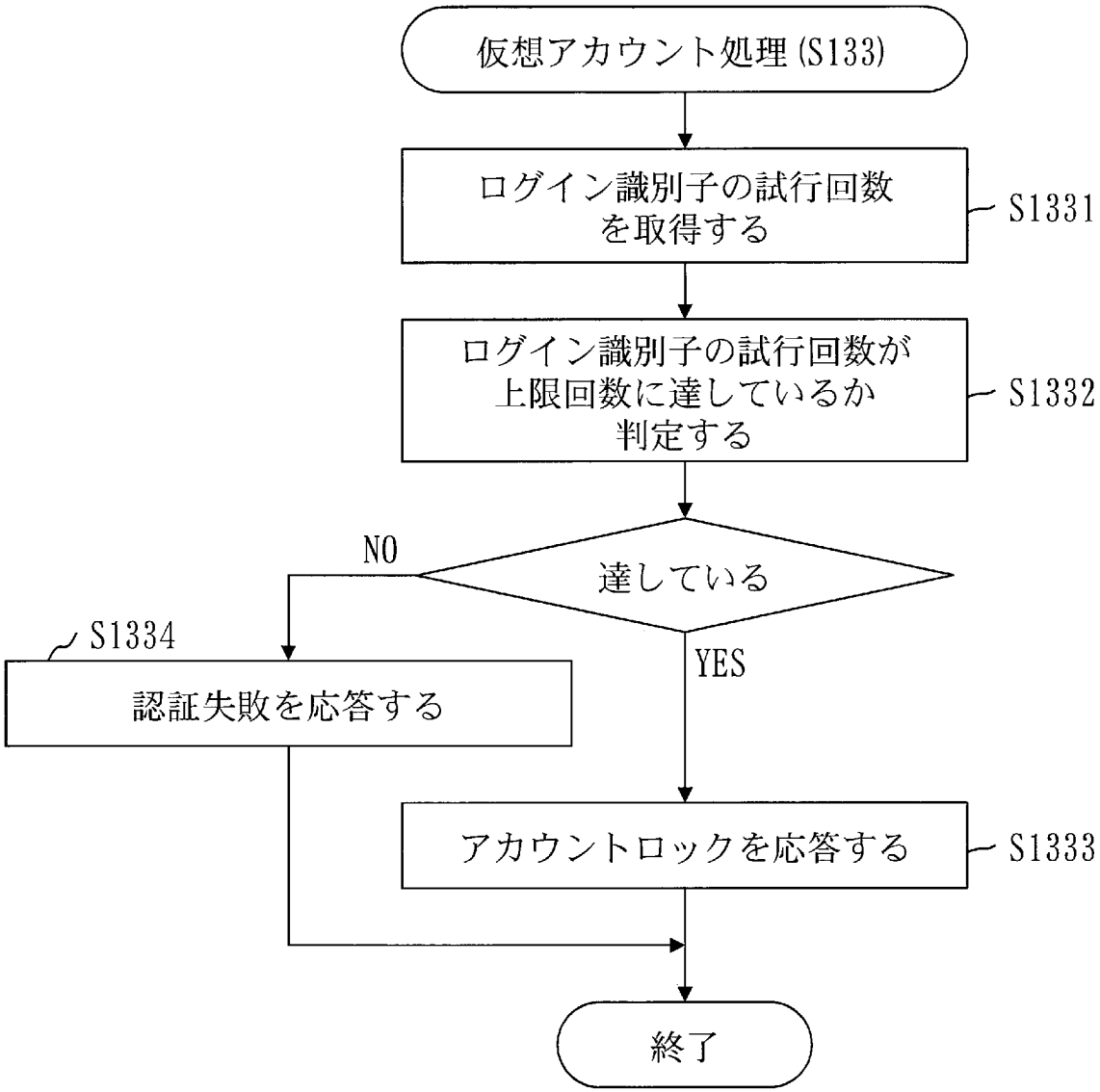
[図9]


ログイン失敗処理(S130)
認証失敗の理由を判定する
S131
理由
パスワード誤り
S132
実在アカウント処理
アカウント無し
S133
仮想アカウント処理
ロック中
アカウントロックを応答する
S134
終了

[図10]


実在アカウント処理(S132)
ログイン識別子の試行回数を取得する
S1321
ログイン識別子の試行回数が上限回数に達しているか判定する
S1322
達している
NO
YES
S1325
認証失敗を応答する
ロック状態フラグに「ロック中」を設定する
S1323
アカウントロックを応答する
S1324
終了

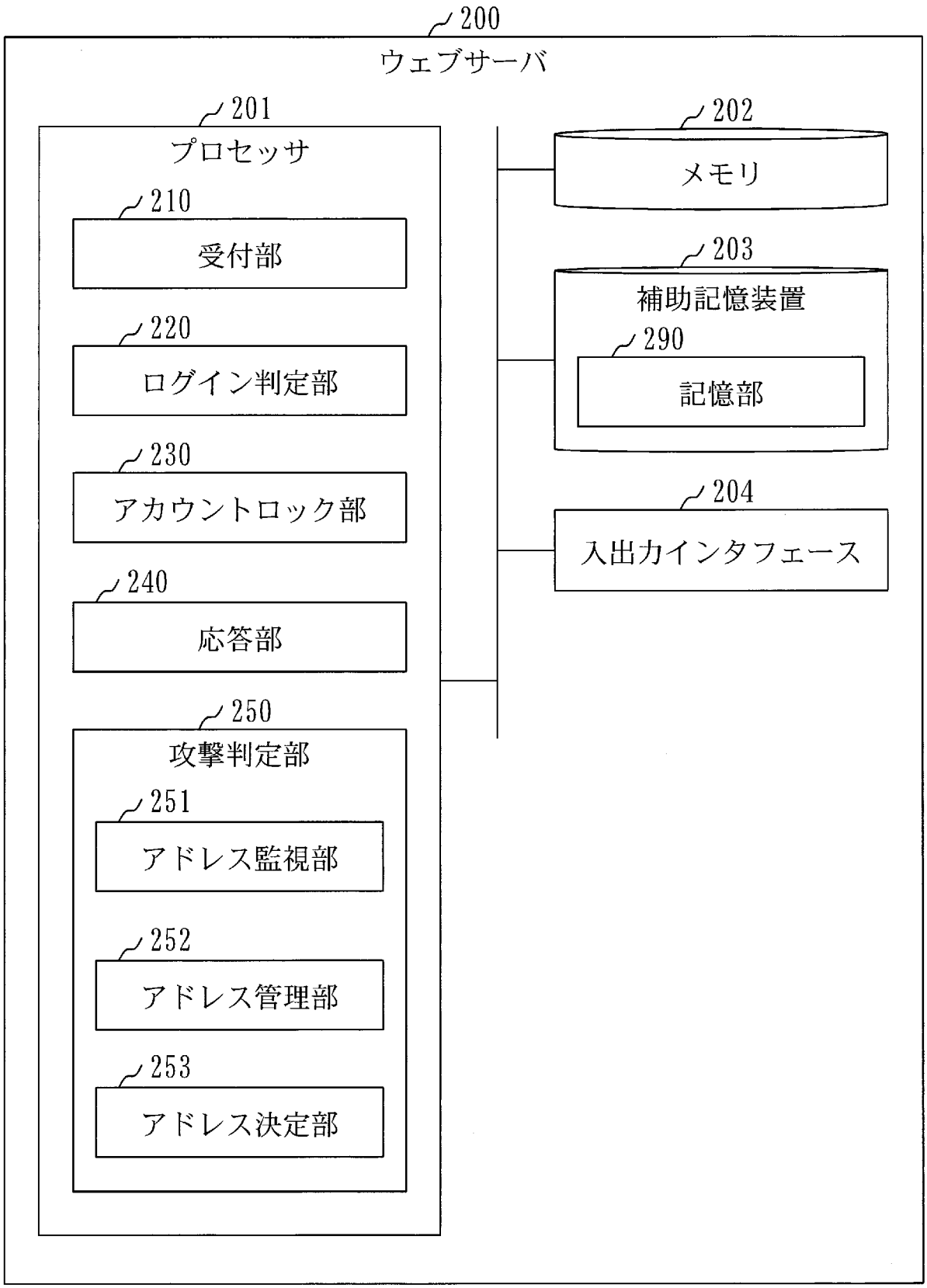
[図11]


仮想アカウント処理(S133)
ログイン識別子の試行回数を取得する
S1331
ログイン識別子の試行回数が上限回数に達しているか判定する
S1332
達している
NO
YES
S1334
認証失敗を応答する
アカウントロックを応答する
S1333
終了

[図12]

試行回数	アカウントの有無	ロック状態	応答内容
上限未満	無し	ー	認証失敗
	有り	未ロック	認証失敗
		ロック中	アカウントロック
上限以上	無し	ー	アカウントロック
	有り	未ロック	アカウントロック (未ロック→ロック中)
		ロック中	アカウントロック

[図13]


200
ウェブサーバ
201
プロセッサ
210
受付部
220
ログイン判定部
230
アカウントロック部
240
応答部
250
攻撃判定部
251
アドレス監視部
252
アドレス管理部
253
アドレス決定部
202
メモリ
203
補助記憶装置
290
記憶部
204
入出力インタフェース

[図14]

293R:アドレステーブル

試行識別子 : Red	
番号	試行元アドレス
1	x.x.x.x
2	x.x.x.x
3	x.x.x.x
4	x.x.x.x
—	—

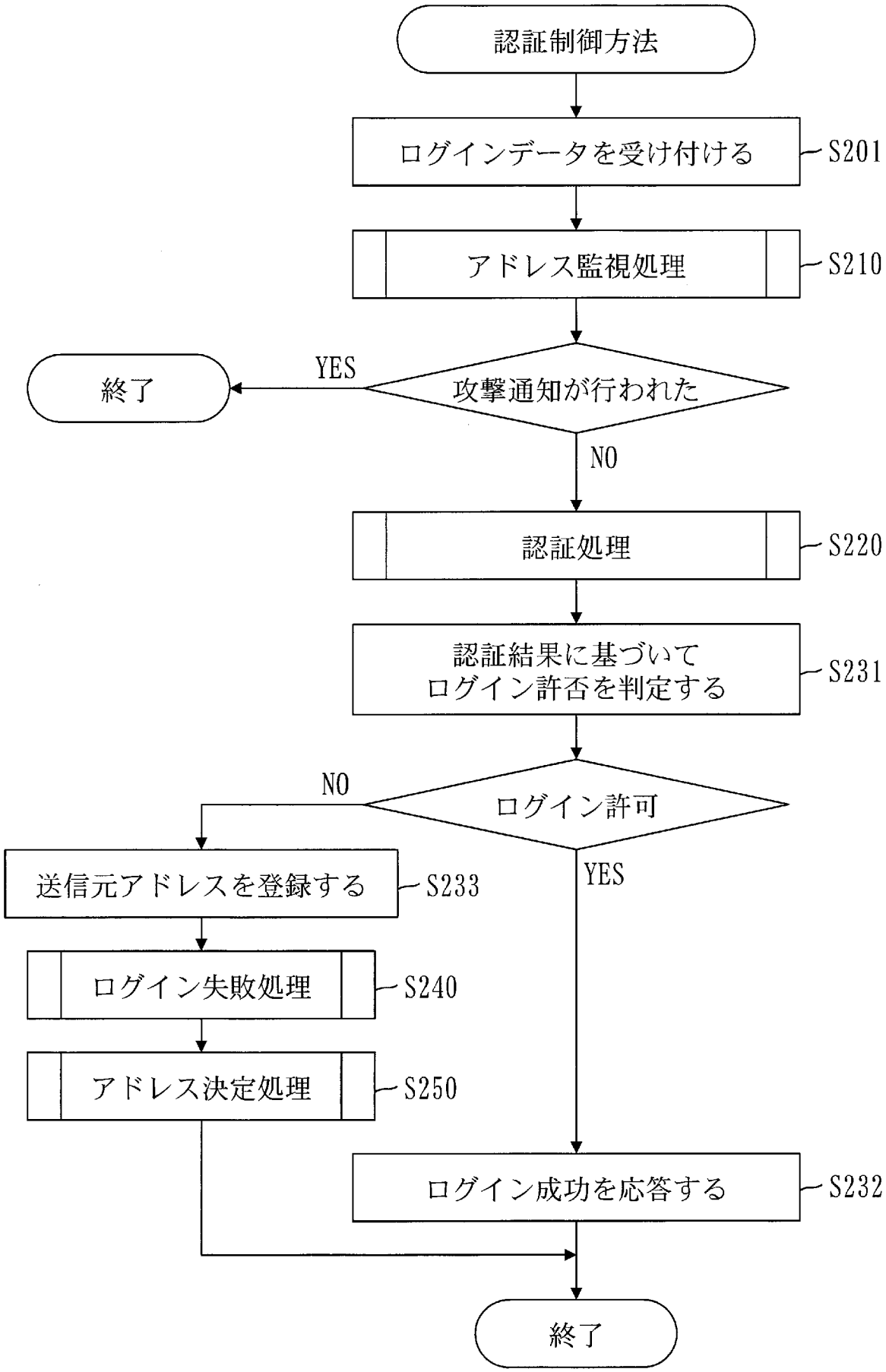
293Y:アドレステーブル

試行識別子 : Yellow	
番号	試行元アドレス
1	y.y.y.y
2	y.y.y.y
3	y.y.y.y
—	—
—	—

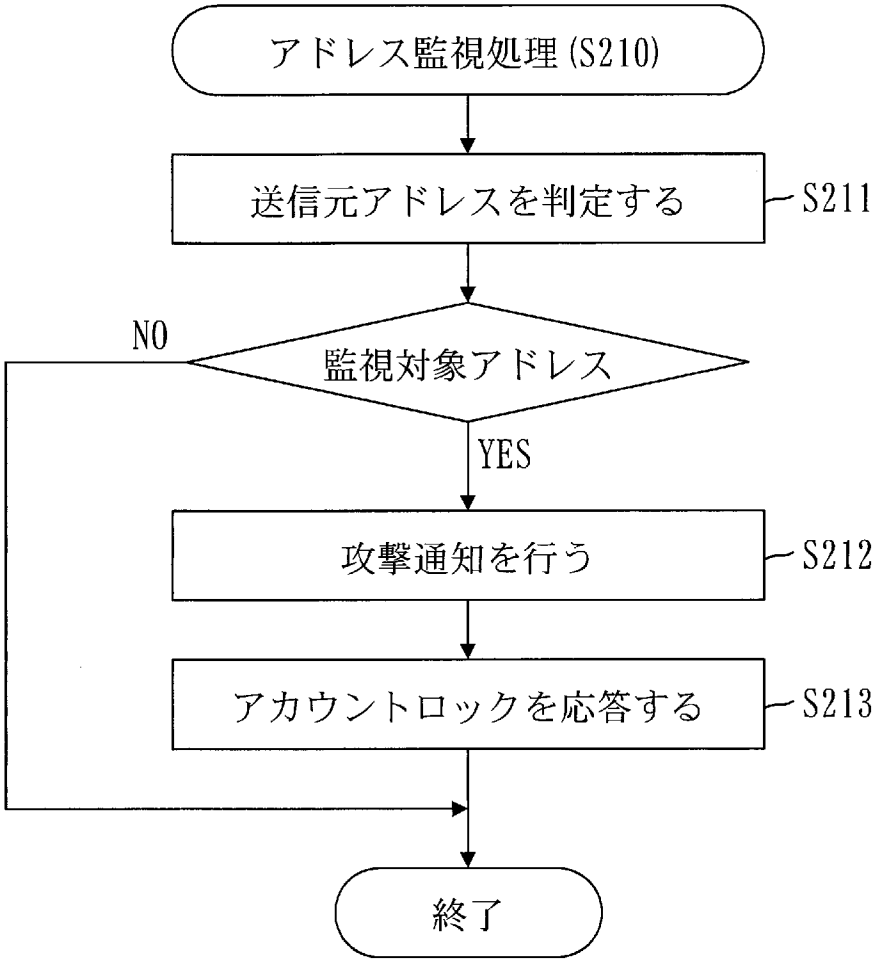
293X:アドレステーブル

試行識別子 : X	
番号	試行元アドレス
1	n.n.n.n
—	—
—	—
—	—
—	—

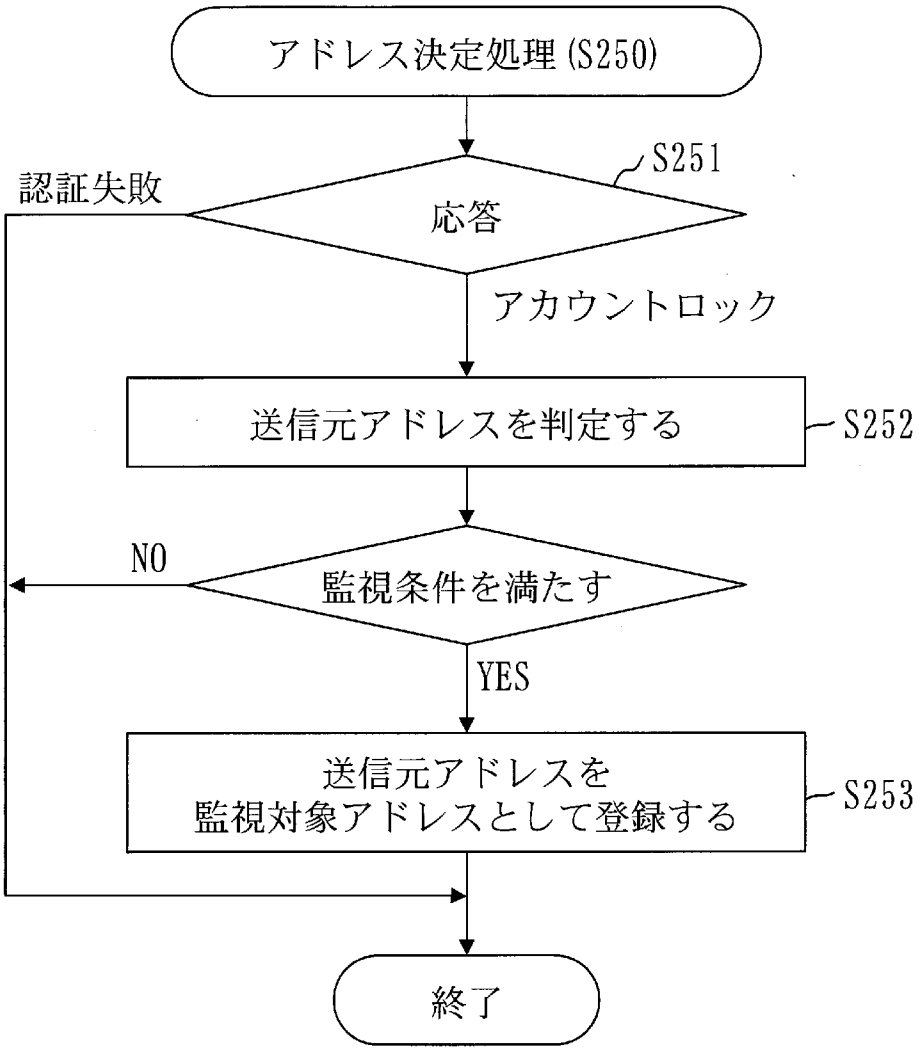
[図15]


認証制御方法
ログインデータを受け付ける
S201
アドレス監視処理
S210
攻撃通知が行われた
YES
終了
NO
認証処理
S220
認証結果に基づいて
ログイン許否を判定する
S231
ログイン許可
NO
YES
送信元アドレスを登録する
S233
ログイン失敗処理
S240
アドレス決定処理
S250
ログイン成功を応答する
S232
終了

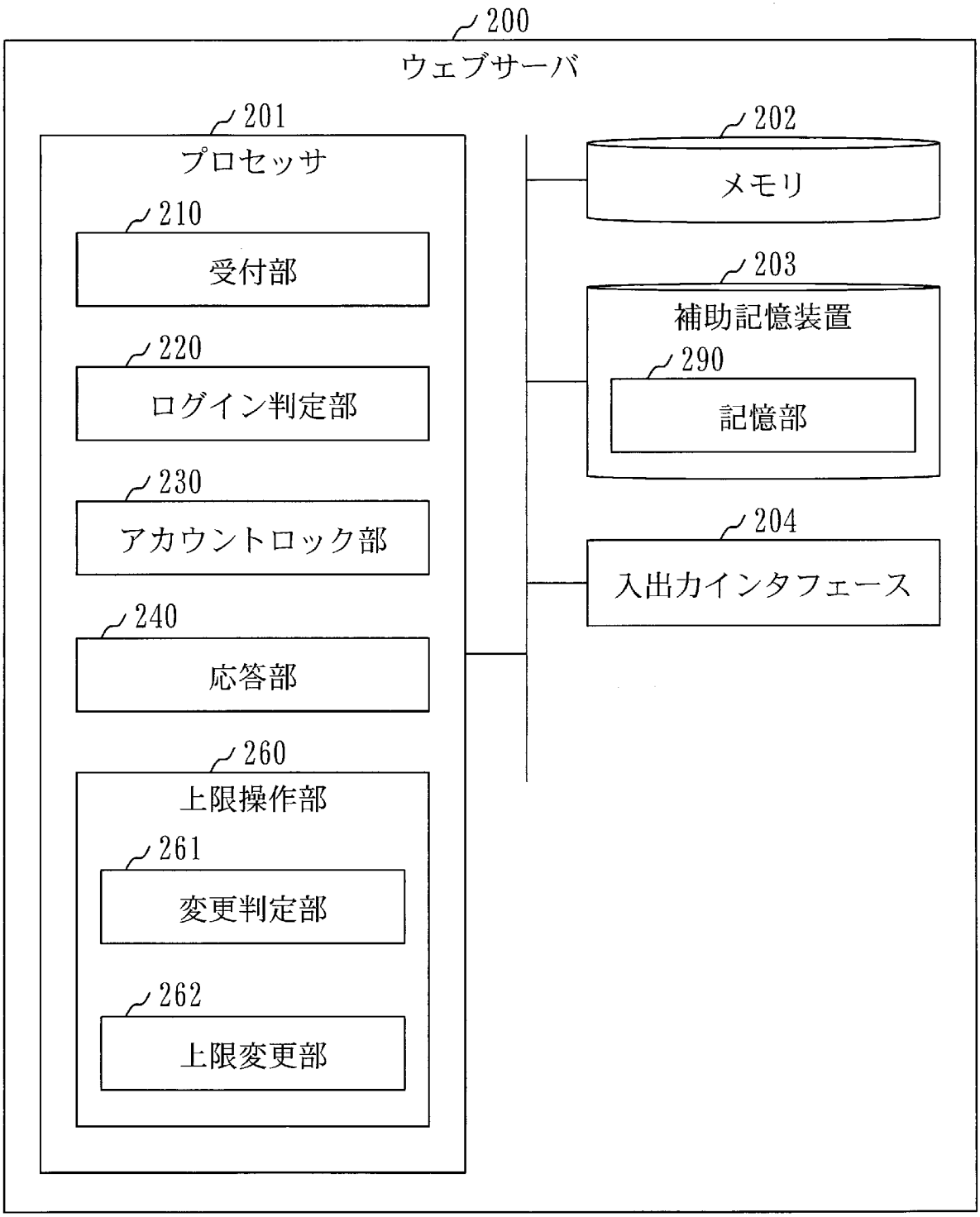
[図16]


アドレス監視処理(S210)
送信元アドレスを判定する
S211
監視対象アドレス
NO
YES
攻撃通知を行う
S212
アカウントロックを応答する
S213
終了

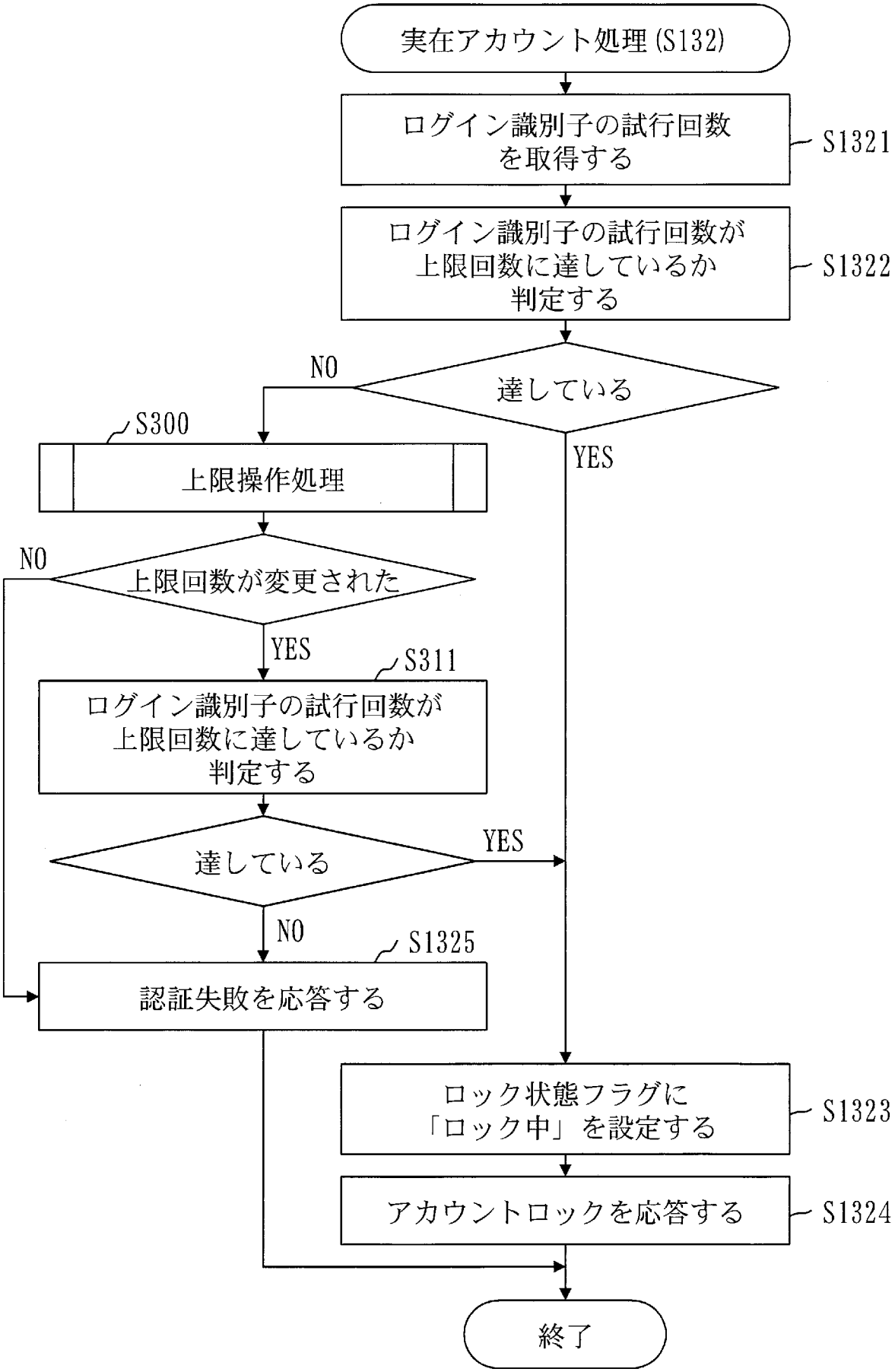
[図17]


アドレス決定処理(S250)
S251
認証失敗
応答
アカウントロック
送信元アドレスを判定する
S252
NO
監視条件を満たす
YES
送信元アドレスを
監視対象アドレスとして登録する
S253
終了

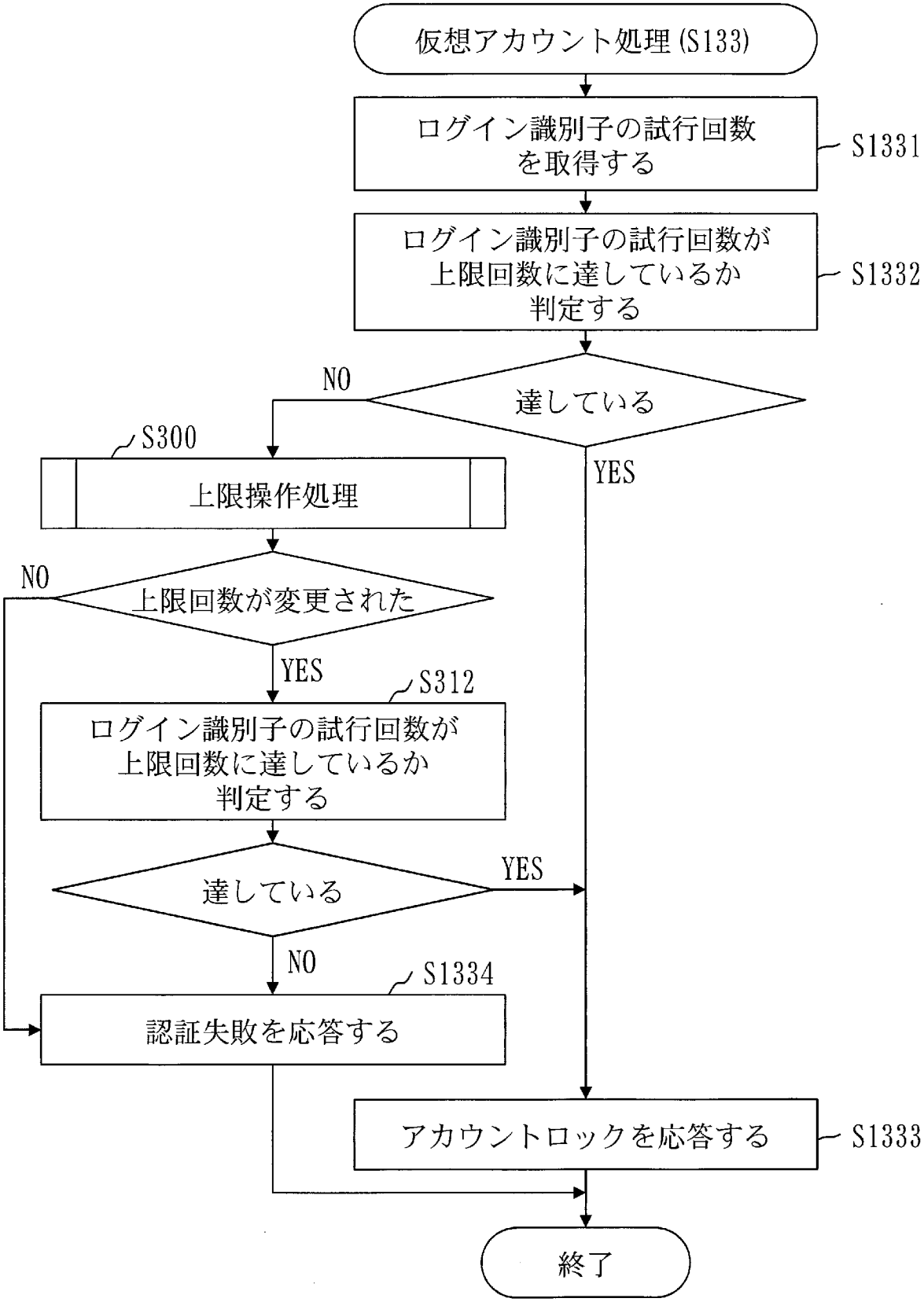
[図18]


200
ウェブサーバ
201
プロセッサ
210
受付部
220
ログイン判定部
230
アカウントロック部
240
応答部
260
上限操作部
261
変更判定部
262
上限変更部
202
メモリ
203
補助記憶装置
290
記憶部
204
入出力インタフェース

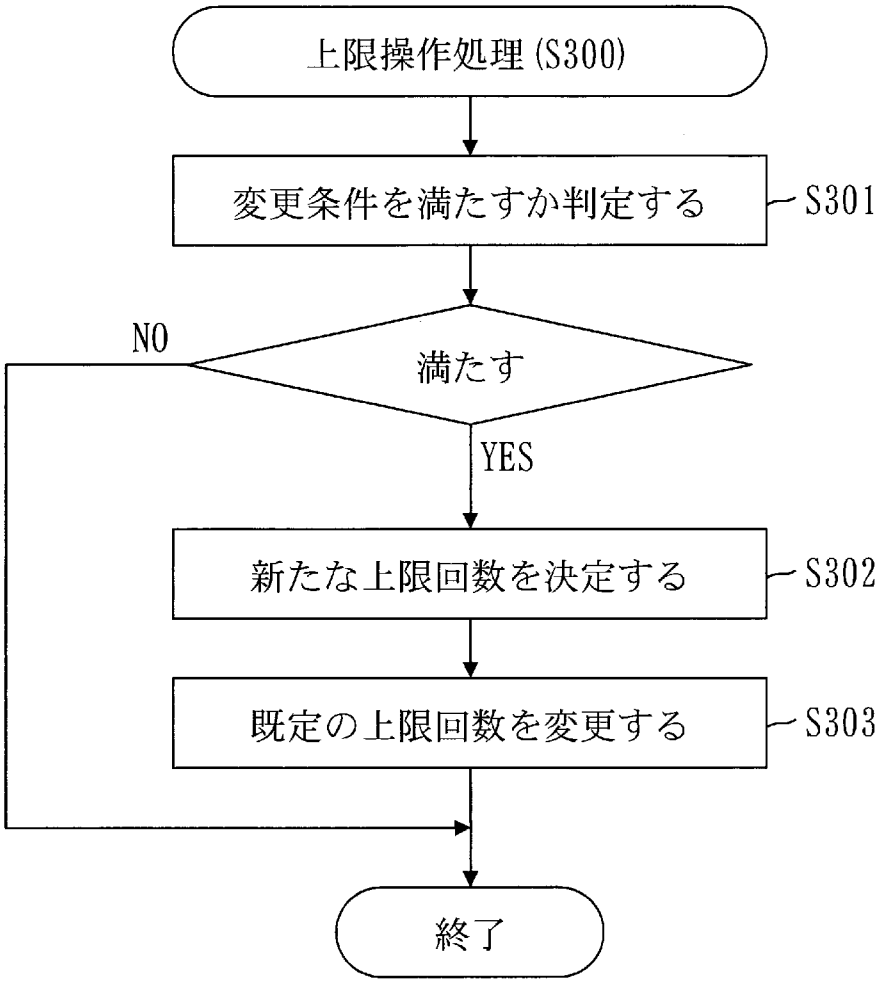
[図19]


実在アカウント処理(S132)
ログイン識別子の試行回数を取得する
S1321
ログイン識別子の試行回数が上限回数に達しているか判定する
S1322
達している
NO
YES
S300
上限操作処理
上限回数が変更された
NO
YES
S311
ログイン識別子の試行回数が上限回数に達しているか判定する
達している
YES
NO
S1325
認証失敗を応答する
ロック状態フラグに「ロック中」を設定する
S1323
アカウントロックを応答する
S1324
終了

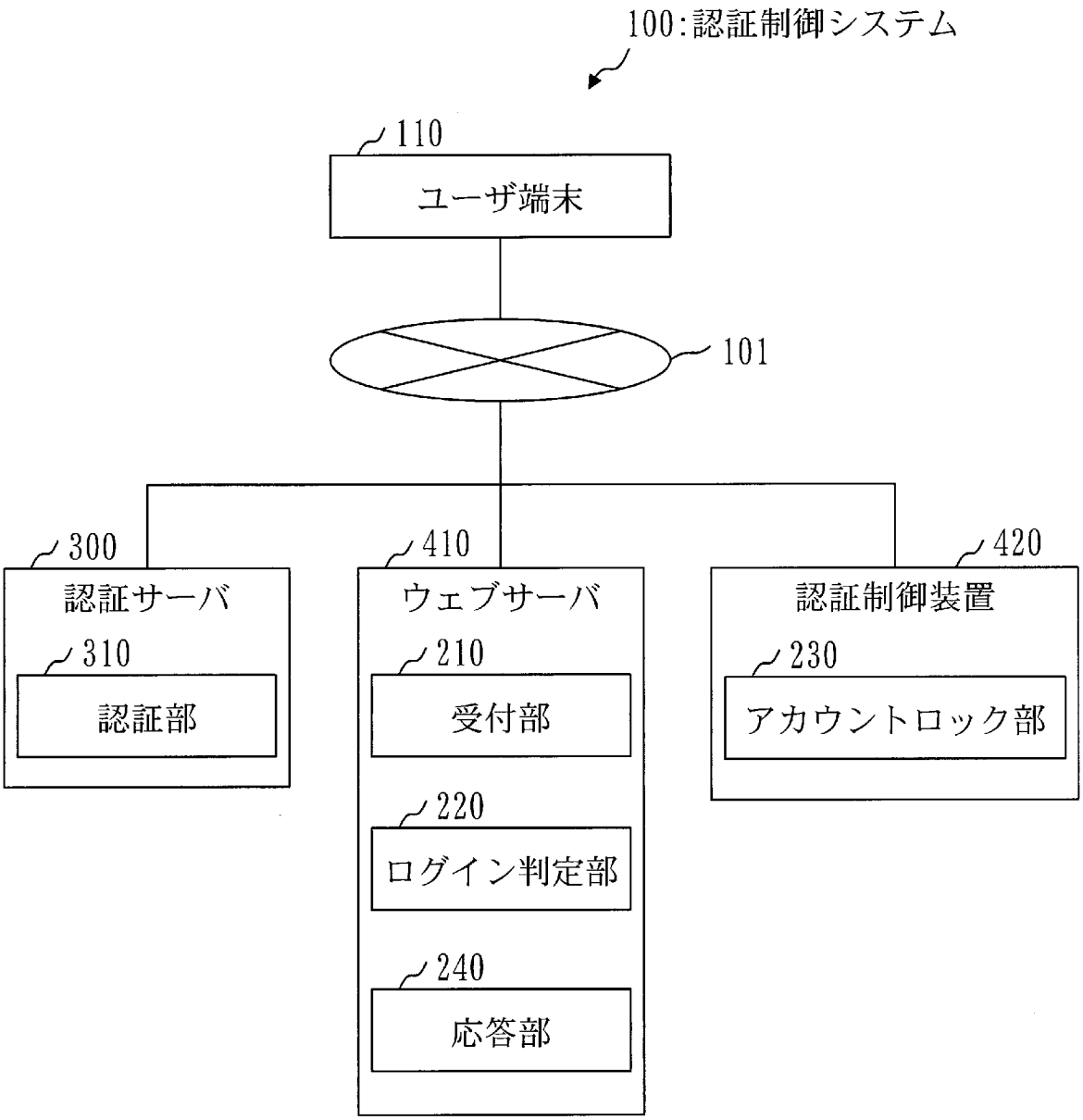
[図20]


仮想アカウント処理(S133)
ログイン識別子の試行回数を取得する
S1331
ログイン識別子の試行回数が上限回数に達しているか判定する
S1332
達している
NO
YES
S300
上限操作処理
上限回数が変更された
NO
YES
S312
ログイン識別子の試行回数が上限回数に達しているか判定する
達している
YES
NO
S1334
認証失敗を応答する
アカウントロックを応答する
S1333
終了

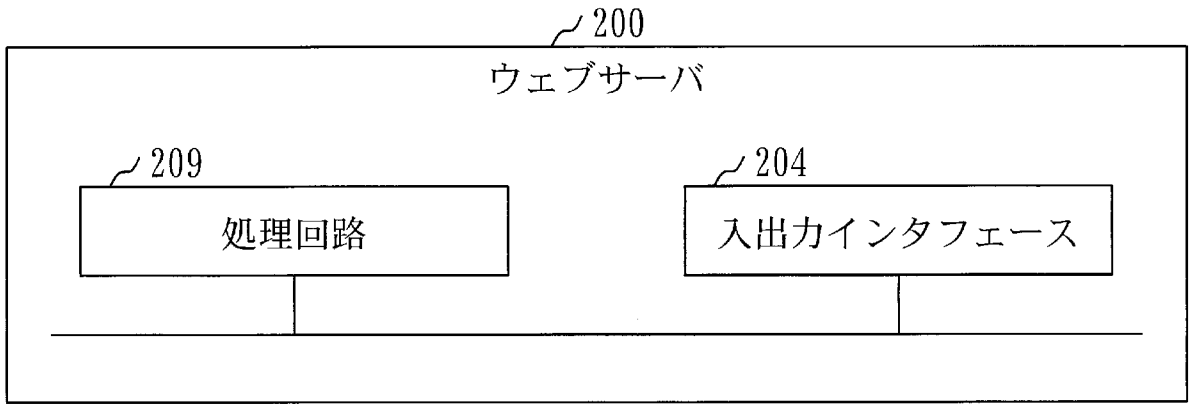
[図21]


上限操作処理(S300)
変更条件を満たすか判定する
S301
満たす
NO
YES
新たな上限回数を決定する
S302
既定の上限回数を変更する
S303
終了

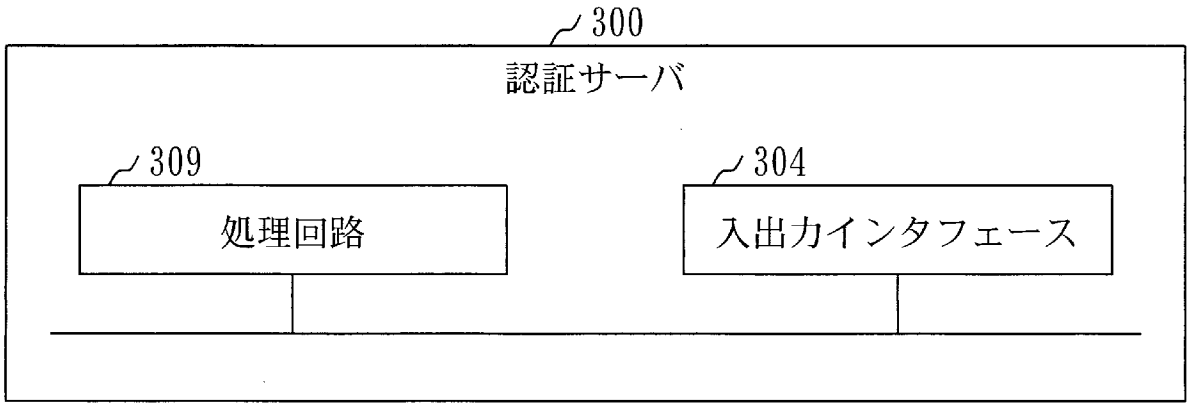
[図22]


100:認証制御システム
110
ユーザ端末
101
300
認証サーバ
310
認証部
410
ウェブサーバ
210
受付部
220
ログイン判定部
240
応答部
420
認証制御装置
230
アカウントロック部

[図23]


200
ウェブサーバ
209
処理回路
204
入出力インタフェース

[図24]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2018/027067

A. CLASSIFICATION OF SUBJECT MATTER
Int. Cl. G06F21/31(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)
Int. Cl. G06F21/31

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Published examined utility model applications of Japan 1922-1996
Published unexamined utility model applications of Japan 1971-2018
Registered utility model specifications of Japan 1996-2018
Published registered utility model applications of Japan 1994-2018

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 2013/0198819 A1 (GORDON, Ariel) 01 August 2013, paragraphs [0030]-[0034], fig. 2 & WO 2013/116169 A1 & CN 104094269 A	1-10
A	JP 2016-119017 A (CANON MARKETING JAPAN INC.) 30 June 2016, paragraphs [0094], [0124]-[0126], fig. 10 (Family: none)	1-10

☐ 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	Date of mailing of the international search report
24.08.2018	04.09.2018
Name and mailing address of the ISA/ Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Authorized officer Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１８／０２７０６７

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

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

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	１９７１－２０１８年
日本国実用新案登録公報	１９９６－２０１８年
日本国登録実用新案公報	１９９４－２０１８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 2013/0198819 A1 (GORDON, Ariel) 2013.08.01, 段落[0030]-[0034],図２ & WO 2013/116169 A1 & CN 104094269 A	1-10
A	JP 2016-119017 A（キヤノンマーケティングジャパン株式会社) 2016.06.30, 段落[0094],[0124]-[0126],図10（ファミリーなし）	1-10

☐　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
「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
「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）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「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
「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
「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
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
２４．０８．２０１８	０４．０９．２０１８

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
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）　５Ｓ　９０７１
平井　誠
電話番号　０３－３５８１－１１０１　内線　３５４６