(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 12 月 8 日(08.12.2016)

WIPO | PCT

(10) 国際公開番号
WO 2016/195090 A1

(51) 国際特許分類:
G06F 21/55 (2013.01) *H04L 12/26* (2006.01)

(21) 国際出願番号: PCT/JP2016/066642

(22) 国際出願日: 2016 年 6 月 3 日(03.06.2016)

(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 2015-115034 2015 年 6 月 5 日(05.06.2015) JP

(71) 出願人: 日本電信電話株式会社(NIPPON TELEGRAPH AND TELEPHONE CORPORATION) [JP/JP]; 〒1008116 東京都千代田区大手町一丁目５番１号 Tokyo (JP).

(72) 発明者: 鐘 揚(ZHONG, Yang); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ 知的財産センタ内 Tokyo (JP). 朝倉 浩志(ASAKURA, Hiroshi); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ 知的財産センタ内 Tokyo (JP). 大嶋 嘉人(OSHIMA, Yoshihito); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ 知的財産センタ内 Tokyo (JP).

(74) 代理人: 特許業務法人酒井国際特許事務所 (SAKAI INTERNATIONAL PATENT OFFICE); 〒1000013 東京都千代田区霞が関３丁目８番１号 虎の門三井ビルディング Tokyo (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.

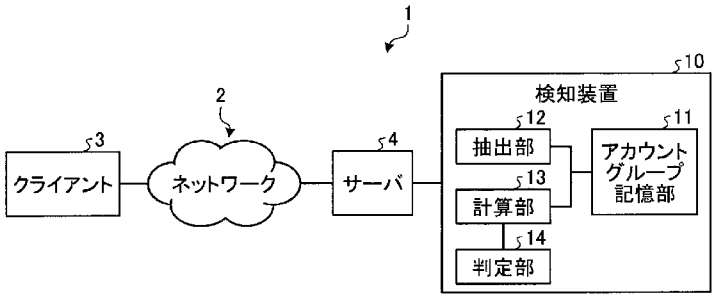
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, 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:

— 国際調査報告（条約第 21 条(3)）

(54) **Title**: DETECTION SYSTEM, DETECTION DEVICE, DETECTION METHOD AND DETECTION PROGRAM

(54) 発明の名称 : 検知システム、検知装置、検知方法及び検知プログラム



2 Network
3 Client
4 Server
10 Detection device
11 Account group storage unit
12 Extracting unit
13 Calculation unit
14 Determination unit

(57) **Abstract**: A detection device (10): extracts accounts and transmission source addresses of the accounts from authentication information obtained from an authentication device that performs user authentication; groups the accounts for each time slot of a prescribed time interval and for each transmission source address in accordance with time stamps and transmission source addresses of the accounts; and extracts account groups by excluding repetition of the same accounts in the same groups. The detection device (10) calculates the number of accounts that repeatedly appear among the extracted account groups. If the number of account groups having the same transmission source address, for which the calculated number of accounts exceeds a first threshold, exceeds a second threshold, the detection device (10) determines that this same transmission source address is the address of an account attacker.

(57) 要約:

[続葉有]

WO 2016/195090 A1

検知装置（１０）は、ユーザ認証を行う認証装置から取得した認証情報からアカウント及びアカウントの送信元アドレスを抽出し、アカウントのタイムスタンプ及び送信元アドレスに応じて、所定時間間隔のタイムスロット毎かつ送信元アドレス毎にアカウントをグループ化し、同一グループ内で同一アカウントの重複を除外したアカウントグループを抽出する。そして、検知装置（１０）は、抽出した各アカウントグループ間で重複するアカウント数を計算する。そして、検知装置（１０）は、計算したアカウント数が第１閾値を越える同一送信元アドレスのアカウントグループの数が第２閾値を越える場合に、この同一送信元アドレスがアカウント攻撃者のアドレスであると判定する。

明　細　書

発明の名称 ：

検知システム、検知装置、検知方法及び検知プログラム

技術分野

[0001] 本発明は、検知システム、検知装置、検知方法及び検知プログラムに関する。

背景技術

[0002] インターネット上のサービスでは、本人性を確認するために、アカウント認証が用いられることが多い。例えば、ユーザは、サービスを利用するためにアカウント認証を試み、認証された場合のみサービスにログインして利用できる。一般的に、アカウント認証は、アカウント及びパスワードを用いる。近年、大量のアカウント及びパスワードを用いてアカウント認証の試行を繰り返すアカウントハッキングにより偶然認証されたアカウント及びパスワードを用い、不正ログインされるという被害が発生している。

[0003] そこで、アカウントハッキングによる被害を防止するため、一定時間内のアカウント認証及び認証失敗の数を計数し、認証失敗の数が一定数を超えた場合、アカウントハッキングとして検知する方法がある。なお、正常の利用でもパスワード忘れなどにより認証失敗はある程度の割合で発生する。企業や無線ＬＡＮ（Local Area Network）スポット等、複数利用者が同一ＩＰ（Internet Protocol）アドレスや同一回線を共用する場合、同一アドレスや同一回線からの認証失敗の数がより多くなり、一定時間内の認証失敗の数が一定数を超える場合がある。この場合も、アカウントハッキングと検知されてしまうおそれがある。よって、実用上は、一定時間内の認証失敗数及び認証成功数と、認証試行数との比率、すなわち、認証失敗率及び認証成功率を用いることが一般的である。

先行技術文献

非特許文献

[0004] 非特許文献1：“リスト型アカウントハッキングによる不正ログインへの対応方策について（サイト管理者などインターネットサービス提供事業者向け対策集）”、総務省、平成２５年（２０１３年）１２月

発明の概要

発明が解決しようとする課題

[0005] しかしながら、認証失敗率及び認証成功率を用いてアカウントハッキングの検知を行う場合、攻撃者は、ダミーアカウントを用意することで、認証失敗率及び認証成功率を低下させずに不正ログインを大量に行う。

[0006] 具体的には、攻撃者は、ログインが成功するダミーアカウント及び不正ログインを行おうとするアカウント（ターゲットアカウント）の両方を用意し、ダミーアカウント及びターゲットアカウントが混在したリストに基づいてログイン試行する。そして、攻撃者は、ターゲットアカウントそのものあるいはターゲットアカウントのパスワードを変えながらログイン試行を繰り返す。そのため、かかるアカウントハッキングは、認証失敗率及び認証成功率に対して閾値を設ける従来の検知方法では、認証失敗率及び認証成功率が低下しないため、閾値で検知できないという課題がある。

[0007] 本願が開示する実施形態の一例は、上記に鑑みてなされたものであって、アカウントハッキングの検知精度を向上させることを目的とする。

課題を解決するための手段

[0008] 本願が開示する実施形態の一例は、ユーザ認証を行う認証装置から取得した認証情報からアカウント及びアカウントの送信元アドレスを抽出し、アカウントのタイムスタンプ及び送信元アドレスに応じて、所定時間間隔のタイムスロット毎かつ送信元アドレス毎にアカウントをグループ化する。そして、同一グループ内で同一アカウントの重複を除外したアカウントグループを抽出する。そして、抽出した各アカウントグループ間で重複するアカウント数を計算する。そして、計算したアカウント数が第１閾値を越える同一送信元アドレスのアカウントグループの数が第２閾値を越える場合に、この同一送信元アドレスがアカウント攻撃者のアドレスであると判定する。

発明の効果

[0009] 本願が開示する実施形態の一例によれば、例えば、アカウントハッキングの検知精度を向上させることができる。

図面の簡単な説明

[0010] [図1]図１は、実施形態に係るシステムの一例を示すブロック図である。

[図2]図２は、実施形態に係るアカウントグループの一例を示す図である。

[図3]図３は、実施形態に係る検知処理の一例を示すフローチャートである。

[図4]図４は、実施例１に係る検知処理の概要の一例を示す図である。

[図5]図５は、実施例２（実施例３）に係る検知処理の概要の一例を示す図である。

[図6]図６は、実施例４（実施例５）に係る検知処理の概要の一例を示す図である。

[図7]図７は、プログラムが実行されることにより検知装置が実現されるコンピュータの一例を示す図である。

発明を実施するための形態

[0011] ［実施形態］

以下、本願が開示する検知システム、検知装置、検知方法及び検知プログラムの実施形態を説明する。なお、以下の実施形態は、一例を示すに過ぎず、本願が開示する技術を限定するものではない。また、以下に示す種々の形態及び実施例は、矛盾しない範囲で適宜組合せてもよい。

[0012] （実施形態に係るシステムの一例）

図１は、実施形態に係るシステムの一例を示すブロック図である。実施形態に係るシステム１は、公衆網等のネットワーク２を介して接続されたクライアント３及びサーバ４を含む。また、サーバ４には、検知装置１０が接続される。ユーザは、ネットワーク２を介してサーバ４に対して認証要求を行い、サーバ４はその結果をユーザに返す。その際、サーバ４は、認証ユーザの情報及び認証の結果を認証レコードとして保持し、検知装置１０に送信する。

[0013] クライアント３は、ネットワーク２を介してサービスを利用するユーザの端末である。実施形態では、クライアント３は、アカウントハッキングによる攻撃者の端末も含む。サーバ４は、サービスを提供するアプリケーションサーバにおけるアカウントによるユーザ認証を行うサーバである。サーバ４は、クライアント３から受信したユーザアカウント及びパスワード等のユーザ情報を用いて、当該ユーザを認証する。

[0014] そして、サーバ４は、認証レコードを出力する。認証レコードは、例えばユーザアカウント（以下、アカウントと呼ぶ）、パスワード、タイムスタンプ、アカウント及びパスワードの送信元のクライアント３のＩＰアドレス等を含む。認証レコードは、ログ形式で出力されてもよい。サーバ４は、サービスを提供するアプリケーションサーバとハードウェア的又はソフトウェア的に一体に構成されてもよい。また、サーバ４は、後述する検知装置２０とハードウェア的又はソフトウェア的に一体に構成されてもよい。

[0015] 検知装置１０は、サーバ４へのアカウントハッキングによる攻撃を検知する。検知装置１０は、アカウントグループ記憶部１１、抽出部１２、計算部１３、判定部１４を有する。

[0016] 抽出部１２は、サーバ４から受信した認証レコードから、認証毎のアカウント、タイムスタンプ、アカウントの送信元のクライアント３のＩＰアドレス（以下、送信元ＩＰアドレスと呼ぶ）を抽出する。なお、アカウントの送信元のクライアント３を特定可能なネットワーク識別子であれば、送信元ＩＰアドレスに限らず、ＭＡＣ（Media Access Control）アドレス等を用いてもよい。また、抽出部１２がサーバ４から受信した認証レコードから抽出するタイムスタンプは、当該アカウントを用いてユーザがサーバ４における認証を試行した時刻である。あるいは、タイムスタンプは、当該認証レコードがサーバ４から検知装置１０へ到着した時刻もしくは検知装置１０において当該認証レコードからアカウントが抽出された時刻であってもよい。

[0017] そして、抽出部１２は、抽出したアカウントを、アカウントのタイムスタンプ及び送信元ＩＰアドレスに応じて、それぞれが期間Δのタイムスロット

毎かつ送信元ＩＰアドレス毎にアカウントをグループ化する。そして、抽出部１２は、グループ化したアカウントの同一グループ内で同一アカウントの重複を除外する。以上が、抽出部１２が行うアカウントグループの抽出である。そして、抽出部１２は、抽出したアカウントグループをアカウントグループ記憶部１１に保存する。

[0018] 図２は、実施形態に係るアカウントグループの一例を示す図である。図２の（ａ）は、タイムスタンプの時刻及び送信元ＩＰアドレスが異なる複数のアカウントを認証レコード群として模式的に示す。検知装置１０の抽出部１２は、認証レコード群を、図２の（ｂ）に示すように、タイムスタンプが属する所定期間Δ（タイムスロットＫ、Ｋ－１）毎かつ送信元ＩＰアドレス（ＩＰアドレスＡ、Ｂ、Ｃ）毎にアカウントをグループ化する。そして、抽出部１２は、同一アカウントグループ内でのアカウントの重複を除外する。

[0019] 例えば、アカウント＝ａａａは、タイムスタンプ＝ｔ１がタイムスロットＫ－１に含まれ、送信元ＩＰアドレス＝Ａである場合には、図２の（ｂ）に示すアカウントグループＡＧ［Ａ］［Ｋ－１］に含まれる。なお、タイムスロットＫは、タイムスロットＫ－１の直後に続く期間である。そして、図２の（ｂ）は、一例を示すに過ぎず、タイムスロットの数、送信元ＩＰアドレスの数は、図２の（ｂ）に示すものに限られない。

[0020] 計算部１３は、抽出部１２により抽出され、アカウントグループ記憶部１１に保存されたアカウントグループを読み出し、各アカウントグループ間で重複するアカウント数（以下、アカウント重複数と呼ぶ）を計算する。例えば、計算部１３は、抽出部１２により抽出された２つのアカウントグループ｛ａａａ，ｂｂｂ，ｃｃｃ｝、｛ｂｂｂ，ｃｃｃ｝がある場合、アカウントｂｂｂ及びｃｃｃが２つのアカウントグループ間で重複するので、アカウント重複数＝２と計算する。計算部１３による計算例は、実施例１～５をもとに後述する。

[0021] 判定部１４は、計算部１３による計算結果をもとに、送信元ＩＰアドレス単位で、アカウント重複数＞α（第１閾値）（αは所定正数）となるアカウ

ントグループの数＞β（第２閾値）（βは所定正数）の場合、当該送信元ＩＰアドレスは、アカウントハッキングによる攻撃者のクライアント３のＩＰアドレスであると判定する。判定部１４による処理例は、実施例１～５をもとに後述する。

[0022] （実施形態に係る検知処理）

図３は、実施形態に係る検知処理の一例を示すフローチャートである。実施形態に係る検知処理は、検知装置１０により実行される。先ず、検知装置１０は、タイムスロットの基準タイムスタンプＢＴを現在時刻で初期化する。そして、検知装置１０は、タイムスロットＩＤ＿Ｋを１で初期化する。そして、検知装置１０は、アカウントグループを格納する配列ＡＧを初期化する（以上、ステップＳ１１）。

[0023] 次に、検知装置１０は、図示しないコンソールから、システム管理者による終了命令がシステム１へ入力されたか否かを判定する（ステップＳ１２）。検知装置１０は、システム管理者による終了命令が入力されたと判定した場合（ステップＳ１２：Ｙｅｓ）、検知処理を終了する。一方、検知装置１０は、システム管理者による終了命令が入力されていないと判定した場合（ステップＳ１２：Ｎｏ）、ステップＳ１３へ処理を移す。

[0024] ステップＳ１３では、検知装置１０は、未処理の認証レコードＲが到着したか否かを判定する。検知装置１０は、未処理の認証レコードＲが到着したと判定した場合（ステップＳ１３：Ｙｅｓ）、ステップＳ１４へ処理を移す。一方、検知装置１０は、未処理の認証レコードＲが到着していないと判定した場合（ステップＳ１３：Ｎｏ）、ステップＳ１２へ処理を移す。

[0025] ステップＳ１４では、検知装置１０は、ステップＳ１３で到着と判定した未処理の認証レコードＲのタイムスタンプからタイムスロットの基準タイムスタンプＢＴを減算した結果が所定期間Δより大であるか否かを判定する。すなわち、検知装置１０は、ステップＳ１４において、ステップＳ１３で到着と判定した未処理の認証レコードＲのタイムスタンプが、ステップＳ１１又は後述のステップＳ１５において現在時刻で初期化したタイムスロットの

基準タイムスタンプＢＴ＋所定期間Δの時間内であるか否かを判定する。

[0026] 検知装置１０は、ステップＳ１３で到着と判定した未処理の認証レコードＲのタイムスタンプからタイムスロットの基準タイムスタンプＢＴを減算した結果が所定期間Δより大であると判定した場合（ステップＳ１４：Ｙｅｓ）、ステップＳ１５へ処理を移す。一方、検知装置１０は、ステップＳ１３で到着と判定した未処理の認証レコードＲのタイムスタンプからタイムスロットの基準タイムスタンプＢＴを減算した結果が所定期間Δ以下と判定した場合（ステップＳ１４：Ｎｏ）、ステップＳ１９へ処理を移す。

[0027] ステップＳ１５では、検知装置１０は、タイムスロットＩＤ＿Ｋを１インクリメントし、タイムスロットの基準タイムスタンプＢＴを現在時刻で初期化する。次に、検知装置１０は、タイムスロットＩＤ＿Ｋ≧Ｎであるか否かを判定する（ステップＳ１６）。ここで、Ｎは、アカウント重複数を計算する対象のタイムスロット数を示す所定自然数である。検知装置１０は、タイムスロットＩＤ＿Ｋ≧Ｎであると判定した場合（ステップＳ１６：Ｙｅｓ）、ステップＳ１７へ処理を移す。一方、検知装置１０は、タイムスロットＩＤ＿Ｋ＜Ｎと判定した場合（ステップＳ１６：Ｎｏ）、ステップＳ１２へ処理を移す。

[0028] ステップＳ１７では、検知装置１０は、アカウント重複数を計算する。アカウント重複数の計算の詳細は、実施例１～５をもとに後述する。次に、検知装置１０は、ステップＳ１７のアカウント重複数の計算結果から、アカウントハッキングの攻撃者のクライアント３のＩＰアドレスを判定する（ステップＳ１８、攻撃判定）。攻撃判定の詳細は、実施例１～５をもとに後述する。検知装置１０は、ステップＳ１８が終了すると、ステップＳ１９へ処理を移す。

[0029] 他方、ステップＳ１９では、検知装置１０は、配列ＡＧがステップＳ１３で到着したとした未処理の認証レコードＲのＩＰアドレスのキーを持っているかどうかを判定する。検知装置１０は、配列ＡＧがステップＳ１３で到着したとした未処理の認証レコードＲのＩＰアドレスのキーを持っていると判

定した場合（ステップＳ１９：Ｙｅｓ）、ステップＳ２１へ処理を移す。一方、検知装置１０は、配列ＡＧがステップＳ１３で到着したとした未処理の認証レコードＲのＩＰアドレスのキーを持っていないと判定した場合（ステップＳ１９：Ｎｏ）、ステップＳ２０へ処理を移す。

[0030] ステップＳ２０では、検知装置１０は、配列ＡＧ［認証レコードＲのＩＰアドレス］を空の配列で初期化する。なお、配列ＡＧ［送信元ＩＰアドレス］［Ｋ］は、送信元ＩＰアドレス及びタイムスロットＩＤ＿Ｋで定まるアカウントグループに属するアカウントを格納する配列である。

[0031] 続いて、ステップＳ２１では、検知装置１０は、配列ＡＧ［認証レコードＲのＩＰアドレス］［Ｋ］に、ユニーク性を保つようにアカウントを追加する。すなわち、ステップＳ２１では、検知装置１０は、配列ＡＧ［認証レコードＲのＩＰアドレス］［Ｋ］に、既に格納されているアカウントは格納せず、未格納のアカウントのみを追加する。または、ステップＳ２１では、検知装置１０は、配列ＡＧ［認証レコードＲのＩＰアドレス］［Ｋ］に、重複を除外しつつアカウントを追加する。検知装置１０は、ステップＳ２１が終了すると、ステップＳ１２へ処理を移す。

[0032]（実施形態による効果）

実施形態は、攻撃者が用意するダミーアカウントが有限であり、ダミーアカウントが繰り返し用いられていることに着目し、各送信元ＩＰアドレスから一定期間中にログイン試行したアカウント重複数に基づき攻撃検知を行う。よって、実施形態によれば、攻撃者が、ターゲットアカウントにダミーアカウントを混在させたリストを用いてアカウントハッキングを行っても、攻撃を検知することができる。

実施例 1

[0033] 図４は、実施例１に係る検知処理の概要の一例を示す図である。実施例１では、タイムスロットＩＤ＿Ｋに含まれるある送信元ＩＰアドレスＸに対して、ＡＧ［Ｘ］［Ｋ］と、ＡＧ［Ｘ］［Ｋｉ］のアカウント重複数Ｈ［Ｘ］［Ｘ］［Ｋ］［Ｋｉ］を下記の式（１）により計算する。ここで、Ｋｉは、

あるタイムスロットＩＤ（Ｋ－Ｎ＋１≦Ｋｉ≦Ｋ（Ｎ＞０））である。ただし、｜＊｜は、集合＊の要素数を示す。実施例１では、計算部１３は、下記の式（１）によるＨ［Ｘ］［Ｘ］［Ｋ］［Ｋｉ］を用いてアカウント重複数を計算する。

[0034] [数1]

$$H[X][X][K][Ki]=|AG[X][K]\cap AG[X][Ki]| \quad \cdots(1)$$

ただし、$K-N+1\leqq Ki\leqq K(N>0)$

[0035] また、実施例１では、判定部１４は、所定正数αに対してＨ［Ｘ］［Ｘ］［Ｋ］［Ｋｉ］＞αの場合１、Ｈ［Ｘ］［Ｘ］［Ｋ］［Ｋｉ］≦αの場合０となる関数ＴＨ（Ｈ［Ｘ］［Ｘ］［Ｋ］［Ｋｉ］）に関し、下記の式（２）で定義されるＣ［Ｘ］を計算する。そして、判定部１４は、下記の式（３）により、所定正数βに対してＣ［Ｘ］＞βとなる送信元ＩＰアドレスＸは、攻撃者のクライアント３のＩＰアドレスであると判定する。なお、判定部１４は、所定正数βに対してＣ［Ｘ］≦βとなる送信元ＩＰアドレスＸは、攻撃者のクライアント３のＩＰアドレスではないと判定する。

[0036] [数2]

$$C[X]=\sum_{K-N+1\leqq Ki\leqq K} TH(H[X][X][K][Ki]) \quad \cdots(2)$$

ただし、$TH(H[X][X][K][Ki])=\begin{cases}1(H[X][X][K][Ki]>\alpha)\\0(H[X][X][K][Ki]\leqq\alpha)\end{cases}$

[0037] [数3]

$$C[X]>\beta \Rightarrow \text{IPアドレスXは攻撃者のIPアドレスである} \quad \cdots(3)$$

[0038] 例えば、図４に示すように、カウントグループＡＧが存在するとする。図４の例では、Ｋ＝２、Ｎ＝２である。計算部１３は、アカウント重複数を次のように計算する。すなわち、ＡＧ［Ａ］［２］と、ＡＧ［Ａ］［２］との間では、“DDD”“DUMMY1”“DUMMY2”“DUMMY3”が重複アカウントであるので、Ｈ［Ａ］［Ａ］［２］［２］＝４となる。また、ＡＧ［Ａ］［２］と、ＡＧ［Ａ］［１］との間では、“DUMMY1”“DUMMY2”“DUMMY3”が重複アカ

ウントであるので、Ｈ［Ａ］［Ａ］［２］［１］＝３となる。ゆえに、α＝２とすると、Ｃ［Ａ］＝２となる。同様にして、Ｃ［Ｂ］＝１、Ｃ［Ｃ］＝２となる。

[0039] そして、β＝２とすると、Ｃ［Ｘ］＞２となる送信元ＩＰアドレスＸが存在しないため、判定部１４は、上記の式（３）により、いずれの送信元ＩＰアドレスも攻撃者のクライアント３のＩＰアドレスではないと判定する。

実施例 2

[0040] 実施例２は、攻撃者が複数のＩＰアドレスを用いて攻撃を行うことに対応するため、同一の送信元ＩＰアドレスに対してだけでなく、他の複数の送信元ＩＰアドレスに対してアカウント重複数を計算する。図５は、実施例２に係る検知処理の概要の一例を示す図である。

[0041] 実施例２では、タイムスロットＩＤ＿Ｋに含まれるある送信元ＩＰアドレスＸ、Ｙ（Ｘ＝Ｙの場合も含む）に対して、ＡＧ［Ｘ］［Ｋ］と、ＡＧ［Ｙ］［Ｋｉ］（Ｋ－Ｎ＋１≦Ｋｉ≦Ｋ（Ｎ＞０））のアカウント重複数Ｈ［Ｘ］［Ｙ］［Ｋ］［Ｋｉ］を下記の式（４）により計算する。実施例２では、計算部１３は、下記の式（４）によるＨ［Ｘ］［Ｙ］［Ｋ］［Ｋｉ］を用いてアカウント重複数を計算する。

[0042] [数4]

$$H[X][Y][K][Ki]=|AG[X][K]\cap AG[Y][Ki]| \quad \cdots (4)$$

ただし、$K-N+1\leqq Ki\leqq K(N>0)$

[0043] また、実施例２では、判定部１４は、所定正数αに対してＨ［Ｘ］［Ｙ］［Ｋ］［Ｋｉ］＞αの場合１、Ｈ［Ｘ］［Ｙ］［Ｋ］［Ｋｉ］≦αの場合０となる関数ＴＨ（Ｈ［Ｘ］［Ｙ］［Ｋ］［Ｋｉ］）に関し、下記の式（５）で定義されるＣ［Ｘ］を計算する。そして、判定部１４は、上記の式（３）により、所定正数βに対してＣ［Ｘ］＞βとなる送信元ＩＰアドレスＸは、攻撃者のクライアント３のＩＰアドレスであると判定する。判定部１４は、所定正数βに対してＣ［Ｘ］≦βとなる送信元ＩＰアドレスＸは、攻撃者の

クライアント３のＩＰアドレスではないと判定する。

[0044] [数5]

$$C[X]=\sum_{K-N+1\leqq Ki\leqq K,\forall Y} TH(H[X][Y][K][Ki]) \quad \cdots (5)$$

ただし、$TH(H[X][Y][K][Ki])=\begin{cases}1(H[X][Y][K][Ki]>\alpha)\\0(H[X][Y][K][Ki]\leqq\alpha)\end{cases}$

[0045] 例えば、図５に示すように、カウントグループＡＧが存在するとする。図５の例では、Ｋ＝２、Ｎ＝２である。計算部１３は、アカウント重複数を次のように計算する。すなわち、ＡＧ［Ａ］［２］と、ＡＧ［Ａ］［２］との間では、“DDD”“DUMMY1”“DUMMY2”“DUMMY3”が重複アカウントであるので、Ｈ［Ａ］［Ａ］［２］［２］＝４となる。また、ＡＧ［Ａ］［２］と、ＡＧ［Ａ］［１］との間では、“DUMMY1”“DUMMY2”“DUMMY3”が重複アカウントであるので、Ｈ［Ａ］［Ａ］［２］［１］＝３となる。同様に、ＡＧ［Ａ］［２］と、ＡＧ［Ｂ］［２］との間では、“DUMMY1”が重複アカウントであるので、Ｈ［Ａ］［Ｂ］［２］［２］＝１となる。また、ＡＧ［Ａ］［２］と、ＡＧ［Ｂ］［１］との間では、“DUMMY1”“DUMMY2”“DUMMY3”が重複アカウントであるので、Ｈ［Ａ］［Ｂ］［２］［１］＝３となる。同様に、ＡＧ［Ａ］［２］と、ＡＧ［Ｃ］［２］との間では、“DUMMY1”“DUMMY2”“DUMMY3”が重複アカウントであるので、Ｈ［Ａ］［Ｃ］［２］［２］＝３となる。また、ＡＧ［Ａ］［２］と、ＡＧ［Ｃ］［１］との間では、“DUMMY2”“DUMMY3”が重複アカウントであるので、Ｈ［Ａ］［Ｃ］［２］［１］＝２となる。ゆえに、α＝２とすると、Ｃ［Ａ］＝４となる。同様にして、Ｃ［Ｂ］＝１、Ｃ［Ｃ］＝５となる。

[0046] そして、β＝２とすると、Ｃ［Ａ］＞２、Ｃ［Ｃ］＞２となるため、判定部１４は、上記の式（３）により、送信元ＩＰアドレスＡ及びＣが攻撃者のクライアント３のＩＰアドレスであると判定する。

実施例 3

[0047] 実施例３は、実施例２に加え、判定部１４は、上記の式（５）においてＴＨ（Ｈ［Ｘ］［Ｙ］［Ｋ］［Ｋｉ］）＝１（Ｋ－Ｎ＋１≦Ｋｉ≦Ｋ（Ｎ＞０

））となるＫｉが存在する場合、送信元ＩＰアドレスＹも攻撃者のクライアント３のＩＰアドレスであると判定する。つまり、判定部１４は、下記の式（６）により、Ｃ［Ｘ］＞βとなる送信元ＩＰアドレス、及び、Ｃ［Ｘ］≦βかつＴＨ（Ｈ［Ｘ］［Ｙ］［Ｋ］［Ｋｉ］）＝１（Ｋ－Ｎ＋１≦Ｋｉ≦Ｋ（Ｎ＞０））となるＫｉが存在する場合の送信元ＩＰアドレスＹは、攻撃者のクライアント３のＩＰアドレスであると判定する。

[0048] [数6]

$$C[X]>\beta \Rightarrow \text{IPアドレスXは攻撃者のIPアドレスである}$$
$$\text{攻撃者のIPアドレスXに対して、}$$
$$TH(H[X][Y][K][Ki])=1\text{となる}Ki(K-N+1\leqq Ki\leqq K(N>0))\text{が存在する}$$
$$\Rightarrow \text{IPアドレスYは攻撃者のIPアドレスである} \quad \cdots (6)$$

[0049] 実施例３は、α＝２、β＝２とすると、図５においてＣ［Ａ］＞２、Ｃ［Ｃ］＞２となるため、上記の式（６）により、送信元ＩＰアドレスＡ及びＣが攻撃者のクライアント３のＩＰアドレスであると判定する。さらに、実施例３は、図５においてＴＨ（Ｈ［Ａ］［Ｂ］［２］［１］）＝１となるため、送信元ＩＰアドレスＢも攻撃者のクライアント３のＩＰアドレスであると判定する。

[0050] 以上の実施例２及び３によれば、ダミーアカウントを利用した複数の送信元ＩＰアドレスによる不正ログインを検出し、攻撃者による不正ログインを減少させることが可能である。

実施例 ４

[0051] 実施例４は、判定部１４が、アカウント重複数を計算する際、送信元ＩＰアドレス間と、タイムスロット間との違いを考慮し、アカウントグループ毎に重み付けを行ってアカウント重複数を計算する。図６は、実施例４に係る検知処理の概要の一例を示す図である。

[0052] 実施例４は、下記の式（７）に示すように、アカウントグループＡＧ［Ｙ］［Ｋｉ］（Ｋ－Ｎ＋１≦Ｋｉ≦Ｎ（Ｎ＞０））毎に加重係数Ｗ［Ｙ］［Ｋｉ］（Ｋ－Ｎ＋１≦Ｋｉ≦Ｎ）をＴＨ（Ｈ［Ｘ］［Ｙ］［Ｋ］［Ｋｉ］）（

Ｋ－Ｎ＋１≦Ｋｉ≦Ｎ（Ｎ＞０））に乗算してＣ［Ｘ］を算出する。

[0053] [数7]

$$C[X]=\sum_{K-N+1\leqq Ki\leqq K,\forall Y} W[Y][Ki]*TH(H[X][Y][K][Ki]) \quad \cdots (7)$$

ただし、$TH(H[X][Y][K][Ki])=\begin{cases}1(H[X][Y][K][Ki]>\alpha)\\0(H[X][Y][K][Ki]\leqq\alpha)\end{cases}$

[0054] 例えば、図６に示すように、カウントグループＡＧが存在するとする。そして、ＡＧ［Ｙ］［Ｋｉ］（Ｋ－Ｎ＋１≦Ｋｉ≦Ｋ－１）と対応する加重係数Ｗ［Ｙ］［Ｋｉ］の初期値は、全て１．０であるとする。例えば、送信元ＩＰアドレス間の重複をより重視する場合（以下、ルール１と呼ぶ）、Ｘ＝Ｙの場合にＷ［Ｙ］［Ｋｉ］の値を相対的に小さく、Ｘ≠Ｙの場合にＷ［Ｙ］［Ｋｉ］の値を相対的に大きくする。これにより、送信元ＩＰアドレスが異なる場合の重複がより強調される。また、例えば、タイムスロットの時刻の近接に応じて重複をより重視する場合（以下、ルール２と呼ぶ）、送信元ＩＰアドレスＸに対する送信元ＩＰアドレスＹの加重係数Ｗ［Ｙ］［Ｋｉ］について、Ｗ［Ｙ］［Ｋ－１］＞Ｗ［Ｙ］［Ｋ－２］＞・・・＞Ｗ［Ｙ］［Ｋ－Ｎ＋１］となるようにＷ［Ｙ］［Ｋｉ］の値を設定する。これにより、近接する時刻におけるアカウントの重複がより強調される。なお、重み付けの方法は、ルール１及び２に限らず、例えばルール１及びルール２を組合せたルールであってもよい。

[0055] 図６に示す例では、ルール１に基づき、Ｗ［Ａ］［１］＝Ｗ［Ａ］［２］＝０．１、Ｗ［Ｂ］［１］＝Ｗ［Ｂ］［２］＝Ｗ［Ｃ］［１］＝Ｗ［Ｃ］［２］＝１．０と設定する。そして、ＡＧ［Ａ］［２］と、ＡＧ［Ａ］［２］との間では、“DDD”“DUMMY1”“DUMMY2”“DUMMY3”が重複アカウントであるので、Ｈ［Ａ］［Ａ］［２］［２］＝４となる。また、ＡＧ［Ａ］［２］と、ＡＧ［Ａ］［１］との間では、“DUMMY1”“DUMMY2”“DUMMY3”が重複アカウントであるので、Ｈ［Ａ］［Ａ］［２］［１］＝３となる。同様に、ＡＧ［Ａ］［２］と、ＡＧ［Ｂ］［２］との間では、“DUMMY1”が重複アカウントであるので、Ｈ［Ａ］［Ｂ］［２］［２］＝１となる。また、ＡＧ［

Ａ］［２］と、ＡＧ［Ｂ］［１］との間では、“DUMMY1”“DUMMY2”“DUMMY3”が重複アカウントであるので、Ｈ［Ａ］［Ｂ］［２］［１］＝３となる。同様に、ＡＧ［Ａ］［２］と、ＡＧ［Ｃ］［２］との間では、“DUMMY1”“DUMMY2”“DUMMY3”が重複アカウントであるので、Ｈ［Ａ］［Ｃ］［２］［２］＝３となる。また、ＡＧ［Ａ］［２］と、ＡＧ［Ｃ］［１］との間では、“DUMMY2”“DUMMY3”が重複アカウントであるので、Ｈ［Ａ］［Ｃ］［２］［１］＝２となる。ゆえに、α＝２とすると、Ｃ［Ａ］＝０．１×ＴＨ（Ｈ［Ａ］［Ａ］［２］［２］）＋０．１×ＴＨ（Ｈ［Ａ］［Ａ］［２］［１］）＋１．０×ＴＨ（Ｈ［Ａ］［Ｂ］［２］［２］）＋１．０×ＴＨ（Ｈ［Ａ］［Ａ］［２］［１］）＋１．０×ＴＨ（Ｈ［Ａ］［Ｃ］［２］［２］）＋１．０×ＴＨ（Ｈ［Ａ］［Ｃ］［２］［１］）＝０．１×１＋０．１×１＋１．０×０＋１．０×１＋１．０×１＋１．０×０＝２．２となる。

[0056] そして、β＝２とすると、Ｃ［Ａ］＞２となるため、判定部１４は、上記の式（３）により、送信元ＩＰアドレスＡが攻撃者のクライアント３のＩＰアドレスであると判定する。

[0057] 同様に、Ｗ［Ｃ］［１］＝Ｗ［Ｃ］［２］＝０．１、Ｗ［Ｂ］［１］＝Ｗ［Ｂ］［２］＝Ｗ［Ａ］［１］＝Ｗ［Ａ］［２］＝１．０と設定する。そして、ＡＧ［Ｃ］［２］と、ＡＧ［Ｃ］［２］との間では、“CCC”“DUMMY1”“DUMMY2”“DUMMY3”“DUMMY4”が重複アカウントであるので、Ｈ［Ｃ］［Ｃ］［２］［２］＝４となる。また、ＡＧ［Ｃ］［２］と、ＡＧ［Ｃ］［１］との間では、“DUMMY2”“DUMMY3”“DUMMY4”が重複アカウントであるので、Ｈ［Ｃ］［Ｃ］［２］［１］＝３となる。同様に、ＡＧ［Ｃ］［２］と、ＡＧ［Ｂ］［２］との間では、“DUMMY1”“DUMMY4”が重複アカウントであるので、Ｈ［Ｃ］［Ｂ］［２］［２］＝２となる。また、ＡＧ［Ｃ］［２］と、ＡＧ［Ｂ］［１］との間では、“DUMMY1”“DUMMY2”“DUMMY3”が重複アカウントであるので、Ｈ［Ｃ］［Ｂ］［２］［１］＝３となる。同様に、ＡＧ［Ｃ］［２］と、ＡＧ［Ａ］［２］との間では、“DUMMY1”“DUMMY2”“DUMMY3”が重複アカウントであるので、Ｈ［Ｃ］［Ａ］［２］［２］＝

３となる。また、ＡＧ［Ｃ］［２］と、ＡＧ［Ａ］［１］との間では、“DUMMY1”“DUMMY2”“DUMMY3”が重複アカウントであるので、Ｈ［Ｃ］［Ａ］［２］［１］＝３となる。ゆえに、α＝２とすると、Ｃ［Ｃ］＝０．１×ＴＨ（Ｈ［Ｃ］［Ｃ］［２］［２］）＋０．１×ＴＨ（Ｈ［Ｃ］［Ｃ］［２］［１］）＋１．０×ＴＨ（Ｈ［Ｃ］［Ｂ］［２］［２］）＋１．０×ＴＨ（Ｈ［Ｃ］［Ｂ］［２］［１］）＋１．０×ＴＨ（Ｈ［Ｃ］［Ａ］［２］［２］）＋１．０×ＴＨ（Ｈ［Ｃ］［Ａ］［２］［１］）＝０．１×１＋０．１×１＋１．０×０＋１．０×１＋１．０×１＋１．０×１＝３．２となる。

[0058] そして、β＝２とすると、Ｃ［Ｃ］＞２となるため、判定部１４は、上記の式（３）により、送信元ＩＰアドレスＣは攻撃者のクライアント３のＩＰアドレスであると判定する。

実施例 5

[0059] 実施例５は、実施例３と実施例４の組合せである。すなわち、実施例５は、実施例４に加え、さらに、判定部１４は、上記の式（７）においてＴＨ（Ｈ［Ｘ］［Ｙ］［Ｋ］［Ｋｉ］）＝１（Ｋ－Ｎ＋１≦Ｋｉ≦Ｋ（Ｎ＞０））となるＫｉが存在する場合、送信元ＩＰアドレスＹも攻撃者のクライアント３のＩＰアドレスであると判定する。つまり、判定部１４は、上記の式（６）により、Ｃ［Ｘ］＞βとなる送信元ＩＰアドレス、及び、Ｃ［Ｘ］≦βかつＴＨ（Ｈ［Ｘ］［Ｙ］［Ｋ］［Ｋｉ］）＝１（Ｋ－Ｎ＋１≦Ｋｉ≦Ｋ（Ｎ＞０））となるＫｉが存在する場合の送信元ＩＰアドレスＹは、攻撃者のクライアント３のＩＰアドレスであると判定する。

[0060] 実施例５は、α＝２、β＝２とすると、図６においてＣ［Ａ］＞２、Ｃ［Ｃ］＞２となるため、上記の式（６）により、送信元ＩＰアドレスＡ及びＣが攻撃者のクライアント３のＩＰアドレスであると判定する。さらに、実施例５は、図６においてＴＨ（Ｈ［Ｃ］［Ｂ］［２］［１］）＝１となるため、送信元ＩＰアドレスＢも攻撃者のクライアント３のＩＰアドレスであると判定する。

[0061] 以上の実施例４及び５によれば、ダミーアカウントを利用した複数の送信

元ＩＰアドレスによる不正ログインをより高精度に検出し、攻撃者による不正ログインを減少させることが可能である。

[0062] なお、以上の実施例１～５では、計算部１３は、各アカウントグループ間のアカウント重複数を算出する際に、各アカウントグループの自身同士のアカウント重複数も含めて算出するとした。しかし、これに限らず、計算部１３は、各アカウントグループ間のアカウント重複数を算出する際に、各アカウントグループの自身同士のアカウント重複数を除外し、異なるアカウントグループ間のアカウント重複数のみを算出するとしてもよい。この場合、上記した所定正数であるα及びβも、適切な値となるよう調整される。

[0063] 以上の実施例１～５に示すように、本願が開示する実施形態は、認証失敗率及び認証成功率に依存せず、攻撃者が利用するダミーアカウントを検出することで攻撃判別を行う。このため、実施形態は、攻撃者が自ら用いる送信元ＩＰアドレスからの認証失敗率及び認証成功率を恣意的に操作して大量に不正ログインを行うことに対して攻撃検知が可能になり、攻撃者による不正ログインを減少させることができる。

[0064] （検知装置の装置構成について）

図１に示す検知装置１０の各構成要素は機能概念的なものであり、必ずしも物理的に図示のように構成されていることを要しない。すなわち、検知装置１０の機能の分散及び統合の具体的形態は図示のものに限られず、全部又は一部を、各種の負荷や使用状況等に応じて、任意の単位で機能的又は物理的に分散又は統合して構成することができる。

[0065] また、検知装置１０において行われる各処理は、全部又は任意の一部が、ＣＰＵ（Central Processing Unit）等の処理装置及び処理装置により解析実行されるプログラムにて実現されてもよい。また、検知装置１０において行われる各処理は、ワイヤードロジックによるハードウェアとして実現されてもよい。

[0066] また、実施形態及び実施例において説明した各処理のうち、自動的に行われるものとして説明した処理の全部又は一部を手動的に行うこともできる。

もしくは、実施形態及び実施例において説明した各処理のうち、手動的に行われるものとして説明した処理の全部又は一部を公知の方法で自動的に行うこともできる。この他、上記及び図示の処理手順、制御手順、具体的名称、各種のデータやパラメータを含む情報については、特記する場合を除いて適宜変更することができる。

[0067] （プログラムについて）

図７は、プログラムが実行されることにより、検知装置が実現されるコンピュータの一例を示す図である。コンピュータ１０００は、例えば、メモリ１０１０、ＣＰＵ１０２０を有する。また、コンピュータ１０００は、ハードディスクドライブインタフェース１０３０、ディスクドライブインタフェース１０４０、シリアルポートインタフェース１０５０、ビデオアダプタ１０６０、ネットワークインタフェース１０７０を有する。コンピュータ１０００において、これらの各部はバス１０８０によって接続される。

[0068] メモリ１０１０は、ＲＯＭ（Read Only Memory）１０１１及びＲＡＭ１０１２を含む。ＲＯＭ１０１１は、例えば、ＢＩＯＳ（Basic Input Output System）等のブートプログラムを記憶する。ハードディスクドライブインタフェース１０３０は、ハードディスクドライブ１０３１に接続される。ディスクドライブインタフェース１０４０は、ディスクドライブ１０４１に接続される。例えば磁気ディスクや光ディスク等の着脱可能な記憶媒体が、ディスクドライブ１０４１に挿入される。シリアルポートインタフェース１０５０は、例えばマウス１０５１、キーボード１０５２に接続される。ビデオアダプタ１０６０は、例えばディスプレイ１０６１に接続される。

[0069] ハードディスクドライブ１０３１は、例えば、ＯＳ１０９１、アプリケーションプログラム１０９２、プログラムモジュール１０９３、プログラムデータ１０９４を記憶する。すなわち、検知装置１０の各処理を規定するプログラムは、コンピュータ１０００によって実行される指令が記述されたプログラムモジュール１０９３として、例えばハードディスクドライブ１０３１に記憶される。例えば、検知装置１０における機能構成と同様の情報処理を

実行するためのプログラムモジュール１０９３が、ハードディスクドライブ１０３１に記憶される。

[0070] また、上記の実施形態での処理で用いられる設定データは、プログラムデータ１０９４として、例えばメモリ１０１０やハードディスクドライブ１０３１に記憶される。そして、ＣＰＵ１０２０が、メモリ１０１０やハードディスクドライブ１０３１に記憶されたプログラムモジュール１０９３やプログラムデータ１０９４を必要に応じてＲＡＭ１０１２に読み出して実行する。

[0071] なお、プログラムモジュール１０９３やプログラムデータ１０９４は、ハードディスクドライブ１０３１に記憶される場合に限らず、例えば着脱可能な記憶媒体に記憶され、ディスクドライブ１０４１等を介してＣＰＵ１０２０によって読み出されてもよい。あるいは、プログラムモジュール１０９３やプログラムデータ１０９４は、ネットワーク（ＬＡＮ（Local Area Network）、ＷＡＮ（Wide Area Network）等）を介して接続された他のコンピュータに記憶されてもよい。そして、プログラムモジュール１０９３やプログラムデータ１０９４は、ネットワークインタフェース１０７０を介してＣＰＵ１０２０によって読み出されてもよい。

[0072] 以上の実施形態ならびに実施形態の変形例は、本願が開示する技術に含まれると同様に、請求の範囲に記載された発明とその均等の範囲に含まれるものである。

符号の説明

[0073] １ システム

２ ネットワーク

３ クライアント

４ サーバ

１０ 検知装置

１１ アカウントグループ記憶部

１２ 抽出部

１３　計算部

１４　判定部

１０００　コンピュータ

１０１０　メモリ

１０２０　ＣＰＵ

請求の範囲

[請求項1] ユーザ認証を行う認証装置と、

前記認証装置から取得した認証情報からアカウント及びアカウントの送信元アドレスを抽出し、アカウントのタイムスタンプ及び送信元アドレスに応じて、所定時間間隔のタイムスロット毎かつ送信元アドレス毎にアカウントをグループ化し、同一グループ内で同一アカウントの重複を除外したアカウントグループを抽出する抽出部と、

前記抽出部により抽出された各アカウントグループ間で重複するアカウント数を計算する計算部と、

前記計算部により計算されたアカウント数が第１閾値を越える同一送信元アドレスのアカウントグループの数が第２閾値を越える場合に、該同一送信元アドレスが攻撃者のアドレスであると判定する判定部と

を備える検知装置と

を含むことを特徴とする検知システム。

[請求項2] 認証装置から取得した認証情報からアカウント及びアカウントの送信元アドレスを抽出し、アカウントのタイムスタンプ及び送信元アドレスに応じて、所定時間間隔のタイムスロット毎かつ送信元アドレス毎にアカウントをグループ化し、同一グループ内で同一アカウントの重複を除外したアカウントグループを抽出する抽出部と、

前記抽出部により抽出された各アカウントグループ間で重複するアカウント数を計算する計算部と、

前記計算部により計算されたアカウント数が第１閾値を越える同一送信元アドレスのアカウントグループの数が第２閾値を越える場合に、該同一送信元アドレスが攻撃者のアドレスであると判定する判定部と

を備えることを特徴とする検知装置。

[請求項3] 前記計算部は、第１の送信元アドレスのアカウントグループのうち

の最新のタイムスロットに該当するアカウントグループと、該第１の送信元アドレスのアカウントグループのうちの最新のタイムスロット以前の所定数の各タイムスロットに該当する各アカウントグループとの間で重複する第１のアカウント数をそれぞれ計算し、

前記判定部は、前記第１のアカウント数が前記第１閾値を越えるアカウントグループの数が前記第２閾値を越える場合に、該第１の送信元アドレスが攻撃者のアドレスであると判定する

ことを特徴とする請求項２に記載の検知装置。

[請求項4] さらに、

前記計算部は、前記第１の送信元アドレスのアカウントグループのうちの最新のタイムスロットに該当するアカウントグループと、前記第１の送信元アドレス以外の送信元アドレスのアカウントグループのうちの最新のタイムスロット以前の所定数の各タイムスロットに該当する各アカウントグループとの間で重複する第２のアカウント数をそれぞれ計算し、

前記判定部は、前記第２のアカウント数が前記第１閾値を越えるアカウントグループの数が前記第２閾値を越える場合に、該第１の送信元アドレスが攻撃者のアドレスであると判定する

ことを特徴とする請求項３に記載の検知装置。

[請求項5] さらに、

前記判定部は、前記第２のアカウント数が前記第１閾値を越えるアカウントグループが存在する場合に、前記第２のアカウント数が前記第１閾値を越えるアカウントグループに該当する前記第１の送信元アドレス以外の送信元アドレスが攻撃者のアドレスであると判定する

ことを特徴とする請求項４に記載の検知装置。

[請求項6] 前記判定部は、前記計算部により計算されたアカウント数にタイムスロット又は送信元アドレスに応じた各加重係数を乗算した値をもとに攻撃者のアドレスを判定する

ことを特徴とする請求項２に記載の検知装置。

[請求項7] ユーザ認証を行う認証装置及び検知装置を含む検知システムにおける検知方法であって、

前記検知装置が、

前記認証装置から取得した認証情報からアカウント及びアカウントの送信元アドレスを抽出し、アカウントのタイムスタンプ及び送信元アドレスに応じて、所定時間間隔のタイムスロット毎かつ送信元アドレス毎にアカウントをグループ化し、同一グループ内で同一アカウントの重複を除外したアカウントグループを抽出し、

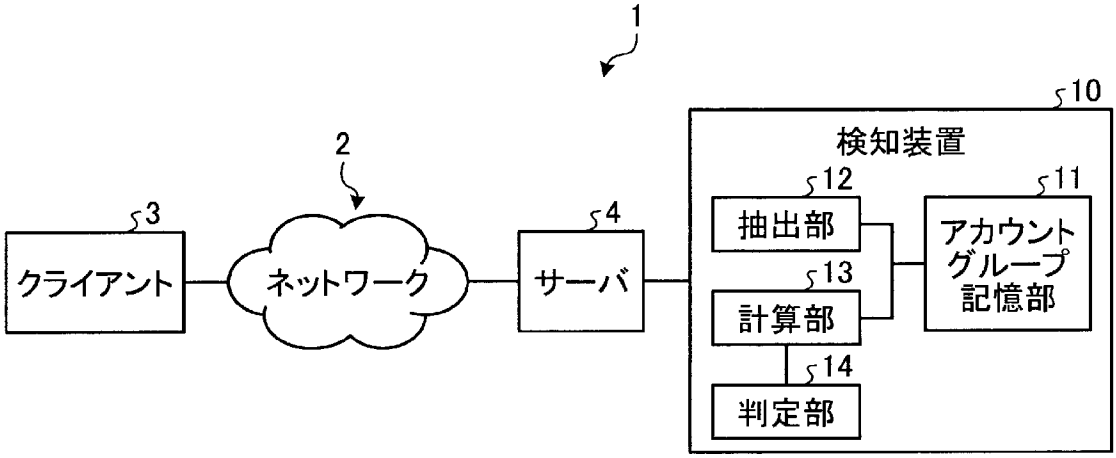
抽出した各アカウントグループ間で重複するアカウント数を計算し、

計算したアカウント数が第１閾値を越える同一送信元アドレスのアカウントグループの数が第２閾値を越える場合に、該同一送信元アドレスが攻撃者のアドレスであると判定する

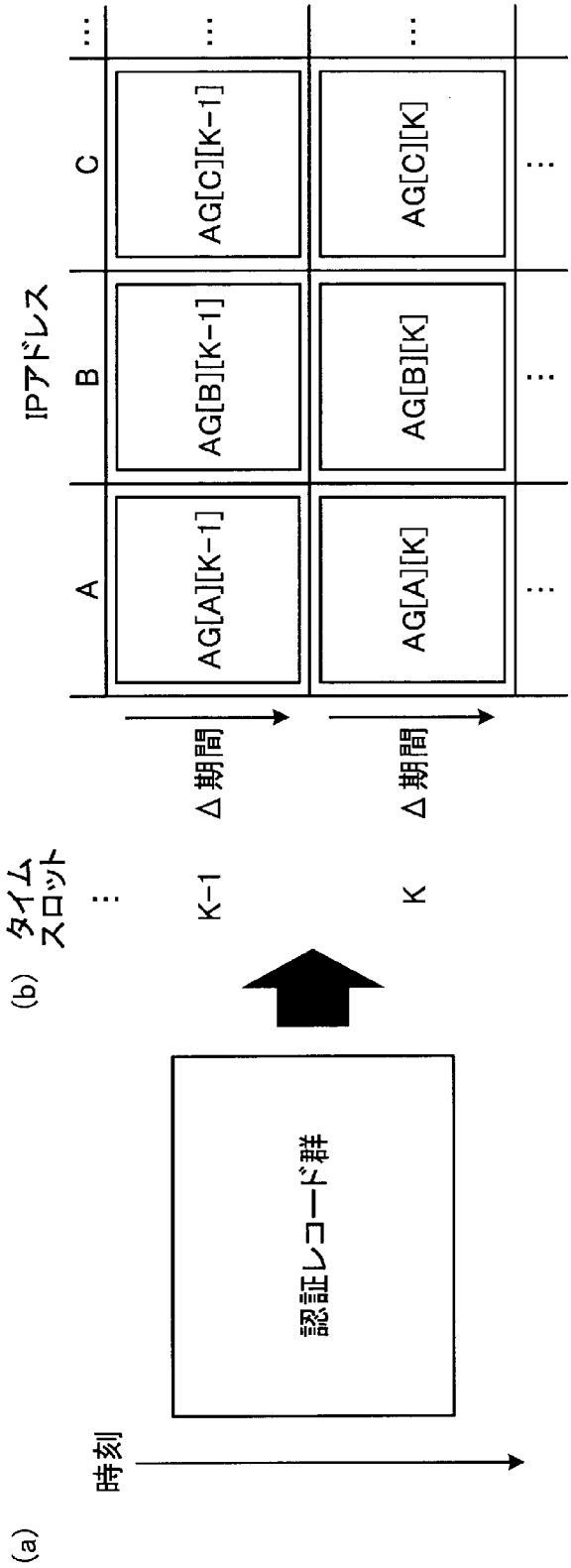
処理を含んだことを特徴とする検知方法。

[請求項8] 請求項２に記載の検知装置としてコンピュータを機能させる検知プログラム。

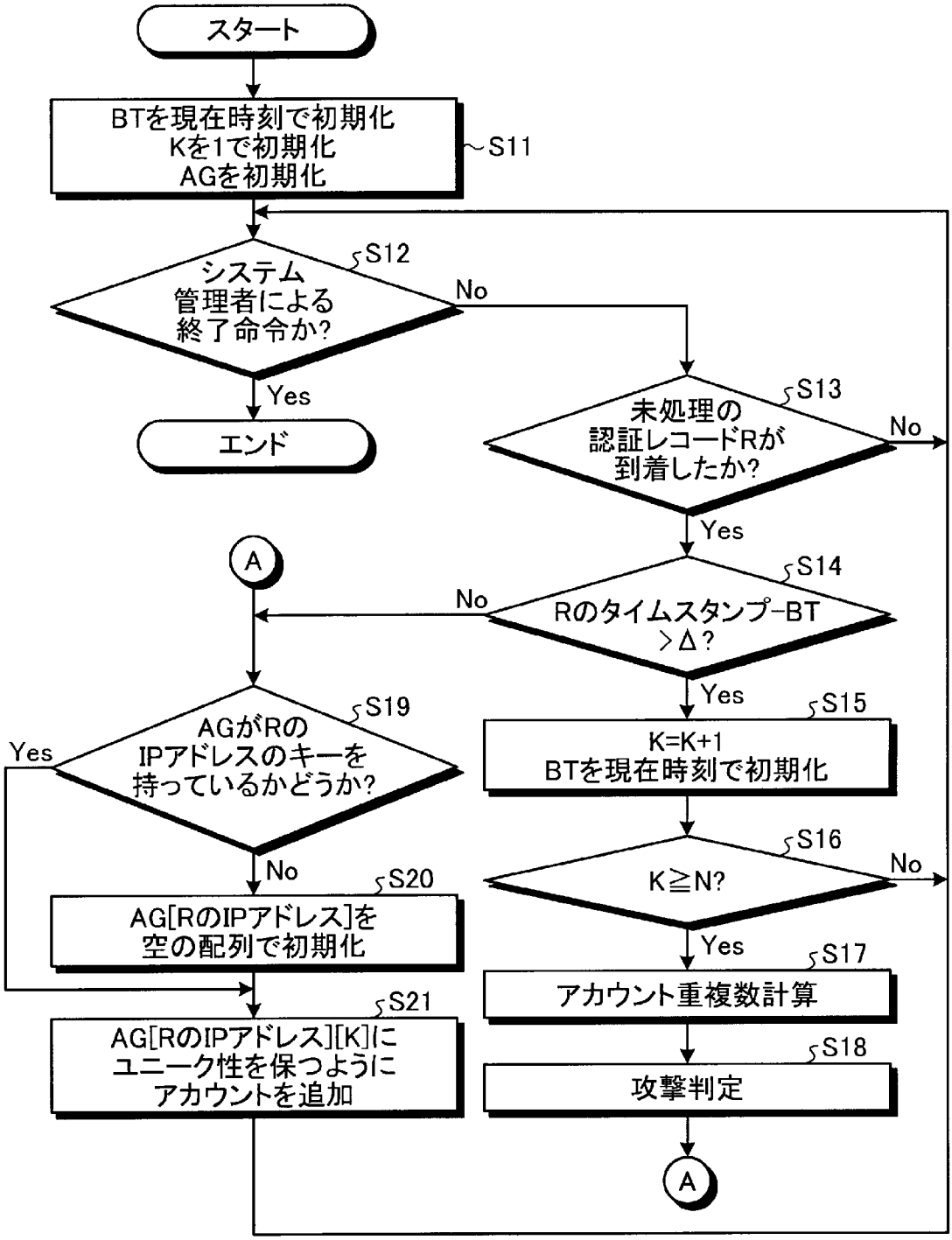
[図1]


1
10
検知装置
2
3
4
クライアント
ネットワーク
サーバ
12
抽出部
11
アカウント
グループ
記憶部
13
計算部
14
判定部

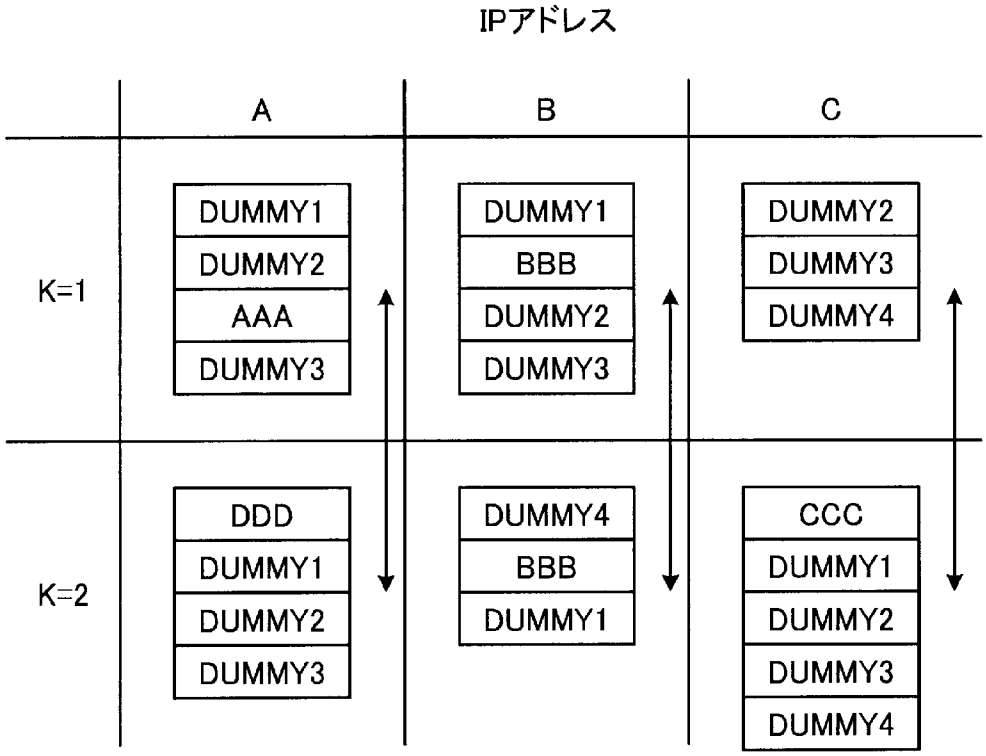
[図2]


(a)
時刻
認証レコード群
(b)
タイムスロット
IPアドレス
A
B
C
K-1
K
Δ期間
Δ期間
AG[A][K-1]
AG[B][K-1]
AG[C][K-1]
AG[A][K]
AG[B][K]
AG[C][K]

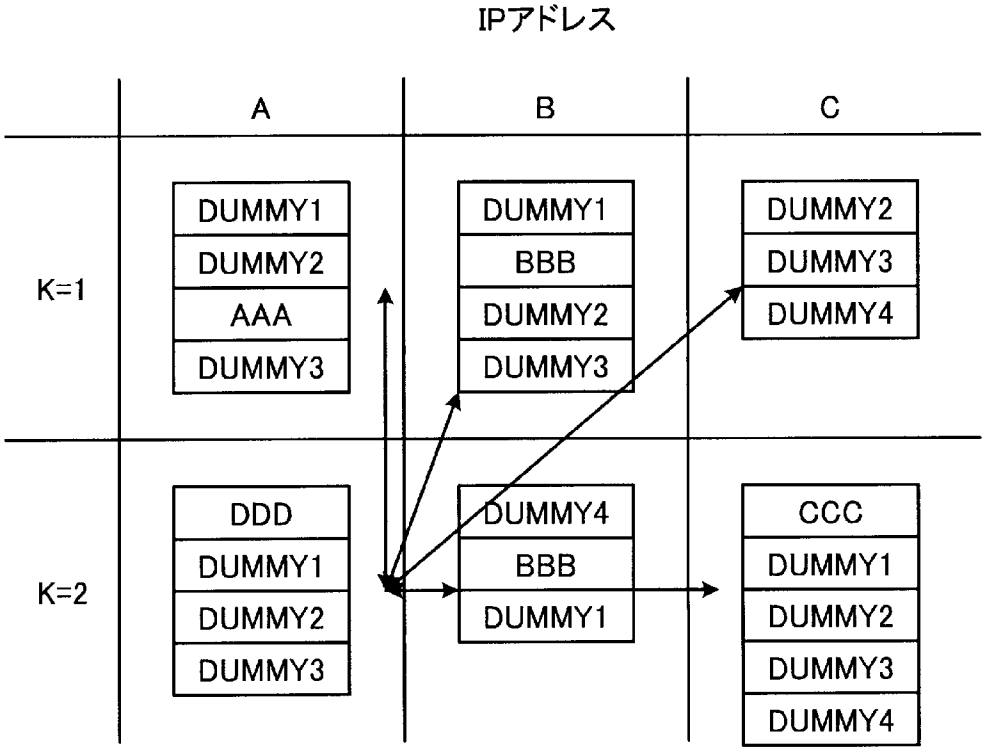
[図3]


スタート
BTを現在時刻で初期化
Kを1で初期化
AGを初期化
S11
システム
管理者による
終了命令か?
S12
No
Yes
エンド
未処理の
認証レコードRが
到着したか?
S13
No
Yes
A
Rのタイムスタンプ-BT
>Δ?
S14
No
Yes
K=K+1
BTを現在時刻で初期化
S15
K≧N?
S16
No
Yes
アカウント重複数計算
S17
攻撃判定
S18
A
AGがRの
IPアドレスのキーを
持っているかどうか?
S19
Yes
No
AG[RのIPアドレス]を
空の配列で初期化
S20
AG[RのIPアドレス][K]に
ユニーク性を保つように
アカウントを追加
S21

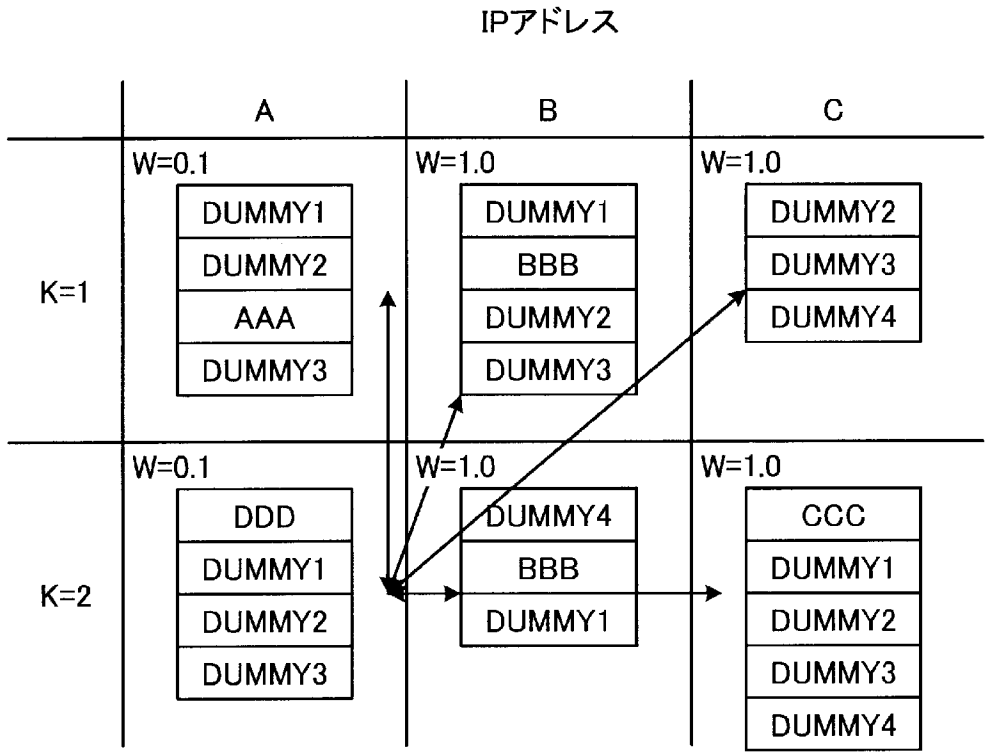
[図4]


IPアドレス
A
B
C
K=1
DUMMY1
DUMMY2
AAA
DUMMY3
DUMMY1
BBB
DUMMY2
DUMMY3
DUMMY2
DUMMY3
DUMMY4
K=2
DDD
DUMMY1
DUMMY2
DUMMY3
DUMMY4
BBB
DUMMY1
CCC
DUMMY1
DUMMY2
DUMMY3
DUMMY4

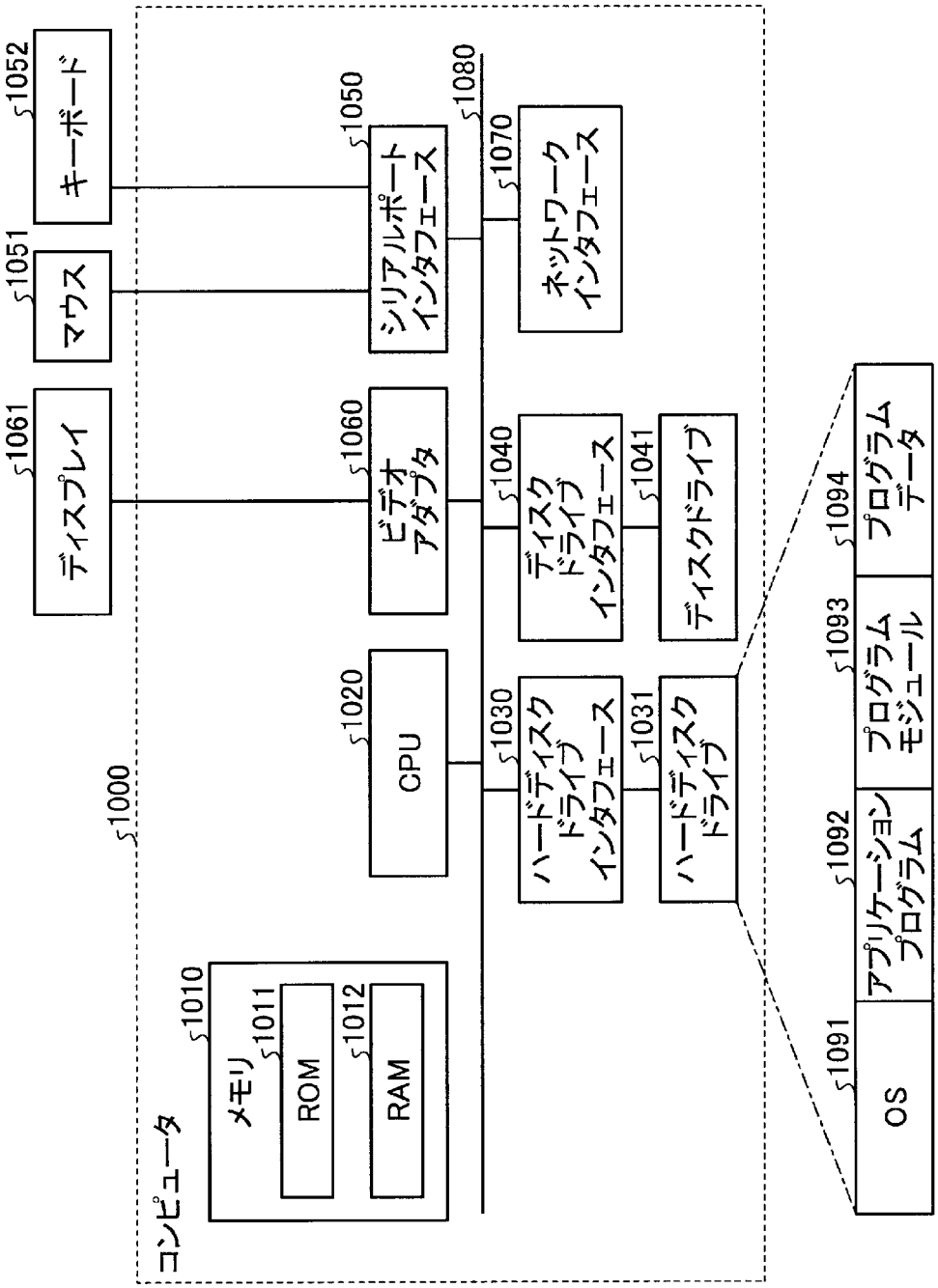
[図5]


IPアドレス
A
B
C
K=1
DUMMY1
DUMMY2
AAA
DUMMY3
DUMMY1
BBB
DUMMY2
DUMMY3
DUMMY2
DUMMY3
DUMMY4
K=2
DDD
DUMMY1
DUMMY2
DUMMY3
DUMMY4
BBB
DUMMY1
CCC
DUMMY1
DUMMY2
DUMMY3
DUMMY4

[図6]


IPアドレス
A
B
C
K=1
K=2
W=0.1
W=1.0
W=1.0
DUMMY1
DUMMY2
AAA
DUMMY3
DUMMY1
BBB
DUMMY2
DUMMY3
DUMMY2
DUMMY3
DUMMY4
W=0.1
W=1.0
W=1.0
DDD
DUMMY1
DUMMY2
DUMMY3
DUMMY4
BBB
DUMMY1
CCC
DUMMY1
DUMMY2
DUMMY3
DUMMY4

[図7]


1000
コンピュータ
1010
メモリ
1011
ROM
1012
RAM
1020
CPU
1030
ハードディスクドライブインタフェース
1031
ハードディスクドライブ
1040
ディスクドライブインタフェース
1041
ディスクドライブ
1050
シリアルポートインタフェース
1051
マウス
1052
キーボード
1060
ビデオアダプタ
1061
ディスプレイ
1070
ネットワークインタフェース
1080
1091
OS
1092
アプリケーションプログラム
1093
プログラムモジュール
1094
プログラムデータ

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2016/066642

A. CLASSIFICATION OF SUBJECT MATTER
G06F21/55(2013.01)i, *H04L12/26*(2006.01)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)
G06F21/55, H04L12/26

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)
JSTPlus/JMEDPlus/JST7580(JDreamIII), IEEE Xplore, Intrusion detection, account, timestamp, address

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 03/100619 A1 (Fujitsu Ltd.), 04 December 2003 (04.12.2003), page 4, line 13 to page 14, line 14	1-8
A	US 2005/0216955 A1 (MICROSOFT CORP.), 29 September 2005 (29.09.2005), paragraphs [0022] to [0061]	1-8
A	JP 2005-341217 A (Fujitsu Ltd.), 08 December 2005 (08.12.2005), paragraphs [0021] to [0093]	1-8
A	US 2007/0220605 A1 (CHIEN, Daniel), 20 September 2007 (20.09.2007), paragraphs [0019] to [0053]	1-8

[×] 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
22 August 2016 (22.08.16)	30 August 2016 (30.08.16)
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/JP2016/066642

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2011/0185419 A1 (BAE SYSTEMS INFORMATION AND ELECTRONIC SYSTEMS INTEGRATION), 28 July 2011 (28.07.2011), paragraphs [0075] to [0134]	1-8
A	JP 2011-150612 A (Fujitsu Ltd.), 04 August 2011 (04.08.2011), paragraphs [0019] to [0068]	1-8

WO 03/100619 A1	2003.12.04	US 2005/0086538 A1 2005.04.21 paragraphs [0020] to [0063]
US 2005/0216955 A1	2005.09.29	(Family: none)
JP 2005-341217 A	2005.12.08	US 2005/0289649 A1 2005.12.29 paragraphs [0039] to [0123]
US 2007/0220605 A1	2007.09.20	WO 2007/106902 A2 2007.09.20
US 2011/0185419 A1	2011.07.28	(Family: none)
JP 2011-150612 A	2011.08.04	(Family: none)

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１６／０６６６４２

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/55(2013.01)i, H04L12/26(2006.01)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.　G06F21/55, H04L12/26

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）

JSTPlus/JMEDPlus/JST7580 (JDreamIII), IEEE Xplore
Intrusion detection, account, timestamp, address

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	WO 03/100619 A1 (富士通株式会社) 2003.12.04, 4頁13行-14頁14行	1-8
A	US 2005/0216955 A1 (MICROSOFT CORPORATION) 2005.09.29, 段落[0022]-[0061]	1-8
A	JP 2005-341217 A (富士通株式会社) 2005.12.08, 段落[0021]-[0093]	1-8
A	US 2007/0220605 A1 (CHIEN, Daniel) 2007.09.20, 段落[0019]-[0053]	1-8

☑　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
２２．０８．２０１６	３０．０８．２０１６

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　９３６４
中里　裕正
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	US 2011/0185419 A1 (BAE SYSTEMS INFORMATION AND ELECTRONIC SYSTEMS INTEGRATION) 2011.07.28, 段落[0075]-[0134]	1-8
A	JP 2011-150612 A（富士通株式会社）2011.08.04, 段落[0019]-[0068]	1-8

WO 03/100619 A1	2003.12.04	US 2005/0086538 A1, 段落[0020]-[0063]	2005.04.21
US 2005/0216955 A1	2005.09.29	ファミリーなし	
JP 2005-341217 A	2005.12.08	US 2005/0289649 A1, 段落[0039]-[0123]	2005.12.29
US 2007/0220605 A1	2007.09.20	WO 2007/106902 A2	2007.09.20
US 2011/0185419 A1	2011.07.28	ファミリーなし	
JP 2011-150612 A	2011.08.04	ファミリーなし	