(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
2014 年 8 月 7 日(07.08.2014)

WIPO | PCT

(10) 国際公開番号
WO 2014/119669 A1

(51) 国際特許分類:
*H04L 12/70* (2013.01)

(21) 国際出願番号: PCT/JP2014/052134

(22) 国際出願日: 2014 年 1 月 30 日(30.01.2014)

(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 2013-015288 2013 年 1 月 30 日(30.01.2013) 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: 倉上 弘(KURAKAMI, 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).

(74) 代理人: 酒井 宏明, 外(SAKAI, Hiroaki et al.); 〒1006020 東京都千代田区霞が関三丁目２番５号 霞が関ビルディング 酒井国際特許事務所 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, LT, 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, 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

[続葉有]

(54) **Title**: LOG ANALYSIS DEVICE, INFORMATION PROCESSING METHOD AND PROGRAM

(54) 発明の名称 : ログ分析装置、情報処理方法及びプログラム

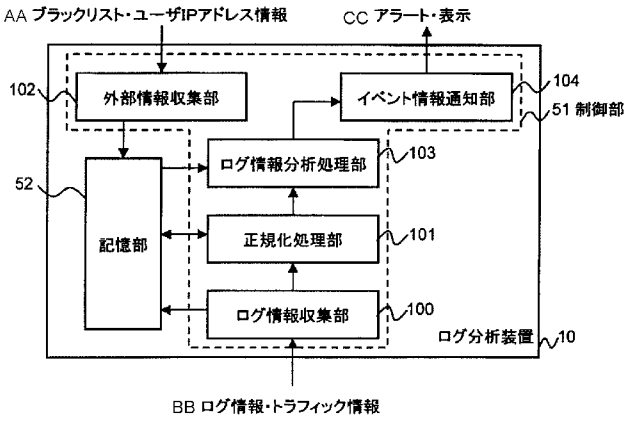



FIG. 2:

| | |
|---|---|
| 10 | Log analysis device |
| 51 | Control unit |
| 52 | Storage unit |
| 100 | Log information collection section |
| 101 | Normalization processing section |
| 102 | External information collection section |
| 103 | Log information analysis processing section |
| 104 | Event information notification section |
| AA | Blacklist/user IP address information |
| BB | Log information/traffic information |
| CC | Alert/display |

(57) **Abstract**: This log analysis device has: a log information collection section that collects log information and traffic information output from multiple communication devices that are included in a network; a normalization processing section that normalizes the log information and traffic information collected by the log information collection section; a log information analysis processing section that extracts related log information and traffic information from the normalized log information and traffic information and analyzes the extracted information in accordance with predetermined rules in order to determine whether or not an unauthorized access is present; and an event information notification section that outputs event information, including information about a degree of importance, that is based on the determination result of the log information analysis processing section.

(57) 要約: ネットワークに含まれる複数の通信機器から出力されるログ情報及びトラフィック情報を収集するログ情報収集部と、ログ情報収集部が収集したログ情報及びトラフィック情報を正規化する正規化処理部と、正規化されたログ情報及びトラフィック情報から関連するログ情報及びトラフィック情報を抽出して予め決められたルールにしたがって分析し、不正アクセスがあるか否かを判定するログ情報分析処理部と、ログ情報分析処理部が判定した結果に基づく、重要度を示す情報を含むイベント情報を出力するイベント情報通知部と、を有する。

WO 2014/119669 A1

(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 ： ログ分析装置、情報処理方法及びプログラム

## 技術分野

[0001] 本発明は、ログ分析装置、情報処理方法及びプログラム、特に、ネットワークセキュリティに関する攻撃を検出する技術に関する。

## 背景技術

[0002] ＩＰ（Internet Protocol）ネットワークにおいて、不正侵入を検出するため、ログ情報を用いた解析が行われている。特許文献１には、ネットワーク上の異常なアクセスをロギングする侵入検知装置が出力する大量のログに対して、イベントの属性であるイベント種別やアドレスなどの違いを考慮したイベント間の同時相関に基づいて複数のイベントをグループ化することで、監視や分析を容易にする方法が開示されている。

## 先行技術文献

## 特許文献

[0003] 特許文献1：特開２００５－０３８１１６号公報

## 発明の概要

## 発明が解決しようとする課題

[0004] しかしながら、侵入方法に基づいた複数のログ情報の関連付けや分析を行わないと、パケットに対する複数のログ情報のグループ化だけでは、不正侵入の検出は困難と考えられる。

[0005] 本発明の目的は、複数の通信機器からのログ情報及びトラフィック情報に基づいて不正アクセスの有無を総合的に判定可能にしたログ分析装置、情報処理方法、及びコンピュータに実行させるためのプログラムを提供することである。

[0006] 本発明の上記及びその他の目的と新規な特徴は、本明細書の記述及び添付図面によって明らかにする。

## 課題を解決するための手段

[0007] 上記目的を達成するための本発明のログ分析装置は、ネットワークのセキュリティ管理を行うログ分析装置であって、

前記ネットワークに含まれる複数の通信機器から出力されるログ情報及びトラフィック情報を収集するログ情報収集部と、

前記ログ情報収集部が収集したログ情報及びトラフィック情報を正規化する正規化処理部と、

正規化されたログ情報及びトラフィック情報から関連するログ情報及びトラフィック情報を抽出して予め決められたルールにしたがって分析し、不正アクセスがあるか否かを判定するログ情報分析処理部と、

前記ログ情報分析処理部が判定した結果に基づく、重要度を示す情報を含むイベント情報を出力するイベント情報通知部と、

を有する構成である。

[0008] また、本発明の情報処理方法は、ネットワークのセキュリティ管理を行うログ分析装置による情報処理方法であって、

前記ネットワークに含まれる複数の通信機器から出力されるログ情報及びトラフィック情報を収集し、

収集されたログ情報及びトラフィック情報を正規化し、

正規化されたログ情報及びトラフィック情報から関連するログ情報及びトラフィック情報を抽出して予め決められたルールにしたがって分析し、不正アクセスがあるか否かを判定し、

前記判定の結果に基づく、重要度を示す情報を含むイベント情報を出力するものである。

[0009] さらに、本発明のプログラムは、ネットワークのセキュリティ管理を行うコンピュータに、

前記ネットワークに含まれる複数の通信機器から出力されるログ情報及びトラフィック情報を収集する手順と、

収集されたログ情報及びトラフィック情報を正規化する手順と、

正規化されたログ情報及びトラフィック情報から関連するログ情報及びト

ラフィック情報を抽出して予め決められたルールにしたがって分析し、不正アクセスがあるか否かを判定する手順と、

前記判定の結果に基づく、重要度を示す情報を含むイベント情報を出力する手順を前記コンピュータに実行させるものである。

## 発明の効果

[0010] 本発明により、ネットワーク内の複数の通信機器から出力されるログ情報及びトラフィック情報に基づいて、不正アクセスの攻撃による通信コネクションが引き起こす問題の重要度を総合的に判定することができる。

## 図面の簡単な説明

[0011] [図1]図１は、本実施形態のログ分析装置がセキュリティ管理を行うネットワークの一構成例を示すブロック図である。

[図2]図２は、本実施形態のログ分析装置の一構成例を示すブロック図である。

[図3]図３は、ログフォーマットの一例を示す図である。

[図4]図４は、本実施形態のログ分析装置の動作手順を示すフローチャートである。

## 発明を実施するための形態

[0012] 本発明の実施形態について、図面を用いて説明する。なお、以下に説明する実施形態は、本発明の特許請求の範囲の解釈を限定するものではない。

[0013] 図１は本実施形態のログ分析装置がセキュリティ管理を行うネットワークの一構成例を示すブロック図である。

[0014] 図１に示すように、ユーザＩＰネットワーク３０は、ユーザ端末１１、Ｐｒｏｘｙサーバ１２、ＤＮＳ（Domain Name System）サーバ１３、メールサーバ１４、ファイルサーバ１５、Ｗｅｂサーバ１６、ＩＰＳ（Intrusion Prevention System）１７、ファイアーウォール１８、スイッチ１９及びルータ２０を有する。本実施形態では、説明を簡単にするためにユーザ端末１１が１台の場合で説明するが、複数のユーザ端末がユーザＩＰネットワーク３０内に設けられていてもよい。

[0015] Ｐｒｏｘｙサーバ１２、ＤＮＳ（Domain Name System）サーバ１３、メールサーバ１４、ファイルサーバ１５、Ｗｅｂサーバ１６及びユーザ端末１１がスイッチ１９と接続されている。スイッチ１９は、ＩＰＳ １７、ファイアーウォール１８及びルータ２０を介してインターネットと接続されている。ＩＰＳ １７及びファイアーウォール１８は、インターネット側からの不正アクセスやウイルスによる攻撃を防ぐ。ルータ２０に、ユーザＩＰネットワーク３０のセキュリティ管理を行うログ分析装置１０が接続されている。

[0016] 不正アクセスとして、例えば、ユーザ端末１１の場合、使用権限のない者がユーザ端末１１のセキュリティ上の弱点を攻撃してユーザ端末１１を不正に使用したり、ユーザ端末１１内のデータを改ざんしたり、ユーザ端末１１を使用不能にしたりすること等が考えられる。

[0017] なお、ルータ２０に接続されるインターネットは外部ネットワークの一例であり、外部ネットワークはインターネットに限らない。また、ユーザＩＰネットワーク３０は、セキュリティの管理対象となるネットワークの一例であり、ＩＰにしたがってデータを伝送可能なネットワークであればよく、例えば、ＬＡＮ（Local Area Network）である。ユーザＩＰネットワーク３０に含まれる情報通信機器は図１に示す構成に限らない。

[0018] 次に、本実施形態のログ分析装置の構成を説明する。図２は本実施形態のログ分析装置の一構成例を示すブロック図である。

[0019] ログ分析装置１０は制御部５１及び記憶部５２を有する構成である。制御部５１は、ログ情報収集部１００と、正規化処理部１０１と、ログ情報分析処理部１０３と、イベント情報通知部１０４と、外部情報収集部１０２とを有する。

[0020] 制御部５１には、プログラムにしたがって処理を実行するＣＰＵ（Central Processing Unit）（不図示）と、プログラムを記憶するメモリ（不図示）とが設けられている。ＣＰＵがプログラムにしたがって処理を実行することで、図２に示すログ情報収集部１００、正規化処理部１０１、ログ情報分

析処理部１０３、イベント情報通知部１０４及び外部情報収集部１０２がログ分析装置１０に仮想的に構成される。

[0021] ログ情報収集部１００は、ルータ２０、スイッチ１９、ファイアーウォール１８、ＩＰＳ　１７、Ｗｅｂサーバ１６、ファイルサーバ１５、メールサーバ１４、ＤＮＳサーバ１３及びＰｒｏｘｙサーバ１２からログ情報を受信すると、ログ情報から取得した機器識別情報毎にログ情報を記憶部５２に保存する。ログ情報収集部１００は、ユーザ端末１１からログ情報を受信すると、ログ情報から取得したユーザＩＤ（Identifier：識別子）及び機器識別情報に対応してログ情報を記憶部５２に保存する。ユーザＩＤはユーザ端末のユーザ毎に異なる識別子である。

[0022] また、ログ情報収集部１００は、ルータ２０及びスイッチ１９等からトラフィック情報を受信すると、トラフィック情報から取得した機器識別情報毎にトラフィック情報を記憶部５２に保存する。機器識別情報は、ログ情報又はトラフィック情報の送信元となる通信機器を識別するための情報であり、通信機器毎に異なる情報である。

[0023] 正規化処理部１０１は、記憶部５２に収集されたログ情報及びトラフィック情報に対して、これらの情報をログ情報分析処理部１０３が検索及び分析しやすいデータ形式に統一的に整理する正規化を行う。例えば、ルータ２０が出力するトラフィック情報のフォーマットと、スイッチ１９が出力するトラフィック情報のフォーマットが異なることがある。

[0024] 具体的には、正規化処理部１０１は、予め決められた共通カテゴリールールにしたがって、ログ情報及びトラフィック情報に含まれる項目（例えば、送信元ＩＰアドレス、宛先ＩＰアドレス、送信元ポート情報、宛先ポート情報、プロトコル情報、機器識別情報及びユーザＩＤ等）が全機器共通のフォーマットに合うようにログ情報及びトラフィック情報を更新する。

[0025] また、正規化処理部１０１は、同一のＩＰコネクションのログ情報又はトラフィック情報に、コネクション毎に異なる識別子であるコネクション識別子を付与して記憶部５２に保存する。ＩＰコネクションが同一か否かの判定

方法として、例えば、ログ情報又はトラフィック情報が、一定時間内のタイムスタンプで、ユーザＩＤ、送信元ＩＰアドレス、宛先ＩＰアドレス、送信元ポート情報、宛先ポート情報及びプロトコル情報が同一であれば、機器識別情報が異なっていても同一コネクションと判定する。コネクション識別情報の一例として、ハッシュ値を算出して用いることが可能である。ログフォーマットの一例を図３に示す。

[0026] 外部情報収集部１０２は、ログ情報分析処理部１０３が通信の向き（パケットの送信方向）の判定や攻撃の分析に利用するために、悪質なサイトを示すネットワークアドレスとしてＵＲＬ（Uniform Resource Locator）及びＩＰアドレスが列挙されたブラックリストと、ユーザＩＰアドレスとを含む外部情報を外部から取得して記憶部５２に保存する。ブラックリストは、インターネットに接続されたサーバ（不図示）に格納されていてもよく、ユーザＩＰネットワーク３０内のサーバに格納されていてもよい。ユーザＩＰアドレスは、ユーザ端末１１から取得することが可能である。

[0027] ログ情報分析処理部１０３は、予め決められた分析ルールに基づいて、正規化されたログ情報及びトラフィック情報を分析して、ユーザにとって脅威となるか否か重要度の指標となるスコアを複数求め、複数のスコアの合計と予め決められた基準値とを比較し、比較結果に基づいて不正アクセスがあるか否かを判定する。スコアの合計が基準値よりも大きい場合、ログ情報分析処理部１０３は、脅威となる不正アクセスがあると判定する。本実施形態では、２種類の分析ルールによるスコアの算出方法を説明する。

[0028] １つ目の分析ルールは、一定時間の時系列のログ情報及びトラフィック情報から総合的に判定してスコアを付与するものである。

[0029] ログ情報分析処理部１０３は、タイムスタンプの情報から一定時間の時系列のログ情報及びトラフィック情報を抽出して参照し、ユーザＩＰアドレスが送信元ＩＰアドレス及び宛先ＩＰアドレスの項目のうち、いずれの項目に記述されているかにより、通信の向きを判別する。なお、ログ情報及びトラフィック情報に通信の向きの情報が含まれていてもよく、この場合、ログ情

報分析処理部１０３は、その情報を利用してもよい。

[0030] 続いて、ログ情報分析処理部１０３は、抽出したログ情報及びトラフィック情報に対して分析ルールに基づいて、指定された特徴を持つイベントである指定イベントがあるか分析する。分析の結果、ログ情報分析処理部１０３は、指定イベントを検出すると、指定イベントが指定時間内に発生した回数（発生頻度）に対応してスコアを付け、指定イベントの発生間隔に基づいてスコアを付け、複数の指定イベントが発生した順序及び指定イベント毎の発生間隔に基づいてスコアを付け、指定イベントが指定時間内に発生しない時間に基づいてスコアを付け、複数の指定された項目毎に指定時間で足し合わせた量を比較した結果に基づいてスコアを付ける。そして、ログ情報分析処理部１０３は、これらのスコアの合計を求める。

[0031] 上記のスコア付けは、種々の不正アクセスによって生じる現象を漏れなく検出するために規定されたものであるが、スコア付けは上記の５つの現象に限らない。

[0032] 上記のスコア付けでは、指定イベントの発生頻度が大きいほどスコアが大きくなり、指定イベントの発生間隔が小さいほどスコアが大きくなる。また、複数の指定イベントの発生順序及び指定イベント毎の発生間隔が予め決められた発生順序と発生間隔に近いほど、スコアが大きくなる。指定時間内で指定イベントの発生しない時間が短いほど、スコアが大きくなる。

[0033] 複数の指定された項目毎に指定時間で足し合わせた量を比較した結果に基づくスコアの一例を、図３を参照して説明する。ここでは、図３に示すログ情報がユーザ端末１１から出力されたものとする。複数の指定された項目を送信バイト数及び受信バイト数とすると、指定時間内の送信バイト数を足し合わせた量である送信バイト量と指定時間内の受信バイト数を足し合わせた量である受信バイト量とを比較する。送信バイト量が受信バイト量よりも極端に大きい場合、ユーザ端末１１から個人情報が大量に送出される現象が起きていると考えられ、スコアを大きくすることで、このような不正アクセスを検出可能となる。

[0034] ２つ目の分析ルールは、同一コネクションの複数の通信処理を特定し、特定した複数の通信処理に基づいて総合的に判定してスコアを付与するものである。

[0035] ログ情報分析処理部１０３は、タイムスタンプの情報を参照して一定時間のログ情報及びトラフィック情報を抽出し、抽出したログ情報及びトラフィック情報に付与されたコネクション識別情報を参照する。そして、ログ情報分析処理部１０３は、参照したコネクション識別情報が一致するログ情報及びトラフィック情報を同一コネクションに基づくイベントによるものと認識し、認識したログ情報及びトラフィック情報を分析ルールに基づいて分析することで、通信機器毎に指定イベントの検出の有無に応じたスコアを付与し、複数の通信機器のスコアの合計を求める。

[0036] 具体的には、ログ情報分析処理部１０３は、同一コネクションと認識したログ情報及びトラフィック情報に含まれる機器識別情報を参照して、機器識別情報毎にログ情報又はトラフィック情報を分析し、分析の結果、指定イベントを検出すると、その機器識別情報に対応する通信機器にスコアを付与し、指定イベントを検出しないと、スコアを付与しない。

[0037] 分析対象となるログ情報及びトラフィック情報の関連づけは、１つ目の分析ルールでは一定時間の時系列によって行われ、２つ目の分析ルールでは同一のコネクション識別情報によって行われる。

[0038] また、上記２種類の分析ルールによるスコア付けの他に、ログ情報分析処理部１０３は、ログ情報及びトラフィック情報にブラックリストのＵＲＬ又はＩＰアドレスが含まれているか否かを判定し、ブラックリストのＵＲＬ又はＩＰアドレスがログ情報又はトラフィック情報に含まれている場合、スコアに所定の値を加算する。

[0039] イベント情報通知部１０４は、ログ情報分析処理部１０３の判定結果に基づいて、不正アクセスに関する重要度を示す情報としてスコアの合計の情報を含むイベント情報を出力する。また、ログ情報分析処理部１０３が不正アクセスを検出したと判定すると、イベント情報通知部１０４は、不正アクセ

スに関して予め設定された脅威度以上の危険性があることをセキュリティ管理者に通知するために、同一コネクションに基づくイベントと判定された、複数の通信機器のログ情報及びトラフィック情報を関連情報としてイベント情報に紐付けして出力する。

[0040] セキュリティ管理者がログ分析装置１０を操作している場合、イベント情報通知部１０４は、セキュリティ管理者に警告するために、ログ分析装置１０に接続された表示装置（不図示）にイベント情報を表示させる。

[0041] セキュリティ管理者は、表示装置に出力されるイベント情報を参照することで、イベント情報に含まれるスコア合計に基づいて不正アクセスの可能性がある否か、その重要性を判定することが可能となる。また、関連情報がイベント情報に添付されている場合、セキュリティ管理者は、脅威となる不正アクセスが検出されたことを認識するとともに、関連情報を詳細に分析することが可能となる。

[0042] セキュリティ管理者が直接にログ分析装置１０を操作していなくても、例えば、セキュリティ管理者が操作可能な情報端末（不図示）がインターネットに接続され、その情報端末がログ分析装置１０と通信可能になっていればよい。この場合、イベント情報通知部１０４は、イベント情報をルータ２０及びインターネットを介してその情報端末に送信すればよい。

[0043] なお、本実施形態では、ＣＰＵがプログラムを実行することで、ログ情報収集部１００、正規化処理部１０１、ログ情報分析処理部１０３、イベント情報通知部１０４及び外部情報収集部１０２が仮想的に構成される場合で説明したが、これらの構成の一部又は全部が各機能に対応した専用回路で構成されてもよい。

[0044] 次に、本実施形態のログ分析装置の動作を、図１、図２及び図４を参照して説明する。図４は本実施形態のログ分析装置の動作手順を示すフローチャートである。

[0045] ここでは、ログ分析装置１０に表示装置（不図示）が接続され、セキュリティ管理者がログ分析装置１０を操作可能な状態にあるとする。

[0046] 図１に示したブロック図において、ファイアーウォール１８及びＩＰＳ１７は、通過するＩＰパケットを監視し、ＩＰパケットから取得したログ情報をログ分析装置１０にルータ２０を介して送信する。ルータ２０及びスイッチ１９は、転送するＩＰパケットの情報を、Ｎｅｔｆｌｏｗ、ｓＦｌｏｗ（登録商標）又はＩＰパケットのトラフィック情報としてログ分析装置１０に送信する。Ｐｒｏｘｙサーバ１２、ＤＮＳサーバ１３、メールサーバ１４、ファイルサーバ１５、Ｗｅｂサーバ１６及びユーザ端末１１は、アクセスに関するログ情報をログ分析装置１０に送信する。ログ分析装置１０のログ情報収集部１００は、ユーザＩＰネットワーク３０内の通信機器からログ情報及びトラフィック情報を収集すると、これらの情報を記憶部５２に格納する（ステップ２０１）。

[0047] 今、ユーザ端末１１は、インターネットを介して、攻撃者の情報端末から攻撃を受けてウイルスに感染し、攻撃者に操られる「Ｂｏｔ」の状態になっているとする。攻撃者からの指示を含むＩＰコネクションは、インターネット側からルータ２０、ファイアーウォール１８、ＩＰＳ　１７、スイッチ１９及びＰｒｏｘｙサーバ１２を経由して、ユーザ端末１１の順に転送されるものとする。このとき、このＩＰコネクションに関して、ルータ２０及びスイッチ１９からトラフィック情報がログ分析装置１０に送信され、ファイアーウォール１８、ＩＰＳ　１７、Ｐｒｏｘｙサーバ１２及びユーザ端末１１からログ情報がログ分析装置１０に送信される。

[0048] 本実施形態では、攻撃者からの指示を含むＩＰコネクションに関するトラフィック情報及びログ情報に、ユーザ端末１１のユーザＩＤと、このＩＰコネクションのコネクション識別情報とが正規化処理部１０１よって付加される（ステップ２０２）。続いて、ログ情報分析処理部１０３は、ＩＰＳ　１７で特定の攻撃の可能性がある特徴に適合するＩＰコネクションに対して、ファイアーウォール１８及びＰｒｏｘｙサーバ１２のログ情報を抽出し、分析ルールに基づいて、指定イベントの特徴を持つＩＰコネクションに該当するか否かを分析する。そのＩＰコネクションに該当すると判定すると、ログ

情報分析処理部１０３は、スコアを付け、そのＩＰコネクションに該当しないと判定すると、スコアを付けない。

[0049] また、ログ情報分析処理部１０３は、特定の攻撃の可能性がある特徴に適合するＩＰコネクションに関して、ルータ２０及びスイッチ１９から出力されたトラフィック情報に対して、分析ルールに基づいて、Ｕｓｅｒ－Ａｇｅｎｔ等ＨＴＴＰ（HyperText Transfer Protocol）ヘッダ異常などの異常を分析し、異常と判定すると、スコア付けを行う。

[0050] そして、ログ情報分析処理部１０３は、ＩＰＳ １７のログ情報に基づくスコア、ファイアーウォール１８のログ情報に基づくスコア、Ｐｒｏｘｙサーバ１２のログ情報に基づくスコア、並びにルータ２０及びスイッチ１９から出力されたトラフィック情報に対するスコアの合計を求める。スコアの合計は、ＩＰコネクションが特定の攻撃の可能性が高いと判定される通信機器の数が多いほど、大きくなる。

[0051] このようにして、攻撃の可能性があるコネクションに関する脅威度について、複数の通信機器から出力されるログ情報及びトラフィック情報から判定されたスコアを組み合わせることにより、不正アクセスの可能性が総合的に判断される。

[0052] ここで、ステップ２０３において、別の分析ルールの場合を説明する。

[0053] ログ情報分析処理部１０３は、２４時間や一週間等の一定時間における時系列のログ情報及びトラフィック情報を分析することで、指定イベントが指定時間内に発生した回数に対応するスコア付け、指定イベントの発生間隔に基づくスコア付け、複数の指定イベントが発生した順序及び指定イベント毎の発生間隔に基づくスコア付け、指定イベントが指定時間内に発生しない時間に基づくスコア付け、複数の指定された項目毎の指定時間で足し合わせた量を比較した結果に基づくスコア付けを行う。続いて、ログ情報分析処理部１０３は、これらのスコアの合計を求める。

[0054] 単独のログ情報から不正アクセスを検出することは困難だが、このようにして、複数の攻撃コネクションの情報を一定時間内の時系列のログ情報及び

トラフィック情報から抽出することで、不正アクセスを検出することが可能となる。

[0055] なお、上記２種類の分析ルールによる方法を別々に説明したが、ログ情報分析処理部１０３がこれら２種類の分析ルールのそれぞれに基づいてスコアを求め、大きい方をステップ２０３の処理結果としてもよい。

[0056] ステップ２０３の処理の後、ログ情報分析処理部１０３は、ログ情報及びトラフィック情報にブラックリストのＵＲＬ又はＩＰアドレスが含まれているか否かを判定する（ステップ２０４）。ブラックリストのＵＲＬ又はＩＰアドレスがログ情報又はトラフィック情報に含まれている場合、ログ情報分析処理部１０３は、スコアに所定の値を加算し（ステップ２０５）、ブラックリストのＵＲＬ及びＩＰアドレスがログ情報及びトラフィック情報に含まれていない場合、ステップ２０６に進む。

[0057] ログ情報分析処理部１０３は、スコアに基づいて重要度を判定するために、スコアの合計と予め決められた基準値とを比較し、スコアの合計が基準値もより大きいか否かを判定する（ステップ２０６）。スコアの合計が基準値以下の場合、ログ情報分析処理部１０３は何もせずに処理を終了する。ステップ２０６の判定の結果、スコアの合計値が基準値以下の場合、イベント情報通知部１０４は、表示装置（不図示）にイベント情報を出力する（ステップ２０７）。ステップ２０６の判定の結果、スコアの合計値が基準値よりも大きい場合、イベント情報通知部１０４は、表示装置（不図示）にイベント情報と共に関連情報を出力する（ステップ２０８）。ログ分析装置１０は図４に示す手順を繰り返す。

[0058] 例えば、ステップ２０３の処理で一定時間における時系列のログ情報及びトラフィック情報を分析する場合、ログ情報分析処理部１０３は、一週間のログ情報及びトラフィック情報に含まれる、送信元ＩＰアドレスと宛先ＩＰアドレス間の送受信量の差分に対応するスコア付けを行い、情報漏えいの攻撃コネクション候補を抽出する。送信元ＩＰアドレスがユーザＩＰアドレスのときに送信量が受信量に比べて極端に大きいと、ユーザ端末１１から外部

に情報漏えいが起きていると考えられるからである。この場合、スコアの値が大きくなる。抽出された攻撃コネクション候補に対して、同じ一定時間の複数の通信機器のログ情報及びトラフィック情報を同様に分析することにより、脅威度を示す判定結果を出力することが可能となる。

[0059] 本実施形態によれば、ネットワーク内の複数の通信機器から出力されるログ情報及びトラフィック情報から関連するログ情報及びトラフィック情報を抽出し、予め決められた分析ルールにしたがって複数のログ情報及びトラフィック情報を分析することで、不正アクセスの攻撃による通信コネクションが引き起こす問題の重要度を、セキュリティ管理者の判断に頼らず、総合的に自動で判定することが可能になる。

[0060] なお、本発明の情報処理方法を実行するための手順を記述したプログラムをコンピュータにインストールし、コンピュータに本発明の情報処理方法を実行させてもよい。

## 符号の説明

[0061]
１０　ログ分析装置
１１　ユーザ端末
１２　Ｐｒｏｘｙサーバ
１３　ＤＮＳサーバ
１４　メールサーバ
１５　ファイルサーバ
１６　Ｗｅｂサーバ
１７　ＩＰＳ
１８　ファイアーウォール
１９　スイッチ
２０　ルータ
１００　ログ情報収集部
１０１　正規化処理部
１０２　外部情報収集部

１０３　　ログ情報分析処理部

１０４　　イベント情報通知部

# 請求の範囲

[請求項1] ネットワークのセキュリティ管理を行うログ分析装置であって、

前記ネットワークに含まれる複数の通信機器から出力されるログ情報及びトラフィック情報を収集するログ情報収集部と、

前記ログ情報収集部が収集したログ情報及びトラフィック情報を正規化する正規化処理部と、

正規化されたログ情報及びトラフィック情報から関連するログ情報及びトラフィック情報を抽出して予め決められたルールにしたがって分析し、不正アクセスがあるか否かを判定するログ情報分析処理部と、

前記ログ情報分析処理部が判定した結果に基づく、重要度を示す情報を含むイベント情報を出力するイベント情報通知部と、

を有するログ分析装置。

[請求項2] 請求項１に記載のログ分析装置において、

前記正規化処理部は、

収集された前記ログ情報及びトラフィック情報を予め決められた共通カテゴリールールに従って正規化し、正規化したログ情報及びトラフィック情報に含まれる複数の項目のうち、所定の項目が共通するログ情報及びトラフィック情報を同一のコネクションと特定し、コネクション毎に異なる識別子であるコネクション識別情報を該ログ情報及びトラフィック情報に付与する、ログ分析装置。

[請求項3] 請求項２に記載のログ分析装置において、

前記ログ情報分析処理部は、

前記正規化されたログ情報及びトラフィック情報から一定時間内に収集されたログ情報及びトラフィック情報を抽出し、抽出したログ情報及びトラフィック情報に付与された前記コネクション識別情報を参照し、該コネクション識別情報が一致するログ情報及びトラフィック情報を同一コネクションに基づくイベントによるものと認識し、認識

したログ情報及びトラフィック情報を前記ルールに基づいて分析することで、指定された特徴を持つイベントである指定イベントの検出の有無に応じたスコアを前記通信機器毎に付与し、付与したスコアの合計を求める、ログ分析装置。

[請求項4] 請求項１に記載のログ分析装置において、

前記ログ情報分析処理部は、

前記正規化されたログ情報及びトラフィック情報から一定時間の時系列のログ情報及びトラフィック情報を抽出し、抽出したログ情報及びトラフィック情報を前記ルールに基づいて分析し、指定された特徴を持つイベントである指定イベントを検出すると、少なくとも、該指定イベントが指定時間内に発生した回数に対応するスコア、該指定イベントの発生間隔に基づくスコア、複数の該指定イベントが発生した順序及び指定イベント毎の発生間隔に基づくスコア、該指定イベントが指定時間内に発生しない時間に基づくスコア、及び複数の指定された項目毎に指定時間で足し合わせた量を比較した結果に基づくスコアの合計を求める、ログ分析装置。

[請求項5] 請求項３又は４に記載のログ分析装置において、

悪質なサイトを示すネットワークアドレスが列挙されたブラックリストを外部から取得する外部情報収集部をさらに有し、

前記ログ情報分析処理部は、

前記ログ情報又はトラフィック情報に含まれるネットワークアドレスが前記ブラックリストに含まれていると、前記スコアの合計に所定の値を加算して前記スコアの合計を更新する、ログ分析装置。

[請求項6] 請求項４に記載のログ分析装置において、

前記ログ情報分析処理部は、

前記スコアの合計と予め決められた基準値とを比較し、該スコアの合計が該基準値よりも大きいと不正アクセスがあると判定し、

前記イベント情報通知部は、

前記重要度を示す情報として前記スコアの合計の情報を含む前記イベント情報を出力し、前記ログ情報分析処理部により不正アクセスがあると判定された場合、同一のイベントに基づくログ情報及びトラフィック情報を関連情報として前記イベント情報と共に出力する、ログ分析装置。

[請求項7] ネットワークのセキュリティ管理を行うログ分析装置による情報処理方法であって、

前記ネットワークに含まれる複数の通信機器から出力されるログ情報及びトラフィック情報を収集し、

収集されたログ情報及びトラフィック情報を正規化し、

正規化されたログ情報及びトラフィック情報から関連するログ情報及びトラフィック情報を抽出して予め決められたルールにしたがって分析し、不正アクセスがあるか否かを判定し、

前記判定の結果に基づく、重要度を示す情報を含むイベント情報を出力する、情報処理方法。

[請求項8] ネットワークのセキュリティ管理を行うコンピュータに、

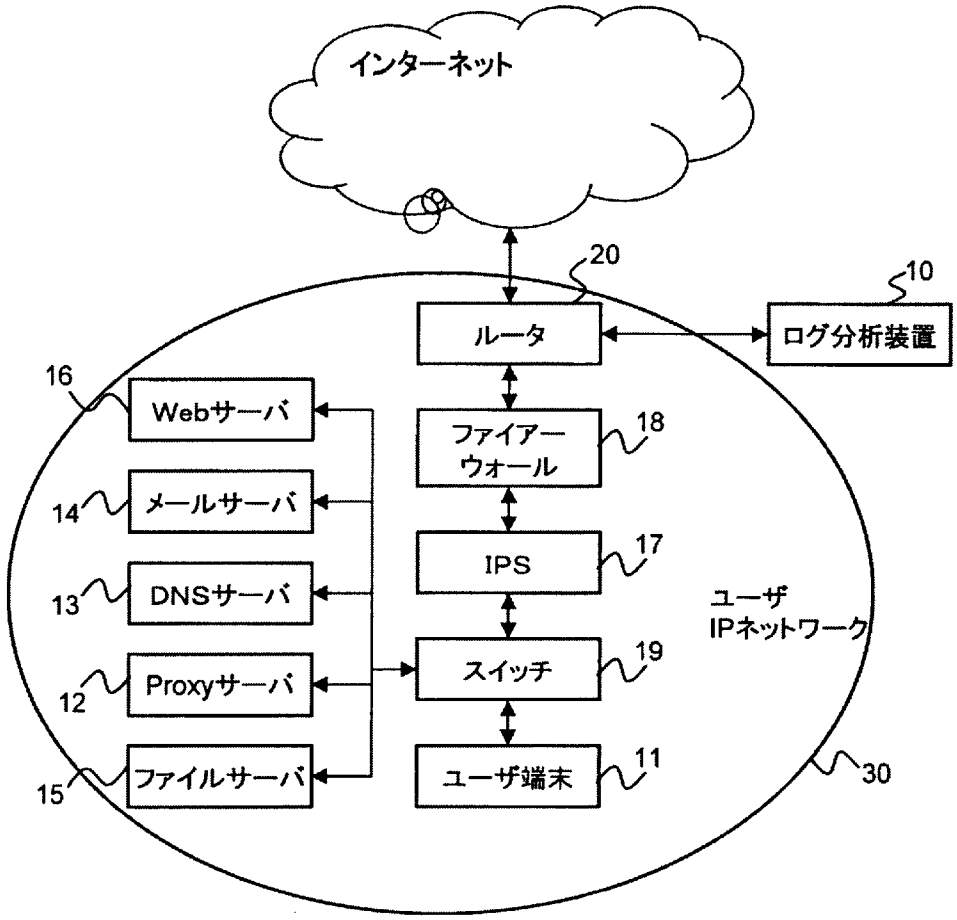
前記ネットワークに含まれる複数の通信機器から出力されるログ情報及びトラフィック情報を収集する手順と、

収集されたログ情報及びトラフィック情報を正規化する手順と、

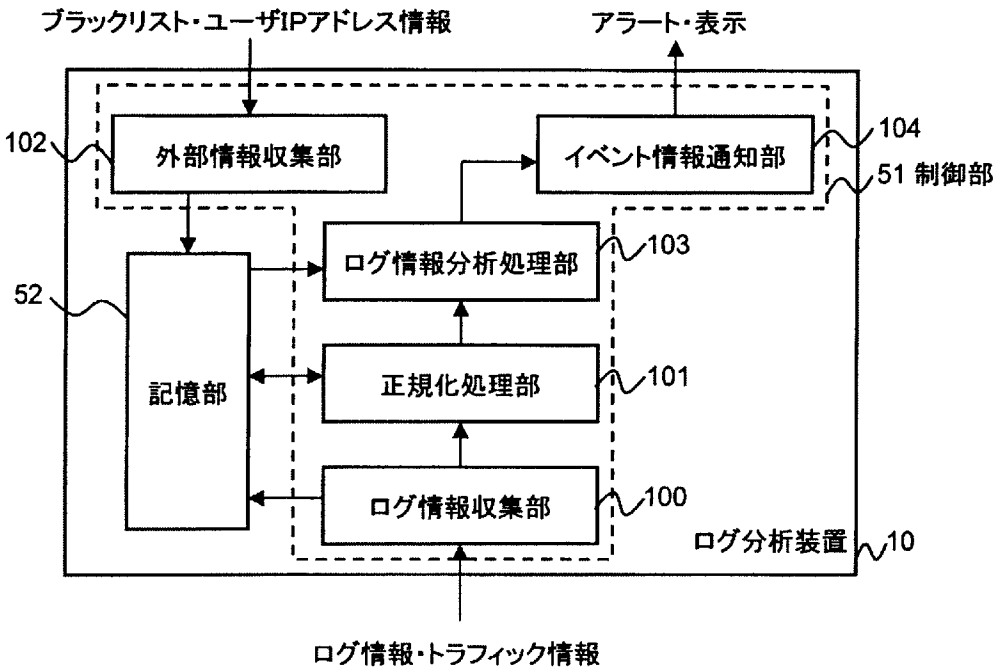
正規化されたログ情報及びトラフィック情報から関連するログ情報及びトラフィック情報を抽出して予め決められたルールにしたがって分析し、不正アクセスがあるか否かを判定する手順と、

前記判定の結果に基づく、重要度を示す情報を含むイベント情報を出力する手順を前記コンピュータに実行させるためのプログラム。

[図1]


インターネット
20
10
ルータ
ログ分析装置
16
Webサーバ
ファイアー
ウォール
18
14
メールサーバ
IPS
17
13
DNSサーバ
ユーザ
IPネットワーク
12
Proxyサーバ
スイッチ
19
15
ファイルサーバ
ユーザ端末
11
30

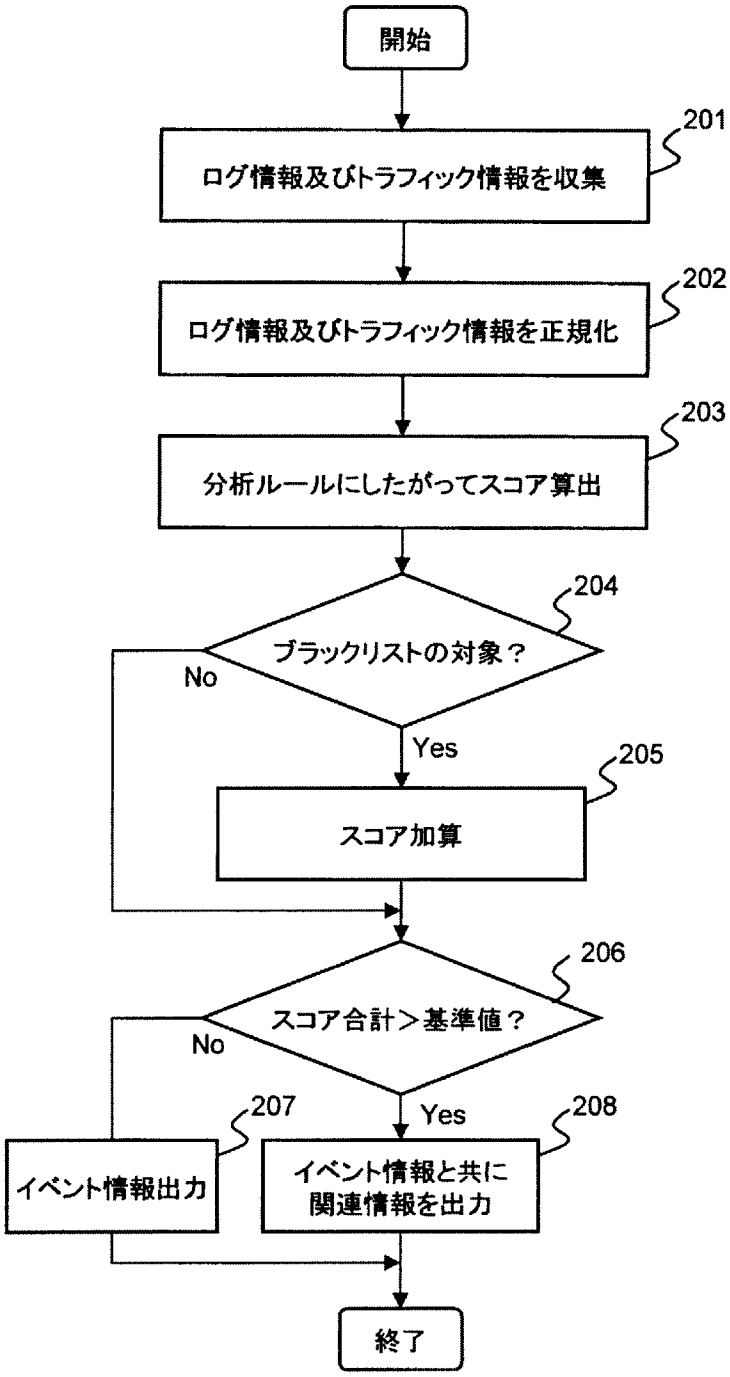
[図2]




[図3]

| No. | 項目 |
|---|---|
| 1 | タイムスタンプ |
| 2 | 送信元IPアドレス |
| 3 | 宛先IPアドレス |
| 4 | 送信元ポート番号 |
| 5 | 宛先ポート番号 |
| 6 | プロトコル |
| 7 | 宛先URL |
| 8 | HTTPメソッド名 |
| 9 | User－Agent名 |
| 10 | 送信バイト数 |
| 11 | 受信バイト数 |
| | : |
| n-1 | 機器識別情報 |
| n | コネクション識別情報 |

[図4]


開始
ログ情報及びトラフィック情報を収集
201
ログ情報及びトラフィック情報を正規化
202
分析ルールにしたがってスコア算出
203
ブラックリストの対象？
204
No
Yes
スコア加算
205
スコア合計＞基準値？
206
No
Yes
イベント情報出力
207
イベント情報と共に
関連情報を出力
208
終了

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2014/052134

A. CLASSIFICATION OF SUBJECT MATTER
*H04L12/70*(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)
H04L12/70

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 | 1996-2014 |
| Kokai Jitsuyo Shinan Koho | 1971-2014 | Toroku Jitsuyo Shinan Koho | 1994-2014 |

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. |
|---|---|---|
| Y<br>A | Masaru SEKIHARA, Kizon System no Sotenken to Ippo Susunda Tsukaikata Firewall Saiteki Katsuyo no Point Dai 3 Bu Firewall Ippo Susunda Katsuyo-ho [Log Kanri, Jocho Kosei, Un'yo Kanshi Service] Part 1 Log o Sekkyokuteki ni Kanri suru, N+I NETWORK, 01 September 2003 (01.09.2003), vol.3, no.8, pages 063 to 067, particularly, pages 063 to 064, 'Log Kanri no Yottsu no Point' | 1,2,7,8<br>3-6 |
| Y<br>A | JP 2005-128609 A (Yasukawa Information Systems Corp.),<br>19 May 2005 (19.05.2005),<br>claim 1<br>(Family: none) | 1,2,7,8<br>3-6 |

☒ 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 |
|---|---|
| 21 April, 2014 (21.04.14) | 28 April, 2014 (28.04.14) |
| Name and mailing address of the ISA/<br>Japanese Patent Office<br><br>Facsimile No. | Authorized officer<br><br>Telephone No. |

**INTERNATIONAL SEARCH REPORT**

International application No.
PCT/JP2014/052134

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y<br>A | JP 2006-246010 A (NTT Docomo Inc.),<br>14 September 2006 (14.09.2006),<br>paragraphs [0016] to [0017]<br>(Family: none) | 1,2,7,8<br>3-6 |
| Y<br>A | JP 2004-30286 A (NTT Data Corp.),<br>29 January 2004 (29.01.2004),<br>claim 1<br>(Family: none) | 1,2,7,8<br>3-6 |
| Y<br>A | JP 2002-318734 A (Kabushiki Kaisha Teamgia),<br>31 October 2002 (31.10.2002),<br>paragraphs [0007] to [0020]<br>& WO 2002/088976 A1 | 2<br>3-6 |

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１４／０５２１３４

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L12/70(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.　H04L12/70

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 | １９７１－２０１４年 |
| 日本国実用新案登録公報 | １９９６－２０１４年 |
| 日本国登録実用新案公報 | １９９４－２０１４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 |
|---|---|---|
| Y<br>A | 関原　優，既存システムの総点検と一歩進んだ使い方　ファイアウォール最適活用のポイント　第３部　ファイアウォール一歩進んだ活用法【ログ管理、冗長構成、運用監視サービス】　Ｐａｒｔ１　ログを積極的に管理する，Ｎ＋Ｉ　ＮＥＴＷＯＲＫ，2003.09.01，第３巻，第８号，p.063～067，<br>特に，０６３ページ～０６４ページ「ログ管理の４つのポイント」 | 1,2,7,8<br>3-6 |
| Y<br>A | JP 2005-128609 A（安川情報システム株式会社）2005.05.19，<br>請求項１（ファミリーなし） | 1,2,7,8<br>3-6 |

☑　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 |
|---|---|
| ２１．０４．２０１４ | ２８．０４．２０１４ |


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）　５Ｘ　９１９９
衣鳩　文彦
電話番号　０３－３５８１－１１０１　内線　３５９６

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 |
|---|---|---|
| Y<br>A | JP 2006-246010 A (株式会社エヌ・ティ・ティ・ドコモ) 2006.09.14, 【００１６】～【００１７】（ファミリーなし） | 1,2,7,8<br>3-6 |
| Y<br>A | JP 2004-30286 A (株式会社エヌ・ティ・ティ・データ) 2004.01.29, 請求項１（ファミリーなし） | 1,2,7,8<br>3-6 |
| Y<br>A | JP 2002-318734 A (株式会社チームガイア) 2002.10.31, 【０００７】～【００２０】 & WO 2002/088976 A1 | 2<br>3-6 |