

(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5月22日(22.05.2014)

(10) 国際公開番号

WO 2014/076773 A1

- (51) 国際特許分類:
G06F 13/00 (2006.01) *H04L 12/66* (2006.01)
G06F 21/55 (2013.01)
- (21) 国際出願番号: PCT/JP2012/079434
- (22) 国際出願日: 2012年11月13日(13.11.2012)
- (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: 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中4丁目1番1号 Kanagawa (JP).
- (72) 発明者: 児島 尚(KOJIMA, Hisashi); 〒2118588 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内 Kanagawa (JP). 中田 正弘(NAKADA, Masahiro); 〒2118588 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内 Kanagawa (JP).
- (74) 代理人: 伊東 忠重, 外(ITOH, Tadashige et al.); 〒1000005 東京都千代田区丸の内二丁目1番1号丸の内 MY PLAZA (明治安田生命ビル) 16階 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, IS, JP, KE, KG, KM, 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, 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: NETWORK FILTERING DEVICE, AND FILTERING METHOD

(54) 発明の名称: ネットワークのフィルタリング装置、及びフィルタリング方法

[図7]

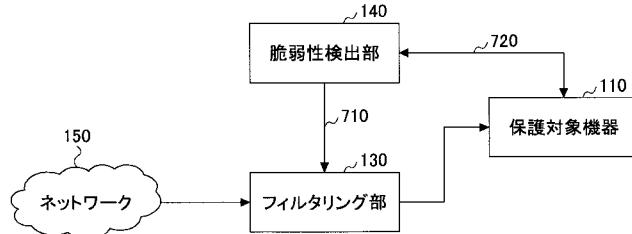


FIG. 7:
110 Device to be protected
130 Filtering unit
140 Vulnerability detector
150 Network

(57) Abstract: One purpose of the present invention is to provide effective protection against vulnerability of a device connected to a network. According to one embodiment of the present invention, provided is a device which filters data received over a network and outputs said data to a device to be protected, and which is provided with: a comparison unit for outputting a result obtained by comparing the received data with a prescribed pattern, among a plurality of patterns imparted to a test device for estimating behaviour of the device to be protected, in which prescribed behaviour is exhibited by the test device; and a blocking unit which, in cases when the comparison result is a positive result signifying that the data should be blocked, blocks the received data.

(57) 要約: 1つの側面では、本発明は、ネットワークに接続された機器の脆弱性に対する効果的な保護を提供することを目的とする。一実施形態によれば、ネットワークを介して受信されたデータをフィルタリングして保護対象機器に出力する装置であって、前記受信されたデータを、所定のパターンと比較した結果を出力する比較部であって、前記所定のパターンは、前記保護対象機器の挙動を推定するためのテスト機器に与えた複数のパターンのうち、前記テスト機器が所定の挙動を示したパターンである、比較部と、前記比較した結果が、データを遮断すべきことを意味する肯定的な結果である場合、前記受信されたデータを遮断する遮断部と、を有する装置が提供される。

WO 2014/076773 A1



(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, 添付公開書類:

NE, SN, TD, TG).

— 国際調査報告（条約第 21 条(3)）

明 細 書

発明の名称 :

ネットワークのフィルタリング装置、及びフィルタリング方法

技術分野

[0001] 本発明は、ネットワーク上で伝送されるデータに対するフィルタリングの技術に関する。

背景技術

[0002] 近年、ファジングとよばれるブラックボックスセキュリティテストの手法が広く利用されつつある。ファジングのためのツールは、脆弱性の検出に有効と考えられるテストデータを何種類も大量にテスト対象製品に試行することにより、脆弱性を検出する。例えば、ファジングツールにより、バッファオーバーフローや整数オーバーフローなどの未知の脆弱性を発見することが行われている。なお、近年では、誰でもがファジングツールを利用できる状況となっており、悪意のある者によって製品の未知の脆弱性を容易に発見されてしまう恐れがある。

[0003] ネットワークと接続される製品は、販売時点において、ネットワークからの攻撃に対して強固なセキュリティ対策が施されていることが理想である。しかしながら、この製品が販売され、消費者に渡った後に、この製品の脆弱性が新たに発見されることも多い。また、製品内には、様々な部品が含まれている。これらの部品の中には、内部を調査することが容易でないブラックボックスモジュール（ソースコードの監査などができるモジュール）も存在する。また、販売された製品が、購入者のシステムに組み込まれて、始めて発見される脆弱性も存在する。また、販売された製品に脆弱性が発見されても、その脆弱性に対応するアップデートソフトウェアなどの配布には時間がかかる場合も多い。

[0004] このため、製品の未知の脆弱性への対策が急務となっている。

[0005] 従来、応用プログラムのソースコードを自動的にスキャンし、応用プログ

ラムレベルの脆弱性を検出する技術が存在する（例えば、特許文献1）。

[0006] また、動作中のアプリケーション上で発生した異常終了動作データを逐次蓄積し表示することで、異常発生原因の分析並びに復旧の対応処理を行う技術が存在する（例えば、特許文献2）。

[0007] また、ネットワークを介して接続されているサーバと通信可能な通信装置であって、POP3サーバからメールメッセージを受信すると、そのメールメッセージにエラーが存在するかどうかを判定し、エラーが存在すると判定されたメールメッセージのユニークIDを登録し、その登録されたユニークIDと同じユニークIDを有するメールメッセージの番号を受信すると、そのメールメッセージの受信を拒否する技術が存在する（例えば、特許文献3）。

先行技術文献

特許文献

[0008] 特許文献1：特開2010-507165号公報

特許文献2：特開平6-35857号公報

特許文献3：特開2003-323383号公報

発明の概要

発明が解決しようとする課題

[0009] 1つの側面では、本発明は、ネットワークに接続された機器の脆弱性に対する効果的な保護を提供することを目的とする。

課題を解決するための手段

[0010] 一実施形態によれば、ネットワークを介して受信されたデータをフィルタリングして保護対象機器に出力する装置であって、前記受信されたデータを、所定のパターンと比較した結果を出力する比較部であって、前記所定のパターンは、前記保護対象機器の挙動を推定するためのテスト機器に与えた複数のパターンのデータのうち、前記テスト機器が所定の挙動を示したパターンである、比較部と、前記比較した結果が、データを遮断すべきことを意味

する肯定的な結果である場合、前記受信されたデータを遮断する遮断部と、を有する装置が提供される。

発明の効果

[0011] 実施態様によれば、ネットワークに接続された機器を簡便に保護することができる。

図面の簡単な説明

[0012] [図1]—実施形態に従った機能ブロック図である。

[図2]—実施形態に従った正常パターンと、テスト用のパターンの例を示す図である。

[図3]—実施形態の方法のフローチャートである。

[図4]—実施形態の方法のフローチャートである。

[図5]パターンを生成するために用いるリストの例を示す図である。

[図6]異常が特定されたパターンを保存するリストの例を示す図である。

[図7]他の実施形態の構成を示す図である。

[図8]他の実施形態の構成を示す図である。

[図9]他の実施形態の構成を示す図である。

[図10]異常検知部の動作を例示するブロック図である。

[図11]—実施形態のハードウェア構成例を示す図である。

発明を実施するための形態

[0013] 以下に、図面を用いて本発明の実施形態を詳細に説明する。なお、以下の実施形態は、発明を理解するためのものであり、本発明の範囲を限定するためのものではない点に留意すべきである。また、以下の複数の実施形態は、相互に排他的なものではない。したがって、矛盾が生じない限り、異なる実施形態の各要素を組み合わせることも意図されていることに留意すべきである。また、請求項に記載された方法やプログラムに係る発明は、矛盾のない限り処理の順番を入れ替えてよく、あるいは、複数の処理を同時に実施してもよい。そして、これらの実施形態も、請求項に記載された発明の技術的範囲に包含されることはあるまでもない。

[0014] また、コンピュータが読み出したプログラムコードを実行することにより、後述の実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているOSなどの他のプログラムが実際の処理の一部または全部を行ない、その処理によって実施形態の機能が実現される場合も、本発明に含まれることは言うまでもない。

[0015] また、本発明の各種実施形態のそれぞれの構成要素は、物理的に分離された複数のハードウェアで実現されてもよい。また、本発明の各種実施形態のそれぞれの構成要素は、1つのサーバ上で動作する複数のバーチャルマシンに分散されて実現されてもよい。

実施例

[0016] 図1は、一実施形態に従った、フィルタリングシステム100の機能ブロック図を示している。保護対象機器110は、フィルタリング部130を介して外部のネットワーク150と接続されている。フィルタリング部130は、保護対象機器110に対して、ネットワーク150から伝達されるデータをフィルタリングする。このフィルタリングによって、保護対象機器110の脆弱性に対して脅威を及ぼすデータを遮断することができる。

[0017] また、フィルタリング部130は、脆弱性検出部140と接続されてもよい。脆弱性検出部140は、テスト機器120に接続されてもよい。

[0018] なお、フィルタリング部130及び脆弱性検出部140は、物理的に分離されてもよい。また、これらは、物理的にどのような場所におかれてもよい。

[0019] 保護対象機器110は、ネットワークに接続され得る、いかなる機器であってもよい。保護対象機器110の具体例としては、サーバ、パーソナルコンピュータ、ハンドヘルドコンピュータ、ゲーム機器、テレビ、家電製品、ナビゲーションシステム、携帯電話などが挙げられる。

[0020] フィルタリング部130は、パターン保存部132、比較部134、遮断部136を含んでもよい。ネットワーク150からフィルタリング部130に対して、伝送路133を介して、パケット列が送られてくる。比較部13

4は、伝送されたパケットの各々を、パターン保存部132に保存されている複数のパターンと比較してもよい。なお、比較の単位は、パケットに限定されるものではない。伝送路133に流れるデータの形式は、パケット以外のいかなる形式であってもよい。また、比較部134は、伝送路に流れるデータの一部とパターン保存部132に保存されたパターンとを比較してもよい。或いは、比較部134は、伝送路に流れるデータが圧縮等で変換されている場合には、逆変換したデータを比較対象としてもよい。比較部134における比較は、完全一致の比較でなくてもよい。比較は、例えば、データが一定の数値範囲に入るか否か、データのビット数の長さが所定の範囲にあるか否かを、1つ以上の閾値を用いて比較（判定）してもよい。したがって、比較は、完全な一致以外に、上述のような比較の幅を持たせることにより、類似の範囲を含んだ判定結果であってもよい。比較結果によって、比較部134は、肯定的な結果又は否定的な結果を出力してもよい。また、比較は、データのシーケンスが所定の規則に従っているか否かを比較（判定）してもよい。

[0021] パターン保存部132は、所定のビット列を格納してもよいが、これに限定されるものではない。例えば、単なるデータ列のパターン以外に、規則としてのパターンが保存されていてもよい。例えば、パラメータ値のビット列の長さ、パラメータ値の範囲などが、規則の形でパターンとして保存されていてもよい。或いは、パターンには、保護対象機器110へのポート番号、データが利用される保護対象機器110のアプリケーションの情報等が含まれてもよい。比較部134は、様々な形式のパターンに基づいて、伝送路133に流れるデータを比較し又は判定し、その結果として肯定的な結果又は否定的な結果を、伝送路135を介して遮断部136に出力してもよい。なお、本明細書において、比較部134の肯定的な結果とは、データとパターンとが所定の規則に従っていることを意味し、そのデータは遮断部136において、遮断されるべきことを意味する。比較器における否定的な結果とは、その逆を意味し、遮断部136においてデータを通過させるべきことを意

味する。

[0022] 遮断部 136 は、ネットワーク 150 と保護対象機器 110との間に位置し、ネットワークから保護対象機器 110 に提供されるデータをフィルタリングしてもよい。なお、保護対象機器 110 からネットワーク 150 へ出力されるデータは、そのまま通過させてもよい。遮断部は、伝送路 133 を入力とし、所定のデータを遮断した後のデータを、伝送路 137 を介して保護対象機器 110 に伝達する。遮断部 136 は、比較部 134 からの制御情報を、伝送路 135 を介して受信する。伝送されるデータがパケットに分離されている場合には、遮断部 136 は、受信したパケットをバッファリングしてもよい。そして、比較部から伝送路 135 を介して送られてくる制御信号の到来を待って、バッファリングしたパケットを遮断するか、通過させるかを実行してもよい。遮断したパケットは、破棄してもよい。或いは、遮断部 136 は、比較部 134 が比較しているデータをバッファリングしてもよい。そして、比較部から伝送路 135 を介して送られてくる制御信号の到来を待って、バッファリングしたデータを遮断するか、通過させるかを実行してもよい。

[0023] 脆弱性検出部 140 に接続されているテスト機器 120 は、保護対象機器 110 の挙動をシミュレートする機器であってもよい。テスト機器 120 は、保護対象機器 110 と同じ仕様の製品を用いてもよい。例えば、保護対象機器 110 がサーバであれば、同じ仕様のサーバであって、同じソフトウェアを搭載したものであることが望ましい。なお、保護対象機器 110 をそのままテスト機器 120 として用いてもよい（この点は、図 7 を用いて後述する）。なお、テスト機器 120 は、挙動をチェックするために、例えばコンソールポートに、異常検知部 146 を接続してもよい。また、ソフトウェアの挙動を監視するために、バーチャルマシン上でソフトウェアを稼働させ、バーチャルマシンのファームウェアによってソフトウェアを監視し、その監視出力を異常検知部 146 に送ってもよい。

[0024] 脆弱性検出部 140 は、パターン生成部 142、送信部 144、異常検知

部 146、パターン特定部 148 を含んでもよい。

[0025] パターン生成部 142 は、様々なパターンのデータを生成してもよい。パターンの例については後述する。データがパケットの形で送られる場合には、パケットを生成してもよい。また、圧縮されたデータなど、所定の処理を施したデータを生成してもよい。生成されるパターンについての例は、図 2 を用いて後述する。

[0026] 送信部 144 は、パターン生成部 142 によって生成されたパターンのデータを、テスト機器 120 に送信する。

[0027] 異常検知部 146 は、テスト機器 120 の挙動を監視する。挙動の監視は、1 つのパターンのデータがテスト機器 120 に送られる度に実行されてもよい。異常検知部 146 は、テスト機器 120 が正常に動作しているか、又は異常終了したかを確認してもよい。テスト機器 120 の挙動の監視としては、例えば、テスト機器のコンソールポートから出力される文字列情報を監視してもよい。例えば、サーバのコンソールポートからは、サーバの異常を知らせるために、コンソールポートにおいて異常を知らせる表示を行うことがある。異常検知部 146 は、この表示に係るデータを捕捉し、サーバの異常を検出してもよい。或いは、一定時間経過後に、死活確認用のパケット（Ping 等）を、異常検知部からテスト機器に送信し、返信があるか否かをチェックしてもよい。例えば、テスト機器が異常終了した場合や、ハングアップしている場合には、ping の返信が行われないことがあるため、ping の返信が無いことによって、テスト機器 120 の異常を確認することができる。

[0028] また、テスト機器上のソフトウェアの挙動を監視するために、バーチャルマシン上でテスト機器を構築してもよい。そして、テスト機器上で注目しているソフトウェアを稼働させ、バーチャルマシンのファームウェアによって、このテスト機器の挙動を監視し、その監視結果を異常検知部 146 に送つてもよい。

[0029] パターン特定部 148 では、異常を引き起こしたパターンを特定する。異

常検知部で異常を検知した場合には、その異常にに関する情報がパターン特定部148に伝達されるため、その直前に送信したパターンを、パターン特定部148が特定することができる。

- [0030] パターン特定部148は、異常を引き起こしたパターンを特定し、パターン保存部132に送ってもよい。また、パターン特定部148は、パターンのデータそのものではなく、パターンの長さ（ビット長）などを、パターンとして特定し、パターン特定部148に送信してもよい。また、パターン特定部148は、パターンと共に、使用したポート番号や対象とするアプリケーションを特定する情報をパターンと関連付けて、パターン保存部132に提供してもよい。
- [0031] 以上のように、フィルタリング部130と脆弱性検出部140とは、連繋を取りながら動作することができる。
- [0032] このようにして、保護対象機器110に内在する新たな脆弱性を効率的に発見することができる。そして、その脆弱性をターゲットとしたネットワークからのデータの传送を、効果的に遮断することができる。このことによって、保護対象機器110の保護を迅速に行うことができる。
- [0033] 図2は、一実施形態に従った正常パターンと、テスト用のパターンの例を示している。保護対象機器110がWebサーバであるとして、HTTPリクエストとしてテストデータ（パケット）を送信する例が示されている。
- [0034] 正常パターン200は、HTTPプロトコルの各種ヘッダ部分である。この情報が、1つのパケットに含まれる。テストパターン1（210）ないしテストパターン4（240）は、パターン生成部142が生成するパターンの例を示している。これらのテストパターンは、主としてバッファオーバーフローをチェックするためのパターンである。4種類のヘッダが存在するため、各ヘッダに、Xが256個連續するデータが用いられている。
- [0035] テストパターン1（210）は、ホストアドレスとして、通常ではあり得ないビット長のアドレス（XXXX…XXXX）を含む。テストパターン2（220）は、受信側の利用するデータ形式を示すアクセプトパラメータと

して、通常ではあり得ないビット長のパラメータ（XXXX…XXX）を含む。テストパターン3（230）は、受信側の利用する言語を示す言語パラメータとして、通常ではあり得ないビット長のパラメータ（XXXX…XXX）を含む。テストパターン4（240）は、受信側の利用するユーザエージェントのパラメータとして、通常ではあり得ないビット長のパラメータ（XXXX…XXX）を含む。なお、Xの代わりに、Nullとしたり、文字列の長さを256個ではなく、それよりも長い文字列を用いたりしてもよい。

- [0036] 図3は、一実施形態の比較部134の処理のフローチャート300を示している。この方法は、例えば、ネットワーク150からのデータ（パケット）の入力イベントによって開始されてもよい（ステップ310）。例えば、受信した複数のパケットの各々に対してこのフローを実行してもよい。
- [0037] ステップ320において、パターン生成部142に保存されているパターンと、ネットワーク150から受信されたデータとが比較される。比較はパケットの単位であってもよい。ステップ320は、比較結果が肯定的であれば、「はい」を出力する。肯定的であることは、受信されたデータ（パケット）を遮断すべきであることを示しており、ステップ330に進む。比較結果が肯定的でない場合（「いいえ」）であれば、受信されたデータは、通過させてよいことを意味し、ステップ340に進む。
- [0038] ステップ330において、遮断部136は、受信されたデータ（パケット）を遮断する。この遮断によって、保護対象機器110に対して異常をもたらすデータが伝達されることを効果的に防止できる。
- [0039] ステップ240において、遮断部136はrx、受信されたデータを通過させ、保護対象機器110に、データを伝達する。
- [0040] 図4は、一実施形態における脆弱性検出部140の処理のフローチャートを示している。
- [0041] ステップ410において、全てのパターンがテストされたかが判断される。図2に示したように、テストするパターンは、複数存在する。したがって

、このステップ410において、全てのテストパターンのテストが終了すれば、この処理は終了する。全てのパターンのテストが終了していない場合には、ステップ420に進む。

- [0042] ステップ420において、パターン生成部142によって、1つのパターンが生成される。1つのパターンは、1つのパケットであってもよい。
- [0043] ステップ430において、生成されたパターンが送信部144によってテスト機器120に送信される。なお、テスト機器120として保護対象機器110とが同じ機器である場合には、生成されたパターンは、送信部144によって保護対象機器110に送られてもよい。
- [0044] ステップ440において、異常検知部146によって、テスト機器120の挙動が検知される。異常検知の方法としては、テスト機器のコンソール出力の異常表示の有無、Pingによる返信が受信できるか否か等を自動的にチェックしてもよい。
- [0045] ステップ450において、所定の挙動例えば異常が検知されたか否かが判断される。この判断結果が「はい」であれば、ステップ460に進む。この判断が「いいえ」であれば、ステップ470に進む。
- [0046] ステップ460において、テスト機器120に異常を引き起こしたパターンを特定する。特定されたパターンは、パターン保存部132に通知されてもよい。
- [0047] ステップ480において、チェック結果を記録してもよい。この記録によって、テスト対象機器に対するテストの進捗管理を行ってもよい。また、この記録を用いて、保護対象機器110の脆弱性の管理を行ってもよい。或いは、この記録に基づいて、例えば、保護対象機器110に内在するアプリケーションプログラムのバージョンアップを行ってもよい。バージョンアップが行われ、保護対象機器110の脆弱性が改善できた場合には、その情報を基に、パターン保存部132に保存されているパターンから、脆弱性が改善できた不要なパターンを削除するようにしてもよい（不図示）。
- [0048] 図5は、パターンを生成するために用いるリスト500の例を示している

。図5に示す情報を、例えば、脆弱性検出部140に記憶してもよい。リスト500には、例えば以下の情報が保存されてもよい。

[0049] 以下が図5に示すようなテスト情報保存手段に予め保存されているものとする。

- (1) 保護対象機器110のIPアドレス：192.168.1.10
- (2) 保護対象機器110のポート番号：80
- (3) テスト方法：テスト1
- (4) 保護対象機器110の対象アプリケーション：業務プログラム1
- (5) テスト1の正常パターン：正常パターンの保存アドレス
- (6) テスト1のテストパターンの総数：4
- (7) テスト1の次にテストすべきパターンの番号：1

上記(1)には、送信部144が送信するパターンを送信する宛先のテスト機器120のアドレスを示す情報を保存してもよい。上記(2)には、保護対象機器110のポート番号を特定してもよい。一般に、保護対象機器110のポート番号によって、脆弱性は異なるからである。上記(3)には、テスト方法を特定する情報が格納されてもよい。ここでは、「テスト1」が保存されており、例えば、「テスト1」は、上述のバッファオーバーフローに関するテストであることを示している。そして、例えば「テスト2」としては、ヘッダの名前を置き換えるテストであることを特定してもよい。上記(4)には、保護対象機器110において動作しているテスト対象のアプリケーションを特定する情報が保存されてもよい。この項目を利用するには、動作するアプリケーション毎に脆弱性が異なる場合が想定されるからである。上記(5)は、テスト1の正常パターンを特定する項目である。これは、例えば、正常パターンが格納されているアドレスにより特定されてもよい。上記(6)は、テスト1のテストパターンの総数を示している。図4に示したステップ410を実行する際に、この情報が利用されてもよい。上記(7)は、図4に示したステップ410を実行する際に、この情報が利用されてもよい。この値をインクリメントすることにより、次のテストのパターンを

生成することができる。図5においては、値が「1」となっているため、初期値であることを示しており、テスト1はまだ実行されていないことを示している。

- [0050] 図6は、異常が特定されたパターンを保存するリスト600の例を示している。「テスト番号」は、1から順にインクリメントする番号であり、エントリの位置を特定するために用いてもよい。「テスト方法」は、どのテストによって異常が検出されたかを示すものとして利用され得る。「テスト1の正常パターン」は、正常なパターンを確認したい場合に利用されてもよい。「テスト1のパターン情報」は、具体的に異常を引き起こしたパターンのアドレスが格納されてもよい。或いは、パターンに付与されたシーケンスの番号を保存し、パターンを特定してもよい。リスト600は、パターン保存部132に格納され得る。
- [0051] 図7は、他の実施形態の構成を示している。脆弱性検出部140は、伝送路720によって保護対象機器110に接続されている。この場合には、脆弱性検出部140は、保護対象機器110に接続されているため、例えば、保護対象機器110がサーバの場合、システムダウンを起こす可能性がある。したがって、保護対象機器110のシステムメンテナンス時などに、脆弱性検出部140を稼働させ、脆弱性のテストを行うことが望ましい。あるいは、再稼働が迅速に行える保護対象機器110であれば、保護対象機器110の稼働中に、脆弱性検出部140を動作させてもよい。この実施例の場合には、保護対象機器110を直接チェックできるため、保護対象機器110の挙動を推定するためのテスト機器120が不要となる。また、テスト機器120を使用する場合よりも、より正確な脆弱性のチェックが行える。脆弱性検出部140によって特定されたパターンは、伝送路740を介してフィルタリング部130に伝達することができる。
- [0052] 図8は、他の実施形態の構成を示している。フィルタリング部130が、保護対象機器110内に組み込まれている実施例である。フィルタリング部130を保護対象製品内のフロントエンド部に設置することができる。した

がって、保護対象機器 110 毎にフィルタリング部 130 におけるフィルタリングの動作をカスタマイズでき、保護対象機器 110 に対して、より適合した脆弱性の対策を講じることができる。なお、図 8 の場合には、脆弱性検出部 140 が、保護対象機器 110 に、伝送路 820 を介して接続されているが、別途テスト機器 120 を設置してもよい（不図示）。脆弱性検出部 140 によって特定されたパターンは伝送路 810 を介してフィルタリング部 130 に伝達される。

[0053] 図 9 は、他の実施形態の構成を示している。保護対象機器 110 内に脆弱性検出部 140 とフィルタリング部 130 が位置している。なお、この実施例の場合には、脆弱性検出部 140 が、保護対象機器 110 内に存在するため、保護対象機器 110 の異常動作が、脆弱性検出部 140 の動作に影響することが予想される。したがって、保護対象機器 110 の異常動作が保護対象機器 110 によるパターンの特定に影響する場合がある。このような事態に対処するためには、同一のサーバに複数のバーチャルマシンを動作させ、脆弱性検出部 140 と、保護対象機器 110 とを、別のバーチャルマシンで動作させてもよい。このようにすれば、保護対象機器 110 の異常動作が保護対象機器 110 によるパターンの特定に影響するのを飛躍的に減少させることができる。

[0054] 図 10 は、異常検知部の動作を例示するブロック図である。例えば、テスト機器 120 がサーバの場合には、コンソールポートなどが装備されている場合がある。したがって、伝送路 1030 を介して、テスト機器 120 のコンソールポートを異常検知部 146 に接続してもよい。異常検知部 146 は、テスト機器 120 のコンソールポートの出力を解析することによって、テスト機器 120 の異常の有無を調べることができる。通常、サーバなどのコンソールポートからの出力には、サーバの異常を知らせる種々の情報が出力されるからである。

[0055] また、図 10 に示すように、異常検知部 146 からテスト機器 120 に ping などの死活確認用のパケットを送ってもよい。そして、一定時間経過

後に、その返信があるか否かを確認してもよい。返信が確認できない場合には、テスト機器120がシステムダウンを起こしていたり、ハングアップしていたりする可能性が非常に高いことが分かる。したがって、死活確認用のパケットの送信により、テスト機器120の異常の発生を確認することができる。或いは、異常検知部146から、ステータス確認用のコマンドを送信し、テスト機器120の種々のステータスを確認して、異常の有無を検知してもよい。

- [0056] 本発明は、これらの実施例に限定されるものではない。
- [0057] 図11は、本発明の実施形態のハードウェア（コンピュータ）の構成例を示している。ハードウェアは、CPU1110、メモリ1115、入力装置1120、出力装置1125、外部記憶装置1130、可搬記憶媒体駆動装置1135、ネットワーク接続装置1145が含まれる。そして、それぞれの機器は、バス1150によって接続されている。また、可搬記憶媒体駆動装置1135は、可搬記憶媒体1140を読み書きすることができる。そして、ネットワーク接続装置1145には、ネットワーク1160が接続されている。
- [0058] なお、本実施形態の全部又は一部はプログラムによってインプリメントされ得る。このプログラムは、可搬記憶媒体1140に格納することができる。可搬記憶媒体1140とは、構造を有する1つ以上の非一時的（non-transitory）な記憶媒体を言う。例示として、可搬記憶媒体1140としては、磁気記録媒体、光ディスク、光磁気記録媒体、不揮発性メモリなどがある。磁気記録媒体には、HDD、フレキシブルディスク（FD）、磁気テープ（MT）などがある。光ディスクには、DVD（Digital Versatile Disc）、DVD-RAM、CD-ROM（Compact Disc-Read Only Memory）、CD-R（Recordable）／RW（ReWritable）などがある。また、光磁気記録媒体には、MO（Magneto-Optical disk）などがある。可搬型記録媒体に格納されたプログラムが読み込まれ、CPUによって実行されることにより、本発明の実施形態の全部又は一部が実施され得る。

符号の説明

[0059] 100 フィルタリングシステム

110 保護対象機器

120 テスト機器

130 フィルタリング部

132 パターン保存部

134 比較部

136 遮断部

140 脆弱性検出部

142 パターン生成部

144 送信部

146 異常検知部

148 パターン特定部

150 ネットワーク

請求の範囲

- [請求項1] ネットワークを介して受信されたデータをフィルタリングして保護対象機器に出力する装置であって、
前記受信されたデータを、所定のパターンと比較した結果を出力する比較部であって、前記所定のパターンは、前記保護対象機器の挙動を推定するためのテスト機器に与えた複数のパターンのデータのうち、前記テスト機器が所定の挙動を示したパターンである、比較部と、
前記比較した結果が、データを遮断すべきことを意味する肯定的な結果である場合、前記受信されたデータを遮断する遮断部と、
を有する装置。
- [請求項2] 前記比較部は、前記受信されたデータと、前記所定のパターンが類似する場合に、肯定的な結果を出力する、
請求項1記載の装置。
- [請求項3] 前記所定のパターンは、脆弱性検出部により提供され、
前記脆弱性検出部は、
前記複数のパターンのデータを生成する生成部と、
生成された前記複数のパターンのデータの各々を前記テスト機器に与える送信部と、
前記テスト機器の挙動の異常を検知する異常検知部と、
前記挙動の異常が検知された場合、前記挙動の異常の原因となつた前記所定のパターンを特定するパターン特定部と、
を更に有する、
請求項1又は2記載の装置。
- [請求項4] 前記保護対象機器と前記テスト機器は、同一の機器である、請求項1ないし3のうち何れか1項に記載の装置。
- [請求項5] 前記所定のパターンは、ポート番号、及び又は、前記受信されたデータを利用するアプリケーションを特定する情報を含む、請求項1ないし4のうち何れか1項に記載の装置。

- [請求項6] ネットワークを介して受信されたデータをフィルタリングして保護対象機器に出力するためのプログラムであって、
前記受信されたデータを、所定のパターンと比較した結果を出力し
、前記所定のパターンは、前記保護対象機器の挙動を推定するためのテスト機器に与えた複数のパターンのデータのうち、前記テスト機器が所定の挙動を示したパターンであり、
前記比較した結果が、データを遮断すべきことを意味する肯定的な結果である場合、前記受信されたデータを遮断する、
処理をコンピュータに実行させるプログラム。
- [請求項7] 前記比較した結果を出力する処理は、前記受信されたデータと、前記所定のパターンが類似する場合に、肯定的な結果を出力する、
請求項6記載のプログラム。
- [請求項8] 前記複数のパターンのデータを生成し、
生成された前記複数のパターンのデータの各々を前記テスト機器に与え、
前記テスト機器の挙動の異常を検知し、
前記挙動の異常が検知された場合、前記挙動の異常の原因となつた前記所定のパターンを特定する、
処理をコンピュータに実行させるプログラムを更に有する、
請求項6又は7記載のプログラム。
- [請求項9] 前記保護対象機器と前記テスト機器は、同一の機器である、請求項6ないし8のうち何れか1項に記載のプログラム。
- [請求項10] 前記所定のパターンは、ポート番号、及び又は、前記受信されたデータを利用するアプリケーションを特定する情報を含む、請求項6ないし9のうち何れか1項に記載のプログラム。
- [請求項11] ネットワークを介して受信されたデータをフィルタリングして保護対象機器に出力するための方法であって、
前記受信されたデータを、所定のパターンと比較した結果を出力す

る工程であって、前記所定のパターンは、前記保護対象機器の挙動を推定するためのテスト機器に与えた複数のパターンのデータのうちで、前記テスト機器が所定の挙動を示したパターンである、工程と、前記比較した結果が、データを遮断すべきことを意味する肯定的な結果である場合、前記受信されたデータを遮断する工程と、を有する方法。

[請求項12] 前記比較した結果を出力する工程は、前記受信されたデータと、前記所定のパターンが類似する場合に、肯定的な結果を出力する、請求項1 1 記載の方法。

[請求項13] 前記複数のパターンのデータを生成する工程と、生成された前記複数のパターンのデータの各々を前記テスト機器に与える工程と、前記テスト機器の挙動の異常を検知する工程と、前記挙動の異常が検知された場合、前記挙動の異常の原因となつた前記所定のパターンを特定する工程と、を更に有する、請求項1 1 又は1 2 記載の方法。

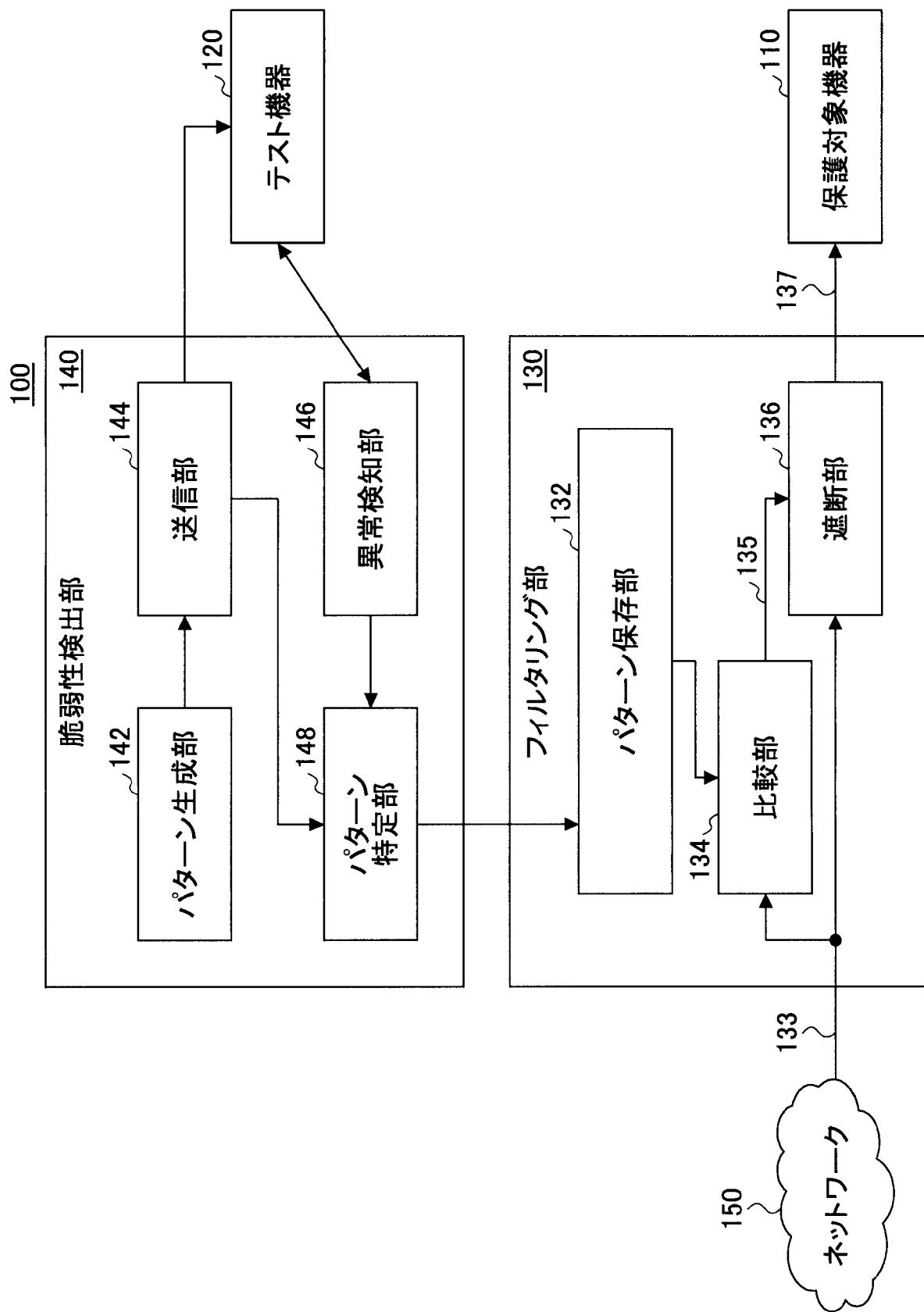
[請求項14] 前記保護対象機器と前記テスト機器は、同一の機器である、請求項1 1ないし1 3のうち何れか1 項に記載の方法。

[請求項15] 前記所定のパターンは、ポート番号、及び又は、前記受信されたデータを利用するアプリケーションを特定する情報を含む、請求項1 1ないし1 4のうち何れか1 項に記載の方法。

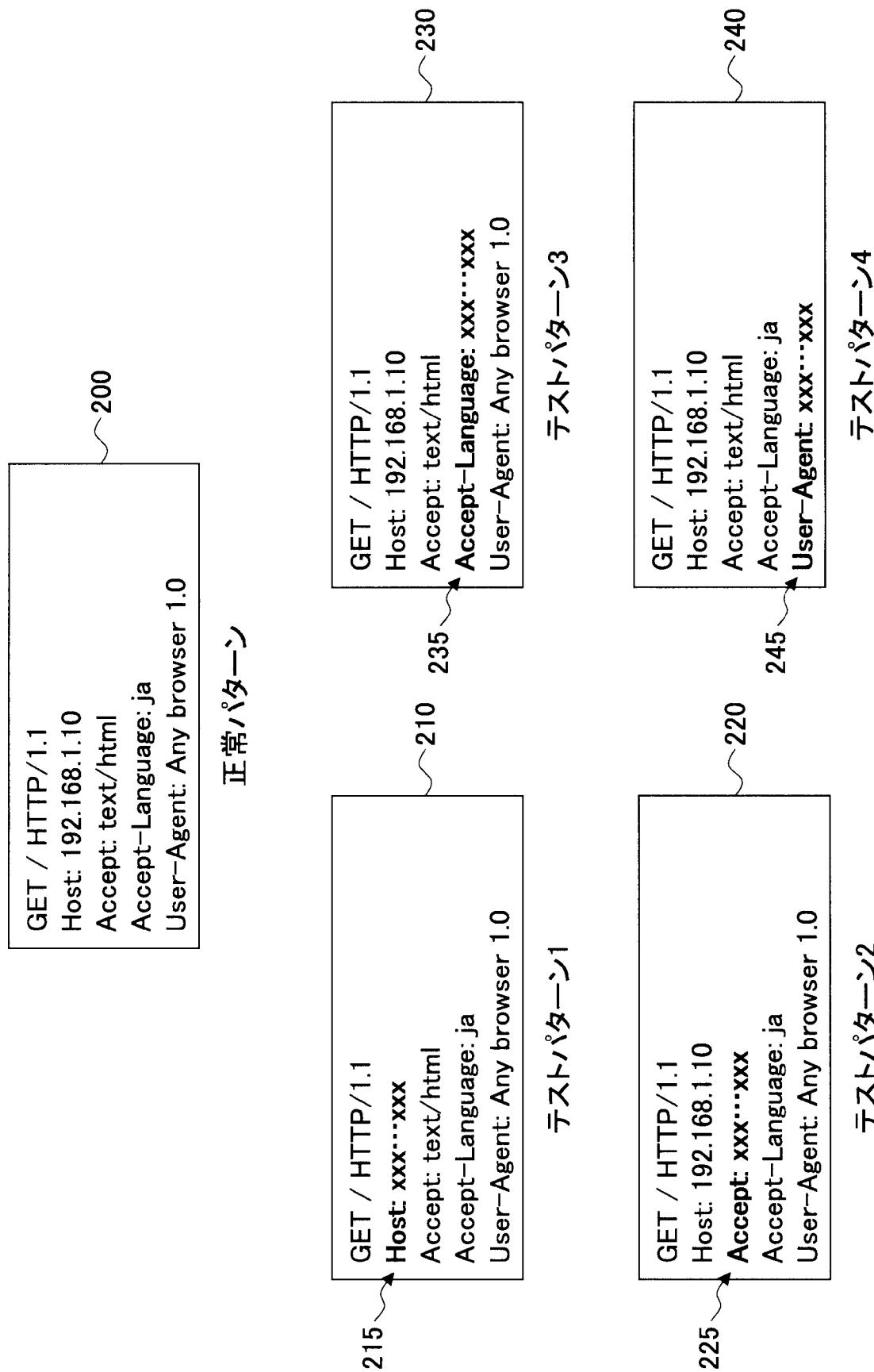
[請求項16] ネットワークを介して受信されたデータをフィルタリングして保護対象機器に出力するシステムであって、複数のパターンのデータを生成する生成部と、生成された前記複数のパターンのデータの各々を、保護対象機器の挙動を推定するためのテスト機器に与えるパターンデータ送信部と、前記テスト機器の挙動を検知する異常検知部と、

前記テスト機器の所定の挙動が検知された場合、前記所定の挙動の原因となった所定のパターンを特定する特定部と、前記受信されたデータを、前記所定のパターンと比較した結果を出力する比較部と、前記比較した結果が、データを遮断すべきことを意味する肯定的な結果である場合、前記受信されたデータを遮断する遮断部と、を有するシステム。

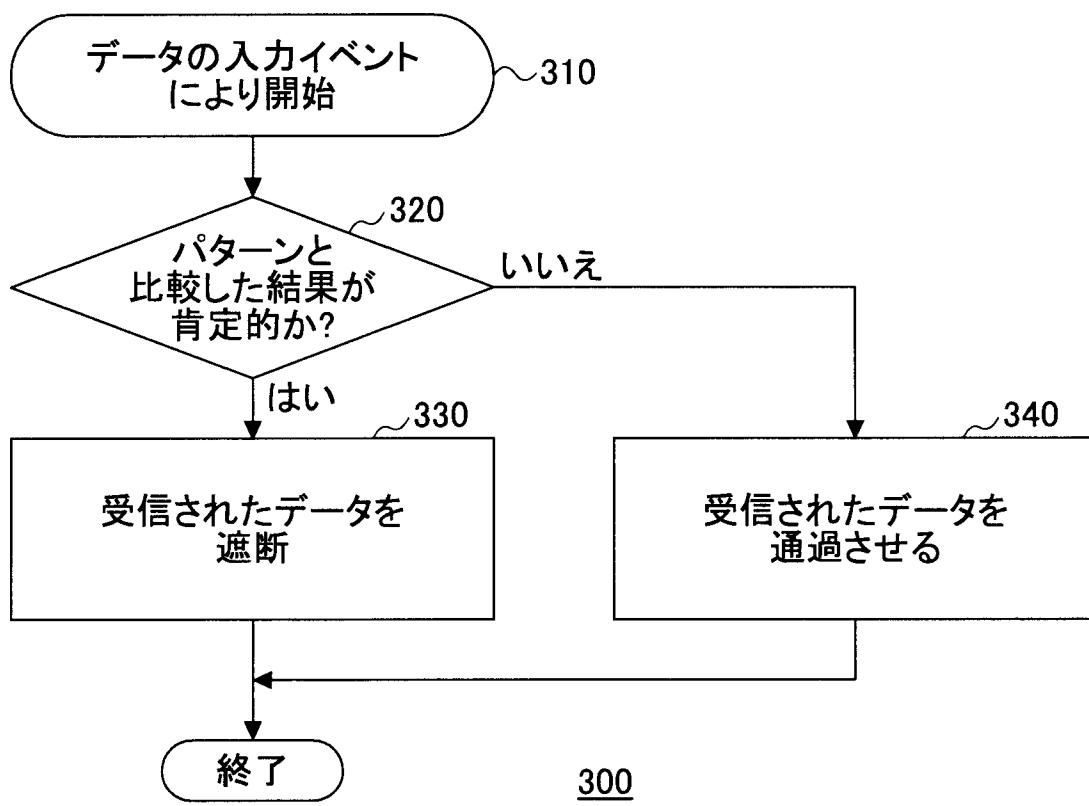
[図1]



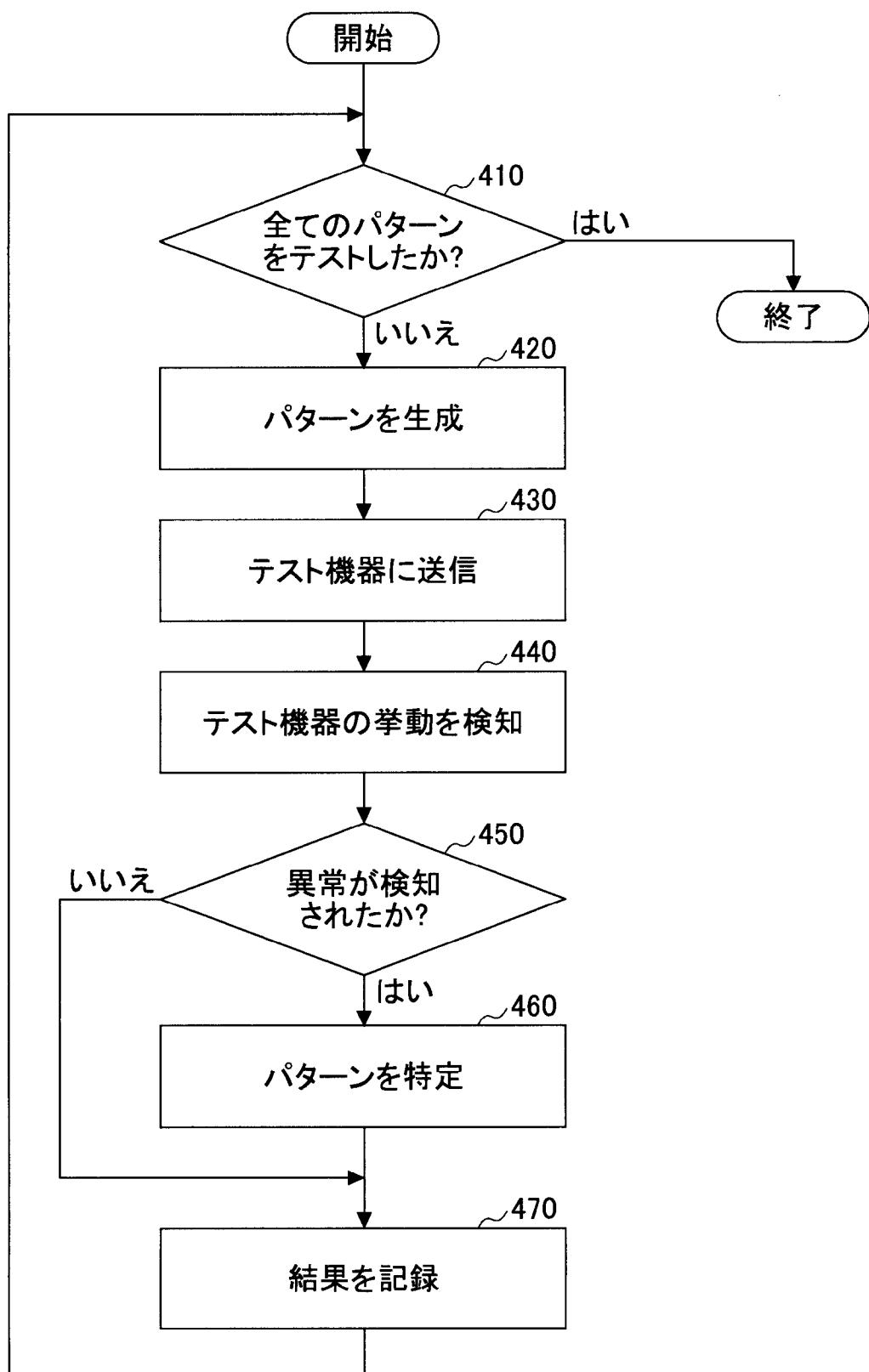
[図2]



[図3]



[図4]



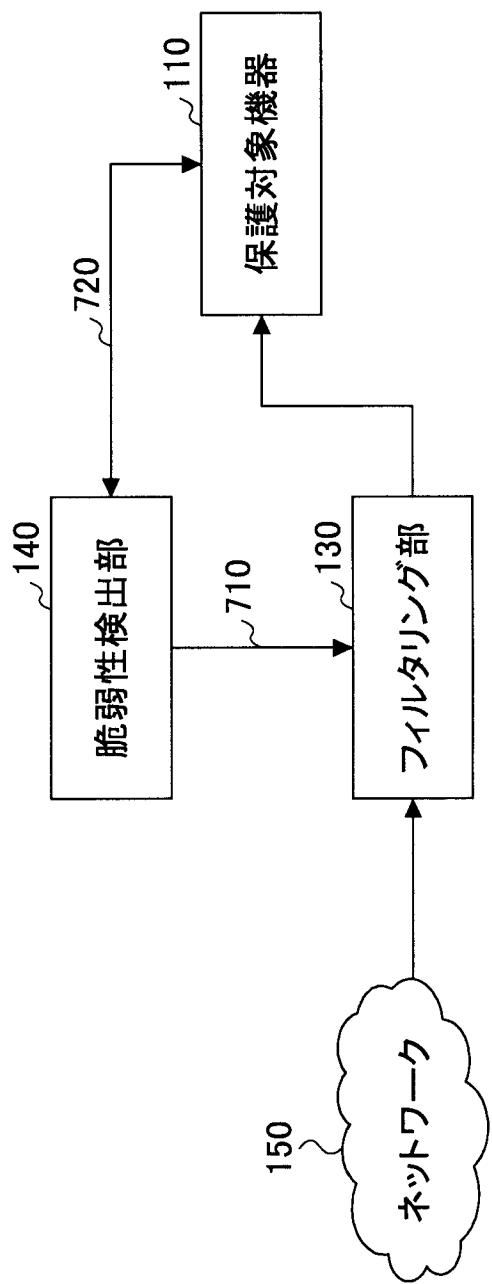
[図5]

500	
保護対象機器のIPアドレス	192.168.1.10
保護対象機器のポート番号	80
保護対象機器のアプリケーション	業務プログラム1
テスト方法	テスト1
テスト1の正常パターン	正常パターンの保存アドレス
テスト1のテストパターンの総数	4
テスト1の次にテストすべきパターンの番号	1

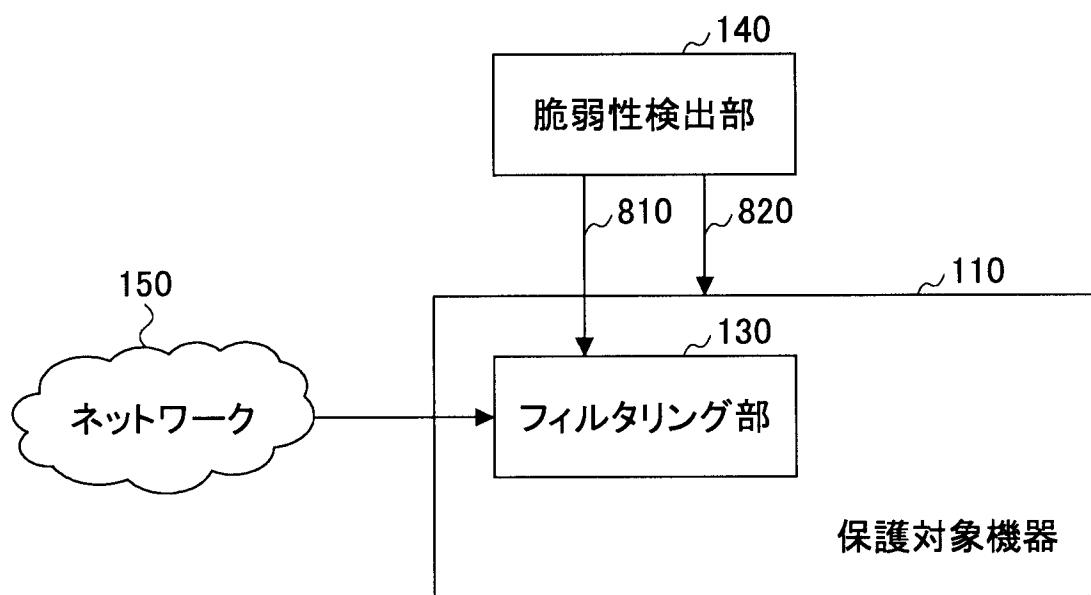
[図6]

テスト番号	テスト方法	テスト1の正常パターン情報	
		テスト1の正常パターン	テスト1のパターン情報
1	テスト1	正常パターンの格納アドレス	パターン1の格納アドレス
2	テスト1	正常パターンの格納アドレス	パターン2の格納アドレス
...

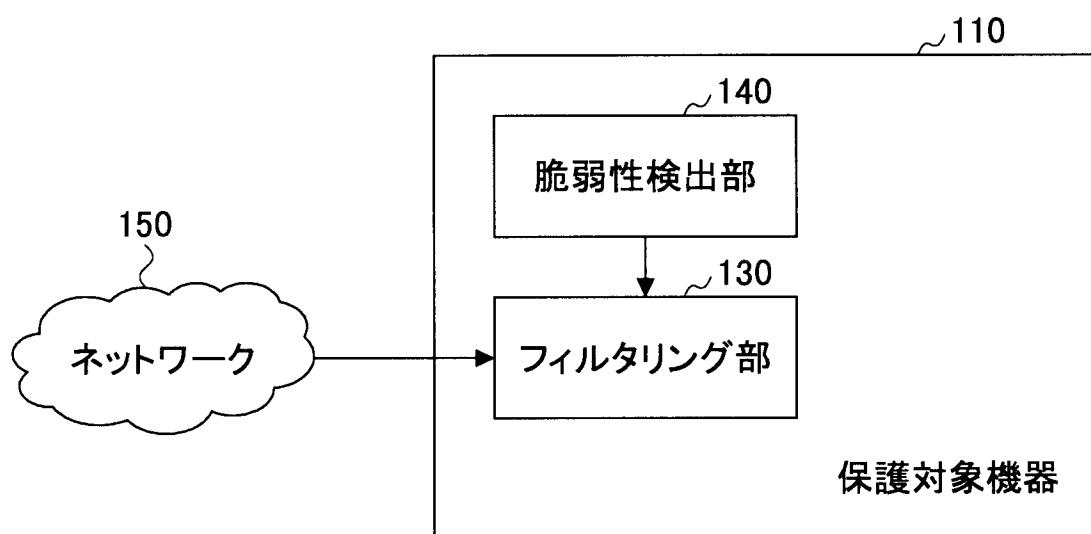
[図7]



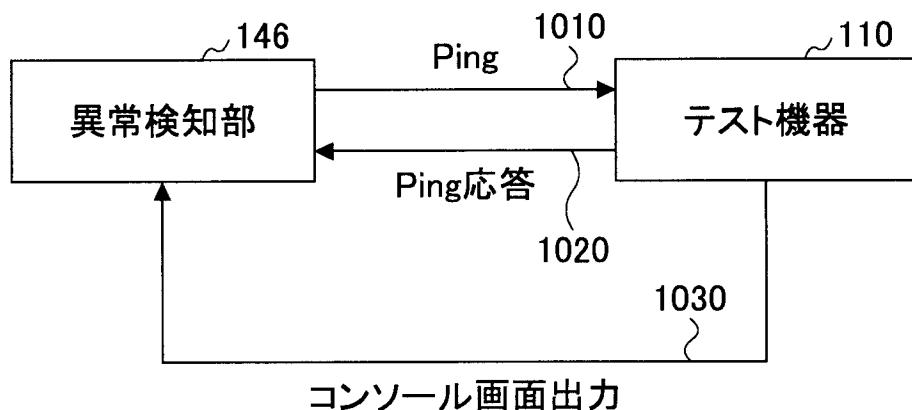
[図8]



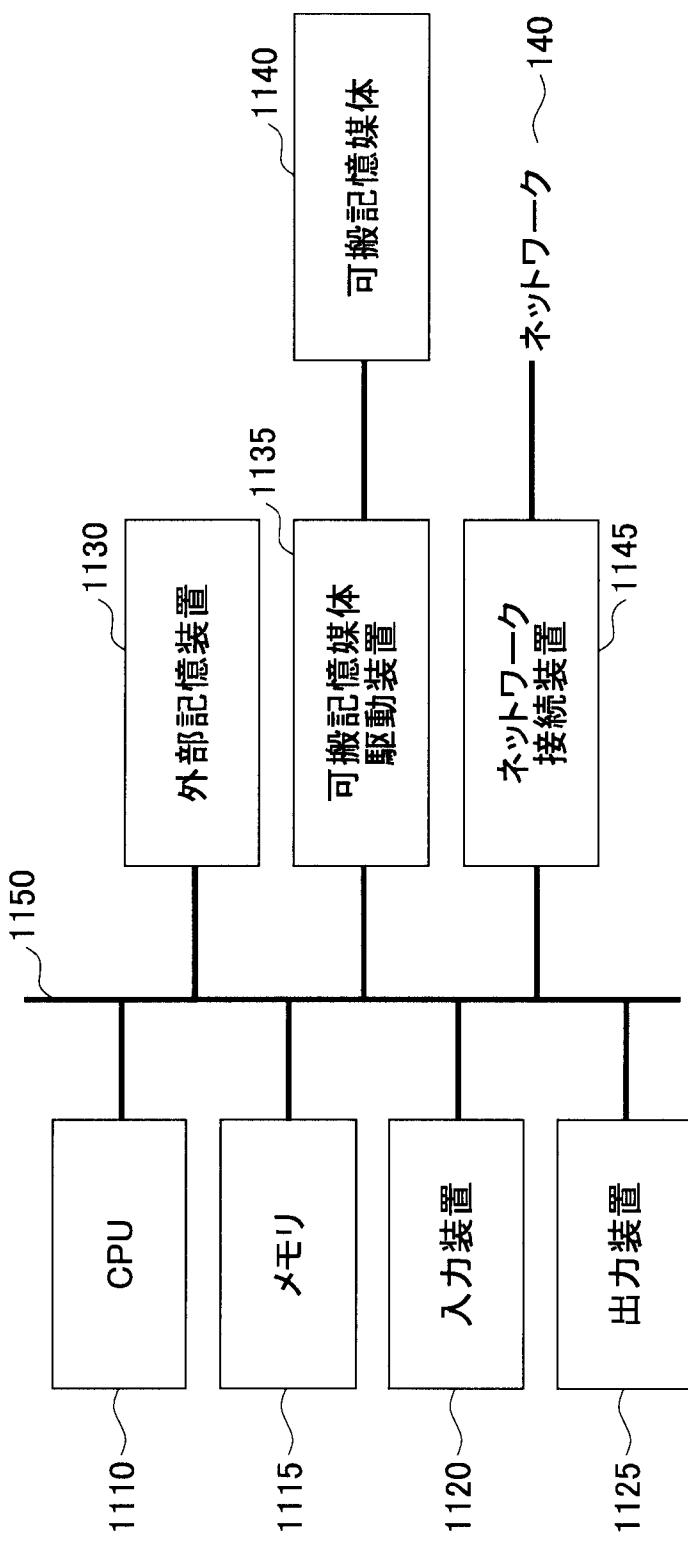
[図9]



[図10]



[図11]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2012/079434

A. CLASSIFICATION OF SUBJECT MATTER

G06F13/00(2006.01)i, *G06F21/55*(2013.01)i, *H04L12/66*(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)

G06F13/00, G06F21/55, H04L12/66

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

<i>Jitsuyo Shinan Koho</i>	1922-1996	<i>Jitsuyo Shinan Toroku Koho</i>	1996-2013
<i>Kokai Jitsuyo Shinan Koho</i>	1971-2013	<i>Toroku Jitsuyo Shinan Koho</i>	1994-2013

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.
X	WO 2012/011270 A1 (NEC Corp.), 26 January 2012 (26.01.2012), paragraphs [0020] to [0022], [0028] to [0034] & JP 2012-27618 A	1, 4, 6, 9, 11, 14, 16 2, 3, 5, 7, 8, 10, 12, 13, 15
Y	JP 2007-157059 A (Secure Brain Corp.), 21 June 2007 (21.06.2007), paragraph [0017] (Family: none)	2, 7, 12
Y	WO 2012/063493 A1 (Kyocera Communication Systems Co., Ltd.), 18 May 2012 (18.05.2012), abstract & JP 2012-133406 A	3, 8, 13

Further documents are listed in the continuation of Box C.

See patent family annex.

* Special categories of cited documents:

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier application or patent but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search
25 March, 2013 (25.03.13)

Date of mailing of the international search report
02 April, 2013 (02.04.13)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2012/079434

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2004-185622 A (Docomo Communications Laboratories U.S.A. Inc.), 02 July 2004 (02.07.2004), paragraphs [0031] to [0032] & US 2004/0111519 A1	5,10,15

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl. G06F13/00(2006.01)i, G06F21/55(2013.01)i, H04L12/66(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. G06F13/00, G06F21/55, H04L12/66

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	1971-2013年
日本国実用新案登録公報	1996-2013年
日本国登録実用新案公報	1994-2013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
X	WO 2012/011270 A1 (日本電気株式会社) 2012.01.26, 段落[0020]-[0022], [0028]-[0034] & JP 2012-27618 A	1, 4, 6, 9, 11, 14, 16
Y		2, 3, 5, 7, 8, 10, 12, 13, 15
Y	JP 2007-157059 A (株式会社セキュアブレイン) 2007.06.21, 段落[0017] (ファミリーなし)	2, 7, 12

 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 25. 03. 2013	国際調査報告の発送日 02. 04. 2013
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	特許序審査官（権限のある職員） 小林 秀和 電話番号 03-3581-1101 内線 3568 5T 3449

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	WO 2012/063493 A1 (京セラコミュニケーションシステム株式会社) 2012.05.18, [要約] & JP 2012-133406 A	3, 8, 13
Y	JP 2004-185622 A (ドコモ コミュニケーションズ ラボラトリーズ ユー・エス・エー インコーポレーティッド) 2004.07.02, 段落[0031]-[0032] & US 2004/0111519 A1	5, 10, 15