(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2日(02.01.2020)

WIPO | PCT

(10) 国際公開番号
WO 2020/004489 A1

(51) 国際特許分類:
H04L 12/70 (2013.01)

(21) 国際出願番号： PCT/JP2019/025447

(22) 国際出願日： 2019年6月26日(26.06.2019)

(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 2018-124884 2018年6月29日(29.06.2018) JP

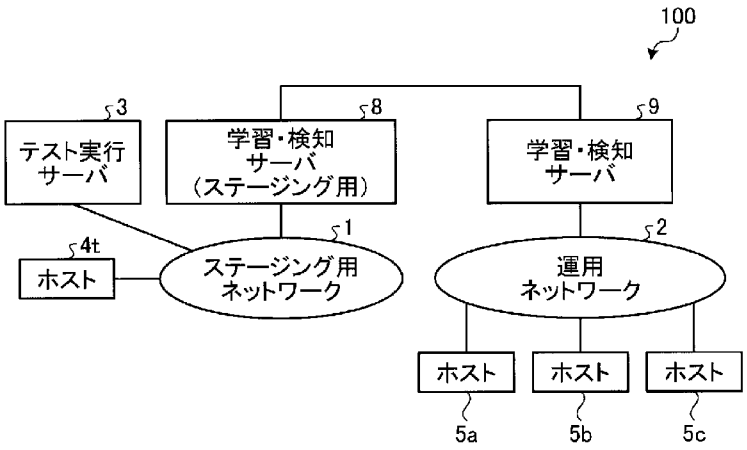
(71) 出願人: 日本電信電話株式会社 (**NIPPON TELEGRAPH AND TELEPHONE CORPORATION**) [JP/JP]; 〒1008116 東京都千代田区大手町一丁目５番１号 Tokyo (JP).

(72) 発明者: 南 拓也(**MINAMI, Takuya**); 〒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). 佐藤 友康(**SATO, Tomoyasu**); 〒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). 藤木 直人(**FUJIKI, Naoto**); 〒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). 中津留 毅(**NAKATSURU, Takeshi**); 〒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). 泉 雅巳(**IZUMI, Masami**); 〒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**

(54) **Title:** COMMUNICATION SYSTEM AND COMMUNICATION METHOD

(54) 発明の名称： 通信システム及び通信方法



1 Network for staging
2 Operation network
3 Text execution server
4t, 5a, 5b, 5c Host
8 Learning/detection server (for staging)
9 Learning/detection server

(57) **Abstract:** This communication system (100) is a communication system comprising a second network including: an operation network (2) which has a host (5) and a learning/detection server (9); and a network for staging (1) which has a host (4t) of the same type as the host (5), a test execution server (3), and a learning/detection server (8), wherein the test execution server (3) performs a communication test for transmitting, to the host (4t), a test communication of a normal state, and for receiving a communication by the host (4t). The learning/detection server (8) learns the communication

WO 2020/004489 A1

［続葉有］

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, 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, KE, KG, KH, KN, KP, KR, KW, 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：

一　国際調査報告（条約第21条(3)）

of the host (4t), generates an initial model for detecting an abnormal communication of the host (4t), and transmits the initial model to the learning/detection server (9). The learning/detection server (9) uses the initial model received from the learning/detection server (8) to monitor a communication of the host (5), learns the communication of the host (5), and generates a model for detecting an abnormal communication of the host (5).

(57) 要約：通信システム（１００）は、ホスト（５）と学習・検知サーバ（９）とを有する運用ネットワーク（２）と、ホスト（５）と同型のホスト（４ｔ）とテスト実行サーバ（３）と学習・検知サーバ（８）とを有するステージング用ネットワーク（１）とを有する第２のネットワークとを有する通信システムであって、テスト実行サーバ（３）は、ホスト（４ｔ）に正常状態のテスト通信を送信し、ホスト（４ｔ）による通信を受信する通信テストを行い、学習・検知サーバ（８）が、ホスト（４ｔ）の通信を学習してホスト（４ｔ）の異常通信を検知する初期モデルを生成し、初期モデルを学習・検知サーバ（９）に送信し、学習・検知サーバ（９）は、学習・検知サーバ（８）から受信した初期モデルを用いてホスト（５）の通信を監視しながら、ホスト（５）の通信を学習してホスト（５）の異常通信を検知するモデルを生成する。

明　細　書

発明の名称 ： 通信システム及び通信方法

技術分野

[0001] 本発明は、通信システム及び通信方法に関する。

背景技術

[0002] 近年の経済活動や生活環境のＩＣＴ（Information and Communication Technology）化は、便利さが供給される反面、セキュリティインシデント発生時の影響度が大きくなっており、セキュリティ対策の重要性は、日々高まっている。

[0003] 刻々と変化するサイバー分野での脅威に対し、セキュリティベンダや研究機関によりセキュリティ対策技術の研究開発が進められている。しかしながら、現在、ゼロデイ攻撃といった既存の検知ルールでは検知できない未知の攻撃は、大きな脅威となっている。このような未知の攻撃への対抗策として、正常状態を定義し、正常状態と識別できない状態を異常状態と識別するアノマリ検出手法の採用が始まっている。

[0004] ＩＣＴ環境、例えば、ＩｏＴ（Internet of Things）に代表される全てのモノがネットワークに繋がる環境下において、サイバー攻撃の標的とされる機器の多くがネットワーク経由で攻撃を受ける。このため、ネットワークに流れる通信を監視することは、セキュリティ対策として効果的であり、ネットワークの通信監視にアノマリ検出手法を適用することは、さらに効果的な手法であるといえる。

[0005] アノマリ検出手法では、正常状態の定義を、学習することが現在のトレンドとなっており、アノマリ検出手法をネットワーク通信監視に適用する場合には、ネットワークに流れる通信群に対し、学習により正常状態を定義する方法を用いる。

[0006] ネットワーク通信監視におけるアノマリ検出手法は、正常状態と定義したネットワークに流れる通信を正常状態の通信として学習する期間（以降、学

習フェーズ）と、学習完了後にネットワークに流れる通信が、学習した状態と同じであることが識別できない場合に異常であると検知する期間（以降、検知フェーズ）との２つのフェーズを設けている。実際にアノマリ検出手法が使用される際は、学習フェーズを行い、その後、検知フェーズを行う。

[0007] ここで、学習フェーズにおいて生成される正常状態を表現するデータは、例えば、通信フロー情報の場合であれば、通信先やプロトコルなど値や文字列で表される。また、正常状態を表現するデータは、通信の特徴を機械学習の入力とするものであれば、数理モデル（数式やパラメータの集まり）で表される。アノマリ検出手法の実装の仕方によって、正常状態を表現するデータは様々である。以降、この正常状態を表現するデータをモデルと呼ぶこととする。

[0008] アノマリ検出手法の一例として、学習・検知機能からなるホワイトリスト機能を有するネットワークスイッチ製品がある。このネットワークスイッチ製品は、学習フェーズではネットワークに流れたトラフィックの通信フロー（通信先やプロトコルなど）のそれぞれを正常なものとして学習（ホワイトリストとして定義）し、検知フェーズでは正常なものとは異なる通信フローをアノマリ検出する（非特許文献１参照）。

[0009] また、他の例として、主にＩｏＴ機器を対象に、機器の通信の正常パターンを機械学習によりモデル化し、これを正常状態と定義し、モデルに当てはまらないパターンの通信を識別することでアノマリ検出を行うという技術がある（非特許文献２参照）。

先行技術文献

非特許文献

[0010] 非特許文献1：アラクサラネットワークス　ネットワーク・セキュリティホワイトリスト機能、［online］、［平成３０年６月１４日検索］、インターネット＜ＵＲＬ：https://www.alaxala.com/jp/solution/security/wl/＞

非特許文献2：Zingbox Enabling the Internet of Trusted Things、［online］、［平成３０年６月１４日検索］、インターネット＜ＵＲＬ：htt

ps://www.zingbox.com/＞

発明の概要

発明が解決しようとする課題

[0011] 上記のアノマリ検出手法を実現するにあたり学習フェーズが不可欠である。ここで、アノマリ検出手法においては、学習フェーズ中に異常通信が混入した場合、その通信が正常状態の一部として学習され、その後の検知フェーズにおいて混入した異常通信を検出することができないという問題がある。

[0012] すなわち、学習という手段を使うアノマリ検出手法には、学習フェーズ中が脆弱な期間になるという弱点がある。

[0013] このため、学習フェーズを行う際は、信頼された機器群を基にネットワークを初期構築し、その環境上で学習フェーズを行い、その後検知フェーズに移行するという、学習フェーズ時のネットワークの健全性を担保するための特別な段取りが必要となる。

[0014] しかしながら、ネットワークの運用上、初期構築から始められない場合がある。例えばネットワーク運用中の接続機器のソフトウェア改変がある場合や、運用ポリシーの変更の場面によって通信の正常状態が刻々と変化していく場合である。非特許文献１に記載の技術の場合、運用中のネットワークの正常状態に変化があると、再度学習フェーズに切り替え、正常状態の定義のアップデートが必要となる。

[0015] ここで、非特許文献１記載の技術を用いる場合には、再学習を行う際に学習フェーズ時に異常が混入していないことの担保、つまり、再学習の学習フェーズの健全性の担保が難しいという課題がある。

[0016] このような課題に対し、非特許文献２記載の技術のように、個々の機器を監視する仕組みとし、接続機器ごとに正常状態を作る処理を行えば、機器ごとのフェーズ切り替えにより、学習フェーズ中の脆弱な期間を機器毎に極小化はできる。しかしながら、非特許文献２記載の技術でも、再学習において学習フェーズの健全性の担保が難しいという課題がある点は、非特許文献１に記載の技術とは何ら変わりない。

[0017] また、非特許文献１記載の技術と非特許文献２記載の技術において、仮に学習フェーズ中に異常の検知ができたとしても、この検知が本当の異常によるものか、誤って正常を検知してしまったものかを分析し、正常状態に取り込むか否かを判断しなければ、学習フェーズが進められないため、学習期間が長期化するという課題も潜在している。

[0018] 本発明は、上記に鑑みてなされたものであって、異常通信を検知する際の学習フェーズをよりセキュアに実行する通信システム及び通信方法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

[0019] 上述した課題を解決し、目的を達成するために、本発明に係る通信システムは、第１のネットワークと、第２のネットワークとを有する通信システムであって、第１のネットワークは、第１の通信装置と、第１の通信装置に正常状態のテスト通信を送信し、第１の通信装置による通信を受信する通信テストを行うテスト装置と、テスト通信と第１の通信装置による通信とを学習して第１の通信装置の異常通信を検知する初期モデルを生成し、初期モデルを第２のネットワークに送信する第１のサーバ装置と、を有し、第２のネットワークは、第１の通信装置と同型の第２の通信装置と、第１のサーバ装置から受信した初期モデルを用いて第２の通信装置の通信を監視しながら、第２の通信装置の通信を学習して第２の通信装置の異常通信を検知する第１のモデルを生成する第２のサーバ装置と、有することを特徴とする。

発明の効果

[0020] 本発明によれば、異常通信を検知する際の学習フェーズをよりセキュアに実行する。

図面の簡単な説明

[0021] [図1]図１は、実施の形態１における通信システムの構成の一例を示す図である。

[図2]図２は、図１に示す学習・検知サーバの構成の一例を示すブロック図である。

[図3]図３は、図１に示す通信システムにおける処理の流れについて説明する図である。

[図4]図４は、図１に示すステージング用ネットワークにおけるホストに対する通信及び学習の状態を模式的に示した図である。

[図5]図５は、図１に示す運用ネットワークにおけるホストに対する通信及び監視の状態を模式的に示した図である。

[図6]図６は、実施の形態１に係る通信処理の処理手順を示すシーケンス図である。

[図7]図７は、従来技術による学習・検知サーバにおけるホストに対する通信及び監視の状態を模式的に示した図である。

[図8]図８は、実施の形態２における通信処理の流れについて説明する図である。

[図9]図９は、モデルが学習した通信とホストの通信との関係を示す図である。

[図10]図１０は、実施の形態２におけるステージング用ネットワークにおけるホストに対する通信、学習及び監視の状態を模式的に示した図である。

[図11]図１１は、モデルが学習した通信とホストの通信との関係を示す図である。

[図12]図１２は、実施の形態２におけるステージング用ネットワークにおけるホストに対する通信、学習及び監視の状態を模式的に示した図である。

[図13]図１３は、実施の形態２に係る通信処理の処理手順を示すシーケンス図である。

[図14]図１４は、モデルが学習した通信とホストの通信との関係を示す図である。

[図15]図１５は、モデルが学習した通信とホストの通信との関係を示す図である。

[図16]図１６は、実施の形態３における運用ネットワークにおけるホストに対する通信、学習及び監視の状態を模式的に示した図である。

[図17]図１７は、実施の形態３に係る通信処理の処理手順を示すシーケンス図である。

[図18]図１８は、従来技術における通信の監視及び過検知通信の学習について説明する図である。

[図19]図１９は、実施の形態３における通信の監視及び過検知通信の学習について説明する図である。

[図20]図２０は、プログラムが実行されることにより、学習・検知サーバ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

[0022] 以下、図面を参照して、本発明の一実施形態を詳細に説明する。なお、この実施の形態により本発明が限定されるものではない。また、図面の記載において、同一部分には同一の符号を付して示している。

[0023] ［実施の形態１］

まず、本発明の実施の形態１について説明する。図１は、実施の形態１における通信システムの構成の一例を示す図である。

[0024] 図１に示すように、実施の形態１に係る通信システム１００は、ステージング用ネットワーク１（第１のネットワーク）と、運用ネットワーク２（第２のネットワーク）とを有する。

[0025] 運用ネットワーク２は、実際にＩｏＴ機器等が運用されるシステム環境である。運用ネットワーク２は、ホスト５ａ，５ｂ，５ｃ（第２の通信装置）と、学習・検知サーバ８（第２のサーバ装置）とを有する。

[0026] ホスト５ａ，５ｂ，５ｃは、ＩｏＴ機器等の通信装置である。なお、複数のホスト５ａ，５ｂ，５ｃのそれぞれを区別することなく総称する場合に単にホスト５と記載する。また、図１に例示された運用ネットワーク２は、３台のホスト５ａ，５ｂ，５ｃを有するが、ホスト５の台数は、一以上であればよい。

[0027] 学習・検知サーバ９は、正常通信を学習したモデルを用いて、ホスト５ａ，５ｂ，５ｃの通信の異常を検知する。学習・検知サーバ９は、正常通信を

学習してモデルを生成する。学習・検知サーバ９は、学習・検知サーバ８（後述）と同じ機能を有し、モデルを相互に交換できる。学習・検知サーバ９は、学習・検知サーバ８から受信した初期モデルを用いてホスト５ａ，５ｂ，５ｃの通信を監視しながら、５ａ，５ｂ，５ｃの通信を学習して５ａ，５ｂ，５ｃの異常通信を検知する第１のモデルを、５ａ，５ｂ，５ｃごとに生成する。

[0028] ステージング用ネットワーク１は、運用ネットワーク２と類似するシステム環境であり、検証用（テスト用）に使用される。ステージング用ネットワーク１は、ホスト５と同型のホスト４ｔ（第１の通信装置）と、テスト実行サーバ３（テスト装置）と、学習・検知サーバ８（第１のサーバ装置）とを有する。

[0029] テスト実行サーバ３は、テスト機器であるホスト４ｔに、正常状態のテスト通信を送信し、ホスト４ｔによる通信を受信する通信テストを行う。

[0030] 学習・検知サーバ８は、テスト実行サーバ３によるテスト通信及びホスト４ｔから発生した通信を学習してホスト４ｔの異常通信を検知する初期モデルを生成する。学習・検知サーバ８は、初期モデルを学習・検知サーバ９に送信する。

[0031] なお、本実施の形態１において、ステージング用ネットワーク１における学習・検知サーバ８と学習・検知サーバ９とにおけるモデルの交換のうち、ステージング用ネットワーク１の学習・検知サーバ８から運用ネットワーク２の学習・検知サーバ９への受け渡しをインポートとし、その逆方向をエクスポートとする。

[0032] 実施の形態１に係る通信システム１００では、ステージング用ネットワーク１において、ホスト５と同型のホスト４ｔを用いて初期モデルを事前に生成しておく。通信システム１００では、監視対象機器であるホスト５が運用ネットワーク２で実際に使用される際に、事前生成した初期モデルを、ステージング用ネットワーク１から運用ネットワーク２へインポートする。

[0033] そして、運用ネットワーク２では、この初期モデルを、各通信装置の通信

の監視に使用しながら、ホスト５の通信を学習して、ホスト５ごとに第１のモデルを生成する。これによって、通信システム１００では、検知フェーズと学習フェーズとの同時実行を可能とし、学習フェーズ中の脆弱な期間の発生を抑止してリスクを低減している。

[0034] ［学習・検知サーバの構成］

次に、学習・検知サーバ８，９の構成について説明する。図２は、図１に示す学習・検知サーバ８，９の構成の一例を示すブロック図である。図２に示すように、学習・検知サーバ８，９は、通信部１１、記憶部１２及び制御部１３を有する。

[0035] 通信部１１は、ネットワーク等を介して接続された他の装置との間で、各種情報を送受信する通信インタフェースである。通信部１１は、ＮＩＣ（Network Interface Card）等で実現され、ＬＡＮ（Local Area Network）やインターネットなどの電気通信回線を介した他の装置と制御部１３（後述）との間の通信を行う。

[0036] 記憶部１２は、例えば、ＲＡＭ（Random Access Memory）、フラッシュメモリ（Flash Memory）等の半導体メモリ素子、又は、ハードディスク、光ディスク等の記憶装置によって実現され、学習・検知サーバ８，９を動作させる処理プログラムや、処理プログラムの実行中に使用されるデータなどが記憶される。記憶部１２は、モデル１２１を有する。モデル１２１は、ホスト４ｔ，５の通信を学習して、ホスト４ｔ，５の異常通信を検知するために使用される。モデル１２１は、異常通信検知のために使用される演算式やパラメータを含む。

[0037] 制御部１３は、学習・検知サーバ８，９全体を制御する。制御部１３は、各種の処理手順などを規定したプログラム及び所要データを格納するための内部メモリを有し、これらによって種々の処理を実行する。例えば、制御部１３は、ＣＰＵ（Central Processing Unit）やＭＰＵ（Micro Processing Unit）などの電子回路である。また、制御部１３は、各種のプログラムが動作することにより各種の処理部として機能する。制御部１３は、学習部１

３１、監視・検知部１３２及びモデル送受信部１３３を有する。

[0038] 学習部１３１は、ホスト４ｔ，５の通信をキャプチャして、ホスト４ｔ，５の通信を学習し、モデルの生成、或いは、モデルの更新を行う。学習部１３１は、生成したモデルのモデルパラメータ、或いは、更新したモデルのモデルパラメータを記憶部１２に格納する。

[0039] ここで、学習・検知サーバ８の場合、学習部１３１は、テスト実行サーバ３による通信テスト実行時に、テスト実行サーバ３によるテスト通信及びホスト４ｔから発生した通信を学習してホスト４ｔの異常通信を検知する初期モデルを生成する。また、学習・検知サーバ９の場合、学習部１３１は、ホスト５の通信を学習してホスト５の異常通信を検知する第１のモデルをホスト５ごとに生成する。

[0040] 監視・検知部１３２は、モデル１２１を用いて、ホスト４ｔ，５の通信を監視し、異常通信を検知する。

[0041] モデル送受信部１３３は、学習部１３１が生成したモデルを、他方の学習・検知サーバ８，９に送信する。また、モデル送受信部１３３は、他方の学習・検知サーバ８，９が生成したモデルを受信する。

[0042] ［全体の処理の流れ］

次に、通信システム１００における処理の流れについて説明する。図３は、図１に示す通信システム１００における処理の流れについて説明する図である。

[0043] まず、ステージング用ネットワーク１では、学習・検知サーバ８は、テスト実行サーバ３によるテスト通信、及び、テスト実行サーバ３によるホスト４ｔへの通信テストによってホスト４ｔから発生した通信を学習する。具体的には、学習・検知サーバ８は、テスト実行サーバ３によるテストシナリオとホスト４ｔとを用いて、運用ネットワーク２用の最新の初期モデルｔ０を生成する（図３の（１）参照）。続いて、学習・検知サーバ８は、最新の初期モデルを、運用ネットワーク２の学習・検知サーバ９にインポートする（図３の（２）参照）。

[0044] そして、運用ネットワーク２では、学習・検知サーバ９が、新ホスト（図ではホスト５ａ）の接続時に、ホスト５ａの通信を、最新の初期モデルｔ０を使って監視しながら、ホスト４ａ用のモデルａ１（第１のモデル）を生成する（図３の（３）参照）。そして、学習・検知サーバ９は、生成したモデルａ１を用いて、ホスト５ａの通信を監視し、異常通信の検知を行う。

[0045] ［ステージング用ネットワークの処理の流れ］

次に、ステージング用ネットワーク１における初期モデルの生成処理の流れについて説明する。図４は、図１に示すステージング用ネットワーク１におけるホスト４ｔに対する通信及び学習の状態を模式的に示した図である。

[0046] 図４以降の同様の図は、縦軸に時間軸を取った図で、上段に記載しているホストにおける通信・監視状態を模式的に表している。図４以降の同様の図は、時間軸に沿って、ホストに対する状況のうち、ホストに対する試験の状況を「試験状況」ラベルを振ったレーン（以降、「試験状況レーン」）、通信に関する状況を「通信状況」ラベルを振ったレーン（以降、「通信状況レーン」）、監視に関する状況を「監視状況」ラベルを振ったレーン（以降、「監視状況レーン」）、検知に関する状況を「検知状況」ラベルを振ったレーン（以降、「検知状況レーン」）に分けて、通信、学習、監視・検知の状況を説明する。図４以降の図において、モデルに取り込んだ通信は黒丸を始点とする矢印（例えば、通信区間Ｐ３－１から左に伸びる矢印）で表現している。

[0047] 図４に示すように、ステージング用ネットワーク１では、運用ネットワーク２での動作確認をするため、一般に、運用ネットワーク２のホスト５と同型機であるホスト４ｔを用いた全機能を網羅的にチェックする総合的なテストが行われる。

[0048] まず、図４の「試験状況レーン」では、テスト用のホスト４ｔへのテスト通信に関する試験シナリオＴ０が示され、テスト実行サーバ３は、この試験シナリオＴ０が行われた期間を、試験期間Ｐ２－１として、全機能を網羅的にチェックする総合的なテスト通信を行う。この際に、ホスト４ｔが発生す

る通信は「通信状況レーン」の通信区間Ｐ３－１に示す。

[0049] そして、学習・検知サーバ８は、通信区間Ｐ３－１の通信を取り込むことによって、「学習状況レーン」に示すように、初期モデルｔ０を生成する（図４の（１）参照）。この初期モデルｔ０は、運用ネットワーク２のモデルのテンプレートにあたるものとなる。

[0050] ［運用ネットワークの処理の流れ］

次に、運用ネットワーク２における監視及びモデル生成の処理の流れについて説明する。図５は、図１に示す運用ネットワーク２におけるホスト５ａに対する通信及び監視の状態を模式的に示した図である。

[0051] 図５に示すように、学習・検知サーバ９は、「監視状況レーン」の通信区間Ｐ２－２の間のホスト５ａの通信を、図４で生成した初期モデルｔ０を使用して監視している（図５の（１）参照）。この初期モデルｔ０の受け渡しは、ステージング用ネットワーク１の学習・検知サーバ８と運用ネットワーク２の学習・検知サーバ９との間の通信により、ステージング用ネットワーク１から運用ネットワーク２にインポートされることで実現される。

[0052] これにより、図５では、学習・検知サーバ９は、初期モデルｔ０を使用して通信区間Ｐ２－２におけるホスト５ａの通信を監視しながら、運用ネットワーク２で実際に、自装置とホスト５ａとの間の通信を取り込んでモデルａ１を生成する（図５の（２）参照）。その後の通信期間Ｐ３－２以降、学習・検知サーバ９は、生成したモデルａ１を使用して、ホスト５ａの通信を監視する（図５の（３）参照）。

[0053] ［通信処理の処理手順］

図６は、通信システム１００における処理の流れについて説明する。図６は、実施の形態１に係る通信処理の処理手順を示すシーケンス図である。

[0054] まず、ステージング用ネットワーク１では、学習・検知サーバ８は、テスト実行サーバ３によるテスト通信（ステップＳ１）によって発生したホスト４ｔとテスト実行サーバ３との間の通信（ステップＳ２）をキャプチャし（ステップＳ３）、ホスト４ｔの通信を学習して初期モデルを生成する（ステ

ップＳ４）。

[0055] 運用ネットワーク２では、学習・検知サーバ９は、ホスト状況を確認し（ステップＳ５）、新規ホスト追加または監視外のホストを発見したかを判定する（ステップＳ６）。学習・検知サーバ９は、新規ホスト追加及び監視外のホストを発見していないと判定した場合（ステップＳ６：Ｎｏ）、ステップＳ５に戻り、ホスト状況の確認を継続する。

[0056] これに対し、学習・検知サーバ９が、新規ホスト追加または監視外のホストを発見したと判定した場合（ステップＳ６：Ｙｅｓ）について説明する。この場合、学習・検知サーバ９は、ステージング用ネットワーク１から初期モデルのインポートを受け（ステップＳ７）、この初期モデルを用いて、新たなホスト５と他の装置（例えば、第１の通信先の装置）との間の通信（ステップＳ８－１）をキャプチャして（ステップＳ８－２）監視しながら、ホスト５のモデルを生成する（ステップＳ９）。

[0057] 学習・検知サーバ９は、ホスト５のモデル生成後、生成したホスト５のモデルを用いて、ホスト５と第１の通信先の装置との間の通信（ステップＳ１０－１）をキャプチャして（ステップＳ１０－２）、ホスト５の通信を監視し（ステップＳ１１）、異常通信の検知を行う。

[0058] ［実施の形態１の効果］

ここで、従来技術について説明する。図７は、従来技術による学習・検知サーバにおけるホストｘに対する通信及び監視の状態を模式的に示した図である。図７に示すように、従来の学習・検知サーバは、新規接続・通信を開始したホストｘに対し、「学習状況レーン」に示すように通信区間Ｐ２－３でホストｘの通信を取り込んでモデルｘ１を生成する（図７の（１）参照）。その後、従来の学習・検知サーバは、「監視状況レーン」に示すように、モデルｘ１を用いて、「通信状況レーン」の通信区間Ｐ５－３の通信を監視することによって（図７の（２）参照）、異常通信の有無を検知する。したがって、従来技術では、学習を行っている際に通信の監視は行っておらず、学習終了後から、通信の監視を実行するため、学習フェーズ中に脆弱な期間

が発生するという問題があった。

[0059] これに対し、本実施の形態１では、予め、ステージング用ネットワーク１において、運用ネットワーク２のホスト５と同型のホスト４ｔに対するテスト通信を学習してホスト４ｔ用の初期モデルを生成している。本実施の形態１では、この初期モデルが運用ネットワーク２にインポートされ、学習・検知サーバ９は、この初期モデルｔ０を用いてホスト５ａの通信も監視しながら、ホスト５ａの通信を学習してホスト５ａに対応するモデルａ１を生成する。したがって、学習・検知サーバ９は、学習フェーズ中も監視を実行するため、学習フェーズ中の脆弱な期間の発生を抑止でき、異常通信を検知する際の学習フェーズをよりセキュアに実行することができる。

[0060] ［実施の形態２］

次に、実施の形態２について説明する。実施の形態２では、実施の形態１で説明した初期モデルをさらに高精度化する方法について説明する。実施の形態２に係る通信システムは、実施の形態１に係る通信システム１００と同じ構成を有する。

[0061] ［全体の処理の流れ］

次に、実施の形態２における通信処理の流れについて説明する。図８は、実施の形態２における通信処理の流れについて説明する図である。図８では、学習・検知サーバ９が、生成したモデルａ１を用いて、ホスト５ａ，５ｂ，５ｃの通信を監視した後の処理について説明する。すなわち、学習・検知サーバ９では、ホスト５ａ，５ｂ，５ｃのモデルが完成している状態である（図８の（１）参照）。この状態において、学習・検知サーバ９は、ホスト５ａ，５ｂ，５ｃのモデル（ａ１，ｂ１，ｃ１）を、ステージング用ネットワーク１の学習・検知サーバ８にエクスポートする（図８の（２）参照）。

[0062] 学習・検知サーバ８は、テスト実行サーバ３によるテストシナリオと、ホスト５ａ，５ｂ，５ｃのモデル（ａ１，ｂ１，ｃ１）を使って、より精度の高い初期モデルを生成する（図８の（３）参照）。言い換えると、学習・検知サーバ８は、テスト実行サーバ３によるテストシナリオと、ホスト４ｔを

使って、運用ネットワーク２用の初期モデル（ｔ１）を生成して、初期モデルを最新化する（図８の（４）参照）。そして、学習・検知サーバ８は、生成した最新の初期モデルｔ１を学習・検知サーバ９にインポートする（図８の（５）参照）。

[0063] 続いて、学習・検知サーバ９は、新ホスト（図８ではホスト５ｎ）接続時に、最新の初期モデルｔ１でホスト５ｎの通信を監視しながら、ホスト５ｎ用のモデルを生成する（図８の（６）参照）。すなわち、学習・検知サーバ９は、新たに接続するホスト５ｎについては、新しい初期モデルを使って、監視しながら、学習をする（図８の（７）参照）。

[0064] このように、本実施の形態２では、ステージング用ネットワーク１は、運用ネットワーク２からエクスポートされた各ホスト５のモデルを用いて、初期モデルを最新化し、最新の初期モデルを運用ネットワーク２にインポートする。

[0065] ここで、実施の形態１においても説明したように、ステージング用ネットワーク１のホスト４ｔと同型の機器であれば、運用ネットワーク２のホスト５導入時に、ステージング用ネットワーク１で生成した初期モデルｔ０を運用ネットワーク２にインポートしてくることで、学習フェーズ中も、この初期モデルｔ０を用いて、通信を監視することができる。

[0066] ただし、実施の形態１では、初期モデルは、ホスト４ｔの全機能の網羅的なテスト通信に応じた全通信を用いて生成しているため、運用ネットワーク２では実際には使われない通信も学習として取り込まれている。図９は、モデルが学習した通信とホストの通信との関係を示す図である。

[0067] 具体的には、図９に示すテスト中にテスト実行サーバ３によるテスト通信及びホスト４ｔが発生する通信群Ｇｔが、初期モデルｔ０の入力情報となる。この通信群Ｇｔの通信のうち、通信Ｃｔは、運用中に、実際にホスト５ａが発生する通信群Ｇａに含まれる通信であり、テストトラフィック中、真に監視が必要な通信である。

[0068] これに対し、通信Ｃｊは、通信群Ｇａに含まれない通信であり、運用中に

は使用されない未使用機能であるため、正常状態に含めないでよい通信である。この通信Ｃｊは、初期モデルを使って監視した場合には、正常なものと識別される通信であるものの、仮に、この通信Ｃｊと同様の通信を介してサイバー攻撃が行われた場合、見逃しのリスクとなってしまう。言い換えると、通信Ｃｊは、運用ネットワーク２では未使用機能であるため、ステージング用ネットワーク１のモデル生成時においても、正常状態に含めるべきではない通信となる。

[0069] このため、本実施の形態２では、ステージング用ネットワーク１において２回目以降に初期モデルを生成する場合、この通信Ｃｊを、初期モデルｔ１の学習対象から排除することによって、初期モデルの精度を上げている。具体的に、図１０を参照して、ステージング用ネットワーク１における初期モデルｔ１生成について説明する。図１０は、実施の形態２におけるステージング用ネットワーク１におけるホスト４ｔに対する通信、学習及び監視の状態を模式的に示した図である。

[0070] 図１０に示すように、学習・検知サーバ８が、運用ネットワーク２で生成したホスト５ａのモデルａ１を使用し、新しい初期モデルｔ１を生成するまでの処理を示す。まず、図１０の「監視状況レーン」に示すように、モデルａ１は、運用ネットワーク２からステージング用ネットワーク１にエクスポートしてきたモデルであり、ステージング用ネットワーク１の通信の監視に使用される。

[0071] そして、試験シナリオＴ０の実施によって、学習・検知サーバ８は、試験区間Ｐ３－４の間のホスト４ｔの通信のうち、モデルａ１を使って抽出される通信、つまり、モデルａ１で正常とは異なるものと識別される通信Ｃｊ４を検知する。図１０の例では、学習・検知サーバ８は、「検知状況レーン」にあるように、テスト通信のうち「テストｎでの検知」や「テストｎ＋１での検知」というように、通信Ｃｊ４がどのテストにより発生させられたかを、テスト実行サーバ３との連携により識別できる（図１０の（１）参照）。

[0072] したがって、学習・検知サーバ８は、モデルａ１でホスト４ｔの通信を監

視することによって、モデルａ１において異常通信と検知される通信Ｃｊ４を抽出できる。

[0073] 続いて、テスト実行サーバ３は、試験シナリオＴ０から、通信Ｃｊ４を発生するテストを除外した（図１０の（２）参照）試験シナリオＴ１を作成する。そして、学習・検知サーバ８は、「試験状況レーン」に示すように、試験シナリオＴ１の実施によって、試験区間Ｐ６－４の間のホスト４ｔの通信から初期モデルｔ１を生成する（図１０の（４）参照）。この試験区間Ｐ６－４に対応する通信区間Ｐ２－２の間のホスト４ｔの通信に対し、モデルａ１の検知はない（図１０の（３）参照）。したがって、学習・検知サーバ８は、不要な通信Ｃｊ４が学習に取り込まれていない、初期モデルｔ０より高精度の初期モデルｔ１を生成できる。

[0074] 図１１は、モデルが学習した通信とホストの通信との関係を示す図である。図１１に示すように、初期モデルｔ１は、図１１の領域Ａｔの通信から生成されたモデルとなる。すなわち、初期モデルｔ１は、ホスト４ｔが発生する通信群Ｇｔのうち、不要な通信Ｃｊを除外した、真に監視が必要な通信Ｃｔのみが含まれる領域Ａｔの通信を入力として生成される。

[0075] 学習・検知サーバ８は、この最新の初期モデルｔ１を運用ネットワーク２にインポートし、運用ネットワーク２において新たに接続されるホスト５ｎのモデルとして使用することによって、運用ネットワーク２において、より適切に監視を行いながら安全にモデルを生成することができる。

[0076] なお、図１０では、ホスト５ａのモデルａ１を用いて初期モデルを最新化する場合を例として示したが、もちろんこれに限らない。図１２は、実施の形態２におけるステージング用ネットワーク１におけるホスト４ｔに対する通信、学習及び監視の状態を模式的に示した図である。

[0077] ステージング用ネットワーク１では、学習・検知サーバ８は、図１２のように３つのホスト５ａ，５ｂ，５ｃのそれぞれが生成したモデルａ１，ｂ１，ｃ１がエクスポートされた場合、この３つのモデルａ１，ｂ１，ｃ１を使用し、図１０と同様の処理を行うことで、ホスト群の特徴をより抜き出した

初期モデルｔ１を生成することが可能となる。

[0078] 例えば、試験シナリオＴ０の実施によって、学習・検知サーバ８は、試験区間Ｐ３－４の間のホスト４ｔの通信のうち、モデルａ１，ｂ１，ｃ１を使って検知される通信Ｃｊ４ａ，Ｃｊ４ｂ，Ｃｊ４ｃを検知する。図１２の例では、学習・検知サーバ８は、「検知状況レーン」にあるように、モデルａ１はテストｍで通信ＣＪ４ａを検知し、モデルｂ１はテストｍ＋１で通信Ｃｊ４ｂを検知し、モデルｃ１はテストｍ＋２で通信Ｃｊ４ｃを検知したことを識別できる（図１２の（１－ａ），（１－ｂ），（１－ｃ）参照）。

[0079] 続いて、テスト実行サーバ３は、試験シナリオＴ０から、通信Ｃｊ４ａ～Ｃｊ４ｃを発生するテストを除外した（図１２の（２）参照）試験シナリオＴ１を作成する。そして、学習・検知サーバ８は、「試験状況レーン」に示すように、試験シナリオＴ１の実施によって、試験区間Ｐ６－４の間のホスト４ｔの通信から初期モデルｔ１を生成する。これによって、学習・検知サーバ８は、不要な通信Ｃｊ４ａ，Ｃｊ４ｂ，Ｃｊ４ｃが学習に取り込まれていない初期モデルｔ１であって、初期モデルｔ０より精度の高い初期モデルｔ１を生成できる（図１２の（４）参照）。この試験区間Ｐ６－４の間のホスト４ｔの通信に対し、モデルａ１，ｂ１，ｃ１の検知はない（図１２の（３－ａ，３－ｂ，３－ｃ）参照）。

[0080] ［通信処理の処理手順］

次に、実施の形態２における通信処理の流れについて説明する。図１３は、実施の形態２に係る通信処理の処理手順を示すシーケンス図である。

[0081] 図１３に示すステップＳ２１～ステップＳ３１は、図６に示すステップＳ１～ステップＳ１１と同じ処理内容である。そして、学習・検知サーバ９は、生成したモデルを学習・検知サーバ８にエクスポートする（ステップＳ３２）。

[0082] 続いて、ステージング用ネットワーク１では、学習・検知サーバ８は、テスト実行サーバ３によるホスト４ｔへのテスト通信（ステップＳ３３）によって発生したホスト４ｔとテスト実行サーバ３との間の通信（ステップＳ３

４）をキャプチャし（ステップＳ３５）、ホスト４ｔの通信を、学習・検知サーバ９が生成したモデルを用いて監視する（ステップＳ３６）。

[0083] そして、学習・検知サーバ８は、学習・検知サーバ９が生成したモデルが検知した通信があるか否かを判定する（ステップＳ３７）。学習・検知サーバ８は、学習・検知サーバ９が生成したモデルが検知した通信があると判定した場合（ステップＳ３７：Ｙｅｓ）、検知した通信をテスト実行サーバ３に通知する（ステップＳ３８）。

[0084] テスト実行サーバ３は、学習・検知サーバ９が生成したモデルが検知した通信をテスト通信から除外し（ステップＳ３９）、テスト通信を行う（ステップＳ４０）。これに応じて、学習・検知サーバ８は、ホスト４ｔとテスト実行サーバ３との間の通信（ステップＳ４１）とをキャプチャする（ステップＳ４２）。学習・検知サーバ８は、学習・検知サーバ９が生成したモデルでホスト４ｔの通信を監視しながら、ホスト４ｔの通信を学習して最新の初期モデルを生成する（ステップＳ４３）。

[0085] 運用ネットワーク２では、学習・検知サーバ９は、ホスト状況を確認し（ステップＳ４４）、新規ホスト追加または監視外のホストを発見したかを判定する（ステップＳ４６）。学習・検知サーバ９は、新規ホスト追加及び監視外のホストを発見していないと判定した場合、ステップＳ４４に戻り、ホスト状況の確認を継続する。

[0086] これに対し、学習・検知サーバ９は、ホスト５ｎの新規接続（ステップＳ４５）によって、新規ホスト追加または監視外のホストを発見したと判定した場合について説明する。この場合、学習・検知サーバ９は、ステージング用ネットワーク１から最新の初期モデルのインポートを受け（ステップＳ４７）、この初期モデルを用いて、新たなホスト５ｎと他の装置（例えば、第２の通信先の装置）と間の通信（ステップＳ４８－１）をキャプチャして（ステップＳ４８－２）監視しながら、ホスト５ｎのモデルを生成する（ステップＳ４９）。続いて、学習・検知サーバ９は、生成したホスト５ｎのモデルを用いて、ホスト５ｎと例えば、第２の通信先の装置との間の通信（ステ

ップＳ５０－１）をキャプチャして（ステップＳ５０－２）、ホスト５ｎの通信を監視し（ステップＳ５１）、異常通信の検知を行う。

[0087] ［実施の形態２の効果］

このように、実施の形態２では、運用ネットワーク２の学習・検知サーバ９は、自装置が生成したホスト５のモデル（第１のモデル）を、ステージング用ネットワーク１の学習・検知サーバにエクスポートする。そして、テスト実行サーバ３は、第１の通信テストを行う。この際、学習・検知サーバ８は、第１のモデルを用いて、第１の通信テストにおいてテスト通信とホスト４ｔによる通信とから異常通信を検知する。そして、テスト実行サーバ３は、学習・検知サーバ８が異常通信として検知したテスト通信を除外して第２の通信テストを行う。そして、学習・検知サーバ８は、第２の通信テストにおいてテスト通信とホスト４ｔによる通信とを学習して新たな初期モデルを生成して、新たな初期モデルを学習・検知サーバ９にインポートする。

[0088] したがって、実施の形態２では、運用中には使用されない未使用機能であるため正常状態に含めないでよい通信を、初期モデルの学習対象から排除することによって、初期モデルの精度を向上することができる。

[0089] ［実施の形態３］

次に、実施の形態３について説明する。実施の形態３では、運用ネットワーク２において、監視・検知処理の過程において異常と検知された正常な過検知通信が発生した場合であっても、学習・検知サーバ９における学習フェーズ完了の長期化を防止しながら過検知通信を学習・検知する方法について説明する。実施の形態３に係る通信システムは、実施の形態１に係る通信システム１００と同じ構成を有する。実施の形態３では、運用ネットワーク２におけるホストとしてホスト５ｄ，５ｅが接続された場合を例に説明する。

[0090] 実施の形態１，２では、ホスト５の運用ネットワーク２のホスト５の通信として、ホスト４ｔの全機能を網羅的にチェックする総合的なテストによりホスト４ｔから発生する通信のサブセットを基にする場合の例を示した。しかしながら、運用ネットワーク２によっては、その運用ネットワーク２特有

の通信が発生することが考えられる。例えば、既に運用ネットワーク２に監視システムが存在しており、新規に接続したホスト５に対し、ヘルスチェックの通信や、メンテナンスなどの普段とは違う機能の使い方による普段とは異なる通信が発生する場合である。

[0091] この状況を、運用ネットワーク２に新たにホスト４ｄとホスト４ｅが接続した場合を例に説明する。図１４は、モデルが学習した通信とホスト４ｄの通信との関係を示す図である。図１５は、モデルが学習した通信とホスト４ｅの通信との関係を示す図である。

[0092] 図１４及び図１５は、学習・検知サーバ９が、ステージング用ネットワーク１からインポートしてきた初期モデルｔ１を使用して監視をしている場合を想定する。領域Ａｄ，Ａｅは、ステージング用ネットワーク１からインポートされた最新の初期モデルｔ１が学習した通信の集合であり、初期モデルｔ１に入力された通信情報である。前述のように、運用ネットワーク２によっては、その運用ネットワーク２特有の通信が発生することが考えられる。例えば、運用中に実際にホスト５ｄ，５ｅが発生する通信群Ｇｄ，Ｇｅ内の通信Ｃｄ，Ｃｅは、運用中にホスト４ｄおよびホスト４ｅに対して特有の使い方をした場合に発生する通信である。しかしながら、これらの通信Ｃｄ，Ｃｅは、初期モデルｔ１の入力情報には含まれない。

[0093] この結果、学習・検知サーバ９が、初期モデルｔ１を用いて監視・検知を行った場合、通信Ｃｄ，Ｃｅは、異常ではないのに異常と判断される通信として検知されてしまうことになる。この通信Ｃｄ，Ｃｅは、本来なら異常として検知されるべきではない通信である。以降、このような通信Ｃｄ，Ｃｅを、過検知通信とする。

[0094] ここで、過検知通信は、正常状態として学習すべき通信である。具体的には、学習・検知サーバ９は、ホスト５ｄでの過検知通信を、ホスト５ｄのモデルに取り込み、ホスト５ｅでの過検知通信は、ホスト５ｅのモデルに取り込んで学習することによって、その後の過検知通信を抑制することができる。

[0095] しかしながら、学習・検知サーバ９が、過検知通信を各ホスト５のモデルに取り込んで学習する場合、モデルへ取り込みまでに一定のタイムラグが発生する。これは、所定の分析装置において、検知された通信を分析し、異常であるか過検知通信であるかを識別してから、過検知通信であることが判明した後に、この通信を学習に取り込むためである。このタイムラグの発生が、学習フェーズの長期化を招くことになる。以降、この学習フェーズ完了までのタイムラグを「遅延問題」と呼ぶこととする。この遅延問題は、モデルの完成が遅れる、つまり、より新しいモデルでの監視の開始が遅れるという影響を及ぼす。そこで、本実施の形態３では、この遅延問題を発生させず過検知通信の抑止も行う方法を提案する。

[0096] ［運用ネットワークにおける処理の流れ］

図１６は、実施の形態３における運用ネットワーク２におけるホスト５ｄ，５ｅに対する通信、学習及び監視の状態を模式的に示した図である。図１６の模式図のうち、左図は、学習・検知サーバ９における運用ネットワーク全体に対する学習状況及び監視状況を示し、中央図は、学習・検知サーバ９におけるホスト５ｄに対する学習状況及び監視状況を示し、右図は、学習・検知サーバ９におけるホスト５ｅに対する学習状況及び監視状況を示す。

[0097] 図１６の中央図及び右図に示すように、学習・検知サーバ９は、通信区間Ｐ１－５，Ｐ２－５の間のホスト５ｄ，５ｅの通信を、ステージング用ネットワーク１において生成された最新の初期モデルｔ１を使用して監視しながら、ホスト５ｄ，５ｅの通信を取り込んでモデルｄ´１，ｅ´１を生成する。この際、通信区間Ｐ１－５，Ｐ２－５において、初期モデルｔ１によって、通信Ｃｄ１，Ｃｄ２，Ｃｅ１，Ｃｅ２が異常であると検知される。なお、図１６の例では、学習・検知サーバ９は、「検知状況レーン」にあるように、通信Ｃｄ１，Ｃｅ１が初期モデルｔ１によって「トラフィックｒ１で検知」されたこと、通信Ｃｄ２が初期モデルｔ１によって「トラフィックｓ１で検知」されたこと、及び、通信Ｃｅ２が初期モデルｔ１によって「トラフィックｓ６で検知」されたことを識別できるものとする（図１６の（１－ｄ１

），（１－ｄ２），（１－ｅ１），（１－ｅ２）参照）。

[0098] 学習・検知サーバ９は、中央図及び右図に示すように、５ｄ，５ｅの通信のうち、初期モデルｔ１によって検知された通信Ｃｄ１，Ｃｄ２，Ｃｅ１，Ｃｅ２は学習に含めずに（図１６の（２－ｄ），（２－ｅ）参照）、各ホスト５ｄ，５ｅに対するモデルを生成する（図１６の（３－ｄ），（３－ｅ）参照）。すなわち、学習・検知サーバ９は、５ｄ，５ｅの通信から、初期モデルｔ１を用いて異常通信と検知された通信を除外した通信を学習して、ホスト５ｄ用のモデルｄ´１（第１のモデル）及びホスト５ｅ用のモデルｅ´１（第１のモデル）を生成する。そして、学習・検知サーバ９は、それぞれ生成したモデルｄ´１及びホスト５ｅ用のモデルｅ´１を用いて、ホスト５ｄ，５ｅを監視する。

[0099] さらに、学習・検知サーバ９は、左図に示すように、運用ネットワーク２全体について、初期モデルｔ１によって異常通信であると検知された通信が過検知通信の場合に、この過検知通信である通信Ｃｄ，Ｃｅを学習して、過検知通信以外の異常通信を検知するモデルｕ１（第２のモデル）を生成する（図１６の（４），（５）参照）。

[0100] そして、学習・検知サーバ９は、運用ネットワーク２全体については、モデルｕ１を用いて、運用ネットワーク２全体の通信を監視する（図１６の（６）参照）。したがって、図１６に示す例では、最終的に、学習・検知サーバ９は、運用ネットワーク２全体については、モデルｕ１による監視を行い（通信区間Ｐ７－５参照）、ホスト５ｄについては、モデルｄ’１による監視を行い（通信区間Ｐ３－５参照）、ホスト５ｅについては、モデルｅ’１による監視を行う（通信区間Ｐ９－５参照）。

[0101] 具体的な監視の処理は、学習・検知サーバ９は、ホスト５ｄ，５ｅの通信を、過検知通信を学習したモデルｕ１を用いて監視を行うとともに（図１６の矢印Ｙｄ，Ｙｅ参照）、ホスト５ｄ，５ｅそれぞれで生成したモデルｄ’１とモデルｅ’１とを用いた監視を行う。

[0102] そして、ホスト５ｄ，５ｅの通信において、仮に過検知通信があった場合

、モデルｄ’１またはモデルｅ’１では検知されるが、モデルｕ１では検知されない。このため、学習・検知サーバ９は、これらのモデル間の検知状況の違いから、検知された事象が過検知通信であるか否か、つまり正常として判断してよいか否か、を識別することができる（図１６の（７）参照）。

[0103] すなわち、学習・検知サーバ９は、モデルｄ’１またはモデルｅ’１を用いて異常通信と検知された通信であって、モデルｕ１を用いて異常通信と検知されなかった通信を過検知通信として識別する。一方、学習・検知サーバ９は、モデルｄ’１またはモデルｅ’１を用いて異常通信と検知された通信であって、モデルｕ１を用いて異常通信と検知された通信を分析対象の通信として出力する。以降、学習・検知サーバ９は、ホスト５ｄ，５ｅの通信から、モデルｄ’１またはモデルｅ’１を用いて異常通信と検知された通信を除外した通信を学習してモデルｄ’１またはモデルｅ’１を更新する。これとともに、学習・検知サーバ９は、モデルｄ’１またはモデルｅ’１によって異常通信と検知された通信のうち過検知通信を学習しモデルｕ１を更新する。

[0104] ［通信処理の処理手順］

次に、実施の形態３における通信処理の流れについて説明する。図１７は、実施の形態３に係る通信処理の処理手順を示すシーケンス図である。

[0105] 図１７に示すステップＳ６１～ステップＳ６６は、図６に示すステップＳ１～ステップＳ６と同じ処理内容である。そして、学習・検知サーバ９は、初期モデルを用いて、新たなホスト５と他の装置との通信を監視しながら、ホスト５のモデル生成のために学習を行う（ステップＳ６７）。この際、学習・検知サーバ９は、ホスト５用のモデル（初期モデル）において検知した通信があるか否かを判定する（ステップＳ６８）。

[0106] 学習・検知サーバ９は、ホスト５用のモデルにおいて検知した通信があると判定した場合（ステップＳ６８：Ｙｅｓ）、ホスト５の通信から検知した通信を除去して（ステップＳ６９）、ホスト５の通信を学習し、ホスト５のモデルを生成する（ステップＳ７０）。これに対し、学習・検知サーバ９は

、ホスト５用のモデルにおいて検知した通信がないと判定した場合には（ステップＳ６８：Ｎｏ）、そのままホスト５の通信を学習し、ホスト５のモデルを生成する（ステップＳ７０）。

[0107] そして、学習・検知サーバ９は、ホスト５用のモデルにおいて検知した通信があると判定した場合（ステップＳ６８：Ｙｅｓ）、この検知した通信が過検知通信の場合、この検知した過検知通信を学習に含めて（ステップＳ７１）、運用ネットワーク２全体用のモデルを生成する（ステップＳ７２）。

[0108] 学習・検知サーバ９は、ホスト５と他の装置（例えば、第１の通信装置）との間の通信（ステップＳ７３－１）をキャプチャし（ステップＳ７３－２）、ステップＳ７０において生成したモデルを用いてホスト５の監視を行う（ステップＳ７４）とともに、ステップＳ７２において生成した運用ネットワーク２全体用のモデルを用いて、運用ネットワーク２全体の監視を行う（ステップＳ７５）。

[0109] そして、学習・検知サーバ９は、ホスト５用のモデルで検知した通信があるか否かを判定する（ステップＳ７６）。学習・検知サーバ９は、ホスト５用のモデルで検知した通信がないと判定した場合（ステップＳ７６：Ｎｏ）、ホスト５用のモデルで検知されていない通信を用いて学習を行いホスト５用のモデルを更新する（ステップＳ７７）。

[0110] これに対し、学習・検知サーバ９は、ホスト５用のモデルで検知した通信があると判定した場合（ステップＳ７６：Ｙｅｓ）、この通信が全体モデルでも検知されたか否かを判定する（ステップＳ７８）。学習・検知サーバ９は、この通信が全体モデルでは検知されないと判定した場合（ステップＳ７８：Ｎｏ）、この通信は、過検知通信である、すなわち、正常であると識別し（ステップＳ７９）、次の通信に対する監視・検知に戻る。

[0111] 一方、学習・検知サーバ９は、この通信が全体モデルでも検知されたと判定した場合（ステップＳ７８：Ｙｅｓ）、分析対象として外部の分析装置等に出力する（ステップＳ８０）。学習・検知サーバ９は、この通信に対する分析結果が異常である場合には（ステップＳ８１：異常）、本通信に対する

対処の依頼通知を外部の対処装置等に出力する（ステップＳ８２）。また、学習・検知サーバ９は、この通信に対する分析結果が正常である場合には（ステップＳ８１：正常）、本通信が過検知通信であるとして学習に含める指示を受け付けると（ステップＳ８３）、この通信を過検知として学習に含め（ステップＳ７１）、全体用モデルを更新する（ステップＳ７２）。

[0112] ［従来技術との比較］

従来技術と本実施の形態３とにおける通信処理の流れについて説明する。図１８は、従来技術における通信の監視及び過検知通信の学習について説明する図である。図１９は、実施の形態３における通信の監視及び過検知通信の学習について説明する図である。

[0113] 図１８に示すように、従来では、ホスト５ｄ，５ｅの通信を取り込んでモデルを生成している最中に、異常を検知した通信（例えば、通信ｃｄ１，ｃｅ１）を取り込むか否かは、他の分析装置或いは解析担当者の分析結果を待つ必要があった。したがって、従来では、通信の異常を検知した時から、この検知した通信が過検知通信であると分析され学習に取り込むまでの期間Ｔｄ´，Ｔｅ´が長く、ホスト５ｄ，５ｅのモデルを生成するまで時間がかかっていた（例えば、時間ｔｄ´，ｔｅ´）。

[0114] これに対し、本実施の形態３では、図１９に示すように、学習・検知サーバ９は、ホスト５ｄ，５ｅの通信を取り込んでモデルを生成している最中に通信ｃｄ１，ｃｅ１の異常を検知した場合、この通信ｃｄ１，ｃｅ１を学習対象から除外して、ホスト５ｄ，５ｅそれぞれのモデルを完成させる。そして、学習・検知サーバ９は、通信ｃｄ１，ｃｅ１が過検知通信である場合には、この過検知通信を学習して、運用ネットワーク２全体のモデルを生成する。

[0115] このように、本実施の形態３では、ホスト５のモデル（第１のモデル）と、運用ネットワーク２全体用のモデル（第２のモデル）とを分離して、運用ネットワーク２全体のモデルに過検知通信を学習させる手法を取る。この結果、学習・検知サーバ９は、通信の異常を検知した時から、この検知した通

信が過検知通信であると分析され学習に取り込むまでの期間Ｔｄ´，Ｔｅ´を必要としないため、従来と比して、ホスト５ｄ，５ｅのモデルを生成するまでの時間がｔｄ（＜ｔｄ´），ｔｅ（＜ｔｅ´）に短縮することができる。

[0116] 以上より、実施の形態３においては、学習・検知サーバ９は、異常通信が発生した場合に、ホスト５ごとのモデルで検知するほか、運用ネットワーク２全体用のモデルでも検知を行う。そして、学習・検知サーバ９は、ホスト５ごとのモデルと、全体用のモデルとにおける検知結果を比較することによって、異常通信と過検知通信との識別が可能となる。

[0117] すなわち、実施の形態３では、過検知通信をホスト５のモデル（第１のモデル）の学習に含めず、運用ネットワーク２全体のモデル（第２のモデル）の学習に含めるという分離した学習手法を取る。この結果、実施の形態３では、運用ネットワーク２のホスト５特有の使用による通信（過検知）に影響を受けない形で、かつ、遅延問題を発生させずに各ホストのモデルの生成と過検知通信の学習とが可能となり、学習フェーズ中の脆弱な期間の長期化を抑止することができる。

[0118] ［システム構成等］

図示した各装置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如く構成されていることを要しない。すなわち、各装置の分散・統合の具体的形態は図示のものに限られず、その全部又は一部を、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・統合して構成することができる。さらに、各装置にて行なわれる各処理機能は、その全部又は任意の一部が、ＣＰＵ及び当該ＣＰＵにて解析実行されるプログラムにて実現され、あるいは、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得る。本実施の形態に係る推定装置１０，２１０は、コンピュータとプログラムによっても実現でき、プログラムを記録媒体に記録することも、ネットワークを通して提供することも可能である。

[0119] また、本実施の形態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おこなうこともでき、あるいは、手動的に行な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おこなうこともできる。この他、上記文書中や図面中で示した処理手順、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任意に変更することができる。

[0120] ［プログラム］

図２０は、プログラムが実行されることにより、学習・検知サーバ８，９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。これらの各部は、バス１０８０によって接続される。

[0121] 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１０９０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１１００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１１００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１１１０、キーボード１１２０に接続される。ビデオアダプタ１０６０は、例えばディスプレイ１１３０に接続される。

[0122] ハードディスクドライブ１０９０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、学習・検知サーバ８，９の各処理を規定するプログラムは、コンピュータ１０００により実行可能なコードが記述されたプログラムモジュール１０９３として実装される。プログラムモジュール１０９３は、例えばハードディスクドライブ１０９０に記憶される。例

えば、学習・検知サーバ８，９における機能構成と同様の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１０９０に記憶される。なお、ハードディスクドライブ１０９０は、ＳＳＤ（Solid State Drive）により代替されてもよい。

[0123] また、上述した実施形態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１０９０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１０９０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。

[0124] 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１０９０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１１００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及びプログラムデータ１０９４は、ネットワーク（ＬＡＮ、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及びプログラムデータ１０９４は、他のコンピュータから、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。

[0125] 以上、本発明者によってなされた発明を適用した実施形態について説明したが、本実施形態による本発明の開示の一部をなす記述及び図面により本発明は限定されることはない。すなわち、本実施形態に基づいて当業者等によりなされる他の実施形態、実施例及び運用技術等は全て本発明の範疇に含まれる。

符号の説明

[0126] １　ステージング用ネットワーク

２　運用ネットワーク

３　テスト実行サーバ

４ｔ，５，５ａ～５ｅ，５ｎ　ホスト

８，９　学習・検知サーバ

１１　通信部

１２　記憶部

１３　制御部

１２１　モデル

１３１　学習部

１３２　監視・検知部

１３３　モデル送受信部

請求の範囲

[請求項1] 第１のネットワークと、第２のネットワークとを有する通信システムであって、

前記第１のネットワークは、

第１の通信装置と、

前記第１の通信装置に正常状態のテスト通信を送信し、前記第１の通信装置による通信を受信する通信テストを行うテスト装置と、

前記テスト通信と前記第１の通信装置による通信とを学習して前記第１の通信装置の異常通信を検知する初期モデルを生成し、前記初期モデルを前記第２のネットワークに送信する第１のサーバ装置と、

を有し、

前記第２のネットワークは、

前記第１の通信装置と同型の第２の通信装置と、

前記第１のサーバ装置から受信した前記初期モデルを用いて前記第２の通信装置の通信を監視しながら、前記第２の通信装置の通信を学習して前記第２の通信装置の異常通信を検知する第１のモデルを生成する第２のサーバ装置と、

有することを特徴とする通信システム。

[請求項2] 前記第２のサーバ装置は、前記第１のモデルを前記第１のサーバ装置に送信し、

前記テスト装置は、第１の前記通信テストを行い、

前記第１のサーバ装置は、前記第１のモデルを用いて、前記第１の通信テストにおいて前記テスト通信と前記第１の通信装置による通信とから異常通信を検知し、

前記テスト装置は、前記第１のサーバ装置が異常通信として検知した前記テスト通信を除外して第２の前記通信テストを行い、

前記第１のサーバ装置は、前記第２の通信テストにおいて前記テスト通信と前記第１の通信装置による通信とを学習して新たな前記初期

モデルを生成し、前記新たな初期モデルを前記第２のサーバ装置に送信することを特徴とする請求項１に記載の通信システム。

[請求項3] 前記第２のサーバ装置は、前記第２の通信装置の通信から、前記初期モデルまたは前記第１のモデルを用いて異常通信と検知された通信を除外した通信を学習して、前記第１のモデルを生成或いは更新するとともに、前記異常通信と検知された通信のうち正常である過検知通信を学習して前記過検知通信以外の異常通信を検知する第２のモデルを生成することを特徴とする請求項１または２に記載の通信システム。

[請求項4] 前記第２のサーバ装置は、前記第１のモデルを用いて異常通信と検知された通信であって前記第２のモデルを用いて異常通信と検知されなかった通信を前記過検知通信として識別し、前記第１のモデルを用いて異常通信と検知された通信であって前記第２のモデルを用いて異常通信と検知された通信を分析対象の通信として出力することを特徴とする請求項３に記載の通信システム。

[請求項5] 第１の通信装置とテスト装置と第１のサーバ装置とを有する第１のネットワークと、前記第１の通信装置と同型の第２の通信装置と第２のサーバ装置とを有する第２のネットワークと、を有する通信システムが実行する通信方法であって、

前記テスト装置が、前記第１の通信装置に正常状態のテスト通信を送信し、前記第１の通信装置による通信を受信する通信テストを行う工程と、

前記第１のサーバ装置が、前記テスト通信と前記第１の通信装置による通信とを学習して前記第１の通信装置の異常通信を検知する初期モデルを生成する工程と、

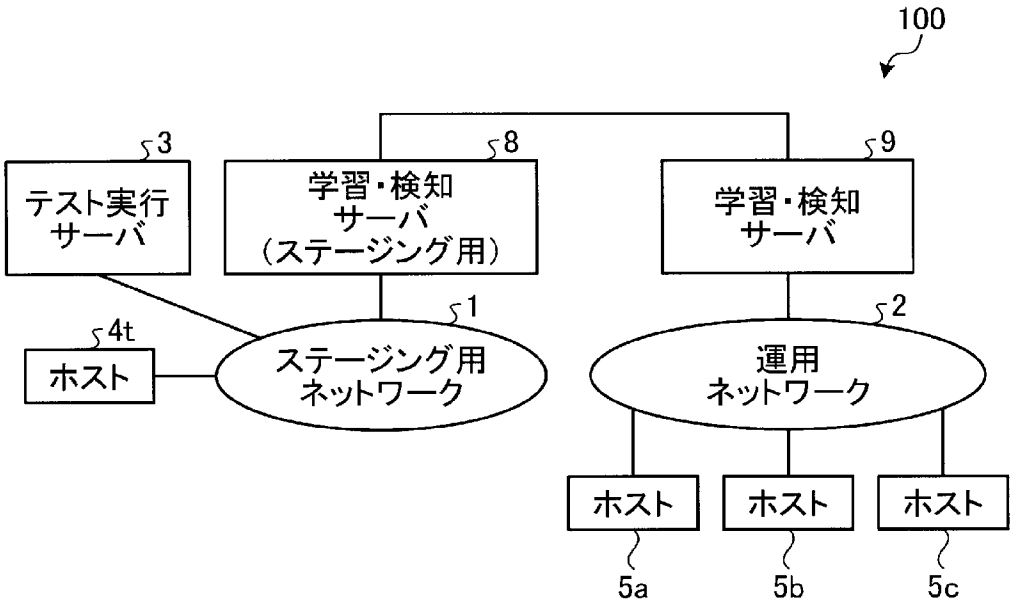
前記第１のサーバ装置が、前記初期モデルを前記第２のサーバ装置に送信する工程と、

前記第２のサーバ装置が、前記第１のサーバ装置から受信した前記

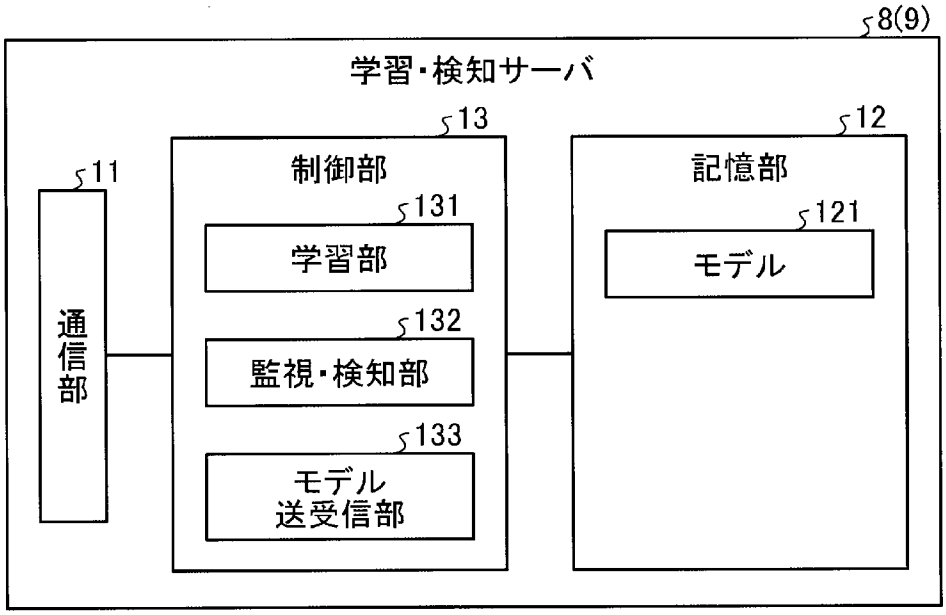
初期モデルを用いて前記第２の通信装置の通信を監視しながら、前記第２の通信装置の通信を学習して前記第２の通信装置の異常通信を検知する第１のモデルを生成する工程と、

を含んだことを特徴とする通信方法。

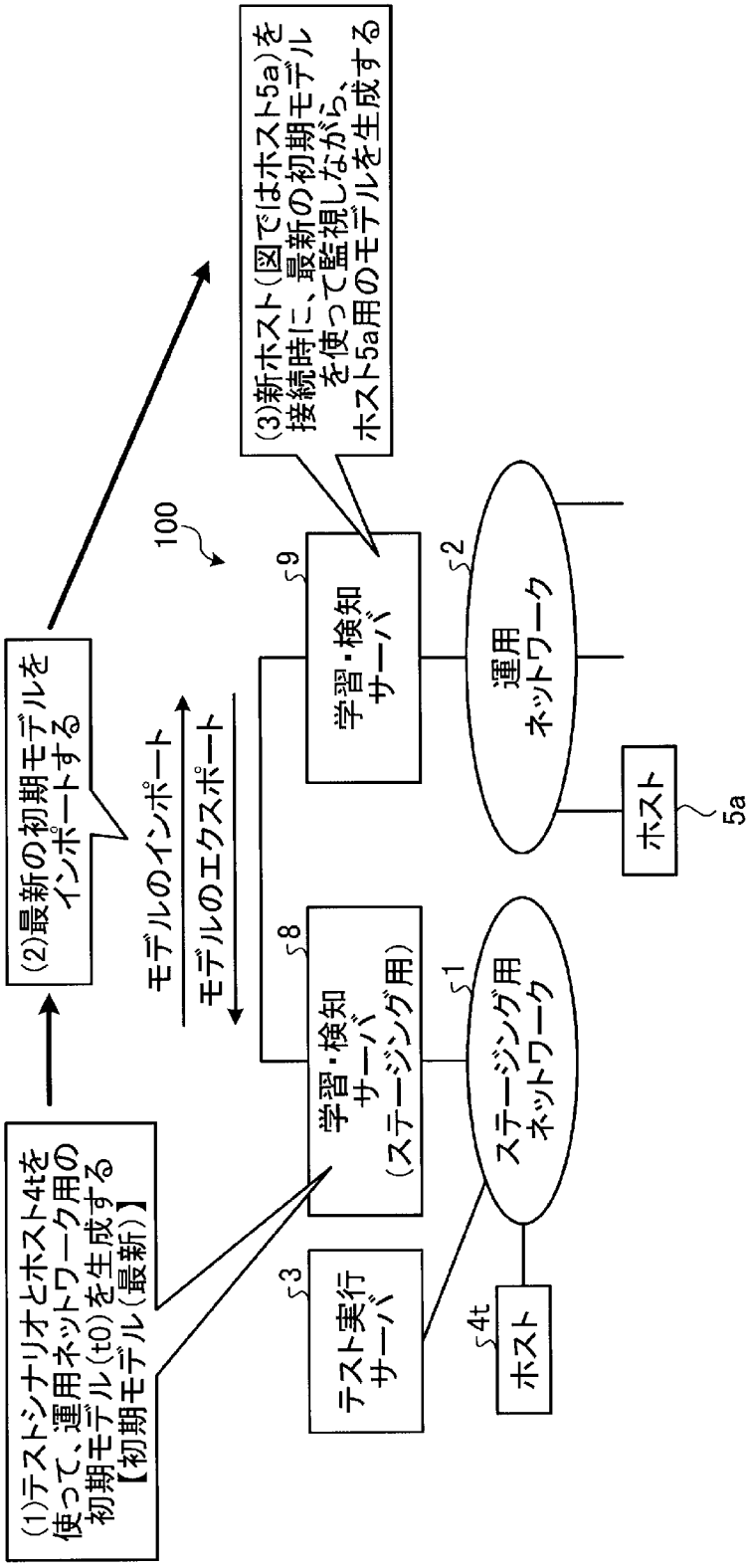
[図1]


100
3
テスト実行
サーバ
8
学習・検知
サーバ
(ステージング用)
9
学習・検知
サーバ
1
2
4t
ホスト
ステージング用
ネットワーク
運用
ネットワーク
ホスト
ホスト
ホスト
5a
5b
5c

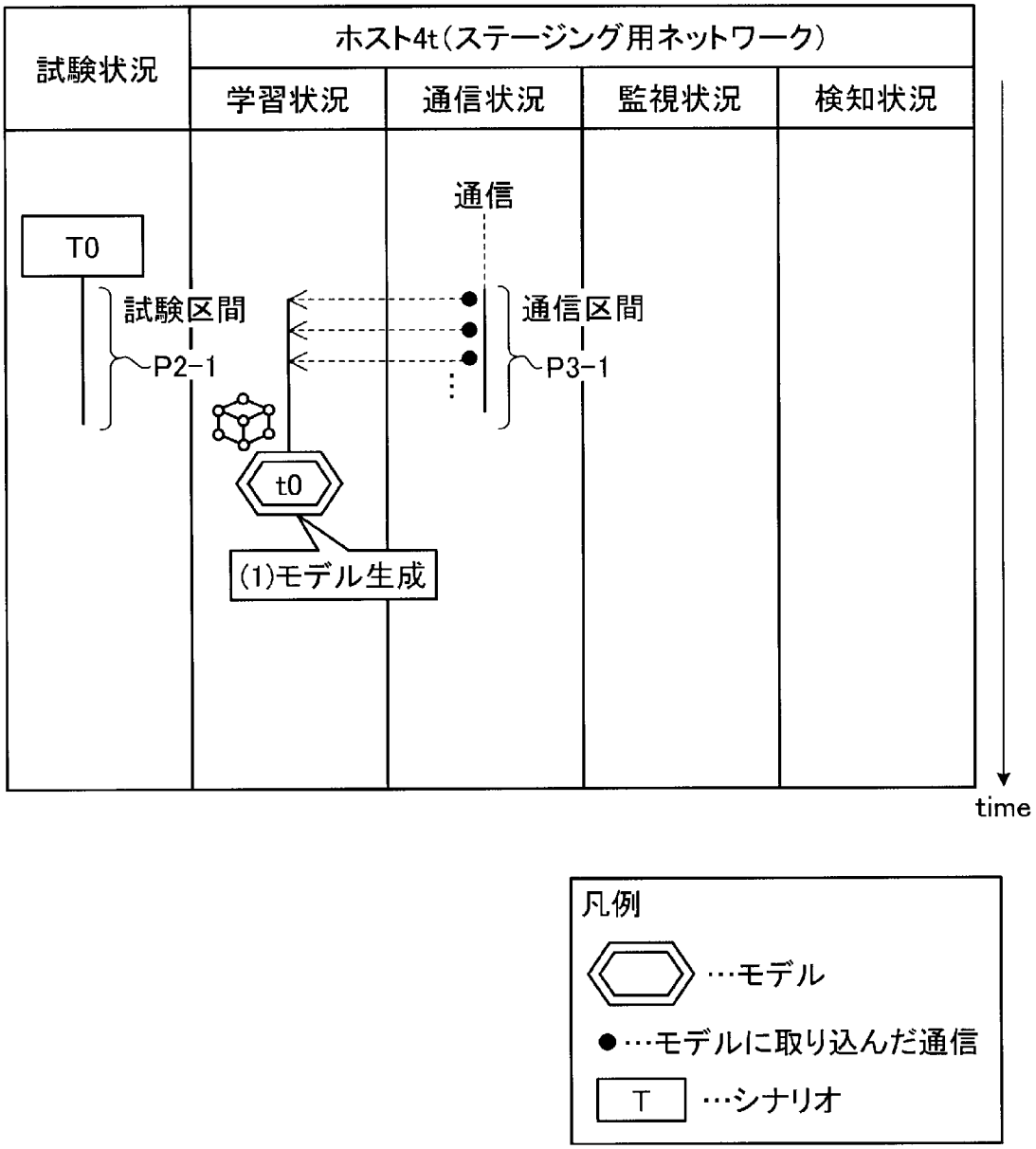
[図2]


8(9)
学習・検知サーバ
13
制御部
131
学習部
132
監視・検知部
133
モデル
送受信部
11
通信部
12
記憶部
121
モデル

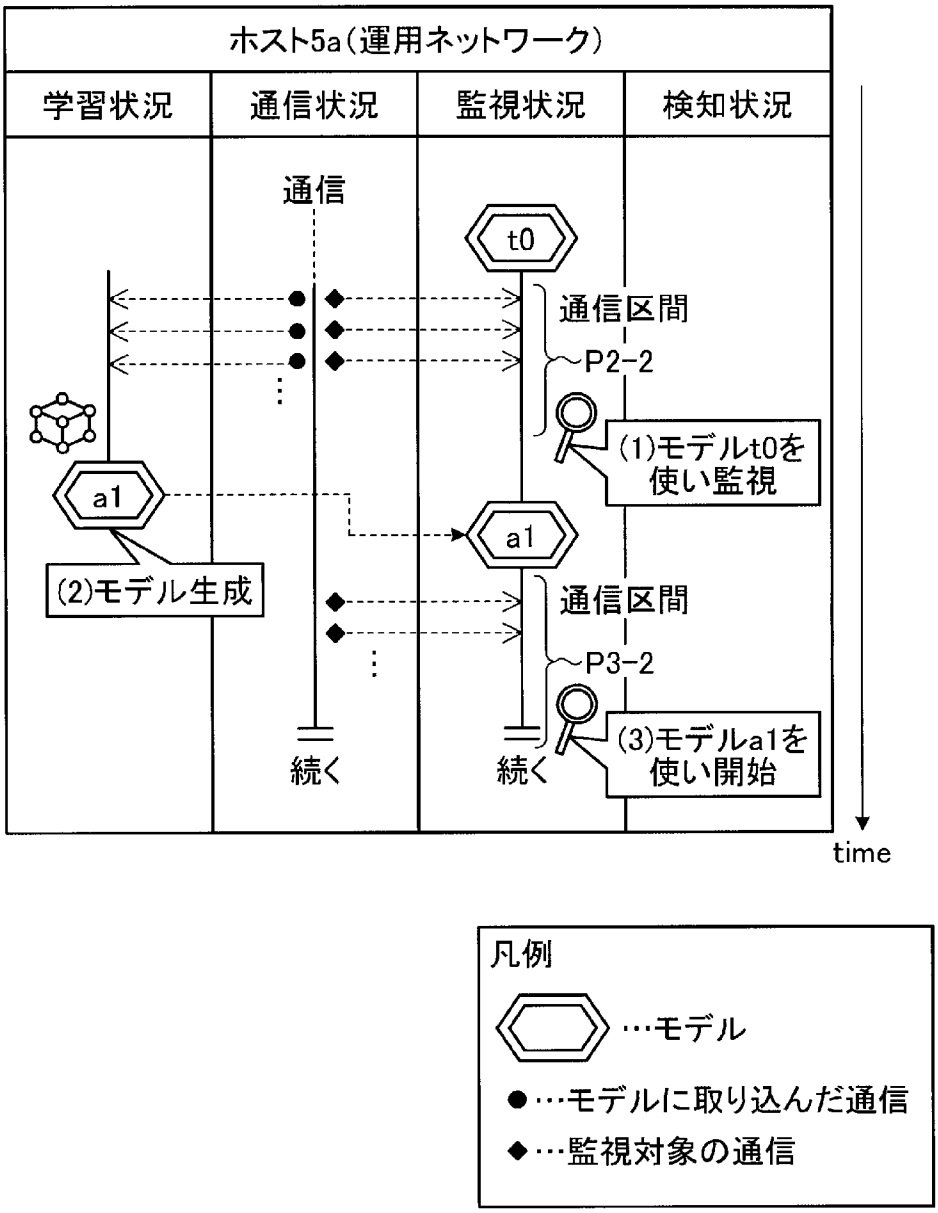
[図3]


(1)テストシナリオとホスト4tを使って、運用ネットワーク用の初期モデル(t0)を生成する【初期モデル(最新)】
(2)最新の初期モデルをインポートする
(3)新ホスト(図ではホスト5a)を接続時に、最新の初期モデルを使って監視しながら、ホスト5a用のモデルを生成する
100
モデルのインポート
モデルのエクスポート
学習・検知サーバ (ステージング用)
8
学習・検知サーバ
9
テスト実行サーバ
3
ステージング用ネットワーク
1
運用ネットワーク
2
ホスト
4t
ホスト
5a

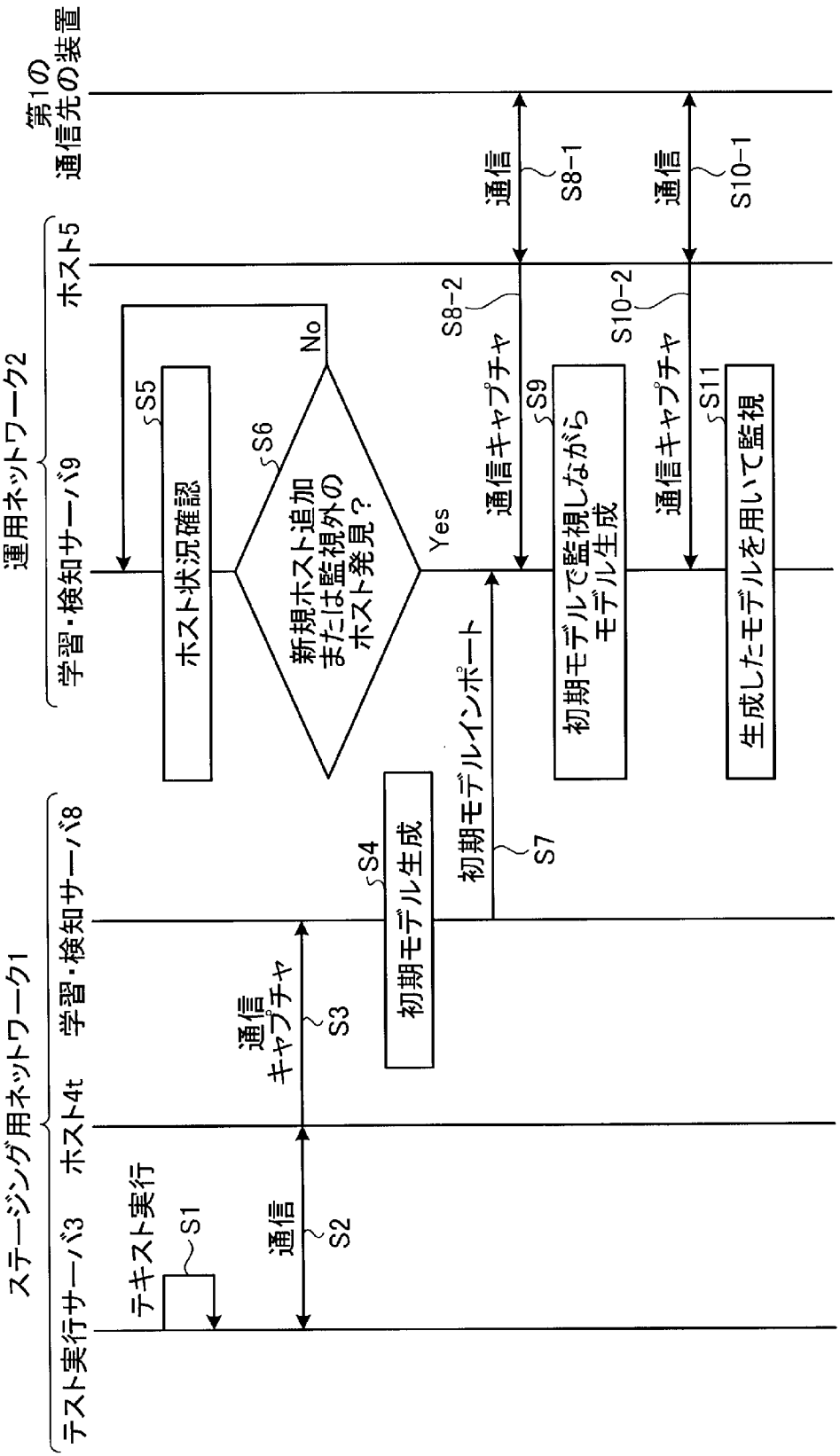
[図4]


試験状況
ホスト4t(ステージング用ネットワーク)
学習状況
通信状況
監視状況
検知状況
通信
T0
試験区間
P2-1
通信区間
P3-1
t0
(1)モデル生成
time
凡例
…モデル
●…モデルに取り込んだ通信
T
…シナリオ

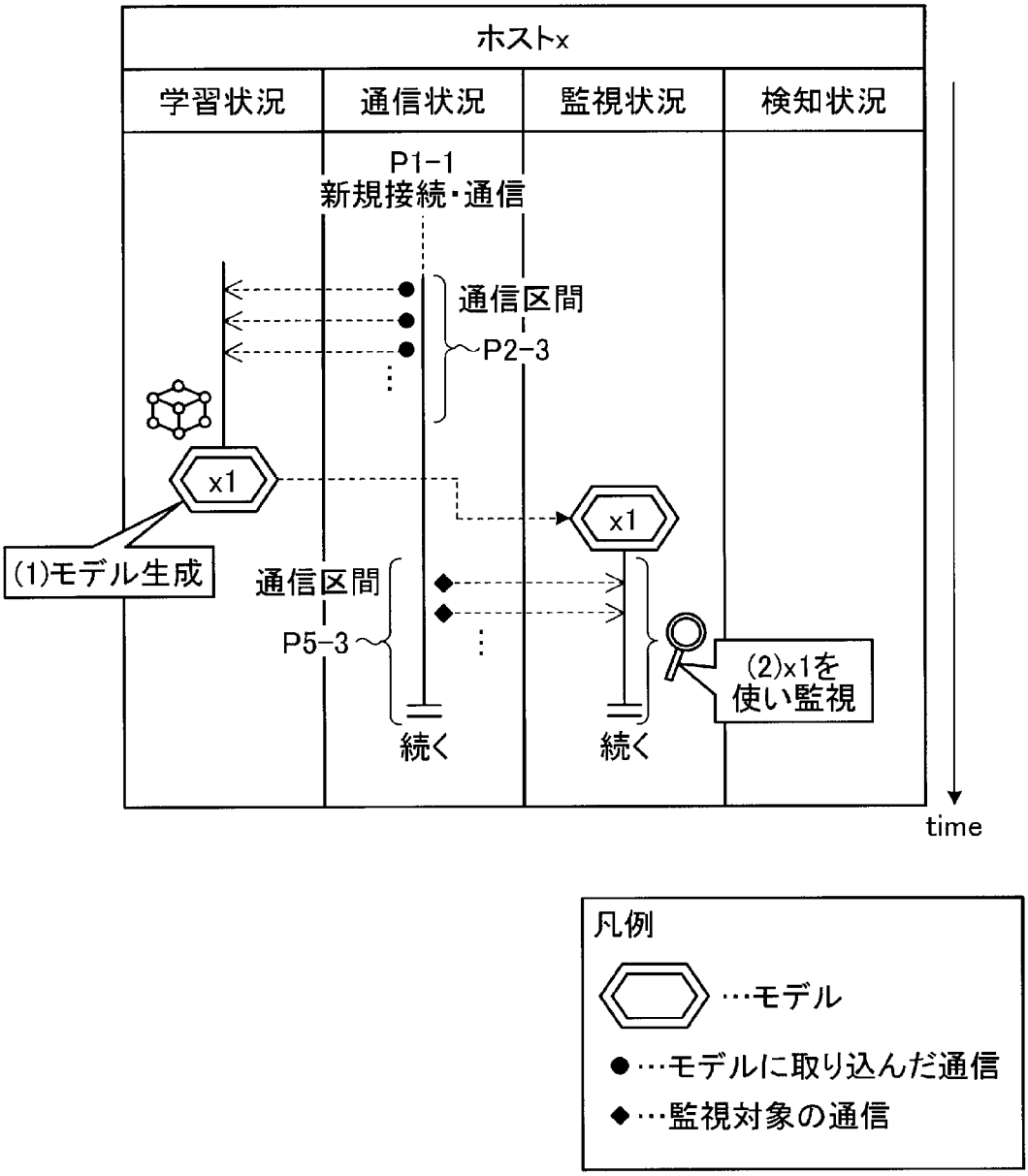
[図5]


ホスト5a(運用ネットワーク)
学習状況
通信状況
監視状況
検知状況
通信
t0
通信区間
P2-2
(1)モデルt0を
使い監視
a1
a1
(2)モデル生成
通信区間
P3-2
(3)モデルa1を
使い開始
続く
続く
time
凡例
…モデル
●…モデルに取り込んだ通信
◆…監視対象の通信

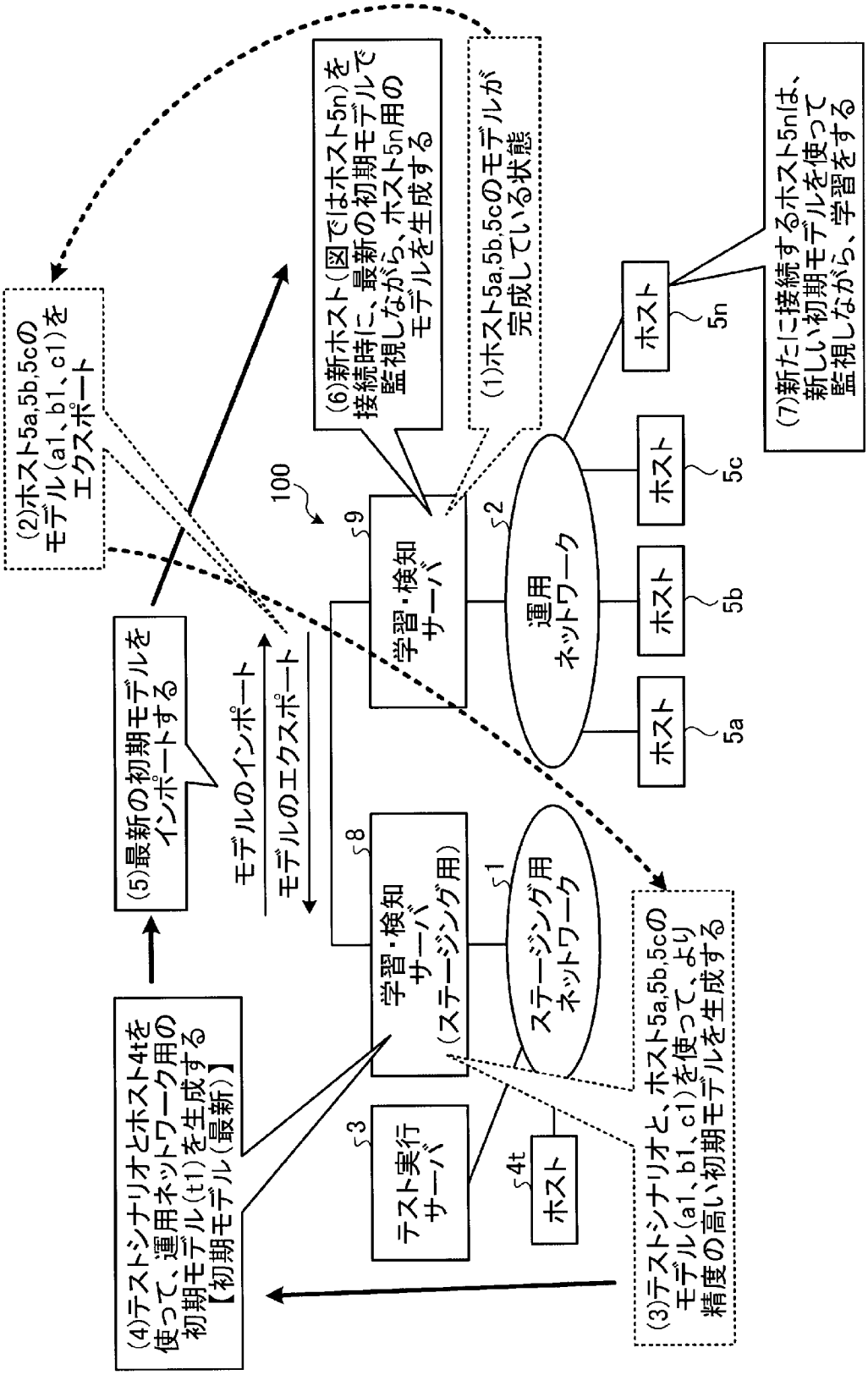
[図6]


ステージング用ネットワーク1
テスト実行サーバ3
ホスト4t
学習・検知サーバ8
運用ネットワーク2
学習・検知サーバ9
ホスト5
第1の通信先の装置
テキスト実行
S1
通信
S2
通信キャプチャ
S3
初期モデル生成
S4
ホスト状況確認
S5
新規ホスト追加またはは監視外のホスト発見？
S6
No
Yes
初期モデルインポート
S7
通信キャプチャ
S8-2
通信
S8-1
初期モデルで監視しながらモデル生成
S9
通信キャプチャ
S10-2
通信
S10-1
生成したモデルを用いて監視
S11

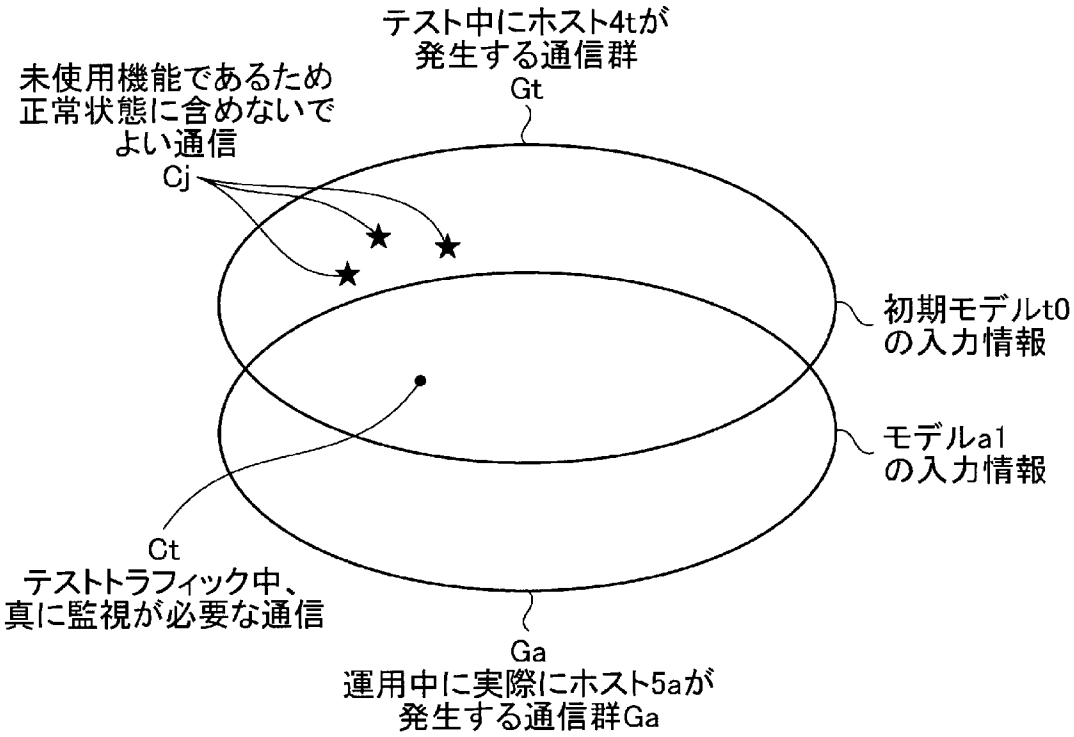
[図7]


ホストx
学習状況
通信状況
監視状況
検知状況
P1-1
新規接続・通信
通信区間
P2-3
x1
(1)モデル生成
x1
通信区間
P5-3
(2)x1を
使い監視
続く
続く
time
凡例
…モデル
●…モデルに取り込んだ通信
◆…監視対象の通信

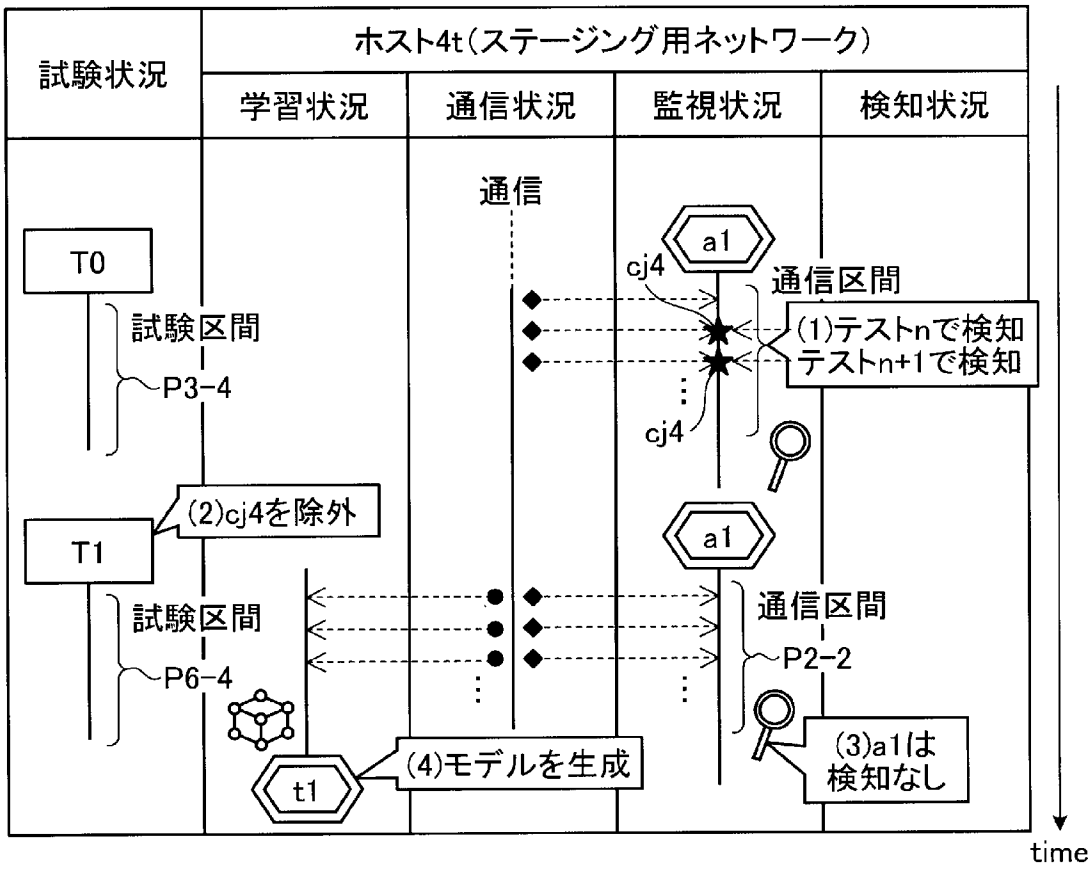
[図8]

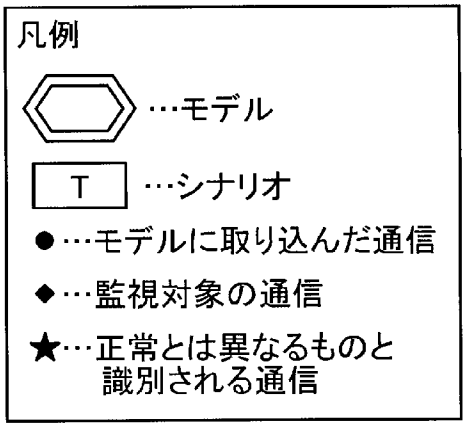

(2)ホスト5a,5b,5cのモデル(a1、b1、c1)をエクスポート
(6)新ホスト(図ではホスト5n)を接続時に、最新の初期モデルで監視しながら、ホスト5n用のモデルを生成する
(1)ホスト5a,5b,5cのモデルが完成している状態
(7)新たに接続するホスト5nは、新しい初期モデルを使って監視しながら、学習をする
100
9
2
学習・検知サーバ
運用ネットワーク
ホスト
5n
ホスト
5c
ホスト
5b
ホスト
5a
(5)最新の初期モデルをインポートする
モデルのインポート
モデルのエクスポート
8
1
学習・検知サーバ(ステージング用)
ステージング用ネットワーク
3
テストサーバ
4t
ホスト
(4)テストシナリオとホスト4tを使って、運用ネットワーク用の初期モデル(t1)を生成する【初期モデル(最新)】
(3)テストシナリオと、ホスト5a,5b,5cのモデル(a1、b1、c1)を使って、より精度の高い初期モデルを生成する

[図9]

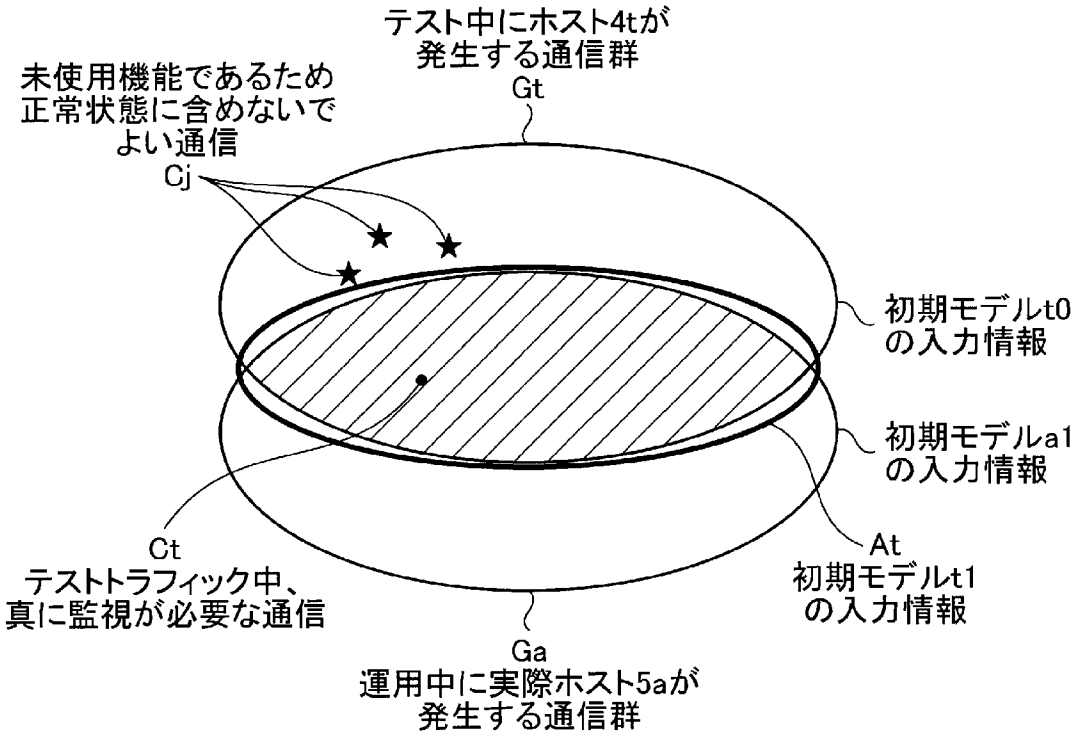

テスト中にホスト4tが
発生する通信群
Gt
未使用機能であるため
正常状態に含めないで
よい通信
Cj
初期モデルt0
の入力情報
モデルa1
の入力情報
Ct
テストトラフィック中、
真に監視が必要な通信
Ga
運用中に実際にホスト5aが
発生する通信群Ga

[図10]

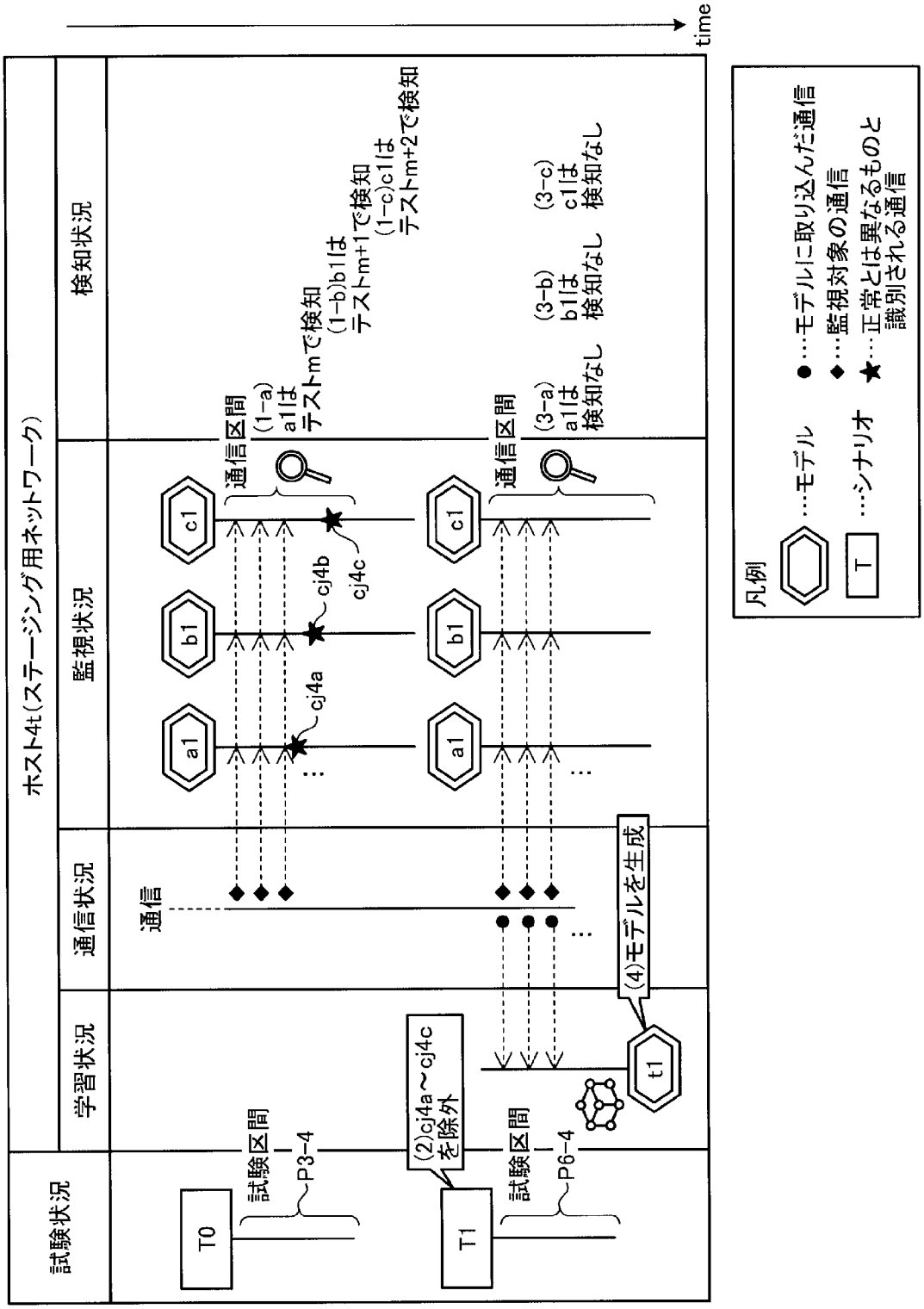

試験状況
ホスト4t(ステージング用ネットワーク)
学習状況
通信状況
監視状況
検知状況
通信
T0
試験区間
P3-4
a1
cj4
通信区間
(1)テストnで検知
テストn+1で検知
cj4
(2)cj4を除外
T1
a1
試験区間
P6-4
通信区間
P2-2
(3)a1は
検知なし
t1
(4)モデルを生成
time


凡例
…モデル
T
…シナリオ
●…モデルに取り込んだ通信
◆…監視対象の通信
★…正常とは異なるものと
識別される通信

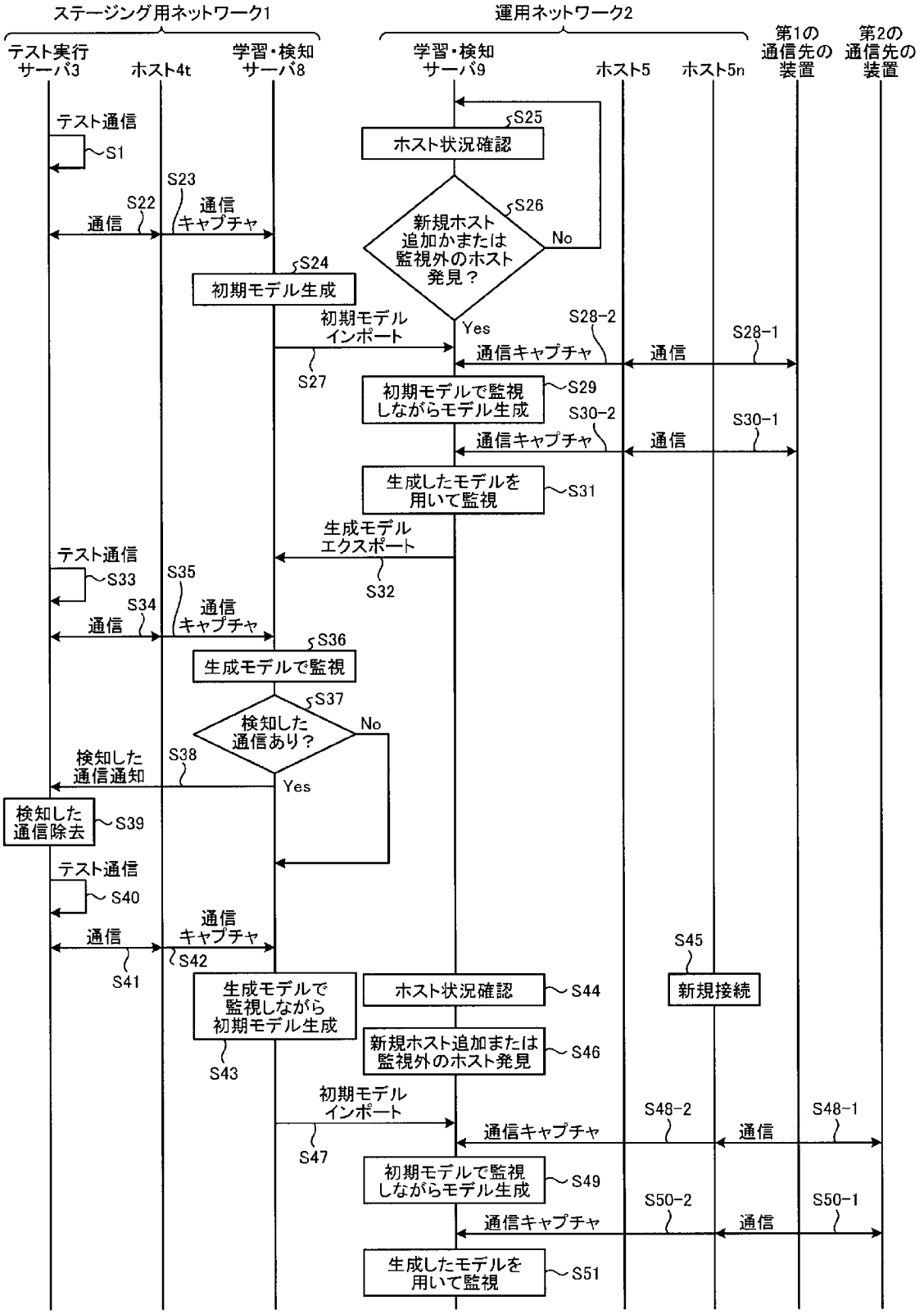
[図11]


テスト中にホスト4tが
発生する通信群
Gt
未使用機能であるため
正常状態に含めないで
よい通信
Cj
初期モデルt0
の入力情報
初期モデルa1
の入力情報
Ct
テストトラフィック中、
真に監視が必要な通信
At
初期モデルt1
の入力情報
Ga
運用中に実際ホスト5aが
発生する通信群

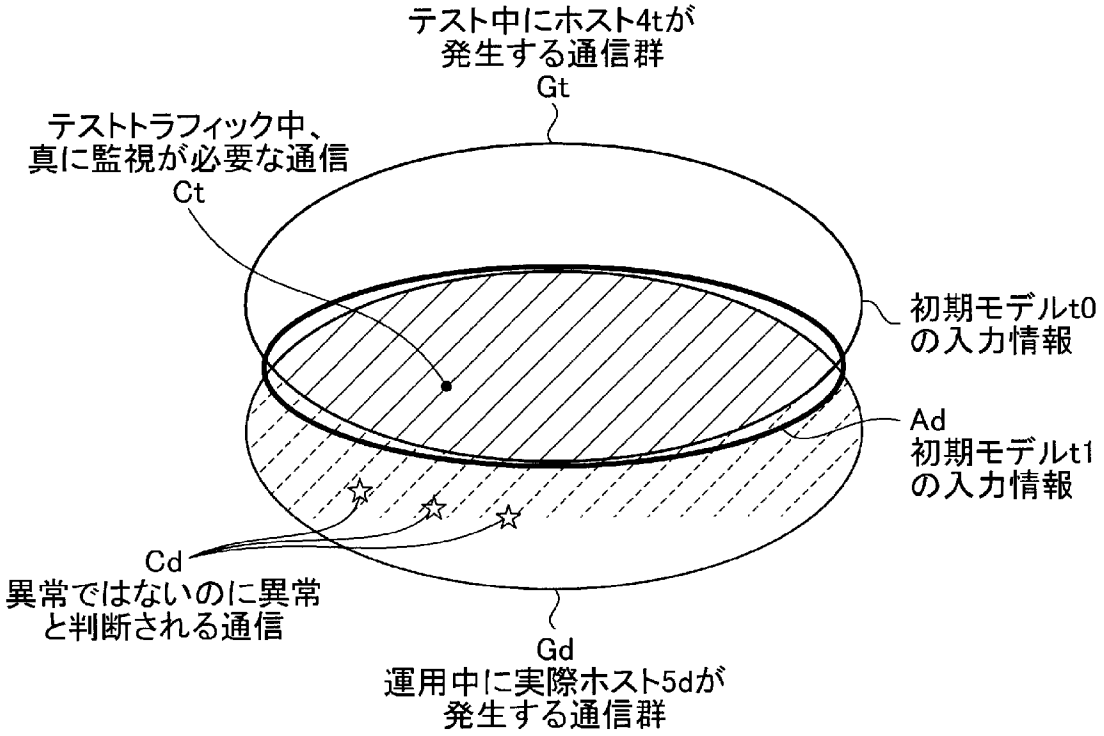
[図12]


time
ホスト4t(ステージング用ネットワーク)
試験状況
学習状況
通信状況
監視状況
検知状況
T0
試験区間
P3-4
T1
試験区間
P6-4
(2)cj4a～cj4c
を除外
通信
a1
b1
c1
cj4a
cj4b
cj4c
通信区間
(1-a)
a1は
テストmで検知
(1-b)b1は
テストm+1で検知
(1-c)c1は
テストm+2で検知
(3-a)
a1は
検知なし
(3-b)
b1は
検知なし
(3-c)
c1は
検知なし
(4)モデルを生成
t1
凡例
…モデル
…シナリオ
●…モデルに取り込んだ通信
◆…監視対象の通信
★…正常とは異なるものと
識別される通信

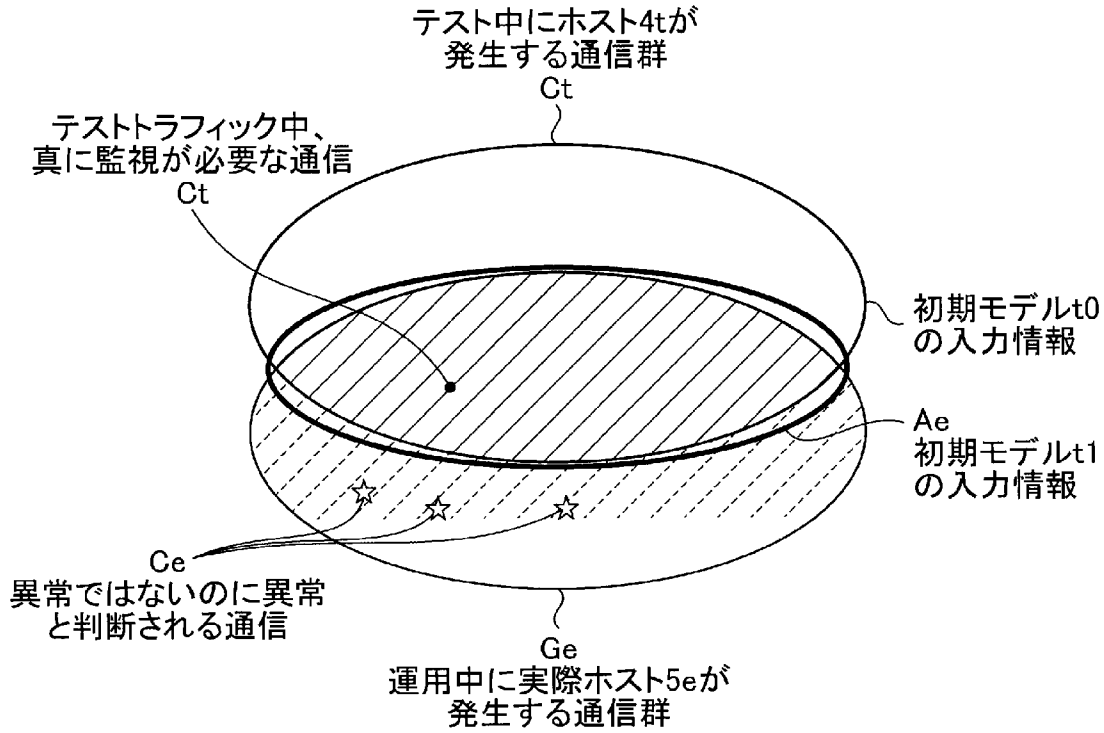
[図13]


ステージング用ネットワーク1
運用ネットワーク2
テスト実行サーバ3
ホスト4t
学習・検知サーバ8
学習・検知サーバ9
ホスト5
ホスト5n
第1の通信先の装置
第2の通信先の装置
テスト通信
S1
S22
通信
S23
通信キャプチャ
S24
初期モデル生成
初期モデルインポート
S27
S25
ホスト状況確認
新規ホスト追加かまたは監視外のホスト発見？
S26
No
Yes
S28-2
通信キャプチャ
通信
S28-1
初期モデルで監視しながらモデル生成
S29
S30-2
通信キャプチャ
通信
S30-1
生成したモデルを用いて監視
S31
生成モデルエクスポート
S32
テスト通信
S33
S34
通信
S35
通信キャプチャ
S36
生成モデルで監視
S37
検知した通信あり？
No
Yes
検知した通信通知
S38
検知した通信除去
S39
テスト通信
S40
通信
S41
通信キャプチャ
S42
生成モデルで監視しながら初期モデル生成
S43
ホスト状況確認
S44
S45
新規接続
新規ホスト追加または監視外のホスト発見
S46
初期モデルインポート
S47
S48-2
通信キャプチャ
通信
S48-1
初期モデルで監視しながらモデル生成
S49
S50-2
通信キャプチャ
通信
S50-1
生成したモデルを用いて監視
S51

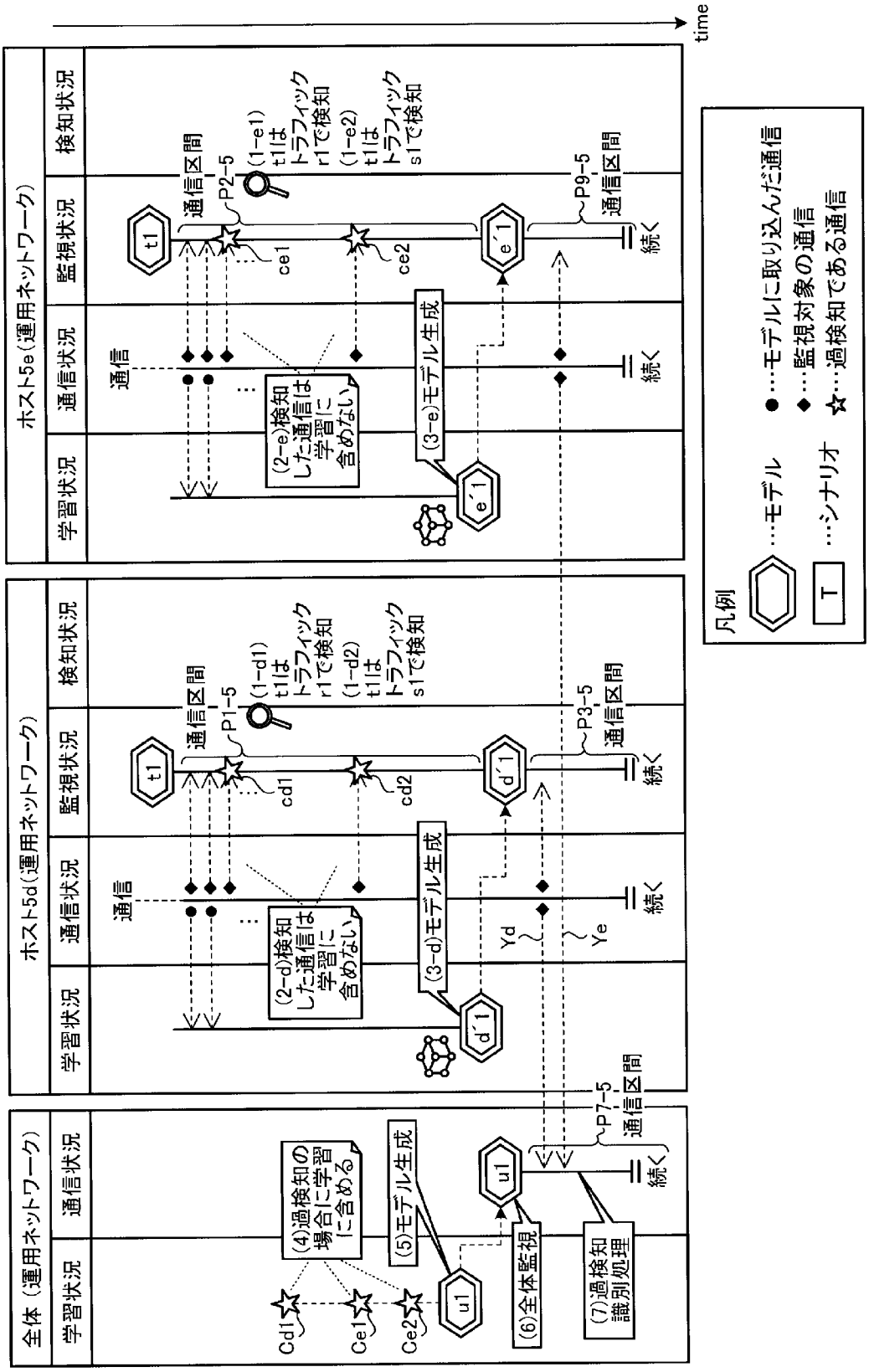
[図14]


テスト中にホスト4tが
発生する通信群
Gt
テストトラフィック中、
真に監視が必要な通信
Ct
初期モデルt0
の入力情報
Ad
初期モデルt1
の入力情報
Cd
異常ではないのに異常
と判断される通信
Gd
運用中に実際ホスト5dが
発生する通信群

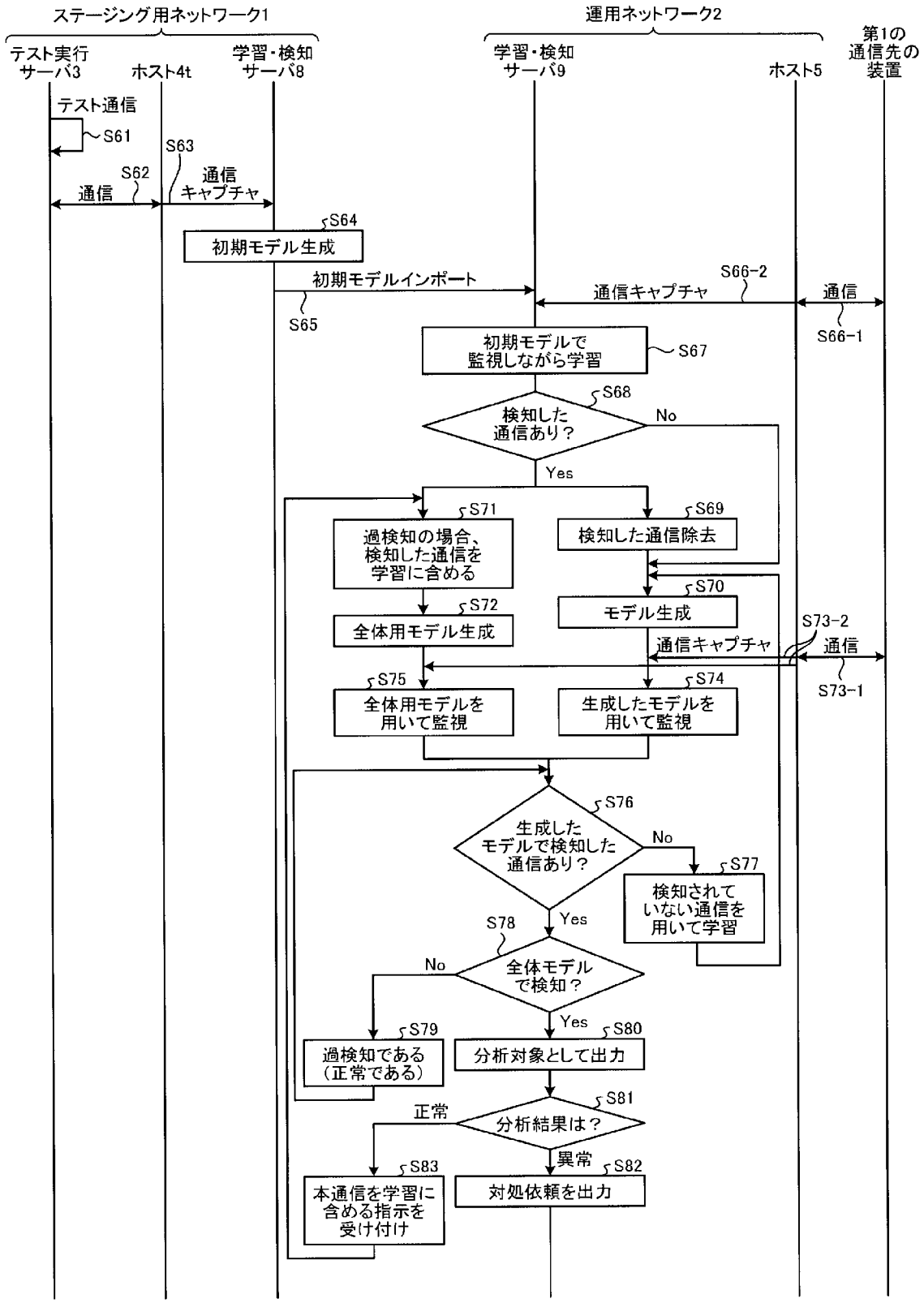
[図15]


テスト中にホスト4tが
発生する通信群
Ct
テストトラフィック中、
真に監視が必要な通信
Ct
初期モデルt0
の入力情報
Ae
初期モデルt1
の入力情報
Ce
異常ではないのに異常
と判断される通信
Ge
運用中に実際ホスト5eが
発生する通信群

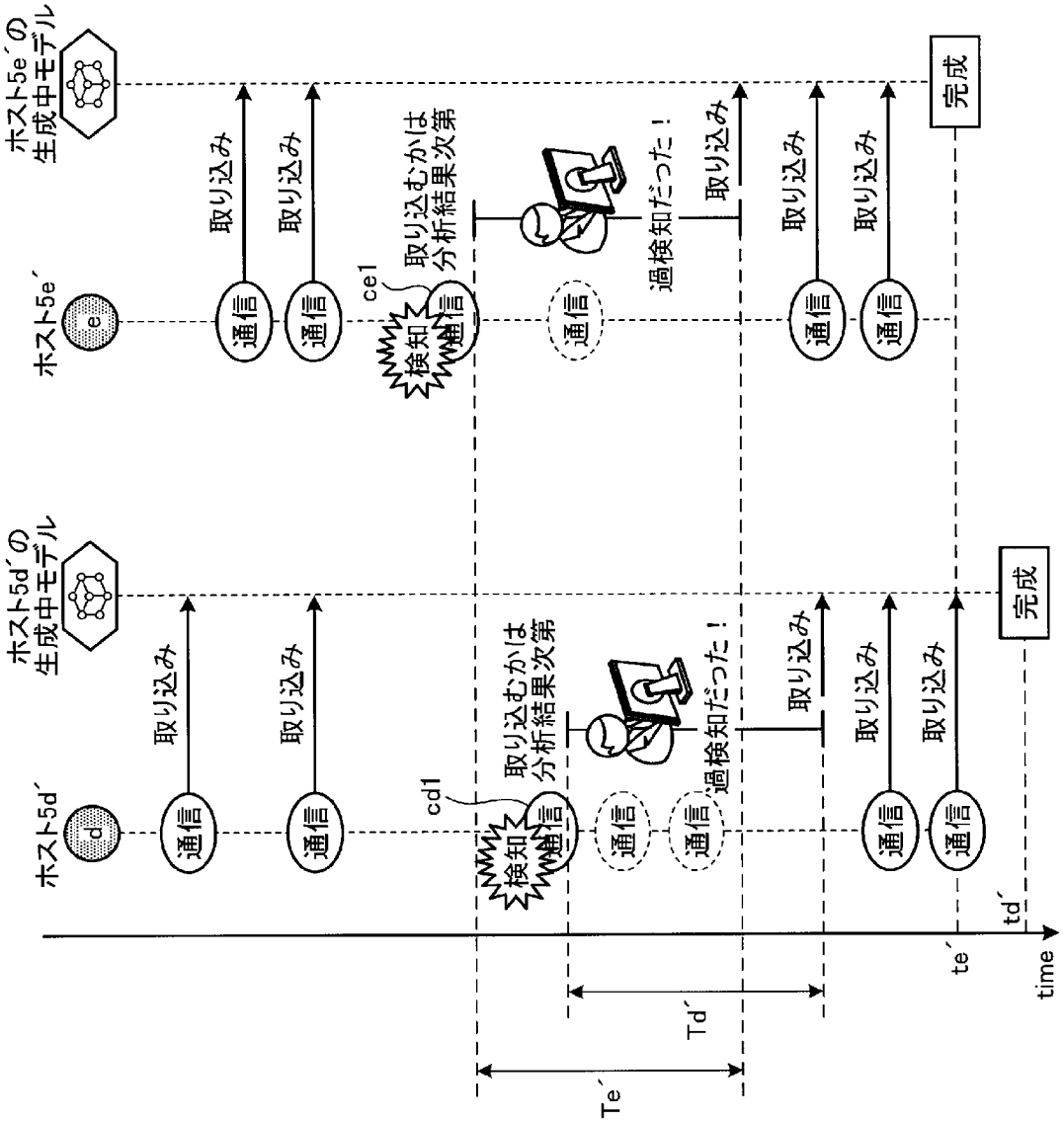
[図16]


time
全体（運用ネットワーク）
学習状況
通信状況
ホスト5d（運用ネットワーク）
学習状況
通信状況
監視状況
検知状況
ホスト5e（運用ネットワーク）
学習状況
通信状況
監視状況
検知状況
通信
通信区間
P1-5
(1-d1)
t1は
トラフィック
r1で検知
(1-d2)
t1は
トラフィック
s1で検知
cd1
cd2
(2-d)検知
した通信は
学習に
含めない
(3-d)モデル生成
d´1
Yd
Ye
P3-5
通信区間
続く
P7-5
通信区間
続く
Cd1
Ce1
Ce2
(4)過検知の
場合に学習
に含める
(5)モデル生成
u1
(6)全体監視
(7)過検知
識別処理
通信
通信区間
P2-5
(1-e1)
t1は
トラフィック
r1で検知
(1-e2)
t1は
トラフィック
s1で検知
ce1
ce2
(2-e)検知
した通信は
学習に
含めない
(3-e)モデル生成
e´1
P9-5
通信区間
続く
凡例
…モデル
…シナリオ
●…モデルに取り込んだ通信
◆…監視対象の通信
☆…過検知である通信

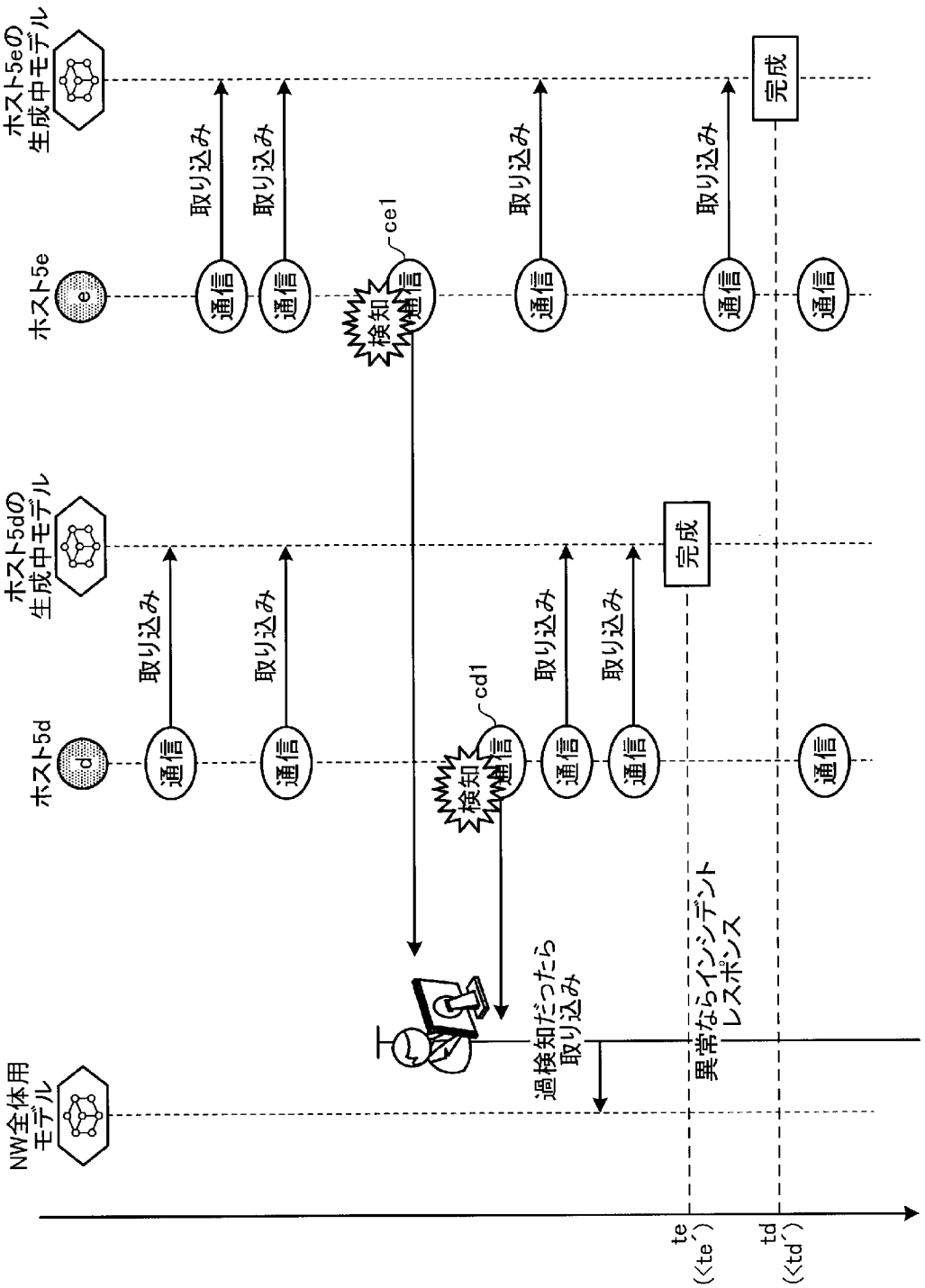
[図17]


ステージング用ネットワーク1
運用ネットワーク2
テスト実行サーバ3
ホスト4t
学習・検知サーバ8
学習・検知サーバ9
ホスト5
第1の通信先の装置
テスト通信
S61
S62
通信
S63
通信キャプチャ
S64
初期モデル生成
初期モデルインポート
S65
S66-2
通信キャプチャ
通信
S66-1
初期モデルで監視しながら学習
S67
S68
検知した通信あり？
No
Yes
S71
過検知の場合、検知した通信を学習に含める
S69
検知した通信除去
S70
モデル生成
S72
全体用モデル生成
S73-2
通信キャプチャ
通信
S73-1
S75
全体用モデルを用いて監視
S74
生成したモデルを用いて監視
S76
生成したモデルで検知した通信あり？
No
S77
検知されていない通信を用いて学習
Yes
S78
全体モデルで検知？
No
Yes
S79
過検知である（正常である）
S80
分析対象として出力
S81
分析結果は？
正常
異常
S83
本通信を学習に含める指示を受け付け
S82
対処依頼を出力

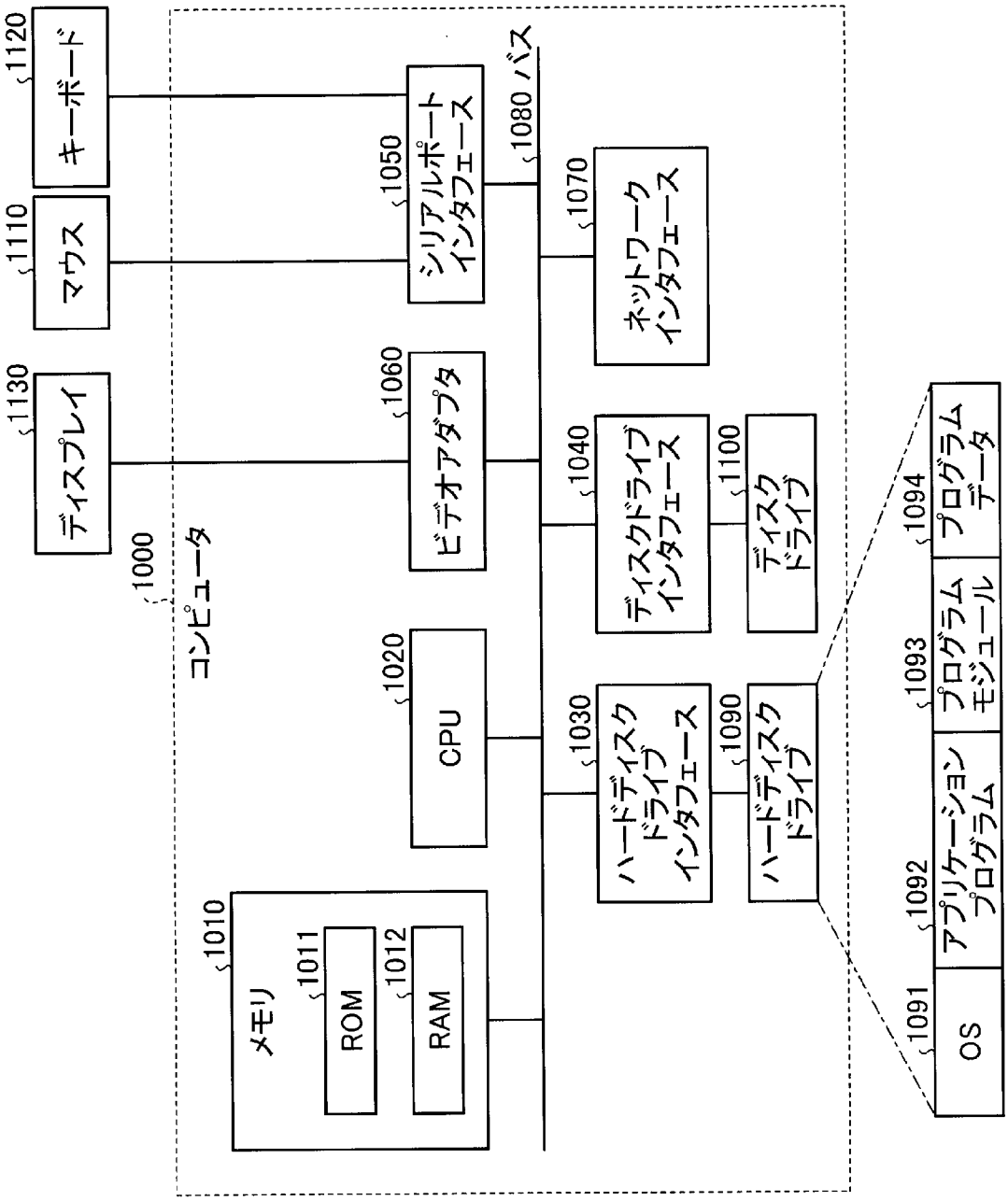
[図18]


ホスト5e´の生成中モデル
ホスト5e´
e
取り込み
通信
ce1
検知
取り込むかは分析結果次第
過検知だった！
完成
ホスト5d´の生成中モデル
ホスト5d´
d
cd1
Te´
Td´
te´
td´
time

[図19]


ホスト5eの生成中モデル
ホスト5e
e
通信
取り込み
ce1
検知
ホスト5dの生成中モデル
ホスト5d
d
cd1
完成
過検知だったら取り込み
異常ならインシデントレスポンス
NW全体用モデル
te
(<te')
td
(<td')

[図20]


1120
キーボード
1110
マウス
1130
ディスプレイ
1000
コンピュータ
1050
シリアルポート
インタフェース
1080 バス
1070
ネットワーク
インタフェース
1060
ビデオアダプタ
1040
ディスクドライブ
インタフェース
1100
ディスク
ドライブ
1020
CPU
1030
ハードディスク
ドライブ
インタフェース
1090
ハードディスク
ドライブ
1010
メモリ
1011
ROM
1012
RAM
1094
プログラム
データ
1093
プログラム
モジュール
1092
アプリケーション
プログラム
1091
OS

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2019/025447

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl. 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)
Int.Cl. H04L12/70

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	1971-2019
Registered utility model specifications of Japan	1996-2019
Published registered utility model applications of Japan	1994-2019

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	JP 2004-312083 A (KDDI CORPORATION) 04 November 2004 (Family: none)	1-5
A	JP 2001-44993 A (FUJITSU LTD.) 16 February 2001 & US 7031895 B1	1-5

☐ 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
16 August 2019 (16.08.2019)	27 August 2019 (27.08.2019)

Name and mailing address of the ISA/	Authorized officer
Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１９／０２５４４７

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	１９７１－２０１９年
日本国実用新案登録公報	１９９６－２０１９年
日本国登録実用新案公報	１９９４－２０１９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	JP 2004-312083 A（ＫＤＤＩ株式会社）2004.11.04,（ファミリーなし）	１－５
A	JP 2001-44993 A（富士通株式会社）2001.02.16, & US 7031895 B1	１－５

☐　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
１６．０８．２０１９	２７．０８．２０１９

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　４１８５
大石　博見
電話番号　０３－３５８１－１１０１　内線　３５９６