(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
2024年9月12日(12.09.2024)

WIPO | PCT

(10) 国際公開番号
WO 2024/185162 A1

(51) 国際特許分類:
H04L 12/66 (2006.01) *H04L 41/06* (2022.01)
H04L 12/22 (2006.01) *H04L 43/08* (2022.01)

(21) 国際出願番号： PCT/JP2023/024528

(22) 国際出願日： 2023年6月30日(30.06.2023)

(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 2023-033209 2023年3月3日(03.03.2023) JP

(71) 出願人: エヌ・ティ・ティ・コミュニケーションズ株式会社(**NTT COMMUNICATIONS CORPORATION**) [JP/JP]; 〒1008019 東京都千代田区大手町二丁目３番１号 Tokyo (JP).

(72) 発明者: ▲ 高 ▼ 津 健 (**TAKATSU, Takeshi**); 〒1008019 東京都千代田区大手町二丁目３番１号 エヌ・ティ・ティ・コミュニケーションズ株式会社内 Tokyo (JP). 畑田 充弘(**HATADA, Mitsuhiro**); 〒1008019 東京都千代田区大手町二丁目３番１号 エヌ・ティ・ティ・コミュニケーションズ株式会社内 Tokyo (JP).

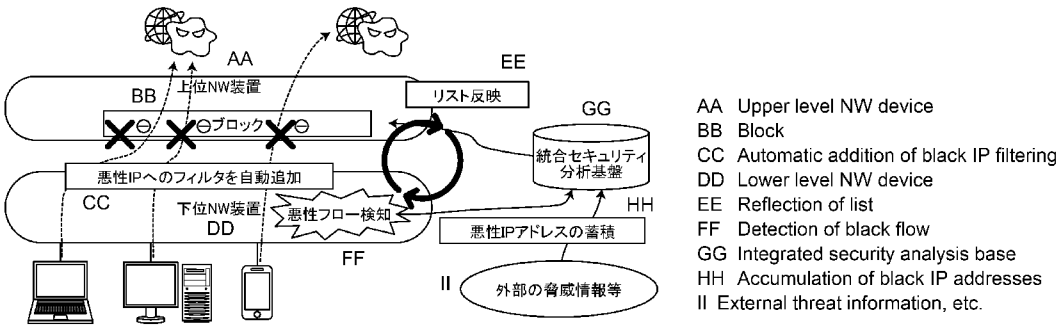
(74) 代理人: 弁理士法人酒井国際特許事務所 (**SAKAI INTERNATIONAL PATENT OFFICE**); 〒1000013 東京都千代田区霞が関３丁目８番１号 虎ノ門ダイビルイースト Tokyo (JP).

(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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR,

(54) **Title:** INFORMATION PROCESSING SYSTEM, INFORMATION PROCESSING METHOD, AND INFORMATION PROCESSING PROGRAM

(54) 発明の名称： 情報処理システム、情報処理方法および情報処理プログラム

[図5]



(57) **Abstract:** An information processing system (1) comprises: an upper level NW device (100) which constitutes an overlay network and a lower level NW device (200) which constitutes an underlay network. The lower level NW device (200) acquires information related to communication by terminals connected to the lower level NW device (200), detects unauthorized communication on the basis of the acquired information related to the communication by the terminals connected to the lower level NW device (200), notifies the upper level NW device (100) of the information on the detected unauthorized communication. The upper level NW device (100) blocks the unauthorized communication on the basis of the information on the unauthorized communication notified by the lower level NW device (200).

WO 2024/185162 A1

[続葉有]

HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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)）

(57) 要約：情報処理システム（１）は、オーバレイネットワークを構成する装置である上位ＮＷ装置（１００）とアンダーレイネットワークを構成する装置である下位ＮＷ装置（２００）とからなる情報処理システムであって、下位ＮＷ装置（２００）は、下位ＮＷ装置（２００）に接続される端末の通信に関する情報を取得し、取得された下位ＮＷ装置（２００）に接続される端末の通信に関する情報に基づいて、不正な通信を検知し、検知された不正な通信の情報を、上位ＮＷ装置（１００）に通知し、上位ＮＷ装置（１００）は、下位ＮＷ装置（２００）から通知された不正な通信の情報に基づいて、不正な通信を遮断する。

明　細　書

発明の名称 ：

情報処理システム、情報処理方法および情報処理プログラム

技術分野

[0001] 本発明は、情報処理システム、情報処理方法および情報処理プログラムに関する。

背景技術

[0002] 従来、不正通信を検知する技術が存在する。例えば、ゲートウェイにおけるファイアウォール、ＩＰＳ（Intrusion Prevention System）の設置や通信監視により、不審な通信や挙動を行う端末を特定する技術が知られている。

先行技術文献

非特許文献

[0003] 非特許文献1：Ｃ＆Ｃサーバとは？マルウェア感染したＰＣからの攻撃の自動遮断による対策方法、[２０２３年６月２０日検索]、インターネット（https://www.ntt.com/bizon/sec/cybersec04.html）

発明の概要

発明が解決しようとする課題

[0004] 従来技術においては、セキュリティの問題が存在していた。例えば、感染直後のＰＣ（personal computer）宛等検知ブロックでは対処できない場合がある。

[0005] 本発明は、上記に鑑みてなされたものであって、堅牢なセキュリティを実現するための情報処理システム、情報処理方法および情報処理プログラム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

[0006] 上述した課題を解決し、目的を達成するために、本発明の情報処理システ

ムは、オーバレイネットワークを構成する装置である上位ＮＷ（network）装置とアンダーレイネットワークを構成する装置である下位ＮＷ装置とからなる情報処理システムであって、前記上位ＮＷ装置は、前記下位ＮＷ装置から通知された不正な通信の情報に基づいて、前記不正な通信を遮断する遮断部を有し、前記下位ＮＷ装置は、前記下位ＮＷ装置に接続される端末の通信に関する情報を取得する取得部と、前記取得部により取得された前記下位ＮＷ装置に接続される端末の通信に関する情報に基づいて、前記不正な通信を検知する検知部と、前記検知部により検知された前記不正な通信の情報を、前記上位ＮＷ装置に通知する通知部とを有することを特徴とする。

発明の効果

[0007] 本発明によれば、堅牢なセキュリティを実現することができる。

図面の簡単な説明

[0008] [図1]図１は、従来技術について説明するための図である。

[図2]図２は、実施形態に係る情報処理システムの構成の一例を示す図である。

[図3]図３は、実施形態に係る上位ＮＷ装置の構成の一例を示す図である。

[図4]図４は、実施形態に係る下位ＮＷ装置の構成の一例を示す図である。

[図5]図５は、実施形態に係る情報処理システムが行う処理概要を説明するための図である。

[図6]図６は、実施形態に係る情報処理システムが行う検知処理と遮断処理の一例を説明するための図である。

[図7]図７は、実施形態に係る情報処理システムによる処理の流れの一例を示すフローチャートである。

[図8]図８は、情報処理プログラムを実行するコンピュータの例を示す図である。

発明を実施するための形態

[0009] 以下、図面を参照して、本願に係る情報処理システム、情報処理方法および情報処理プログラムの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おり、重複する説明は省略される。

[0010] ［従来技術］

まず、図１を用いて、従来技術について説明する。図１は、従来技術について説明するための図である。

[0011] なお、以下では、オーバレイネットワークを構成する装置を上位ＮＷ装置と記載し、アンダーレイネットワークを構成する装置を下位ＮＷ装置と記載する。ここで上位ＮＷ装置とは、例えば、クラウドプロキシサーバやＵＴＭ（Unified Threat Management）のことをいう。また、下位ＮＷ装置とは、例えば、ＤＰＩ（Deep Packet Inspection）、ルータ、スイッチなどのネットワーク機器のことをいう。

[0012] 従前のセキュリティ対策は、信頼できる「内側」と信頼できない「外側」にネットワークを分け、その境界線で対策を講じることが行われていた。例えば、内側のネットワークとしては、社内ＬＡＮ（Local Area Network）やＶＰＮ（Virtual Private Network）で接続されたデータセンタなどが該当し、外側のネットワークとしては、インターネットが該当する。例えば、境界線で講じられる対策として、境界線にファイアウォールやプロキシー、ＩＤＳ（Intrusion Detection System）／ＩＰＳ（Intrusion Prevention System）などのセキュリティ機器を設置し、通信の監視や制御を行うことで外部からのサイバー攻撃を遮断する。

[0013] こうした従前のセキュリティ対策は、保護すべきデータやシステムがネットワークの内側にあることを前提としている。しかし、クラウドが普及したことにより、外側であるインターネット上に保護すべきものがある状況が珍しくない。このように、守るべき対象がさまざまな場所に点在するようになったことで境界が曖昧になり、従来の考え方では十分な対策を講じることが難しくなりつつある。

[0014] そこで広まっているのがゼロトラストの考え方である。ゼロトラストセキュリティサービスにおいては、すべての通信を信頼しないことを前提に、さ

まざまなセキュリティ対策を講じている。具体的には、ネットワークの内外に関わらない通信経路の暗号化や多要素認証の利用などによるユーザ認証の強化、ネットワークやそれに接続される各種デバイスの統合的なログ監視などが挙げられる。ゼロトラストを実現するためのセキュリティソリューションはすでに多数登場している。例えば、クライアント装置の監視とログの分析によりサイバー攻撃の早い検知と対処を可能にするＥＤＲ（Endpoint Detection and Response）などを設けることが行われている。

[0015] また、従来、不正通信を検知する技術が存在する。例えば、ゲートウェイにおけるファイアウォール、ＩＰＳの設置や通信監視により、不審な通信や挙動を行う端末を特定する技術が知られている。

[0016] 従来技術においては、セキュリティの問題が存在していた。例えば、図１に例示するように、不審な通信や挙動を行う端末を特定することが可能である一方、正常に機能していたＰＣがマルウェア等に感染した場合には、検知ブロックでは対処することが難しく、不審な通信を許容してしまう場合がある。

[0017] そこで、以下に記載する本実施の形態の情報処理システム１は、オーバレイネットワークを構成する装置である上位ＮＷ装置１００とアンダーレイネットワークを構成する装置である下位ＮＷ装置２００とからなる情報処理システムであって、上位ＮＷ装置１００は、下位ＮＷ装置２００から通知された不正な通信の情報に基づいて、不正な通信を遮断し、下位ＮＷ装置２００は、下位ＮＷ装置２００に接続される端末の通信に関する情報を取得し、取得した下位ＮＷ装置２００に接続される端末の通信に関する情報に基づいて、不正な通信を検知し、検知した不正な通信の情報を、上位ＮＷ装置１００に通知する。

[0018] このような情報処理システムにより、堅牢なセキュリティの実現といった効果が得られる。

[0019] また、情報処理システム１では、リモートワーク等の新しい働き方やＩｏＴ等の活用による新たな事業拡大によって一層複雑化、サイバーリスクの高

まるＩＣＴ（Information and Communication Technology）環境に対し、アンダーレイＮＷとオーバレイＮＷが連携して防御する、回線事業者（キャリア）ならではのゼロトラストセキュリティサービスを提供する。

[0020] 情報処理システム１は、オーバレイＮＷの機能とアンダーレイＮＷの機能が密接に連携したセキュアなＮａａＳ（Network as a Service）型ＩＣＴサービスを提供する。この情報処理システム１のサービスを受ける企業は、ＩＴ（Information Technology）ベンダー委託にコストを費やしたり、ＮＷ設計に掛かるコストを掛けたりすることなく、管理ポータルサイトから申し込むことで、即時に、本情報処理システム１のサービスの開始、変更、解約が容易に可能となり、設計から運用の稼働に係るコストを削減することが可能である。

[0021] ［情報処理システムの構成］

次に、図２を用いて、情報処理システム１の構成について説明する。図２が示すように、情報処理システム１は、上位ＮＷ装置１００と、下位ＮＷ装置２００とを有する。以下、これら各装置について説明する。なお、情報処理システム１において、上位ＮＷ装置１００と下位ＮＷ装置２００とは、それぞれ一つである場合に限定されるものではなく、複数設けられていてもよい。

[0022] 上位ＮＷ装置１００は、情報処理システム１の上位のネットワークを制御する装置である。上位ＮＷ装置１００は、下位ＮＷ装置２００から通知された不正な通信の情報を用いて、不正な通信を遮断する。

[0023] 下位ＮＷ装置２００は、情報処理システム１の下位のネットワークを制御する装置である。下位ＮＷ装置２００は、下位ＮＷ装置２００に接続される端末（例えば、ＯＡ機器、ＩｏＴ機器等）の通信に関する情報を取得し、取得した情報に基づいて、不正な通信を検知し、不正な通信の情報を上位ＮＷ装置１００に通知する。

[0024] ［上位ＮＷ装置の構成］

次に、図３を用いて、上位ＮＷ装置１００の構成について説明する。図３

が示すように、上位ＮＷ装置１００は、通信部１１０と、制御部１２０と、記憶部１３０とを有する。なお、これらの各部は、複数の装置が分散して保持してもよい。以下にこれら各部の処理を説明する。

[0025] 通信部１１０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外部装置と制御部１２０の通信を可能とする。例えば、通信部１１０は、外部装置と制御部１２０との通信を可能とする。

[0026] 記憶部１３０は、ＲＡＭ（Random Access Memory）、フラッシュメモリ（Flash Memory）等の半導体メモリ素子、または、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る。記憶部１３０が記憶する情報としては、例えば、上位ＮＷ装置１００が管理する端末情報、下位ＮＷ装置２００が管理する端末情報、下位ＮＷ装置２００に接続された端末の通信に関する情報、不正な通信に関する情報、検知された不正な通信の情報、その他不正な通信の検知に必要な情報、その他不正な通信の遮断に必要な情報が含まれる。ここで、不正な通信に関する情報には、不正な通信の通信先の種別、端末情報、ＩＰアドレスといった情報が含まれる。なお、記憶部１３０が記憶する情報は上記に記載した例に限定されない。

[0027] 制御部１２０は、ＣＰＵ（Central Processing Unit）やＮＰ（Network Processor）やＦＰＧＡ（Field Programmable Gate Array）等を用いて実現され、メモリに記憶された処理プログラムを実行する。図３に示すように、制御部１２０は、遮断部１２１を有する。以下、制御部１２０が有する各部について説明する。

[0028] 遮断部１２１は、下位ＮＷ装置２００から通知された不正な通信の情報に基づいて、不正な通信を遮断する。例えば、遮断部１２１は、下位ＮＷ装置２００から通知された不正な通信の情報を用いて、不正な通信の通信先への通信を遮断する。例えば、遮断部１２１は、通知部２２３により通知された不正な通信の種別、ＩＰアドレスの情報を用いて、不正な通信の通信先への通信を遮断する。

[0029] 例えば、遮断部１２１は、通知部２２３により通知された不正な通信先のＩＰアドレスの情報を、通信を許可しないＩＰアドレスのリストに追加することで、フィルタリングにより、不正な通信の通信先への通信を遮断する。

[0030] ［下位ＮＷ装置の構成］

次に、図４を用いて、下位ＮＷ装置２００の構成について説明する。図４が示すように、下位ＮＷ装置２００は、通信部２１０と、制御部２２０と、記憶部２３０とを有する。なお、これらの各部は、複数の装置が分散して保持してもよい。以下にこれら各部の処理を説明する。

[0031] 通信部２１０は、ＮＩＣ等で実現され、ＬＡＮやインターネットなどの電気通信回線を介した外部装置と制御部２２０の通信を可能とする。例えば、通信部２１０は、外部装置と制御部２２０との通信を可能とする。

[0032] 記憶部２３０は、ＲＡＭ、フラッシュメモリ等の半導体メモリ素子、または、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る。記憶部２３０が記憶する情報としては、例えば、上位ＮＷ装置１００が管理する端末情報、下位ＮＷ装置２００が管理する端末情報、下位ＮＷ装置２００に接続された端末の通信に関する情報、不正な通信に関する情報、検知された不正な通信の情報、その他不正な通信の検知に必要な情報が含まれる。ここで、記憶部２３０が記憶する不正な通信に関する情報は、下位ＮＷ装置２００が関与する通信内容と、外部装置（統合セキュリティ分析基盤）に記憶される過去のサイバー攻撃の情報等を併せて分析することにより得られる情報が含まれる。なお、記憶部２３０が記憶する情報は上記に記載した例に限定されない。

[0033] 制御部２２０は、ＣＰＵやＮＰやＦＰＧＡ等を用いて実現され、メモリに記憶された処理プログラムを実行する。図４に示すように、制御部２２０は、取得部２２１と、検知部２２２と、通知部２２３とを有する。以下、制御部２２０が有する各部について説明する。

[0034] 取得部２２１は、下位ＮＷ装置２００に接続される端末の通信に関する情報を取得する。例えば、取得部２２１は、下位ＮＷ装置２００に接続される

ＯＡ機器やＩｏＴ機器の通信に関する情報を取得する。

[0035] 例えば、取得部２２１は、通信に関する情報として、通信日時や接続先ＩＰアドレス、接続元ＩＰアドレス等を含むフローデータを取得する。

[0036] 検知部２２２は、取得部２２１により取得された下位ＮＷ装置２００に接続される端末の通信に関する情報に基づいて、不正な通信を検知する。例えば、検知部２２２は、取得部２２１により取得された下位ＮＷ装置２００に接続される端末の通信に関する情報と、記憶部２３０に記憶される不正な通信に関する情報とを照合することにより、不正な通信を検知する。

[0037] また、検知部２２２は、下位ＮＷ装置２００から送信された下位ＮＷ装置２００に接続される端末の通信に関する情報と、外部装置に記憶される不正な通信に関する情報とを照合することにより、不正な通信を検知してもよい。

[0038] なお、検知部２２２は、記憶部１３０に記憶される不正な通信に関する情報そのものを不正な通信として検知してもよい。例えば、検知部２２２は、記憶部１３０が記憶する、下位ＮＷ装置２００が関与する通信内容と、外部装置に記憶される過去のサイバー攻撃の情報等を併せて分析することにより得られる情報そのものを、不正な通信として検知してもよい。

[0039] 例えば、検知部２２２は、アンダーレイＮＷにおいて収集されるＩＳＰ（Internet Serves Provider）のデータとして、例えばトラフィック量の変動の異常、異常なトラフィックのパターン等、通信の特性に応じた検知を行う。なお、検知部２２２は、既存のどのような検知手法を用いてもよい。

[0040] 通知部２２３は、検知部２２２により検知された不正な通信の情報を上位ＮＷ装置１００に通知する。例えば、通知部２２３は、検知部２２２により検知された不正な通信の情報として、不正な通信の検知日時、検知種別、接続先ＩＰアドレス、接続元ＩＰアドレスといった情報を上位ＮＷ装置１００に通知する。

[0041] このように、通知部２２３は、検知部２２２により不正な通信が検知された場合には、不正な通信の情報を上位ＮＷ装置１００へ直ちに通知する。こ

のため、上位ＮＷ装置１００は、通信を許可しないＩＰアドレスのリストに不正なＩＰアドレスを追加することで、即時にオーバレイサービスに反映することが可能となり、オーバレイＮＷとアンダーレイＮＷとが連携して、不正通信の検知精度を高めることが可能となる。

[0042] ［情報処理システムによる処理の概要］

次に、図５を用いて、情報処理システム１による処理について説明する。図５は、情報処理システム１による処理の概要を説明するための図である。

[0043] まず、下位ＮＷ装置２００の取得部２２１は、下位ＮＷ装置２００に接続される端末の通信に関する情報を取得する。例えば、下位ＮＷ装置２００に接続されるＯＡ機器やＩｏＴ機器等の通信に関する情報を取得する。

[0044] 続いて、下位ＮＷ装置２００の検知部２２２は、取得部２２１により取得された下位ＮＷ装置２００に接続される端末の通信に関する情報に基づいて、不正な通信を検知する。

[0045] 続いて、下位ＮＷ装置２００の通知部２２３は、検知部２２２により検知された不正な通信の情報を上位ＮＷ装置１００に通知する。

[0046] そして、上位ＮＷ装置１００の遮断部１２１は、通知部２２３により通知された不正な通信の情報に基づいて、不正な通信の通信先への通信を遮断する。

[0047] 遮断部１２１は、外部装置と連携し、悪性端末のＩＰアドレスをリストに追加し、フィルタリングを行う。例えば、遮断部１２１は、アンダーレイＮＷでフローデータの分析やＤＤｏＳ（Distributed Denial of Service）の分析により発見したＣ２（Command and Control server）サーバのＩＰアドレスが記憶されたデータベースを利用し、上位ＮＷ装置１００であるＵＴＭのセキュリティ機能の１つであるファイアウォールのＡＣＬ（Access Control List）に従ってアクセス制御を行い、Ｃ２への通信を遮断する。

[0048] このように、上位ＮＷ装置１００は、各アンダーレイＮＷで検知された悪性フローの検知結果を集中的に収集しつつ、通信を許可しないＩＰアドレスのリストに追加してオーバレイＮＷで不正通信を遮断することで、検知精度

を高めることを可能にした。さらに、上位ＮＷ装置１００は、利用者がオーバレイＮＷのみを利用し、アンダーレイＮＷは他社を利用している場合であっても、オーバレイＮＷで遮断を実現することで、このような利用者にも不正通信を遮断するサービスを精度よく提供することが可能である。

[0049] また、情報処理システム１では、オーバレイＮＷとアンダーレイＮＷとを同一事業者が提供している。また、情報処理システム１を利用する利用者は、例えば、オーバレイＮＷのみの利用し、アンダーレイＮＷは他社を利用する等の柔軟な利用を可能とする。

[0050] このように、情報処理システム１は、上位ＮＷ装置１００と下位ＮＷ装置２００とが密接に連携して、不正な通信の検知・遮断を行う。

[0051] ［情報処理システムによる検知・遮断処理］

次に、図６を用いて、情報処理システム１による検知処理と遮断処理とについて説明する。図６は、情報処理システム１による検知処理と遮断処理とを説明するための図である。

[0052] 図６（１）に示すように、下位ＮＷ装置２００の記憶部２３０には、不正な通信先の種別、ＩＰアドレスといった不正な通信に関する情報が記憶されている。ここで、記憶部２３０に記憶される不正な通信に関する情報は、下位ＮＷ装置２００が関与する通信内容と、外部装置に記憶される過去のサイバー攻撃の情報等を併せて分析することにより得られる情報であってもよい。

[0053] 例えば、記憶部２３０は、下位ＮＷ装置２００に接続される端末の通信に関する情報と、過去のＤＤｏＳ攻撃情報との分析により得られた、不正な通信先の種別やＩＰアドレスといった不正な通信に関する情報を記憶する。

[0054] 下位ＮＷ装置２００の検知部２２２は、取得部２２１により取得された下位ＮＷ装置２００に接続される端末の通信に関する情報と、記憶部２３０に記憶される不正な通信に関する情報とを照合することにより、不正な通信を検知する。なお、このとき、検知部２２２は、記憶部１３０に記憶される不正な通信に関する情報そのものを不正な通信として検知してもよい。例えば

、検知部２２２は、不正な通信として、種別「Ｃ２サーバ」、ＩＰアドレス「２０３．０．１１３．１５」を検知する。

[0055] 下位ＮＷ装置２００の通知部２２３は、検知部２２２により検知された不正な通信の情報（種別「Ｃ２サーバ」、ＩＰアドレス「２０３．０．１１３．１５」）を上位ＮＷ装置１００に通知する。

[0056] そして、上位ＮＷ装置１００の遮断部１２１は、下位ＮＷ装置２００から通知された不正な通信の情報を用いて、不正な通信の通信先への通信を遮断する。例えば、遮断部１２１は、図６（２）に示すように、通知された不正な通信先のＩＰアドレス「２０３．０．１１３．１５」の情報を、通信を許可しないＩＰアドレスのリストに追加することで、フィルタリングにより、不正な通信の通信先への通信を遮断する。

[0057] このように、情報処理システム１は、上位ＮＷ装置１００と下位ＮＷ装置２００とが連携して、不正な通信を検知し、不正な通信を遮断する。

[0058] ［フローチャート］

次に、図７を用いて、情報処理システム１による処理の流れについて説明する。なお、下記の各ステップは、異なる順序で実行することもでき、また、省略される処理があってもよい。

[0059] まず、下位ＮＷ装置２００の取得部２２１は、下位ＮＷ装置２００に接続される端末の通信に関する情報を取得する（ステップＳ１０１）。例えば、取得部２２１は、下位ＮＷ装置２００に接続されるＯＡ機器やＩｏＴ機器の通信に関する情報を取得する。

[0060] 次に、下位ＮＷ装置２００の検知部２２２は、取得部２２１により取得された下位ＮＷ装置２００に接続される端末の通信に関する情報に基づいて、不正な通信を検知する（ステップＳ１０２）。例えば、検知部２２２は、取得部２２１により取得された下位ＮＷ装置２００に接続される端末の通信に関する情報と、記憶部１３０に記憶される不正な通信に関する情報とを照合することにより、不正な通信を検知する。

[0061] 下位ＮＷ装置２００の通知部２２３は、検知部２２２により検知された不

正な通信の情報を上位ＮＷ装置１００に通知する（ステップＳ１０３）。例えば、通知部２２３は、検知部２２２により検知された不正な通信の情報として、種別、ＩＰアドレスといった情報を上位ＮＷ装置１００に通知する。

[0062] 上位ＮＷ装置１００の遮断部１２１は、通知部２２３により通知された不正な通信の情報に基づいて、不正な通信を遮断する（ステップＳ１０４）。例えば、遮断部１２１は、通知部２２３により通知された不正な通信の情報を用いて、不正な通信の通信先への通信を遮断する。

[0063] ［効果］

実施形態に係る情報処理システム１は、オーバレイネットワークを構成する装置である上位ＮＷ装置１００とアンダーレイネットワークを構成する装置である下位ＮＷ装置２００とからなる情報処理システムであって、上位ＮＷ装置１００は、下位ＮＷ装置２００から通知された不正な通信の情報に基づいて、不正な通信を遮断する遮断部１２１を有し、下位ＮＷ装置２００は、下位ＮＷ装置２００に接続される端末の通信に関する情報を取得する取得部２２１と、取得部２２１により取得された下位ＮＷ装置２００に接続される端末の通信に関する情報に基づいて、不正な通信を検知する検知部２２２と、検知部２２２により検知された不正な通信の情報を、上位ＮＷ装置１００に通知する通知部２２３とを有する。

[0064] これにより情報処理システム１は、下位ＮＷ装置２００が取得した情報から不正な通信を検知し、検知した不正な通信の情報を上位ＮＷ装置１００に通知して遮断することにより、堅牢なセキュリティを実現することができる。

[0065] 実施形態に係る情報処理システム１の下位ＮＷ装置２００における検知部２２２は、取得部２２１により取得された下位ＮＷ装置２００に接続される端末の通信に関する情報と、記憶部２３０に記憶される不正な通信に関する情報とを照合することにより、不正な通信を検知する。

[0066] これにより情報処理システム１は、下位ＮＷ装置２００に接続される端末の通信に関する情報と不正な通信に関する情報とを照合して不正な通信を検

知することにより、堅牢なセキュリティを実現することができる。

[0067] 実施形態に係る情報処理システム１の上位ＮＷ装置１００における遮断部１２１は、下位ＮＷ装置２００から通知された不正な通信の情報を用いて、不正な通信の通信先への通信を遮断する。

[0068] これにより情報処理システム１は、通知された不正な通信の情報を用いて、不正な通信の通信先への通信を遮断することにより、堅牢なセキュリティを実現することができる。

[0069] ［プログラム］

上記実施形態において説明した情報処理システム１が実行する処理をコンピュータが実行可能な言語で記述したプログラムを作成することもできる。この場合、コンピュータがプログラムを実行することにより、上記実施形態と同様の効果を得ることができる。さらに、かかるプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータに読み込ませて実行することにより上記実施形態と同様の処理を実現してもよい。

[0070] 図８は、情報処理プログラムを実行するコンピュータの一例を示す図である。図８に示すように、コンピュータ１０００は、例えば、メモリ１０１０と、ＣＰＵ１０２０と、ハードディスクドライブインタフェース１０３０と、ディスクドライブインタフェース１０４０と、シリアルポートインタフェース１０５０と、ビデオアダプタ１０６０と、ネットワークインタフェース１０７０とを有する。これらの各部は、バス１０８０によって接続される。

[0071] メモリ１０１０は、ＲＯＭ（Read Only Memory）１０１１および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。ディスクドライブ１１００には、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挿入される。シリアルポートインタフェー

ス１０５０には、例えば、マウス１１１０およびキーボード１１２０が接続される。ビデオアダプタ１０６０には、例えば、ディスプレイ１１３０が接続される。

[0072] ここで、図８に示すように、ハードディスクドライブ１０９０は、例えば、ＯＳ（Operating System）１０９１、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およびプログラムデータ１０９４を記憶する。上記実施形態で説明した各テーブルは、例えばハードディスクドライブ１０９０やメモリ１０１０に記憶される。

[0073] また、情報処理プログラムは、例えば、コンピュータ１０００によって実行される指令が記述されたプログラムモジュールとして、ハードディスクドライブ１０９０に記憶される。具体的には、上記実施形態で説明したコンピュータ１０００が実行する各処理が記述された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。

[0074] また、情報処理プログラムによる情報処理に用いられるデータは、プログラムデータとして、例えば、ハードディスクドライブ１０９０に記憶される。そして、ＣＰＵ１０２０が、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、上述した各手順を実行する。

[0075] なお、情報処理プログラムに係る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れず、例えば、着脱可能な記憶媒体に記憶されて、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、制御プログラムに係るプログラムモジュール１０９３やプログラムデータ１０９４は、ＬＡＮやＷＡＮ（Wide Area Network）等のネットワークを介して接続された他のコンピュータに記憶され、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。

[0076] ［その他］

様々な実施形態を、図面を参照して、本明細書で詳細に説明したが、これ

らの複数の実施形態は例であり、本発明をこれらの複数の実施形態に限定することを意図するものではない。本明細書に記載された特徴は、当業者の知識に基づく様々な変形や改良を含む、様々な方法によって実現され得る。

[0077] また、上述した「部（module、-er接尾辞、-or接尾辞）」は、ユニット、手段、回路などに読み替えることができる。例えば、通信部（communication module）、制御部（control module）および記憶部（storage module）は、それぞれ、通信ユニット、制御ユニットおよび記憶ユニットに読み替えることができる。

符号の説明

[0078]

１ 情報処理システム

１００ 上位ＮＷ装置

１１０ 通信部

１２０ 制御部

１２１ 遮断部

１３０ 記憶部

２００ 下位ＮＷ装置

２１０ 通信部

２２０ 制御部

２２１ 取得部

２２２ 検知部

２２３ 通知部

２３０ 記憶部

請求の範囲

[請求項1] オーバレイネットワークを構成する装置である上位ＮＷ装置とアンダーレイネットワークを構成する装置である下位ＮＷ装置とからなる情報処理システムであって、

前記上位ＮＷ装置は、

前記下位ＮＷ装置から通知された不正な通信の情報に基づいて、前記不正な通信を遮断する遮断部

を有し、

前記下位ＮＷ装置は、

前記下位ＮＷ装置に接続される端末の通信に関する情報を取得する取得部と、

前記取得部により取得された前記下位ＮＷ装置に接続される端末の通信に関する情報に基づいて、前記不正な通信を検知する検知部と、

前記検知部により検知された前記不正な通信の情報を、前記上位ＮＷ装置に通知する通知部と

を有することを特徴とする情報処理システム。

[請求項2] 前記検知部は、前記取得部により取得された前記下位ＮＷ装置に接続される端末の通信に関する情報と、記憶部に記憶される不正な通信に関する情報とを照合することにより、不正な通信を検知する

ことを特徴とする請求項１に記載の情報処理システム。

[請求項3] 前記遮断部は、下位ＮＷ装置から通知された不正な通信の情報を用いて、前記不正な通信の通信先への通信を遮断する

ことを特徴とする請求項１に記載の情報処理システム。

[請求項4] オーバレイネットワークを構成する装置である上位ＮＷ装置とアンダーレイネットワークを構成する装置である下位ＮＷ装置とが実行する情報処理方法であって、

前記下位ＮＷ装置が、前記下位ＮＷ装置に接続される端末の通信に関する情報を取得する取得工程と、

前記下位ＮＷ装置が、前記取得工程により取得された前記下位ＮＷ装置に接続される端末の通信に関する情報に基づいて、不正な通信を検知する検知工程と、

前記下位ＮＷ装置が、前記検知工程により検知された前記不正な通信の情報を、前記上位ＮＷ装置に通知する通知工程と

前記上位ＮＷ装置が、前記下位ＮＷ装置から通知された不正な通信の情報に基づいて、前記不正な通信を遮断する遮断工程と

を含むことを特徴とする情報処理方法。

[請求項5] オーバレイネットワークを構成する装置である上位ＮＷ装置としてのコンピュータと、アンダーレイネットワークを構成する装置である下位ＮＷ装置としてのコンピュータに実行させる情報処理プログラムであって、

前記上位ＮＷ装置としてのコンピュータに、

前記下位ＮＷ装置から通知された不正な通信の情報に基づいて、前記不正な通信を遮断する遮断ステップ

を実行させ、

前記下位ＮＷ装置としてのコンピュータに、

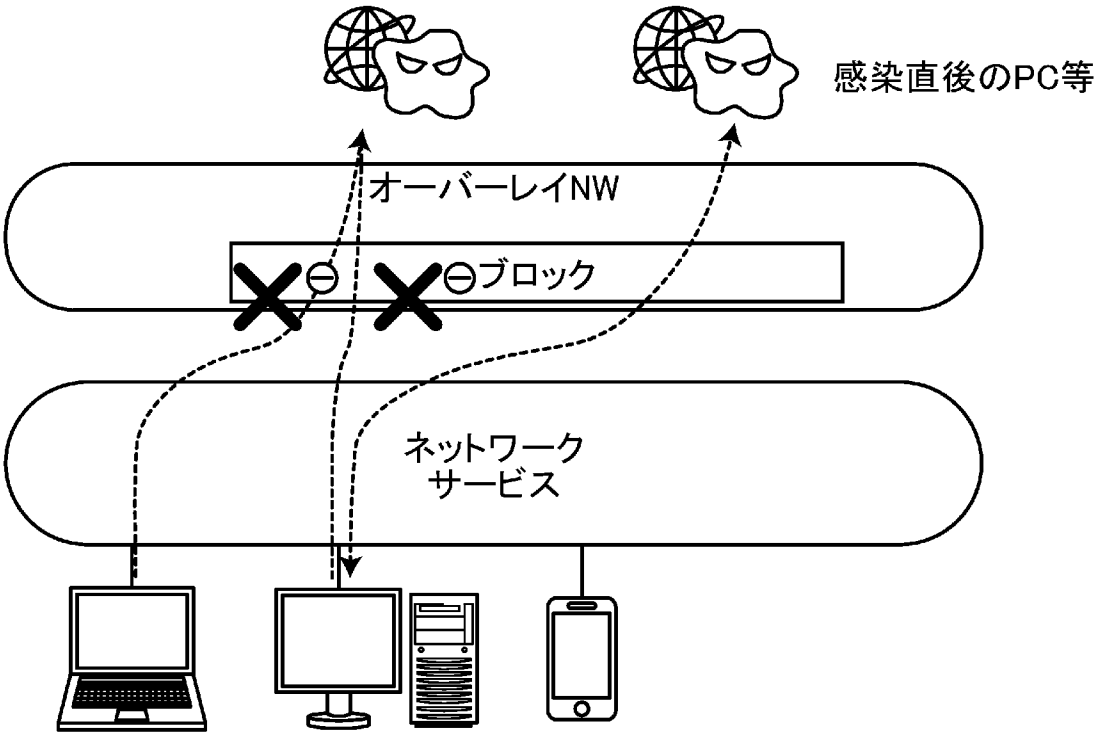
前記下位ＮＷ装置に接続される端末の通信に関する情報を取得する取得ステップと、

前記取得ステップにより取得された前記下位ＮＷ装置に接続される端末の通信に関する情報に基づいて、前記不正な通信を検知する検知ステップと、

前記検知ステップにより検知された前記不正な通信の情報を、前記上位ＮＷ装置に通知する通知ステップと

を実行させることを特徴とする情報処理プログラム。

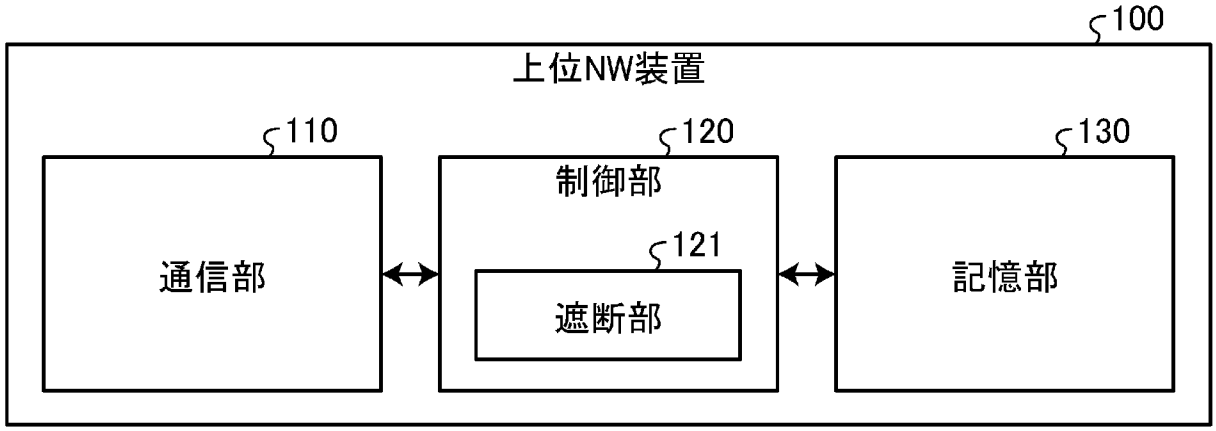
[図1]


感染直後のPC等
オーバーレイNW
ブロック
ネットワーク
サービス

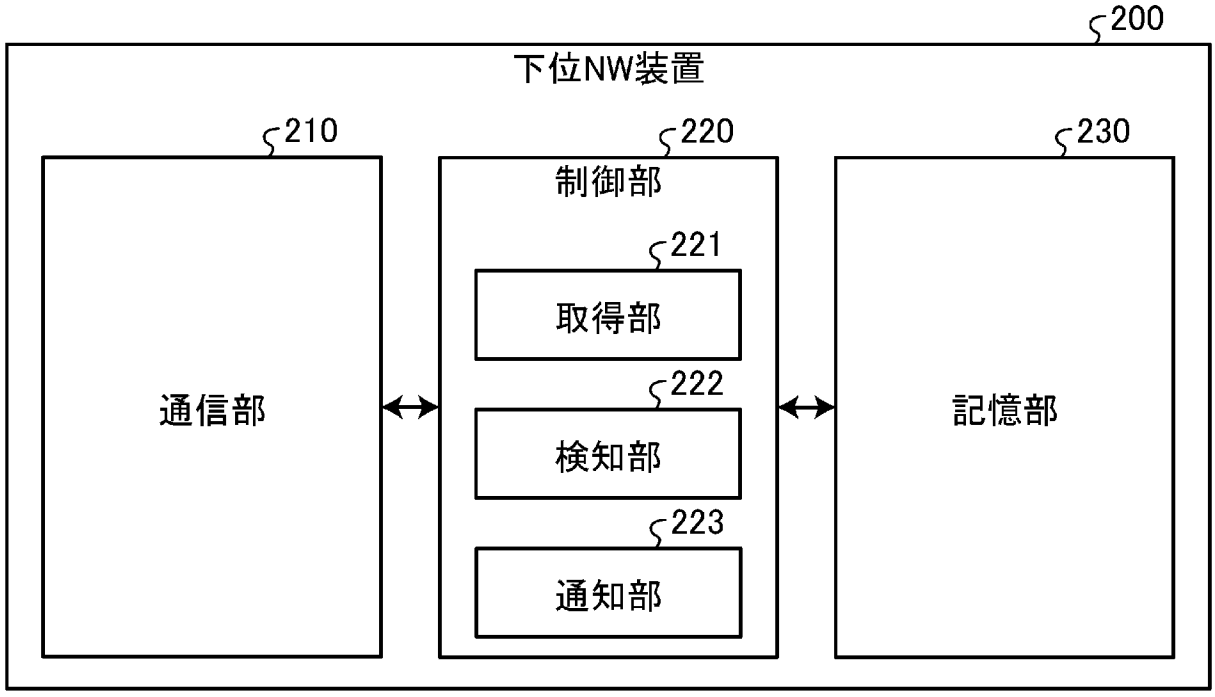
[図2]


1
情報処理システム
100
上位NW装置
200
下位NW装置

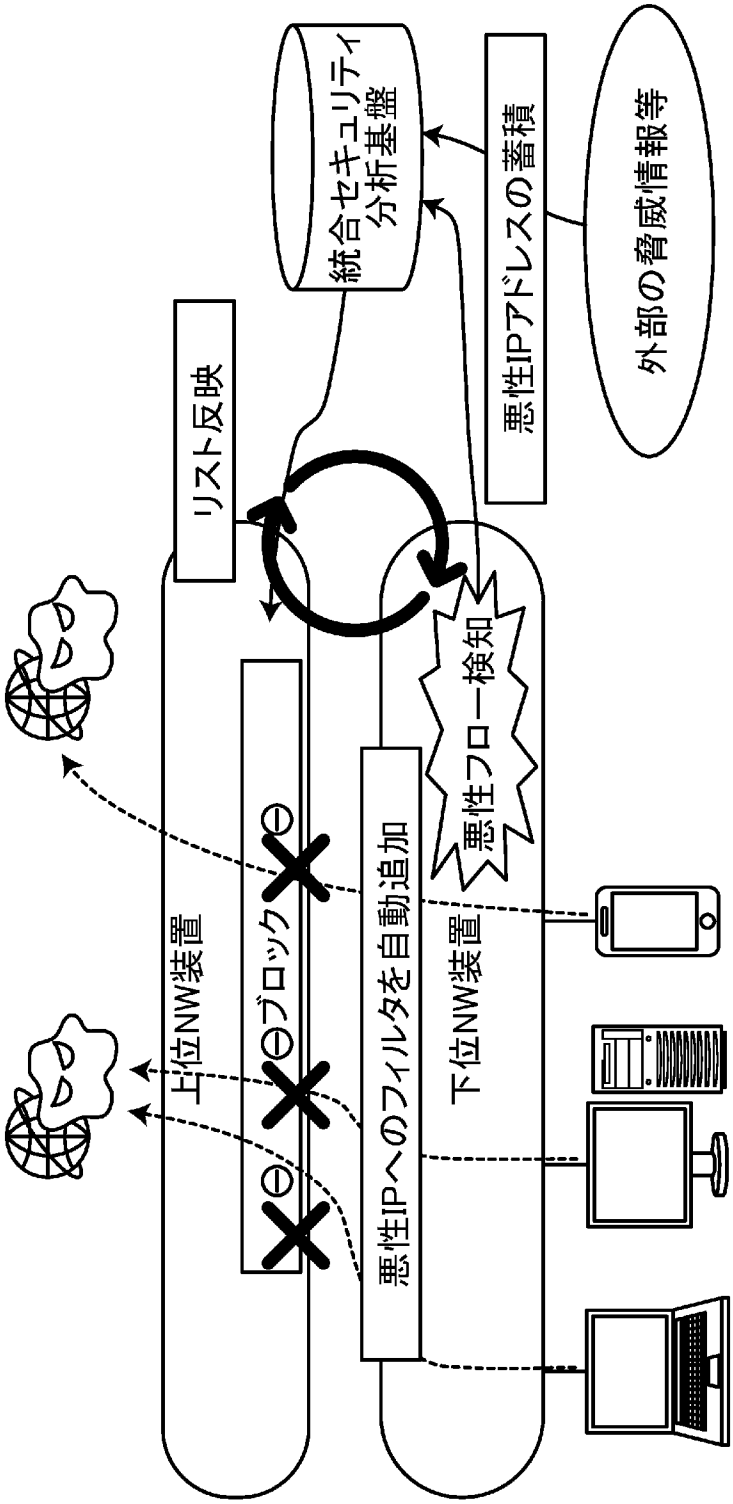
[図3]


100
上位NW装置
110
通信部
120
制御部
121
遮断部
130
記憶部

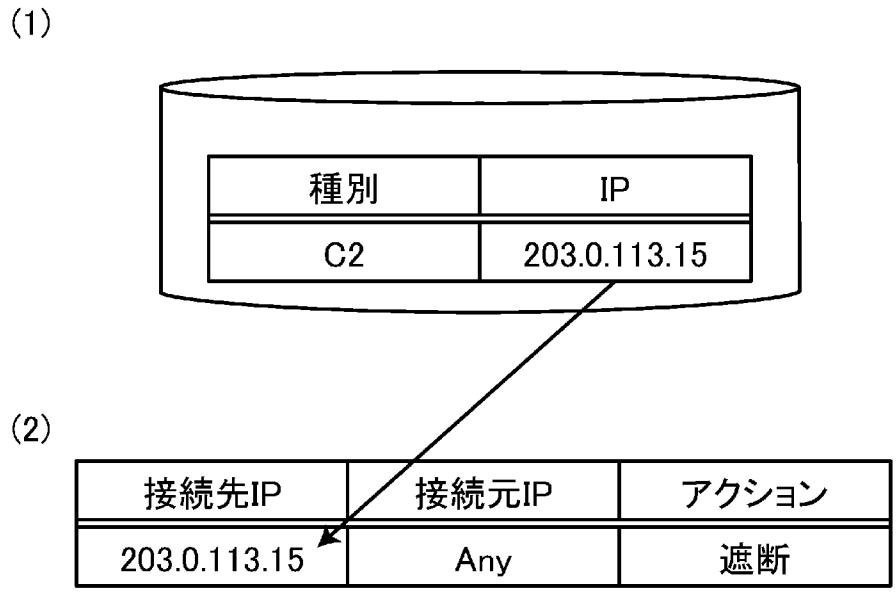
[図4]


200
下位NW装置
210
通信部
220
制御部
221
取得部
222
検知部
223
通知部
230
記憶部

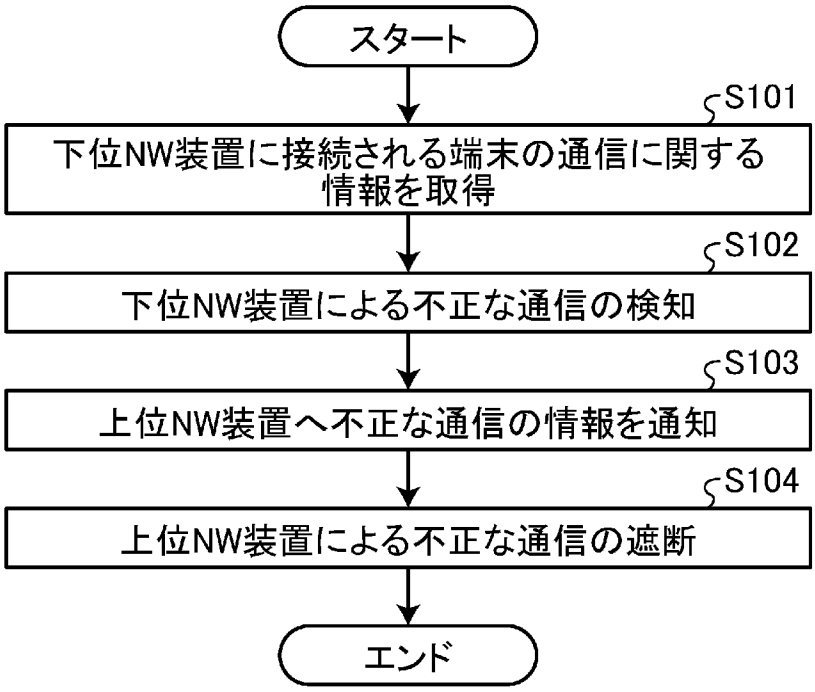
[図5]


統合セキュリティ
分析基盤
悪性IPアドレスの蓄積
外部の脅威情報等
リスト反映
悪性フロー検知
悪性IPへのフィルタを自動追加
ブロック
上位NW装置
下位NW装置

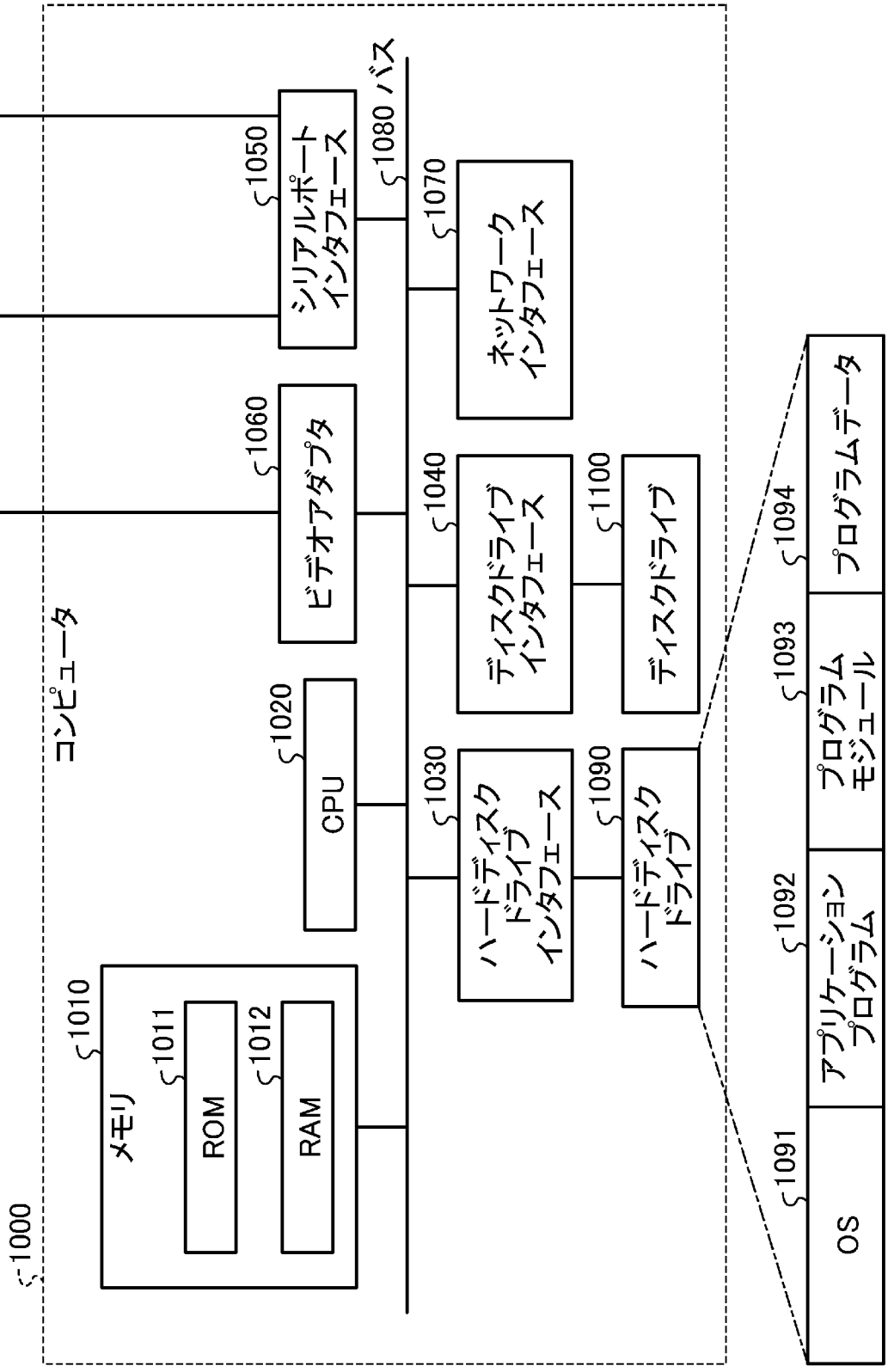
[図6]


(1)
種別
IP
C2
203.0.113.15
(2)
接続先IP
接続元IP
アクション
203.0.113.15
Any
遮断

[図7]


スタート
S101
下位NW装置に接続される端末の通信に関する情報を取得
S102
下位NW装置による不正な通信の検知
S103
上位NW装置へ不正な通信の情報を通知
S104
上位NW装置による不正な通信の遮断
エンド

[図8]


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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2023/024528

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/66(2006.01)i; ***H04L 12/22***(2006.01)i; ***H04L 41/06***(2022.01)i; ***H04L 43/08***(2022.01)i
FI: H04L12/66; H04L41/06; H04L43/08; H04L12/22

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)

H04L12/66; H04L12/22; H04L41/06; H04L43/08

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 1971-2023
Registered utility model specifications of Japan 1996-2023
Published registered utility model applications of Japan 1994-2023

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	US 2017/0070531 A1 (ARBOR NETWORKS, INC.) 09 March 2017 (2017-03-09) particularly, paragraphs [0018]-[0033], fig. 1, 2, etc.	1-5
A	US 2022/0278889 A1 (ZSCALER, INC.) 01 September 2022 (2022-09-01) particularly, paragraphs [0041]-[0052], fig. 1, 2, etc.	1-5
A	JP 2010-508598 A (ALCATEL-LUCENT USA INC.) 18 March 2010 (2010-03-18) paragraphs [0014]-[0042], fig. 1, 2, 3, 6, etc.	1-5
A	マルウェア対策強化とネットワークのトラブル対応迅速化, FUJITSU Network VELCOUN-X/Palo Alto PAシリーズ連携, Interop Tokyo 2019, 12 June 2019 (received date), non-official translation (Strengthen anti-malware measures and speed up response to network troubles, Palo Alto PA series cooperation) entire text, all drawings	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
21 July 2023	**01 August 2023**
Name and mailing address of the ISA/JP **Japan Patent Office (ISA/JP)** **3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915** **Japan**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2023/024528

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
US 2017/0070531 A1	09 March 2017	(Family: none)	
US 2022/0278889 A1	01 September 2022	(Family: none)	
JP 2010-508598 A	18 March 2010	US 2008/0109905 A1 paragraphs [0016]-[0045], fig. 1, 2, 3, 6 WO 2008/063343 A2 KR 10-2009-0087437 A CN 101529862 A	

国際調査報告

国際出願番号
PCT/JP2023/024528

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

H04L 12/66(2006.01)i; H04L 12/22(2006.01)i; H04L 41/06(2022.01)i; H04L 43/08(2022.01)i
FI: H04L12/66; H04L41/06; H04L43/08; H04L12/22

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））

H04L12/66; H04L12/22; H04L41/06; H04L43/08

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	１９７１－２０２３年
日本国実用新案登録公報	１９９６－２０２３年
日本国登録実用新案公報	１９９４－２０２３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	US 2017/0070531 A1 (ARBOR NETWORKS, INC.) 09.03.2017 (2017-03-09) 特に、[0018]-[0033],FIG.1,2等	1-5
A	US 2022/0278889 A1 (ZSCALER, INC.) 01.09.2022 (2022-09-01) 特に、[0041]-[0052], FIGs.1,2等	1-5
A	JP 2010-508598 A (アルカテルールーセント ユーエスエー インコーポレーテッド) 18.03.2010 (2010-03-18) [0014]-[0042],図1,2,3,6等	1-5
A	マルウェア対策強化とネットワークのトラブル対応迅速化、ＦＵＪＩＴＳＵ Ｎｅｔｗｏｒｋ ＶＥＬＣＯＵＮ－Ｘ／Ｐａｌｏ Ａｌｔｏ ＰＡシリーズ連携，Ｉｎｔｅｒｏｐ Ｔｏｋｙｏ ２０１９，2019.06.12（受入日） 全文、全図	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抵触するものではなく、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
21.07.2023	01.08.2023

名称及びあて先
日本国特許庁(ISA/JP)
〒100-8915
日本国
東京都千代田区霞が関三丁目４番３号

権限のある職員（特許庁審査官）
羽岡　さやか 5X 3149
電話番号 03-3581-1101 内線 3596

国際調査報告
パテントファミリーに関する情報

国際出願番号
PCT/JP2023/024528

引用文献	公表日	パテントファミリー文献	公表日
US 2017/0070531 A1	09.03.2017	（ファミリーなし）	
US 2022/0278889 A1	01.09.2022	（ファミリーなし）	
JP 2010-508598 A	18.03.2010	US 2008/0109905 A1 [0016]-[0045],FIGs.1,2,3,6 WO 2008/063343 A2 KR 10-2009-0087437 A CN 101529862 A	