広島大学先進理工系科学研究科情報科学プログラム修士論文

組織内ネットワークにおけるチェックリスト型ネットワーク診断モデルに基づく対話型自己診断システムの開発と評価

2024年2月

広島大学先進理工系科学研究科情報科学プログラム

M225832

中野 敦斗

指導教員 近堂 徹

広島大学

Thesis for Master Degree
Informatics and Data Science Program, Graduate School of Advanced Science and Engineering,
Hiroshima University

Development and Evaluation of Interactive Self-Diagnosis System of Large-Scale Network Based on Checklist-based Network Diagnostic Model

February 2024

Informatics and Data Science Program,
Graduate School of Advanced Science and Engineering,
Hiroshima University

M225832

Nakano, Atsuto

Supervisor: Kondo, Tohru

Hiroshima University

要旨

ネットワークインフラとして無線 LAN サービスが組織活動に不可欠な役割を担うようになり，無線 LAN 接続に対して高速で高い信頼性が求められるようになった．多数の人数が集中して利用するような無線 LAN 環境においては，「ネットワークに繋がらない」あるいは「ネットワークの通信速度が遅い」といった接続トラブルが発生する可能性がある．無線 LAN が通信に用いる電波は不可視なものであり，トラブルに遭遇した利用者が原因および解決策を特定するために十分な情報が得られるとは限らない．このことから，利用者に対して，直面する接続トラブルの解決に導くために，迅速に接続状態や品質といった情報を適切にフィードバックする仕組みが必要になると考えられる．

既存の取り組みとして，ネットワーク管理ツールおよび管理手法が提案されている．これらの管理手法は主にネットワーク管理者によって利用されることを前提として設計されており，ネットワーク利用者に対して直接問題解決の支援を行うものではない．これに対し，利用者にネットワーク統計情報を公開することで，利用者自身によるトラブル解決を促す仕組みがある．しかし，提供される情報から解決のための行動を導き出せるかは個人のリテラシーに依存する．

以上を踏まえ，ネットワーク利用者自身が解決可能な問題については，ネットワークログおよび利用端末の状態をもとに原因と解決策の特定を行い，利用者自身に直接フィードバックすることを考える．本研究では，システムによる組織内ネットワークの自律的な診断を可能とする診断モデルチェックリスト型ネットワーク診断モデルを提案し，モデルを実装したプロトタイプシステム Netdoctor の開発および評価を行った．

チェックリスト型ネットワーク診断モデルは，診断を行う際にチェックリストに列挙された問題の発生有無をネットワーク統計情報及び利用者との対話の中から逐一確認していくことで問題箇所を特定していく方法である．チェックリストに列挙された問題それぞれに対して，ADU(Atomic Diagnosis Unit) と呼ぶ対話フローと，ADU を症状別に分類した ADUS(ADUs by Symptom) を定義し，開発システムに導入した．開発システムの動作の様子は，`https://youtu.be/0fM5CdN5bJ0`(URL) から確認できる．

評価は，提案システムと類似ツールの機能面での比較による定性的評価と評価実験の 2 種類を行った．評価実験では，意図的にネットワーク障害を発生させた無線 LAN 環境を用意し，広島大学構成員からなる被験者に対して開発システムによる問題解決を体験してもらい，質問紙によるアンケートによるシステム評価を行った．その結果，収集データの多様性には課題が残るものの，利用者に直接フィードバックする機能は開発システムの独自性であることを確認した．また，実験評価では発生する問題の種類に依存しない安定した診断が行われるようにシステムを改善する必要はある一方で，今回想定したシナリオではほとんど全ての被験者が迅速に問題解決に至ることが分かった．これにより，受付時間外など窓口での対応が困難な場合でも以前より迅速なトラブル解決が可能となることが期待される．

Abstract

Wireless LAN services have come to play an indispensable role in organizational activities as network infrastructure, and high speed and high reliability are required for wireless LAN connections. In a wireless LAN environment where a large number of people are concentrated, connection problems such as "no network connection" or "slow network speed" may occur. The radio waves used by wireless LANs for communication are invisible, and users who encounter problems do not always have sufficient information to identify the causes and solutions. Therefore, it is considered necessary to provide users with a mechanism to promptly and appropriately feed back information such as connection status and quality in order to help them solve the connection problems they face.

Existing efforts have proposed network management tools and techniques. These management methods are mainly designed to be used by network administrators and do not provide direct problem-solving support to network users. On the other hand, there is a mechanism that encourages users to solve problems by themselves by disclosing network statistics to them. However, it depends on individual literacy to be able to derive actions for solving problems from the information provided.

Based on the above, we decided to feedback the trouble factors and solutions directly to network users, using network log and the status of the terminal. In this research, we proposed Checklist-based Network Diagnostic Model(CNDM), developed and evaluated a prototype system "Netdoctor" which the CNDM applied to.

Model CNDM is a method of identifying problem areas by checking the occurrence of each of the problems listed in the checklist from network logs and the status of the user's terminal during diagnosis. For each of the problems listed in the checklist, we defined a dialogue flow called ADU(Atomic Diagnosis Unit), and ADUS(ADUs by Symptom), which classifies ADU according to symptoms, and introduced them into the system to develop. The system behavioral demonstration can be found at the following URL: `https://youtu.be/0fM5CdN5bJ0`.

The system evaluation was conducted in two ways: 1)the functional comparison between the similar systems and 2)the experimental demonstration. In the experimental demonstration, the environment in which the network failure was intentionally generated was prepared, and subjects consisting of Hiroshima University members experienced solving the problems. After that, a questionnaire was conducted to the subjects. As the result, while it remains a challenge of the diversity of data collections, we confirmed that the functionality that the system provided network users with solutions was the originality of this research. Also, while the system is to be independent from the variation of the trouble, in these scenarios, almost all of subjects could solved the problem. This is expected to enable quicker troubleshooting than before, even when it is difficult to respond to a problem at the counter, such as after hours.

目次

第 1 章　はじめに

1.1　研究背景

リモートワークやオンライン講義などの普及に伴い，教育研究機関および企業といった大規模な組織において，構成員がリソースへのアクセスにネットワークを用いることが一般的となった．構成員がネットワークにアクセスする方法としては，無線 LAN を利用する形態が広く普及している．無線 LAN を利用したネットワークシステムの一例として，広島大学におけるキャンパスネットワーク「HINET Wi-Fi」では 1,200 台以上の無線 LAN アクセスポイント (以下，AP) が学内全ての講義室および共用スペース (図書館・食堂など) を中心に設置されている [1]．広島大学においても，無線 LAN が教職員および学生を含む構成員によるネットワークへのアクセス手段として主要なものとして利用されており，特に学習管理システム (LMS) およびオンライン授業を含む教育研究活動を実施するために利用されている．HINET を含む無線 LAN が組織活動に不可欠な役割を担う組織においては，無線 LAN を利用したネットワークアクセスの信頼性が高く保証されている必要がある．

無線 LAN 通信に一般的に用いられるプロトコルである IEEE802.11 シリーズでは，CSMA/CA(Carrier Sense Multiple Access/Collision Avoidance) がチャネルアクセス方式として採用されている．そのため，AP と通信端末間での電波状態および通信端末の状態によっては，「ネットワークに繋がらない」「ネットワークの通信速度が極端に遅い」といった接続品質低下が発生する可能性がある．また，1 台の AP に対して 80 台程度の多数の端末による通信が行われている環境において，モバイル Wi-Fi を含む Rogue AP による同一チャネル上の通信が正規の AP との通信に悪影響を与えることが指摘されているほか [2]，無線 LAN の接続規格および周波数によって通信可能な最大の同時接続可能台数が変化することが報告されている [3]．接続品質低下の要因としては有線ネットワーク区間における輻輳がある一方で，利用端末がアソシエーションしている AP が不適切な場合といったように，利用者自身が端末ごと移動するなど利用者自身によるアクションにより解決できるものも存在する．しかしながら，電波は実際に目に見えないことから，利用者には漠然と「繋がらない」「遅い」といった症状を経験するだけで，原因を特定するために十分な情報が得られるとは限らない．そのため，多くの利用者にとっては自力で問題解決をすることは困難である．

これに対し，一部の組織では IT 管理部門などが相談窓口が設けられ，構成員がネットワークを利用できないといったトラブルに対処できる仕組みづくりが行われている．しかし，相談窓口における対応は一般的に時間がかかるものであり，また窓口の営業時間外に発生したトラブルに関しては対処できない．それにより，トラブルが発生するタイミングによってはネットワークが活動に不可欠な役割を担っているような場合に組織活動そのものが停止してしまう可能性がある．

以上を踏まえ，ネットワーク状況を利用者に対してフィードバックする仕組みを整えることで，ネットワーク整備による解決が難しく，かつネットワーク利用者のみで解決が行える接続トラブルを迅速に解決することが可能であることが考えられる．

1.2　既存研究

■ ネットワーク監視への取り組み

ネットワーク信頼性を維持するため，多くの管理ツール・手法が提案されている．ネットワーク管理ツールはいずれもネットワーク管理者によって利用されることを前提として設計されており，またツールによって監視対象のネットワーク区間が異なる場合がある．大規模な無線 LAN システムにおいて，ネットワーク区間は大分類として有線区間と無線区間があり，有線区間を管理するツールにも，サービスを提供するサーバやネッ

トワークのリソース状態を監視するものと，ネットワークスイッチや DNS といったネットワーク機器に対して設定投入するソリューションが存在する．

サーバ・ネットワーク監視ツール　特に，サーバの状態を監視するツールの代表的な例としては，オープンソースソフトウェアである Nagios[*1]，Prometheus[*2]，Zabbix[*3]といった監視ソリューションがあるが，これらのソリューションは対象ネットワーク上のサーバおよびサービス，ネットワーク機器から統計情報を収集し，ネットワーク管理者に対して収集した情報の可視化や，アラートの発令を実施することで管理を実現している．

ネットワーク構成管理システム　ネットワーク機器を設定・管理するツールに関しては導入対象のネットワークで用いられている機器やネットワークトポロジーにより構成方法が異なる場合があり，東京工業大学における Titanet4[4] や山口大学のネットワーク運用支援システム [5]，広島大学の HINET[1] など一部の教育研究機関で独自のツールが開発されている他，Red Hat, Inc. による Ansible[*4]や，HashiCorp 社による Terraform[*5]といった，サーバおよびネットワーク構成自動化ツールが製品として提供されている．

■ 無線 LAN 監視への取り組み

ベンダ製無線 LAN 監視ツール　無線 LAN に特化したネットワーク管理ツールがベンダから提供されている場合がある．代表的な例として，シスコシステムズ合同会社[*6]による無線 LAN ログ可視化無線 LAN システム管理を実施する Cisco Prime Infrastructure[*7]や Cisco Meraki[*8]などがある．そのほか，Aruba Network[*9]社が提供する Aruba Airwave[*10]や，Fortinet 社[*11]が提供する FortiGate[*12]無線 LAN コントローラ統合コンソールといったツールでも可視化が実現可能である．

キャンパスネットワークにおける取り組み　関連する研究として，石原氏らの研究 [6]，矢切氏らの研究 [7]，SINDAN Project[8, 9]，著者らの研究 [10, 11] が存在する．石原氏らは，時系列データベースを利用して無線 LAN コントローラから取得できる情報の蓄積・可視化を行うシステムを構築し，マルチベンダ環境におけるネットワーク統計情報の分析を実現している．矢切氏らは所属する研究機関におけるネットワークシステムに設置された各 AP から抽出できる特徴量に着目した分析を行うシステムを開発し，ネットワーク管理者がプロアクティブに異常の検出を行える仕組みの構築を行なっている．また，SINDAN Project では，利用者側からの接続品質を測定する目的で，AP に接続したセンサノードからネットワーク測定を行い，管理者による問題把握の迅速化を実現している．そのほか，著者らは組織内無線 LAN の品質情報を収集する基盤システムの開発と，システムで採用するデータベースに対する評価・検討を行った．これらの管理ツール及び既存研究は，管理者がネットワークの整備およびネットワークで発生した障害の特定，修正を行うことを目的として提供および開発が行われている．これらの管理者に対するデータ提供に加え，利用者への直接的なアプローチを行うことで，接続台数の急増といったように，利用者自身のアクションにより対処が可能な問題に対して利用者側で迅速に対処することができると期待される．

[*1] https://www.nagios.org/
[*2] https://prometheus.io/
[*3] https://www.zabbix.com/
[*4] https://www.ansible.com/
[*5] https://www.terraform.io/
[*6] https://www.cisco.com/
[*7] https://www.cisco.com/c/ja_jp/products/cloud-systems-management/prime-infrastructure/index.html
[*8] https://meraki.cisco.com/ja-jp/
[*9] https://www.arubanetworks.com/
[*10] https://www.arubanetworks.com/ja/products/network-management-operations/airwave/
[*11] https://www.fortinet.com/jp
[*12] https://www.fortinet.com/jp/products/next-generation-firewall

ネットワーク利用状況の公開　一部の教育研究機関においては，ネットワーク利用者に対してネットワーク状況を公開することで，接続品質を維持する取り組みが実際に行われている．具体例として，京都工業繊維大学情報科学センターでは，学内に設置された無線 LAN の利用状況，SSID ごとに公開する取り組みが行われている [12]．この事例では，ネットワーク利用者自身が混雑したアクセスポイントを回避し，適切な AP の接続を行うための支援を行うことを目的としている．また，神戸大学 [13] や九州工業大学 [14] においても同様の取り組みが行われている．これらの取り組みでは，ネットワーク利用者にネットワーク状況を直接フィードバックすることで，接続時のトラブルに遭遇している利用者に対して部屋の移動などの直接的なアクションを起こさせることを目的としている．一方で，これらの事例では提供されたネットワーク統計情報の解釈は全てネットワーク利用者が行う必要がある．そのため，与えられた情報から自分がとるべきアクションを導き出せるかどうかはネットワーク利用者個人のリテラシーに依存してしまう課題があると考えられる．

チャットボットによる問題特定　一方で，Juniper Networks, Inc による対話型 AI Marvis のような対話型 UI による接続品質低下要因の特定を管理者とチャットボットとの対話により実施するソリューションも存在する．これらの事例を踏まえ，接続品質に不満を持つネットワーク利用者に対してネットワークの状況を提供するだけでなく，統計やログから得られた情報を分析することで発生している問題内容と具体的なアクションを，チャットボットを通じてネットワーク利用者に提供する仕組みを提案する．

1.3　研究目的

ネットワーク整備のみでは解決できず，またネットワーク利用者が部屋の移動等解決策を実施するほうが組織の相談窓口にて対処を行うよりも早く解決ができる問題に関しては，事前に相談窓口等のトラブル対応にノウハウのある構成員がネットワーク内で発生する可能性のあるトラブルや障害，およびそれらに対する対処法を列挙しておき，構成員により表形式のチェックリストとしていつでも参照できるような仕組みを整えることにより対処が可能であると想定される．ネットワークのトラブルに遭遇したネットワーク利用者はここで作成されたチェックリストを利用し，問題の特定と対処を行うことで相談窓口へ向かうよりも迅速かつ簡便に問題解決が行えることが期待できる．

しかしながら，ここで作成されたチェックリストの内容には専門的な内容が含まれている可能性があり，通信技術に詳しいとは言えない一般的なネットワーク利用者が直接参照することは難しい可能性がある．また，問題要因を特定するためにはネットワークシステムから取得するデータが必要である可能性が想定される．実際，一つの AP に対して多数の端末による接続が集中していることにより通信速度が遅くなる問題を特定する場合，接続先 AP に接続されている他の端末に関する情報を取得する必要がある．この情報は AP および AP を管理する無線 LAN コントローラからのみ取得可能な情報であるが，通信技術に対して専門知識を持たず，ネットワークシステムの管理権限を持たないネットワーク利用者がこれらのデータにアクセスし，分析することはできない．そのため，ネットワークシステムにアクセス可能な診断システムが代わりにデータを取得し，チェックリストを基に原因を特定し，利用者に対して解決策の提示までを自律的に行う仕組みが必要である．

以上の課題に対し，本稿ではシステムによる組織内ネットワークの自律的な診断を可能とするモデル「チェックリスト型ネットワーク診断モデル」を提案する．「チェックリスト型ネットワーク診断モデル」では，ネットワーク管理者やヘルプデスクなどネットワークで発生するトラブルに対するノウハウを有する構成員が，事前にネットワークシステムで発生する可能性のあるトラブルとそれに対する解決策などを列挙したチェックリストを作成し，これに基づいて診断を行うものである．開発システムは，チェックリストで列挙された問題を特定するために必要なネットワーク機器および利用者との対話を ADU(Atomic Diagnosis Unit) として定義し，検出された問題に対して利用者に発生要因と解決策を提示する．

本研究では，通信技術に精通していない構成員を有し，かつ 1,000 台以上の AP が設置された大規模な無線 LAN システムを持つ組織において，接続品質に関わるトラブルに遭遇したネットワーク利用者に対し，迅速かつ的確な問題解決を支援するシステムの開発を行う．システム構築の前段階として大規模ネットワークシステムにおける診断モデル「チェックリスト型ネットワーク診断モデル」を開発し，モデルを採用した診断プロトタイプシステムである「Netdoctor」の開発・評価を行うことで，ネットワークにおける接続品質の低下・接続トラブルの迅速な解決に貢献することを確認する．

1.4 論文の構成

本稿では，第 2 章で大規模なネットワークにおける運用の現状とそこで発生しうる接続品質低下について議論したのち，第 3 章で本稿で提案するネットワーク診断モデル「チェックリスト型ネットワーク診断モデル」について説明する．第 4 章でチャットボットを利用したネットワーク診断を行うシステム「Netdoctor」の設計及び実装について議論する．第 5 章では，プロトタイプシステムの評価とその結果について述べる．第 6 章では提案する診断システムの有効性について考察し，今後の課題をまとめる．

第 2 章　大規模無線 LAN 運用の現状

2.1　大規模無線 LAN 運用と監視技術

■ 大規模無線 LAN の事例

大規模無線 LAN は企業や教育研究機関をはじめとした大規模な組織で構成員がネットワークにアクセスするための手段として運用されている．特に教育研究機関で運用されるキャンパスネットワークは大多数の機関が導入しており，代表例として九州工業大学における九州工業大学情報コンセント・無線 LAN サービス [15, 16]，東京工業大学における titanet4[4]，広島大学における HINET[17] が挙げられる．

まず九州工業大学情報コンセント・無線 LAN は，学生数 5,600 名を有する九州工業大学で運用されるキャンパスネットワークで，AP 数 603 台のスター型ネットワークである．現行バージョンのネットワークは新型コロナウイルスの流行期の前にあたる 2019 年に更改が行われ，現行バージョンでは，①利用端末数の増加に対応するための AP 増設，②利用端末が稠密になる可能性を考慮 (IEEE802.11ax，以下単に 11ax) 導入，③トラフィック増加に備えた有線ネットワーク増強，④教育研究活動に直接関係のないトラフィック制御，⑤調査した利用動向に基づく機材の選定の 5 つを満たす設計とされている．

次に，titanet4 は，学生数 10.500 名，教職員数 1,700 名を有する東京工業大学において 2010 年から運用されているキャンパスネットワークで，AP 数は最低でも 1,000 台，有線側では機関スイッチ 4 台，建物スイッチ 86 台が運用されている大規模なスター型ネットワークである．本ネットワークは要件として先進性・信頼性 (冗長性)・生産性 (セキュリティ) を挙げている．具体的に，先進性は無線区間のギガビット対応 (11ax 対応) および全学 IPv6 対応など，信頼性 (冗長性) はキャンパスそれぞれへの対外接続回線の増強および対外接続機器の冗長化，生産性 (セキュリティ) はセキュリティゲートウェイの設置，端末管理の導入などが該当する．構成管理システムとして，前バージョンである titanet3 における Wiki ページ上での管理から，2021 年の titanet4 への更改に伴い，OSS である Netbox および Ansible を活用したものが利用されており，運用コスト削減が図られている．

最後に，HINET は学生数 15,000 名，教職員数 3,500 名，を有する広島大学において運用されているキャンパスネットワークであり，AP1,200 台，ネットワークスイッチ約 500 台が設置されている．詳細は 4.1 節で述べるが，2015 年までに行われたネットワーク更改により，①スイッチポート設定・VLANID などのリソースの一元管理・ネットワーク利用者による申請に応じたそれらの割り当て，②申請に対し 3 分以内に設定処理が自動で完了すること，③ネットワーク機器に依存しない制御を要件とした自動構成機能を有するキャンパスネットワーク管理システムが導入された．これにより広島大学では，ネットワーク構成設定のオートメーションが実現されている．

■ 大規模無線 LAN における通信品質低下要因

講義室など，一つの AP に多数の端末が接続する環境においてネットワーク接続に悪影響を与える要因に関する研究がこれまで行われている．群馬大学の浜元氏らは，群馬大学内図書館の教育用端末 120 台と，図書館内に設置された AP を用いてスループットの計測実験を行った結果，接続規格および周波数によって最大の同時接続可能台数が存在することが報告されている [3]．具体的には，実験において 5Mbps の平均スループットを維持できた接続台数として，11n(2.4GHz) では 12 台，11n(5GHz) では 30 台，11ac(5GHz) では 36 台とされている．一方，東京大学の石原氏らは，オンライン講義におけるリアルタイム音声や動画ストリーミングに対する無線 LAN の影響を調査した [2]．調査によると，80 台の端末によるオンライン講義視聴が行われる環境において，モバイル Wi-Fi を含む Rogue AP による同一チャネル上の通信がオンライン講義の品質に悪影響を与える．特に，実験結果としてはオンライン講義配信サーバから観測されたパケットロス計測値およびオ

ンライン講義受講者のスコアリングともに顕著な悪化が見られることが報告されている．

これらの報告に基づくと，組織内ネットワークにおいて利用者が十分なスループットでリソースにアクセスできる状態を維持するためには，適切な台数の AP の設置，および一台の AP に接続される端末数を監視し，接続数を調整することが必要であることがいえる．また，組織無線 LAN で用いるものと同一のチャネルで通信を行うモバイル Wi-Fi ルータ (Rogue AP) の使用禁止，および使用が確認されかつ組織内無線 LAN の通信に支障をきたしている場合には，組織内無線 LAN 利用者に対して別の AP への接続を誘導することが必要であると言える．

■ 有線ネットワークにおける監視技術

ネットワーク利用者がトラブルに遭遇した場合の解決支援をネットワーク管理者が行う際には，ネットワーク監視システムから原因を特定するための情報を確認し，利用者に対してアクションを求めるか，ネットワーク上の障害を取り除く作業が行われる．管理者がネットワーク監視システムにより的確にトラブルの検出を行えるためには，監視システムが収集している情報が問題特定に充分であること，および問題特定が容易に行えるユーザーインターフェースが備えられている必要がある．Sihyung Lee らは，ネットワーク監視を行う上で 5 つの論理的測定機能を定義し，それぞれ収集層，プレゼンテーション層，レポート層，解析層，プレゼンテーション層と定義している [18]．このうち測定データをネットワーク管理者に視覚的，文字的表現などの形式で提示する方法論を示すプレゼンテーション層に関する取り組みとして，ATLAS TDAQ Network におけるパフォーマンス監視システム [19] や国立研究開発法人情報通信研究機構が開発する NIRVANA[20] などが挙げられる．

ATLAS TDAQ Network におけるパフォーマンス監視システムでは，実験棟の 4 階層にまたがる 3 つの独立したネットワークで構成されている ATLAS TDAQ ネットワークを対象にした監視システムである．プレゼンテーション層としてデータソースに関係なく，全てのプロットを表示する単一の Web アプリケーションを実装し，最大 4 回のクリックで任意のプロットを取得できること，及び異なる統計間の相互相関レポートを取得するのに必要な時間が数秒であるという特徴を有している．

NIRVANA は実ネットワークを管理するネットワーク管理者を対象にトラフィックをリアルタイムで可視化することにより，切断等の障害や設定ミス等を瞬時に見つけ出すことを可能にする．

■ 無線ネットワークにおける監視技術

一方，多くの企業内ネットワーク及びキャンパスネットワークにおいては，新型コロナウィルス流行によるオンライン授業やリモートワークの増加を背景として，構成員が自分の端末を持ち込み，無線 LAN によりネットワークに接続することでリソースにアクセスする事例が発生した．これに伴い，流行発生前に比べ，1 日あたりの無線 LAN 利用者数及び 1 台のアクセスポイントに接続する平均端末数の増加が発生する．具体例として，九州工業大学におけるキャンパスネットワークでは 2018 年 BYOD を実施しており，キャンパス無線の導入当初の 2014 年から利用者数は約 2.5 倍，端末数は約 2.9 倍に増加した．その結果，1 台の AP に対する平均接続利用者数は 75 人から 89 人に上ることが報告されている [21].

一般的に，大規模な無線ネットワークにおいては，ローミングによる複数 AP 間での接続端末数の均衡化が行われている．そのため，ある教室で極端に端末数や通信量が多い場合，隣接する別の部屋の AP に接続される場合がある．無線 LAN における接続品質低下の原因として，周辺の AP 及び電子レンジといった電波発生源との電波干渉があるが，大規模な教育研究機関においては，教室で利用される無線 LAN 端末が隣接する別の部屋の AP に接続したり，周囲の部屋に設置された AP のチャネルと干渉することにより，事前に行われるサイトサーベイでは把握できない電波干渉が発生する可能性がある．これにより周辺の教室で端末及び通信量が多い場合には，別の教室の通信品質にも影響を与えるという事象が発生する．この問題に対して山崎氏らは，無線 LAN アクセスポイントの接続端末情報及び認証ログの集計，分析を行うことにより，無線 LAN 品

質低下事象の検出手法を確立した [22]．この検出手法を利用することにより，電波干渉の継続的な把握及び改善策の効果の検証を行うことにより解決を試みた．

また，構成員が利用するスマートフォンのテザリングなどによる Rogue AP が発する電波によりチャネル間干渉を起こす可能性も指摘されている．以上から，無線ネットワークの設計及び整備を行う段階だけではなく，運用する段階におけるネットワーク接続品質の低下の監視と，トラブルが発生した場合の解決支援が必要である．

以上に示すように，ネットワーク利用者のアクションにより無線 LAN における接続品質の改善を支援する仕組みの導入が進んでいる．本研究では，以上に挙げた事例をさらに高度化し，自律的に診断を行うことで，利用者が遭遇する問題に対して直接解決支援を行うことを目的としたシステムの開発を行う．

2.2 IEEE802.11 シリーズにおける接続品質低下

IEEE802.11 シリーズは，1997 年から継続して策定が行われている通信プロトコルであり，現在も無線 LAN 通信において一般的に用いられている [23]．実際の無線 LAN において，端末の台数や伝送レートは時々刻々と変化するため，整備されたネットワーク環境下であっても接続される端末状態や電波状況の変化により接続品質の低下や，全く接続できないといったトラブルが発生する可能性がある．

無線 LAN においては有線 LAN によるネットワークと異なり，通信路が直接見えないという特徴があるため，ネットワーク利用者の利用端末が意図しない AP に接続されていたり，周囲の電波干渉の影響を受けたりすることにより，送信帯域が減少するといった現象が発生する．これらの現象のうち，電波干渉や Rogue AP による通信障害は，IEEE802.11 シリーズにおいて採用されているチャネルアクセス方式である CSMA/CA(Carrier Sense Multiple Access/Collision Avoidance) と呼ばれる仕組みが原因で引き起こされる場合がある．

■ CSMA/CA

CSMA/CA は，IEEE802.11 シリーズにおいて複数端末間のアクセス調停方式として用いられている [23, 24]．ここで，AP に対して接続を行う端末のことをこの文脈では STA(**STA**tion) と呼ぶことにする．CSMA/CA は，一つの AP に同一チャネルで複数の STA がアソシエーションされており，かつそのうち複数の STA の送信キューに送信フレームが存在する場合に，送信フレームの衝突を回避する方法の一つである．基本原理としては，各 STA が利用するチャネル上に閾値以上の強度を持つ信号が送信されていないかを確認するキャリアセンスを行い，一定期間未使用であれば送信，使用中であれば未使用になるまで送信を延期するというものである．以下に CSMA/CA により STA から AP に対してフレームを送信する際の動作を説明し，その内容を図 1 に示す．

フレーム送信時の動作　ここでは，一台の AP に対して複数の STA が存在している環境を想定する．CSMA/CA を用いたチャネルアクセス制御では，ある STA がフレームを送信しているときには，他の STA および AP はビジー状態となり出力を停止する．STA による送信が終了した直後に，IFS(Inter Frame Space) と呼ばれる待ち時間が置かれる．

IFS　IFS は BSS 内のすべての端末が送信を停止する時間である．IFS の間に同じチャネルで電波を受信した端末は，その電波の送信が終了するまでビジー状態となり，電波の受信を終えたのちに再度 IFS を置く．この現象は，周囲に存在し，かつ同じチャネルを利用する他の BSS からの電波を受信した場合や，電子レンジやレーダーといった同一周波数帯を利用する電波干渉が原因で引き起こされる可能性がある．また，IFS はさらに DIFS(DFC Inter Frame Space) と SIFS(Short Inter Frame Space) に分類される．IEEE802.11a において，DIFS 時間は $T_{DIFS} = 34\mu s$, SIFS 時間は $T_{SIFS} = 16\mu s$ と定義されている [25].

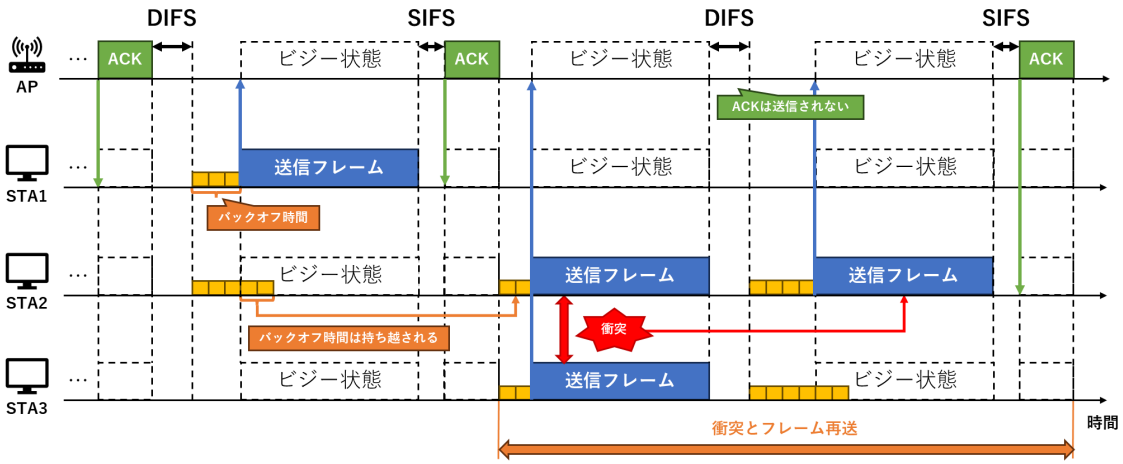


図 1: CSMA/CA バックオフ時間及びフレームの衝突・再送

用語「BSS(Basic Service Set)」

無線ネットワークのグループを指す [26]．本文の文脈では，一台の AP と AP に対してアソシエーションを行った STA のグループを指している．

バックオフ　IFS が終了した直後，バックオフと呼ばれる端末ごとに異なる待ち時間が置かれ，その直後にパケットが送信される．バックオフは，送信キューにフレームが存在する STA の間で各 STA がそれぞれ有限範囲の一様分布に従う乱数を生成し，その乱数により指定される分だけ待機した後にフレームを送信するという仕組みである．この仕組みにより，ある送信フレームを持つ STA3 よりも先に別の STA2 がフレームを送信するということが起こりうるが，この場合，STA3 は STA2 からの送信が終わるまでビジー状態となる．

ACK フレーム　AP が STA からのパケットを受信すると，IFS の間待機した後直ちに ACK フレームを送信元 STA あてに送信する．IEEE802.11 シリーズにおいて，ACK フレームはバックオフの原則に当てはまらず，ビジー状態が解除され，IFS が終了すれば直ちに送信される．これは後述する「衝突」が発生したか否かを検出できるようにするための仕組みで，データ送受信の完全性を保証するために必要な仕組みである．

フレームの衝突　一つの AP に対する STA の数が増加すると，STA 同士でバックオフ時間が等しくなり，複数の STA が同時にフレームを送信し始める現象が発生する．この現象のことを衝突 (Collision) と呼ぶ．STA から AP への送信パケットが衝突を起こした場合，AP からの ACK は返答されない．これにより，全ての送信元 STA はパケットが衝突したことを認識する．パケット衝突を認識した STA は全ての STA からの送信が終わるのを待機し，IFS の間待機した後，再度バックオフ時間の設定を行い，フレームの再送を試みる．この際指定されるバックオフ時間の設定は，再送する前に使用したものよりも高い上限値を指定した一様乱数が用いられる．

■ 無線 LAN における Performance Anomaly

一般的に AP に接続される端末の伝送レートは信号強度及びノイズ比，フレームエラー率などのメトリクスによって動的に決定される．複数の端末が一台の AP に接続されている時，一台でも極端に低い伝送レートが設定された端末がある場合，AP 全体のスループットが低下することが知られており，この現象は無線 LAN 通信における Performance Anomaly と呼ばれている [27]．

無線 LAN 通信における Performance Anomaly は，マルチビットレート環境において同一チャネルを使用する機器にビットレートの低いものが存在する場合，他のすべての機器のスループットが低下する現象であ

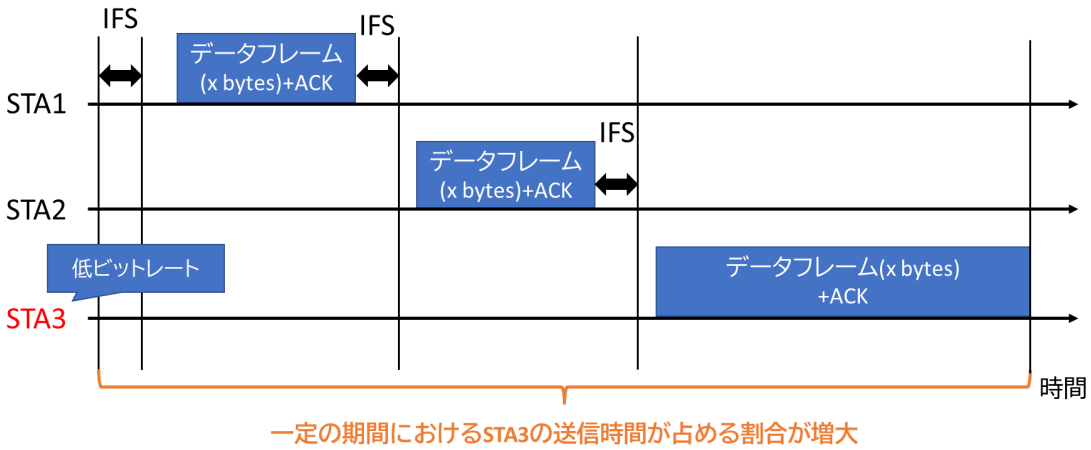


図 2: 無線 LAN における Performance Anomaly

る [27]．ビットレートの決定方法は無線 LAN アダプタによって異なるが，一般的には STA から計測される RSSI(Received Signal Strength Indicator; 受信信号強度) や SNR(signal-noise ratio; 信号対雑音比) をもとに各 STA が決定する．そのため，一つの BSS 内に異なるビットレートを持つ複数の端末が存在することが可能である．

用語「マルチビットレート環境」

本文においては，一台の AP に対して複数の STA が存在するとき，STA ごとに異なるビットレートを持つような BSS を指す．

発生原理　CSMA/CA によるチャネルアクセス制御においては，等しい大きさのデータフレームを送信する場合でも，低いビットレートの STA は高いビットレートの STA に比べて送信に時間がかかる．この現象は，チャネルボンディングおよびガードインターバル，Spatial Steram が同一のものであると仮定した状態で，ビットレートの違いが変調方式の違いに起因することによる．IEEE802.11 シリーズにおいては，同一のバージョン内では変調方式やその他のパラメータを問わずシンボル長が同一であると規定されている．このことから，変調方式が異なることで，一つのシンボルに割り振ることのできるビット数が異なる．例えば，BPSK(Binary Phase Shift Keying) においては搬送波の位相を 180 度ずつ回転させることにより 1 ビットを表現する一方で，IEEE802.11ax において初めて導入された 1024-QAM と呼ばれる変調方式においては位相の回転および出力強度の大小により 1024 ビットの情報を 1 シンボルで伝送することが可能である．これにより，同一の長さを持つフレームを送信するとき，1 シンボルで表現できる情報が小さい変調方式を採用している STA は，反対に大きい変調方式を採用している STA よりも送信を開始してからすべてのビットを送信し終わるまでにかかる時間が大きくなる．具体的には，BPSK と 1024-QAM を比較すると，誤り訂正符号を無視したとき，BPSK は 1024-QAM を採用した場合に比べて同じ大きさのフレーム送信に 1024 倍の時間がかかる．以上のことから，CSMA/CA においてある AP に対する複数の STA が任意の時点でチャネル送信できる確率が STA 間で等しく，かつそれぞれの STA が全く同じ長さのフレームを送信し続けると仮定したとき，ある STA の送信ビットレートが低いほど任意の時間区間で送信時間を長く占めることになる (図 2．これが原因で，高ビットレート端末の送信時間を低ビットレート端末の送信時間が圧迫してしまうことにより，高ビットレート端末の送信スループットが極端に減少してしまうことが報告されている．この現象が無線 LAN における Performance Anomaly と呼ばれているものである．

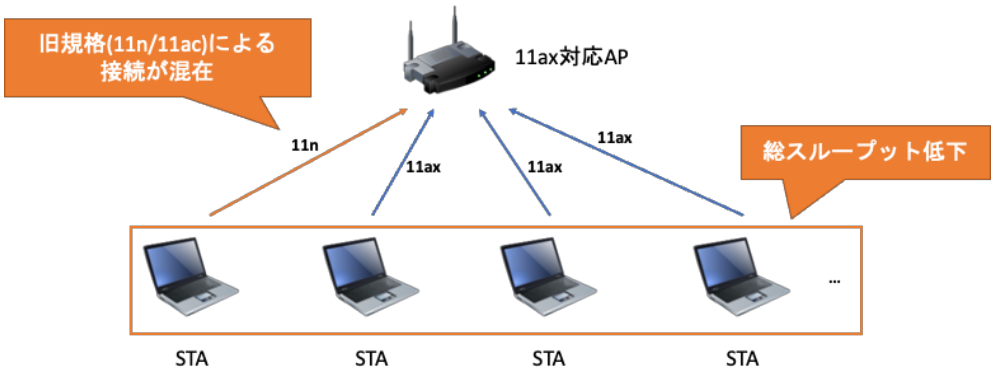


図 3: 11ax 対応 AP に旧規格で接続する STA が存在する場合

実証　Martin らは IEEE802.11b を用いた実環境下で Performance Anomaly が発生することを実証するため，一台の AP に IEEE802.11b を利用してアソシエーションを確立した複数の STA，および AP と有線で接続されたサーバを用意し，各 STA から netperf を用いたパケット送信およびスループットの測定を行った．STA は最大 4 台用意し，マルチレート環境下で一台の STA(STA_1 とする) はビットレートを低い値に変更する一方，その他の STA のビットレートは 11Mbps に固定した．これにより，Performance Anomaly が起こりうる環境を構築した．サーバ側では netserver を実行する一方，STA 側で netperf を実行し，サーバに対して固定長の UDP および TCP パケットの継続的送信を行うことでスループットを計測した．STA が 2 台設置されている状態で UDP を利用した場合の結果として，STA_1 のビットレートを 11Mbps にした場合のもう一方の STA の平均スループットが 3.36Mbps であるのに対し，STA_1 を 1Mbps に指定した場合には 0.76Mbps に低下している．同様の現象は STA を増加させた場合にも発生することが報告されている．STA が 4 台設置されている状態で UDP を利用した場合の結果として，STA_1 のビットレートを 11Mbps にした場合の STA_1 以外の STA の平均スループットが 1.54Mbps であるのに対し，STA_1 のビットレートを 1Mbps に指定した場合の平均スループットは 0.53Mbps に低下することが示されている．また，同様の事象が IEEE802.11ac のマルチレート環境においても発生することが報告されている [28].

規格混在によるスループット低下　同様に，IEEE802.11ax に対応する AP に対して，旧規格 (IEEE802.11ac, IEEE802.11n) による接続を行う STA が混在した場合 (図 3)，AP 側から見た総スループットは全ての STA が IEEE802.11ax であった場合よりも低減することが報告されている [29]．特に，IEEE802.11n による接続が混在した場合には総スループット特性が最大 100Mbps 以上低下する可能性が指摘されている．

まとめ　以上の議論から，低ビットレートの STA が AP にアソシエーションすることは，他の STA のスループットを減少させる傾向があることが報告されているほか，各 STA のスループットは競合 STA の数に強く依存していることが示唆される．組織内無線 LAN においても，RSSI の減少やノイズ比の上昇により低ビットレートが指定された端末が AP に接続される可能性が否定できない．また，大規模なネットワークにおいては一つの AP に対して 70 台以上の端末が接続される可能性があり [21]，AP が処理する総通信量によっては各 STA のスループットが著しく低下する可能性がある．そのため，無線 LAN 接続品質の問題に遭遇した利用者に対する診断において検討されるべき問題の一つに，低ビットレート端末および多数の端末がアソシエーションすることによる総スループット低下を挙げる必要性がある．

第 3 章　チェックリスト型ネットワーク診断モデル

開発システムが採用するネットワークの診断モデルとして，チェックリスト型ネットワーク診断モデルを提案する．本モデルでは事前に組織内ネットワークで発生すると想定できる問題の要因，ユーザの症状及び検出パラメーターをチェックリストとして定義し，システムが診断を行う際には，チェックリストに列挙された問題の発生を ADU という対話・データフローにより逐一確認することで検出する方法を取った．チェックリストは IT 部門における相談窓口担当といったネットワークトラブルに対するノウハウは持つが専門知識は持たない構成員により作成される一方，ADU は システム開発者といった専門知識を有する人により作成される．

3.1　チェックリスト

定義　チェックリストは表 1 に示すように，発生の可能性がある問題の内容 (発生問題)，ネットワーク利用者が体験する症状 (症状)，問題を検出するためにシステムが用いるパラメータ (検出パラメータ)，ユーザーに提示する解決策 (ユーザーの対処) を列挙したものである．チェックリストはシステム導入時にネットワーク管理者が作成し，システムによる診断時には後述する対応 ADU(Atomic Diagnosis Unit) を実行することで，列挙された問題がネットワーク上で発生していないかを逐一確認していく．

「発生問題」列[*13]　「発生問題」列には，対象とする問題の発生区間およびその概要が表現されている．具体例として HINET 向けのチェックリスト（付録を参照）では，No.2-2 において「Rogue AP による電波干渉」という発生問題が定義されており，発生区間として「AP↔ 端末」（AP と利用端末間の無線区間）が定義されている．

「症状」列　ネットワークシステム上でトラブルに遭遇した利用者が経験する症状は種類が限定されており，以下の四つに分類されると想定した．チェックリストには以下の 4 つの症状のうち一つまたは複数が登録される．これにより，診断の際には利用者が訴える症状に応じて発生有無の確認を行う問題を事前に絞り込むことが可能である．

表 1: チェックリスト (一例)

No.	発生問題	症状	検出パラメータ	ユーザーの対処
…				
2-1	ユーザーが入力した認証情報の誤り	ネットワークに全く接続できない	(ユーザー) 入力した認証情報の誤りを確認	認証情報の再入力
…				
2-3	外部干渉源 (電子レンジなど) による電波干渉	ネットワークに全く接続できない または 通信速度が遅い	接続先 AP で外部干渉源を検出していること	部屋の移動 (接続先 AP の変更)
2-4	一つの AP に対する接続端末の増加	ネットワークに全く接続できない または 通信速度が遅い	接続先 AP の接続端末数増大していること	部屋の移動 (接続先 AP の変更)
…				

[*13] 付録のチェックリスト中では「発生区間」・「要因」として表現されている．紙面の都合上，ここでは統合して表現した．

- ネットワークに全く接続できない
- 通信速度が遅い
- ネットワークに接続できるが，時々途切れる
- 一部のアプリケーション/Web ページのみ接続できない[*14]

「検出パラメータ」列[*15]　チェックリスト型ネットワーク診断モデルは，対象のネットワークシステムに設置されたネットワーク機器及びネットワーク利用者の利用端末から情報を取得できるシステムで採用されることを前提としている．そのため，問題の検出にはネットワークシステムおよび利用者の利用端末から収集した情報を利用し，「検出パラメータ」列に記載された条件で評価することにより当該問題の発生有無を判断する．具体例として Rogue AP を検出する No.2-2 では，WLC から利用端末の接続先 AP でのノイズ比が増大していることおよび同一チャネルを利用する Rogue AP が検出されていることを検出パラメータとして利用している．

「ユーザーの対処」列　システムがチェックリスト中の問題がネットワーク上で発生していることを検出した場合，「ユーザーの対処」列に記載の内容を利用者に提示することで問題解決を促す．これにより，事前にネットワーク管理者が想定した問題のうち，ユーザーが直面している問題のみを的確に選択することを可能にしている．ユーザーの対処は以下の 7 つに分類されたものか選択する形式をとった．ただし，対象とする問題によって今後追加される可能性がある．

- 認証情報の修正
- 部屋の移動 (接続先 AP の変更)
- 端末 WLAN の再接続
- 席の移動
- 対処の必要なし
- 端末の設定修正 (修正内容は対象の問題によって異なる)
- ネットワーク管理者への報告

3.2　ADU(Atomic Diagnosis Unit)

チェックリストに列挙された問題それぞれに対して，ADU(Atomic Diagnosis Unit) と呼ぶシステムとユーザーおよびネットワークシステム間の対話および情報取得フローを定義する．

定義　図 4 に示す通り，ADU はチェックリストに列挙された問題一つに対してシステムが情報取得および問題発生有無の判断方法，問題が発生していると判断された場合には利用者へフィードバックする解決策の内容が定義されている．この例において，チェックリスト中で No.2-3 と定義された問題に対して ADU2-3 という ADU がさらに定義されている．ADU2-3 においては対応するチェックリスト中の問題の検出パラメータを利用するため，実装時に具体的にどのネットワーク機器からどの情報を取得するか，あるいは利用者の端末から情報を取得する際にはユーザーに対して具体的にどのような問い合わせを行うかが定義されている．また，取得した情報をもとに対応する問題の発生有無を判断する具体的な条件と，発生していると判断された場合に利用者にフィードバックする具体的なメッセージが定義されている．

[*14] 付録のチェックリスト中では「一部のアプリが繋がらない」・「一部のページで繋がらない」として表現されている．ここでは統合して表現した．

[*15] 付録のチェックリスト中では「ユーザーが提供する情報」・「システムがネットワーク機器から取得する情報」として表現されている．紙面の都合上，ここでは統合して表現した．

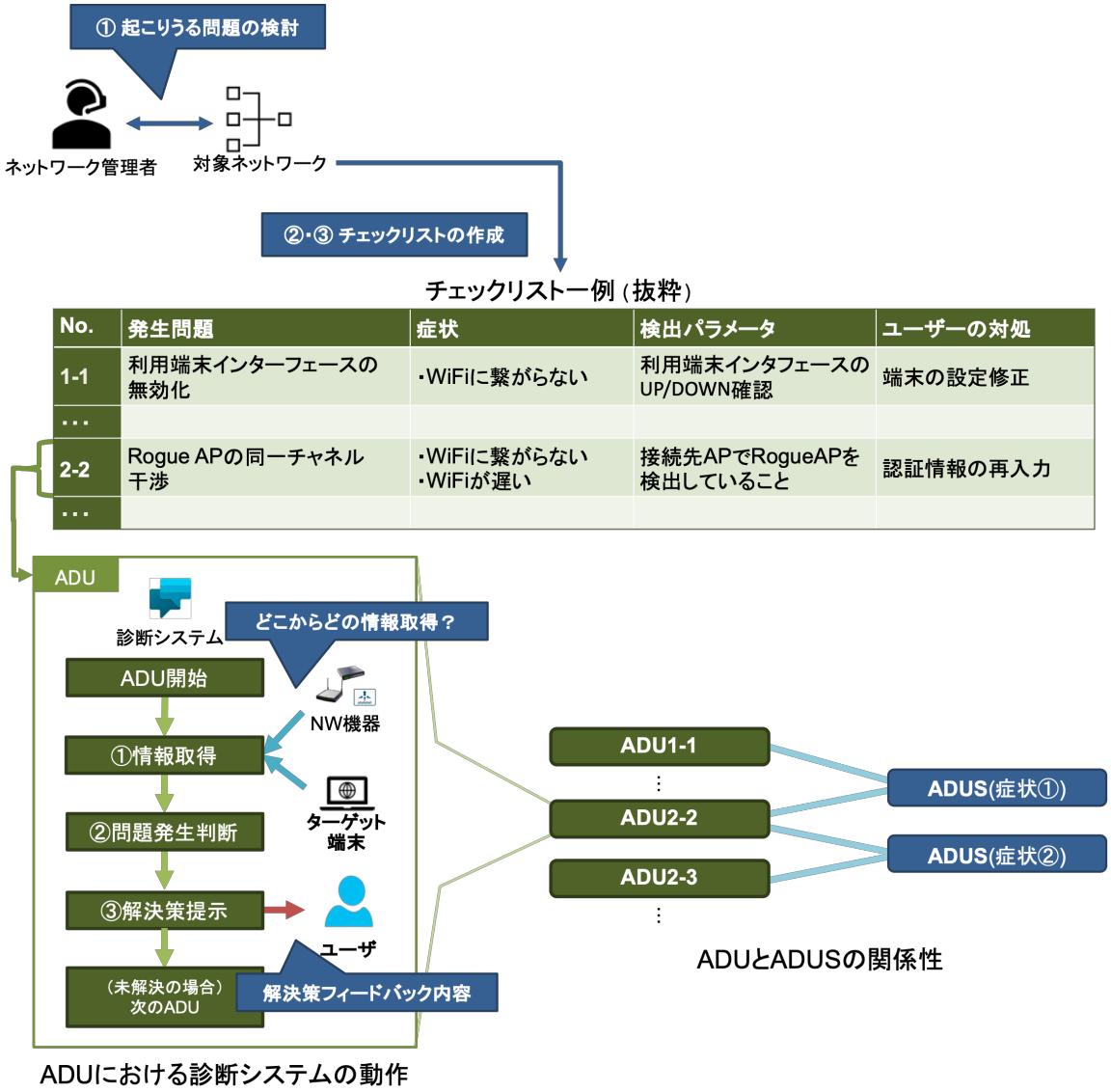


図 4: チェックリスト，ADU，ADUS の関係性

動作フロー　システムが ADU を実行する際の具体的動作は図 5 に示す通りである．図 5 中，「診断システム (チャットボット)」は開発システム，ログシステムはネットワークシステム中のネットワーク機器から情報の取得を行い，「診断システム (チャットボット)」に取得した情報を渡すシステムコンポーネントを示す．図 5 は左から右に向かって時系列が進行し，ADU の実行中に発生するコンポーネント及びシステム利用者間のデータフローを示したものである．ADU が実行されると，システムはまずシステム利用者 (ユーザ) 及びネットワーク機器に対して対応する問題の検出に必要な情報を取得する (図 5 中「①情報取得」)．ここで，ユーザーには手持ちの端末を操作する指示を出すことにより利用端末の設定およびログを表示させる．ユーザーが診断システムのユーザーインターフェースを通じてシステムに出力結果を入力することにより，診断システムは利用端末の情報を取得することができる．次に，取得した情報をもとに，当該 ADU に対応する問題が発生しているか否かを判定する (図 5 中「②問題有無判定」)．判定にはチェックリストで定義された検出パラメータが利用され，その中で定義された条件を満たした場合に問題が発生していると判断する．ここで問題があると判断された場合には，診断システムは利用者に対してチェックリストで定義された問題解決策をフィードバック

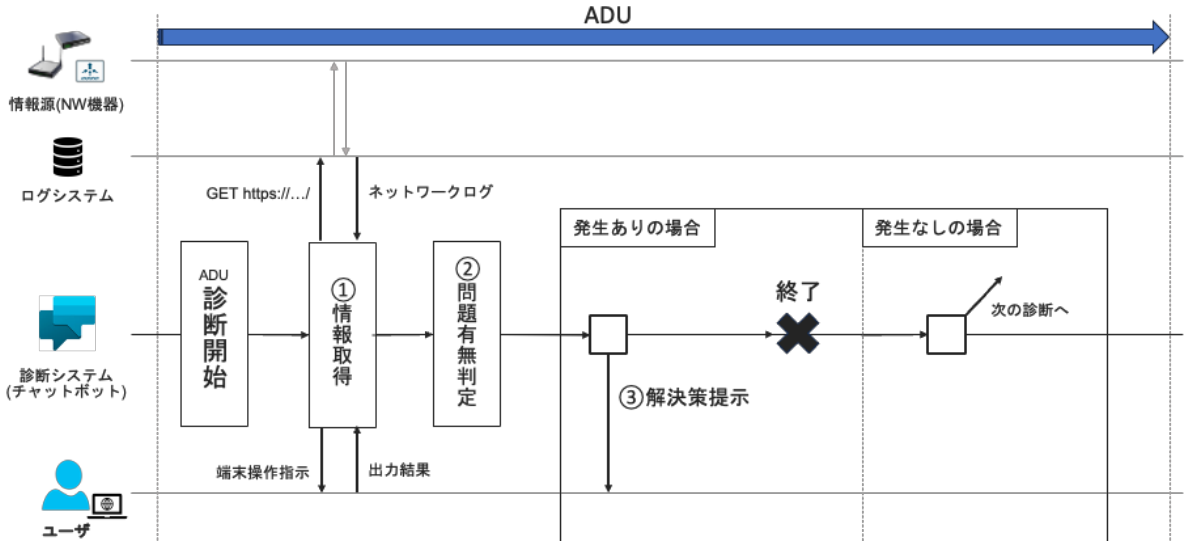


図 5: ADU の動作フロー

し，ADU を終了する．問題があると判断されなかった場合にはユーザーにフィードバックせずに ADU を終了し，後述する通り次の ADU を実行する．

具体例　ADU2-3 の具体例を図 6 に示す．この ADU は利用端末の接続先 AP で電子レンジなどの任意の電波干渉源による接続障害に対応するものである．図は上から下に向かって時系列を示し，システムコンポーネント間で交わされるメッセージおよびデータの自然言語による説明が記載されている．ここで，システムコンポーネントのうち「診断システム」はチャットボットと同義である．まず「診断システム」がログシステムおよびネットワーク機器に対して利用者の接続先 AP で外部干渉源が検知されているかを確認し，応答を受信する．もし検知されていると判断された場合には，利用者に対して解決策として部屋の移動と，無線 LAN の再接続を指示する．その結果，解決した場合には診断自体を終了し，解決していない場合または干渉源が検出されなかった場合には次の ADU を実行する．

3.3　ADUS(ADUs by Symptom)

定義　ADUS(ADUs by Symptom) は，ADU を対応する問題の症状別に分類し，その実行順序を定義したものである．3.1 節で述べた通り，チェックリストに列挙する問題の症状は 4 種類に限定されているため，各問題に一対一で対応する ADU も症状別に分類することが可能である (図 7)．システムは問題に遭遇したネットワーク利用者のアクセスを受けて診断を開始する際，診断開始前に利用者が遭遇している症状を利用者から取得させることを前提としている．システムは診断を迅速に実行できるようにするため，利用者の症状に該当する ADUS のみを実行することで，実行する ADU の数を削減している．

具体例　図 8 に示すのは，「ネットワークに全く接続できない」という症状に対応する ADUS において，システムが実行する ADU 及び図の上から下に向かってその実行順序，各 ADU が必要とする情報源を示したものである．前述のとおり，ADUS は利用者が訴える症状に一対一で対応しているため，システムは入力された症状に対応する ADU を順番に実行していく．ADU は主にネットワークを診断するものと，利用者の利用端末を診断するものに分類することができる．主にネットワークを診断するものとして ADU2-2 があるが（付録参照），これは利用者のいる部屋で無線 LAN と同一のチャネルで通信を行う Rogue AP による干渉が発生していることを検出し，検出された場合には利用者に部屋の移動を呼びかけるものである．ADU2-2 を実行する

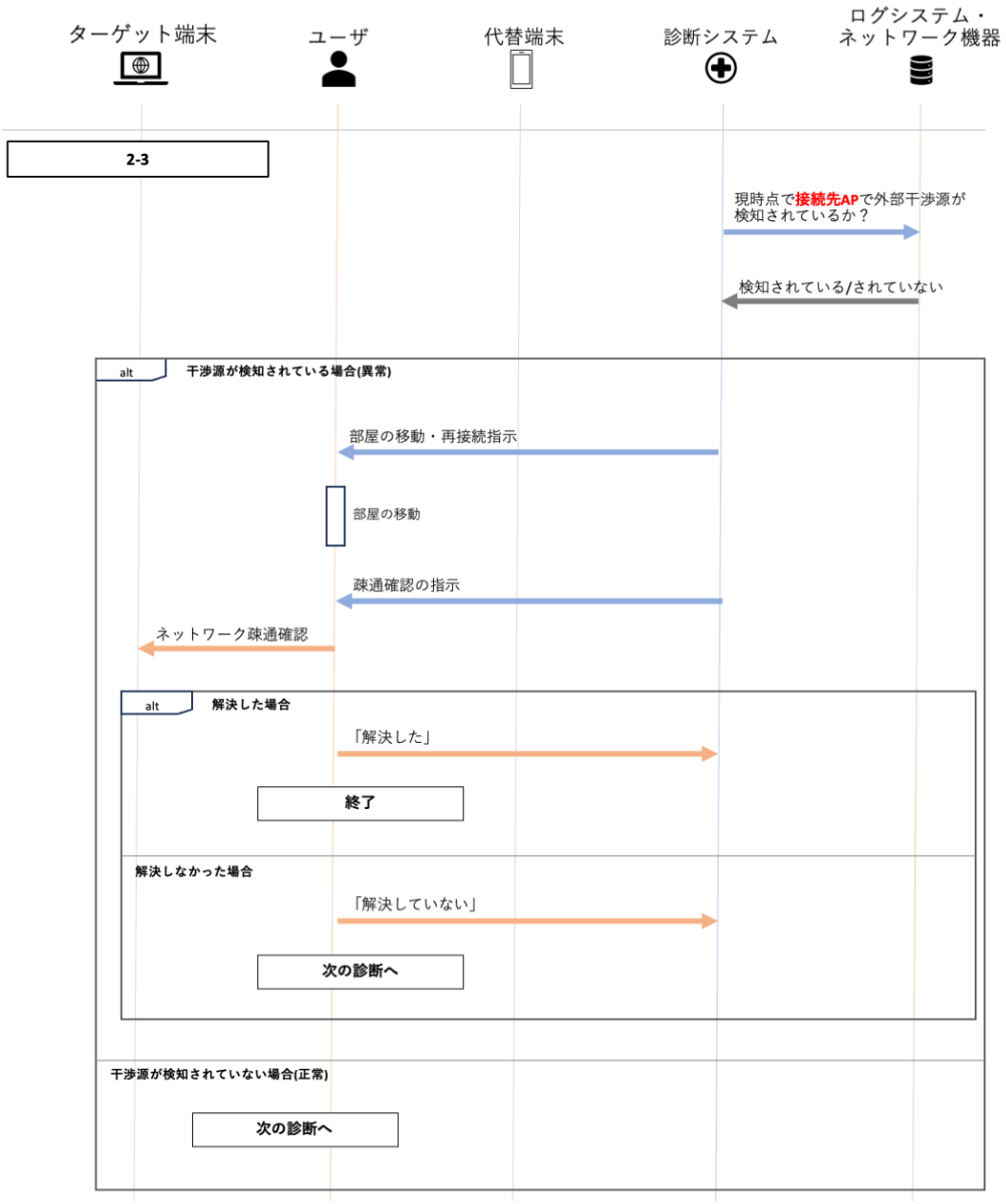


図 6: ADU データフロー具体例 (ADU2-3)

際，システムは無線 LAN コントローラ (WLC) に対し，利用端末が接続されている AP のノイズ比と検出できる Rogue AP の一覧を取得する．もしノイズ比が通常時よりも高く，取得した Rogue AP の一覧にチャネルが同一のものが存在している場合には，問題が発生しているとみなし利用者に部屋の移動を促す．一方，利用端末を診断するものの具体例としては ADU2-1 がある．ADU2-1 はユーザーが端末に設定した Wi-Fi 認証情報の誤りを検出するため，ユーザーに対して端末操作を指示し，出力されたログの内容をユーザーインターフェース経由で入力させる．情報蟷螂誤りが発生していると判断された場合には，ユーザーに対して認証情報の修正を指示する．ネットワークを主に診断する ADU は診断システムがネットワーク機器に問い合わせを行うことで完結し，利用者の操作を必要としない一方，利用端末を診断する ADU は利用者による端末操作および出力結果の入力を必要とする．そのため，ADUS において ADU を実行する順序は，初めにネットワークを

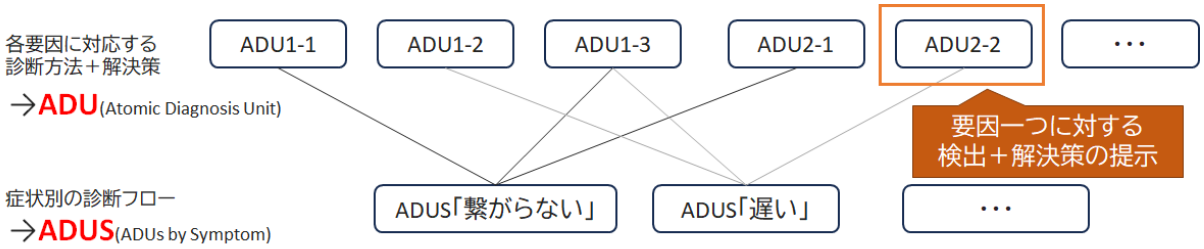


図 7: ADU と ADUS の関係性

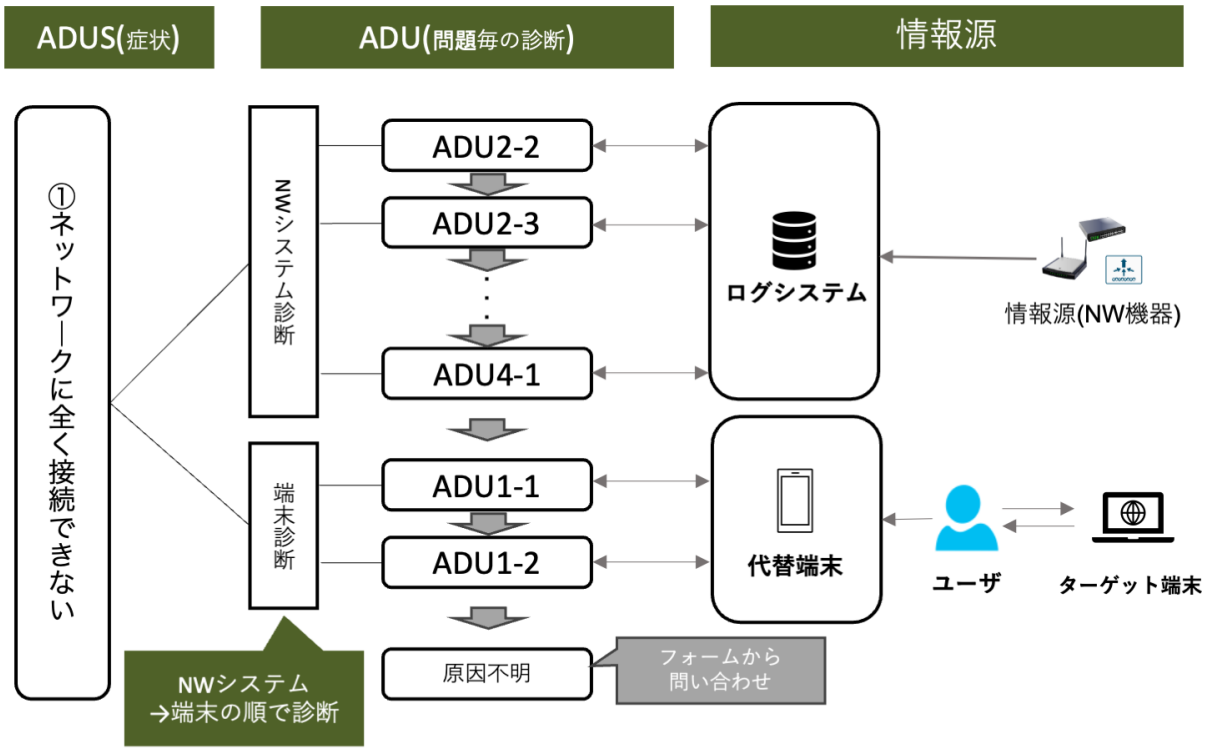


図 8: ADUS の実行順序

主に診断する ADU を実行したのち，利用端末を診断する ADU を実行する．これにより，利用者の端末操作を省き，迅速な診断が行えることを期待する．

第 4 章　開発システム「Netdoctor」

4.1　実装対象のネットワーク

4.1.1　ネットワーク要件

本システムが実装対象とするネットワークは，構成員が通信やネットワーク技術に専門知識を有していない大規模な組織で運用されており，AP が 1,000 台以上設置されている組織内無線 LAN である．このようなネットワークにおいては，時間帯や場所によってネットワークの利用が突発的に集中する可能性が生じるほか，多数設置された AP の間での AP ローミングによりネットワーク利用者の利用端末が不適切な AP に接続されるといったトラブルが発生する可能性が高くなる．本システムはこのような問題を検出及び特定するため，ネットワーク機器にアクセスし，統計情報およびログを参照する必要がある．ネットワーク機器からのデータ取得は，後述する「ログシステム」と呼ばれるシステムコンポーネントにより実施される．実装対象ネットワークの要件として，ネットワーク機器にアクセスすることができ，かつ外部ネットワーク (インターネット) からの着信接続が可能なサーバが設置されている必要がある．この条件を満たすサーバ上でログシステムが稼働する．また，システムコンポーネントのうちチャットボットはクラウド上で動作し，ネットワーク利用者はシステムにインターネットを経由してアクセスすることを想定している．そのため，構成員は利用端末のほか携帯回線などを経由して外部ネットワークにアクセスできる端末を持っているような環境である必要がある．

4.1.2　広島大学キャンパスネットワークシステム「HINET」

本稿におけるプロトタイプシステムではこれらの条件を満たすネットワークとして，広島大学で運用されているキャンパスネットワークシステム「HINET」に対してシステム実装を行う．HINET は，広島大学において運用されているキャンパスネットワークであるが，その一部として無線のネットワーク「HINET Wi-Fi」が運用されている [30, 31]．図 9 に示す通り，HINET はスター型トポロジーを有するネットワークで，L3 スイッチで構成されるコアネットワークを中心に，キャンバスや建物，フロアごとに設置された L2 スイッチを介して AP 及び利用端末が接続される．HINET Wi-Fi 内で運用されている AP の数は 1,200 台以上であり，すべてコアネットワークに接続されている無線 LAN コントローラーの管理下に置かれている．構成員が無線 LAN を経して，ネットワークにアクセスする際，通信内容は，CAPWAP を介してすべて無線 LAN コントローラーを経由する．そのため，無線コントローラーは AP で発生した通信について統計情報を取得可能である．

広島大学において，学生は自分のパソコンを携帯する BYOD が導入されている [32]．そのため，ネットワーク利用者を学生としたとき，個人 PC によるネットワークアクセスができなくなった場合でも，スマートフォンによる携帯回線を経由したシステムへのアクセスが可能である．

4.2　実装

4.2.1　要件

本システムは教育研究機関及び企業といった一般的な組織に導入されることを想定している．そのため，ネットワーク利用者が無線 LAN の接続品質低下及び問題に遭遇した際，組織活動継続の必要性から迅速な解決が要求されることが多いと想定される上，また，システム利用者が必ずしも通信技術やコンピュータに精通しているとは言えない．管理者向けの監視システムにおいては，Juniper Networks Inc.[*16]による対話型 AI

[*16] https://www.juniper.net/

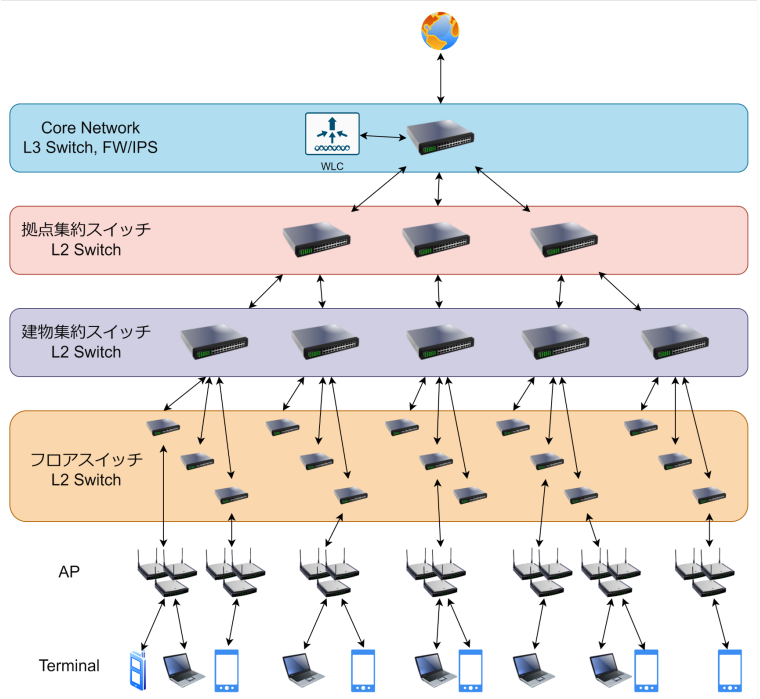


図 9: HINET ネットワークトポロジー

Marvis を代表として，作成したチャットボットを通じてネットワーク上で発生している障害を含むトラブル要因を特定する仕組みの開発が行われている．この仕組みを利用者側で利用可能にし，利用者自身がチャットボットを通じて問題の解決を行う仕組みを整えることで，ネットワーク管理者の負担削減及び迅速かつ的確なトラブル解決が可能であると期待される．また，利用者が遭遇するトラブルが利用端末に起因する場合も想定されることから，ネットワークシステムおよび利用端末の両方を対象にすることでより正確な診断が行えることが期待される．

一方，京都工業繊維大学情報科学センターなどで行われているネットワーク上のメトリクスを利用者に公開する仕組みであっても，問題の発生有無を判断するのはネットワーク利用者側のリテラシーに依存しており，問題に対する対処も利用者側での調査が必要となる場合がある [12]．これらのことから，開発システムに求められる要件として以下の二つを定義した．

- ネットワーク利用者は専門知識がなくてもシステムを通じて管理者を介さず診断から解決までを行うことができる．
- ネットワークシステムおよび利用端末両方の診断が可能である．

4.2.2 Microsoft Copilot Studio

Microsoft Copilot Studio(以下，MCS) は，Microsoft 社が提供するノンコードのチャットボット開発フレームワークである．本システムでは MCS を用いて作成したチャットボットをユーザーインターフェースとして採用した．MCS で開発したチャットボットはクラウド上で動作し，Microsoft Teams 上でチャットボットとして公開できるほか，自作の Web インタフェースを通じて，ユーザーとインタラクションする機能を有する．

MCS において，ユーザーとの対話の一連の流れは「トピック」という単位で構成される．トピックはチャットボットからユーザーへの質問やメッセージ，及び条件分岐などを集約したものであり，他のトピックから呼

表 2: システムコンポーネント

名称	説明
ターゲット端末	組織内ネットワークで接続品質の問題に遭遇した端末
ユーザー	本システムの利用者
代替端末	ユーザーが外部ネットワーク経由でシステムにアクセスするために用いる端末 (スマートフォンなど)
チャットボット (Netdoctor)	ユーザーとの対話を行うチャットボットシステム
ログシステム	組織内ネットワーク内のログを収集し，チャットボットに提供するシステム

び出されるか，ユーザーがチャットボットに事前に指定したキーワードを入力することにより実行可能である．

図 10 には，「あいさつ」という名称のトピックの一例を示す．このトピックではユーザーがチャットボットに「こんにちは」もしくは「おはようございます」と送信した場合に実行され，返答としてチャットボットからユーザーに対して「おはようございます．以下の選択肢を選択してください.」と質問する．質問に対する回答は選択肢として定義することができ，今回は「選択肢 1」と「選択肢 2」を定義している．また，ユーザーからの回答によって対話を分岐させることができ，この例で「選択肢 1」を選択した場合，チャットボットは「選択肢 1 が選択されました」というメッセージ，「選択肢 2」を選択した場合，チャットボットは「選択肢 2 が選択されました」というメッセージをユーザーに返却する．

また，MCS は Microsoft Power Automate で作成したワークフローを呼び出すことにより，外部 API エンドポイントを参照することが可能である．Microsoft Power Automate は，自動ワークフローを作成するためのノーコードクラウドサービスで，一般的に RPA(Robotic Process Automation) を実現したり，Microsoft Power Platform のバックエンドを実装したりする際に使用される．本システムでは MCS による対話の中で，外部 API を呼び出す目的で使用している．

4.2.3 実装

節 4.2.1 の要件を満たすプロトタイプシステムの構成及びシステムコンポーネントを図 12 及び表 2 に，フロントエンドのスクリーンショットを図 11 に示す．また，完成したプロトタイプシステムのデモンストレーションは `https://youtu.be/0fM5CdN5bJ0` (URL) から確認できる．

トラブルに遭遇したネットワーク利用者はチャットボット (Netdoctor) にアクセスし，ネットワークシステムで発生したログ及びユーザの利用端末から収集できる情報に基づいた診断を行う．システムへのアクセスは問題に直面している端末 (ターゲット端末) ではなく，スマートフォン等無線 LAN を経由しない回線を通じてインターネットへアクセス可能な端末 (代替端末) を利用して行う．また，システム利用者とシステムとの対話はチャットボットにより行われる．システムがチャットボットを通じて，利用者に対する端末を作指示や利用者からの入力の受付，また解決策のフィードバックなどを行う．

図 13 はシステム利用者がシステムにアクセスしてから診断及び解決策のフィードバックが終了するまでのデータフロー及び対話の流れを左から右に時系列で示したものである．システム利用者は手持ちの端末が接続品質の低下やネットワークに接続できないといったトラブルに遭遇した時点でシステムにアクセスする．この際，トラブルが発生した端末 (ターゲット端末) とは別にスマートフォンなどトラブルが発生していないネットワーク回線を経由してインターネットにアクセスできる端末 (代替端末) を利用してチャットボットにアクセスする．システム利用者はチャットボットにアクセスした後，ユーザ認証を行う．これによりネットワークシステムにおいてアカウントに紐付けられた利用端末を識別することを可能とする．次にユーザが症状を入力し

図 10: Microsoft Copilot Studio トピック一例「あいさつ」(スクリーンショット)

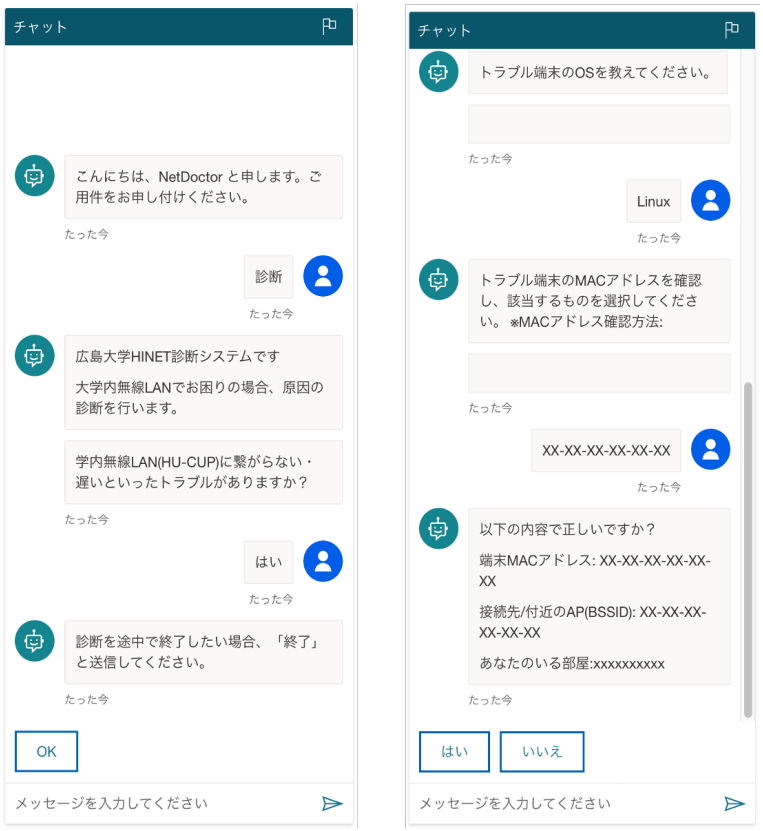


図 11: Netdoctor スクリーンショット

た後，ネットワーク機器から取得した情報及びターゲット端末からユーザを介して入力された情報をもとに診断を行う．診断終了後，システム利用者が直面していたトラブルに対する解決策をフィードバックする．ここでシステムが原因を特定できなかった場合，診断の際に取得したログとともに，組織の IT 管理部門に問い合わせるようシステム利用者に促す．

4.2.4 ログシステム

ログシステムは Netdoctor を構成するシステムコンポーネントで，対象ネットワークシステムに存在するネットワーク機器から取得したメトリクス，およびログなどの情報をチャットボットに提供する役割を担っている．ログシステムは対象ネットワーク内のネットワーク機器および外部ネットワークの両方にアクセスできるサーバ上で動作することが想定されており，チャットボットからの情報取得リクエストに応じて，ネットワーク機器から取得した情報をチャットボットにレスポンスとして返却する．ログシステムは，本来常時定期的にネットワーク機器からの情報を取得・蓄積し，チャットボットに対して過去にさかのぼってデータを取得できる仕組みにすることが望ましい．これにより，システム利用者が遭遇している問題要因を過去にさかのぼって特定することが可能となる．本稿における実装では，機器から定期的にデータを取得する際にネットワークおよび対象機器にかかる負荷を考慮して，チャットボットからリクエストがあったタイミングで対象機器に問い合わせを行うという動作を行う．

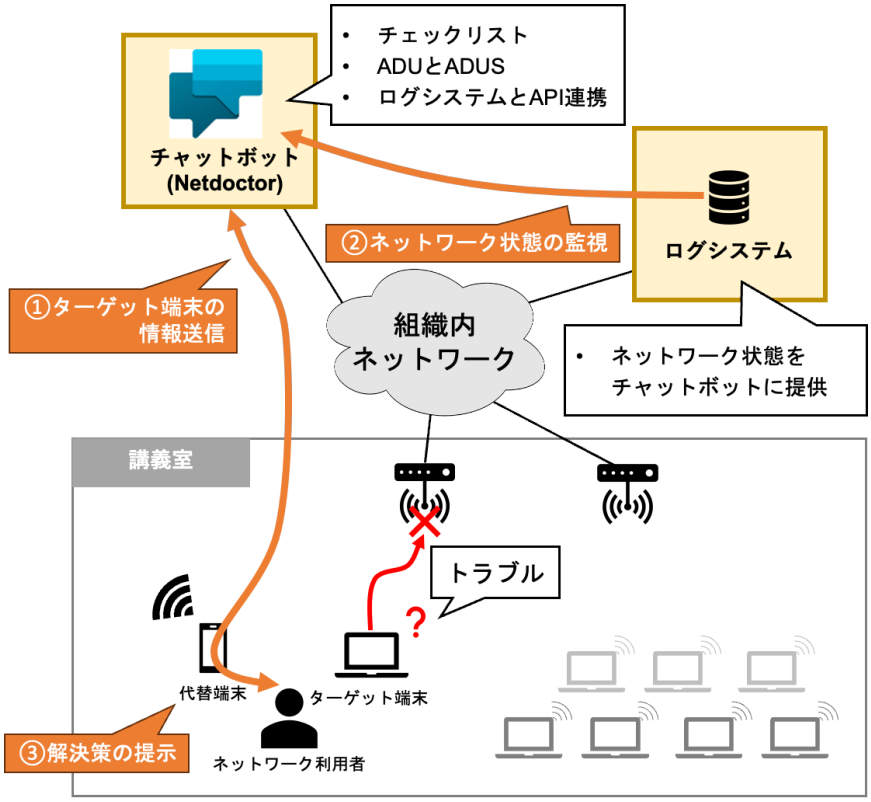


図 12: Netdoctor システム構成

■ アーキテクチャ

ログシステムが提供するエンドポイント　ログシステムは図 14 に示す通り，チャットボットからの RESTful API リクエストを受け付けるためのエンドポイントを有しており，外部ネットワークからアクセス可能である．ログシステムがチャットボットに対して提供するエンドポイントは表 3 に示す．表中の「ネットワーク認証システム」は Microsoft Entra ID[*17]など，エンタープライズ向けの認証基盤を含めた，アカウント情報から組織内ネットワークにおける利用端末情報を特定するためのシステムを指す．執筆時点で提供する情報は表 3 に示すものが全てであるが，今後，システムが検出対象とする問題が変更されたり，ネットワーク環境が変更されることにより取り扱うデータを変更する可能性がある [33]．エンドポイントに対するリクエストパラメータおよび各エンドポイントが呼び出された際に実行される外部スクリプトとその機能に関しては後述する．

ログシステム動作　ここで本実装におけるログシステムの動作について説明する．チャットボットはネットワーク機器の診断およびネットワークシステムから取得可能なユーザー認証情報を取得する際，ログシステムで提供される対象のエンドポイントに対して HTTP GET リクエストを送信する．リクエストを受けたログシステムは，ネットワーク機器からデータを取得するため，「外部スクリプト」と呼ばれるプログラムを，リクエスト内でパラメータとして与えられた絞り込みなどの条件を引数として実行する．外部スクリプトは Linux シェルスクリプトまたは Python スクリプトなど任意の言語により書かれたスクリプトで，提供されるエンドポイントに一対一で対応する形で存在しており (図 14)，ログシステムとは独立した形でサーバー内にインストールされている．「外部スクリプト」は対象のネットワーク機器との通信を直接行い，機器からログなどのデータを取得する．外部スクリプトは取得したデータを呼び出し元のプロセスに標準出力経由で CSV 形式で

[*17] https://www.microsoft.com/ja-jp/security/business/identity-access/microsoft-entra-id

表 3: ログシステムが提供するエンドポイント一覧

提供する情報	情報問い合わせ先	エンドポイント
IMC アカウントに紐づけられた MAC アドレス	ネットワーク認証システム	/users/{imc-account}/mac-addresses
端末が接続している AP の BSSID		/devices/{mac-address}/access-points/bssid
AP の設置場所	WLC (無線 LAN コントローラ)	/access-points/{bssid}/location
AP の接続端末		/access-points/{bssid}/connected-devices
AP の状態		/access-points/{bssid}/status
AP で検出された Rogue AP		/access-points/{bssid}/rogue-aps
AP で検出された干渉源		/access-points/{bssid}/interferences
AP で発生した DFS のステータス		/access-points/{bssid}/dfs/status
AP のリソース状態		/access-points/{bssid}/resources/usage
WLC のリソース状態		/wireless-controllers/{wireless-controller-id}/resource-usage
端末の接続履歴		/devices/{mac-address}/history
NW スイッチのフレームドロップ率	ネットワークスイッチ	/network-switches/{switch-id}/frame-drop-rate

パスパラメーター一覧

{imc-account}: 利用者の IMC アカウント (学内アカウント)

{mac-address}: ターゲット端末 (トラブル遭遇の利用端末) の MAC アドレス

{bssid}: ある AP の BSSID

{wireless-controller-id}: WLC(無線 LAN コントローラ) を識別する ID

{switch-id}: 有線ネットワーク区間のスイッチを識別する ID

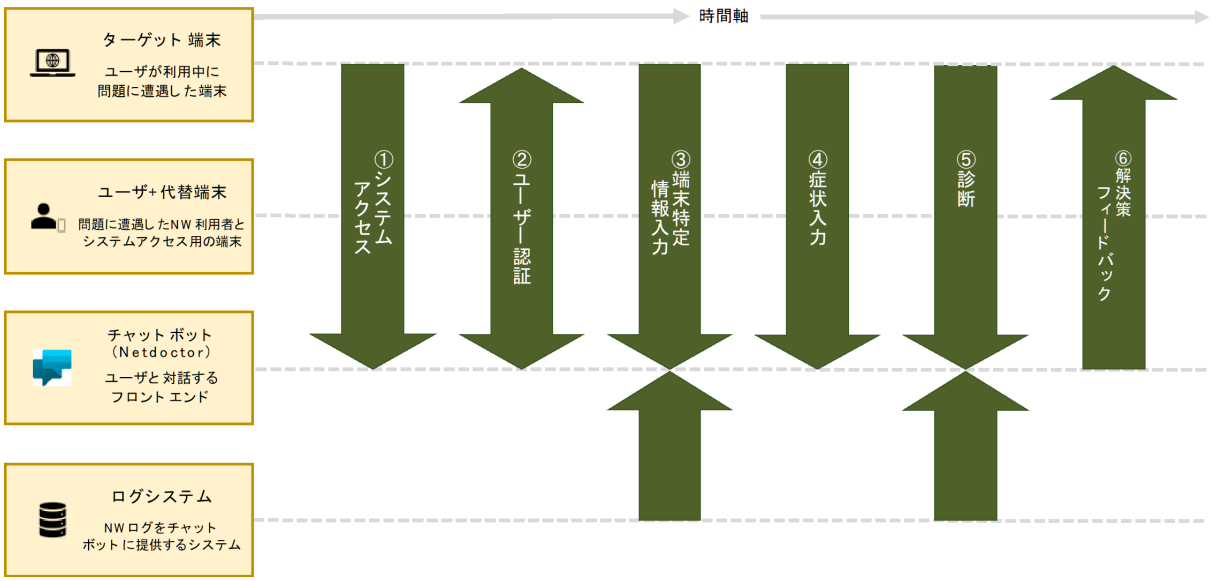


図 13: システムアクセスから診断までの流れ

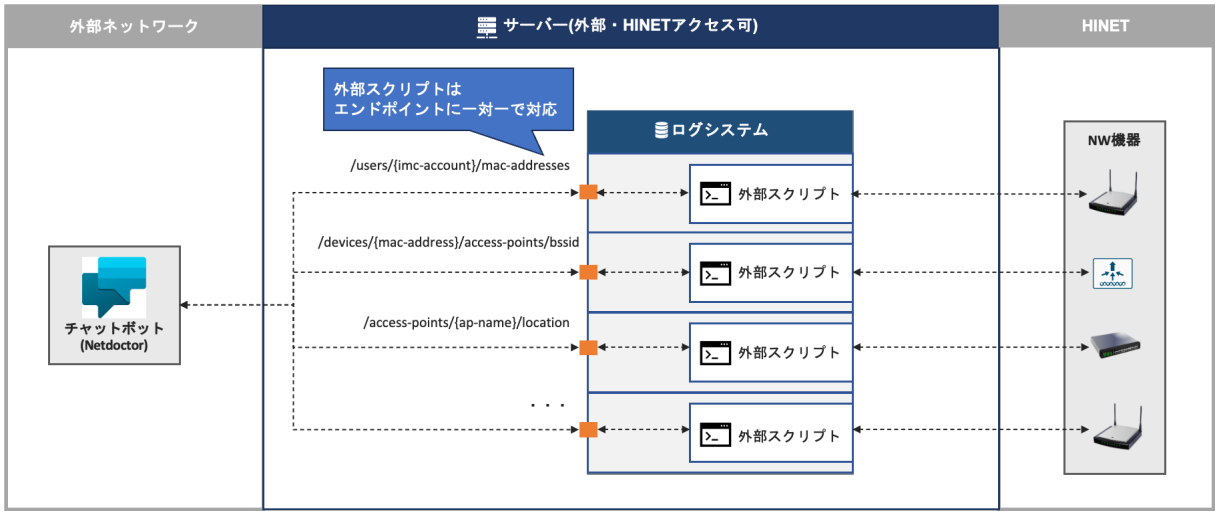


図 14: ログシステム

返却することが要件であり，本実装では呼び出し元であるログシステムにネットワーク機器から取得したデータを引き渡す．このように，ネットワーク機器との通信を直接行うスクリプトをエンドポイントとロジックを分離することにより，対象ネットワークに専門知識を持たないアプリケーション開発者によるログシステムの保守と対象ネットワークの専門家による外部スクリプト保守といったようにシステム保守の分業を達成することができる．外部スクリプトからデータを受け取ったログシステムは，その時点で受け取った CSV データをチャットボットが受理する JSON 形式に変換し，レスポンスとして返却する．ネットワーク機器からのデータに基づく障害及び問題の発生有無の判断はチャットボット側で実行するものであり，ログシステムではデータ形式の変換以外にデータの改変を行うことはない．

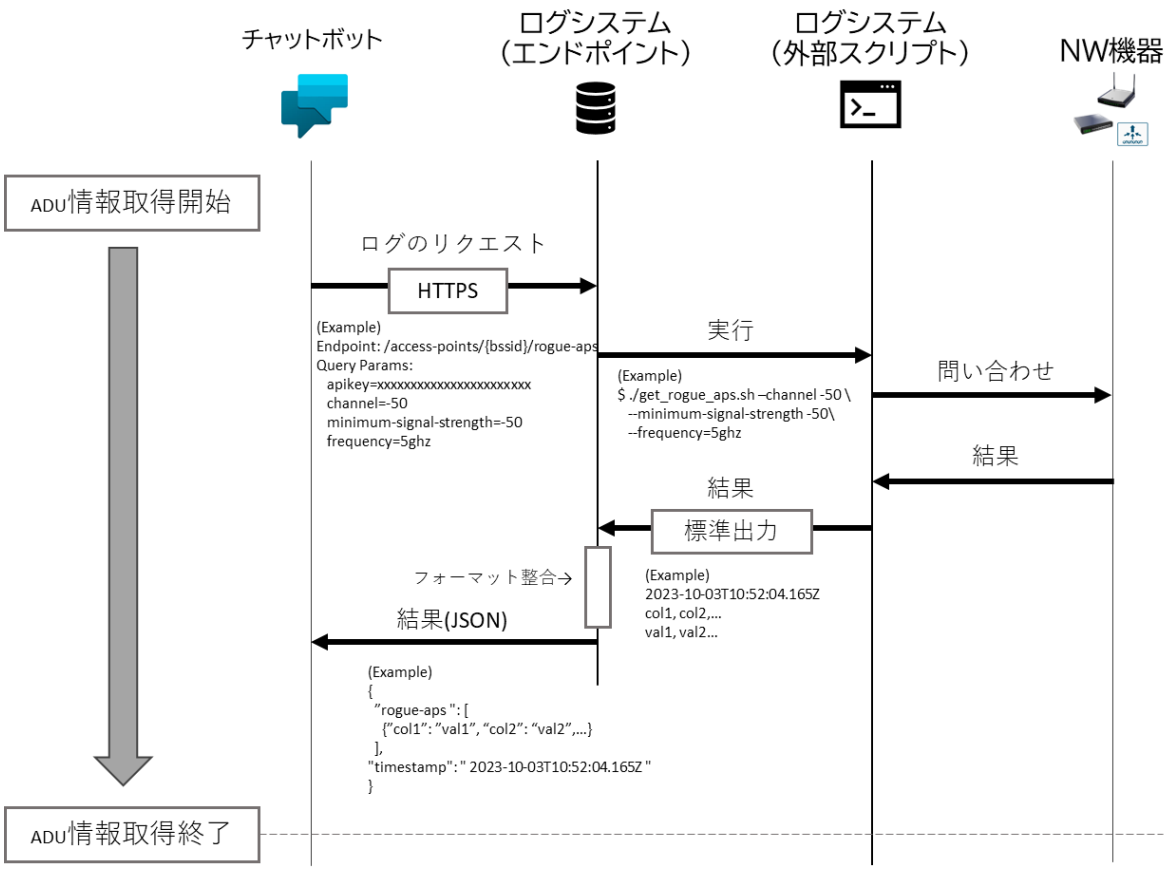


図 15: ログシステム動作フロー

■ データフロー

システムコンポーネント間のデータフロー　図 15 に示すのは，ログシステム・外部スクリプト・ネットワーク機器を含むシステムコンポーネント間の具体的なリクエストのフローを，上から下へ向かう時系列により示したものである．本フローは，ネットワーク側で発生する問題に対応する ADU における「情報取得」ステップにおいて発生するフローである (図 4 参照)．チャットボットがネットワーク機器から情報を取得する際には，まずログシステムに対して取得情報を絞り込む条件および認証用の API キーをリクエストパラメータとして指定した HTTPS リクエストを送信する．図中の例では，Rogue AP の発生有無を問い合わせるエンドポイントに対してパラメータ `apikey` に API キー, `channel`(発生チャネル) に 50, `minimum-signal-strength`(検出したとみなす最小の信号強度) として 50，`frequency`(検出対象周波数) として `5ghz` を指定している．リクエストを受信したログシステムは，クエリパラメータに記載されたパラメータを引数に，外部スクリプト `get_rogue_ap.sh` を実行し，外部スクリプトからの標準出力として対象機器からの結果を CSV 形式で受け取る．ログシステムはその時点で CSV 形式の変換を行い，JSON 形式に変更したのち，チャットボットにレスポンスボディとして送信する．以下に，それぞれのシステムコンポーネント間で行われる通信のフォーマットについて説明する．

各エンドポイントと実行する外部スクリプト　表 4 に示すのは，ログシステムが提供するエンドポイントに対して，それぞれ実行する外部スクリプトとパラメータの一覧を表したものである．先述したように，ログシステムは各エンドポイントに対するリクエストを受信したタイミングで直ちに表に挙げた外部スクリプトを実行

表 4: 各エンドポイントとパラメータ

エンドポイント	実行する外部スクリプト	パラメータ名称
/users/{imc-account}/mac-addresses	get_mac_addresses.sh	imc-account
		apikey
/devices/{mac-address}/access-points/bssid	get_connected_bssid.sh	mac-address
		apikey
/access-points/{bssid}/location	get_ap_location.sh	bssid
		apikey
/access-points/{bssid}/rogue-aps	get_rogue_aps.sh	bssid
		channel
		minimum-signal-strength
		frequency
		apikey
/access-points/{bssid}/interferences	get_interferences.sh	bssid
		minimum-signal-strength
		frequency
		apikey
/access-points/{bssid}/connected-devices	get_connected_devices.sh	bssid
		apikey
/access-points/{bssid}/status	get_ap_status.sh	bssid
		apikey
/access-points/{bssid}/dfs/status	get_dfs_status.sh	bssid
		apikey
/access-points/{bssid}/resources/usage	get_ap_resource_usage.sh	bssid
		apikey
/wireless-controllers/{wireless-controller-id}/resource-usage	get_wlc_resource_usage.sh	wireless-controller-id
		apikey
/network-switches/{switch-id}/frame-drop-rate	get_sw_frame_drop_rate.sh	switch-id
		apikey

パラメータ説明

apikey: API キー

bssid: 対象 AP の BSSID

channel: 検出対象のチャネル

frequency: 無線 LAN 周波数帯

imc-account: IMC アカウント (広島大学学内アカウント)

mac-address: 利用端末の MAC アドレス

minimum-signal-strength: 検出とみなす最低信号強度

switch-id: ネットワークスイッチの識別 ID

wireless-controller-id: 無線 LAN コントローラ識別 ID

する．各外部スクリプトは適用されるネットワークシステムや機器に応じて，ネットワーク管理者により作成されるものである．本実装においては HINET を想定したエンドポイント及び外部スクリプトを作成しており，利用者の利用端末などネットワークシステムにおける認証情報に紐づく情報の取得は IMC アカウントと呼ばれる広島大学学内アカウントを用いて行われることが想定されている．ただし，認証形態はシステムを適用するネットワークシステムによって変化する可能性があり，認証情報に紐づく情報の取得の実装はエンドポイントと外部スクリプトの両方を適用対象ネットワークシステムによって再実装する必要がある．エンドポイントのパラメータはパスパラメータ及びクエリパラメータにより表現されており，IMC アカウント (広島大学学内アカウント)`imc-account` や情報取得対象端末の MAC アドレスである `mac-address`，対象の AP の BSSID である `bssid`，無線 LAN コントローラ識別用 ID である `wireless-controller-id`，ネットワークスイッチ ID である `switch-id` といったリソースを表現するパラメータはパスパラメータ，その他の情報を絞り込むために用いられるパラメータはクエリパラメータとして表現されている．また，ログシステムはアクセス元を認証するために事前にチャットボットとログシステム間で共有した API キーを用いる．各エンドポイントの `apikey` パラメータに事前共有したキー以外の文字列が指定された状態でログシステムに HTTPS リクエストが送信された場合，`404 Forbiden` を返却する．

■ 外部スクリプト

表 5 に示すのは，本プロトタイプシステムにて実装した外部スクリプトとそれぞれのスクリプトが受け付けるオプション引数を一覧にしたものである．ログシステムはエンドポイントに対して送信されたパラメータのうち API キー以外のパラメータを対応する外部スクリプトの引数としてそのまま指定し，実行する．そのため，対象ネットワークシステムが変更され，外部スクリプトの動作に必要な引数が変化する場合にはログシステム側でのエンドポイントで受け付けるパラメータもそれに応じて実装を変更する必要がある．

ソースコード 1: 外部スクリプト出力 (一例)

```
2023-11-14T08:31:29+00:00
rogue_aps
rssi,channel
100,36
100,36
92,36
92,36
92,36
87,36
60,36
59,36
44,36
```

■ ログシステムからチャットボットへの返却値

ソースコード 1 に示すのは，外部スクリプトがログシステムに対して標準出力経由で返却する値の一例である．全ての外部スクリプトは，1 行目にネットワーク機器に対してデータを取得した時刻を表すタイムスタンプ，2 行目にデータの名称，3 行目以降に CSV 形式でデータを列挙するフォーマットであり，3 行目には列の名称，4 行目以降には具体的なデータの内容が続く．ソースコード 1 に示す例では，1 行目の内容から UTC 時間における 2023 年 11 月 14 日 08 時 31 分 29 秒に取得したデータであり，2 行目の内容からデータの名称が `rogue_aps` であること，3 行目の内容から列の名称が `rssi` および `channel` であることがわかる．ここで，`get_ap_location.sh` が提供する指定された AP の設置場所など，必ず一つのレコードのみを返却する場合に関しても，先述の形式で外部スクリプトが出力を行うことに注意されたい．

ソースコード 2: ログシステムからのレスポンスボディ (一例)

表 5: 外部スクリプトと各オプション引数一覧

スクリプト名	説明	引数一覧
get_mac_addresses.sh	IMC アカウント (学内アカウント) に紐づけられた利用端末の MAC アドレス取得	imc-account
get_connected_bssid.sh	利用端末の接続先 AP の BSSID 取得	mac-address
get_ap_location.sh	AP の設置場所取得	bssid
get_rogue_aps.sh	AP で検出された Rogue AP 一覧取得	bssid
		channel
		minimum-signal-strength
		frequency
get_interferences.sh	AP で検出された電波干渉源取得	bssid
		minimum-signal-strength
		frequency
get_connected_devices.sh	ある AP に接続された端末の状態取得	bssid
get_ap_status.sh	AP の死活状態を取得	bssid
get_dfs_status.sh	AP の DFS 発生状況を取得	bssid
get_ap_resource_usage.sh	AP のリソース使用量を取得	bssid
get_wlc_resource_usage.sh	WLC のリソース使用量を取得	wireless-controller-id
get_sw_frame_drop_rate.sh	あるスイッチでのフレーム破棄率を取得	switch-id

引数説明

bssid: 対象 AP の BSSID

channel: 検出対象のチャネル

frequency: 無線 LAN 周波数帯

imc-account: IMC アカウント (広島大学学内アカウント)

mac-address: 利用端末の MAC アドレス

minimum-signal-strength: 検出とみなす最低信号強度

switch-id: ネットワークスイッチの識別 ID

wireless-controller-id: 無線 LAN コントローラ識別 ID

```
{
  "rogue_aps": [
    {
      "channel": 36,
      "rssi_last": 100
    },
    {
      "channel": 36,
      "rssi_last": 100
    },
    {
      "channel": 36,
      "rssi_last": 92
    },
    {
      "channel": 36,
      "rssi_last": 92
    },
    {
      "channel": 36,
      "rssi_last": 92
    },
    {
      "channel": 36,
      "rssi_last": 85
    },
    {
      "channel": 36,
      "rssi_last": 60
    },
    {
      "channel": 36,
      "rssi_last": 60
    },
    {
      "channel": 36,
      "rssi_last": 45
    }
  ],
  "timestamp": "2023-11-14T08:31:29+00:00"
}
```

ログシステムは標準入力から受け取った外部スクリプトの出力を，直ちにチャットボットへのレスポンスボディとして返却するため JSON 形式に変換する．変換後の形式はソースコード 2 に例を示すとおりである．外部スクリプトの出力における 2 行目の内容をキーとして，その子項目にリストとして 3 行目以降の内容が展開され，外部スクリプトから受け取ったタイムスタンプを JSON に追加する．このように，外部スクリプトが比較的単純な CSV 形式を返却し，ログシステム側で固定された法則に従って JSON 形式のレスポンスを生成することにより，ネットワークシステムの変更や将来の拡張により外部スクリプトの変更・追加が行われた場合でも比較的容易に対応が可能な実装としている．

第 5 章　プロトタイプシステムの評価

5.1　評価概要

本章ではチェックリスト型ネットワーク診断モデルを実装したプロトタイプシステム「Netdoctor」の評価を行う．チェックリスト型ネットワーク診断モデルは，ネットワーク利用者向けの問題検出・診断モデルの一つとして本稿で提案された手法である．そのため，モデルを用いた診断の有効性および診断の迅速性について評価することにより，既存のシステムや取り組みと比較してネットワーク利用者に対して的確かつ迅速に問題解決のアプローチが行えること，およびその目的を達成する上で必要となる課題を特定することが今回の評価目的となる．

評価は，システムの仕様をもとに類似ツールとの比較により行われる定性的な評価と，広島大学内で被験者を募りプロトタイプシステム「Netdoctor」の利用と質問紙によるアンケートを行うことにより行う実験評価の 2 種類を実施する．定性的な評価は，「Netdoctor」と同様のネットワーク監視システムおよび運用支援システムである SINDAN Project および Cisco Meraki との比較を行うことにより実施した．評価観点は以下の 4 種類を想定した．

- システムの利用目的
- システムの利用対象者
- システムの利用タイミング
- 分析対象データ

また，実験評価は学内ネットワークに見立てた実験用ネットワーク内で仮想的に 2 種類の障害および問題を発生させ，その環境内で利用端末および Netdoctor を用いた診断を被験者に行ってもらうことにより実施した．実験後，利用者にはアンケートに回答してもらい，チェックリスト型ネットワーク診断モデルによる診断の迅速性・的確性・解決に至った割合を調査した．

5.2　類似システムとの比較評価

類似システムとの比較評価を行うに当たっては，Netdoctor と同様にネットワークシステムのトラブル対処に利用されるツールや取り組みを対象に，システムの基本情報に対してそれぞれ評価を行う．評価項目は，「利用目的」「利用対象者」「利用タイミング」「分析対象ログ」の 4 つを挙げた．特に，「利用対象者」とはシステムのユーザーインターフェースを操作し，ネットワーク状態を実際に閲覧する対象者のことを指し，「利用タイミング」とは利用対象者がユーザーインターフェースにアクセスしシステムを利用するタイミングのことを指す．また，「分析対象ログ」はシステムがネットワーク監視および診断に用いるデータの情報源を示しており，複数存在する可能性がある．

Netdoctor との比較対象としては，組織内ネットワークを管理・監視する仕組みのうち，以下の条件を満たすものを選択した．

- 無線 LAN に特化したツール・取り組みであること
- 組織構成員に対して，ネットワーク利用者の接続トラブルの特定・解決策を考慮する上で判断材料となる情報提供を行うもの

表 6: Netdoctor および類似ツールの比較表

	Netdoctor	SINDAN Project	Cisco Meraki
利用目的	NW 利用者へのトラブル解決の直接的支援	利用者視点での情報に基づく NW 障害点の検出	無線 LAN 監視
利用対象者	NW 利用者	NW 管理者	NW 管理者
利用タイミング	NW 利用者が接続トラブルに直面した際	NW 管理者が利用者からのトラブル申告を受けた際	ネットワーク管理・監視・設計を行う際
分析対象ログ	・組織内 NW ログ (限定的) ・利用端末ログ	・センサデバイスからのログ	・AP ログ

これら 2 点の条件を満たす取り組みとして，SINDAN Project[8, 9]，Cisco Meraki[*18]を比較対象として選択した．

■ 比較結果

類似ツールとの比較の結果は，表 6 に示す．

利用目的　いずれもネットワークシステムで発生する障害およびトラブルに対して，その特定または解決の手掛かりとなる情報を提供する点では共通している．ただし，Netdoctor の情報提供先のみがネットワーク管理者ではなく利用者を対象としたものであるという点が特筆すべき点である．

利用対象者　Netdoctor のみがネットワーク利用者を対象としたシステムである一方，他の 2 点はネットワーク管理者によって利用されることが想定されている．

利用タイミング　Cisco Meraki が異常時のアラートも含めた定常的なネットワークシステムの監視を実施する一方で，Netdoctor および SINDAN Project は，接続トラブルに遭遇したネットワーク利用者が発生した場合に利用される点で共通している．ただし，SINDAN Project はトラブルに遭遇したネットワーク利用者から申告を受けたネットワーク管理者が利用することを想定している一方，Netdoctor はトラブルに遭遇したネットワーク利用者自身が利用することが想定されている．

分析対象ログ　Netdoctor は限定的な組織内ネットワーク統計情報およびネットワーク利用者の利用端末から出力できる情報を対象とする．一方，SINDAN Project は接続端末側に設置されたセンサデバイスから観測したネットワーク状態，Cisco Meraki は AP から取得できるほとんど全ての情報を分析可能であり，どちらも Netdoctor と比較して対象とする情報の種類は多様である．

■ 考察

今回比較対象としたツールのうち，Netdoctor のみがネットワーク利用者への直接的なトラブル解決支援を目的としたツールであった．本評価においては，ネットワーク管理者を介したトラブル解決ではなく，ネットワーク利用者による迅速なトラブル回避を直接支援する点が Netdoctor の独自性であることを確認した．一方，分析対象のログおよびデータに注目すると，Netdoctor と比較して他の 2 点がより多様なデータを収集可能であることが言える．今後の展望として，他ツールが収集したログを診断時の判断に応用する仕組みを作ることで，より多様かつ的確なトラブルに対する診断が行えることが期待できる．

[*18] https://meraki.cisco.com/ja-jp/

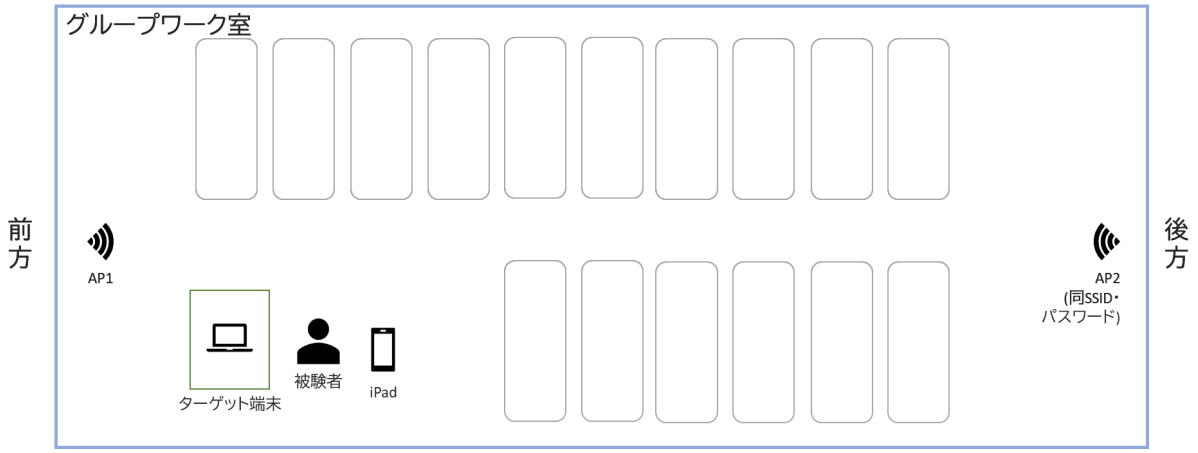


図 16: グループワーク室配置

5.3 評価実験

5.3.1 実験環境

実験は，広島大学情報メディア教育センター本館内の一室 (グループワーク室) に実験用ネットワークを構築し，被験者が部屋の中を自由に動き回れるような環境で行った．グループワーク室を上部から見下ろした配置図を図 16 に示す．グループワーク室には最前方と最後方にそれぞれ AP を一台ずつ配置し，同じ SSID およびパスワードの組み合わせて実験用ネットワークに接続できるようにした．配置した AP はそれぞれ AP1, AP2 と呼ぶことにする．

■ 利用端末

被験者には実験者が用意した Windows PC および iPad をそれぞれターゲット端末および代替端末として利用してもらう．iPad は実験用ネットワークとは別の正常に通信できるネットワークに接続してあり，スマートフォンと同様，実験用ネットワークの影響を受けずにシステムにアクセスすることが可能となっている．そのため，被験者によるシステムの利用体験が行われる際には事前に iPad からチャットボットのインターフェースにアクセスできるように設定しておき，Windows PC で実験用ネットワークへの接続と，トラブルへの遭遇を被験者に行ってもらったタイミングで iPad を利用して Netdoctor による診断を行ってもらう．

■ 実験用ネットワーク

実験において事前に構築した実験用ネットワークの構成は図 17 に示す通りである．また，本実験において使用したマシンのスペックを表 7，表 8，表 9，表 10 に示す．仮想ネットワークは `VirtualBox(Windows)` と呼ばれる物理 Windows マシン上に構築され，仮想マシンプラットフォーム VirtualBox を用いて構築されている．本物理マシンは 3 つの NIC を持つマシンであり，VirtualBox 上で構築された `VM1(Logsystem Server)` と呼ばれる仮想マシンは物理 NIC `enp0s8` に接続されている．`enp0s8` は外部からの着信接続が可能なネットワークに接続されており，クラウド上のチャットボットからのリクエストを受信することが可能である．`VM1(Logsystem Server)` 上では NAPT・ACL，および Docker 上でログシステムが動作しており，ログシステムは NAPT および ACL により構成された内部ネットワーク (`192.168.0.0/24` へのアクセスおよびインターネットからのアクセスが可能な設定となっている．`VM 1(Logsystem Server)` 上で稼働する NAPT ゲートウェイにはグローバル IP アドレス `133.51.117.51` が割り当てられており，インターネット上の任意の IP アドレスからアクセスが可能である．また，`133.51.117.51:443` 宛のパケット

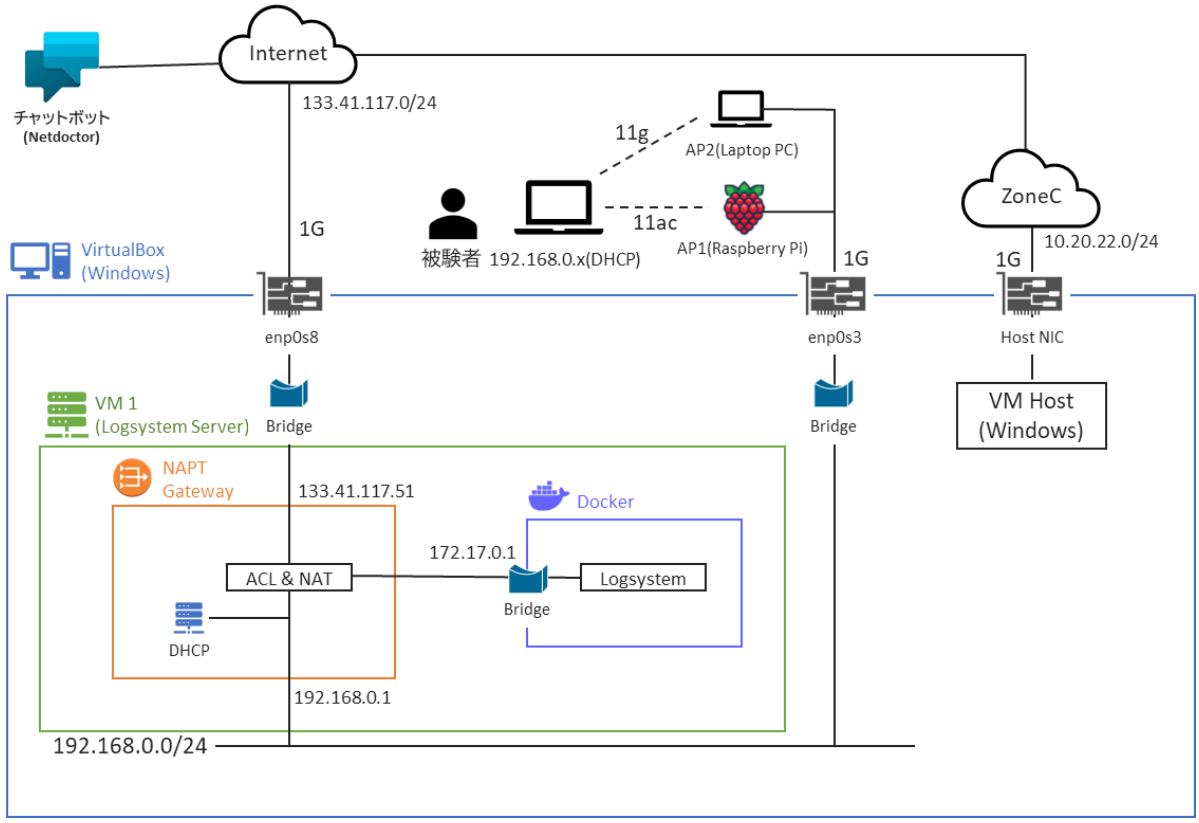


図 17: 実験用ネットワーク

はログシステム (172.17.0.1) 宛にポートフォワーディングされるように NAPT を構成している．そのため，チャットボットがログシステムにリクエストを送信する際，133.41.117.51:443 宛にリクエストを送信することでログシステムからの応答を得る．VM 1(Logsystem Server) はインターネット上の任意のアドレスからアクセスすることが可能であるが，セキュリティ上の理由から ACL により IP アドレスフィルタリングを行うことによりチャットボットが存在するサーバ以外からのアクセスを拒否するように設定されている．内部ネットワークは物理 NIC enp0s3 を経由して，Raspberry Pi により構成された AP から無線 LAN 経由で被験者の利用するターゲット端末と接続されている．AP でのスループット低下などの障害を再現する際は，Raspberry Pi 上で帯域制限を実施することにより実現する．

VM 1(Logsystem Server) が有するグローバル IP アドレスである 133.51.117.51 に対しては 1610-051.a.hiroshima-u.ac.jp というドメインが割り当てられているため，このドメインを利用してドメイン認証を行う TLS 証明書を Let's Encrypt[*19]を用いて発行した．これにより，チャットボットとログシステム間の通信は HTTPS プロトコルにより行われる．

ホストマシンはゾーン C(図中 ZoneC) と呼ばれる研究室内のネットワークを経由してインターネットにアクセス可能としている．ここで用いる NIC は実験に用いる NIC とは独立したもの (Host NIC) を利用している．

[*19] https://letsencrypt.org/

表 7: 物理マシン: Virtualbox(Windows) の性能

CPU	AMD Ryzen 9 5900X 12-Core, 3701MHz
メモリ	32GB
SSD	1TB
NIC	・Realtek PCIe GbE Family Controller ・Realtek PCIe 2.5GbE Family Controller(x2) ・Intel® 82599 10 Gigabit Network Connection

表 8: 仮想マシン: VM 1(Logsystem Server) の性能

vCPU	4
メモリ	8GiB
VM ホスト	Virtualbox(Windows)
NIC 割り当て	Realtek PCIe 2.5 GbE(x2)(enp0s3 および enps8 として)

表 9: 物理マシン: AP1 の性能

モデル	Raspberry Pi 4 Model B
CPU	Broadcom BCM2711, quad-core Cortex-A72 (ARM v8) 64-bit SoC
メモリ	8GiB
無線 LAN	IEEE802.11b/g/n/ac(2.4GHz/5GHz)

表 10: 物理マシン: AP2 の性能

モデル	ASUS Vivobook E203NA
CPU	Intel Celeron N3350(Apollo Lake) 1.1GHz/2-core
メモリ	4GB
無線 LAN	IEEE802.11a/b/g/n/ac(2.4GHz/5GHz)

5.3.2 実験内容

実験は，広島大学先進理工系科学研究科および情報科学部，総合科学部の学生計 9 名，情報メディア教育研究センター職員 3 名を被験者として行った．実験内容はプロトタイプシステムの被験者による利用体験と，体験後のアンケート回答とした．システムが利用するチェックリスト・ADU・ADUS は HINET 向けのものを利用した（内容は付録を参照）．被験者による利用体験については，障害および問題を仮想的に発生させた実験用ネットワークにおいて，実験者が用意した Windows PC および iPad の 2 台の端末をそれぞれターゲット端末，代替端末としてトラブルの診断を被験者に行ってもらう形態で行った．一方，体験後のアンケート回答については，Microsoft Forms[*20]を用いた質問紙法によるアンケート回答を行ってもらった．

実験は図 18 に示す手順で実験を行った．本実験では，仮想的に 2 種類の障害及び接続トラブルを仮想的に

[*20] https://www.microsoft.com/ja-jp/microsoft-365/online-surveys-polls-quizzes

図 18: 実験手順

表 11: シナリオ①設定

再現トラブル	Rogue AP による電波干渉
チェックリスト・ADU 番号	No.2-2(図 19)
AP 設定	表 12，表 13，表 14 に記載
対処法想定	利用端末の部屋内移動
操作ステップ数 (チャットボット)	9

再現し，それぞれの障害・トラブルを「シナリオ①」,「シナリオ②」として定義している．以下にそれぞれのシナリオについての説明を行う．

■ シナリオ①

再現する問題　まず，「シナリオ①」に関しては，接続先の AP が利用しているチャネルと同一のチャネルで Rogue AP による電波干渉が発生しており，AP と利用端末間のスループットが非常に低下しているというシナリオを想定している．チェックリスト中 No.2-2 を再現したシナリオで，対応する ADU のフローは図 19 に示す．AP ローミングが整備された環境においては，このようなシナリオでは端末を Rogue AP の干渉が発生していない別のチャネルを利用する AP に再接続することにより，正常な通信に復旧することができる．この状況を再現するため，本実験においては，部屋前方に設置された AP1 付近に AP1 と同じチャネルで通信を行うアクセスポイントを設置したうえで，AP1 に対して `tc` コマンドを用いた帯域制限を付与した．帯域制限はネットワークから端末へ向かう方向のみに設定を行い，端末から見てアップロード速度には制限がかかっていない．この時，AP1 に接続した端末とインターネット間のスループットはダウンロード速度が 85$kbps$ 程度で，端末は AP とのアソシエーションを確立できるものの，大多数の Web ページおよびネットワークを利用するアプリケーションが閲覧できない状態になる．計測には fast.com[*21]を用いた．一方，後方に設置されている AP2 には帯域制限を含めたトラブルを再現しておらず，アソシエーションした場合には正常な通信が可能となる．AP1, AP2 はともに `sudo iwconfig {interface_name} txpower 0` コマンドを入力する

[*21] https://fast.com/

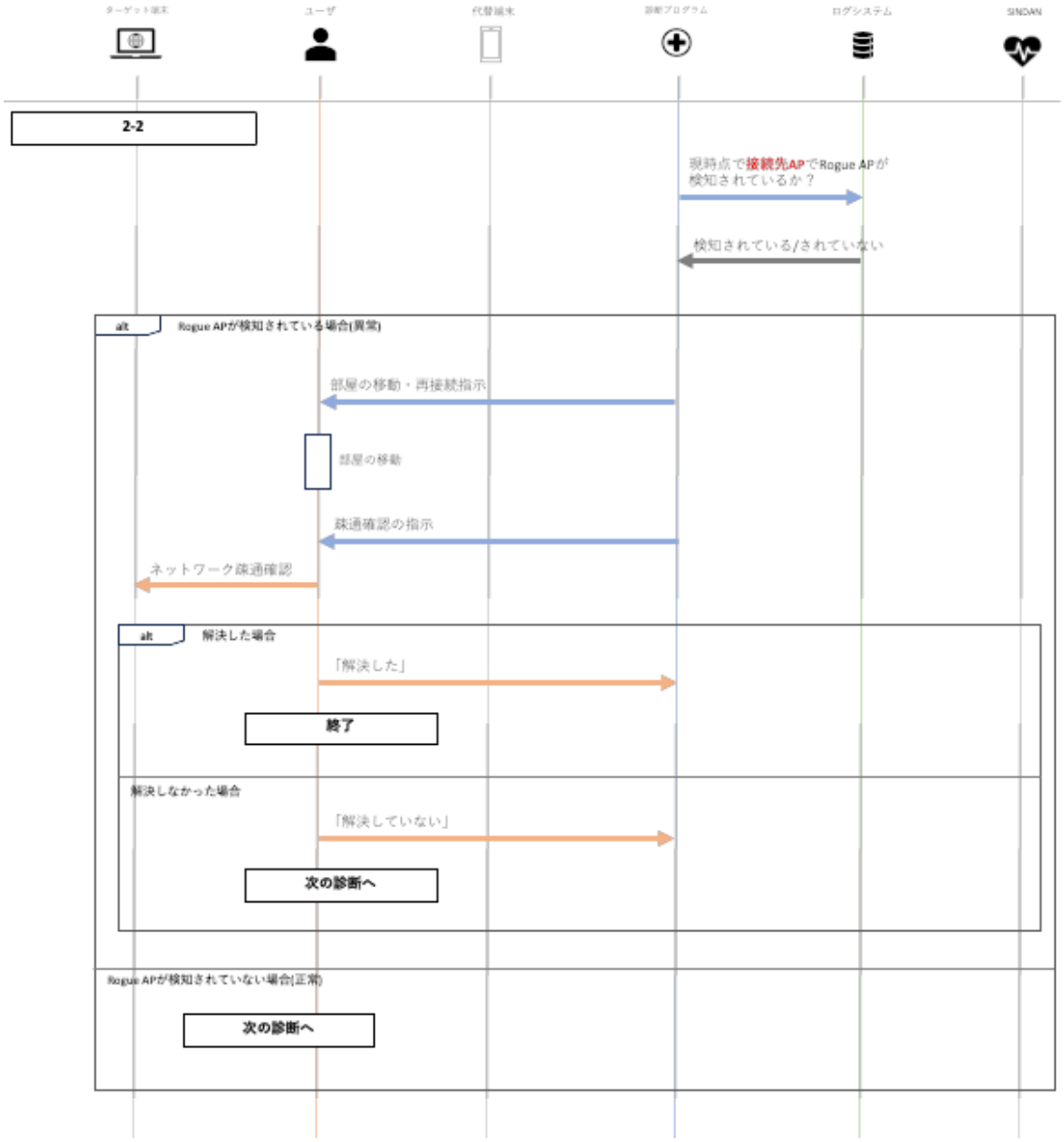


図 19: データフロー: ADU2-2

ことにより電波出力強度を小さくしている．ここで，{interface_name} には各 AP の電波送受信に用いられる NIC 名称が入る．また，診断システムが Rogue AP を検出できるようにするため，AP1 及び AP2 とは別のアンテナを用いて，AP1 と同一チャネル上で通信を行う Rogue AP を実際に構築する．以上を踏まえて，実験環境は表 11 に示すように設定した．

表 12: シナリオ①-AP1 の設定

規格	IEEE802.11ac
SSID	PrvNW-GroupWorkRoom-NetdocExp1
パスフレーズ	`enter-wrote-key`
使用チャネル	36
チャネルボンディング	20MHz

表 13: シナリオ①-AP2 の設定

規格	IEEE802.11g
SSID	PrvNW-GroupWorkRoom-NetdocExp1
パスフレーズ	`enter-wrote-key`
使用チャネル	1
チャネルボンディング	20MHz

表 14: シナリオ①-Rogue AP の設定

規格	IEEE802.11ac
SSID	PrvNW-GroupWorkRoom-Interrupt
使用チャネル	36
チャネルボンディング	20MHz

用語「tc コマンド」

tc コマンドは，Linux カーネルにおけるトラフィック制御を行うために用いられるコマンドである [34]. Linux カーネルが NIC に対してパケットを送信しようとするとき，パケットは qdisc(queuing discipline) と呼ばれるバッファに格納される．デフォルトでは `pfifo` と呼ばれる qdisc が使用されており FIFO 型のキューとして機能するが，tc コマンドを使用することにより，別のデータ構造を持つ qdisc に変更することができる．本文においては，ネットワークをエミュレートする `netem` と呼ばれる qdisc を使用することにより，特定の NIC に対して帯域制限を設定している．

実験手順　ここまで説明したシナリオ①の環境における実験手順を説明する．まず，被験者に対してはネットワークで何か問題が発生したり，つながらない，あるいは通信が遅い場合には iPad を利用して Netdoctor を利用するように事前に声掛けを行う．その後被験者は図 16 に示すようにグループワーク室の前方にてターゲット端末のセットアップを行ってもらう．この際にセットアップを行う項目は AP1 および AP2 の SSID およびパスフレーズで，被験者は無線 LAN を通じて実験用ネットワークへのアクセスを試みる．この時点で被験者に任意の Web ブラウザやネットワークを利用するアプリケーションを利用するように声掛けを行う．ターゲット端末は AP1 とのアソシエーションを行うものの，帯域制限を受けているため Web ページおよび Web アプリケーションの利用が困難な状態となっている．利用者はこのタイミングで iPad を利用して Netdoctor にアクセスを行い，診断を開始する．診断を実施したのち，最終的にシステムから解決策として「グループワーク室後方へ移動し，端末の Wi-Fi を再起動」するようにアドバイスがフィードバックされる．ユーザーはこの指示に従い，部屋の後方に移動し，端末の無線 LAN を再起動する．最終的には，グループワーク室後方に設置した AP2 にターゲット端末がアソシエーションされることにより，正常な通信が可能となる．この時

表 15: シナリオ②設定

再現問題	認証情報の誤り
チェックリスト・ADU 番号	No.2-1(図 20)
AP 設定	表 16，表 17 に記載
対処法想定	認証情報の確認と再入力
操作ステップ数 (チャットボット)	13

表 16: シナリオ②-AP1 の設定

規格	IEEE802.11ac
SSID	PrvNW-GroupWorkRoom-NetdocExp2
パスフレーズ	`right-Ianguage-kerneI`
使用チャネル	36
チャネルボンディング	20MHz

点で Netdoctor による診断を終了し，シナリオ①に関する実験は終了となる．

■ シナリオ②

再現する問題 「シナリオ②」に関しては，ネットワーク利用者の利用端末に設定された認証情報 (SSID・パスワードの組み合わせ) に誤りがあり，端末が AP にアソシエーションできないというシナリオを想定している．チェックリスト中 No.2-1 の問題を再現させたシナリオで，対応する ADU フローは図 20 に示す．IEEE802.1X を用いて組織内無線 LAN への接続端末を認証する仕組みが整備された環境においては，構成員のパスワード変更など，接続するために必要な認証情報が変更されたにも関わらず，変更前の認証情報が利用端末に残留しているために接続できないといったトラブルが想定される．このようなシナリオでは，端末に正しい認証情報を入力することで正常な通信を復旧することができる．この状況を再現するため，本実験においては，WPA2 認証を行う AP1 および AP2 において認証時に用いるパスフレーズである PSK(Pre-Shared Key) として誤ったものをユーザーに入力させることで，AP にアソシエーションできない状態を作り出す．具体的には，正確なパスフレーズは `right-Ianguage-kerneI` であるところを，被験者には `right-language-kernel` と入力させる．以上を踏まえて，実験環境は表 15 に示すように設定した．

用語「IEEE802.1X」

IEEE802.1X はバックエンドに設置された RADIUS などの認証サーバの情報を利用して，有線 LAN および無線 LAN への接続資格の有無を判断する認証方式である [35]．組織構成員がネットワークを利用しようとする際，認証サーバに登録された ID およびパスワードを入力することにより認証が行われる．端末で入力した認証情報が誤っていた場合，Windows では利用者のコマンド操作を行うことで認証に失敗した旨が無線 LAN 接続レポートとして取得できる．

なお，今回被験者が経験する症状は「ネットワークに全くつながらない」というものであるが，Netdoctor が本症状に対応する ADUS を実行する際には「パスフレーズなどの認証情報の誤り」を検出する ADU よりも前に「Rogue AP による接続品質低下」を検出する ADU も実行する．シナリオ②では AP1 の帯域制限は発生させず，かつ Rogue AP を有効にした状態で行う．そのため，被験者は認証情報の誤りを Netdoctor から指摘される前に一度シナリオ①と同様のフィードバックを受ける．

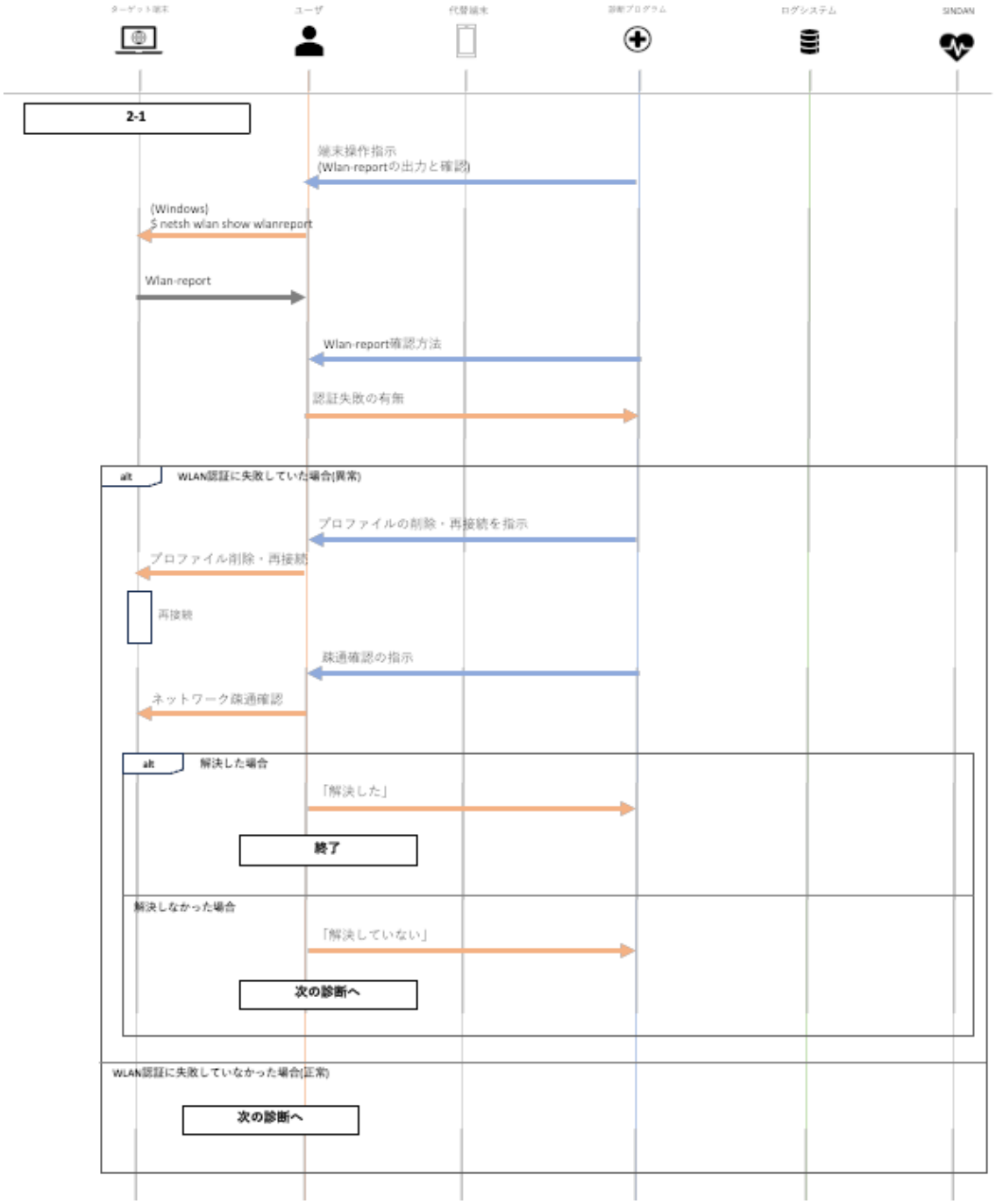


図 20: データフロー: ADU2-1

表 17: シナリオ②-AP2 の設定

規格	IEEE802.11g
SSID	PrvNW-GroupWorkRoom-NetdocExp1
パスフレーズ	`right-Ianguage-kerneI`
使用チャネル	1
チャネルボンディング	20MHz

実験手順　ここまでに説明したシナリオ②の環境における実験手順を説明する．シナリオ①と同様，被験者に対してはネットワーク上のトラブルを認識した時点で Netdoctor を利用するように事前に声掛けを行い，グループワーク室前方にてターゲット端末のセットアップを行ってもらう．ここではシナリオ①とは異なる SSID およびパスワードの組み合わせに接続するよう被験者に案内し，誤りのあるパスフレーズを入力させる．この時点で，被験者はターゲット端末で AP1, AP2 のいずれにもアソシエーションできない状態となり，Netdoctor で診断を開始する．先述の通り，Netdoctor は「Rogue AP による接続品質低下」を検出する ADU を先に実行するため，被験者はまず診断の結果としてシナリオ①で受けたものと同じ解決策がフィードバックされ，実行する．ただし，ここで被験者が実行した解決策によりネットワークへのアクセスが回復するわけではないため，Netdoctor は引き続き診断を継続する．次に Netdoctor は被験者に対して無線 LAN 接続状況のログを出力するコマンドをターゲット端末上の PowerShell[*22]経由で入力してもらい，出力されたログから AP 接続時の認証情報に誤りがある可能性を示す出力を探してもらう．最終的に被験者は出力を発見し，その旨を Netdoctor に入力することで「教員に対して正しい認証情報を再確認してください」という趣旨の解決策がフィードバックされる．被験者には事前に実験者が教員役としてふるまうことを説明しているため，この時点で被験者は実験者に対してパスフレーズの確認を行い，正しいパスフレーズをターゲット端末に入力する．これによりターゲット端末が AP2 を経由して正常な通信が可能となるため，この時点で診断およびシナリオ②に対する実験は終了となる．

5.3.3　実験後アンケート

■ 検証仮説

1.3 節の議論から，開発プロトタイプシステムに求められる要件及び対応する評価観点として以下の項目を想定した．

- 診断により問題解決に至ること (問題解決率)
- 解決策が的確であること (解決策の的確性)
- 利用者による端末操作が迅速に完了すること (操作指示数の適切さ)
- 診断が迅速であること (診断の迅速性)
- 利用者に対する指示が的確であること (操作指示の的確性)
- 関係者がシステムを利用したいと考えていること (システムの利用願望)

これらの要件を確認するため，評価に当たっては事前に以下の仮説を想定することとした．評価実験の結果得られたデータをもとに，仮説の検証を行うことでシステムが要件を満たすことを確認する．

1. (問題解決率・解決策の的確性) システムの提示した解決策は利用者にとって理解ができるものであり，

[*22] https://learn.microsoft.com/ja-jp/powershell/

実際に問題解決までに至った.

2. (診断の的確性) システムが利用者に要求する操作手順は，いずれの問題に対しても冗長性がなく，かつ不足がない.
3. (操作指示数の適切さ) システムからの端末操作指示および解決策は無線 LAN に関する知識の浅い人たちにも的確なものである.
4. (診断の迅速性) システムの診断は窓口に比べていずれの症状に対しても迅速に対処が可能である.
5. (システムの利用願望) 利用者・管理者ともに，本システムを導入したいと考える.

■ アンケート項目

実験後アンケートの項目としては，主にチェックリスト型ネットワーク診断モデルにおける「診断の的確性」「診断の迅速性」「問題解決に至った割合」を調査することを主眼に，表 18 に示すような質問を作成した.

質問はカテゴリーを主に以下の 4 つに区分し，それぞれに対して質問項目の作成を行った.

- 所属・属性に関する質問群
- シナリオ①における Netdoctor 診断に関する質問群
- シナリオ②における Netdoctor 診断に関する質問群
- 事務的な質問群

所属・属性に関する質問群　まず「所属・属性に関する質問群」では，被験者が学生か教職員であるかを識別する属性と所属に加えて，プロトタイプシステムの導入対象ネットワークである HINET Wi-Fi の利用頻度および接続トラブルの遭遇経験の有無及び遭遇した場合の対処法，無線 LAN に関する背景知識の有無について質問を行っている，特に，無線 LAN に関する背景知識の有無はクイズ形式により行っており (第 6 問目・第 7 問目)，正答率が高ければ背景知識が高いと判断できる．これにより，ネットワーク利用者である学生と窓口にてネットワークトラブルのサポートを行う立場である教職員との間における評価の差，および無線 LAN におけるトラブル対処能力の高い集団と高いとは言えない集団について評価について差の有無を評価する.

Netdoctor 診断に関する質問群　次に「シナリオ①における Netdoctor 診断に関する質問群」では，シナリオ①におけるシステムの利用体験に対して診断の的確性，迅速性，問題解決に至ったか否かを確認する．第 8 問目の質問で被験者が問題解決を行うことができたかを回答し，第 10 問目から第 13 問目ではチャットボットによる端末指示及びフィードバックする解決策の的確性を回答する．第 14 問目および第 15 問目では IT 管理部門におけるヘルプデスク等の窓口を比較対象に，被験者が主観的に判断した診断の迅速性を回答する．「シナリオ②における Netdoctor 診断に関する質問群」においても，シナリオ②を体験した後の被験者に対して同じ質問が行われる.

事務的な質問群　最後に「事務的な質問群」に関しては，Netdoctor が実際に構成員から利用可能になった場合に利用したいと思うか否か，およびヘルプデスク等の窓口において経験したトラブルや不満，任意の質問や意見を回答させる質問を追加した.

5.3.4　結果

以下にそれぞれの仮説に関連する結果と，その考察を述べる．完全な結果は付録を参照されたい.

■ 得られたデータについて

本実験では，合計 12 人の広島大学構成員 (うち，学生 9 名，職員 3 名) から回答を得られた.

表 18: 実験後アンケート質問一覧

番号	質問カテゴリー	質問内容
1	所属・属性に関する質問	あなたの属性を選択してください.
2		所属を教えてください (教職員の方は「その他」から入力をお願いします).
3		授業期には週に平均してどれくらい HINET Wi-Fi(HU-CUP) を利用していますか.
4		HINET Wi-Fi を利用する際に遭遇したことのある症状を全て選択してください.
5		トラブルに遭遇したことがある場合，どのようにして解決しましたか？全て選択してください.
6		以下のうち，無線 LAN による接続速度を低下または接続を困難にさせる可能性のある要因として，実際に起こりうるものを全て選択してください.
7		以下のうち，無線 LAN の規格について正しいものを全て選択してください.
8,17	(シナリオ①,②) 診断に関する質問	チャットボットによる診断の結果，問題を解決することができましたか.
9,18		チャットボットによる診断を開始してから終了するまでにあなたが行った操作手順の数は，解決しようとしている症状に対して多いと感じましたか？
10,19		9,18 番の質問で適切なものでなかったと判断した場合，どのような操作にそう感じましたか。
11,20		チャットボットからの端末の操作指示は，あなたが端末を操作する上で的確なものでしたか？
12,21		11,21 番の質問で的確なものでなかったと判断した場合，どのような情報が欲しかったですか．または，どのような情報が冗長だと感じましたか.
13,22		チャットボットからフィードバックされた「問題の要因」および「問題の解決策」は，あなたが問題を解決する上で的確な内容でしたか？
14,23		13,22 番の質問で的確なものでなかったと判断した場合，どのような情報が欲しかったですか．または，どのような情報が冗長だと感じましたか.
15,24		窓口で対応を受ける場合の方が，問題解決が迅速に行えると感じましたか.
16,25		15,24 番の回答について，そのように考えた理由を教えてください.
26	その他の質問	このシステム (Netdoctor) が HINET に導入されたら，利用したと思いますか？
27		(任意)PC サポートデスク等を利用したことがある場合，窓口でトラブルを相談する際に困った経験はありますか？
28		その他，質問などがありましたらご記入ください.

無線 LAN に関する知識レベルの高低による群の分類　本アンケートでは質問番号 6 および 7 に無線 LAN に関する知識レベルを判定するために用意されたクイズがある．これらの質問に対する正答数により，知識レベルの高い群と低い群に分類し，それぞれで診断システムに対する評価に違いが表れるかを考察する．知識レベルの基準は，質問 6 の正答数と質問 7 の正答数を足した数字を基準とし，中央値である 7.5 以下のスコアを持つ被験者は無線 LAN 知識レベルの低い群，それ以上のスコアを持つ群は高い群に分類する．それぞれの群に分類されたサンプル数は表 19 に示す．なお，質問 6 の正答数および質問 7 の正答数との間の相関係数は

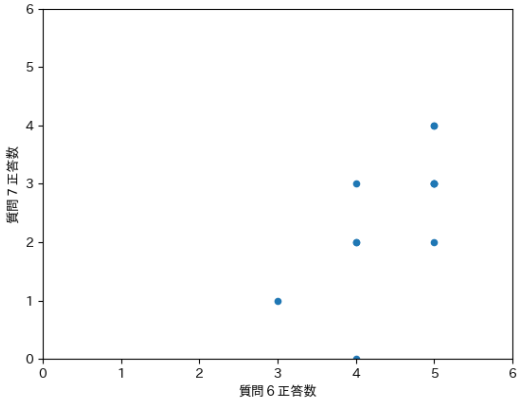


図 21: 質問 6 および 7 の正答数に対する散布図

表 19: 各群のサンプル数

群名称	サンプル数
無線 LAN 知識レベルの低い群 (以下，単に低い群)	6
無線 LAN 知識レベルの高い群 (以下，単に高い群)	6

$r = 0.692820 (n = 12)$ であり，おおむね正の相関があると言える．散布図は図 21 に示す．

■ 仮説 1：システムの提示した解決策は利用者にとって理解ができるものであり，実際に問題解決までに至った．

問題解決に至った人数　図 22 に示すのは，Netdoctor による診断の結果，問題の解決に至ったあるいは至らなかった回答者数をシナリオ別に示したものである．このグラフは質問番号 8 及び 17 の回答結果に対応しており，横軸における「はい」が解決に至った人数，「いいえ」が至らなかった人数である．結果としては，シナリオ①，②のそれぞれ 1 人を除いてすべての被験者が問題解決に至った．このことから，システム利用者の大多数が実際に問題解決に至ることができると読み取れる．一方，シナリオ①で解決に至らなかった 1 人は，iPad 及びチャットボット自体の操作に慣れておらず，正しく端末操作を実行することができなかったため，問題自体の解決に至らなかった．実験時にチャットボット自体の利用方法をさらに詳しく説明することにより，解決に至ることができたものであると考えている．また，シナリオ②で解決に至らなかった 1 人は実験中に発生した別のトラブルにより問題解決に至ることがなかったものである．

実験中のトラブル　トラブルの内容として，シナリオ②において，AP1 の帯域制限が有効になっており，かつ AP2 がダウンしており電波を発信していなかった．そのため，被験者は正しいパスワードを入力しても強制的に帯域制限がかかった AP1 に接続されてしまった．この問題に対しては利用者による解決策の実施後，利用端末が確実に別の AP(実験では AP2) に接続されていることを検証し，検証に失敗した場合には再度 Wi-Fi の再起動を行わせるかさらに別の場所へ移動させるといった二次的な対応を利用者に取らせることが理想的なシステム動作である．そのため，チェックリストおよび ADU で想定の問題を拡充すること，および解決策実行後，解決しなかった場合の端末およびネットワークのステータスを分析し，それに応じてその後の ADU 実行順序を動的に構築する仕組みを整えることが今後必要であると考えられる．

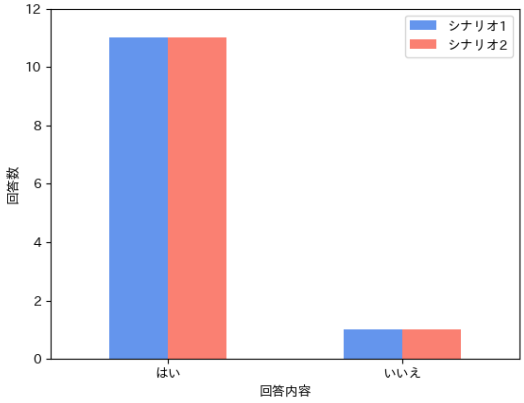


図 22: 質問 8 及び質問 17 の回答者数 (シナリオ別)

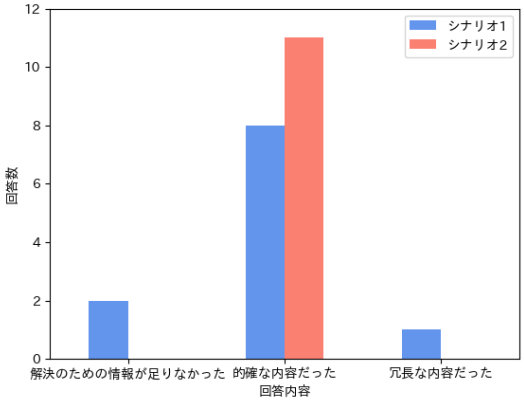


図 23: 質問 13 及び質問 22 の回答者数 (シナリオ別)

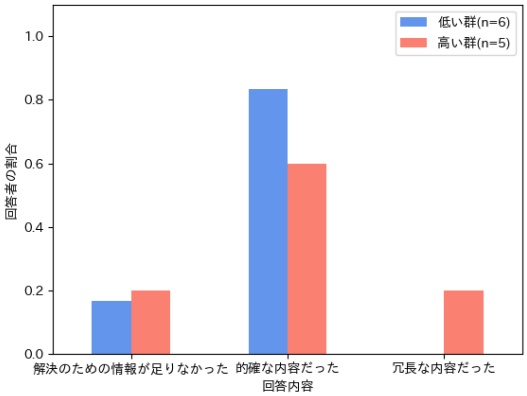


図 24: 質問 13 の回答者数 (知識レベル別)

解決策の的確性　次に，図 23 に示すのは，フィードバックされた解決策の的確性に対する評価である．このグラフは質問番号 13 及び 22 の回答結果に対応しており，横軸における項目が左から順に解決策中の情報に不足があった，的確な解決策の内容だった，冗長な内容だったとする回答に対する回答人数をそれぞれシナリオ別に示している[*23]．シナリオ②では回答した全員が適切と判断した一方，シナリオ①では判断が分かれた．理由を調べるため，図 24 にシナリオ①における知識レベル別の回答状況を分析したものを示す．この結果から，知識レベルによる明確な差はみられなかったが，原因としてはシナリオ②で提示された解決策が「パスワードを教員に確認してください」という単純な指示であったのに対し，シナリオ①の解決策は部屋の移動および無線 LAN アダプタの再起動という比較的複雑な操作を必要としたためであると想定される．実際，シナリオ①において「解決のための情報が足りなかった」と回答した被験者はその理由について，解決策が完了したかどうかを検証するフェーズがなかったため，解決策を取ったのちも同様の症状が発生してしまったと質問番号 14 で回答している．このケースでは，最終的に本人が iPad を利用して解決策が実行されたことを確認したため問題解決に至ったが，一般的には確認されることはなく，実際の運用ではシステムが問題特定できない可能性も想定される．一方，「冗長な内容だった」と回答している被験者から，「シナリオ①において解決策と

[*23] 質問内容の都合上，本質問項目は問題解決に至った被験者のみを対象にし，至らなかった被験者には回答しないよう指示した（未回答の扱いとした）．

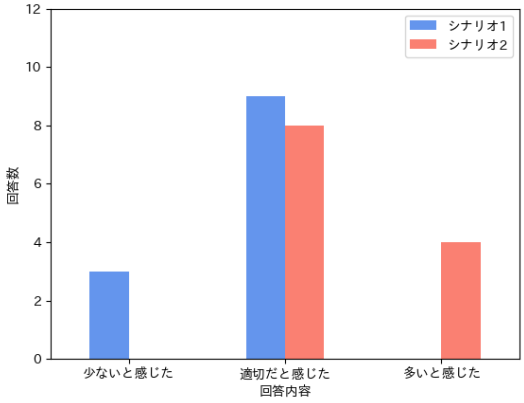


図 25: 質問 9 及び質問 18 の回答者数 (シナリオ別)

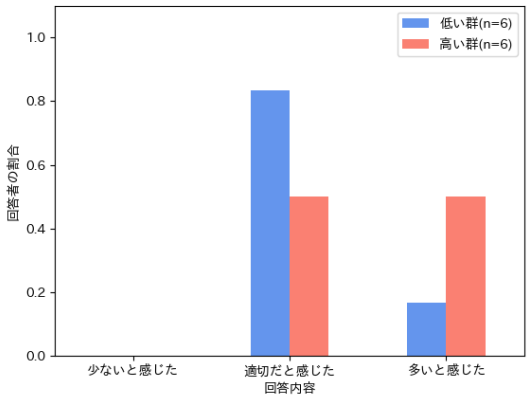


図 26: 質問 18 の回答者数割合 (知識レベル別)

して端末操作が冗長であるため」という回答理由を得た．これは ADU 実行時に利用者にフィードバックする解決策の操作内容が冗長であるということを示している．解決のための端末操作は利用者によっては大きく時間や労力を消費することが想定される．そのため，ADU に登録する解決策は利用者が確実に問題を解決できる最小限の端末操作となるようにする必要がある．

検証結果　以上の議論を踏まえ，本仮説に対する検証結果としては，問題解決に至った人数の割合の観点から考えるとおおむね満足していると言える．しかしながら，フィードバックされた解決策の的確性に関してはシナリオごとに評価が分かれる結果となった．原因としては主に解決策が正しく実行できているかを確認するフェーズが ADU になかったことが考えられ，ADU の実行フローの見直しが今後の課題である．

■ 仮説 2：システムが利用者に要求する操作手順の数は，冗長性がなくかつ不足がない．

端末の操作手順数に対する評価　図 25 に示すのは，チャットボットによる指示に基づく端末の操作手順数に対する評価とその回答数である．質問番号 9 及び 18 に対応する．シナリオ①に対しては全て適切だ (少ない含む) という回答である一方，シナリオ②に対しては多いと感じたと回答した人が一定数いた．この理由としては，シナリオ②は，シナリオ①で扱っていた問題を特定・解決するための動作があった点およびシナリオ②は AP パスフレーズが間違っていることを確認するため，利用端末を利用者が操作する必要があった点が考えられる．さらに，シナリオ②の回答に対して，無線 LAN の知識レベル別に回答者の割合を表したものを図 26 に示す．図によると，知識レベルの高い人が操作手順数が多いと回答する傾向にあり，低い人が操作手順数が少ないと回答する傾向にあった．この理由として知識レベルの高い人は，パスフレーズが間違っていることを特定するために，ADU が提示したものとは別にさらに手順数の少ない方法を知っている，あるいはそれを調べようとしていた可能性があることが考えられる．一方，知識レベルの低い群はパスフレーズの誤りであるという予想ができず，またパスフレーズ誤りのより良い確認方法も知らなかったため，操作手順について適切だと回答した割合が高いものと想定される．

検証結果　以上の議論を踏まえ，本仮説に対する検証結果としてはトラブルのシナリオによっては満足していると言えるものの，遭遇している症状の原因に対してある程度の予想ができている利用者にとっては，チャットボットによる端末操作指示の数が多いと感じる傾向があった．これを踏まえ，極力利用者の操作なしにネットワークシステムから取得できる情報をもとに診断を完結させる改善が必要である．

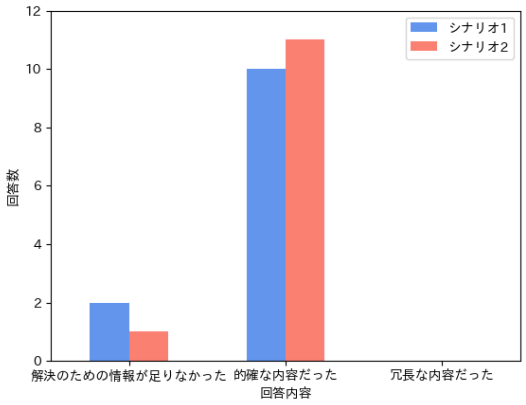


図 27: 質問 11 及び質問 20 の回答者数 (シナリオ別)

図 28: MAC アドレスの確認を促すチャットボットの指示

■ 仮説 3：システムからの端末操作指示および解決策の指示内容は的確なものである．

端末操作指示の的確性　図 27 に示すのは，チャットボットによる端末操作指示に対するシナリオごとの評価とその回答数である．質問番号 11 及び 20 に対応する．この結果，シナリオ①では 2 人，②では 1 人を除いて的確なものであると回答した．シナリオ①で「解決のための情報が足りなかった」と回答した 1 人はその後の記述欄において，システムに症状を入力する際に必要となる端末操作に対する説明が足りないと回答している．この問題に対しては，端末操作に不慣れな場合であっても，手順を踏んで端末を操作できるようにユーザーに対するインストラクションを検討することにより解決が可能であると考えている．一方，シナリオ②で「解決のための情報が足りなかった」と回答した 1 人はその後の記述欄において，MAC アドレスの調べ方がわからなかったと回答している．現状では広島大学情報メディア教育研究センターの関連ウェブページにハイパーリンクをタップさせることでアクセスさせ，記載の指示に従って操作をしてもらう形式をとっている (図 28)．改善点としては，チャットボットからシームレスに手順を踏んで操作してもらうことも検討する必要がある．解決策の的確性に関しては仮説 1 で示したとおり，的確な内容であったと判断するか否かは検出対象のトラブルによって変動する可能性がある．

検証結果　以上の議論を踏まえ，本仮説に対する検証結果としては，おおむねシステムからの端末操作指示および解決策の指示内容は的確なものであるといえる．ただし，一部の利用者はチャットボットの指示をすべて読み切れない場合があるため，チャットボット上でメッセージを少しずつ表示するといった表現方法の工夫が必要である．

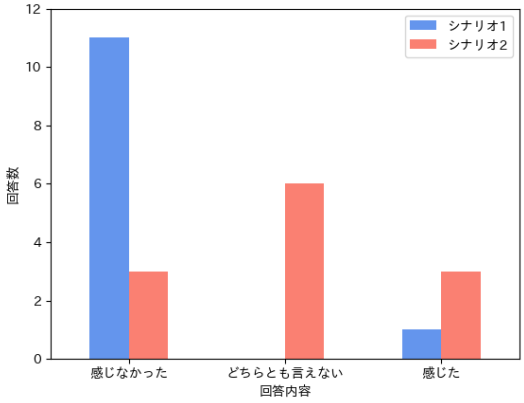


図 29: 質問 15 及び質問 24 の回答者数 (シナリオ別)

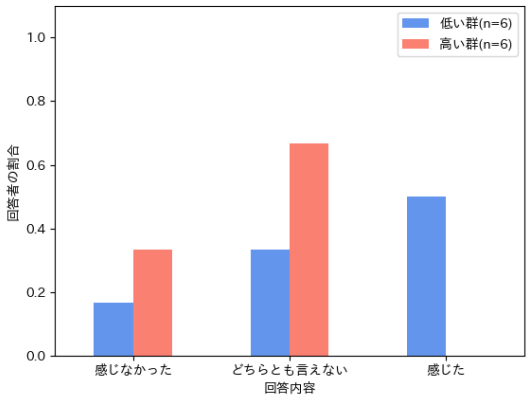


図 30: 質問 24 の回答者数割合 (知識レベル別)

■ 仮説 4：システムの診断は窓口に比べていずれの症状に対しても迅速に対処が可能である．

シナリオ別に分析した診断の迅速性　図 29 に示すのは，窓口で対応を受ける場合の方が問題解決が迅速に行えると感じたかという質問に対するシナリオごとの回答である．本質問に対しては，結果が発生させた問題によって変わり，シナリオ①では 1 人を除く回答者全員が Netdoctor による診断のほうが問題解決を迅速に行えると回答した一方，シナリオ②では窓口で対応を受ける場合の方が迅速に行えると回答した人の数が増加した．これは，シナリオ②においては，シナリオ①にて必要のなかった問題特定のための端末操作が必要だったためと考えられる．また，システムが診断を行う際，Rogue AP(シナリオ①) の問題を特定する ADU が先に実行されてしまい，かつそこで問題が発生していると判断されたため，アカウント情報の入力ミスが単独で発生しているというシチュエーションに比べて診断に必要とする時間の増加および余計な解決策をユーザーに提示してしまったことも理由の一つであると考えられる．なお，シナリオ①で「窓口のほうが迅速に問題解決が行えると感じた」と回答した一名はチャットボット及び端末の操作に慣れておらず，端末操作に補助が必要であり，かつ診断そのものに非常に時間がかかったことが原因であると考えられる．

シナリオ②について知識レベル別に分析した診断の迅速性　図 30 は，図 29 でシナリオ②における回答を知識レベル別に示したものである．知識レベルの低い群が「窓口の対応が迅速に行えると判断できる」と回答する傾向があった一方，知識レベルの高い群は「チャットボットがより迅速に対応を行える」と回答する傾向がみられる．この原因として，知識レベルの高い群が端末の無線 LAN 設定をスムースに行える点，並びに操作の必要性を理解したうえで端末操作を行えるため，迅速にチャットボットによる問題解決が行えると感じられたのだと想定される．無線 LAN に対する知識の浅い利用者に対するフィードバックや端末操作指示をより迅速に行えるようにするため，解決策のフィードバックの表現方式を改良する (文字のみではなく，動画やアニメーションを利用など) ことにより，改善ができるものと想定される．

検証結果　以上の議論を踏まえ，本仮説に対する検証結果に関しても，シナリオに依存する結果となった．特にシナリオ②に対する診断の迅速性が低いと評価した被験者が多い．そのため仮説 2 に対する検証結果で述べたものと同様，ユーザ利用端末側で発生する問題に対してはユーザ自身に端末操作させるのではなく，極力ネットワークログのみで診断を完結させることが対策として考えられる．

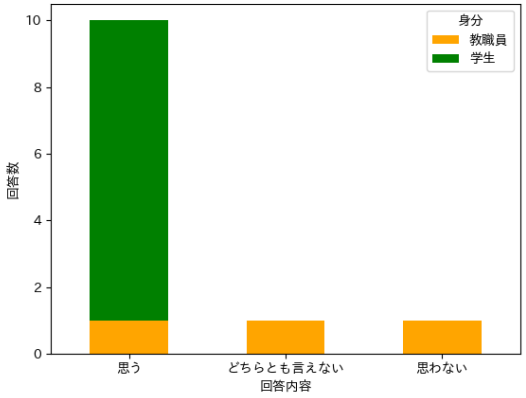


図 31: 質問 26 の回答者数 (身分別)

■ 仮説 5：利用者・管理者ともに，本システムを導入したいと考える．

システム利用願望の有無　図 31 は，システムが導入されたら利用したいか否かという質問に対する回答を身分 (学生または教職員) 別に示したものである．学生の身分を持つ被験者は全員が利用したいと回答した一方，教職員では 3 名中 1 名が利用したいと思わないと回答した．この理由として，導入後のメンテナンスの困難さおよび想定されたシナリオでは実際に発生する問題をカバーできていないことが自由記述により理由として挙げられていた．この点を踏まえ，今後実環境で運用するにあたっては，開発プロトタイプシステムの保守容易性の観点から仕組みを改善していくことが求められると考えられる．

検証結果　検証結果として，学生を含むネットワーク利用者にとっては導入した後の積極的な利用が想定される一方で，システム管理者側から見た保守容易性については検討が必要であることがいえる．

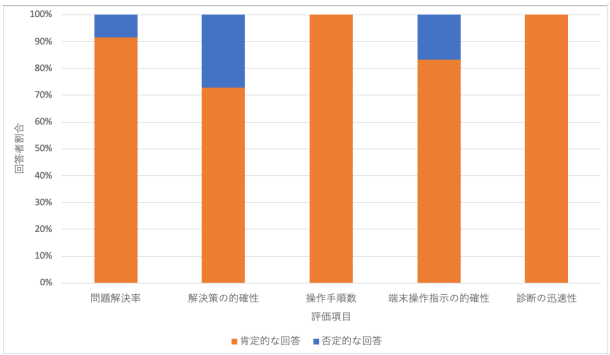


図 32: シナリオ①回答

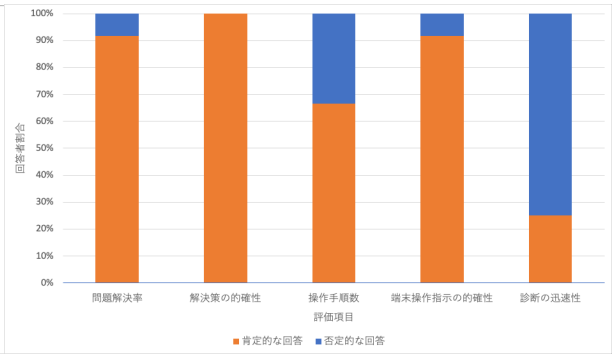


図 33: シナリオ②回答

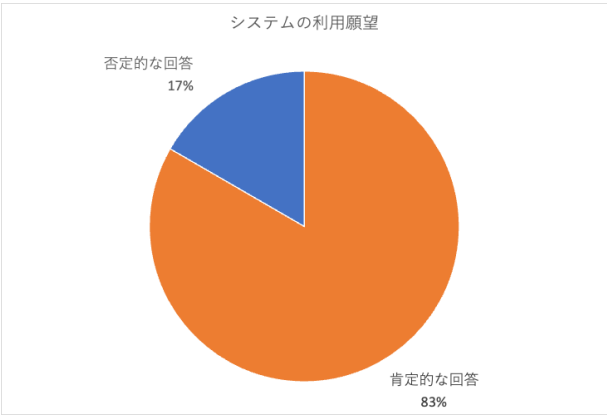


図 34: システムの利用願望

表 20: 各評価項目の質問番号と「肯定的な回答」に対応する回答内容

評価項目	**質問番号**	**肯定的な回答**
問題解決率	8, 17	はい
解決策の的確性	13, 22	的確な内容だった
操作手順数	9, 18	少ないと感じた・適切だと感じた
端末操作指示の的確性	11, 20	的確な内容だった
診断の迅速性	15, 24	感じなかった
システムの利用願望	26	思う

5.3.5 考察

図 32，33 は，シナリオ①，②それぞれで評価項目ごとに肯定的な回答と否定的な回答の割合[*24]をまとめたものである．問題解決率・端末操作指示の的確性はいずれも 80% 以上の高い水準を示した．これにより，システムは今回対象としたトラブルについて適切にユーザーを誘導し，問題解決に導くことができることが示された．

一方，解決策の的確性及び操作手順数の適切さについては，シナリオ間で若干の差が見られた．特に，解決策の的確性が低いシナリオ①に関しては，前節までの議論で，解決策が利用者側で正確に実行されたことを確認するステップを ADU に設けることで対策が可能であると考えられる．

また，シナリオ②では，診断の迅速性に対して否定的な評価が顕著に増加している．これはシナリオ②では利用者による端末操作手順の増加及び併発させていたシナリオ①に対する解決策の実施も行う必要があったためと推測できる．対策として，利用端末側で発生しているトラブルであっても，極力ネットワークログのみで診断を完結させる仕組みを整えることが必要であると考えられる．

最後に，図 34 は，システムの利用願望について回答割合をまとめたものである．前節での議論から，学生を中心に「システムが導入されれば利用したい」という回答を得た．システム管理者側から見たシステムの保守容易性には課題が残るものの，今回実験の対象とした広島大学においては，導入後のネットワーク利用者による積極的な利用が見込まれる．

[*24] 各評価項目で「肯定的な回答」に分類した回答内容は表 20 に示す通り．「否定的な回答」は「肯定的な回答」に分類されなかった回答内容．

第 6 章　まとめと今後の課題

本研究では，大規模な組織で導入されるネットワークシステムを対象に，トラブルに遭遇するネットワーク利用者に直接問題の原因を推定し，解決策まで提示するプロトタイプシステム Netdoctor の開発及び評価を行った．開発システムには，ネットワークで発生する可能性のある問題を列挙したチェックリストを用いて診断を行うチェックリスト型ネットワーク診断モデルを採用した．システム評価では，利用者に直接トラブル要因及び解決策をフィードバックする機能が開発システムの独自性であることを確認した．また，広島大学構成員を対象とした実験評価では想定したシナリオで一人を除く全ての被験者が迅速に問題解決に至ったことから，ネットワーク利用者を的確に問題解決に導けることが示された．以上から，本研究成果を用いることにより，受付時間外や休業期といったように，組織において IT 相談対応窓口での対応が困難な場合やネットワーク利用者自身が迅速な対応を必要とする場合でも，迅速なトラブル解決が可能となることが期待できる．

今後の課題としては，以下に挙げるものがある．これらの改善策を実施することで，さらに多様かつ的確なネットワーク診断，及び診断の迅速性の向上が行えることが期待される．

- 他ツールからのデータを診断に用いる仕組みづくり
- 診断時，ユーザーが解決策を正常に完了したかを確認する ADU 動作ステップの追加
- 利用端末側で発生しているトラブルをネットワークログから特定するための仕組みづくり

参考文献

[1] 近堂徹, 田島浩一, 岸場清悟, 岩田則和, 相原玲二. 自動構成機能を有する大規模キャンパスネットワーク管理システムの実装と評価. 情報処理学会論文誌, Vol. 57, No. 3, pp. 998–1007, mar 2016.

[2] 石原知洋, 四本裕子, 角野浩史, 玉造潤史, 中村遼, 小川剛史, 相田仁, 工藤知宏. 教室におけるオンライン講義受講のための無線接続環境評価. 情報処理学会論文誌デジタルプラクティス（TDP）, Vol. 3, No. 3, pp. 66–76, jul 2022.

[3] 浜元信州, 井田寿朗, 齋藤貴英, 小田切貴志, 綿貫明広, 横山重俊. 無線 lan 規格による端末同時接続性能差について. 情報処理学会研究報告 (Web), Vol. 2020, No. IOT-50, 2020.

[4] 北口善明, 金勇, 友石正彦. Oss を活用したキャンパスネットワークの構成管理システム. No. 16, jul 2022.

[5] 久長穣, 杉井学, 為末隆弘, 金山知余, 小河原加久冶. 山口大学におけるネットワーク運用支援システム. 学術情報処理研究, Vol. 15, No. 1, pp. 31–39, 2011.

[6] 石原知洋, 関谷勇司. 時系列 db を利用した無線基地局およびクライアント統計情報の継続的な収集と可視化. No. 5, aug 2021.

[7] 八切有市, 青木茂樹, 宮本貴朗. 全学無線 lan 利用状況の可視化. Vol. 2017, , sep 2017.

[8] 北口善明, 石原知洋, 高嶋健人ほか. センサデバイスを利用したネットワーク状態計測手法の評価. マルチメディア, 分散協調とモバイルシンポジウム 2017 論文集, Vol. 2017, pp. 1348–1353, 2017.

[9] 北口善明, 石原知洋, 高嶋健人, 田川真樹, 田中晋太朗. Raspberry pi を用いた無線ネットワーク状態評価手法の提案. No. 8, may 2014.

[10] 中野敦斗, 近堂徹, 相原玲二. 組織内無線 lan 品質情報収集システムの実装とデータベースの検討. 研究報告インターネットと運用技術 (IOT), Vol. 2022-IOT-58, No. 1, pp. 1–7, 7 2022. ISSN 2188-8787.

[11] 中野敦斗, 近堂徹, 相原玲二. 時系列データベースを用いたキャンパス無線 lan 品質情報の収集と分析. 電子情報通信学会技術研究報告; 信学技報, Vol. 121, No. 300, pp. 22–23, 2021.

[12] 京都工芸繊維大学情報科学センター. 無線 lan 接続サービスの使用状況. https://cis.kit.ac.jp/status/wifiusage/. (2023-09-06 アクセス).

[13] 神戸大学情報基盤センター. 無線 lan 混雑状況. https://www.istc.kobe-u.ac.jp/lan_about/. (2023-09-06 アクセス).

[14] 冨重秀樹, 井上純一, 畑瀬卓司, 和田数字郎, 林豊洋, 福田豊. 無線 lan 接続情報を利用した密集度表示システムとその改良. 学術情報処理研究, Vol. 25, No. 1, pp. 1–8, 2021.

[15] 福田豊, 佐藤彰洋, 中村豊, 和田数字郎. 九州工業大学における covid-19 影響下での利用動向に基づく全学無線 lan 整備. 九州工業大学情報基盤センター年報.

[16] 中村豊, 福田豊, 佐藤彰洋. 九州工業大学における全学セキュア・ネットワークの導入について. Technical Report 20, 2015.

[17] 近堂徹, 田島浩一, 岸場清悟, 岩田則和, 相原玲二. 自動構成機能を有する大規模キャンパスネットワーク管理システムの実装と評価. 情報処理学会論文誌, Vol. 57, No. 3, pp. 998–1007, mar 2016.

[18] Sihyung Lee, Kyriaki Levanti, and Hyong S. Kim. Network monitoring: Present and future. *Computer Networks*, Vol. 65, pp. 84–98, 2014.

[19] Dan Octavian Savu, Ali Al-Shabibi, Brian Martin, Rune Sjoen, Silvia Maria Batraneanu, and Stefan Stancu. Integrated system for performance monitoring of the atlas tdaq network. Vol. 331, p. 052031, dec 2011.

[20] 国立研究開発法人情報通信研究機構. トラフィックのリアルタイム可視化ツール”nir-

vana”. https://www.nict.go.jp/out-promotion/other/case-studies/itenweb/nirvana.html. (2022-12-11 アクセス).

[21] 福田豊, 中村豊, 佐藤彰洋, 和田数字郎. 九州工業大学全学ネットワークの更新に向けた無線 lan 利用動向調査. デジタルプラクティス, Vol. 11, No. 3, pp. 636–656, jul 2020.

[22] 山崎國弘, 永田正樹, 長谷川孝博, 磯部千裕. 無線 ap の端末接続情報を使用した教室無線 lan の接続不安定事象の検出と周辺無線 ap との電波干渉の発生把握手法の検討.

[23] Ieee standard for local and metropolitan area networks–port-based network access control. *IEEE Std 802.1X-2020 (Revision of IEEE Std 802.1X-2010 Incorporating IEEE Std 802.1Xbx-2014 and IEEE Std 802.1Xck-2018)*, pp. 1–289, 2020.

[24] 守倉正博, 久保田周治. 802.11 高速無線 LAN 教科書. インプレス R&D, 2004.

[25] 梅原大祐. Ieee802.11a の mac フレーム構成. http://www.ice.is.kit.ac.jp/~umehara/misc/study/doc/20100211_11a-mac-frame.pdf. (2022-10 アクセス).

[26] Toyozi Masuda. ”ネットワーク技術用語集【ＢＳＳ】”. https://lantech.up.seesaa.net/subpage/nw_lan_bss.html. (2024-01-16 アクセス).

[27] M. Heusse, F. Rousseau, G. Berger-Sabbatel, and A. Duda. Performance anomaly of 802.11b. In *IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No.03CH37428)*, Vol. 2, pp. 836–843 vol.2, 2003.

[28] Fash Safdari and Anatoliy Gorbenko. Experimental evaluation of performance anomaly in mixed data rate ieee802.11ac wireless networks. In *2019 10th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, pp. 82–87, 2019.

[29] 福田豊, 畑瀬卓司, 佐藤彰洋, 中村豊, 和田数字郎. 実機を用いた ieee 802.11ax の基本性能評価. No. 19, may 2021.

[30] 広島大学情報メディア教育研究センター. ”hinet の概要”. https://www.media.hiroshima-u.ac.jp/services/hinet/about-hinet/. (2021-12-13 アクセス).

[31] 近堂徹, 渡邉英伸, 田島浩一, 西村浩二, 相原玲二. 広島大学キャンパスネットワークにおける端末管理とネットワーク利用制御手法の導入. Vol. 2021, pp. 75–76, nov 2021.

[32] 広島大学. ”ノートパソコンの必携化について”. https://www.hiroshima-u.ac.jp/about/initiatives/jyoho_ka/hikkei_pc. (2024-01-16 アクセス).

[33] 中野敦斗, 近堂徹. Netdoctor: 組織内無線 lan におけるネットワークログを用いた対話型自己診断システムの開発. インターネットと運用技術シンポジウム論文集, Vol. 2023, pp. 107–108, 11 2023.

[34] Michael Kerrisk. Tc(8) - linux manual page. https://man7.org/linux/man-pages/man8/tc.8.html. (2024-01-18 アクセス).

[35] Ieee standard for local and metropolitan area networks–port-based network access control. *IEEE Std 802.1X-2020 (Revision of IEEE Std 802.1X-2010 Incorporating IEEE Std 802.1Xbx-2014 and IEEE Std 802.1Xck-2018)*, pp. 1–289, 2020.

研究業績

- 中野 敦斗, 近堂 徹, 相原 玲二：”組織内無線 LAN 品質情報収集システムの実装とデータベースの検討”, 研究報告インターネットと運用技術（IOT），2022-IOT-58，1，pp.1-7，ISSN 2188-8787，2022-07-05.
- 中野 敦斗，近堂 徹，相原 玲二：”時系列データベースを用いたキャンパス無線 LAN 品質情報の収集と分析”，信学技報, vol. 121, no. 300, IA2021-32, pp. 22-23, 2021 年 12 月.
- Atsuto Nakano, Tohru Kondo, Reiji Aibara. ”Development of a Wireless LAN Quality Management System with Time-Series Metrics for Improving Wireless LAN Usability”, The 17th Asian Internet Engineering Conference(Poster Session), 2022-Dec-19 to 2022-Dec-21, https://interlab.ait.ac.th/aintec2022/.
- 中野 敦斗, 近堂 徹. ”Netdoctor: 組織内無線 LAN におけるネットワークログを用いた対話型自己診断システムの開発”. インターネットと運用技術シンポジウム論文集. 2023 Nov 30;2023:107-8.

謝辞

本研究を進めるにあたり，広島大学情報メディア教育研究センター 近堂徹教授には指導教官として終始熱心で適切なご指導をいただくとともに，本論文の作成にあたり多大なご支援をいただきました．ここに深謝の意を示します．また，副指導教官としてミーティング及び論文執筆等にて終始適切なご助言をいただいた広島大学情報メディア教育研究センター 渡邊英伸准教授，論文執筆等で適切なご助言をいただいた広島大学大学院先進理工系科学研究科 北須賀輝明准教授に感謝申し上げます．広島大学情報メディア教育研究センター 西村浩二教授には研究室ミーティングの際に活発な議論・ご助言をいただきました．厚くお礼申し上げます．広島大学情報メディア教育研究センター 田島浩一助教，岸場清悟助教，村上祐子助教，下地寛武特任助教，広島大学財務・総務室 相原玲二上席特任学術研究員には数多くのご指導やご助言を頂きました．心から感謝申し上げます．本研究の進行にあたり，快く実験に参加していただいた皆様に感謝申し上げます．最後に，本研究を進めるにあたり日頃多大なご助言，ご協力をいただいた研究室の皆様には，ここに誠意の意を表します．

Appendices

チェックリスト

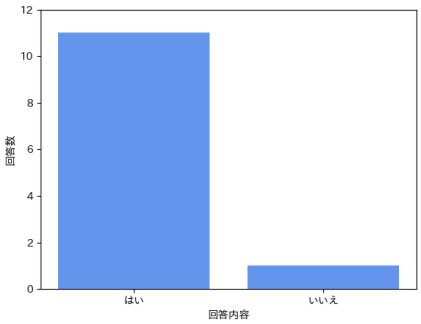
No.	発生区間	症状	要因	ユーザの対処	ユーザーが提供する情報	システムがネットワーク機器から取得する情報
1-1	端末	■WiFi に繋がらない □繋がるが遅い □一部のアプリが繋がらない □一部のページで繋がらない □繋がるが途切れる	端末ネットワークインターフェースの無効化	□認証情報の修正 □部屋の移動(接続先 AP の変更) □端末 WLAN の再接続 □席の移動 □対処の必要なし ■端末の設定修正(端末 WLAN の ON/PC の再起動) □ネットワーク管理者への報告	・(ユーザ)ネットワークインタフェースの UP/DOWN 確認	—
1-2		■WiFi に繋がらない ■繋がるが遅い □一部のアプリが繋がらない □一部のページで繋がらない □繋がるが途切れる	リソースの枯渇	□認証情報の修正 □部屋の移動(接続先 AP の変更) □端末 WLAN の再接続 □席の移動 □対処の必要なし ■端末の設定修正(端末の再起動) □ネットワーク管理者への報告	・(ユーザ)CPU 負荷の確認	—
1-3		■WiFi に繋がらない □繋がるが遅い □一部のアプリが繋がらない □一部のページで繋がらない ■繋がるが途切れる	古いドライバを使用	□認証情報の修正 □部屋の移動(接続先 AP の変更) □端末 WLAN の再接続 □席の移動 □対処の必要なし ■端末の設定修正(端末デバイスドライバーの再インストール) □ネットワーク管理者への報告	・(ユーザ)ドライバのバージョンを確認	—
1-4		■WiFi に繋がらない □繋がるが遅い □一部のアプリが繋がらない ■一部のページで繋がらない ■繋がるが途切れる	MTU 設定の不整合/断片化異常	□認証情報の修正 □部屋の移動(接続先 AP の変更) □端末 WLAN の再接続 □席の移動 □対処の必要なし ■端末の設定修正(端末 MTU の再設定) □ネットワーク管理者への報告	・(ユーザ)OS の MTU 設定を確認	—

No.	発生区間	症状	要因	ユーザの対処	ユーザーが提供する情報	システムがネットワーク機器から 取得する情報
1-5	端末	□WiFi に繋がらない □繋がるが遅い ■一部のアプリが繋がらない □一部のページで繋がらない □繋がるが途切れる	誤ったフィルタリング =不適切なファイアウォール設定	□認証情報の修正 □部屋の移動(接続先 AP の変更) □端末 WLAN の再接続 □席の移動 □対処の必要なし ■端末の設定修正(端末ファイアウォール設定の修正) □ネットワーク管理者への報告	・(ユーザ)ファイアウォール設定の確認	—
2-1	AP↔ 端末	■WiFi に繋がらない □繋がるが遅い □一部のアプリが繋がらない □一部のページで繋がらない □繋がるが途切れる	ユーザーが入力した認証情報の誤り	■認証情報の修正 □部屋の移動(接続先 AP の変更) □端末 WLAN の再接続 □席の移動 □対処の必要なし □端末の設定修正 □ネットワーク管理者への報告	・(ユーザ)入力した認証情報の誤りを確認	—
2-2		■WiFi に繋がらない ■繋がるが遅い □一部のアプリが繋がらない □一部のページで繋がらない □繋がるが途切れる	Rogue AP(テザリング機能などによる不正 AP)の 同一チャネル干渉	□認証情報の修正 ■部屋の移動(接続先 AP の変更) □端末 WLAN の再接続 □席の移動 □対処の必要なし □端末の設定修正 □ネットワーク管理者への報告	—	・(WLC)接続先 AP のノイズ比増大していること かつ (WLC)接続先 AP で RogueAP を検出していること
2-3			外部干渉源(電子レンジなど)による電波干渉		—	・(WLC)接続先 AP のノイズ比増大していること かつ (WLC)接続先 AP で RogueAP を検出していないこと
2-4			一つの AP に対する接続端末の増加		—	・(WLC)接続先 AP の接続端末数増大していること
2-5		□WiFi に繋がらない ■繋がるが遅い □一部のアプリが繋がらない □一部のページで繋がらない □繋がるが途切れる	AP ローミング下で端末が電波強度の比較的小さい AP とのアソシエーションを維持	□認証情報の修正 □部屋の移動(接続先 AP の変更) ■端末 WLAN の再接続 □席の移動 □対処の必要なし □端末の設定修正 □ネットワーク管理者への報告	・(ユーザ)端末側でより RSSI の大きい AP を検出できるか？	—
2-6			データレートが極端に低い端末の存在	□認証情報の修正 ■部屋の移動(接続先 AP の変更) □端末 WLAN の再接続 □席の移動 □対処の必要なし □端末の設定修正 □ネットワーク管理者への報告	—	・(WLC)接続先 AP に低データレート端末があること
2-7	AP↔ 端末	□WiFi に繋がらない □繋がるが遅い □一部のアプリが繋がらない □一部のページで繋がらない ■繋がるが途切れる	AP ローミング下で頻繁に AP との再アソシエーションが発生	□認証情報の修正 □部屋の移動(接続先 AP の変更) □端末 WLAN の再接続 ■席の移動 □対処の必要なし □端末の設定修正 □ネットワーク管理者への報告	—	・(WLC)ターゲット端末が複数 AP 間で頻繁に入れ替わり接続していること

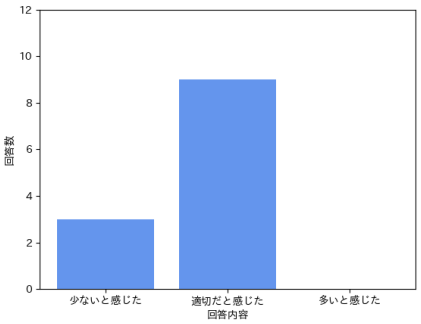
No.	発生区間	症状	要因	ユーザの対処	ユーザーが提供する情報	システムがネットワーク機器から 取得する情報
2-8	AP↔ 端末	□WiFi に繋がらない □繋がるが遅い □一部のアプリが繋がらない □一部のページで繋がらない ■繋がるが途切れる	バンドステアリング機能による接続断	□認証情報の修正 □部屋の移動(接続先 AP の変更) □端末 WLAN の再接続 □席の移動 ■対処の必要なし □端末の設定修正 □ネットワーク管理者への報告	—	・(WLC)ターゲット端末が接続している AP でバンドステアリングが発生していること
3-1	AP	■WiFi に繋がらない ■繋がるが遅い □一部のアプリが繋がらない □一部のページで繋がらない □繋がるが途切れる	ハードウェアの故障	□認証情報の修正 ■部屋の移動(接続先 AP の変更) □端末 WLAN の再接続 □席の移動 □対処の必要なし □端末の設定修正 □ネットワーク管理者への報告	—	・(WLC)接続先 AP がダウンしていること
3-2		■WiFi に繋がらない □繋がるが遅い □一部のアプリが繋がらない □一部のページで繋がらない ■繋がるが途切れる	DFS(Dynamic Frequency Selection)による接続中断	□認証情報の修正 ■部屋の移動(接続先 AP の変更) □端末 WLAN の再接続 □席の移動 □対処の必要なし □端末の設定修正 □ネットワーク管理者への報告	—	・(WLC)接続先 AP で DFS が発生していること
3-3		■WiFi に繋がらない □繋がるが遅い □一部のアプリが繋がらない □一部のページで繋がらない □繋がるが途切れる	AP ソフトウェアの不具合		—	・(WLC)接続先 AP がダウンしていること
3-4		□WiFi に繋がらない ■繋がるが遅い □一部のアプリが繋がらない □一部のページで繋がらない □繋がるが途切れる	認証時に用いるキーの頻繁な更新による過負荷		—	・(WLC)接続先 AP の CPU 負荷
3-5		□WiFi に繋がらない ■繋がるが遅い □一部のアプリが繋がらない □一部のページで繋がらない ■繋がるが途切れる	頻繁な RRM(Radio Resource Management)による接続断		—	・(WLC)接続先 AP で RRM 発生しているか？
4-1	AP↔ WLC	■WiFi に繋がらない ■繋がるが遅い □一部のアプリが繋がらない □一部のページで繋がらない ■繋がるが途切れる	ネットワーク輻輳	□認証情報の修正 ■部屋の移動(接続先 AP の変更) □端末 WLAN の再接続 □席の移動 □対処の必要なし □端末の設定修正 □ネットワーク管理者への報告	—	・(NW 機器)AP↔WLC 間でネットワーク輻輳の発生を確認
4-2			PoE 電力不足による AP ダウン		—	・(WLC)接続先 AP の死活監視
5-1	WLC		WLC の過負荷		—	・(WLC)WLC サーバのリソース
5-2			AP の制御設定ミス		—	—
6-1	ユーザー	□WiFi に繋がらない ■繋がるが遅い □一部のアプリが繋がらない □一部のページで繋がらない □繋がるが途切れる	ユーザーの勘違い	□認証情報の修正 □部屋の移動(接続先 AP の変更) □端末 WLAN の再接続 □席の移動 ■対処の必要なし □端末の設定修正 □ネットワーク管理者への報告	・他のいずれの問題に該当しない　かつ　他端末(定点観測)と実効スループットが同じことを確認	

実験結果

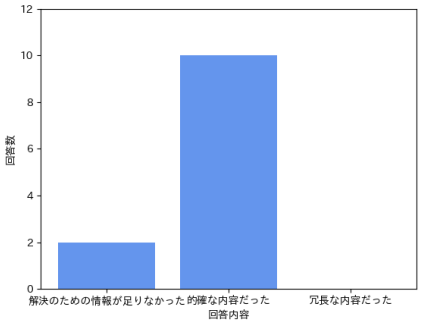
質問ごとの回答数



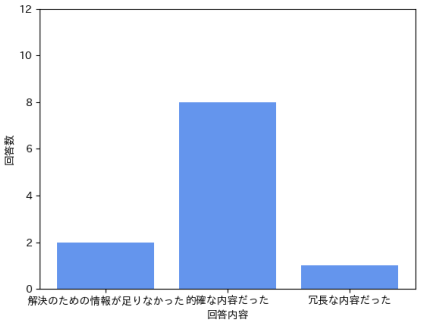
(a) 質問 8



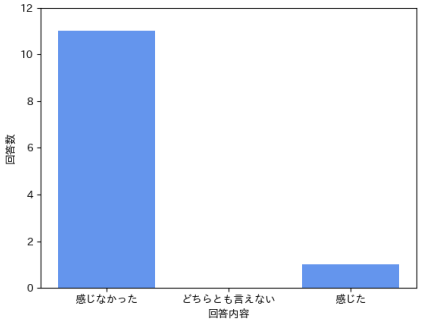
(b) 質問 9



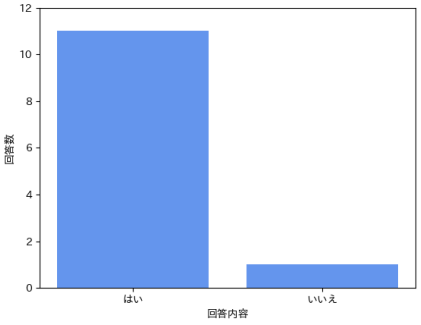
(c) 質問 11



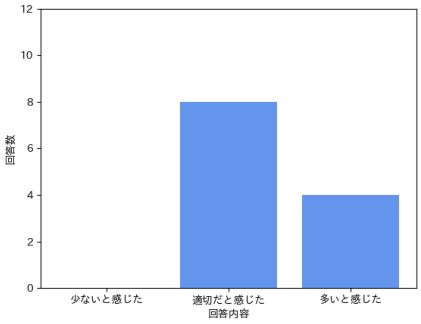
(d) 質問 13



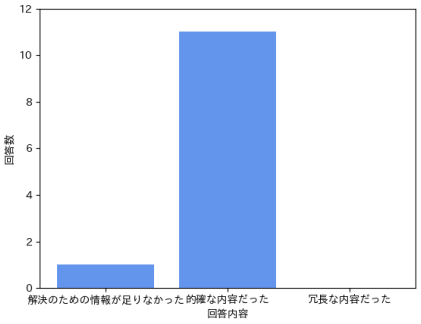
(e) 質問 15



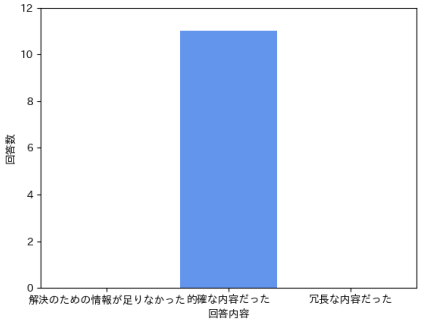
(f) 質問 17



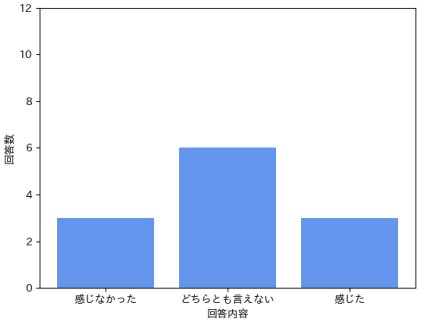
(g) 質問 18



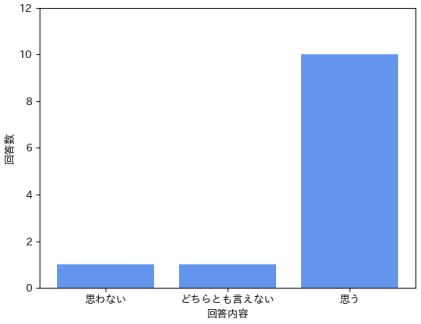
(h) 質問 20



(i) 質問 22

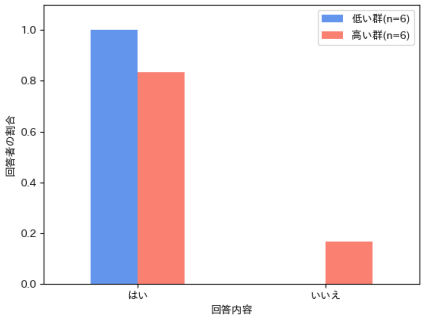


(j) 質問 24

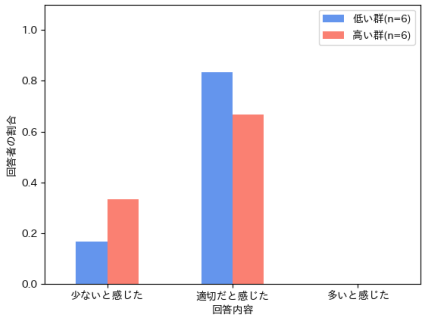


(k) 質問 26

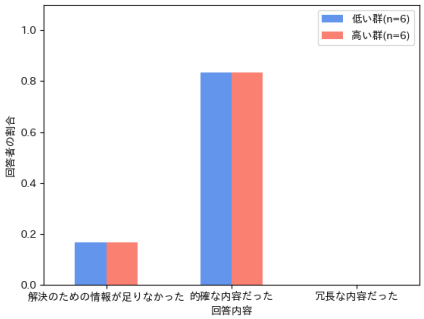
知識レベルごとの回答数割合



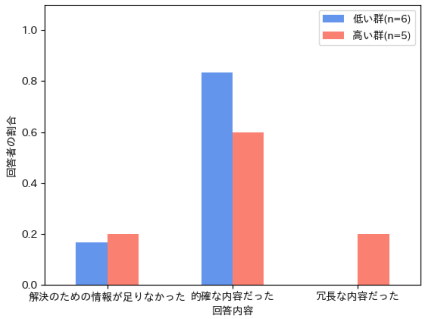
(l) 質問 8



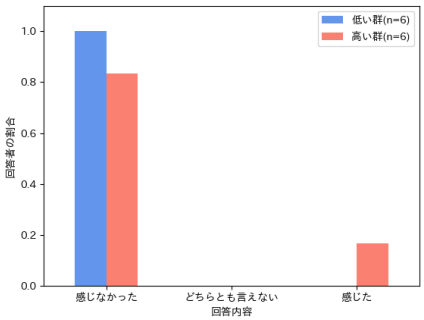
(m) 質問 9



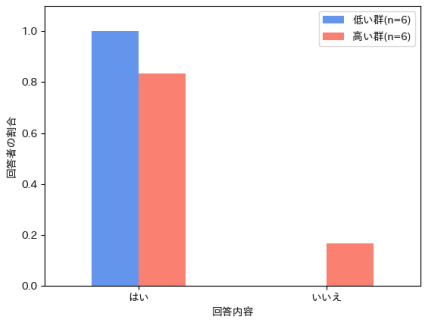
(n) 質問 11



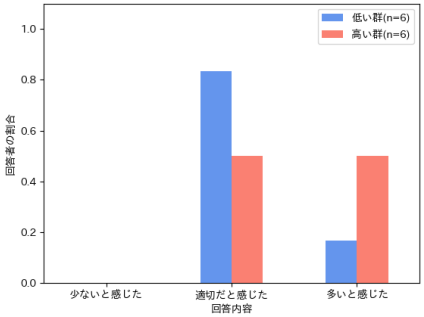
(o) 質問 13



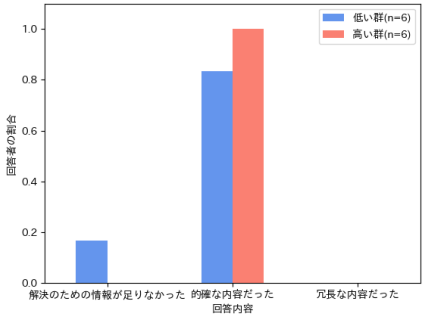
(p) 質問 15



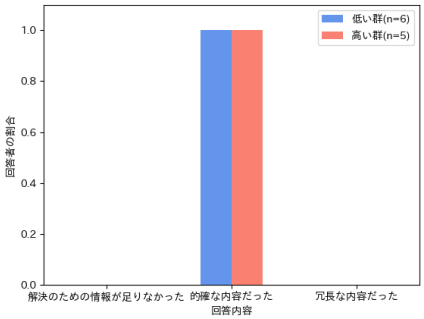
(q) 質問 17



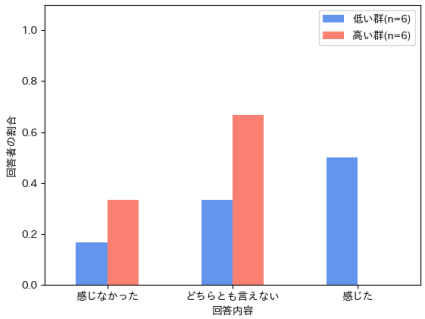
(r) 質問 18



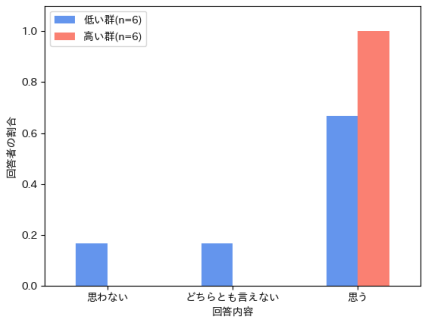
(s) 質問 20



(t) 質問 22



(u) 質問 24



(v) 質問 26

ADU データフロー (Netdoctor)

現段階ではチェックリスト中の問題の一部のみに対して ADU データフローが設計されている．以下には，現時点で設計が完了しているものの全てを示す．

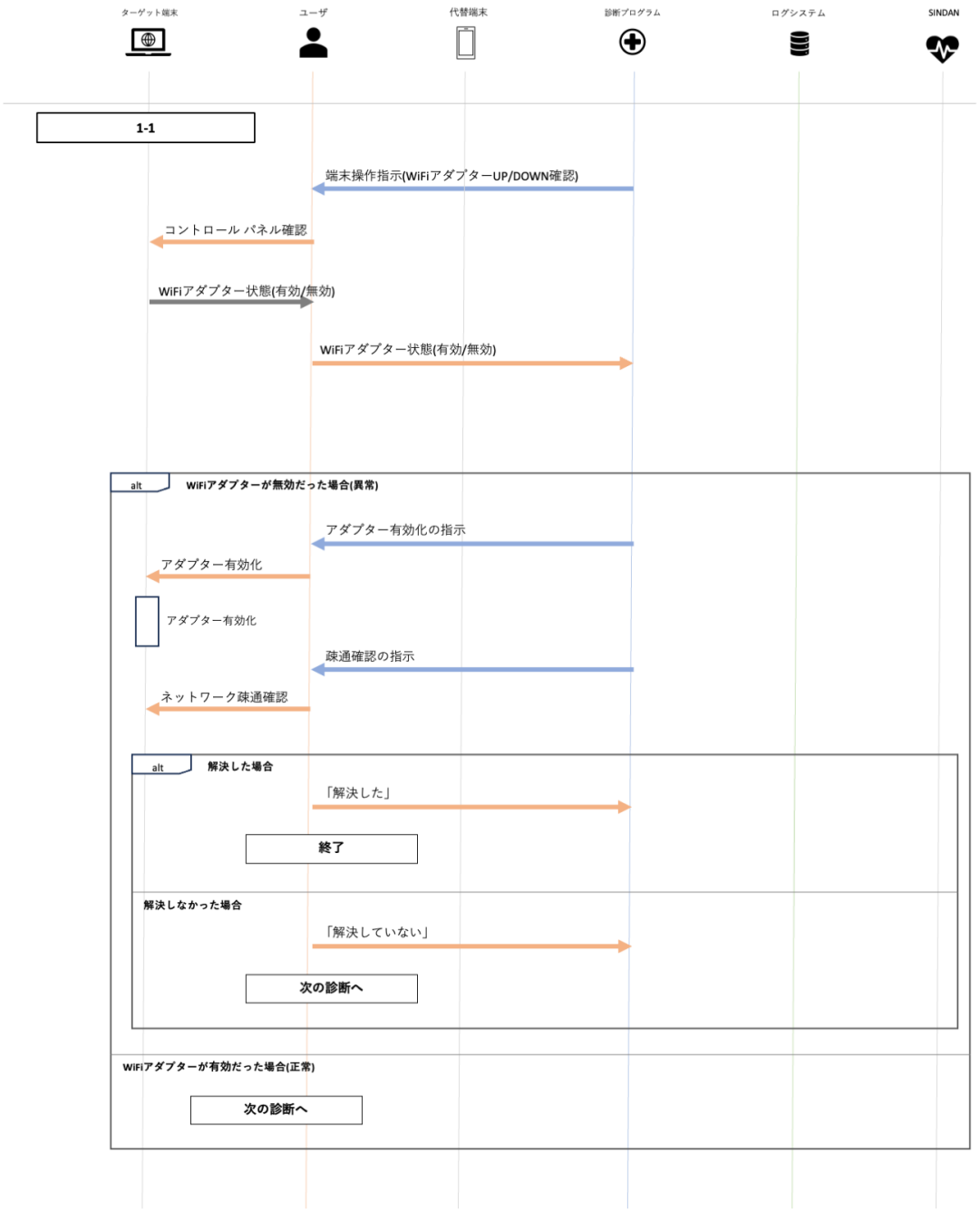


図 35: ADU1-1

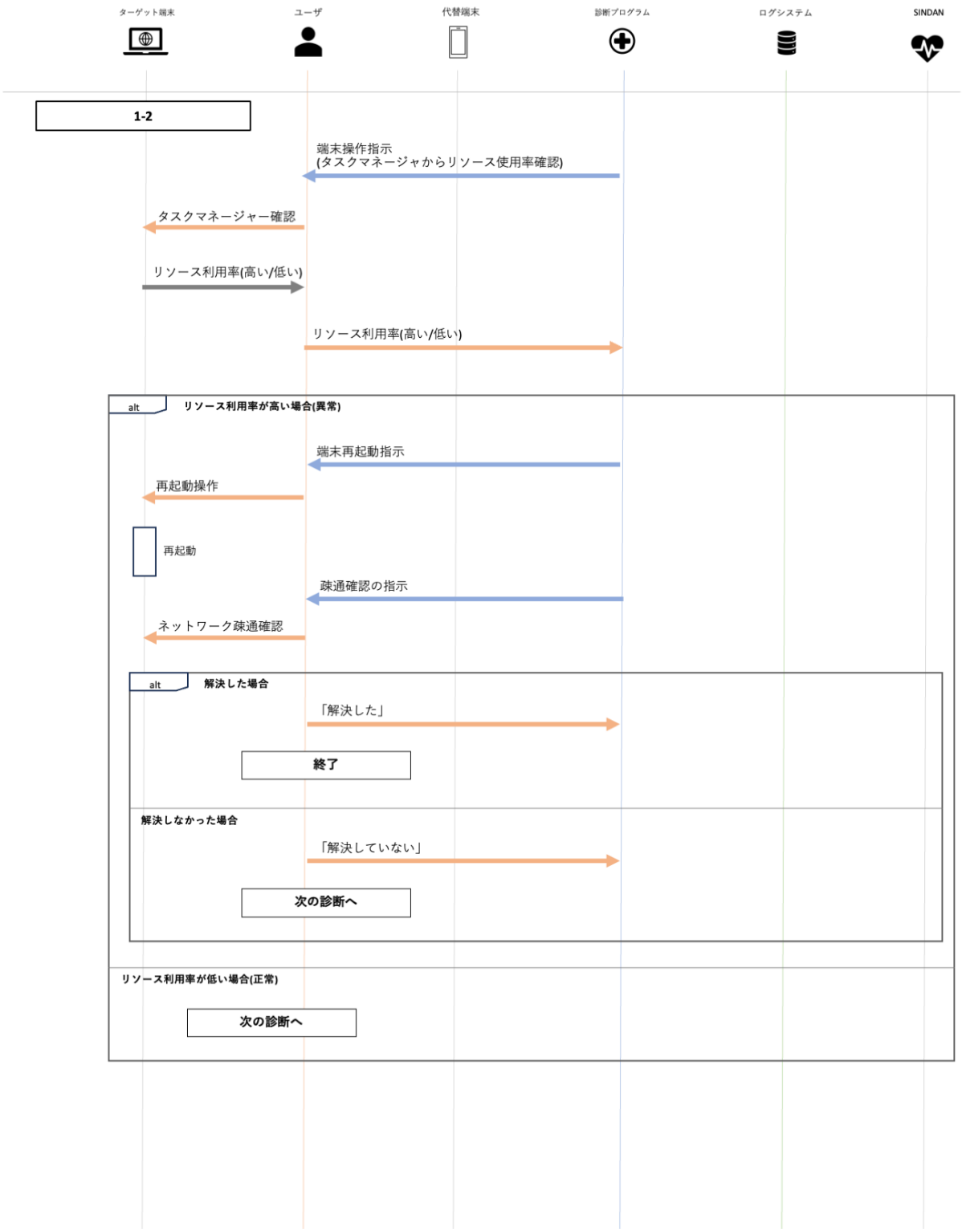

ターゲット端末
ユーザ
代替端末
診断プログラム
ログシステム
SINDAN
1-2
端末操作指示
(タスクマネージャからリソース使用率確認)
タスクマネージャー確認
リソース利用率(高い/低い)
リソース利用率(高い/低い)
alt
リソース利用率が高い場合(異常)
端末再起動指示
再起動操作
再起動
疎通確認の指示
ネットワーク疎通確認
alt
解決した場合
「解決した」
終了
解決しなかった場合
「解決していない」
次の診断へ
リソース利用率が低い場合(正常)
次の診断へ

図 36: ADU1-2

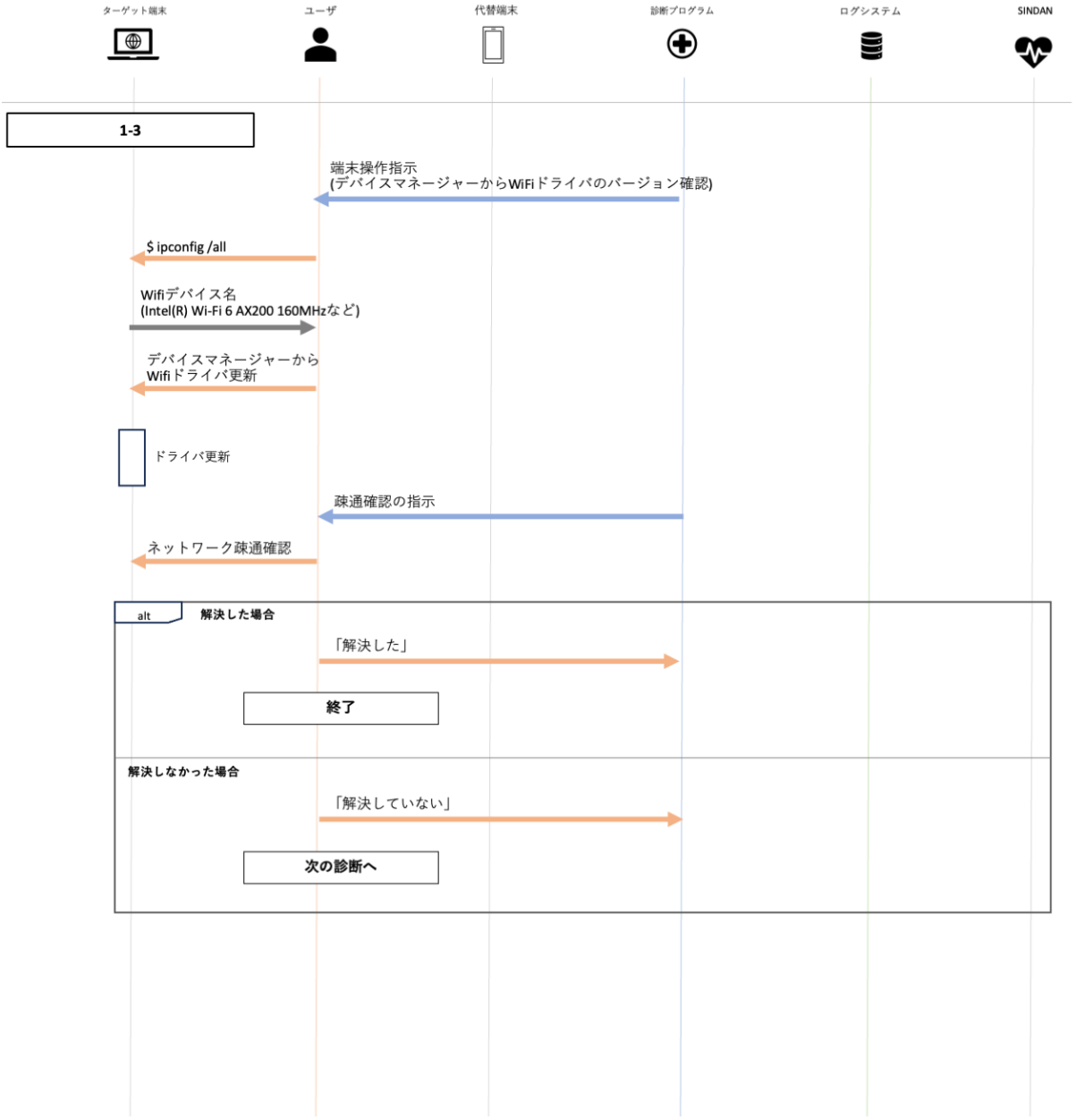

ターゲット端末
ユーザ
代替端末
診断プログラム
ログシステム
SINDAN
1-3
端末操作指示
(デバイスマネージャーからWiFiドライバのバージョン確認)
$ ipconfig /all
Wifiデバイス名
(Intel(R) Wi-Fi 6 AX200 160MHzなど)
デバイスマネージャーから
Wifiドライバ更新
ドライバ更新
疎通確認の指示
ネットワーク疎通確認
alt
解決した場合
「解決した」
終了
解決しなかった場合
「解決していない」
次の診断へ

図 37: ADU1-3

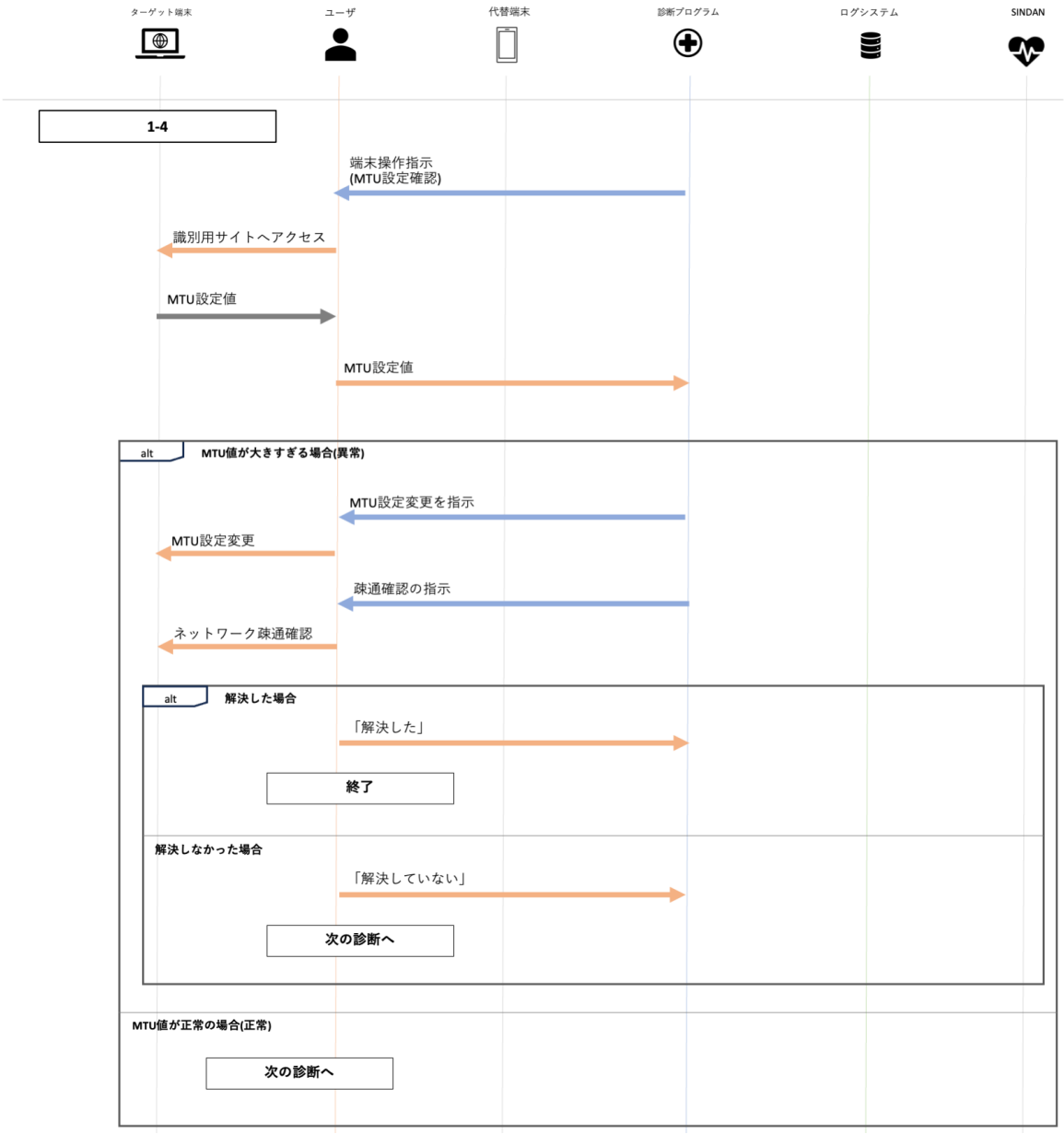

ターゲット端末
ユーザ
代替端末
診断プログラム
ログシステム
SINDAN
1-4
端末操作指示
(MTU設定確認)
識別用サイトへアクセス
MTU設定値
MTU設定値
alt
MTU値が大きすぎる場合(異常)
MTU設定変更を指示
MTU設定変更
疎通確認の指示
ネットワーク疎通確認
alt
解決した場合
「解決した」
終了
解決しなかった場合
「解決していない」
次の診断へ
MTU値が正常の場合(正常)
次の診断へ

図 38: ADU1-4

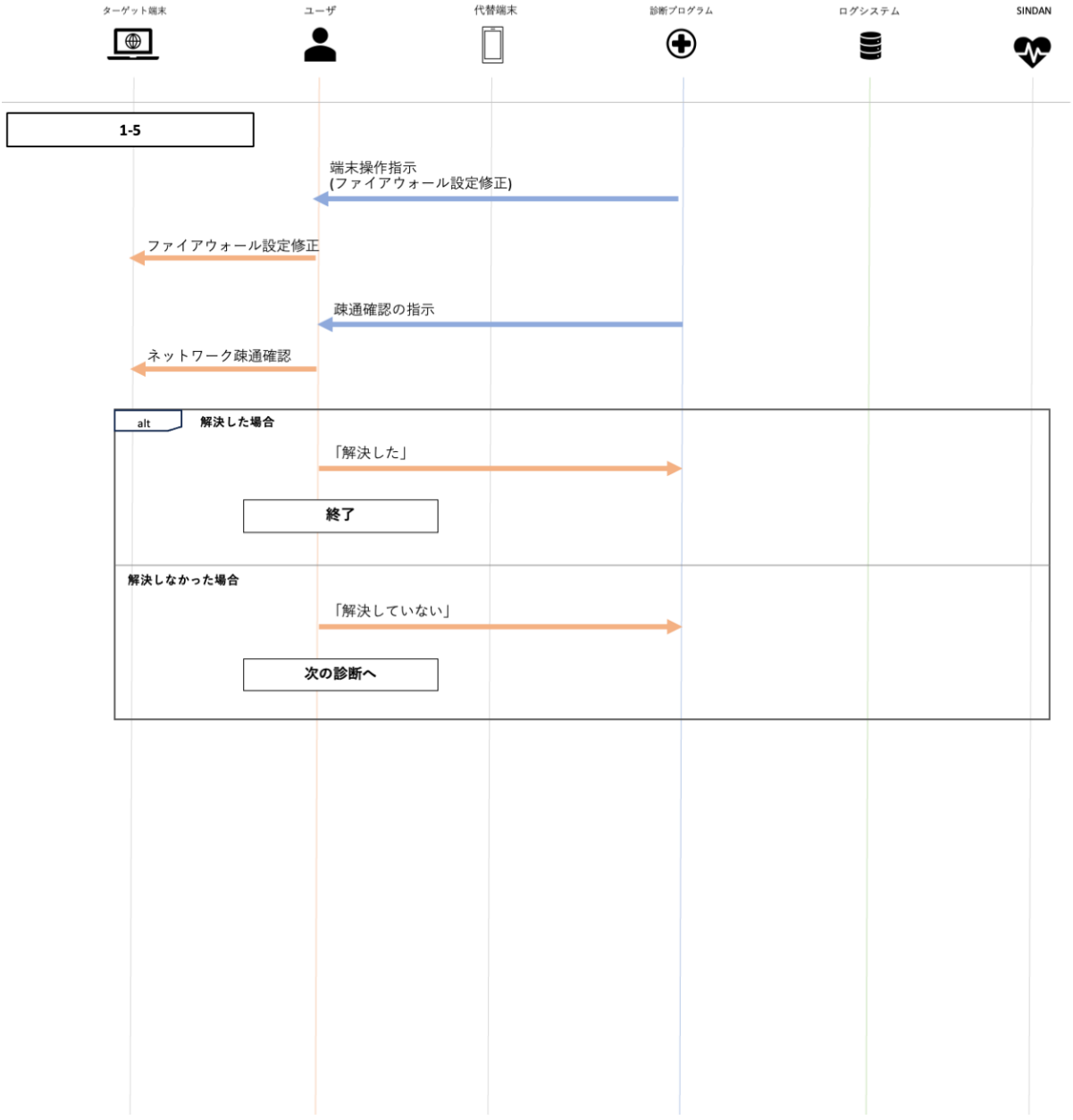

ターゲット端末
ユーザ
代替端末
診断プログラム
ログシステム
SINDAN
1-5
端末操作指示
(ファイアウォール設定修正)
ファイアウォール設定修正
疎通確認の指示
ネットワーク疎通確認
alt
解決した場合
「解決した」
終了
解決しなかった場合
「解決していない」
次の診断へ

図 39: ADU1-5

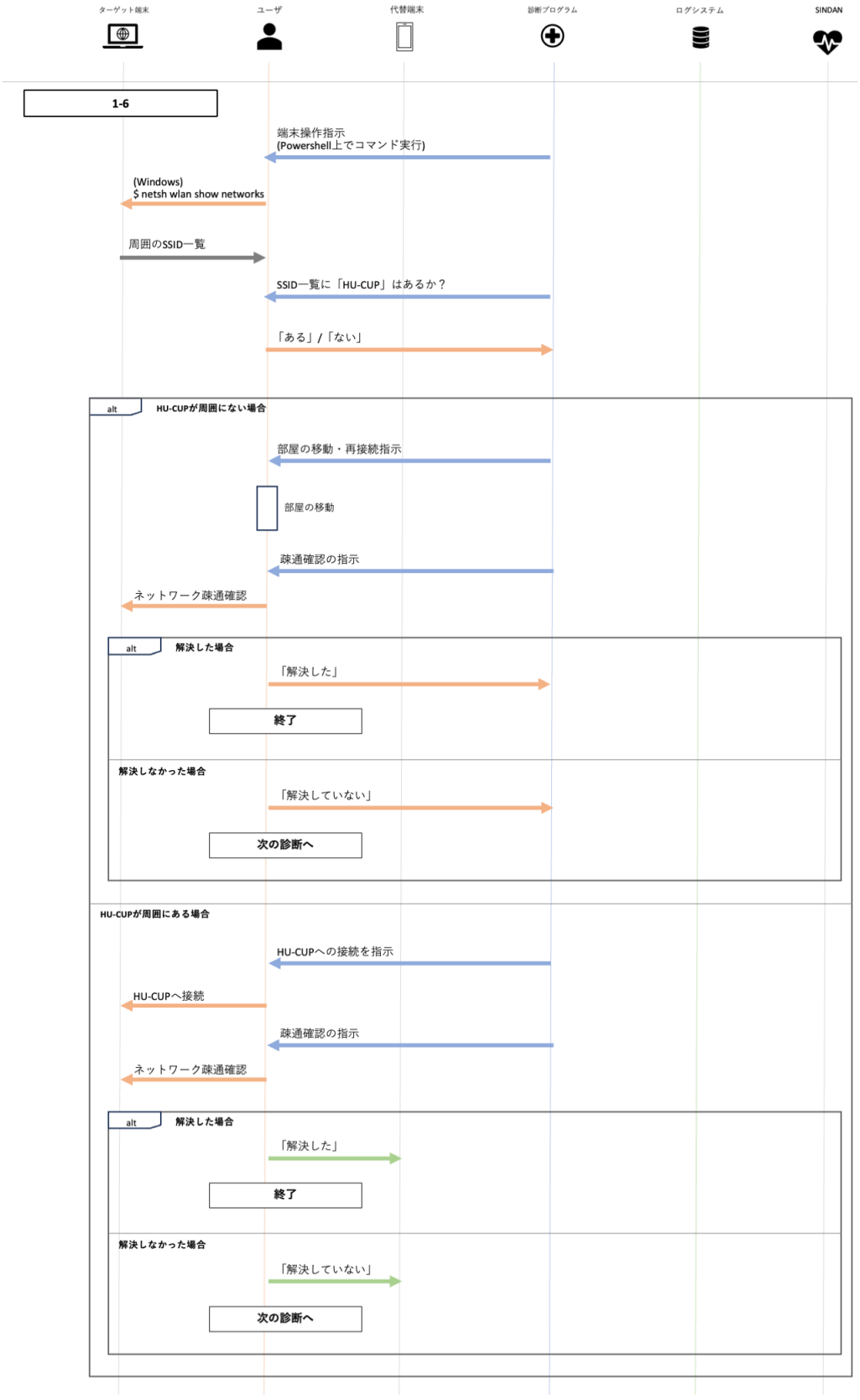

ターゲット端末
ユーザ
代替端末
診断プログラム
ログシステム
SINDAN
1-6
端末操作指示
(Powershell上でコマンド実行)
(Windows)
$ netsh wlan show networks
周囲のSSID一覧
SSID一覧に「HU-CUP」はあるか？
「ある」/「ない」
alt
HU-CUPが周囲にない場合
部屋の移動・再接続指示
部屋の移動
疎通確認の指示
ネットワーク疎通確認
alt
解決した場合
「解決した」
終了
解決しなかった場合
「解決していない」
次の診断へ
HU-CUPが周囲にある場合
HU-CUPへの接続を指示
HU-CUPへ接続
疎通確認の指示
ネットワーク疎通確認
alt
解決した場合
「解決した」
終了
解決しなかった場合
「解決していない」
次の診断へ

図 40: ADU1-6

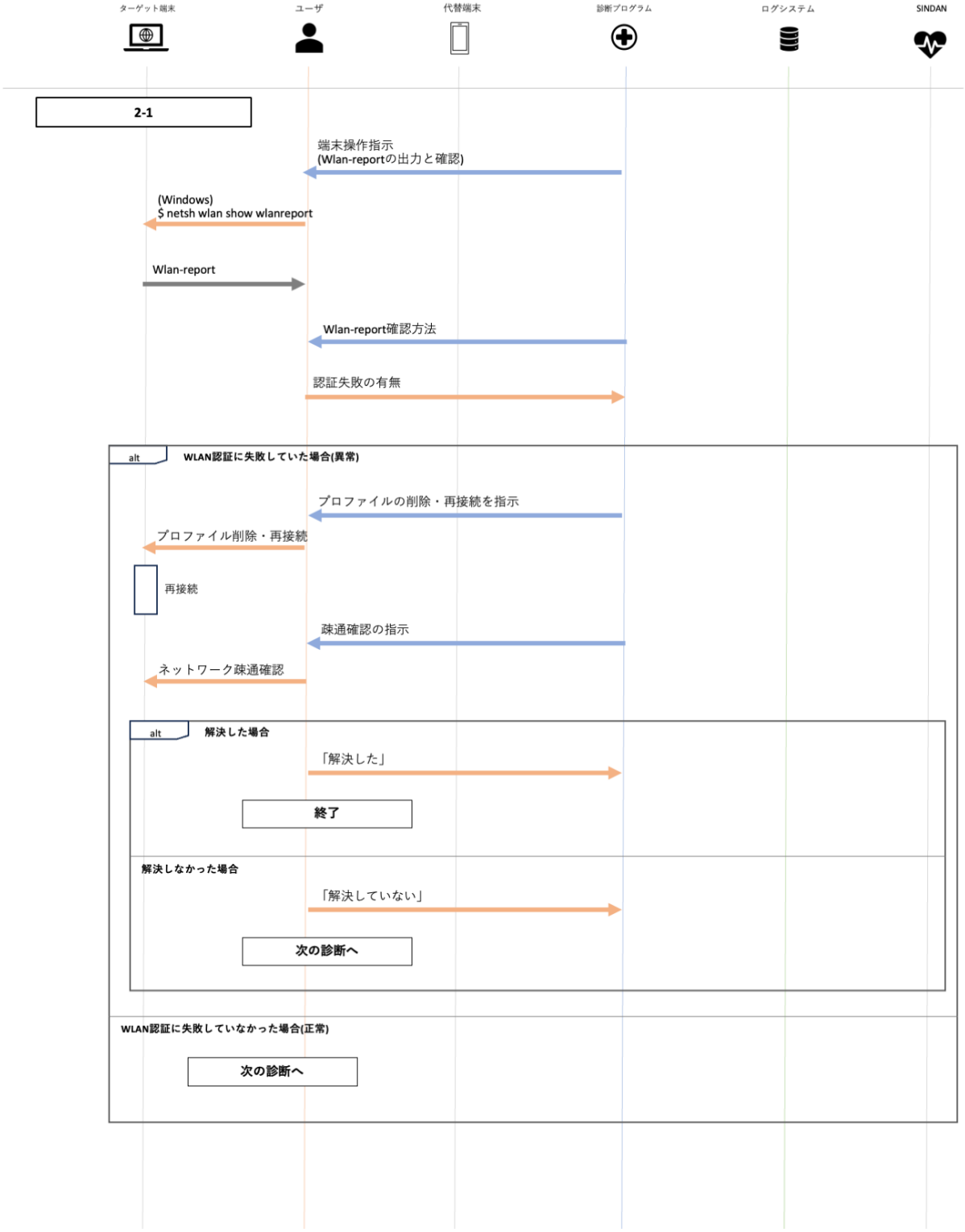

ターゲット端末
ユーザ
代替端末
診断プログラム
ログシステム
SINDAN
2-1
端末操作指示
(Wlan-reportの出力と確認)
(Windows)
$ netsh wlan show wlanreport
Wlan-report
Wlan-report確認方法
認証失敗の有無
alt
WLAN認証に失敗していた場合(異常)
プロファイルの削除・再接続を指示
プロファイル削除・再接続
再接続
疎通確認の指示
ネットワーク疎通確認
alt
解決した場合
「解決した」
終了
解決しなかった場合
「解決していない」
次の診断へ
WLAN認証に失敗していなかった場合(正常)
次の診断へ

図 41: ADU2-1

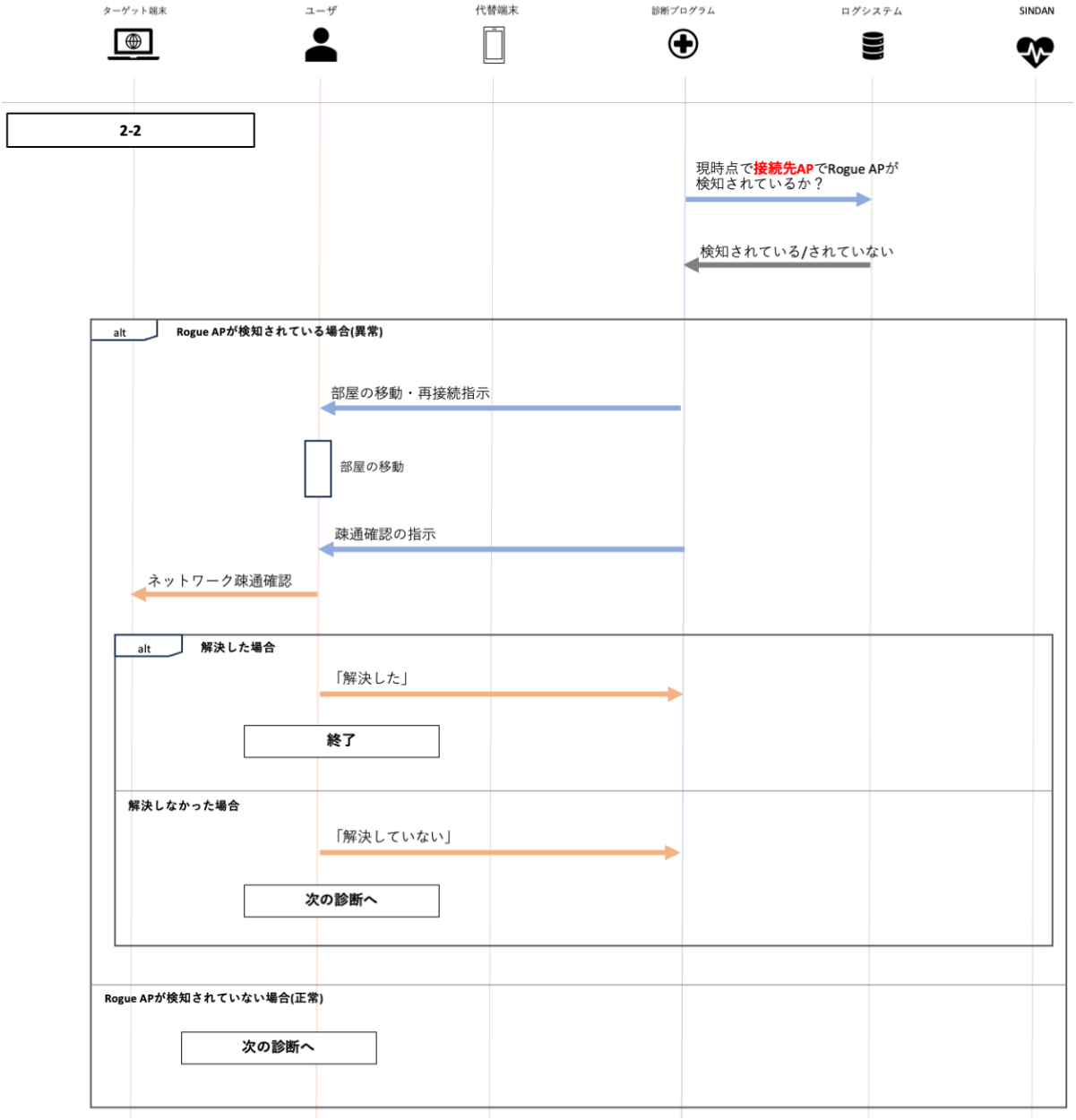

ターゲット端末
ユーザ
代替端末
診断プログラム
ログシステム
SINDAN
2-2
現時点で接続先APでRogue APが検知されているか？
検知されている/されていない
alt
Rogue APが検知されている場合(異常)
部屋の移動・再接続指示
部屋の移動
疎通確認の指示
ネットワーク疎通確認
alt
解決した場合
「解決した」
終了
解決しなかった場合
「解決していない」
次の診断へ
Rogue APが検知されていない場合(正常)
次の診断へ

図 42: ADU2-2

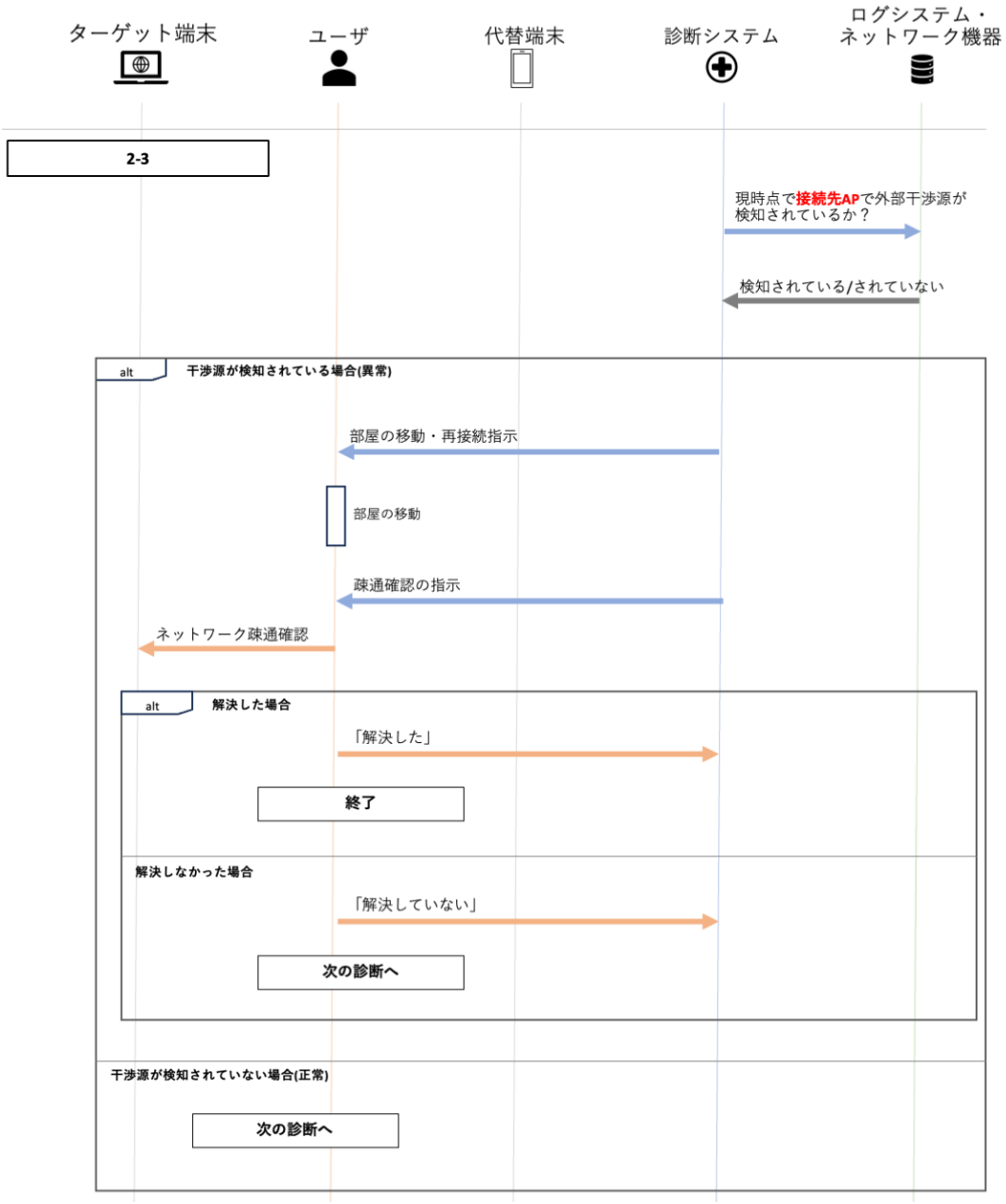

ターゲット端末
ユーザ
代替端末
診断システム
ログシステム・
ネットワーク機器
2-3
現時点で接続先APで外部干渉源が
検知されているか？
検知されている/されていない
alt
干渉源が検知されている場合(異常)
部屋の移動・再接続指示
部屋の移動
疎通確認の指示
ネットワーク疎通確認
alt
解決した場合
「解決した」
終了
解決しなかった場合
「解決していない」
次の診断へ
干渉源が検知されていない場合(正常)
次の診断へ

図 43: ADU2-3

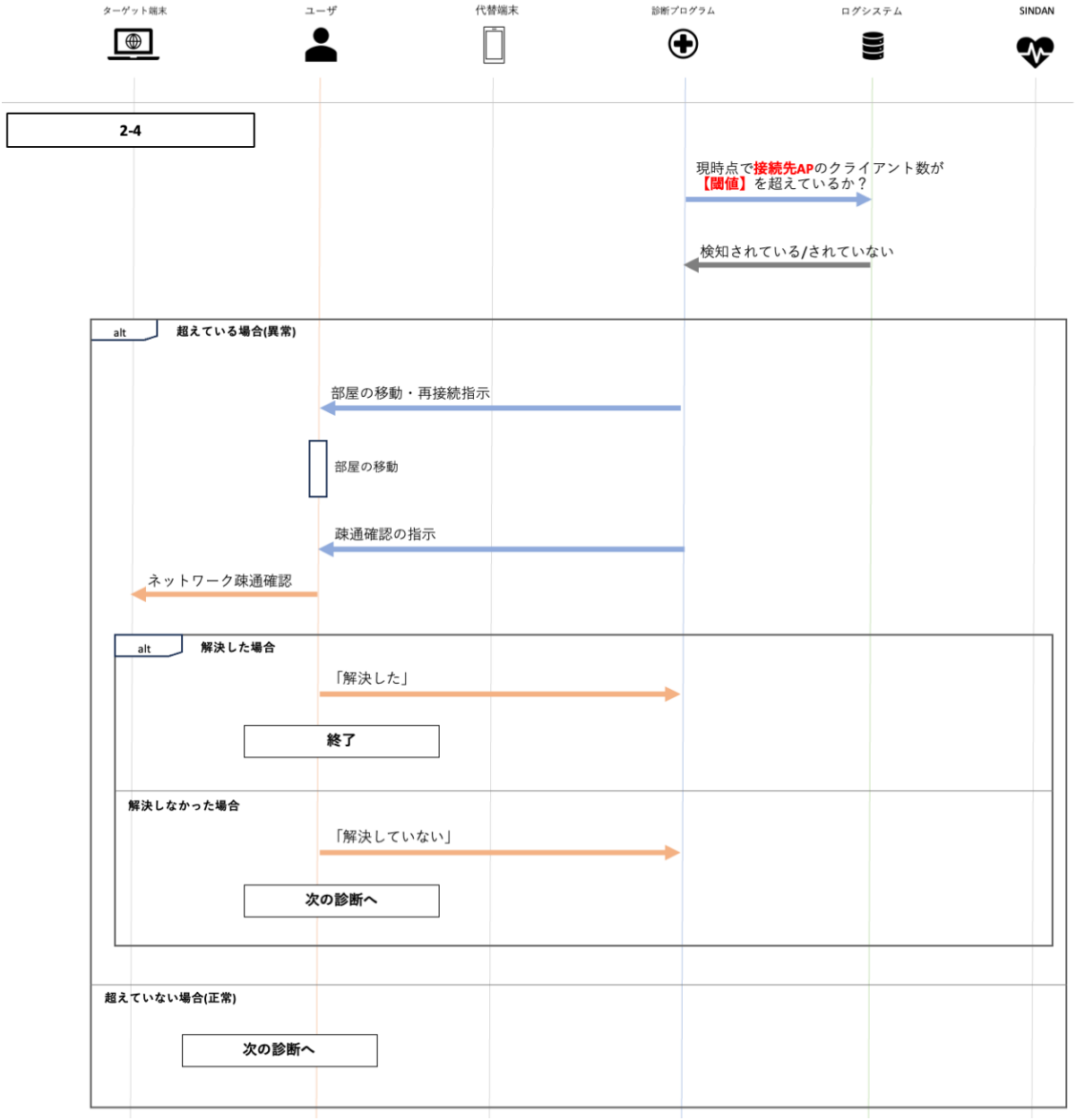

ターゲット端末
ユーザ
代替端末
診断プログラム
ログシステム
SINDAN
2-4
現時点で接続先APのクライアント数が
【閾値】を超えているか？
検知されている/されていない
alt
超えている場合(異常)
部屋の移動・再接続指示
部屋の移動
疎通確認の指示
ネットワーク疎通確認
alt
解決した場合
「解決した」
終了
解決しなかった場合
「解決していない」
次の診断へ
超えていない場合(正常)
次の診断へ

図 44: ADU2-4

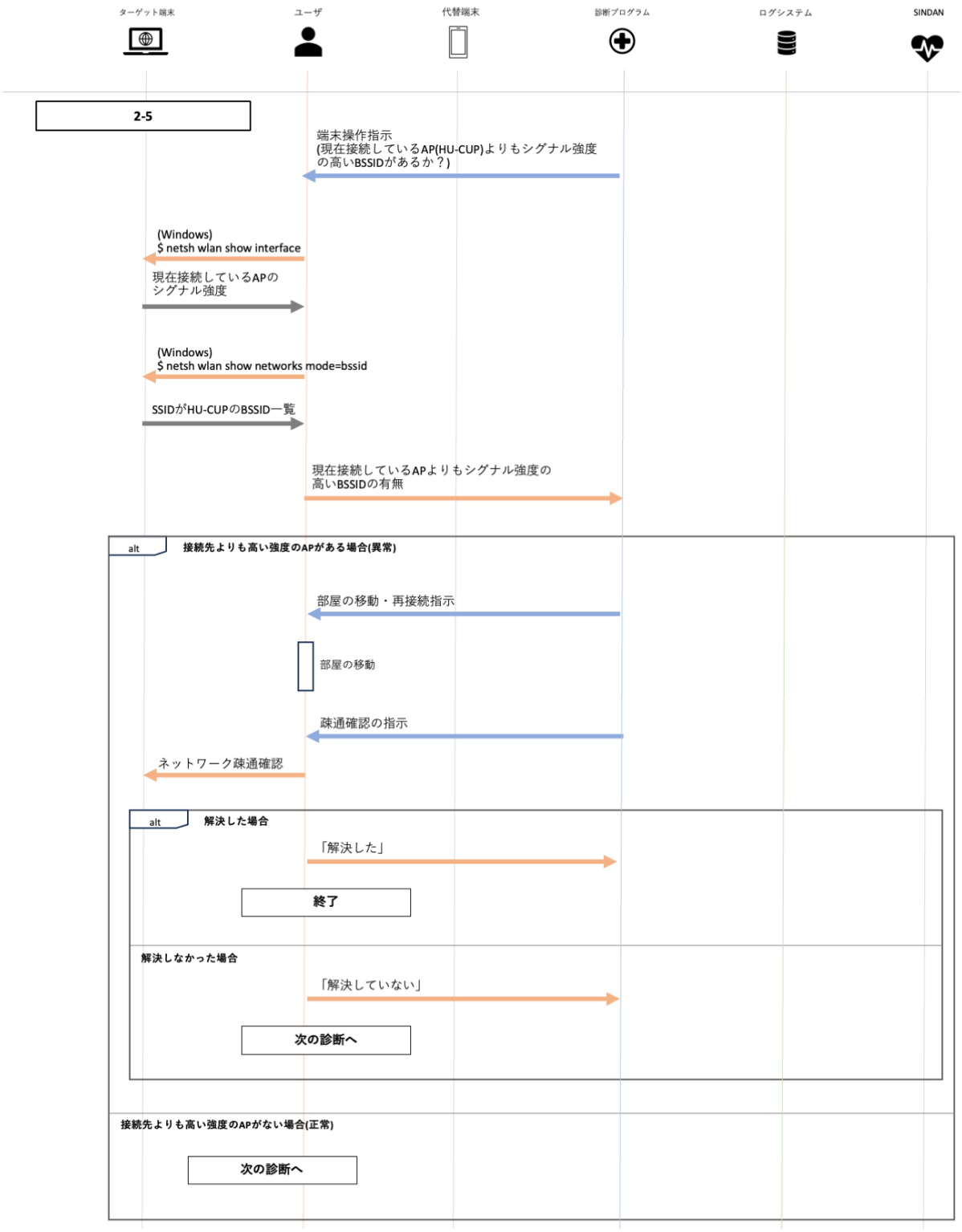

ターゲット端末
ユーザ
代替端末
診断プログラム
ログシステム
SINDAN
2-5
端末操作指示
(現在接続しているAP(HU-CUP)よりもシグナル強度
の高いBSSIDがあるか？)
(Windows)
$ netsh wlan show interface
現在接続しているAPの
シグナル強度
(Windows)
$ netsh wlan show networks mode=bssid
SSIDがHU-CUPのBSSID一覧
現在接続しているAPよりもシグナル強度の
高いBSSIDの有無
alt
接続先よりも高い強度のAPがある場合(異常)
部屋の移動・再接続指示
部屋の移動
疎通確認の指示
ネットワーク疎通確認
alt
解決した場合
「解決した」
終了
解決しなかった場合
「解決していない」
次の診断へ
接続先よりも高い強度のAPがない場合(正常)
次の診断へ

図 45: ADU2-5

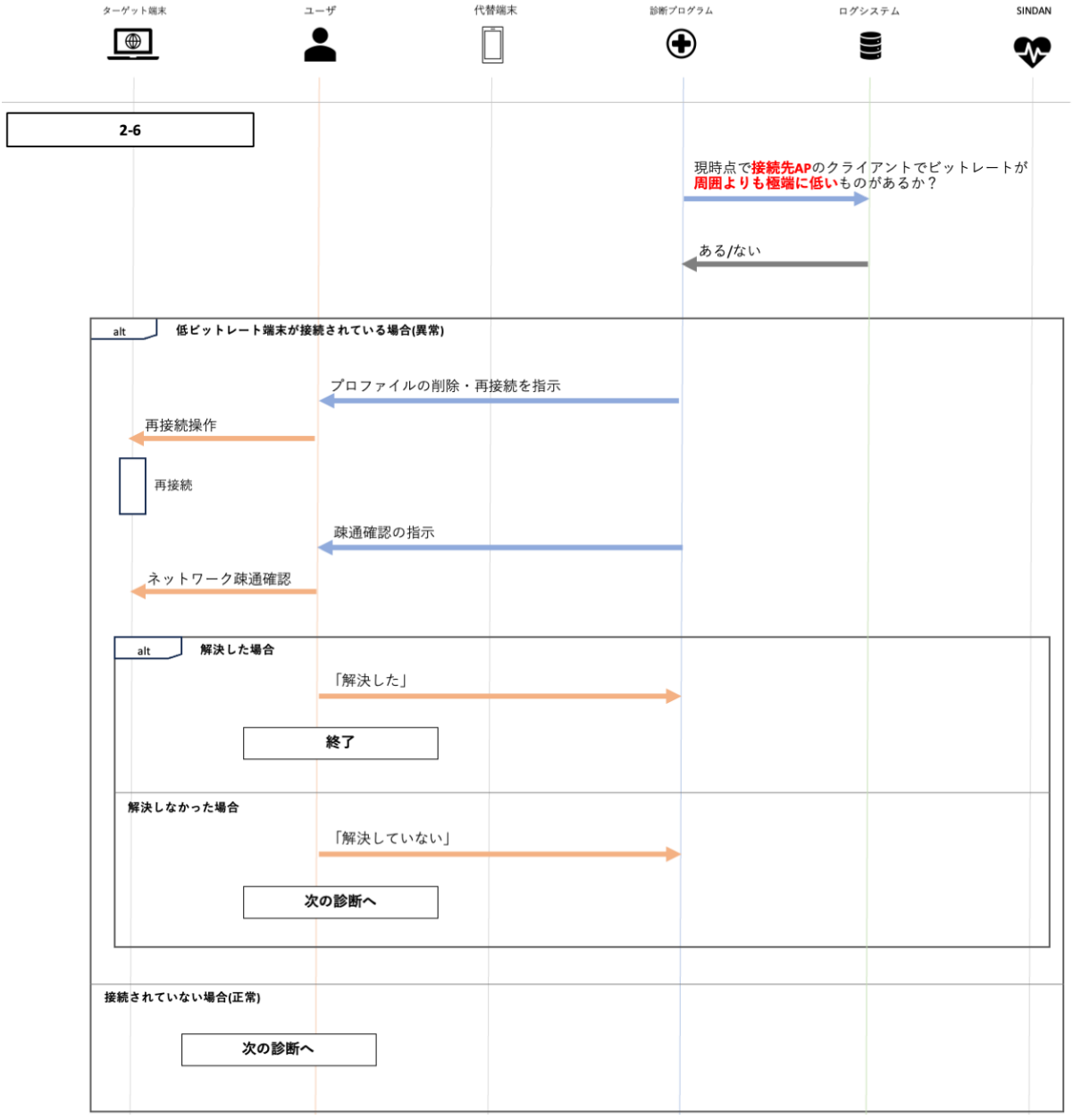

ターゲット端末
ユーザ
代替端末
診断プログラム
ログシステム
SINDAN
2-6
現時点で接続先APのクライアントでビットレートが
周囲よりも極端に低いものがあるか？
ある/ない
alt
低ビットレート端末が接続されている場合(異常)
プロファイルの削除・再接続を指示
再接続操作
再接続
疎通確認の指示
ネットワーク疎通確認
alt
解決した場合
「解決した」
終了
解決しなかった場合
「解決していない」
次の診断へ
接続されていない場合(正常)
次の診断へ

図 46: ADU2-6

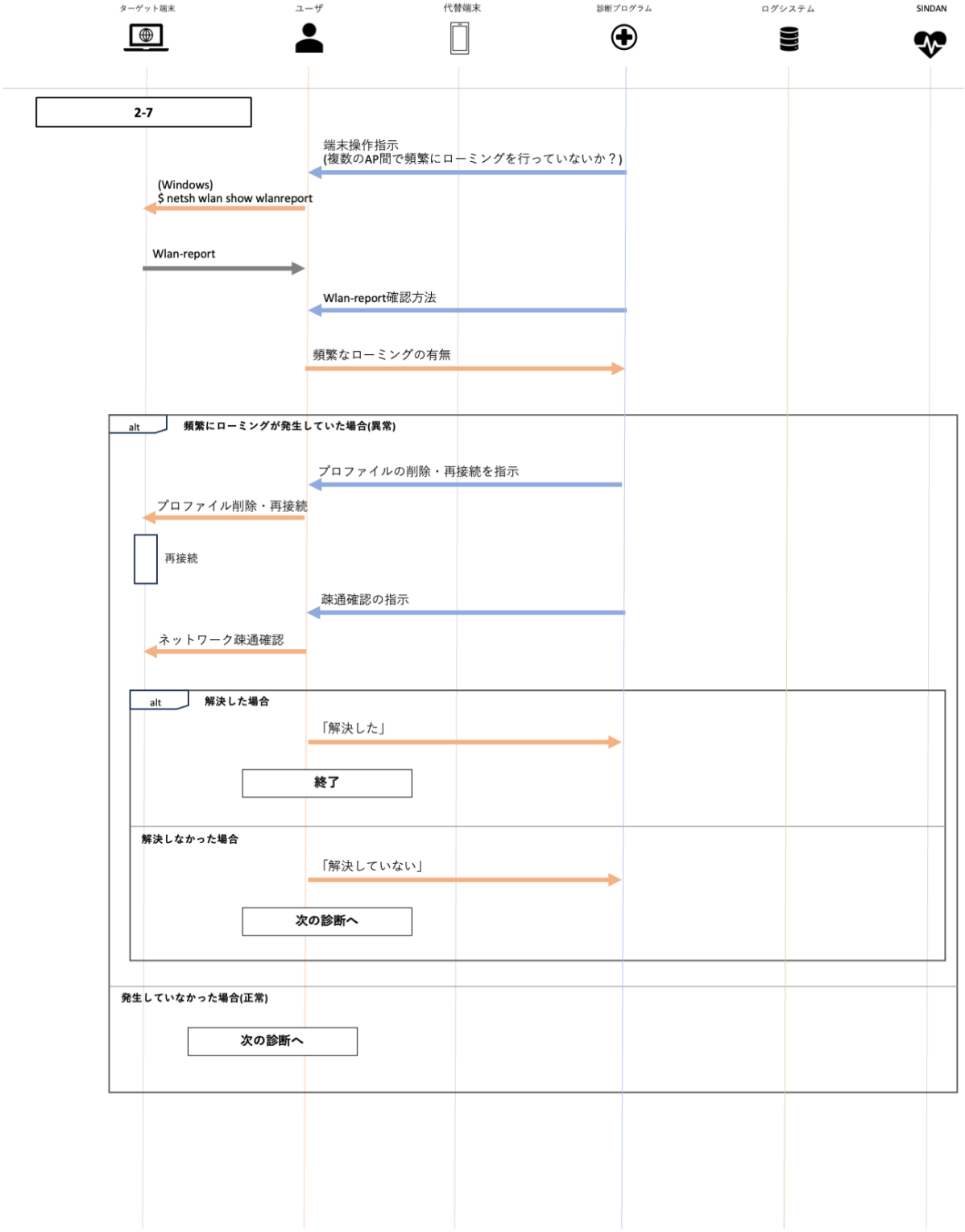

ターゲット端末
ユーザ
代替端末
診断プログラム
ログシステム
SINDAN
2-7
端末操作指示
(複数のAP間で頻繁にローミングを行っていないか？)
(Windows)
$ netsh wlan show wlanreport
Wlan-report
Wlan-report確認方法
頻繁なローミングの有無
alt
頻繁にローミングが発生していた場合(異常)
プロファイルの削除・再接続を指示
プロファイル削除・再接続
再接続
疎通確認の指示
ネットワーク疎通確認
alt
解決した場合
「解決した」
終了
解決しなかった場合
「解決していない」
次の診断へ
発生していなかった場合(正常)
次の診断へ

図 47: ADU2-7

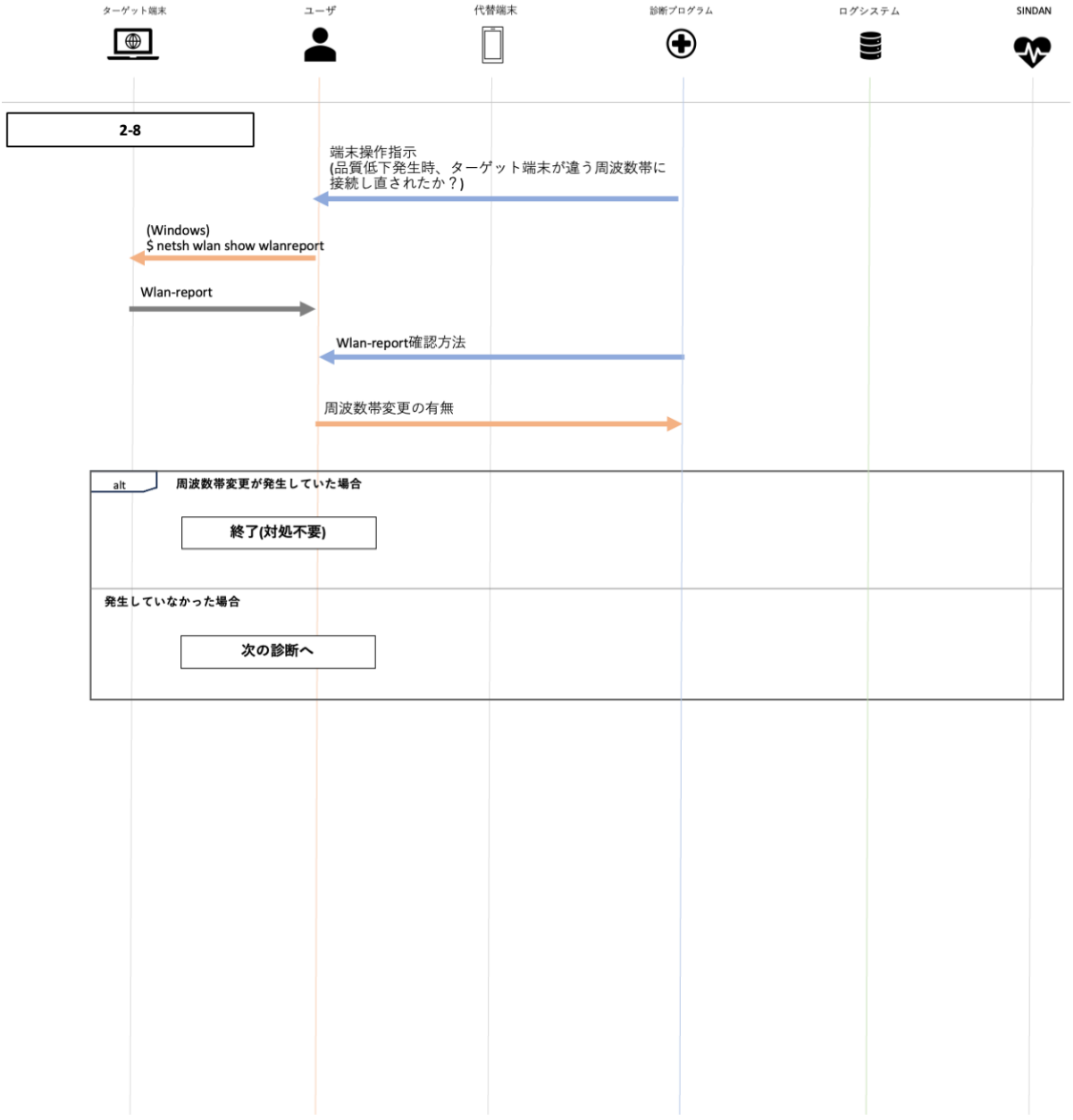

ターゲット端末
ユーザ
代替端末
診断プログラム
ログシステム
SINDAN
2-8
端末操作指示
(品質低下発生時、ターゲット端末が違う周波数帯に
接続し直されたか？)
(Windows)
$ netsh wlan show wlanreport
Wlan-report
Wlan-report確認方法
周波数帯変更の有無
alt
周波数帯変更が発生していた場合
終了(対処不要)
発生していなかった場合
次の診断へ

図 48: ADU2-8

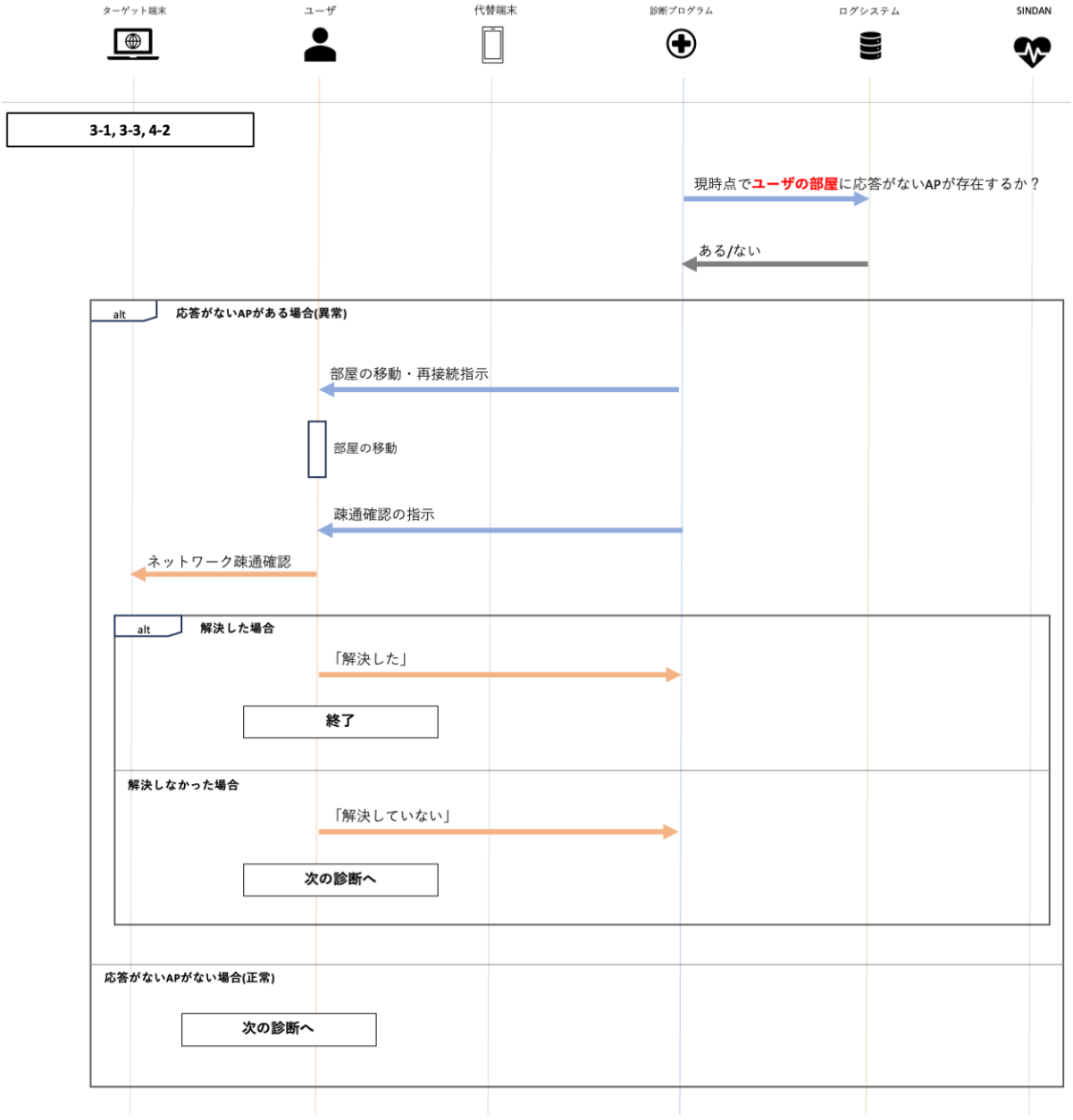


図 49: ADU3-1, 3-3, 4-2

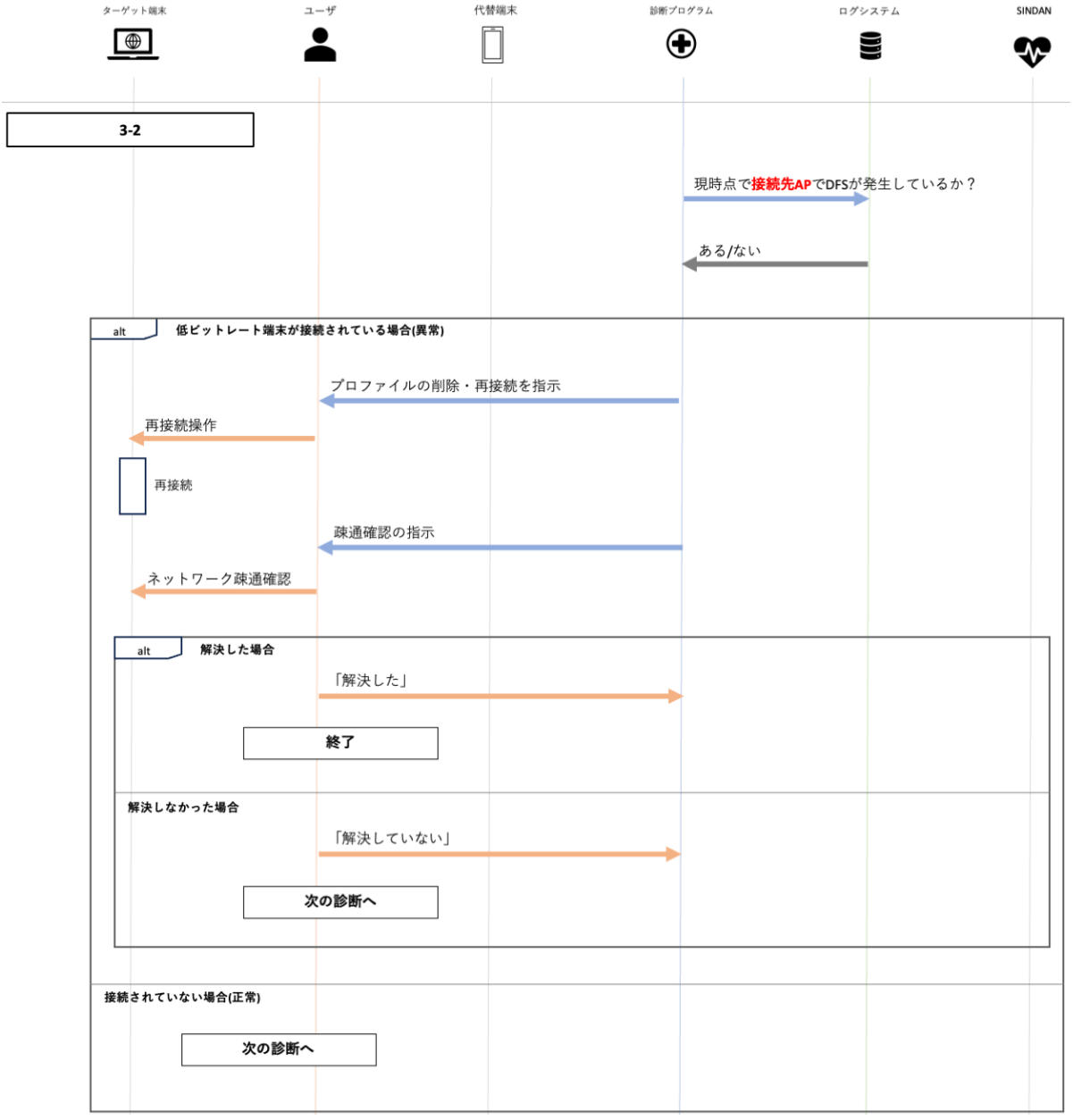

ターゲット端末
ユーザ
代替端末
診断プログラム
ログシステム
SINDAN
3-2
現時点で接続先APでDFSが発生しているか？
ある/ない
alt
低ビットレート端末が接続されている場合(異常)
プロファイルの削除・再接続を指示
再接続操作
再接続
疎通確認の指示
ネットワーク疎通確認
alt
解決した場合
「解決した」
終了
解決しなかった場合
「解決していない」
次の診断へ
接続されていない場合(正常)
次の診断へ

図 50: ADU3-2

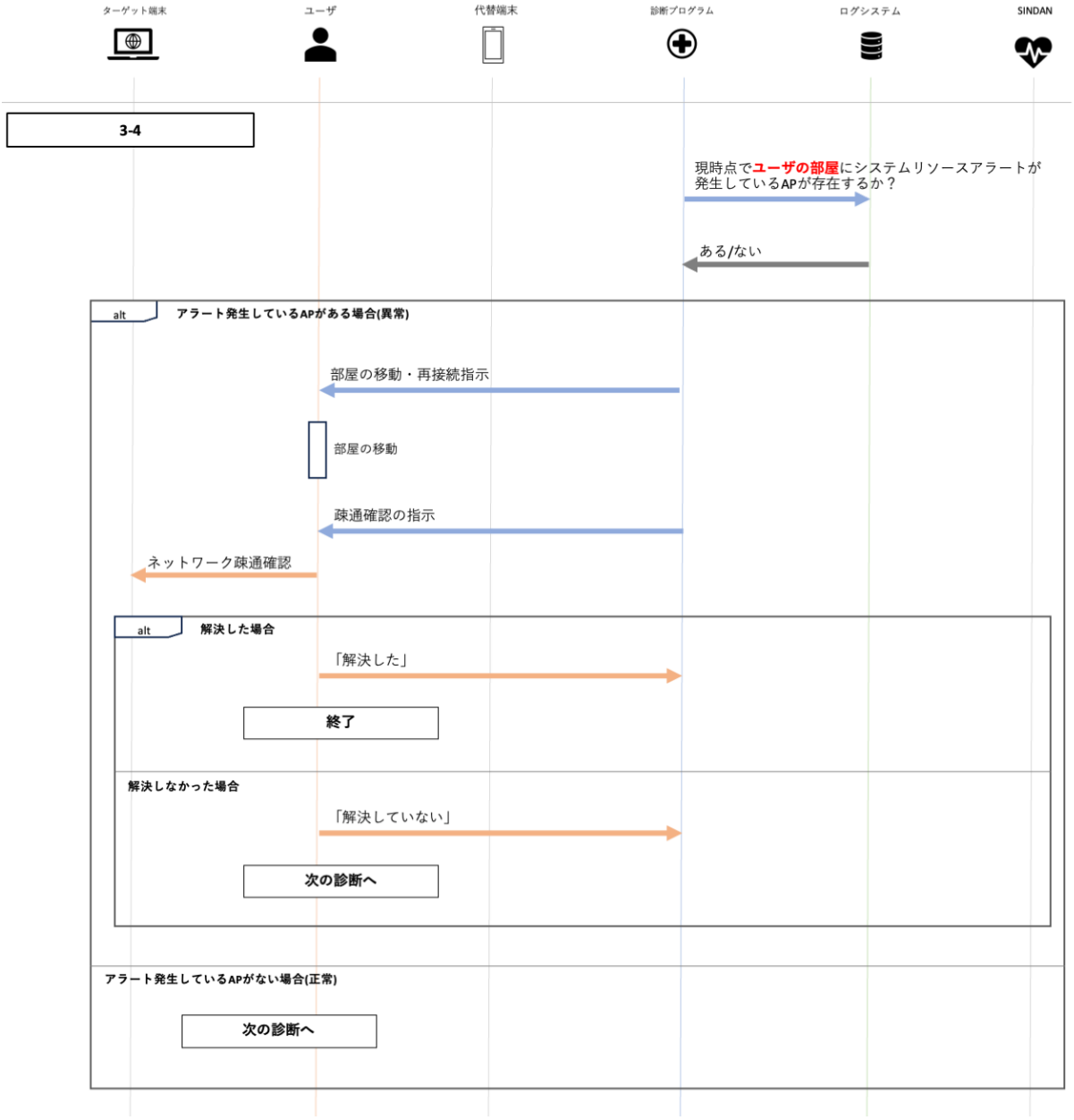

ターゲット端末
ユーザ
代替端末
診断プログラム
ログシステム
SINDAN
3-4
現時点でユーザの部屋にシステムリソースアラートが発生しているAPが存在するか？
ある/ない
alt
アラート発生しているAPがある場合(異常)
部屋の移動・再接続指示
部屋の移動
疎通確認の指示
ネットワーク疎通確認
alt
解決した場合
「解決した」
終了
解決しなかった場合
「解決していない」
次の診断へ
アラート発生しているAPがない場合(正常)
次の診断へ

図 51: ADU3-4

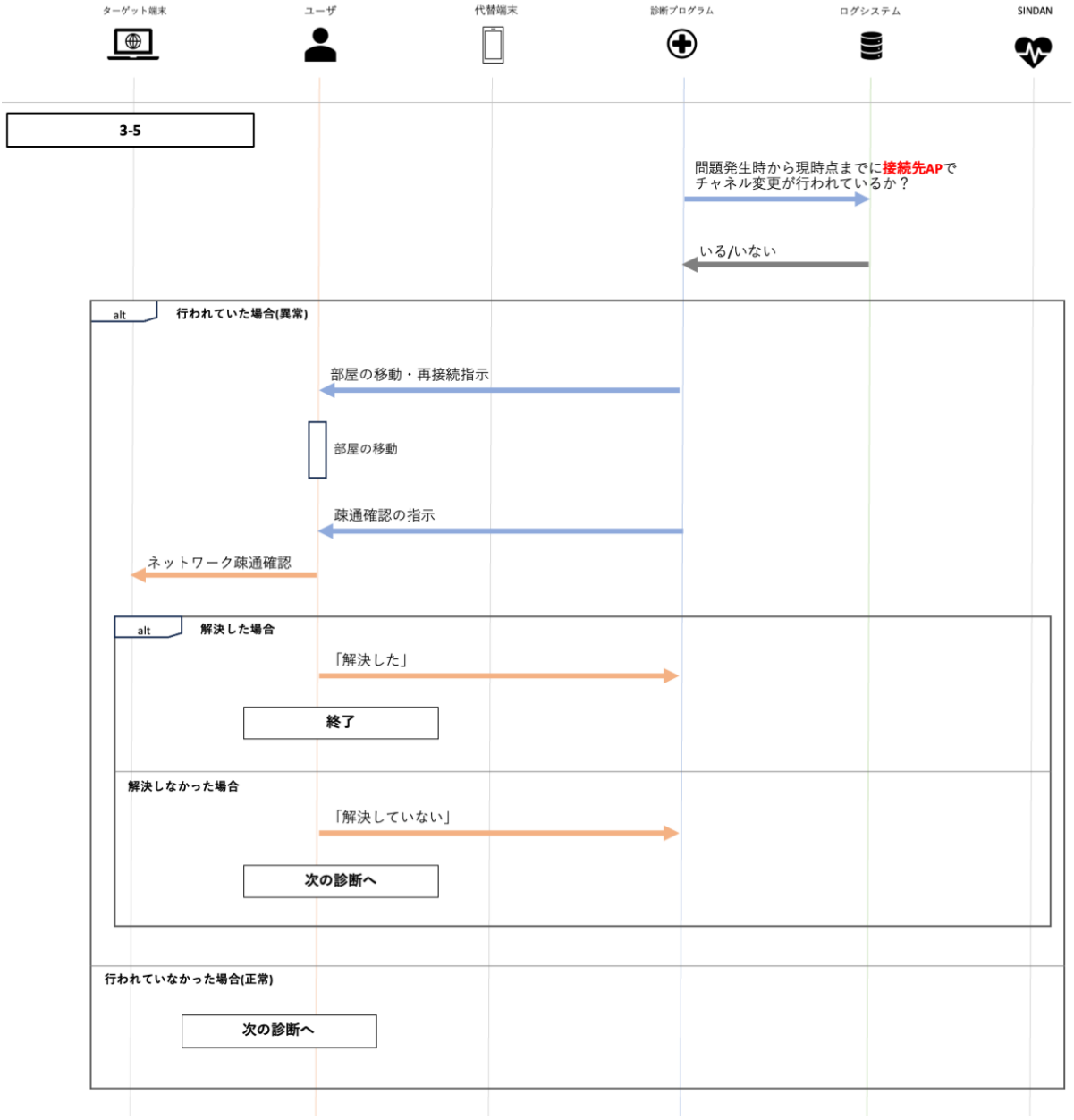

ターゲット端末
ユーザ
代替端末
診断プログラム
ログシステム
SINDAN
3-5
問題発生時から現時点までに接続先APで
チャネル変更が行われているか？
いる/いない
alt
行われていた場合(異常)
部屋の移動・再接続指示
部屋の移動
疎通確認の指示
ネットワーク疎通確認
alt
解決した場合
「解決した」
終了
解決しなかった場合
「解決していない」
次の診断へ
行われていなかった場合(正常)
次の診断へ

図 52: ADU3-5

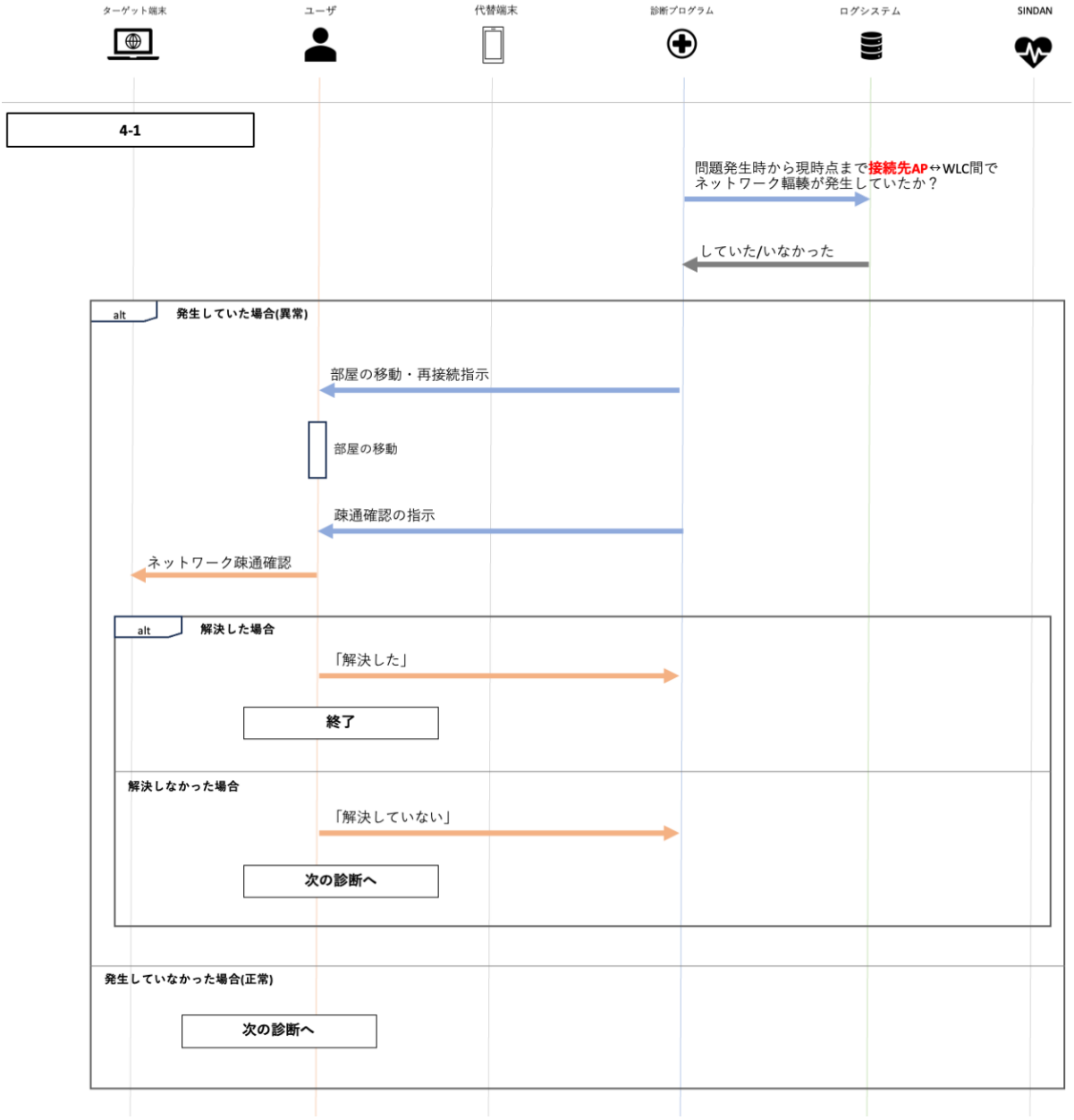

ターゲット端末
ユーザ
代替端末
診断プログラム
ログシステム
SINDAN
4-1
問題発生時から現時点まで接続先AP↔WLC間で
ネットワーク輻輳が発生していたか？
していた/いなかった
alt
発生していた場合(異常)
部屋の移動・再接続指示
部屋の移動
疎通確認の指示
ネットワーク疎通確認
alt
解決した場合
「解決した」
終了
解決しなかった場合
「解決していない」
次の診断へ
発生していなかった場合(正常)
次の診断へ

図 53: ADU4-1


ターゲット端末
ユーザ
代替端末
診断プログラム
ログシステム
SINDAN
メディアセンターHP
5-1
現時点でWLCのリソースは枯渇していないか？
枯渇している/いない
alt
枯渇している場合(異常)
「フォームから問い合わせをしてください」
＋診断過程
リダイレクト
メディアセンターお問い合わせフォーム
症状内容・診断結果
終了
枯渇していない場合(正常)
次の診断へ

図 54: ADU5-1

チャットボット対話シナリオ

現段階ではチェックリスト中の問題の一部のみに対してチャットボット対話シナリオが設計されている．以下には，現時点で設計が完了しているものの全てを示す．

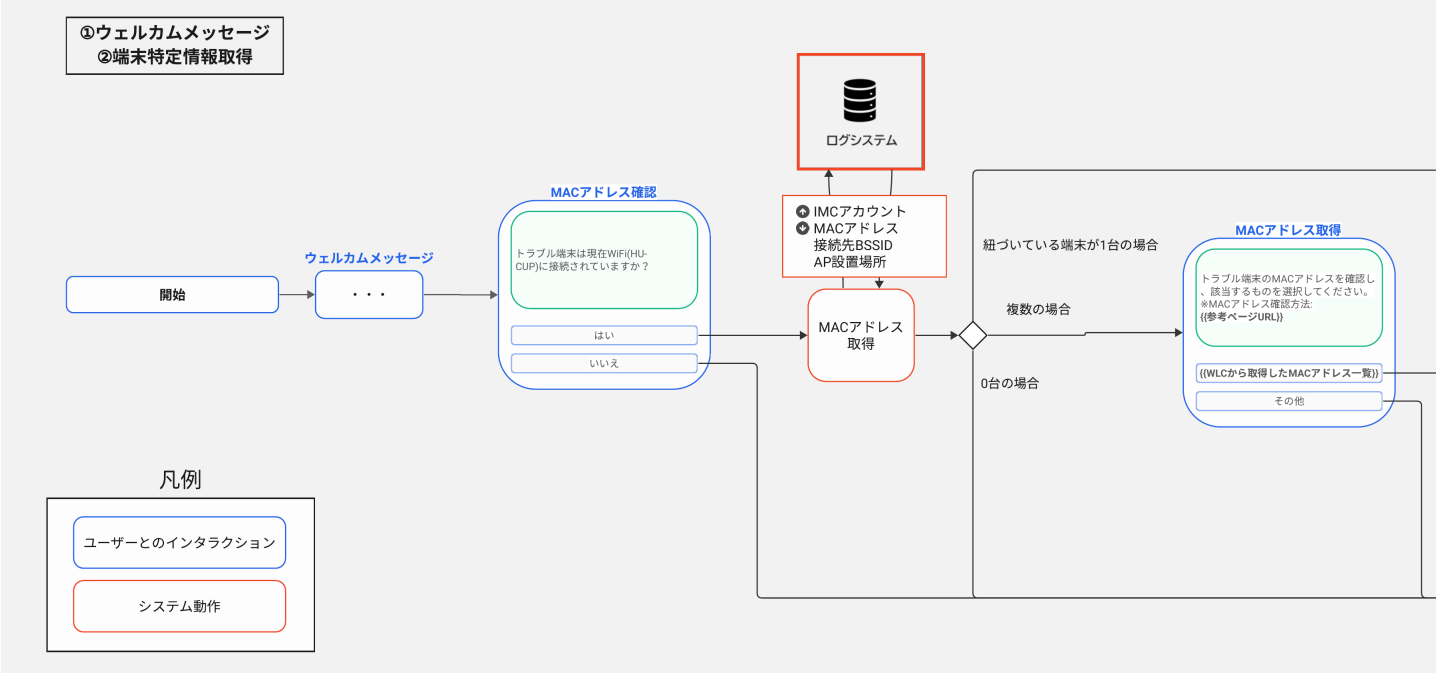


図 55: 図 13 中①，③における対話シナリオ (1)

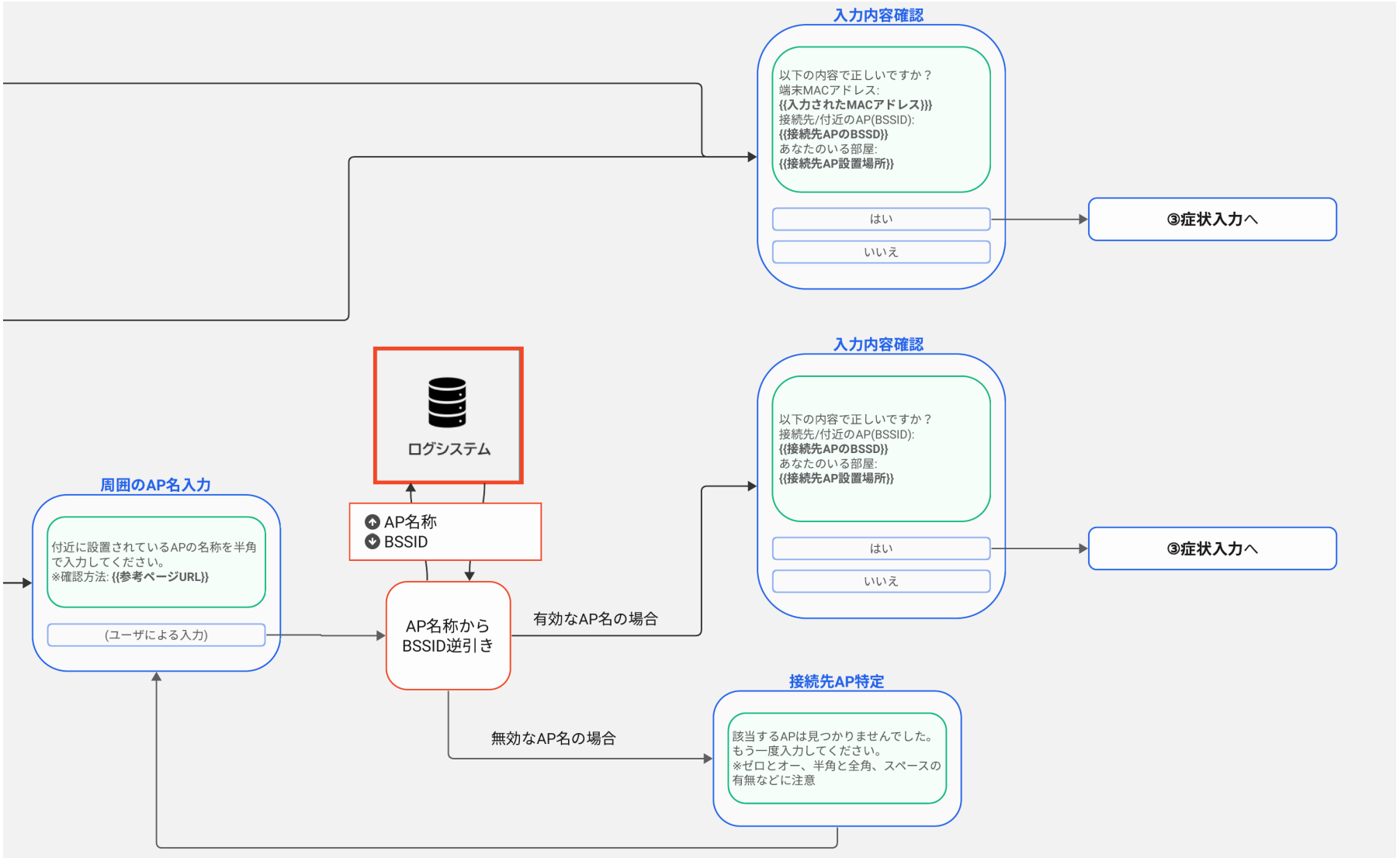


図 56: 図 13 中①，③における対話シナリオ (2)

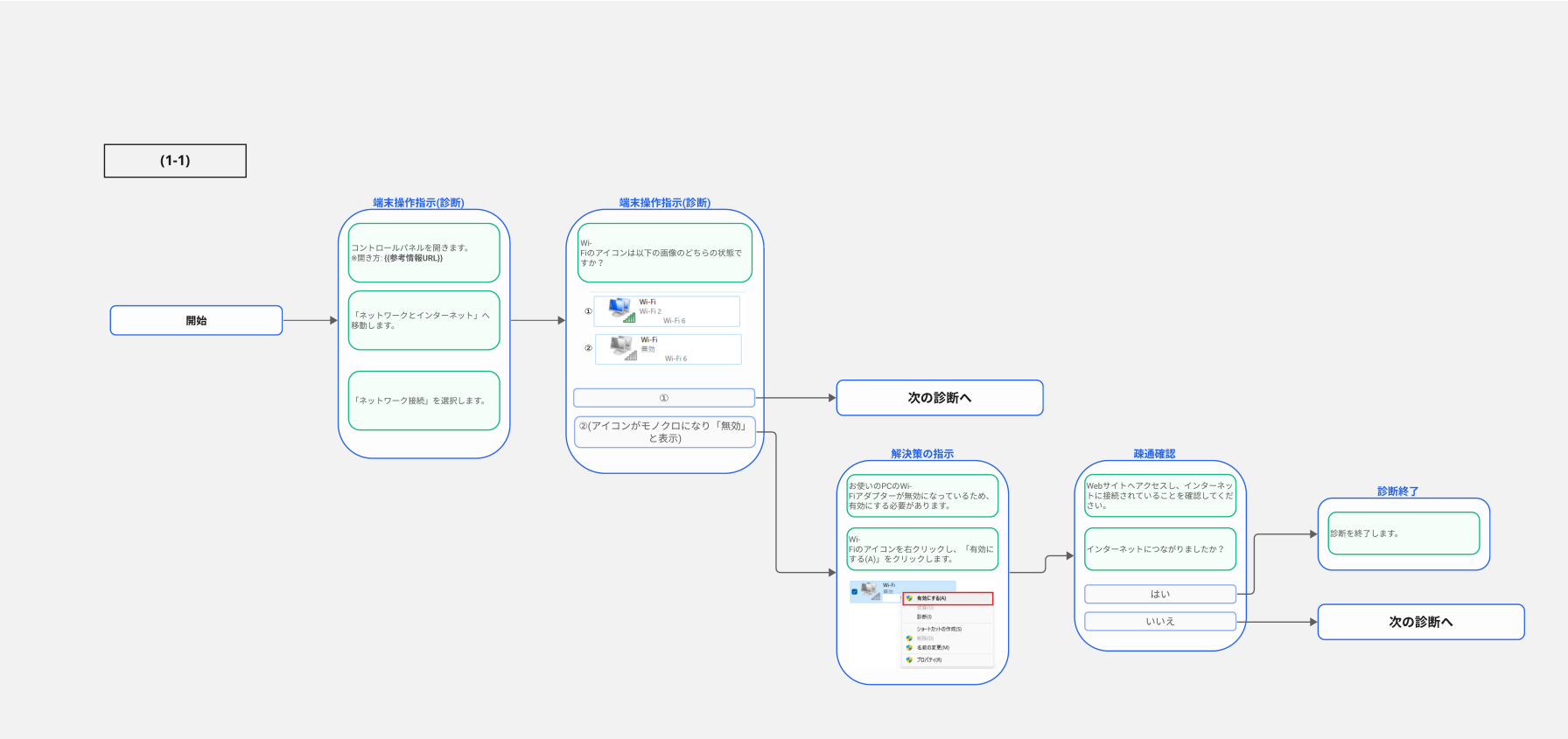


図 57: 対話シナリオ：ADU1-1

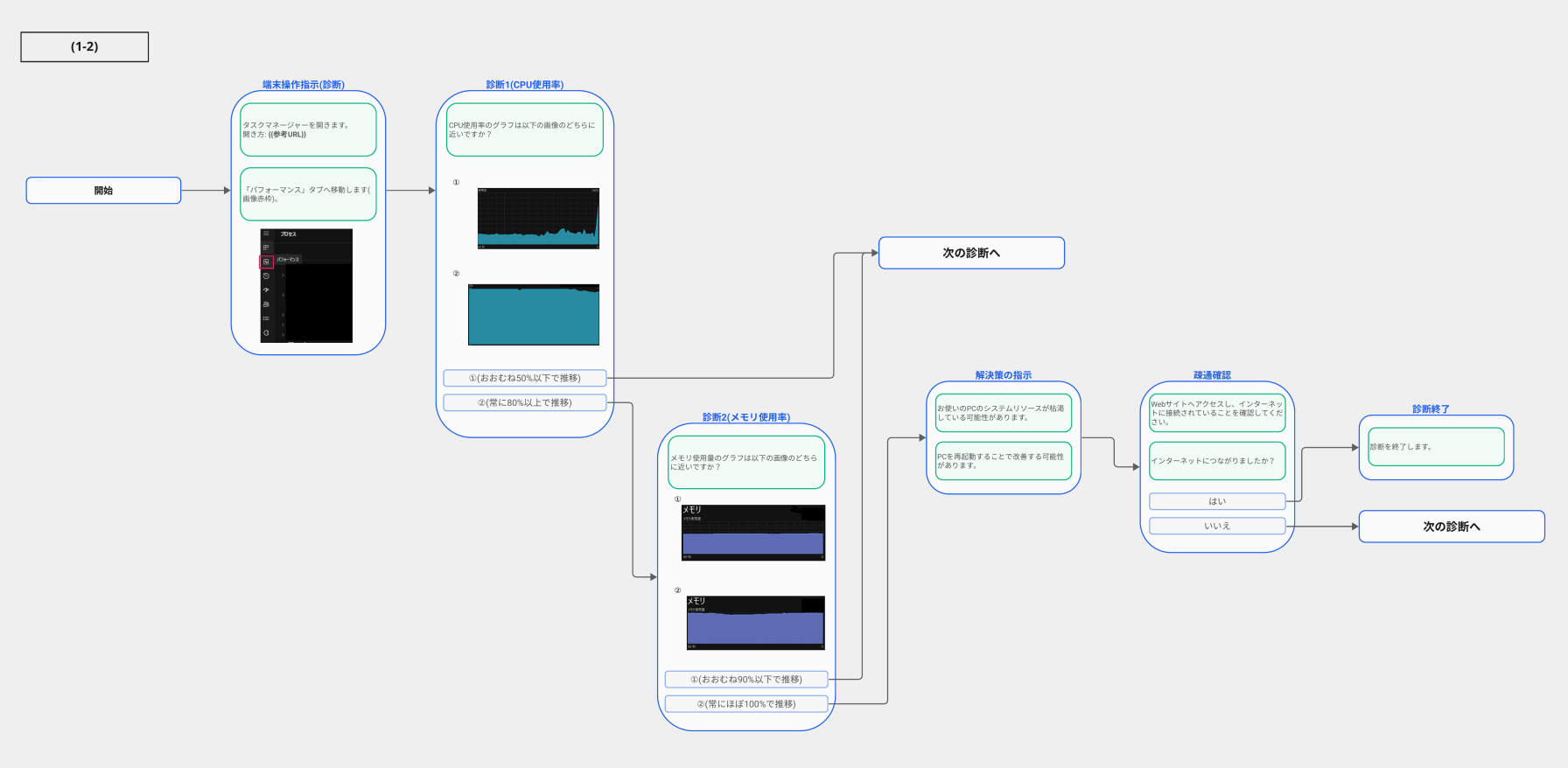


図 58: 対話シナリオ：ADU1-2

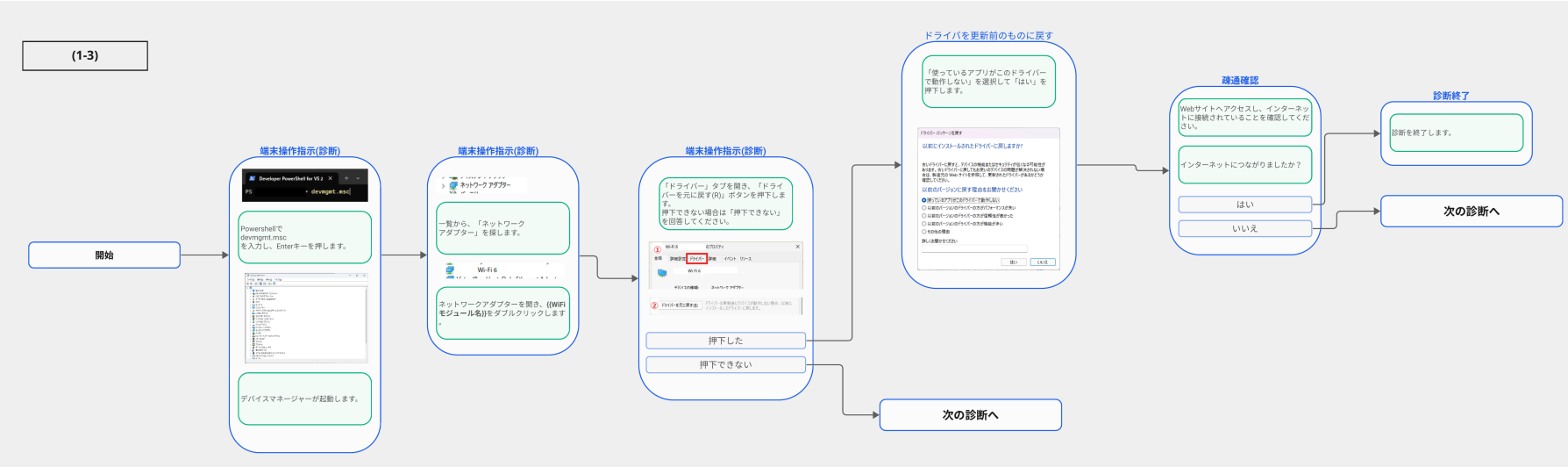


図 59: 対話シナリオ：ADU1-3

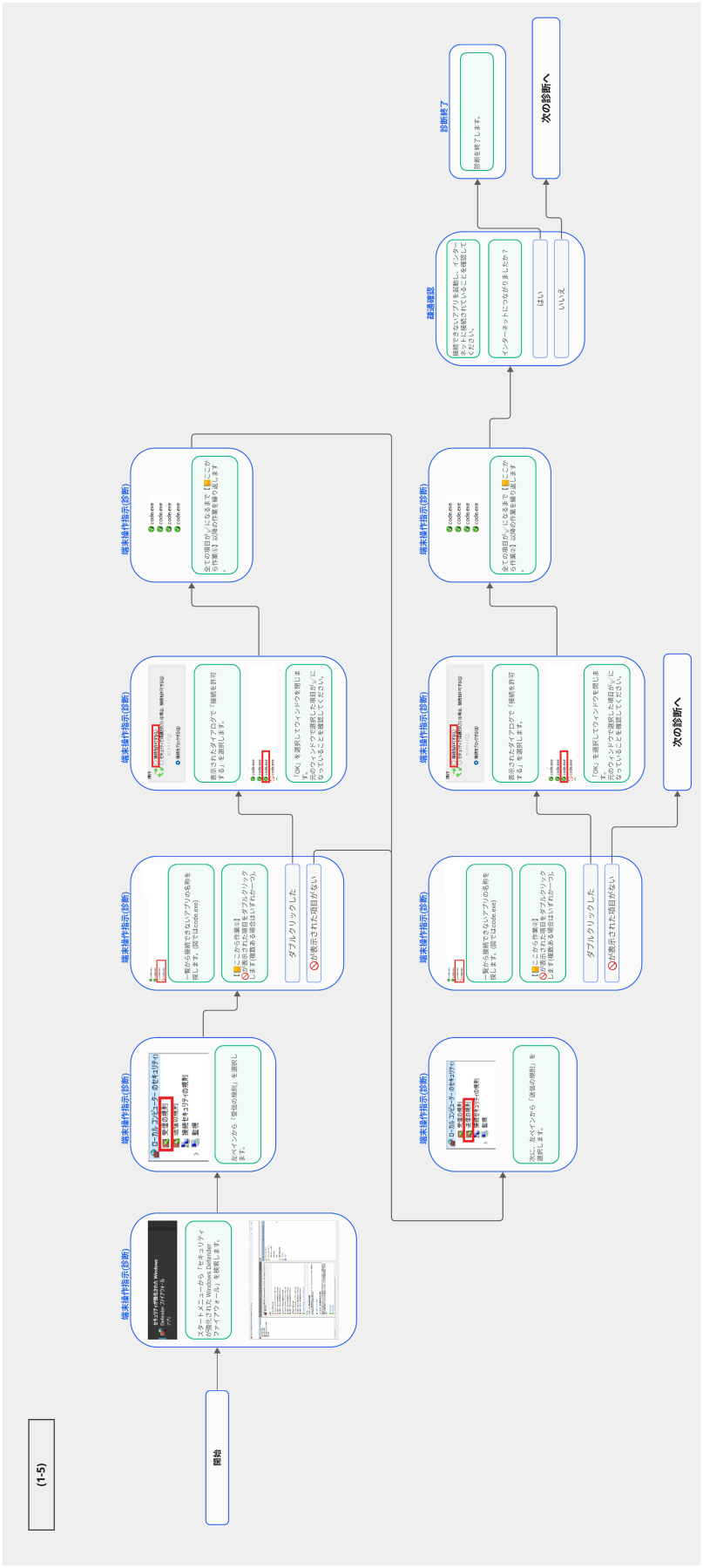


図 60: 対話シナリオ：ADU1-5

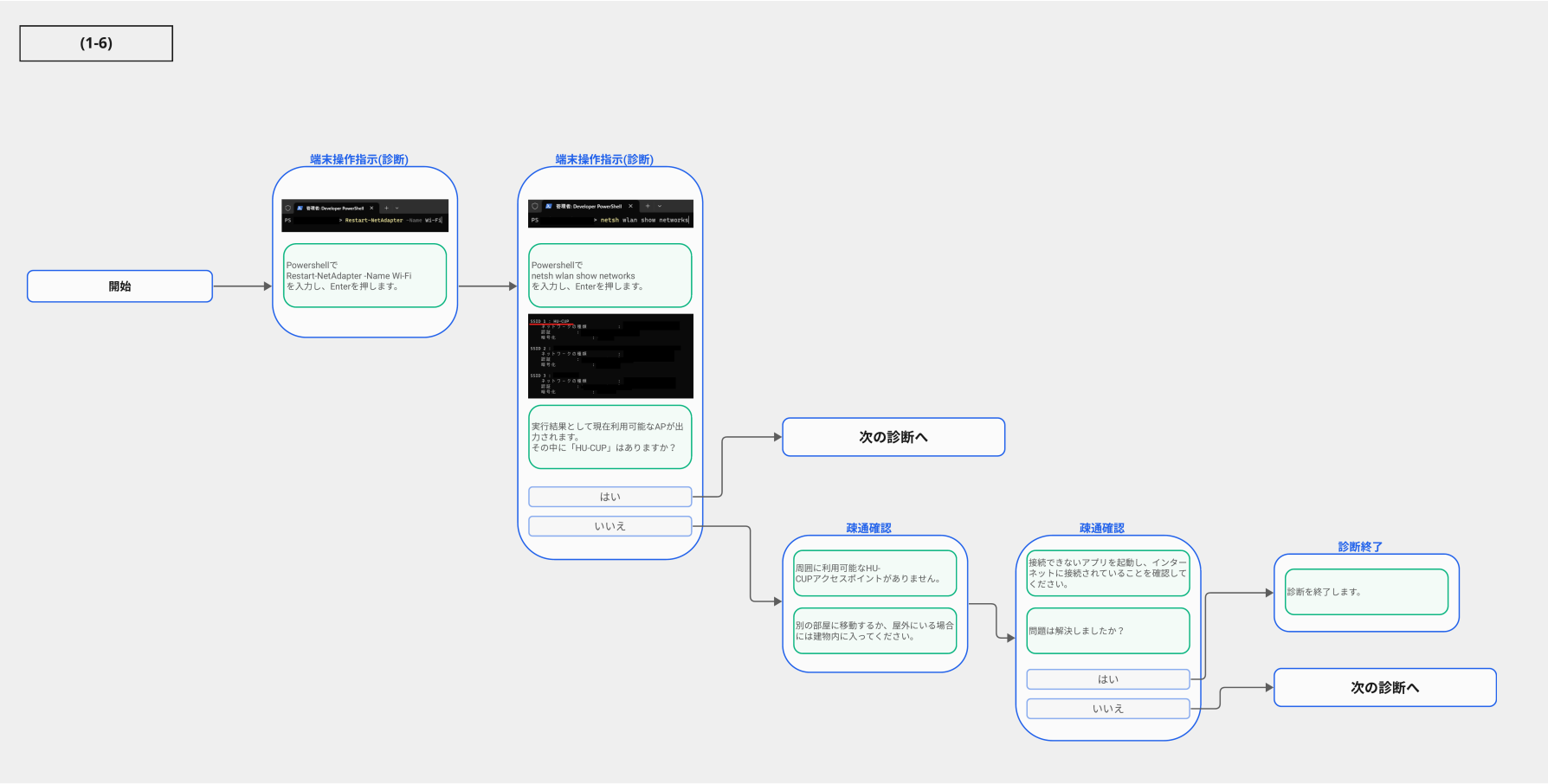


図 61: 対話シナリオ：ADU1-6

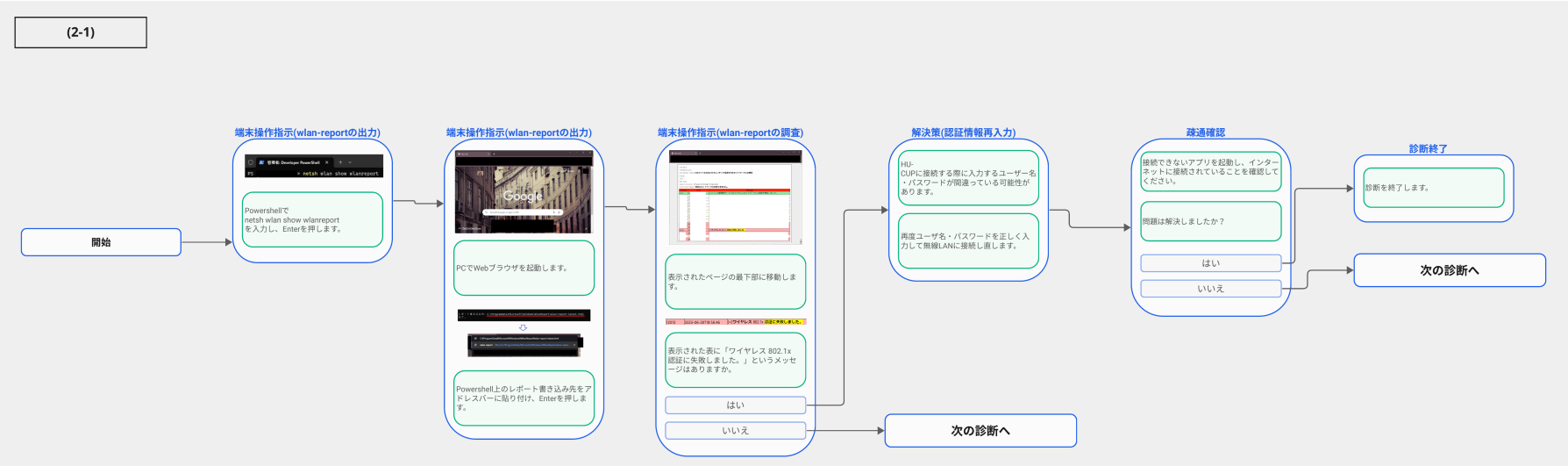


図 62: 対話シナリオ：ADU2-1

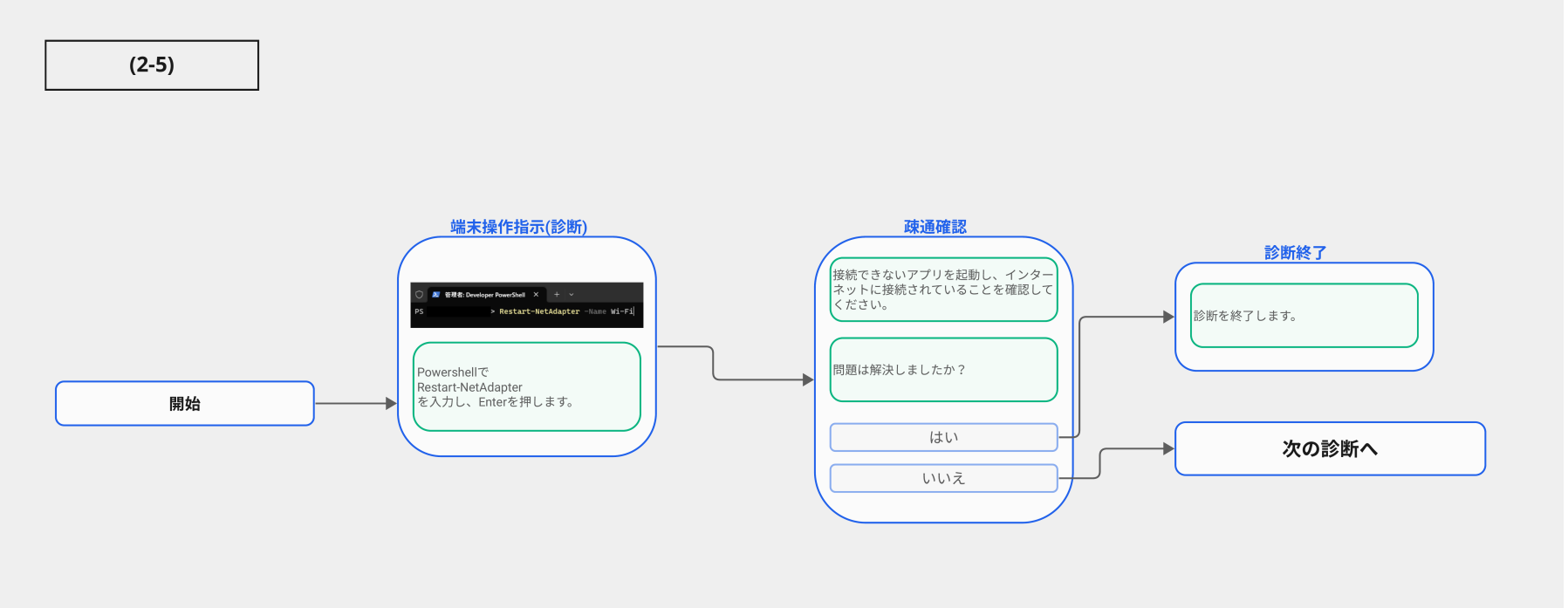


図 63: 対話シナリオ：ADU2-5

ソースコード

関連するソースコードは GitHub リポジトリ
`https://github.com/ksn0ky/netdoctor-logsystem.git` (URL) で確認できる.