P3NK-7572-06Z0

Fujitsu Network SR-M
トラブルシューティング

V20

FUJITSU

はじめに

このたびは、本装置をお買い上げいただき、まことにありがとうございます。
無線LANを使用した安全なネットワークを構築するために、本装置をご利用ください。

2020年12月 初版
2021年 6月 第2版
2021年12月 第3版
2022年 4月 第4版
2023年 1月 第5版
2023年10月 第6版

目次

本書の使いかた

本書では、困ったときの原因・対処方法やご購入時の状態に戻す方法について説明しています。

本書の読者と前提知識

本書は、ネットワーク管理を行っている方を対象に記述しています。

本書を利用するにあたって、ネットワークおよびインターネットに関する基本的な知識が必要です。

ネットワーク設定を初めて行う方でも「機能説明書」に分かりやすく記載していますので、安心してお読みいただけます。

マークについて

本書で使用しているマーク類は、以下のような内容を表しています。

	本装置をお使いになる際に、役に立つ知識をコラム形式で説明しています。
こんな事に気をつけて	本装置をご使用になる際に、注意していただきたいことを説明しています。
	操作手順で説明しているもののほかに、補足情報を説明しています。
	操作方法など関連事項を説明している箇所を示します。
	本装置の機能を使用する際に、対象となる機種名を示します。
	製造物責任法（PL）関連の警告事項を表しています。本装置をお使いの際は必ず守ってください。
	製造物責任法（PL）関連の注意事項を表しています。本装置をお使いの際は必ず守ってください。

本書における商標の表記について

Windows は、米国 Microsoft Corporation の米国およびその他の国における登録商標です。

本書に記載されているその他の会社名および製品名は、各社の商標または登録商標です。

製品名の略称について

本書で使用している製品名は、以下のように略して表記します。

製品名称	本文中の表記
Microsoft® Windows® 10 Home 64 ビット版	Windows 10 または Windows
Microsoft® Windows® 10 Pro 64 ビット版	

本装置のマニュアルの構成

本装置の取扱説明書は、以下のとおり構成されています。使用する目的に応じて、お使いください。

マニュアル名称	内容
ご利用にあたって	本装置の設置方法やソフトウェアのインストール方法を説明しています。
コマンドユーザーズガイド	コマンドを使用して、時刻などの基本的な設定またはメンテナンスについて説明しています。
コマンドリファレンス	構成定義コマンド、運用管理コマンド、およびその他のコマンドの項目やパラメタの詳細な情報を説明しています。
コマンド設定事例集	コマンドを使用した、基本的な接続形態または機能の活用方法を説明しています。
機能説明書	本装置の便利な機能について説明しています。
トラブルシューティング（本書）	トラブルが起きたときの原因と対処方法を説明しています。
メッセージ集	システムログ情報などのメッセージの詳細な情報を説明しています。
仕様一覧	本装置のハード／ソフトウェア仕様と MIB/Trap 一覧を説明しています。
Web ユーザーズガイド	Web 画面を使用して、基本的な設定またはメンテナンスについて説明しています。

1　通信ができない場合には

通信ができない場合、さまざまな原因が考えられます。まず、以下を参考に本装置の動作状況を確認してください。

ヒント

◆ エラー番号からトラブルの原因を探る

エラーログ情報に表示されたエラー番号から、エラーの原因をある程度特定できます。

エラーログ情報をプリントアウトして保管しておくことをお勧めします。

警告

・決してご自身では修理を行わないでください。

・本装置が故障した場合は、弊社の技術員または弊社が認定した技術員によるメンテナンスを受けてください。

1.1　起動時の動作に関するトラブル

本装置起動時のトラブルには、以下のようなものがあります。

● READY ランプが消灯している

【原因】　運用中にランプを消灯する設定になっています。

【対処】　異常ではありません。

【原因】　ETHERNET ポート 1 が、給電装置（POE）と正しく接続されていません。

【対処】　ETHERNET ポート 1 と、IEEE802.3at または IEEE802.3af に準拠した給電装置（POE）をカテゴリー 5 以上のケーブルで正しく接続してください。

【原因】　給電装置（POE）から電力が供給されていません。

【対処】　給電装置（POE）を電力供給可能状態に設定してください。
（各 POE 製品の説明書を確認してください）

【原因】　AC アダプターが、電源コネクタまたはコンセントに正しく接続されていません。

【対処】　AC アダプターを、電源コネクタまたはコンセントに正しく接続してください。

● CHECK ランプが橙色で点灯している

【原因】　本体に異常が発生しました。

【対処】　弊社の技術員または弊社が認定した技術員へ連絡してください。

● CHECK ランプが橙色で点滅している

【原因】　USB メモリのファイルシステムに異常があります。

【対処】　USB メモリを再フォーマットするか、または交換してください。

【原因】　USB ポートで過電流を検出しました。

【対処】　弊社の技術員または弊社が認定した技術員へ連絡してください。

1.2　本装置設定時のトラブル

本装置設定時のトラブルには、以下のようなものがあります。

● 以下のランプが点灯していない

• ETHERNET ランプ

• パソコンまたは HUB のリンクランプ

【原因】 スピード／全二重・半二重のモード設定が接続相手と合っていません。

【対処】 本装置のスピード／全二重・半二重のモード設定とパソコンまたは HUB の接続状態が合っているかを確認してください。本装置は ETHERNET ランプまたはステータスコマンド（show ether）で接続状態が確認できます。

☛ 参照 マニュアル「コマンドリファレンス」の「show ether」

【原因】 接続に誤りがあります。または、LAN ケーブルが断線しています。

【対処】 点灯していない場合は、LAN ケーブルが正しく接続されていないか、または断線している可能性があります。LAN ケーブルがパソコンまたは HUB と本装置に正しく差し込んであるかを確認し、それでも点灯しない場合は、別の LAN ケーブルに交換してください。

【原因】 ETHERNET ポートの AutoMDI/MDI-X の設定が on の状態で、ETHERNET ポートに接続しているパソコンまたは HUB の LAN ポートが AutoMDI/MDI-X となっている場合に、正常に接続できていません。

【対処】 本装置の ETHERNET ポートの AutoMDI/MDI-X の設定を off にします。または、ETHERNET ポートに接続しているパソコンまたは HUB の LAN ポートの設定を off にします。

【原因】 ケーブル長が最大ケーブル長を超えています。

【対処】 ツイストペアケーブルは、最大ケーブル長（100m）を超えないようにしてください。

【原因】 構成定義に矛盾があります。

【対処】 定義矛盾の内容はシステムログに表示されています。システムログを参照して、矛盾が発生している箇所を修正してください。

• WIRELESS ランプ

【原因】 無線 LAN モジュールまたは無線 LAN インタフェースの設定に誤りがあります。

【対処】 無線 LAN モジュールまたは無線 LAN インタフェースの設定を確認してください。
本装置の無線 LAN モジュールの動作状況は、show ieee80211 status コマンドで確認できます。
本装置の無線 LAN インタフェースの動作状況は、show wlan status コマンドで確認できます。
構成定義に矛盾がある場合、定義矛盾の内容はシステムログに表示されています。システムログを参照して、矛盾が発生している箇所を修正してください。

☛ 参照 マニュアル「コマンドリファレンス」の「show ieee80211 status」、「show wlan status」

• 本装置のすべてのランプ

【原因】 運用中に本装置のランプを消灯する設定になっています。

【対処】 運用中に本装置のランプを消灯する設定になっています。
ランプを点灯させる場合は、lamp mode コマンドで運用中にランプを点灯する設定に変更後、本装置を再起動してください。本装置が現在動作している設定は、show running-config コマンドで確認できます。

☛ 参照 マニュアル「コマンドリファレンス」の「show running-config」、「lamp mode」

● CHECK ランプ以外のすべてのランプが点滅している

【原因】 iamhere コマンドが実行されています。

【対処】 iamhere コマンドが実行されると、指定された時間 CHECK ランプ以外のすべてのランプが緑点滅します。点滅が終わるまで、しばらく待ってください。

☛参照 マニュアル「コマンドリファレンス」の「iamhere」

● telnet/ssh で本装置の IP アドレスを指定したがうまくつながらない

【原因】 パソコンの IP アドレスやネットマスクが間違っています。

【対処】 パソコンの設定で IP アドレスやネットマスクを設定している場合は、本装置と通信できる IP アドレスが設定されているかどうかを確認してください。

補足 パソコン側の IP 設定は、ipconfig コマンド（Windows 10 の場合）で確認できます。

【原因】 パソコンの ARP エントリの値がおかしくなっています。

【対処】 本装置と同じ IP アドレスを持つ機器と通信した直後に、パソコンの電源を落とさないまま本装置へ接続を変更した場合は通信できません。しばらく待つか、パソコンを再起動してください。

【原因】 本装置と同じ IP アドレスを持つ機器が接続されています。

【対処】 IP アドレスが重複している機器が LAN 上に存在すると、正しく通信できません。
本装置から設定を行うパソコン以外を接続している LAN ケーブルを外し、パソコンを再起動してください。

【原因】 本装置に IP アドレスが設定されていません。

【対処】 本装置に IP アドレスを設定してください。

【原因】 本装置の IP アドレスが変更されています。

【対処】 変更後の本装置の IP アドレスを指定してください。

【原因】 パソコンの IP アドレスを変更していません。

【対処】 本装置の IP アドレスを変更した場合、必ずパソコン側の IP アドレスもそれに合わせて変更します。
パソコンの IP アドレスを本装置と直接通信可能なアドレスに変更してください。また、ネットマスクを本装置に設定した値と同じ値に設定してください。このとき、DNS サーバの IP アドレスも忘れずに入力してください。

【原因】 サーバ機能が無効に設定されています。

【対処】 サーバ機能を有効に設定してください。

☛参照 マニュアル「コマンドリファレンス」の「serverinfo telnet」、「serverinfo ssh」

● 変更した本装置の IP アドレスがわからなくなった

【対処】 コンソールでログインして、構成定義を確認してください。

● 本装置に設定したパスワードがわからなくなった

【対処】 本装置をご購入時の状態に戻してください。それまでに設定した内容はすべて消えてしまいますので、最初から設定してください。

☛参照 「3 ご購入時の状態に戻すには」（P.18）

1.3　認証機能に関するトラブル

IEEE802.1X認証およびMACアドレス認証機能を利用する際のトラブルには、以下のようなものがあります。

● 認証ポートのリンクがアップしない（共通）

【原因】 認証機能の使用定義で、システム定義またはポート定義の一方のみが設定されています。

【対処】 本装置の認証機能は、装置全体での使用定義（dot1x use、macauth use）と、認証を行うポートに対する使用定義（wlan dot1x use、wlan macauth use）によって動作します。
認証機能を利用する場合は、両方の定義で認証を有効に設定してください。

参照 マニュアル「コマンドリファレンス」の「dot1x use」、「macauth use」、「wlan dot1x use」、「wlan macauth use」

【原因】 認証で使用するAAAグループ定義が定義されていません。

【対処】 AAAグループの定義を追加してください。

【原因】 認証ポートにVLANが定義されています。

【対処】 VLANの定義を削除してください。

【原因】 IEEE802.1X認証とMACアドレス認証を併用している場合で、以下の定義内容が異なっています。

- VLAN割り当て方式の設定
- 端末（Supplicant）に割り当てるデフォルトVLAN ID

【対処】 同じ設定にしてください。

● 認証が成功しない（共通）

【原因】 RADIUSサーバの設定が誤っています。

【対処】 システムログでRADIUSサーバとの通信が失敗していることを示すログが採取されていないかを確認し、該当するログが採取されている場合は、以下の点に注意してRADIUSサーバの設定を見直してください。

- RADIUSサーバのIPアドレスとRADIUSサーバまでの経路情報
- RADIUSサーバのシークレット情報
- RADIUSサーバ側で許容するRADIUSクライアントアドレス

【原因】 RADIUSサーバでSupplicantが登録されていません。

【対処】 RADIUSサーバ側で登録されたユーザ情報を確認してください。

【原因】 本装置にSupplicantに割り当てるVLAN IDと同一のVLAN IDを持つポートが存在しません。

【対処】 Supplicantに割り当てるVLAN IDと同一のVLAN IDを持つポートを設定してください。

● IEEE802.1X認証が成功しない

【原因】 RADIUSサーバで登録された認証アルゴリズムと異なるアルゴリズムをSupplicantが要求しています。

【対処】 RADIUSサーバで登録された認証アルゴリズムとSupplicant側の認証アルゴリズムを同一のアルゴリズムにしてください。

● MACアドレス認証が成功しない

【原因】 RADIUSサーバの認証種別が誤っています。

【対処】 RADIUSサーバの認証種別（EITHER/CHAP/PAP）を、本装置の設定に合わせて設定してください。

● 認証が成功しているのに、Supplicantがネットワークへアクセスできない（共通）

【原因】 Supplicantに割り当てるVLAN IDが設定されていません。

【対処】 認証サーバ（RADIUSサーバ）にSupplicantに割り当てるVLAN IDを設定してください。未設定の場合は、本装置のSupplicantに割り当てるデフォルトVLANの設定（wlan dot1x vid、wlan macauth vid）で定義されたVLAN IDが指定されたものとして動作します。

☛参照 マニュアル「コマンドリファレンス」の「wlan dot1x vid」、「wlan macauth vid」

【原因】 Supplicantに割り当てるVLAN IDが誤っています。

【対処】 認証サーバ（RADIUSサーバ）にSupplicantに割り当てるVLAN IDを設定してください。Supplicantに割り当てられたVLAN IDは、各認証の状態表示コマンド（show dot1x port、show macauth port）で確認できます。

☛参照 マニュアル「コマンドリファレンス」の「show dot1x port」、「show macauth port」

1.4　無線 LAN に関するトラブル

無線 LAN を利用する際のトラブルには、以下のようなものがあります。

● 無線 LAN 端末が接続できない、通信中に切断される

【原因】 無線 LAN 端末が本装置との通信圏外に位置しています。

【対処】 無線 LAN 端末付属のユーティリティなどを利用し、本装置が認識されているかを確認してください。

【原因】 無線 LAN 端末と本装置の無線通信モード、無線 LAN チャネルの設定が一致していません。

【対処】 無線 LAN 端末と本装置の無線通信モード、無線 LAN チャネルの設定を確認してください。
本装置の無線通信モード、無線 LAN チャネルの動作状況は、show ieee80211 status コマンドで確認できます。

☛ 参照 マニュアル「コマンドリファレンス」の「show ieee80211 status」

【原因】 無線 LAN 端末と本装置の SSID の設定が一致していません。

【対処】 無線 LAN 端末と本装置の SSID の設定を確認してください。
本装置の SSID の動作状況は、show wlan status コマンドで確認できます。

☛ 参照 マニュアル「コマンドリファレンス」の「show wlan status」

【原因】 無線 LAN 端末と本装置の認証・暗号化の設定が一致していない、または設定が不足しています。

【対処】 無線 LAN 端末と本装置の認証・暗号化の設定を確認してください。
共通鍵認証の場合は、WEP の設定に不足がないか、WPA-PSK、WPA2-PSK の場合は、WPA/WPA2 事前共有キー WPA3-SAE の場合は、SAE パスワード、WPA/WPA2/WPA3、暗号化モードの設定に不足がないかを確認してください。
本装置の認証・暗号化の動作状況は、show wlan status コマンドで確認できます。

☛ 参照 マニュアル「コマンドリファレンス」の「show wlan status」

【原因】 レーダ検出により設定と異なるチャネルで動作しています。

【対処】 W53/W56 の無線 LAN チャネルで運用している場合、レーダを検出する場合があります。レーダ検出時は現在運用中の無線 LAN チャネルは 30 分間使用できなくなり、ほかの無線 LAN チャネルに自動的に切り替わるため、無線 LAN 端末によっては切断されたり、接続できなくなる場合があります。切り替え後の無線 LAN チャネルを確認し、無線 LAN 端末の設定を変更してから再度接続してください。
本装置のレーダ検出状況は、システムログで確認できます。

☛ 参照 マニュアル「メッセージ集」

【原因】 使用する無線 LAN チャネルが、他 BSS のセカンダリチャネルで使用されています。

【対処】 使用する無線 LAN チャネルが他 BSS のセカンダリチャネルとして使用されていると BSS を開始しません。無線 LAN チャネルの設定を確認してください。

【原因】 PMF 機能を有効（必須）に設定しているが、無線 LAN 端末が PMF 機能をサポートしていない。

【対処】 PMF 機能を有効（オプション）、または無効に設定してください。

【原因】 PMF 機能を有効（必須）または有効（オプション）に設定しているが、無線 LAN 端末の PMF 有効時の挙動に不具合がある可能性があります。

【対処】 無線 LAN 端末のドライバソフトウェアや OS の最新化により、状況が改善するかを確認してください。状況が改善しない場合、PMF 機能を無効に設定してください。

☛参照 マニュアル「コマンドリファレンス」の「wlan wpa pmf mode」

● 無線 LAN の通信が不安定になる

【原因】 本装置周辺に設置されている無線 LAN 装置、または同一周波数帯の電波を発生する機器との電波干渉を起こしています。

【対処】 周辺アクセスポイント検出機能を使用し、周辺の無線 LAN アクセスポイントが使用しているチャネルの状況を確認してください。使用状況が少ない無線 LAN チャネルに変更することで改善される場合があります。また、2.4GHz 帯を利用する場合、同一の無線 LAN チャネル以外にも隣接する無線 LAN チャネルの使用も電波干渉の原因となりますので、使用状況の多い無線 LAN チャネルから離れたチャネルを使用して運用してください。また、電子レンジなど電波を発生する機器が近くにないことを確認してください。

【原因】 11b/11g の無線 LAN 装置が混在しています。

【対処】 無線通信モードを 11g または 11b/g に設定して運用している場合、周辺に無線通信モードが 11b の無線 LAN 装置が存在していると通信が不安定になる場合があります。
周辺に 11b で動作する無線 LAN 装置が存在する可能性がある場合は、11g プロテクションモードを設定してください。

【原因】 ショートガードインターバルが有効になっています。

【対処】 無線通信モードを 11a/n/ac、11a/n、11g/n または 11b/g/n に設定し、かつ、ショートガードインターバルを使用して運用している場合、反射波の影響によりスループットが低下する場合があります。ショートガードインターバルは、オフィスや家庭など比較的近い距離の通信に使用してください。

● 無線 LAN 端末が突然切断されてしまう

【原因】 同周波数帯の全無線 LAN チャネルでレーダを検出しました。

【対処】 W53/W56 で使用可能なすべての無線 LAN チャネルでレーダを検出した場合は、すべての無線 LAN 端末が切断されます。レーダ検出した無線 LAN チャネルのどれかが使用可能になるまで待ってから、再度無線 LAN 端末を接続してください。
本装置のレーダ検出状況は、システムログで確認できます。

☛参照 マニュアル「メッセージ集」

【原因】 本装置で手動スキャンが実行されました。

【対処】 すべてのチャネルの周辺アクセスポイント検出を手動で行う場合、すべての無線 LAN 端末が切断されます。周辺アクセスポイント検出が完了してから、再度無線 LAN 端末を接続してください。

● 無線 LAN の通信が遅い

【原因】 ほかの BSS と電波干渉が発生して、チャネルボンディング機能を有効にしている本装置が 20MHz の帯域幅で BSS を開始しています。

【対処】 本装置と他 BSS との間に電波干渉が発生しないように使用場所を変えるか、使用チャネルを変更してください。
他 BSS の動作状況は、show ieee80211 apscan コマンドで確認できます。

☛参照 マニュアル「コマンドリファレンス」の「show ieee80211 apscan」

【原因】 無線LAN端末の暗号アルゴリズムにTKIPを設定しているため、本装置とレガシーモードで接続しています。

【対処】 IEEE802.11n、IEEE802.11acおよびIEEE802.11ax規格では11n、11acおよび11ax通信にTKIP暗号化を使用することを禁止しています。
本装置ではTKIP暗号化を使用する無線LAN端末がアソシエートした場合、レガシーモードで接続します。11n、11acおよび11axで接続する場合は、無線LAN端末の暗号アルゴリズムをAESに変更してください。

【原因】 端末で必要なリンク速度が得られていません。

【対処】 以下の対処をしてください。

- 本装置の送信電力を大きくする
- 本装置と端末の距離を近づける
- 電子レンジなどのノイズ発生源を取り除く

【原因】 本装置周辺に設置されている無線LAN装置、または同一周波数帯の電波を発生する機器との電波干渉を起こしています。

【対処】 電波干渉により複数の端末で帯域を分けあう場合があります。以下の対処をしてください。

- 隣接無線LANアクセスポイントと離れたチャネルに変更する
- 同一チャネルを使用している他無線LANアクセスポイントの送信電力を低くする

● 無線LAN端末と通信できない

【原因】 PMF機能が有効（必須）または有効（オプション）の場合に、無線LAN端末のPMF有効時の挙動に不具合がある可能性があります。
本装置から送信する切断フレームが正しく処理されず無線LAN端末で破棄されると、本装置と無線LAN端末で無線接続状態の齟齬が発生し、本装置は切断済みの無線LAN端末からのフレームを破棄します。

【対処】 無線LAN端末のドライバソフトウェアやOSの最新化により、状況が改善するかを確認してください。
状況が改善しない場合、PMF機能を無効に設定してください。

1.5　SNMP に関するトラブル

SNMP 機能でネットワークの管理を行う際のトラブルには、以下のようなものがあります。

● SNMP ホストと通信ができない

【原因】 SNMP エージェントアドレスが正しく設定されていません。

【対処】 本装置のインタフェースに割り当てられている IP アドレスのどれかを SNMP エージェントアドレスとして設定してください。

【原因】 SNMP ホストの IP アドレスが正しく設定されていません。

【対処】 本装置にアクセスする SNMP ホストの IP アドレスを確認し、正しい IP アドレスを設定してください。

【原因】 コミュニティ名が正しく設定されていません（SNMPv1 または SNMPv2c 使用時）。

【対処】 本装置にアクセスする SNMP ホストのコミュニティ名を確認し、正しいコミュニティ名を設定してください。

【原因】 SNMP ユーザ名が正しく設定されていません（SNMPv3 使用時）。

【対処】 本装置にアクセスする SNMP ホストの SNMP ユーザ名を確認し、正しい SNMP ユーザ名を設定してください。

【原因】 認証プロトコルまたは認証パスワードが正しく設定されていません（SNMPv3 使用時）。

【対処】 本装置にアクセスする SNMP ホストの認証プロトコルまたは認証パスワードを確認し、正しい認証プロトコルまたは認証パスワードを設定してください。

【原因】 暗号プロトコルまたは暗号パスワードが正しく設定されていません（SNMPv3 使用時）。

【対処】 本装置にアクセスする SNMP ホストの暗号プロトコルまたは暗号パスワードを確認し、正しい暗号プロトコルまたは暗号パスワードを設定してください。

1.6　Web 画面に関するトラブル

WWW ブラウザから本装置を利用する際のトラブルには、以下のようなものがあります。

● 装置にログインできない

【原因】 CLI モードで運用中のため、ログインできません。

【対処】 Web 画面を使用するためには、工場出荷状態から Web 画面での初期セットアップを実施いただく必要があります。コンソールや SSH などから CLI による設定を実施している場合は、Web 画面での装置ログインはできません。

【原因】 ログイン中のユーザが存在するため、ログインできません。

【対処】 Web 画面へログインできるユーザ数は 1 つになります。また、ログアウト操作をせずに自動ログアウト機能が動作した場合など、装置内に古いセッションが残っている可能性があります。その場合、一旦ブラウザを終了させて再度ログイン操作を実施してください。

【原因】 メンバ AP へのログインはできません。

【対処】 集中管理モードはマスタ AP からのみ操作可能となるため、メンバ AP へはログインできません。

● 管理画面での操作で異常が発生した（以下のメッセージがポップアップされた）。

【原因】 管理画面が使用する管理情報に異常を検出しました。

【対処】 この異常は一時的に発生しており、装置を再起動することで復旧する可能性があります。

※AP としての通信動作には影響ありません。そのため通信影響の少ない時間帯に再起動することをお勧めします。

※再起動後も事象が改善しない場合は、弊社の技術員または弊社が認定した技術員へ連絡してください。

【対処】 この異常は退避いただいた設定管理情報を復元することでで復旧する可能性があります。

※AP としての通信動作には影響ありません。また復元時は装置の再起動が必要となります。そのため通信影響の少ない時間帯に復元することをお勧めします。

※万が一、設定管理情報を退避されていない場合は、装置を工場出荷状態に初期化後、再度初期セットアップ操作が必要となります。

☛参照 「3 ご購入時の状態に戻すには」 (P.18)

● ソフトウェア更新後に、更新前のソフトウェアの情報が画面表示されている

【原因】 ブラウザのキャッシュにより、更新前のソフトウェアの情報が画面表示される場合があります。

【対処】 ブラウザのキャッシュを削除してください。キャッシュ削除後、ブラウザ (タブもすべて) を一度終了させて再起動してください。

2　コマンド入力が正しくできないときには

コマンドで設定や操作を行ったときに正しくコマンドが入力できない場合は、まず、以下を参考に本装置の動作状況を確認してください。

2.1　シェルに関するトラブル

シェルで入力編集を行う際のトラブルには、以下のようなものがあります。

- **特定の［CTRL］+［α］キーが動作しない（［α］キー：任意のキー）**

【原因】 端末ソフトウェアが［CTRL］+［α］キーを処理してしまうため入力できません。

【対処】 端末ソフトウェアの設定で、［CTRL］+［α］キーを使用できるよう設定してください。
端末ソフトウェアに［ESC］キー（次に入力したキーをそのまま入力するキー）が用意されているのであれば、［ESC］キーを入力したあと［CTRL］+［α］キーを入力してください。

- **矢印キー（↑、↓、←、→）が動作しない**

【原因】 矢印キーをサポートしていない端末ソフトウェア（HyperTerminal など）を使用しています。

【対処】 矢印キーの代わりに［Ctrl］+［B］キーおよび［Ctrl］+［F］キーでカーソル移動、［Ctrl］+［P］キーおよび［Ctrl］+［N］キーでコマンド履歴移動を行ってください。

3　ご購入時の状態に戻すには

本装置を誤って設定した場合やトラブルが発生した場合は、本装置をご購入時の状態に戻すことができます。また、本装置を移設する場合は、ご購入時の状態に戻してから設定してください。

本装置をご購入時の状態に戻す手順については、「ご利用にあたって」を参照してください。

☛参照 マニュアル「ご利用にあたって」の「本装置をご購入時の状態に戻す」

付録 A エラー番号別の対処一覧

A.1　エラー番号の確認方法

1. 装置にログインします。

2. プロンプトが表示されたら、以下のコマンドを実行してエラーログ情報を表示します。

```
show logging error
```

3. 下記のエラーログが表示されます。

例）

```
2021/05/21 08:55:55 127.0.0.1 SR-M610AP1: rasmng: [85010000:00000000] Thermal error
```

ログ番号　　：エラーログの通し番号です。これまで発生したエラーがこの番号で 101 個まで記録されます。

エラー番号　　：エラー原因を示す 16 進数の番号が表示されます。

A.2　エラー番号別の対処

- **装置設置環境の確認が必要なエラー番号一覧**

  以下に一致するエラー番号が表示された場合は、装置が設置されている環境の温度を確認してください。

  ```
  85010000:00000000
  ```

- **初期化が必要なエラー番号一覧**

  以下に一致するエラー番号が表示された場合は、装置内のファイルが壊れている可能性があるので、reset clear コマンドによる初期化を実施してください。

  ```
  00000000:00000001
  ```

- **多発する場合に処置が必要なエラー番号一覧**

  以下に一致するエラー番号が何度も表示される場合は、弊社技術員または弊社が認定した技術員へ連絡してください。

  ```
  d4000000:00000000, 000000d0:00000000, 00000090:00000000
  ```

- **装置交換が必要なエラー番号一覧**

  以下に一致するエラー番号が多発し、かつ CHECK ランプが橙色で点灯となった場合は、装置交換が必要になります。弊社の技術員または弊社が認定した技術員へ連絡してください。

  ```
  85ff0010:********, 850c0002:********, 850e0010:********, 850d0001:********
  d20000**:********, 85070000:********
  ```

付録 B 障害診断機能による診断結果別の対処一覧

B.1　AP 診断での診断結果と対処方法

AP 診断による異常診断

診断内容	説明	対処方法
当該 AP との接続に失敗	マスタ AP は、当該 AP（メンバ AP）との間で定期的な情報交換を行います。本診断は、その定期的な情報交換を行うためのマスタ AP から当該 AP に対する SSH 通信に失敗したことを通知します。	集中管理のために必要なマスタ AP とメンバ AP 間の定期的な情報交換に失敗しました。マスタ AP から当該 AP（メンバ AP）への SSH 通信に失敗している可能性があります。 なお、マスタ AP で設定反映を実施した場合など、設定内容によっては ether ポートのリンクダウン / リンクアップを伴うために本事象が一時的に発生する可能性があります。この場合は問題ありません。本事象が長時間継続している場合には、以下の対処を実施してください。 【対処方法】 1. 疎通確認画面（メニューから「自装置保守」>「疎通確認 (ping)」を選択）で当該 AP の IP アドレスを入力してマスタ AP との ping 疎通状態を確認してください。 2. 当該 AP とマスタ AP 間の通信経路上で SSH 通信（TCP/22 番ポート）が遮断されていないか確認してください。 3. 当該 AP が正常に起動していることを確認してください。 4. 当該 AP に LAN ケーブルが正しく挿入され、ETHERNET ランプが白色に点灯しリンクアップしているか確認してください。 5. 本診断の直前に当該 AP で「装置故障検出」の診断結果が検出されていないか確認してください。「装置故障検出」の診断結果が検出されている場合、保守情報取得画面（メニューから「保守」>「保守情報取得」を選択）で当該 AP とマスタ AP の解析情報 (tech-support) を取得し、製品保守窓口へ連絡してください。

診断内容	説明	対処方法
当該APの情報取得に失敗	マスタAPは、当該AP（メンバAP）との間で定期的な情報交換を行います。本診断は、その定期的な情報交換に失敗したことを通知します。	集中管理のために必要なSR-M間の定期的な情報交換に失敗しました。 なお、装置の稼動状況により一時的に情報取得に失敗している可能性があります。この場合は問題ありません。本事象が継続している場合には、以下の対処を実施してください。 【対処方法】 1. 本診断結果が繰り返し検出される場合、対象APの再起動を行ってください。 ※APとしての通信動作には影響ありません。 そのため通信影響の少ない時間帯に再起動することをお勧めします。 2. 再起動を実施しても状態が変わらない場合、保守情報取得画面（メニューから「保守」>「保守情報取得」を選択）より当該APとマスタAPの解析情報(tech-support)を取得し、製品保守窓口へ連絡してください。
当該APの装置故障検出	当該APで装置故障の可能性を示すログ情報が確認されたことを通知します。	当該APで装置故障の可能性を示すログ情報が確認されました。 【対処方法】 保守情報取得画面（メニューから「保守」>「保守情報取得」を選択）より当該APの解析情報(tech-support)を取得し、製品保守窓口へ連絡してください。
スマートワイヤレスマネージャの管理情報異常	マスタAP内で管理しているスマートワイヤレスマネージャの管理情報に異常が確認されたことを通知します。	マスタAPがスマートワイヤレスマネージャ管理情報の保存に失敗した可能性があります。 【対処方法】 保守情報取得画面（メニューから「保守」>「保守情報取得」を選択）よりマスタAPの解析情報(tech-support)を取得し、製品保守窓口へ連絡してください。

診断内容	説明	対処方法
当該APの機種変更を検知	マスタAPの管理する機種と今回取得した当該AP（メンバAP）の機種に差分が確認されたことを通知します。スマートワイヤレスマネージャ利用時にはメンバAPのIPアドレスごとに機種を管理しているため、メンバAPの装置を交換する際には同一機種にする必要があります。	マスタAPの管理する機種と今回取得した当該AP（メンバAP）の機種に差分が検出されました。 スマートワイヤレスマネージャ利用時にはメンバAPごとに機種を管理しているため、メンバAPの装置を交換する際には同一機種にする必要があります。 【対処方法】 装置交換を行った当該メンバAPについて、交換前の機種と同じ機種であるか確認してください。 当該APの機種を変更する際には、AP一覧画面（メニューから「設定」>「AP一覧」を選択）で当該APの情報を削除したあと、交換後の機種で新規追加をしてください。
認証自動切替機能にともなうバックアップSSIDへの切り替え	認証自動切替機能により、当該APと認証サーバとの通信に異常が発生した際に利用できるSSID（バックアップSSID）が有効になったことを通知します。	当該APから認証サーバへの通信に異常が発生しました。認証自動切替機能が有効なため、認証サーバとの通信に異常が発生した際に利用できるSSID（バックアップSSID）を有効にしました。当該APと認証サーバの通信が復旧するまでの間は、端末をバックアップSSIDに接続し、無線LANをご利用ください。 当該APと認証サーバの通信を復旧させるために、下記対処方法を確認してください。 【対処方法】 1. 認証サーバの稼動状態を確認してください。 2. 当該APと認証サーバのping疎通状態を確認してください。 3. 当該APと認証サーバとの通信経路上でRADIUS通信（UDP/1812番ポート）が遮断されていないか確認をしてください。 ※当該APと認証サーバの通信復旧後、認証自動切替機能の切替動作設定が手動の場合には、認証自動切替復旧画面(メニューから「操作」>「認証自動切替復旧」を選択)でバックアップ稼動中になっているSSIDをすべて選択し、［一括操作］ボタンをおしてください。

診断内容	説明	対処方法
リンクインテグリティ機能による無線インタフェース閉塞	リンクイングリティ機能により、当該APで有線LANポートのリンクダウン、またはノード監視機能で指定している監視先ノードへのping通信異常が発生したことで、無線LANの電波を停止し、端末が接続できないように対処したことを通知します。	当該APで有線LANポートのリンクダウン、またはノード監視機能で指定している監視先ノードへのping通信異常が発生しました。リンクインテグリティ機能が有効なため、無線LANの電波を停止し、端末が接続できないように対処しました。 【対処方法】 1. 当該APにLANケーブルが正しく挿入されているか、ETHERNETランプが白色に点灯しリンクアップしているか確認してください。 2. ノード監視機能を有効としている場合は、当該APから設定された監視先ノードに対するping疎通状態を確認してください。

AP診断による注意診断

診断内容	説明	対処方法
当該APのソフトウェアバージョンがマスタAPと不一致	マスタAPと当該AP（メンバAP）のソフトウェアバージョンに不一致が確認されたことを通知します。スマートワイヤレスマネージャ利用時にはマスタAPとメンバAPのソフトウェアバージョンを一致させる必要があります。	マスタAPと当該AP（メンバAP）のソフトウェアバージョンが一致していません。スマートワイヤレスマネージャではマスタAPとメンバAPのソフトウェアバージョンを一致させる必要があります。 【対処方法】 すべてのAPのソフトウェアバージョンを一致させてください。ソフトウェア更新画面（メニューから「保守」>「ソフトウェア更新」を選択）から実施できます。
当該APの構成定義変更を検知	マスタAPの管理する構成定義と当該AP（メンバAP）の構成定義に差分が確認されたことを通知します。 スマートワイヤレスマネージャ利用時にはマスタAPでメンバAPの構成定義を変更する必要があります。メンバAPに対して直接、構成定義を変更した場合は、マスタAPで管理していた当該APの構成定義で上書きされます。	マスタAPの管理する構成定義と当該AP（メンバAP）で動作中の構成定義に差分が検出されました。 スマートワイヤレスマネージャでは、マスタAPがすべての管理APの構成定義を一括で管理し、メンバAPに構成定義を配布します。メンバAPに対して直接構成定義を変更された場合でも本診断は検出されますが、その場合マスタAPから構成定義を自動的に再配布するため次回の診断周期で解消されていれば問題ありません。 なお、マスタAPのソフトウェアバージョンと一致しないメンバAPでも、本診断が検出される場合があります。ソフトウェアバージョンが一致していない場合、以下の対処を実施してください。 【対処方法】 メンバAPのソフトウェアバージョンを一致させてください。ソフトウェア更新画面（メニューから「保守」>「ソフトウェア更新」を選択）から実施できます。

診断内容	説明	対処方法
外来波の検出（切り替え候補チャネルの復旧待ち）	運用中のチャネルで気象や航空レーダなどの外来波を検出され、DFS機能によりほかのチャネルへの切り替えを開始するも、切り替え候補のすべてのチャネルで外来波が検出されたため、切り替え候補チャネルの復旧待ちであることを通知します。 なお、本事象を確認したタイミングによってはすでに無線LAN通信が復旧している可能性もあります。 ※5GHz帯のW53、W56では、航空管制レーダや気象レーダとの電波干渉を回避するためのDFS(IEEE802.11h Dynamic Frequency Selection)機能が有効になっています。	運用中のチャネルで気象や航空レーダなどの外来波を検出したため、DFS機能によりほかのチャネルへの切り替えを試みましたが、その切り替え候補のすべてのチャネルで外来波が検出されたため、すべてのチャネルが使えない状態になりました。切り替え可能なチャネルが検出できるまでお待ちください。 なお、本事象を確認したタイミングによってはすでに無線LAN通信が復旧している可能性もあります。
当該APからNXconcierge管理ポータルへの接続失敗	当該APがNXconcierge管理ポータルへ送信に対し応答がない場合に通知します。	NXconcierge管理ポータルへの接続タイムアウトが発生しました。 【対処方法】 ●プロキシサーバを経由してNXconcierge管理ポータルに接続する運用構成の場合 1. プロキシサーバとの疎通確認をしてください。 2. 設定画面（メニューから「設定」>「AP一覧」）より当該APを選択し、デフォルトゲートウェイの設定を確認してください。 3. 設定画面（メニューから「設定」>「APグループ一覧」>「グループ設定」）よりNXconcierge連携設定のプロキシ設定が正しく設定されているか確認してください。 ●プロキシサーバを経由せずNXconcierge管理ポータルに接続する運用構成の場合 1. 当該APからインターネットに接続できることを確認してください。 2. 設定画面（メニューから「設定」>「AP一覧」）より当該APを選択し、デフォルトゲートウェイの設定を確認してください。

診断内容	説明	対処方法
当該APから NXconcierge管理ポータルへの接続失敗	NXconcierge管理ポータルからの応答メッセージで、ネットワーク機器の仮登録完了後、ネットワーク機器が仮登録（承認待ち）や、誤って機器が削除された場合などに通知します。	NXconcierge管理ポータルで当該APが機器登録されていない可能性があります。 【対処方法】 NXconcierge管理ポータルの管理者に、当該APの機器登録の状況を確認してください。
	NXconcierge管理ポータルからの応答メッセージで、当該APからログイン要求を行う際、当該APで指定したテナントキーが誤っている場合に、NXconcierge管理ポータルから通知します。	NXconcierge管理ポータルへの接続で使用するテナントキーに誤りがあります。 【対処方法】 1. 設定画面（メニューから「設定」>「共通設定」>「基本設定」）よりNXconcierge連携設定のテナントキーに正しい値を設定してください。 2. 事象が改善しない場合は、NXconcierge管理ポータルの管理者に、テナントキーの確認を依頼してください。
	NXconcierge管理ポータルからの応答メッセージで、NXconcierge管理ポータル側で内部異常が発生した場合に通知します。	NXconcierge管理ポータルからの応答で異常が通知されました。 【対処方法】 NXconciergeの保守サポート窓口へ連絡してください。
	プロキシサーバのアドレスが解決できないFQDNである場合に通知します。	プロキシサーバのアドレスが名前解決できていない可能性があります。 【対処方法】 1. 設定画面（メニューから「設定」>「APグループ一覧」>「APグループ設定」）よりNXconcierge連携設定のプロキシサーバのFQDNが正しく設定されているか確認してください。 2. プロキシサーバのFQDN設定を見直しても本診断が解消されない場合には、保守情報取得画面（メニューから「保守」>「保守情報取得」を選択）より当該APの解析情報(tech-support)を取得し、製品保守窓口へ連絡してください。

診断内容	説明	対処方法
当該APから NXconcierge管理ポータルへの接続失敗	NXconcierge管理ポータルがDNSで名前解決できない場合に通知します。	NXconcierge管理ポータルのアドレスの名前解決時にDNSサーバとの通信ができていない可能性があります。 【対処方法】 1. 設定画面（メニューから「設定」>「APグループ一覧」>「APグループ設定」）よりNXconcierge連携設定のDNSサーバが正しく設定されているかご確認ください。 2. 当該APにて、DNSサーバとの疎通確認をしてください。 3.DNSサーバおよび設定内容に問題がない場合には、保守情報取得画面（メニューから「保守」>「保守情報取得」を選択）より当該APの解析情報(tech-support)を取得し、製品保守窓口へ連絡してください。
	NXconcierge管理ポータル到達できない場合に通知します。	NXconcierge管理ポータルまでの経路上に問題がある可能性があります。 【対処方法】 ●プロキシサーバを経由してNXconcierge管理ポータルに接続する運用構成の場合 1. プロキシサーバとの疎通確認をしてください。 2. 設定画面（メニューから「設定」>「AP一覧」）より当該APを選択し、デフォルトゲートウェイの設定を確認してください。 3. 設定画面（メニューから「設定」>「APグループ一覧」>「グループ設定」）よりNXconcierge連携設定のプロキシ設定が正しく設定されているか確認してください。 ●プロキシサーバを経由せずNXconcierge管理ポータルに接続する運用構成の場合 1. 当該APからインターネットに接続できることを確認してください。 2. 設定画面（メニューから「設定」>「AP一覧」）より当該APを選択し、デフォルトゲートウェイの設定を確認してください。 上記でも問題が見当たらない場合には、保守情報取得画面（メニューから「保守」>「保守情報取得」を選択）より当該APの解析情報(tech-support)を取得し、製品保守窓口へ連絡してください。

診断内容	説明	対処方法
当該APから NXconcierge管理ポータルへの接続失敗	以下3つの場合が発生事象となり通知します。 1. プロキシのユーザ認証が誤っている場合。 2. プロキシサーバ使用時、接続先がDNS解決できない場合。 3. プロキシサーバ使用時、接続先とのコネクションに失敗する場合。	NXconcierge管理ポータルサーバへのアクセス時に異常を検出しました。 【対処方法】 1. プロキシサーバのユーザ認証をしている場合、設定画面（メニューから「設定」>「APグループ一覧」>「APグループ設定」）よりNXconcierge連携設定のプロキシサーバのユーザID、パスワードが正しく設定されているか確認してください。ユーザIDが正しい場合には、パスワードを再設定して確認してください。 2. プロキシサーバとNXconcierge管理ポータルとの接続に問題がないか確認してください。 3. プロキシサーバで、DNSサーバとの疎通確認をしてください。
	有効期限外の証明書が使用されていることを通知します。	NXconcierge管理ポータルへのアクセスで異常を検出しました。ルート証明書の有効期限切れの可能性があります。 【対処方法】 1. 当該APの現在時刻が正しいか確認してください。 2.NXconcierge管理ポータルへのアクセスのために必要な証明書の有効期限を確認してください。 APモニタリング画面（メニューから「モニタリング」>「APモニタリング」）にて当該APのAP名にマウスカーソルを合わせると装置の詳細情報が確認できます。 3. 上記でも問題が見当たらない場合には、保守情報取得画面（メニューから「保守」>「保守情報取得」を選択）より当該APの解析情報(tech-support)を取得し、製品保守窓口へ連絡してください。

診断内容	説明	対処方法
当該APから NXconcierge管理ポータルへの接続失敗	証明書破損の可能性があることを通知します。	NXconcierge管理ポータルへのアクセスで異常を検出しました。ルート証明書になんらかの問題がある可能性があります。 【対処方法】 1. 当該APで、ルート証明書を更新した場合、ルート証明書に問題がないか確認してください。 APモニタリング画面（メニューから「モニタリング」>「APモニタリング」）で当該APのAP名にマウスカーソルを合わせると装置の詳細情報が確認できます。ルート証明書の有効期限が正しく表示されているか確認してください。 2. ルート証明書の情報が正しく表示されていない場合、更新したルート証明書と共に保守情報取得画面（メニューから「保守」>「保守情報取得」を選択）より当該APの解析情報(tech-support)を取得し、製品保守窓口へ連絡してください。
	エージェント機能の内部異常などが発生したことを通知します。	当該APのNXconcierge管理ポータル連携機能で、内部異常が発生した可能性があります。 【対処方法】 保守情報取得画面（メニューから「保守」>「保守情報取得」を選択）より当該APの解析情報(tech-support)を取得し、NXconcierge管理ポータル保守窓口、製品保守窓口へ連絡してください。

AP診断による通知診断

診断内容	説明	対処方法
マスタAPから当該APに対する保守作業実施中	本診断は、マスタAPから当該AP（メンバAP）に対して「装置再起動、ソフトウェア更新、解析情報(tech-support)取得、定期ログ情報取得、構成定義設定」のいずれかの操作を実行中であるため、当該APのマスタAPとの情報交換処理機能が一時停止していることを通知します。	マスタAPから当該AP（メンバAP）に対して「装置再起動、ソフトウェア更新、解析情報(tech-support)取得、定期ログ情報取得、構成定義設定」のいずれかの保守作業を実施中であるため、当該APのマスタAPとの情報交換処理機能が一時停止しています。マスタAPから当該APに対する保守作業終了後に、自動的に復旧します。

診断内容	説明	対処方法
外来波の検出（切り替え候補チャネルの使用可否調査中）	運用中のチャネルで気象や航空レーダなどの外来波を検出され、DFS 機能により、ほかのチャネルへの切り替えを開始し、切り替え候補のチャネルに対して外来波が検出されないことを確認中（1 分間の無線 LAN 通信停止を伴う）であることを通知します。 なお、本事象を確認したタイミングによってはすでに無線 LAN 通信が復旧している可能性もあります。 ※5GHz 帯の W53、W56 では、航空管制レーダや気象レーダとの電波干渉を回避するための DFS(IEEE802.11h Dynamic Frequency Selection)機能が有効になっています。	運用中のチャネルで気象や航空レーダなどの外来波を検出したため、DFS 機能により、ほかのチャネルへの切り替えを開始し、切り替え候補のチャネルに対して外来波が検出されないことを確認中です（1 分間の無線 LAN 通信停止を伴います）。 なお、本事象を確認したタイミングによってはすでに無線 LAN 通信が復旧している可能性もあります。
外来波の検出（切り替え候補チャネルの復旧）	「外来波の検出（切り替え候補チャネルの復旧待ち）」の状態に対して、切り替え候補のチャネルが使用可能な状態になったことを通知します。	運用中のチャネルで気象や航空レーダなどの外来波を検出したため、DFS 機能によりほかのチャネルへの切り替えを試みましたが、その切り替え候補のすべてのチャネルで外来波が検出されたため、一度すべてのチャネルが使えない状態になりました。切り替え候補のチャネルが利用可能な状態となりました。
外来波の検出（チャネル切り替えの実施）	運用中のチャネルで気象や航空レーダなどの外来波を検出され、DFS 機能により他のチャネルへの切り替えが実施されたことを通知します。 ※5GHz 帯の W53、W56 では、航空管制レーダや気象レーダとの電波干渉を回避するための DFS(IEEE802.11h Dynamic Frequency Selection)機能が有効になっています。	運用中のチャネルで気象や航空レーダなどの外来波を検出したため、DFS 機能により、ほかのチャネルへの切り替えを実施しました。

診断内容	説明	対処方法
ノイズの検出（チャネル切り替えの実施）	運用中のチャネルで隣接チャネルからの干渉などのノイズが検出され、ノイズ回避機能により、ほかのチャネルへの切り替えが行われたことを通知します。	運用中のチャネルで隣接チャネルからの干渉などのノイズを検出したため、ノイズ回避機能により、ほかのチャネルへの切り替えを実施しました。

B.2　端末診断での診断結果と対処方法

端末診断による異常診断

診断内容	説明	対処方法
DHCP による IP アドレス割り当て失敗	リンクローカルアドレス (169.254.0.0 ～ 169.254.255.255) で通信しようとしている端末が存在することを通知します。 当該端末は正常に通信ができません。	当該端末がリンクローカルアドレス（169.254.0.0～169.254.255.255）で通信しようとしています。当該端末は正常に通信ができません。 【対処方法】 1.DHCP サーバの設定を確認し、IP アドレスが正しく払い出されているか確認してください。 2.DHCP サーバがない環境で、当該端末の DHCP 設定が有効になっています。端末に適切な IP アドレスを設定してください。
認証エラーによる接続失敗	WPA(PTK/GTK 鍵交換リトライオーバ) を示すシステムログが出力された場合に通知します。	鍵交換リトライオーバによる認証失敗を検出しました。 本診断結果が繰り返し検出される場合には、以下の対処を実施してください。 【対処方法】 EAPOL-KEY 応答待ち時間、および、EAPOL-KEY 再送回数の設定を増やしてください。設定画面（メニューから「設定」＞「SSID 一覧」＞「SSID 設定」＞「SSID 詳細設定」）から変更できます。
	認証失敗（WPA2-PSK 認証失敗）を示すシステムログが出力された場合に通知します。	WPA2-PSK の事前共有キー不一致による認証失敗を検出しました。 【対処方法】 端末で設定している WPA2-PSK の事前共有キーが AP の設定と合っているか確認してください。

診断内容	説明	対処方法
認証エラーによる接続失敗	認証失敗（VLAN 登録失敗）を示すシステムログが出力された場合に通知します。	認証サーバのデータベースに設定されている VLAN ID と当該 AP で設定されている VLAN ID 不一致による認証失敗を検出しました。 【対処方法】 1. 当該 AP の有線 LAN ポート、または、無線 LAN インタフェースに VLAN ID が正しく設定されているか確認してください。 2. 認証サーバのデータベースに設定されている VLAN ID と当該 AP で設定している VLAN ID が合っているか確認してください。当該 AP につきましては設定画面（メニューから「設定」＞「SSID 一覧」）で確認できます。
	認証失敗（MAC アドレス認証失敗）を示すシステムログが出力された場合に通知します。	MAC アドレス認証の失敗を検出しました。 【対処方法】 1. 認証サーバのデータベースに当該端末の MAC アドレスが設定されているか確認してください。 2. 当該端末でランダム化された MAC アドレスが使用されていないか確認してください。 プライバシー保護のためランダム化された MAC アドレスを利用する設定となっている場合があります。
	認証失敗（IEEE802.1X 認証失敗）を示すシステムログが出力された場合に通知します。	IEEE802.1X 認証の失敗を検出しました。 【対処方法】 1. パスワード認証の場合は、当該端末のパスワードが正しいか確認してください。 2. 証明書認証の場合は、当該端末に正しい証明書が設定されているか確認してください。 3, 認証サーバにユーザが正しく登録されていることを確認してください。
	認証失敗（WPA3-SAE 認証失敗）を示すシステムログが出力された場合に通知します。	WPA3-SAE の事前共有キー不一致による認証失敗を検出しました。 【対処方法】 当該端末で設定している WPA3-SAE の事前共有キーが当該 AP の設定と合っているか確認してください。

診断内容	説明	対処方法
認証エラーによる接続失敗	無線LAN端末が本装置と接続したときにPMFパラメタMFPC/MFPRの不整合を示すシステムログが出力された場合に通知します。	PMFパラメタ(MFPC/MFPR)の不整合を検出しました。 【対処方法】 1. 当該端末がPMF対応端末であるか確認してください。 2. 当該端末のPMF有効時の動作に不具合がある可能性があります。当該端末の無線LANモジュールのソフトウェアを更新してください。 3. 本装置のPMF機能を無効に変更して改善するか確認してください。改善した場合、PMF機能を無効で利用することをご検討ください。
	WPA3-SAE接続時にPMF無効の接続要求を示すシステムログが出力された場合に通知します。	WPA3-SAE接続時にPMF無効が指定されたことによる接続拒否を検出しました。 【対処方法】 1. 当該端末のPMF有効時の動作に不具合がある可能性があります。当該端末の無線LANモジュールのソフトウェアを更新してください。 2. 本装置の認証方式をWPA2-PSK、PMF機能を無効に変更して改善するか確認してください。改善した場合、PMF機能を無効で利用することをご検討ください。
	未サポートのManagement Group Cipher指定による接続拒否を示すシステムログが出力された場合に通知します。	PMF機能で未サポートのブロードキャスト管理フレーム暗号方式が指定されたことによる接続拒否を検出しました。 【対処方法】 1. 当該端末のPMF有効時の動作に不具合がある可能性があります。当該端末の無線LANモジュールのソフトウェアを更新してください。 2. 本装置の認証方式をWPA2-PSK、PMF機能を無効に変更して改善するか確認してください。改善した場合、PMF機能を無効で利用することをご検討ください。

診断内容	説明	対処方法
認証エラーによる接続失敗	PMF 機能動作不可の Pairwise Cipher 指定による接続拒否を示すシステムログが出力された場合に通知します。	PMF 機能で使用できないユニキャストフレーム暗号方式 (TKIP) が指定されたことによる接続拒否を検出しました。 【対処方法】 1. 当該端末の暗号方式から TKIP を除外してください。 2. 当該端末の PMF 有効時の動作に不具合がある可能性があります。当該端末の無線 LAN モジュールのソフトウェアを更新してください。 3. 本装置の PMF 機能を無効に変更して改善するか確認してください。改善した場合、PMF 機能を無効で利用することをご検討ください。

端末診断による注意診断

診断内容	説明	対処方法
IPアドレス未設定	APからIPアドレスが確認できない端末が存在することを通知します。 当該端末は正常に通信ができない可能性があります。	APから当該端末のIPアドレスが確認できません。当該端末は正常に通信ができない可能性があります。 【対処方法】 1. 当該端末のIPアドレスを正しく検出するためには、端末可視化機能が有効である必要があります。 設定画面（メニューから「設定」>「APグループ一覧」>「APグループ設定」>「その他」）より端末可視化機能が「使用する」に設定されている、かつ対象VLAN IDが正しく設定されているか確認してください。 2. DHCP運用の場合は、端末のDHCPクライアントを有効にしてください。 3. IPアドレスを固定的に設定する運用の場合は、適切なIPアドレスを端末に設定してください。
電波が弱くなったことによる性能低下	接続先APから見て受信電波強度(RSSI)が低下している端末が存在することを通知します。 この状態が続くと、端末の無線LAN通信性能が低下する可能性があります。	接続先APから見た当該端末の電波強度が弱くなっています。 この状態が続くと、端末の無線LAN通信性能が低下する可能性があります。 【対処方法】 1. 当該端末が接続しているAPとの距離を近づけてください。 2. 当該端末とAPの間に電波を遮断する遮蔽物がないか確認ください。 3. 当該端末の周辺に複数台のAPが設置されている場合、端末から遠い場所にあるAPに接続している可能性があります。端末から近い場所にあるAPに接続するために、当該端末の無線LANアダプタを一度、無効にして、そのあと有効にしてから接続しなおしてください。

診断内容	説明	対処方法
干渉発生による性能低下	電波干渉が発生している端末が存在することを通知します。 この状態が続くと、当該端末の無線LAN通信性能が低下する可能性があります。	周辺のAPと使用チャネルが重なっている、当該APまたは無線LAN端末付近に干渉源が存在している、または無線LAN端末の接続台数が多い可能性があります。 APモニタリング画面（メニューから「モニタリング」＞「APモニタリング」）でAPの使用チャネルおよび接続端末数が確認できます。 本診断が長時間継続している、および当該端末の無線LAN通信性能が著しく低下している場合には、以下の対処を実施してください。 【対処方法】 1. 当該APグループのチャネル最適化の実施を検討ください。 操作画面（メニューから「操作」＞「チャネル最適化実行」）からグループ単位で「即時実行」が実施できます。 また、APごとの使用チャネルの状況も確認できます。 ※チャネル最適化するAPグループに「即時実行」ボタンが表示されていない場合には、チャネル最適化を有効に設定変更する必要があります。設定画面（メニューから「設定」＞「APグループ一覧」＞「無線LAN設定」）から設定できます。 ※チャネル最適化を実施中はチャネルスキャンを実施するため、対象APグループのAPごとに一時的に端末を接続できなくなるため、接続端末の利用状況が少ない時間帯に実施してください。 2. チャネル最適化を実施しても本診断の検出状況が改善されない場合、および当該端末の無線LAN通信性能が低下している場合には、当該AP付近にある干渉源との距離を離すなど環境の改善を検討してください。

索引

SR-M トラブルシューティング

P3NK-7572-06Z0

発行日　2023年10月

発行責任　富士通株式会社