

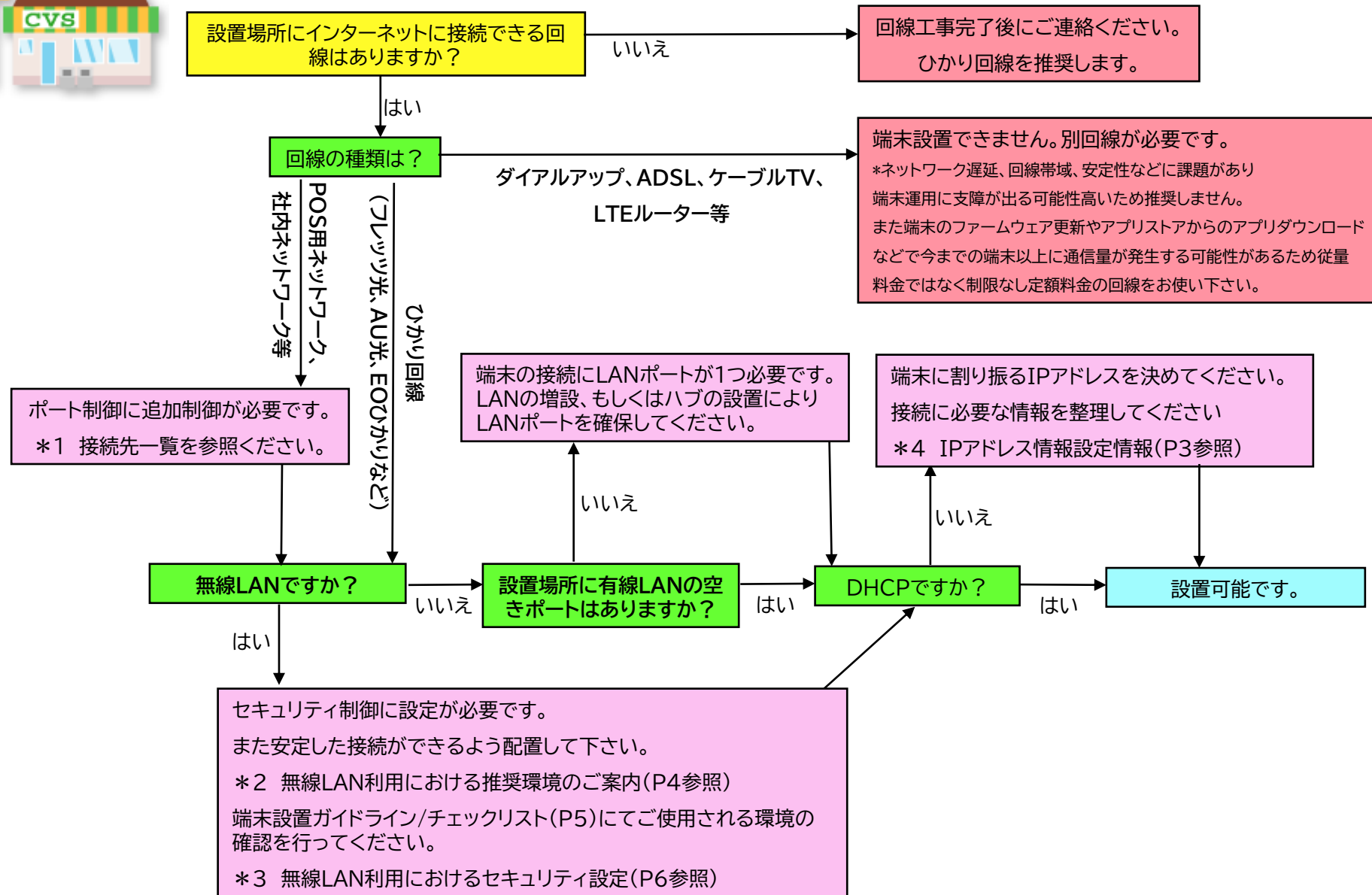
stera terminal unit (JT-VS1S) ネットワークについての確認事項

2025年4月2日 1.1版

パナソニック コネクト株式会社

JT-VS1S ネットワーク環境チェックシート及び注意事項

24



※本端末はIPv4の対応となります。IPv6は対応不可の端末でございます。ご注意願います。

IPアドレス情報設定情報

イーサネット設定	設定項目	設定の説明
IP設定（DHCP）	—	DHCPサーバがIPアドレスを自動的に付与します
IP設定（静的）⇒手動で設定することになります	IPアドレス	本機のローカルIPアドレス
	ゲートウェイ	接続環境のゲートウェイ
	ネットワークプリフィックス長	ネットワーク部のビット長。例えば255.255.255.0であれば24、255.255.255.240であれば28になります。
	DNS 1（プライマリ）	プロバイダ契約あるいは企業内のDNSサーバアドレス、有線DNSサーバともいいます
	DNS 2（セカンダリ）	代替DNSサーバともいいます（任意設定項目）

※JT-VS1SはAndroid OSのため、プロキシ設定がございますが、電子マネーの接続先の制約によりプロキシサーバー経由の通信はできません。ご注意くださいようお願い致します。

イーサネットデバイス設定

イーサネットデバイス
eth0

プロキシ設定
なし

IP設定
静的

IPアドレス
192.168.1.128

ゲートウェイ
192.168.1.1

ネットワークプリフィクス長
24

キャンセル 保存

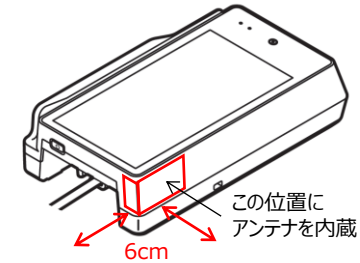
プロキシ設定
なし

プロキシ設定は「なし」で端末の設定をお願いいたします。

無線LAN利用における推奨環境のご案内

- Wi-Fiルーターはできるだけ壁や床に密着させず、見通しの良い場所に設置してください。
- Wi-FiルーターからJT-VS1S端末(以下、端末)の距離は1m以上、20m以内に設置してください
遠くなると電波が弱くなり、通信が不安定になる場合があります。
また、近すぎる場合には電波が強くなりすぎるため、通信が不安定になる場合があります。

- 端末側面のアンテナ内蔵位置から、金属等を概ね6cm以上離して設置してください。
アンテナの周囲に金属などがあると、電波が弱くなり通信が不安定になる場合があります。
端末は、右の〔図1〕の赤枠の箇所にアンテナが内蔵されています。

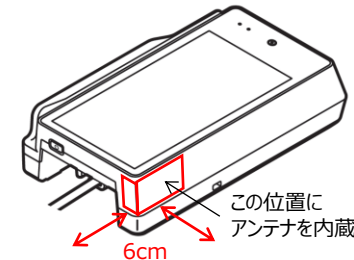


〔図1〕 JT-VS1S端末

- 5GHz Wi-Fiルーターを使用することを推奨します。
Wi-Fiで多く使用されている2.4GHzの周波数帯は、電子レンジ、Bluetooth機器、コードレス電話、リモコンなどの機器でも多く使用されております。また、自店舗内または近隣で使用しているWi-Fiのチャンネルが重複あるいは近接している場合も、接続が不安定になる可能性があります。
これらの機器の干渉が多い環境では、Wi-Fiルーターを5GHz対応のものに替えると、他の機器との干渉を避けられます。5GHz帯対応機器が比較的に少ないこと、「各チャンネル周波数が離れて設定されているため、同じ5GHz帯同士の機器でも干渉がおきにくい」という特長があります。
- 設置環境によって、以上のような改善が難しい場合は、有線LANでのご使用を推奨します。

端末設置ガイドライン/チェックリスト

- ☐ Wi-Fiルーターと端末は、同一部屋内への設置を推奨いたします。
- ☐ Wi-Fiルーターはできるだけ壁や床に密着させないようにして離し、見通しの良い場所に設置してください。
- ☐ JT-VS1S端末(以下、端末)とWi-Fiルーター間の距離は、(Wi-Fiルーター側の性能にもよりますが、目安として)
20m以内、且つ1m以上の位置となるよう設置下さい。
- ☐ 端末周囲に金属物など電波の妨げになるものを置かないでください。
金属物などの遮蔽物を置かざるを得ない場合、
端末のアンテナがある位置の端末側面から、**概ね6cm以上離すように**、設置してください。
- ☐ 2.4GHz帯は、チャンネル干渉が発生しやすく、お客様持ち込み機器との干渉も考えられるために使用を推奨致しません。
5GHz帯のご使用を推奨致します。
- ☐ 5GHz帯を利用する場合、W52の使用を推奨致します。
※W53、W56をご使用された場合、屋外のレーダー波の検出時に、DFSにより無線LAN通信が不安定になる可能性があるため
- ☐ 端末のWi-Fiアンテナバー表示が、設置場所で**必ず100%の状態であること**をご確認ください。



● **設置環境によって、以上のチェック項目を満足できない場合は、有線LANのご使用を強く推奨します。**

無線LAN利用におけるセキュリティ設定

●暗号化による対策

無線LAN利用の際には暗号化を実施してください。本端末は暗号化方式としては、WPA2-Personal/Enterpriseのみをサポートしています。プリシェアードキーを設定する際には、英数記号を組み合わせたランダムな文字列で最低20文字以上とすることを推奨します。

●アクセスポイントSSIDのステルス化による対策

SSIDをステルス化し外部から無線ネットワークの存在を秘匿化することを推奨します。

●端末認証による対策

悪意のある第三者による不正侵入を防止するためにアクセスポイントによるMACアドレスフィルタや認証機能等を利用する対策も推奨します。なお機器の故障交換時に再登録が必要になりますので、再登録の手順等の共有、文書化を推奨します。

●ネットワーク機器のファームウェアの最新化

アクセスポイントやルーター等のファームウェアは最新バージョンに更新してからお使い下さい。

●ネットワーク機器の管理者パスワードの変更

ネットワーク機器の管理者アカウントのパスワードは既知の場合が多いため運用前に必ず変更した上でお使いください。

●ネットワーク機器に接続している端末や機器同士のアクセス

ご使用されるネットワーク機器によっては接続されている機器または端末同士のアクセスを禁止する機能（例：プライバシーセパレータ）が搭載されています。

ネットワーク機器を経由して端末同士のアクセスを利用する機能※をご使用の際には端末同士のアクセスが行えるようネットワーク機器の当該機能の設定をOFFにしてお使いください。

※無線LAN経由でPOSと連動する場合

The background is a dark blue field filled with a repeating pattern of light blue geometric shapes, including squares, rectangles, and semi-circles. The shapes are arranged in a way that creates a sense of depth and movement. The text 'Panasonic' is in white, and 'CONNECT' is in a light blue color that matches the background pattern. The 'C' in 'CONNECT' is stylized with a circular cutout.

Panasonic CONNECT