NTT DATA

# 【CAFIS Arch】

# 無線 LAN 接続ガイドライン

－ 1.3 版－

**株式会社 NTT データ**

**IT サービス・ペイメント事業本部**

**カード＆ペイメント事業部**

## 変更履歴

| 項番 | 変更日 | 版数 | 内容 | 修正ページ | 旧ページ |
|---|---|---|---|---|---|
| 1 | 2016/04/26 | 1.0 | 新規作成 | − | − |
| 2 | 2017/01/19 | 1.1 | 別紙 2「動作確認済み無線 LAN ルータ機種一覧」を追記 | 10 | − |
| 3 | 2017/02/15 | 1.2 | 電子マネー利用時の留意事項を追記 | 4 | 4 |
| 4 | 2017/09/5 | 1.3 | 電子マネー利用時の留意事項を削除 | 4 | 4 |
| 5 | 2017/09/5 | 1.3 | PMF 設定利用時の留意事項を追記 | 7～8 | 7～8 |

# 目次

# 1. 無線 LAN 接続ガイドラインについて

## 1.1 無線 LAN 接続ガイドラインの目的

本ガイドラインは Arch 端末の無線 LAN 機能を用いたネットワーク構築に対して、下記 2 つの観点より必要な条件・注意事項を纏めたものになります。

① Arch 端末を用いた決済処理の安定稼働
② セキュリティ維持

## 1.2 CAFIS Arch とは

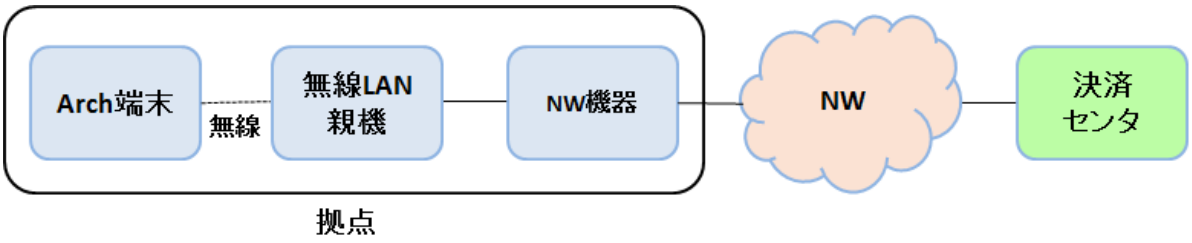
店頭の決済端末やタブレット POS 等に対してクレジット・デビット・電子マネー等の多様な決済機能を提供するクラウドサービス。シンクライアント方式を採用しているため、利用機能の追加や機能拡張が容易に行える点が特長になります。

## 1.3 無線 LAN 導入の前提条件

① Arch 端末を利用する際の回線は、原則、有線 LAN（モバイル端末の場合は LTE 通信）とします。有線 LAN・LTE 通信の使用が難しく、無線 LAN を利用する場合は、本ガイドラインに記載されている対策を講じる事が条件となります。
② 無線 LAN を利用する場合は、セキュリティ確保の観点から認証によるアクセス制限を可能かつ、端末間での通信制限が可能な環境に限り利用を認める事とします。また、一般のユーザに解放されている公衆無線 LAN のアクセスポイントに接続しての利用は原則禁止とします。
③ 無線 LAN の導入前、導入後でも、Arch 端末による決済に影響があると NTT データが判断した場合は、その問題点を解決しなければ、無線 LAN の利用を中止し、有線 LAN・LTE 通信に切り替えるなどの処置をしていただきます。

## 1.4 ネットワーク構成例

無線 LAN を用いたネットワーク構成例を下記に示します。




決済センタ～Arch 端末間はカード決済の安定稼働のために、冗長化することを推奨します。
なお、機器故障等により無線 LAN が使用不可となった場合に備えて、代替手段（交換用の親機準備、運用対処等）のご用意を推奨します。

### 1.5 用語

本書にて扱う用語の説明を以下に記します。

| 用語 | 意味・説明 |
|---|---|
| チャンネル(CH) | 無線通信にてデータ送受信の際に利用する周波数帯域の事です。 |
| DFS | 無線 LAN の通信が気象レーダー等に影響を与えないよう、無線 LAN アクセスポイント側が使用周波数帯を変更する機能です。既存の各種レーダーが使用する周波数帯域に対応しているアクセスポイントにて、レーダー等の干渉波を常にモニタし、検出し次第無線 LAN 通信を別のチャンネルに切り替えます。 |
| ステルス設定 | 無線LANのネットワーク ID(SSID)を隠蔽し、第三者から見えないようにする設定です。 |
| MAC アドレスフィルタリング | 端末ごとに固有の MAC アドレスをアクセスポイントに登録するアクセス制限方式で、第三者がアクセスポイントに接続できないようになります。 |

# 2. 無線 LAN のリスク

## 2.1 カード決済の安定稼働に対するリスク

① 設置環境により、壁等の障害物があったり、2.4Ghz 帯を使用する機器(例:電子レンジ)との干渉があると、通信状態が悪くなる可能性があります。

② 利用環境により、拠点内や近隣で使用している無線 LAN のチャンネルが重複又は近接している場合、安定した通信ができなくなる可能性があります。

③ 5Ghz 帯(W53、W56)を利用する場合、DFS により無線 LAN 通信が不安定になる可能性があります。

## 2.2 セキュリティ維持に対するリスク

① 暗号化されていないデータが傍受・解析されると情報漏洩の可能性があります。

# 3. 無線 LAN のリスク対策

## 3.1 無線通信環境の悪化による決済が不可となるリスクへの対策

### ① 設置環境

・壁等の障害物や、2.4GHz 帯を使用する機器（例：電子レンジ）による電波干渉の影響により、通信状態が悪くなる場合があるため、事前に現地調査を入念に行ってください。

・通信状態が悪い場合は、電波干渉の原因となっている物の排除や移動を検討してください。

### ② 干渉防止

・利用環境によっては、他の無線 LAN 機器が使用しているチャンネルと重複し、安定した通信ができなくなる場合があります。これを防止するためにアクセスポイント側でチャンネル/周波数固定設定を実施してください。

・特定のアクセスポイントに多くの端末を同時接続させると通信速度が落ちてしまうため、接続先のアクセスポイントやチャンネルを分散させる等の対応を行ってください。特に、端末初回起動時やアプリケーション更新時には大量データのダウンロードが必要となる場合があるため、アクセスポイントやチャンネルを分散して設定する事を推奨します。なお、Arch 端末以外の機器によるアクセスによって通信速度が落ちてしまう場合も、同様の対応を行ってください。

・アクセスポイントで PMF 設定を行っている場合に接続が安定しない場合、使用する機器の PMF 設定を確認の上、必要に応じて設定の見直しなどの対応を行ってください。

### ③ 環境の変化

・周辺に公衆無線アクセスポイントが多数設置された場合、安定した通信が確保できなくなる場合があります。このような場合は現地調査の実施を推奨します。また、通信状態が悪化し改善できない場合は有線 LAN への切替等を検討してください。

## 3.2 通信が盗聴・不正使用されるリスクへの対策

### ① 暗号化による対策

・無線通信時は暗号化を実施してください。なお使用する方式については WEP 等の脆弱性がある方式は使用せず、可能な限り強度の強い暗号化設定(WPA2-PSK)を利用してください。

・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 文字以上としてください。また、設定したプリシェアードキーは定期的に変更する事を推奨します。

### ② 決済用アクセスポイント 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してください。

### ③ 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、アクセスポイントによるフィルタ（MAC アドレスフィルタリング）や無線 LAN 機器に搭載されている認証機能等を必ず利用してください。

**④その他のセキュリティ対策**

・管理可能なネットワーク（企業内 LAN 等）を使用してください。
・ルータのファームウェアは定期的に最新バージョンに更新してください。
・SSID や VLAN 等を利用してネットワークを論理的又は物理的に分割し、盗聴・攻撃されないよう防御してください。（アクセスポイントに接続している無線機器間の通信を遮断することを推奨します）
・第三者からのアクセスを避けるために、アクセスポイントの利用範囲以外には極力電波が届かないように、電波の強度を調整することを推奨します。
・不正アクセス、DoS 攻撃、不正パケットの監視を推奨します。
・アクセスポイントへのログインは特定の責任者とし、パスワード変更を定期的に実施することを推奨します。（無線 LAN 親機の管理者の初期パスワードは既知の情報であるため、初期パスワードは必ず変更してください）

以上

## <別紙 1>必須／推奨対策一覧

無線 LAN 導入の際には以下の対策を実施願います。

■必須対策一覧

| 本書項番 | 対策一覧 | チェック欄 |
|---|---|---|
| 3.1 | 事前に現地調査を入念に行ってください。 | □ |
| 3.1 | 電波干渉の原因となっている物の排除や移動を検討してください。 | □ |
| 3.1 | アクセスポイント側でチャンネル／周波数固定設定を実施してください。 | □ |
| 3.1 | 接続先のアクセスポイントやチャンネルを分散させる等の対応を行ってください。 | □ |
| 3.2 | 無線通信時は暗号化を実施してください。なお仕様する方式については WEP 等の脆弱性がある方式は使用しないでください。 | □ |
| 3.2 | 管理可能なネットワーク（企業内 LAN 等）を使用してください。 | □ |
| 3.2 | SSID や VLAN 等を利用してネットワークを論理的または物理的に分割し、盗聴・攻撃されないよう防御してください。 | □ |
| 3.2 | 通信状態が悪化し改善できない場合は有線 LAN への切替等を検討してください。 | □ |
| 3.2 | 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してください。 | □ |
| 3.2 | 悪意のある第三者による不正侵入を防止するため、アクセスポイントによるフィルタ（MAC アドレスフィルタリング）や無線 LAN 機器に搭載されている認証機能等を使用してください。 | □ |

■推奨対策一覧

| 本書項番 | 対策一覧 | チェック欄 |
|---|---|---|
| 1.4 | 決済センタ～Arch 端末間はカード決済の安定稼働のために、冗長化することを推奨します。 | □ |
| 1.4 | 機器故障等により無線 LAN が使用不可となった場合に備えて、代替手段（交換用の親機準備、運用対処等）のご用意を推奨します。 | □ |
| 3.1 | 端末初回起動時やアプリケーション更新時には大量データのダウンロードが必要となる場合があるため、アクセスポイントやチャンネルを分散して設定してください。 | □ |
| 3.1 | 周辺に公衆無線アクセスポイントが多数設置された場合、安定した通信が確保できなくなる場合がありますので、このような場合は現地調査を実施してください。 | □ |
| 3.2 | 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 文字以上としてください。また、設定したプリシェアードキーは定期的に変更してください。 | □ |

## <別紙 2>動作確認済み無線 LAN ルータ機種一覧

弊社にて動作を確認した無線 LAN ルータを下記の通りです。

掲載の機種は NTT データにて独自に調査した結果であり、その内容を保証・サポートするものではございません。

■動作確認済み無線ルーター覧(2016 年 12 月現在)

| 項番 | メーカ名 | 機種名 |
|---|---|---|
| 1 | BUFFALO | AirStation HighPower Giga WXR-1900DHP2 |
| 2 | BUFFALO | AirStation Pro WAPM-1166D |
| 3 | NEC | Aterm WG2600HP2 PA-WG2600HP2 |
| 4 | I/O DATA | WN-AC1167R |
| 5 | I/O DATA | WHG-AC1750AL |
| 6 | NETGEAR | EX6200-100JPS |
| 7 | PLANEX | MZK-1200DHP2 |
| 8 | アライドテレシス | AT-TQ3200 |
| 9 | Cisco | WAP361-J-K9 |
| 10 | ELECOM | WRC-1167GHBK-S |