

QX-W2120AC アクセスコントローラ マニュアル訂正資料

All Rights Reserved

事前に NEC の書面による許可なく、本マニュアルをいかなる形式または方法で複製または配布することを禁止します。

商標

本マニュアルに記載されているその他の商標は、各社が保有します。

注意

本マニュアルの内容は、予告なく変更されることがあります。本マニュアルのすべての記述、情報、および推奨事項は、明示的か暗黙的にかかわらず、いかなる種類の保証の対象になりません。

本資料について

この資料は、以下に示す QX-W2120AC アクセスコントローラに関するマニュアルからの変更内容を記載しています。

マニュアル	マニュアル番号	内容
QX-W2120AC アクセスコントローラインストールレーションマニュアル	GVT-056158-001-00 1.12	システムのインストールについて説明しています。
QX-W2120AC アクセスコントローラオペレーションマニュアル	GVT-056160-001-00 1.32	機能の設定について説明しています。
QX-W2120AC アクセスコントローラコマンドマニュアル	GVT-056161-001-00 1.30	機能に関するコマンドについて説明しています。
QX-W2120AC アクセスコントローラ Web コンソール操作マニュアル	GVT-056162-001-00 1.3	Web コンソールからの装置設定、状態確認等についての操作を記述しています。

発行

2026年4月（3版）

改版履歴

版数	日付	内容
1.0	2026/1/27	初版発行
2.0	2026/2/17	#18215、#18298 を追加
3.0	2026/4/15	#16932 を追加

目次

1章 QX-W2120AC アクセスコントローラ インスタレーションマニュアル	6
2章 QX- W2120AC アクセスコントローラ オペレーションマニュアル	8
02-WLAN	9
9.6.3 802.11r の設定	9
18.9 クライアント高速キープアライブの設定	10
08-ACL and QoS	11
9.2 付録 B デフォルトプライオリティマップ	11
3章 QX- W2120AC アクセスコントローラ コマンドマニュアル	14
02-WLAN	15
8.2.1 ft enable	15
16.1.9 rrop anti-bmc upstream client-rate-limit pps	16
16.1.10 rrop client fast-keep-alive	17
09-セキュリティ	18
1.3.8 primary authentication (RADIUS scheme view)	18
1.3.16 secondary authentication (RADIUS scheme view)	19
4章 QX-W2120AC アクセスコントローラ Web コンソール操作マニュアル	20

1章 QX-W2120AC アクセスコントローラ インストールマニュアル

追加および変更はありません。

2章 QX-W2120AC アクセスコントローラ オペレーションマニュアル

02-WLAN

9.6.3 802.11r の設定

■管理情報

区分	管理番号
変更	#16932

■内容

変更前)

操作	コマンド	補足
3. FT を有効にする	ft enable	デフォルト：無効 FT が有効の時、WPA IE とローカル認証を無効にする必要があります。

変更後)

操作	コマンド	補足
3. FT を有効にする	ft enable	デフォルト：無効 FT が有効の時、WPA IE とローカル認証、WPA3、Enhanced-Open を無効にする必要があります。

18.9 クライアント高速キープアライブの設定

■管理情報

区分	管理番号
変更	#18215

■内容

変更前)

📄 メモ：

クライアント高速キープアライブの設定はソフトウェアバージョン 7.2.63 を含む以降のソフトウェアからサポートしています。

I.クライアント高速キープアライブの設定について

この機能により、AP は、クライアントに送信されたユニキャストパケットの確認応答状態に基づいて、クライアントがまだオンラインであるかどうかを確認できます。キープアライブ間隔 (*interval-value* パラメータで設定) 中に、3 グループのユニキャストパケットの確認応答が受信されなかった場合、AP はクライアントがオフラインであると判断し、クライアントへの接続を終了します。これにより、無線リソースの使用率が向上します。グループ内のユニキャストパケットの数は、*count-value* パラメータで設定します。

変更後)

📄 メモ：

クライアント高速キープアライブの設定はソフトウェアバージョン 7.2.63 を含む以降のソフトウェアからサポートしています。バージョン7.2.63より前のソフトウェアでも本機能はデフォルトのパラメータ値で動作していますが、無効にすることができません。

I.クライアント高速キープアライブの設定について

この機能により、AP は、クライアントに送信されたユニキャストパケットの確認応答状態に基づいて、クライアントがまだオンラインであるかどうかを確認できます。AP はユーザーデータを3つのグループに分けて個別にカウントします。キープアライブ間隔 (*interval-value* パラメータで設定) 中に、3 グループのユニキャストパケットの確認応答が受信されなかった場合、AP はクライアントがオフラインであると判断し、クライアントへの接続を終了します。これにより、無線リソースの使用率が向上します。グループ内のユニキャストパケットの数は、*count-value* パラメータで設定します。

08-ACL and QoS

9.2 付録 B デフォルトプライオリティマップ

■管理情報

区分	管理番号
変更	#18298

■内容

変更前)

表 9-2 デフォルトの dot11e-ip プライオリティマップ

プライオリティの入力値	dot1p-ip マッピング
dot11e	ip
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

表 9-3 デフォルトの dscp-ip プライオリティマップ

プライオリティの入力値	dscp-dot1p マッピング
dscp	dot1p
0 ~ 7	0
8 ~ 15	1
16 ~ 23	2
24 ~ 31	3
32 ~ 39	4
40 ~ 47	5
48 ~ 55	6
56 ~ 63	7

表 9-4 デフォルトの ip-dot1p、ip-dot11e、ip-dscp プライオリティマップ

プライオリティの入力値	ip-dot1p マッピング	ip-dot11e マッピング	dot1p-ip マッピング
ip	dot1p	dot11e	DSCP
0	1	1	0
1	2	2	8
2	0	0	16

3	3	3	24
4	4	4	32
5	5	5	40
6	6	6	48
7	7	7	56

変更後)

表 9-2 デフォルトの dot11e-ip プライオリティマップ

プライオリティの入力値		dot11e-ip マッピング
dot11e		ip
0		2
1		0
2		1
3		3
4		4
5		5
6		6
7		7

表 9-3 デフォルトの dscp-ip プライオリティマップ

プライオリティの入力値	dscp-ip マッピング
dscp	ip
0 ~ 7	0
8 ~ 15	1
16 ~ 23	2
24 ~ 31	3
32 ~ 39	4
40 ~ 47	5
48 ~ 55	6
56 ~ 63	7

表 9-4 デフォルトの ip-dot1p、ip-dot11e、ip-dscp プライオリティマップ

プライオリティの入力値	ip-dot1p マッピング	ip-dot11e マッピング	ip-dscp マッピング
ip	dot1p	dot11e	DSCP
0	1	1	0
1	2	2	8
2	0	0	16
3	3	3	24

4	4	4	32
5	5	5	40
6	6	6	48
7	7	7	56

3章 QX-W2120AC アクセスコントローラ コマンドマニュアル

02-WLAN

8.2.1 ft enable

説明

■管理情報

区分	管理番号
変更	#16932

■内容

変更前)

FT が有効の時、WPA IE と AP 自身での認証(client association location ap)を無効にする必要があります。

変更後)

FT が有効の時、WPA IE と AP 自身での認証(client association location ap)、WPA3、Enhanced-Open を無効にする必要があります。

16.1.9 rrop anti-bmc upstream client-rate-limit pps

■管理情報

区分	管理番号
変更	#18215-1

■内容

変更前)

例

AP が各クライアントから 1 秒あたりに受信できるブロードキャストパケットの最大数を System view で 1024 に制限します

<AC> system-view

[AC] rrop anti-bmc broadcast upstream client-rate-limit pps 1024

例

#AP グループ 1 の QX-W1120 の Radio1 のクライアントの高速キープアライブを有効にし、キープアライブ数を 300 に設定します。

<AP> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1120

[AC-wlan-ap-group-1-ap-model-QX-W1120] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1120-radio-1] rrop client fast-keep-alive 300

変更後)

例

AP が各クライアントから 1 秒あたりに受信できるブロードキャストパケットの最大数を System view で 1024 に制限します

<AC> system-view

[AC] rrop anti-bmc broadcast upstream client-rate-limit pps 1024

16.1.10 rrop client fast-keep-alive

■管理情報

区分	管理番号
変更	#18215-2

■内容

変更前)

📄 メモ :

rrop client fast-keep-alive コマンドはソフトウェアバージョン 7.2.63 を含む以降のソフトウェアからサポートしています。

説明

この機能により、AP は、クライアントに送信されたユニキャストパケットの確認応答状態に基づいて、クライアントがまだオンラインであるかどうかを確認できます。キープアライブ間隔 (*interval-value* パラメータで設定) 中に、3 グループのユニキャストパケットの確認応答が受信されなかった場合、AP はクライアントがオフラインであると判断し、クライアントへの接続を終了します。これにより、無線リソースの使用率が向上します。グループ内のユニキャストパケットの数は、*count-value* パラメータで設定します。

変更後)

📄 メモ :

クライアント高速キープアライブの設定はソフトウェアバージョン 7.2.63 を含む以降のソフトウェアからサポートしています。バージョン 7.2.63 より前のソフトウェアでも本機能はデフォルトのパラメータ値で動作していますが、無効にすることができません。

説明

この機能により、AP は、クライアントに送信されたユニキャストパケットの確認応答状態に基づいて、クライアントがまだオンラインであるかどうかを確認できます。AP はユーザーデータを 3 つのグループに分けて個別にカウントします。キープアライブ間隔 (*interval-value* パラメータで設定) 中に、3 グループのユニキャストパケットの確認応答が受信されなかった場合、AP はクライアントがオフラインであると判断し、クライアントへの接続を終了します。これにより、無線リソースの使用率が向上します。グループ内のユニキャストパケットの数は、*count-value* パラメータで設定します。

09-セキュリティ

1.3.8 primary authentication (RADIUS scheme view)

パラメータ

■管理情報

区分	管理番号
変更	#13634

■内容

変更前)

port-number: プライマリ RADIUS 認証サーバのサービスポート番号を UDP ポート番号で指定します。設定範囲は 1~65535 です。デフォルトは 1812 です。

key: セキュアなプライマリ RADIUS アカウンティングサーバの通信を行うために共有キーを設定します。

cipher: 暗号テキストを指定します。

変更後)

port-number: プライマリ RADIUS 認証サーバのサービスポート番号を UDP ポート番号で指定します。設定範囲は 1~65535 です。デフォルトは 1812 です。

key: プライマリ RADIUS 認証サーバとのセキュア通信のための共有鍵を指定します。

cipher: 暗号テキストを指定します。

1.3.16 secondary authentication (RADIUS scheme view)

パラメータ

■管理情報

区分	管理番号
変更	#13634

■内容

変更前)

port-number: セカンダリ RADIUS 認証サーバのサービスポート番号を UDP ポート番号で指定します。設定範囲は 1~65535 です。デフォルトは 1812 です。

key: セキュアなセカンダリ RADIUS アカウンティングサーバの通信を行うために共有キーを設定します。

cipher: 暗号テキストを指定します。

変更後)

port-number: セカンダリ RADIUS 認証サーバのサービスポート番号を UDP ポート番号で指定します。設定範囲は 1~65535 です。デフォルトは 1812 です。

key: セカンダリ RADIUS 認証サーバとのセキュア通信のための共有鍵を指定します。

cipher: 暗号テキストを指定します。

4 章 QX-W2120AC アクセスコントローラ Web コンソール操作マニュアル

追加および変更はありません。