AX2340S ソフトウェアマニュアル

訂正資料

Ver.1.0 以降対応版

AlaxalA

■はじめに

このマニュアルは，以下に示す AX2340S ソフトウェアマニュアルからの変更内容を記載しています。

マニュアル名	マニュアル番号	発行
AX2340S ソフトウェアマニュアル コンフィグレーションガイド Vol.1（Ver.1.0 対応）	AX23S-S001	2021 年 8 月
AX2340S ソフトウェアマニュアル コンフィグレーションガイド Vol.2（Ver.1.0 対応）	AX23S-S002	2021 年 8 月
AX2340S ソフトウェアマニュアル コンフィグレーションコマンドレファレンス（Ver.1.0 対応）	AX23S-S003	2021 年 8 月
AX2340S ソフトウェアマニュアル 運用コマンドレファレンス（Ver.1.0 対応）	AX23S-S004	2021 年 8 月
AX2340S ソフトウェアマニュアル メッセージ・ログレファレンス（Ver.1.0 対応）	AX23S-S005	2021 年 8 月
AX2340S ソフトウェアマニュアル MIB レファレンス（Ver.1.0 対応）	AX23S-S006	2021 年 8 月

■商標一覧

Cisco は，米国 Cisco Systems, Inc. の米国および他の国々における登録商標です。
Ethernet は，富士ゼロックス株式会社の登録商標です。
Microsoft は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
OpenSSL は，米国およびその他の国における米国 OpenSSL Software Foundation の登録商標です。
Python(R)は，Python Software Foundation の登録商標です。
RSA および RC4 は，米国およびその他の国における米国 EMC Corporation の登録商標です。
sFlow は，米国およびその他の国における米国 InMon Corp. の登録商標です。
ssh は，SSH Communications Security,Inc.の登録商標です。
UNIX は，The Open Group の米国ならびに他の国における登録商標です。
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または商標です。
イーサネットは，富士ゼロックス株式会社の登録商標です。
そのほかの記載の会社名，製品名は，それぞれの会社の商標もしくは登録商標です。

■マニュアルはよく読み，保管してください。

製品を使用する前に，安全上の説明をよく読み，十分理解してください。
このマニュアルは，いつでも参照できるよう，手近な所に保管してください。

■ご注意

このマニュアルの内容については，改良のため，予告なく変更する場合があります。

■発行

２０２１年　１１月　（第２版）　ＳＯＦＴ－ＡＭ－２６４５＿Ｒ１

■著作権

変更内容

■第 2 版の変更内容

表　変更内容

対象マニュアル名	追加・変更内容
コンフィグレーションガイド Vol.1	6　コンフィグレーション 6.4.1 コマンド一覧 8　ログインセキュリティと RADIUS/TACACS+ 8.2.4 RADIUS/TACACS+/ローカルを使用したコマンド承認 12　装置の管理 12.4 内蔵フラッシュメモリへ保存時の注意事項
運用コマンドレファレンス	4　コンフィグレーションとファイルの操作 erase startup-config

なお，単なる誤字・脱字などはお断りなく訂正しました。

目次

3　収容条件

3.1-1 NTP

追加

3.1-1 NTP

本装置での NTP サーバおよびクライアントの最大接続数を次の表に示します。

表 3-1-1　NTP サーバおよびクライアントの最大接続数

機能	最大接続数
ユニキャスト	50 クライアント※
ブロードキャスト	上限なし

注※上位 NTP サーバ，シンメトリック接続サーバ，下位クライアント数の合計です。

本装置での NTP コンフィグレーション設定数を次の表に示します。

表 3-1-2　コンフィグレーション設定数

機能	最大設定数
ユニキャストクライアント(ntp server)	10 ※
シンメトリック接続(ntp peer)	10 ※
ブロードキャストサーバ(ntp broadcast)	10 ※

注※ntp server，ntp peer，ntp broadcast の設定できるエントリ数の合計は最大 10 です。

6　コンフィグレーション

6.4 コンフィグレーションの編集方法

6.4.1 コマンド一覧

追加

表 6–2　運用コマンド一覧［Ver.1.0.B 以降］

表 6–2　運用コマンド一覧

コマンド名	説明
show running-config	ランニングコンフィグレーションを表示します。
show startup-config	スタートアップコンフィグレーションを表示します。
copy	コンフィグレーションをコピーします。
erase configuration	ランニングコンフィグレーションの内容を初期導入時のものに戻します。
erase startup-config	スタートアップコンフィグレーションファイルの内容を初期導入時の状態に戻します。
show file	ローカルまたはリモートサーバ上のファイルの内容と行数を表示します。
：	：

8　ログインセキュリティと RADIUS/TACACS+

8.2 RADIUS/TACACS+の解説

8.2.4 RADIUS/TACACS+/ローカルを使用したコマンド承認

追加

表 8–10　コマンドクラス一覧［Ver.1.0.B 以降］

表 8–10　コマンドクラス一覧

コマンドクラス	許可コマンド	制限コマンド
root 全コマンド無制限クラス	従来どおりすべてのコマンド（マニュアル未掲載のデバッグコマンドを含む）	なし
allcommand 運用コマンド無制限クラス	すべての運用コマンド"all"	なし（マニュアル未掲載のデバッグコマンドは不可）
noconfig コンフィグレーション変更制限クラス（コンフィグレーションコマンド指定も制限します）	制限以外の運用コマンド	"config, copy, erase configuration, erase startup-config"
nomanage ユーザ管理コマンド制限クラス	制限以外の運用コマンド	"adduser, rmuser, clear password, password, killuser"
noenable 装置管理者モードコマンド制限クラス	制限以外の運用コマンド	"enable"

12　装置の管理

12.4 内蔵フラッシュメモリへ保存時の注意事項

追加

表 12–7　内蔵フラッシュメモリへの書き込み契機になる主な運用コマンド[Ver.1.0.B 以降]

表 12–7　内蔵フラッシュメモリへの書き込み契機になる主な運用コマンド

分類	運用コマンド
コンフィグレーションとファイルの操作	copy，cp，rm，delete，undelete，squeeze，erase configuration，erase startup-config
ログインセキュリティと RADIUS/TACACS+	adduser，rmuser，password，clear password
SSH	set ssh hostkey，erase ssh hostkey
：	：

19　高機能スクリプト

19.1 解説

19.1.4 スクリプト使用時の注意事項

追加

(4) 運用コマンド set clock コマンドを使用する際の注意

(4) 運用コマンド set clock コマンドを使用する際の注意

タイマ監視（cron タイマ）は装置の時刻を用いて管理しているので，運用コマンド set clock で時刻を変更した場合，時刻変更した直後は，変更した時間によってイベント発生の周期が変わったり，短い時間に複数回のイベントが発生したりする場合があります。なお，それ以降は，タイマ監視の周期に従って，正常にイベント発生するようになります。

20　イーサネット

20.2 イーサネット共通の解説

20.2.2 フレームフォーマット

削除

(3) 受信フレームの廃棄条件

---

(3) 受信フレームの廃棄条件

次に示すどれかの条件によって受信したフレームを廃棄します。

~~・フレーム長がオクテットの整数倍でない~~

・受信フレーム長（DA～FCS）が 64 オクテット未満，または 1523 オクテット以上
ただし，ジャンボフレーム選択時は，指定したフレームサイズを超えた場合

・FCS エラー

・接続インタフェースが半二重の場合に，受信中に衝突が発生したフレーム

23　MAC アドレス

23.1 解説

23.1.7 MAC アドレステーブルのクリア

削除

表 23–3　MAC アドレステーブルをクリアする契機

表 23–3　MAC アドレステーブルをクリアする契機

契機	説明
:	:
GSRP のマスタ／バックアップ切り替え	~~［本装置が GSRP aware として動作］~~ GSRP スイッチがマスタ状態になった時に送信される GSRP Flush request フレームを受信した場合，MAC アドレステーブルをクリアします。
	~~［GSRP と Ring Protocol を併用しているネットワーク構成で本装置がリングノードとして動作］~~ ~~Ring Protocol と併用している装置がマスタ状態になった時に送信するフラッシュ制御フレームを受信した場合，MAC アドレステーブルをクリアします。~~
Ring Protocol による経路の切り替え	~~［本装置がマスタノードとして動作］~~ ~~経路切り替え時に MAC アドレステーブルをクリアします。~~
	~~［本装置がトランジットノードとして動作］~~ 経路切り替え時にマスタノードから送信されるフラッシュ制御フレームを受信した場合，MAC アドレステーブルをクリアします。 フラッシュ制御フレーム受信待ち保護時間のタイムアウト時に MAC アドレステーブルをクリアします。
	多重障害監視機能適用時，バックアップリングの切り替え／切り戻しに伴い共有ノードから送信されるフラッシュ制御フレームを受信した場合，MAC アドレステーブルをクリアします。
	経路切り替え時にマスタノードから送信される隣接リング用フラッシュ制御フレームを受信した場合，MAC アドレステーブルをクリアします。
:	:

25　VLAN 拡張機能

25.1 VLAN トンネリングの解説

25.1.3 VLAN トンネリング使用時の注意事項

変更

(3) トランクポートのネイティブ VLAN について

変更前

(3) トランクポートのネイティブ VLAN について

VLAN トンネリングのトランクポートは VLAN Tag をスタックするポートとなりますが，ネイティブ VLAN では VLAN Tag をスタックしません。本装置からフレームを送信するときはアクセスポートと同様に動作して，フレームを受信するときは Untagged フレームだけを扱います。ほかの VLAN と異なる動作となるので，VLAN トンネリング網のバックボーン回線の VLAN としては使用できません。VLAN トンネリングを使用する場合，トランクポートのネイティブ VLAN は suspend 状態とすることをお勧めします。

：

変更後

(3) トランクポートのネイティブ VLAN について

VLAN トンネリングのトランクポートは VLAN Tag をスタックするポートとなりますが，ネイティブ VLAN では VLAN Tag をスタックしません。ほかの VLAN と異なる動作となるので，VLAN トンネリング網のバックボーン回線の VLAN としては使用できません。VLAN トンネリングを使用する場合，トランクポートのネイティブ VLAN は suspend 状態にしてください。

：

32　DHCP サーバ機能

32.1 解説

変更

変更前

DHCP サーバ機能は，DHCP クライアントに対して，IP アドレスやオプション情報などを動的に割り当てるための機能です。この節では，本装置の DHCP サーバ機能の仕様および動作内容を説明します。

変更後

本製品では，DHCP サーバ機能は将来サポートする予定です。

DHCP サーバ機能は，DHCP クライアントに対して，IP アドレスやオプション情報などを動的に割り当てるための機能です。この節では，本装置の DHCP サーバ機能の仕様および動作内容を説明します。

1　フィルタ

1.1 解説

1.1.7 フィルタ使用時の注意事項

変更

(5) ほかの機能との同時動作

変更前

(5) ほかの機能との同時動作

(a) sFlow 統計併用時のフィルタ統計

送信側フィルタを VLAN インタフェースに適用して，かつ該当 VLAN に属するイーサネットインタフェースで sFlow 統計の送信サンプリングをしている場合，該当フィルタの統計情報が多く加算されることがあります。

変更後

(5) ほかの機能との同時動作

(a) sFlow 統計，およびポートミラー併用時のフィルタ統計

送信側フィルタを VLAN インタフェースに適用して，かつ該当 VLAN に属するイーサネットインタフェースで sFlow 統計の送信サンプリングをしている場合，およびポートミラーで送信ミラーのモニターポートに指定している場合，該当フィルタの統計情報が多く加算されることがあります。

5　レイヤ 2 認証

5.1 概要

5.1.1 レイヤ 2 認証種別

削除

表 5–1　レイヤ 2 認証でサポートする機能

表 5-1　レイヤ 2 認証でサポートする機能

レイヤ 2 認証	認証モード	概要
IEEE802.1X	ポート単位認証	物理ポート~~またはチャネルグループ~~に対して認証を制御します。一つの物理ポート~~または一つのチャネルグループ~~が一つの認証単位となります。また，ポート単位認証には次に示す三つの認証サブモードがあり，それぞれ認証動作が異なります。 1. シングルモード 一つの認証単位に一つの端末だけ認証して接続します。最初に認証した端末以外の端末から認証要求があると，そのポートの認証状態は未認証状態に戻ります。 2. マルチモード 一つの認証単位に複数端末の接続を許容します。最初に認証した端末以外の端末は認証しません。 3. 端末認証モード 一つの認証単位に複数端末の接続を許容し，端末ごとに認証を行います。

5.2 レイヤ 2 認証と他機能との共存について

5.2.1 レイヤ 2 認証と他機能との共存

変更

表 5-4　他機能との共存仕様

変更前

表 5-4　他機能との共存仕様

レイヤ 2 認証機能	機能名		共存仕様
IEEE802.1X	リンクアグリゲーション		LACP リンクアグリゲーションのチャネルグループで使用できません。
	MAC アドレステーブル	MACアドレス学習抑止	VLAN およびその VLAN を設定したポートで同時に使用できません。
		スタティック MAC アドレス	スタティック MAC アドレスを設定したポートでは使用できません。

変更後

表 5-4　他機能との共存仕様

レイヤ 2 認証機能	機能名		共存仕様
IEEE802.1X	リンクアグリゲーション		認証ポートとして，チャネルグループのポートは使用できません。
	MAC アドレステーブル	MACアドレス学習抑止	VLAN およびその VLAN を設定したポートで同時に使用できません。
		スタティック MAC アドレス	スタティック MAC アドレスを設定したポートでは使用できません。

5.3 レイヤ 2 認証共通の機能

削除

レイヤ 2 認証共通の機能とその機能を設定するに当たり前提となる項目について説明します。

・設定時の認証単位（ポート~~またはチャネルグループ~~単位に実施）

5.3.1 認証前端末の通信許可

削除

(1) 認証専用 IPv4 アクセスリスト

(1)　認証専用 IPv4 アクセスリスト

：

［認証専用 IPv4 アクセスリスト設定時の注意］

コンフィグレーションコマンド authentication ip access-group を設定する場合，次の点に注意してください。

・指定できる認証専用 IPv4 アクセスリストは 1 個だけです。認証対象となるすべてのポートに，コンフィグレーションコマンド authentication ip access-group で同一の設定をしてください。なお，チャネルグループに所属しているポートには設定できません。

・認証専用 IPv4 アクセスリストで設定できるフィルタ条件が収容条件を超えている場合，収容条件内のものだけ設定されます。

・コンフィグレーションコマンド permit または deny によって次のフィルタ条件が指定されても，適用されません。

　・tcp ポートの range 指定

　・udp ポートの range 指定

　・user-priority

　・vlan

・設定した条件以外のパケット廃棄設定は，本設定の収容条件数には含まれません。各認証プログラムで条件以外のパケット廃棄設定が暗黙に設定されます。

~~・認証専用 IPv4 アクセスリストのフィルタ条件としてコンフィグレーションコマンド permit ip host <ip address>に認証端末の IP アドレスを設定した場合，コンフィグレーションコマンド authentication arp-relay を設定しなくても，認証前の端末から送信される ARP パケットは疎通します。~~

・Web 認証専用 IP アドレスは認証専用 IPv4 アクセスリストのフィルタ条件の宛先 IP アドレスの対象外となるため，宛先 IP アドレスとして Web 認証専用 IP アドレスが含まれる設定をした場合でも，Web 認証専用 IP アドレスでのログイン操作ができます。

5.3.4 認証済み端末のポート間移動

削除

図 5-6　認証済み端末のポート間移動例

ケース 2：

移動先の認証対象ポートで，次の条件を満たしている場合に異なる VLAN への移動と見なします。

・コンフィグレーションコマンド switchport mac vlan で異なる VLAN ID が設定されている

~~また，動的に MAC VLAN の VLAN ID が登録されていない場合に IEEE802.1X の端末が移動するときは，異なる VLAN への移動と見なします。~~

変更

表 5-12　IEEE802.1X でのポート間移動時の動作

表 5-14　MAC 認証でのポート間移動時の動作（固定 VLAN モード）

表 5-15　MAC 認証でのポート間移動時の動作（ダイナミック VLAN モード）

表 5-15 の次にある［ポート移動時の注意］

変更前

表 5-12　IEEE802.1X でのポート間移動時の動作

ケース	移動先ポート	VLAN	ユーザ認証状態	移動前ポートの MAC アドレステーブル	移動前ポートの認証状態	移動後の通信可否
1	認証対象ポート	同一 VLAN	移動後，再認証操作	ポート情報が更新	移動前の認証解除	移動後に認証されるまで通信不可
2	認証対象ポート	別 VLAN	移動後，再認証操作	未更新	認証状態が残る	移動後に認証されるまで通信不可
3	認証対象外ポート	同一 VLAN	認証状態が残る	未更新	認証状態が残る	通信不可
4	認証対象外ポート	別 VLAN	認証状態が残る	未更新	認証状態が残る	通信可

表 5-14　MAC 認証でのポート間移動時の動作（固定 VLAN モード）

ケース	移動先ポート	VLAN	ユーザ認証状態	移動前ポートの MAC アドレステーブル	移動前ポートの認証状態	移動後の通信可否
1	認証対象ポート	同一 VLAN	認証が継続される	ポート情報が更新	継続	通信可
2	認証対象ポート	別 VLAN	移動後，再認証※	削除※	移動前の認証解除※	移動後に認証されるまで通信不可※
3	認証対象外ポート	同一 VLAN	認証状態が残る	未更新	認証状態が残る	通信不可

ケース	移動先ポート	VLAN	ユーザ認証状態	移動前ポートの MAC アドレステーブル	移動前ポートの認証状態	移動後の通信可否
4	認証対象外ポート	別 VLAN	認証状態が残る	未更新	認証状態が残る	通信可

注※

認証済み端末からポート移動後にブロードキャスト ARP パケットが送信された場合の　動作です。ブロードキャスト ARP パケット以外のパケットでは，認証解除されないで認証状態が残ります。

表 5-15　MAC 認証でのポート間移動時の動作（ダイナミック VLAN モード）

ケース	移動先ポート	VLAN	ユーザ認証状態	移動前ポートの MAC アドレステーブル	移動前ポートの認証状態	移動後の通信可否
1	認証対象ポート	同一 VLAN	認証が継続される	ポート情報が更新	継続	通信可
2	認証対象ポート	別 VLAN	認証解除※	削除※	移動前の認証解除※	移動後に認証されるまで通信不可※
3	認証対象外ポート	同一 VLAN	認証状態が残る	未更新	認証状態が残る	通信不可
4	認証対象外ポート	別 VLAN	認証状態が残る	未更新	認証状態が残る	通信可

注※

認証済み端末からポート移動後にブロードキャスト ARP パケットが送信された場合の動　作です。ブロードキャスト ARP パケット以外のパケットでは，認証解除されないで認証状態が残ります。

［ポート移動時の注意］

MAC ポートの VLAN に所属している認証済みの端末が，同一 VLAN で，かつ MAC ポート以外の認証ポートに移動した場合，移動元のポートでの認証状態は解除されません。また，移動先のポートで該当端末の通信はできないため，次のどちらかの運用コマンドを使用して，該当端末を認証解除する必要があります。

・Web 認証：clear web-authentication auth-state コマンド

・MAC 認証：clear mac-authentication auth-state コマンド

変更後

表 5-12　IEEE802.1X でのポート間移動時の動作

ケース	移動先ポート	VLAN	ユーザ認証状態	移動前ポートの MAC アドレステーブル	移動前ポートの認証状態	移動後の通信可否
1	認証対象ポート	同一 VLAN	移動後，再認証操作	削除	移動前の認証解除	移動後に認証されるまで通信不可
2	認証対象ポート	別 VLAN	移動後，再認証操作	削除	移動前の認証解除	移動後に認証されるまで通信不可
3	認証対象外ポート	同一 VLAN	認証状態が残る	未更新	認証状態が残る	通信不可
4	認証対象外ポート	別 VLAN	認証状態が残る	未更新	認証状態が残る	通信可

表 5-14　MAC 認証でのポート間移動時の動作（固定 VLAN モード）

ケース	移動先ポート	VLAN	ユーザ認証状態	移動前ポートの MAC アドレステーブル	移動前ポートの認証状態	移動後の通信可否
1	認証対象ポート	同一 VLAN	認証が継続される	ポート情報が更新	継続	通信可
2	認証対象ポート	別 VLAN	移動後，再認証	削除	移動前の認証解除	移動後に認証されるまで通信不可※
3	認証対象外ポート	同一 VLAN	認証状態が残る	未更新	認証状態が残る	通信不可
4	認証対象外ポート	別 VLAN	認証状態が残る	未更新	認証状態が残る	通信可

表 5-15　MAC 認証でのポート間移動時の動作（ダイナミック VLAN モード）

ケース	移動先ポート	VLAN	ユーザ認証状態	移動前ポートの MAC アドレステーブル	移動前ポートの認証状態	移動後の通信可否
1	認証対象ポート	同一 VLAN	認証が継続される	ポート情報が更新	継続	通信可
2	認証対象ポート	別 VLAN	認証解除	削除	移動前の認証解除	移動後に認証されるまで通信不可※
3	認証対象外ポート	同一 VLAN	認証状態が残る	未更新	認証状態が残る	通信不可
4	認証対象外ポート	別 VLAN	認証状態が残る	未更新	認証状態が残る	通信可

［ポート移動時の注意］

・MAC ポートの VLAN に所属している認証済みの端末が，同一 VLAN で，かつ MAC ポート以外の認証ポートに移動した場合，移動元のポートでの認証状態は解除されません。

・異なる認証機能の認証ポートへポート移動した場合（例えば IEEE802.1X 認証のポートから MAC

認証のポート（固定 VLAN モード）へのポート移動），移動元のポートでの認証状態が解除されないケースがあります。

上記の何れの場合でも，移動元のポートに認証状態が残り，移動先のポートで該当端末の通信はできないため，次のどちらかの運用コマンドを使用して，該当端末を認証解除する必要があります。

・IEEE802.1X 認証：clear dot1x auth-state コマンド

・MAC 認証：clear mac-authentication auth-state コマンド

5.5 レイヤ 2 認証共通のコマンドガイド

5.5.2 レイヤ 2 認証共通コンフィグレーションコマンドのパラメータ設定

変更

(6) ポート単位の認証数制限値の設定

変更前

（6）ポート単位の認証数制限値の設定

［設定のポイント］

レイヤ 2 認証のポート単位の認証数制限を設定します。

［コマンドによる設定］

1. (config)# interface gigabitethernet 1/0/5
   (config-if)# switchport mode access
   (config-if)# switchport vlan 10
   (config-if)# web-authentication port
   (config-if)# mac-authentication port
   (config-if)# authentication max-user 64
   (config-if)# exit

認証対象ポート 1/0/5 の認証数制限を 64 に設定します。

変更後

（6）ポート単位の認証数制限値の設定

［設定のポイント］

レイヤ 2 認証のポート単位の認証数制限を設定します。

［コマンドによる設定］

1. (config)# interface gigabitethernet 1/0/5
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 10
   (config-if)# mac-authentication port
   (config-if)# authentication max-user 64
   (config-if)# exit

認証対象ポート 1/0/5 の認証数制限を 64 に設定します。

12　マルチステップ認証

12.1 解説

12.1.2 サポート機能

追加

表 12-4　マルチステップ認証で使用する属性名（Access-Accept）

表 12-4　マルチステップ認証で使用する属性名（Access-Accept）

属性名	Type 値	説明
Filter-Id	11	本装置でマルチステップ認証の認証動作に使用するテキスト文字列です。 端末認証用 RADIUS サーバの場合 @@1X-Auth@@：ユーザ認証として IEEE802.1X 認証をします。 空白（Filter-Id 未設定）またはその他の文字列※：端末認証だけ（シングル認証）で認証成功とします。 ユーザ認証用 RADIUS サーバの場合 ユーザ認証許可オプションを設定したときに使用します。端末認証が失敗したときに，ユーザ認証を許可するかどうかを選択します。 @@MAC-Auth@@：端末認証が失敗したときにユーザ認証を許可しません。 空白（Filter-Id 未設定）またはその他の文字列※：端末認証が失敗しても，ユーザ認証を許可します。 注※　「その他文字列」を使用する場合は，@@1X-Auth@@など，マルチステップ認証で使用する文字列は含めないようにしてください。本装置がその他文字列と認識しません。

12.1.6 認証済み端末のポート間移動

変更

変更前

12.1.6 認証済み端末のポート間移動

マルチステップ認証での認証済み端末のポート間移動については，各認証でのポート間移動の条件のほかに，次に示す条件が加わります。

最終認証が IEEE802.1X 認証

ポート間移動を検出した場合，認証状態は解除となります。

最終認証が MAC 認証

移動前後でポートのコンフィグレーションが完全に一致している場合は，認証状態のままポート移動ができます。条件を次の表に示します。

なお，コンフィグレーションが異なる場合は，認証状態は解除となります。

表 1-6　ポート間移動できるコンフィグレーションの条件（最終認証が MAC 認証）

条件	備考
移動前後で authentication multi-step コマンドの設定があり※，ユーザ認証許可オプションの有無が同じ	authentication multi-step コマンドの設定時に比較します。
移動前後で authentication multi-step コマンドの設定があり※，端末認証 dot1x オプションの有無が同じ	authentication multi-step コマンドの設定時に比較します。

注※

移動前後で authentication multi-step コマンドの設定がないときは，シングル認証同士として処理します。

変更後

12.1.6 認証済み端末のポート間移動

マルチステップ認証での認証済み端末のポート間移動について，次の表に示します。なお，シングル認証のポート移動の動作は，5.3 レイヤ 2 認証共通の機能を参照ください。

表 12-6 マルチステップ認証（端末認証：MAC 認証／ユーザ認証：IEEE802.1X 認証）でのポート間移動時の動作

ケース	移動先ポート	VLAN	ユーザ認証状態	移動前ポートの MAC アドレステーブル	移動前ポートの認証状態	移動後の通信可否
1	認証対象ポート	同一 VLAN	移動後，再認証操作	削除	移動前の認証解除	移動後に認証されるまで通信不可
2	認証対象ポート	別 VLAN	移動後，再認証操作	削除	移動前の認証解除	移動後に認証されるまで通信不可
3	認証対象外ポート	同一 VLAN	認証状態が残る	未更新	認証状態が残る	通信不可
4	認証対象外ポート	別 VLAN	認証状態が残る	未更新	認証状態が残る	通信可

［ポート移動時の注意］

・マルチステップ認証の認証済みの端末が別 VLAN のマルチステップ認証ポートへポート移動すると，ポート移動時の MAC 認証に失敗する場合があります。

また，運用コマンド restart dot1x を実行した場合も同様です。これにより，一定時間（再認証時間間隔)の間，移動先のポートで通信ができません。移動先のポートで通信が可能となるには，再認証時間間隔が経過後に MAC 認証が成功するまで待って下さい。また，マルチステップ認証を使用する場合は，コンフィグレーションコマンド mac-authentication auth-interval-timer で，再認証時間間隔を短い時間に設定してください。

・マルチステップ認証ポートから，シングル認証の認証ポートへポート移動した場合（例えばマルチステップ認証ポートから MAC 認証のポート（固定 VLAN モード）へのポート移動），移動元のポートでの認証状態が解除されないケースがあります。移動先のポートで該当端末の通信はできないため，次のどちらかの運用コマンドを使用して，該当端末を認証解除する必要があります。

・IEEE802.1X 認証：clear dot1x auth-state コマンド

・MAC 認証：clear mac-authentication auth-state コマンド

18　ポートミラーリング

18.1 解説

18.1.2 ポートミラーリングの動作仕様

変更
(6) 送信フレームのミラーリング

変更前

(6) 送信フレームのミラーリング

:

・送信側フィルタで廃棄を設定している場合，廃棄対象フレームのミラーリングは次のとおりになります。

・イーサネットインタフェースに設定した場合，モニターポートでフィルタによって廃棄したフレームもミラーリング対象となり，ミラーポートから送信されます。

・モニターポートが所属する VLAN インタフェースに設定した場合，モニターポートでフィルタによって廃棄したフレームもミラーリング対象となります。

変更後

(6) 送信フレームのミラーリング

:

・送信側フィルタで廃棄を設定している場合，廃棄対象フレームのミラーリングは次のとおりになります。

・イーサネットインタフェースに設定した場合，モニターポートでフィルタによって廃棄したフレームもミラーリング対象となり，ミラーポートから送信されます。

・モニターポートが所属する VLAN インタフェースに設定した場合，モニターポートでフィルタによって廃棄したフレームはミラーポートから送信されません。

18.1.4 ポートミラーリング使用時の注意事項

削除

(1) 送信フレームをミラーリングの対象とする場合の注意事項

---

(1) 送信フレームをミラーリングの対象とする場合の注意事項

・ミラーポートから送信されるフレームの順序は，モニターポートから送信されるフレームの順序と異なることがあります。

~~・次に示す状態のためにモニターポートでは通信できない場合でも，ミラーリングします。~~

~~・スパニングツリーによる Blocking，Discarding，Listening，および Learning 状態~~

~~・Ring Protocol によるブロッキング状態~~

~~・アップリンク・リダンダントでのスタンバイポート~~

~~・IEEE802.1X による未認証~~

変更

(2) ポートミラーリング 802.1Q Tag 付与機能使用時の注意事項

変更前

(2) ポートミラーリング 802.1Q Tag 付与機能使用時の注意事項

:

・ミラーリングフレームは，ミラーポートと同じポートに設定されたリンクアグリゲーションやレイヤ 2 スイッチ機能の通信状態に関係なく送信されます。

変更後

(2) ポートミラーリング 802.1Q Tag 付与機能使用時の注意事項

:

・ミラーリングフレームは，ミラーポートに設定されたレイヤ 2 スイッチ機能の通信状態に関係なく送信されます。

追加

(3)　sFlow 統計と併用する場合の注意事項

---

(3)　sFlow 統計と併用する場合の注意事項

同一ポートにおいて、以下の併用はしないでください。

・sFlow 統計の送信(egress)指定と，送信フレームを対象とするモニターポート

19　sFlow 統計（フロー統計）機能

19.1 解説

19.1.4 本装置の sFlow 統計動作

追加

(7) フロー統計と併用できない機能

---

(7) フロー統計と併用できない機能

同一ポートにおいて，以下の併用はしないでください。

・sFlow 統計の送信（egress）指定と，送信フレームを対象とするポートミラーのモニターポート

第3編　コンフィグレーションコマンドレファレンス

29　IEEE802.1X

dot1x port-control

削除

［入力モード］

［入力モード］

(config-if)

イーサネットインタフェース~~, ポートチャネルインタフェース~~

37　ポートミラーリング

monitor session

追加

［注意事項］

6. source interface パラメータには，最大 24 個のインタフェースが指定できます。

42　コンフィグレーション編集時のエラーメッセージ

42.1 コンフィグレーション編集時のエラーメッセージ

42.1.1 共通

削除

表 42-1 共通のエラーメッセージ

表 42-1　共通のエラーメッセージ

メッセージ	内容
~~Invalid IPv6 address. -- <value1>~~	~~<value1>は IPv6 アドレスの範囲外です。~~ ~~範囲内の値で設定してください。~~
	~~<value1>：不正な値~~
Invalid line type.	回線種別が不正です。 ~~同一 NIF 内に異なる回線種別が設定されています。~~

42.1.24 IEEE802.1X 情報

追加

表 42–24　IEEE802.1X のエラーメッセージ

表 42-24　IEEE802.1X のエラーメッセージ

メッセージ	内容
Relations between the dot1x port-control configuration and the channel-group configuration within same port.	dot1x port-control とポートチャネルのコンフィグレーションは同一ポートには設定できません。

4　コンフィグレーションとファイルの操作

erase startup-config

追加

［Ver.1.0.B 以降］

スタートアップコンフィグレーションファイルの内容を初期導入時の状態に戻します。ランニングコンフィグレーションを初期導入時の状態に戻す場合は本コマンドを実行後，ランニングコンフィグレーションをセーブせずに装置を再起動してください。

［入力形式］

erase startup-config

［入力モード］

装置管理者モード

［パラメータ］

なし

［実行例］

```
# erase startup-config
Do you wish to erase startup-config? (y/n): y
!#
```

［表示説明］

なし

［通信への影響］

なし

［注意事項］

1. 本コマンドを実行後，装置を再起動するとランニングコンフィグレーションが初期導入時の状態に戻ります。ネットワーク経由でログインしている場合は，再起動後にログインできなくなるので注意してください。
2. コンフィグレーション編集中の場合は本コマンドを使用できません。コンフィグレーションモードを終了してください。

7　時刻の設定と NTP

set clock

変更
［パラメータ］

変更前
［パラメータ］

yy

年の下 2 桁を指定します。指定できる値は 69～99（1900 年代）および 00～38（2000 年代）21～37 です。（例：2000 年ならば 00）

変更後
［パラメータ］

yy

年の下 2 桁を指定します。指定できる値は 21～37 です。

変更
［実行例］

変更前
［実行例］

2005 年 6 月 22 日 15 時 30 分に設定する場合は以下のコマンドを入力します。

> set clock 0506221530

Wed Jun 22 15:30:00 UTC 2005

変更後
［実行例］

2021 年 9 月 1 日 15 時 30 分に設定する場合は以下のコマンドを入力します。

> set clock 2109011530

Wed Sep 1 15:30:00 UTC 2021

削除

［注意事項］

［注意事項］

1. 本装置で収集している統計情報の CPU 使用率は，時刻が変更された時点で 0 クリアされます。

~~2. 入力できる範囲は「1969/01/01 00:00:00～2038/01/19 03:14:07」です。~~

9　装置の管理

show system

変更

表 9–2　show system コマンド表示内容

変更前

表 9–2　show system コマンド表示内容

表示項目	表示内容	表示詳細情報
:		
Temperature	装置内温度情報	normal：正常（-10℃より高く 50℃未満） caution：注意（-10℃以下または 50℃以上 60℃未満） 注　温度センサーが 60℃以上になるとソフトウェアが停止します。
:		

変更後

表 9–2　show system コマンド表示内容

表示項目	表示内容	表示詳細情報
:		
Temperature	装置内温度情報	normal：正常（5℃より高く 75℃未満） caution：注意（5℃以下または 75℃以上 80℃未満） 注　温度センサーが 80℃以上になるとソフトウェアが停止します。
:		

show environment

変更

表 9–5　show environment コマンドの表示内容

変更前

表 9–5　show environment コマンドの表示内容

表示項目	表示内容	表示詳細情報
:		
Main	入気温度情報	装置の温度情報を表示
Warning level※3	運用環境レベル	normal：正常 caution：注意（高温または低温）
Accumulated running time※4		
Main	total：装置の累計稼働時間 critical：50℃以上の環境下での装置の累計稼働時間	正常時は累計稼働時間を表示します。 fault：稼働時間読み込み失敗 ****：稼働時間読み込み中

:

注※3　入気温度の変移によって Warning level を表示します。

温度センサーが 80℃以上になるとソフトウェアが停止します。

変更後

表 9–5　show environment コマンドの表示内容

表示項目	表示内容	表示詳細情報
:		
Main	装置内温度	装置の温度情報を表示
Warning level※3	運用環境レベル	normal：正常 caution：注意（高温または低温）
Accumulated running time※4		
Main	total：装置の累計稼働時間 critical：装置内温度が 75℃以上の環境下での装置の累計稼働時間	正常時は累計稼働時間を表示します。 fault：稼働時間読み込み失敗 ****：稼働時間読み込み中

:

注※3　装置内温度の変移によって Warning level を表示します。

温度センサーが 80℃以上になるとソフトウェアが停止します。

14　ソフトウェアの管理

ppupdate

追加

［注意事項］

5. MC 運用モードが有効の場合に本コマンドを実行したときは，update mc-configuration コマンドの処理も自動的に実行されます（test パラメータ指定時を除く）。そのため，update mc-configuration コマンドに対応する運用ログが採取されます。運用ログの詳細は「メッセージ・ログレファレンス」を参照してください。なお，update mc-configuration コマンドの処理でエラーが検出された場合でも，本コマンドは正常終了しています。

5-1. MC 運用モードが有効の場合に本コマンドを実行するときは，no-reload パラメータを指定して実行することを推奨します。no-reload パラメータを指定しない場合，update mc-configuration コマンドの処理にエラーが発生すると MC のソフトウェアと装置情報が更新されないまま再起動するため，本コマンド実行前のソフトウェアと装置状態で起動します。no-reload パラメータを指定した本コマンドで update mc-configuration コマンドの処理にエラーが発生した場合は，update mc-configuration コマンドを手動で実行して MC のソフトウェアと装置情報を更新してから装置を再起動してください。

6. コンフィグレーションコマンド hostname で 8 文字以上の装置名称を設定している場合，本コマンド実行時にユーザ端末に出力される Broadcast message 行は 79 文字目までしか表示されません。

43　応答メッセージ

43.1.2 運用端末とリモート操作

削除

表 43–2　運用端末とリモート操作の応答メッセージ

表 43–2　運用端末とリモート操作の応答メッセージ

メッセージ	内容
<host>: hostname nor servname provided, or not known	ホストに指定したアドレスとオプションで指定した接続方法が異なっています。 <host> リモートホスト

変更

表 43–2　運用端末とリモート操作の応答メッセージ

変更前

表 43–2　運用端末とリモート操作の応答メッセージ

メッセージ	内容
<host>: No address associated with hostname	アドレス解決ができなかったため，ホストに接続できませんでした。 <host> リモートホスト
:	:
No address associated with hostname	アドレス解決ができなかったため，ホストに接続できませんでした。

変更後

表 43–2　運用端末とリモート操作の応答メッセージ

メッセージ	内容
<host>: Name or service not known	アドレス解決ができなかったため，ホストに接続できませんでした。 <host> リモートホスト
:	:
Name or service not known	アドレス解決ができなかったため，ホストに接続できませんでした。

43.1.3 コンフィグレーションとファイルの操作

追加

表 43-3　コンフィグレーションとファイルの操作の応答メッセージ

表 43-3　コンフィグレーションとファイルの操作の応答メッセージ

メッセージ	内容
### List of remote directory.	指定ディレクトリのリスト内容を取得し表示しています。
### Total <number> lines.	表示したファイルの行数は<number>行でした。
Can't create file.	ファイルをコピーできませんでした。 空き容量など，状態を確認の上，再実行してください。
Can't execute.	コマンドを実行できません。再実行してください。
Can't open /dev/sda1: Device or resource busy Cannot initialize 'C:'	ほかのプロセスが MC にアクセスしています。 時間をおいて再実行してください。
Can't open /dev/sda1: Permission denied Cannot initialize 'C:'	MC の認識中です。 時間をおいて再実行してください。
Can't open /dev/sda1: Device or resource busy Cannot initialize 'C:' Bad target c: <file path>	ほかのプロセスが MC にアクセスしています。 時間をおいて再実行してください。 <file path>：コピー先 MC ファイルパス
Can't open /dev/sda1: No such file or directory Cannot initialize 'C:'	MC が搭載されていません。 MC が正しく装置に挿入されているか確認してください。
:	:

43.1.4 ログインセキュリティと RADIUS/TACACS+

削除

表 43-4　ログインセキュリティと RADIUS/TACACS+の応答メッセージ

表 43-4　ログインセキュリティと RADIUS/TACACS+の応答メッセージ

メッセージ	内容
<user name> is not a valid login name	このユーザ名は使用できません。
Can't add user <user name>: can't lock <file name> : <reason>	password ファイルがロックしているのでユーザの追加を中止します。リトライしてください。 <user name>：ユーザ名 <file name>：パスワードファイル名 <reason>：詳細情報
can't lock <file name> : <reason>	password ファイルがロックしているのでユーザの削除を中止します。リトライしてください。 <file name>：パスワードファイル名 <reason>：詳細情報

2　イベント発生部位形式

2.1 EQUIPMENT

変更

表 2-1　イベント発生部位 EQUIPMENT の運用メッセージ

変更前

表 2-1　イベント発生部位 EQUIPMENT の運用メッセージ

メッセージ識別子	イベントレベル	メッセージテキスト
	内容と対応	
00020106	E3	The temperature of hardware reached the warning level (<temperature> degree).
	ハードウェアの温度が，コンフィグレーションコマンド system temperature-warning-level で設定した温度に達しました。 <temperature>　装置の入気温度（摂氏） [対応] 装置の温度が指定した温度に達しているため，装置周辺の環境（ファンの状態，通風，熱源の有無など）を確認してください。	

変更後

表 2-1　イベント発生部位 EQUIPMENT の運用メッセージ

メッセージ識別子	イベントレベル	メッセージテキスト
	内容と対応	
00020106	E3	The temperature of hardware reached the warning level (<temperature> degree).
	ハードウェアの温度が，コンフィグレーションコマンド system temperature-warning-level で設定した温度に達しました。 <temperature>　装置内温度（摂氏） [対応] 装置の温度が指定した温度に達しているため，装置周辺の環境（ファンの状態，通風，熱源の有無など）を確認してください。	

1　サポート MIB の概要

1.2 MIB 一覧

1.2.2 プライベート MIB 一覧

削除

表 1-2　プライベート MIB の MIB グループ一覧

表 1-2　プライベート MIB の MIB グループ一覧

プライベート MIB の MIB グループ		機能	サポート
axsManagement	axsFdbClearMIB グループ	MACアドレステーブル情報をクリアするための MIB です。	○
icmp グループ（HP プライベート MIB）		HP 社のプライベート MIB です。	○

2　標準 MIB(RFC 準拠および IETF ドラフト MIB)

2.1 system グループ(MIB-II)

追加

表 2-1　system グループの実装仕様

表 2-1　system グループの実装仕様

項番	オブジェクト識別子	アクセス	実装仕様	実装有無
4	sysContact {system 4}	R/W	[規格] 管理ノードに関する連絡先。 [実装] ユーザがコンフィグレーションコマンドで設定した文字列（60 文字以内）。デフォルトはなし（NULL）。 本装置では GET のみ可能。	●
5	sysName {system 5}	R/W	[規格] 管理ノードの名称，管理ノードのドメイン名。 [実装] ユーザがコンフィグレーションコマンドで設定した文字列（60 文字以内）。デフォルトはなし（NULL）。 本装置では GET のみ可能。	●
6	sysLocation {system 6}	R/W	[規格] 管理ノードの設置場所。 [実装] ユーザがコンフィグレーションコマンドで設定した文字列（60 文字以内）。デフォルトはなし（NULL）。 本装置では GET のみ可能。	●

2.2 interfaces グループ(MIB-II)

追加

表 2-2　interfaces グループの実装仕様

表 2-2　interfaces グループの実装仕様

項番	オブジェクト識別子	アクセス	実装仕様	実装有無
10	ifAdminStatus {ifEntry 7}	R/W	[規格] このインタフェースの望ましい状態。 ・up（1） ・down（2） ・testing（3） [実装] インタフェースによる。本装置ではGETのみ可能。 ・イーサネットインタフェース：コンフィグレーションで shutdown 指定時は down（2）。 ・ポートチャネルインタフェース：コンフィグレーションで shutdown 指定時は down（2）。 ・VLAN インタフェース：コンフィグレーションで VLAN suspend 指定時は down（2）。 ・ループバックインタフェース：up（1）固定。	●

2.10 rmon グループ(Remote Network Monitoring MIB)

2.10.2 History Control グループ

変更

表 2-26　History Control グループの実装仕様

変更前

表 2-26　History Control グループの実装仕様

項番	オブジェクト識別子	アクセス	実装仕様	実装有無
4	historyControlDataSource {historyControlEntry 2}※1	R/W	[規格] この情報のインタフェースのオブジェクト ID を示します。このオブジェクト・インスタンスは MIB-II の interfaces グループの ifIndex。 [実装] 規格に同じ。	●
5	historyControlBucketsRequested {historyControlEntry 3}※1	R/W	[規格] etherHistoryTable に記憶するデータ数の要求数（デフォルト値 50）。値の範囲は 1～65535。 [実装] 規格に同じ。	●
7	historyControlInterval {historyControlEntry 5}※1	R/W	[規格] etherHistoryTable に記憶するデータのサンプリング間隔（単位：秒）。値の範囲は，1～3600（デフォルト値 1800）。 [実装] 規格に同じ。	●
8	historyControlOwner {historyControlEntry 6}※1	R/W	[規格] エントリを構成する実態およびリソースを割り当てるオーナー。 [実装] 24 文字以内の文字列を読み書きできます。	●
9	historyControlStatus {historyControlEntry 7}	R/W	[規格] エントリの状態。 ・valid（1） ・createRequest（2） ・underCreation（3） ・invalid（4） [実装] このエントリに追加するときは，まず，createRequest（2）を Set します。エントリ内の MIB に Set を行い，最後に valid（1）を Set します。 削除するときは，invalid（4）を Set します。createRequest（2）を Set した後で，Get すると，underCreation（3）を応答し，valid（1）を Set した後で Get すると，valid（1）を応答します。※2 すでにエントリがある場合は，いったん invalid（4）を Set してエントリを削除してから追加してください。 ・valid（1）：historyControlDataSource で取得できる interface の統計情報が取得でき，historyControlInterval の間にサンプリングできます。 ・invalid（4）：interface の統計情報が取得できません。また，historyInterval の間にサンプリングできません。	●

変更後

表 2-26　History Control グループの実装仕様

項番	オブジェクト識別子	アクセス	実装仕様	実装有無
4	historyControlDataSource {historyControlEntry 2}※1	R/W	[規格] この情報のインタフェースのオブジェクト ID を示します。このオブジェクト・インスタンスは MIB-II の interfaces グループの ifIndex。 [実装] 本装置では GET のみ可能。	●
5	historyControlBucketsRequested {historyControlEntry 3}※1	R/W	[規格] etherHistoryTable に記憶するデータ数の要求数（デフォルト値 50）。値の範囲は 1～65535。 [実装] 本装置では GET のみ可能。	●
7	historyControlInterval {historyControlEntry 5}※1	R/W	[規格] etherHistoryTable に記憶するデータのサンプリング間隔（単位：秒）。値の範囲は，1～3600（デフォルト値 1800）。 [実装] 本装置では GET のみ可能。	●
8	historyControlOwner {historyControlEntry 6}※1	R/W	[規格] エントリを構成する実態およびリソースを割り当てるオーナー。 [実装]本装置では GET のみ可能（24 文字以内の文字列）。	●
9	historyControlStatus {historyControlEntry 7}	R/W	[規格] エントリの状態。 ・valid（1） ・createRequest（2） ・underCreation（3） ・invalid（4） [実装] 本装置では GET のみ可能。	●

2.10.4 Alarm グループ

変更

表 2-28　Alarm グループの実装仕様

変更前

表 2-28　Alarm グループの実装仕様

項番	オブジェクト識別子	アクセス	実装仕様	実装有無
4	alarmInterval {alarmEntry 2}※1	R/W	[規格] 閾値と比較する間隔（単位：秒）。設定できる範囲は 1～（2^{32}-1） [実装] 規格に同じ。※2	●
5	alarmVariable {alarmEntry 3}※1	R/W	[規格] サンプリングする MIB のオブジェクト識別子。 [実装] 規格に同じ。	●
6	alarmSampleType {alarmEntry 4}※1	R/W	[規格] 値を閾値と比較する方法を指定します。 ・absoluteValue（1） ・deltaValue（2） [実装] 規格に同じ。	●
8	alarmStartupAlarm {alarmEntry 6}※1	R/W	[規格] 最初にアラームを生成するタイミング。 ・risingAlarm（1） ・fallingAlarm（2） ・rising Or fallingAlarm（3） [実装] 規格に同じ。	●
9	alarmRisingThreshold {alarmEntry 7}※1	R/W	[規格] サンプリングした統計に対する上方閾値。 [実装] 規格に同じ。※2	●
10	alarmFallingThreshold {alarmEntry 8}※1	R/W	[規格] サンプリングした統計に対する下方閾値。 [実装] 規格に同じ。※2	●
11	alarmRisingEventIndex {alarmEntry 9}※1	R/W	[規格] 上方閾値を超えた場合に使用するイベントグループのインデックス番号。設定できる範囲は 0～65535。 [実装] 規格に同じ。	●
12	alarmFallingEventIndex {alarmEntry 10}※1	R/W	[規格] 下方閾値を超えた場合に使用するイベントグループのインデックス番号。設定できる範囲は 0～65535。 [実装] 規格に同じ。	●
13	alarmOwner {alarmEntry 11}※1	R/W	[規格] エントリを構成する実態およびリソースを割り当てたオーナー。 [実装] 24 文字以内の文字列を読み書きできます。	●
14	alarmStatus {alarmEntry 12}	R/W	[規格] エントリの状態を示します。 [実装] このエントリに追加するときは，まず，createRequest（2）を Set します。エントリ内の MIB に Set を行い，最後に valid（1）を Set します。 削除するときは，invalid（4）を Set します。createRequest（2）を Set した後で，Get すると，underCreation（3）を応答し，valid（1）を Set した後で Get すると，valid（1）を応答します。※3 すでにエントリがある場合は，いったん invalid（4）を Set してエントリを削除してから追加してください。	●

項番	オブジェクト識別子	アクセス	実装仕様	実装有無
			・valid（1）：alarmVariable に設定されたオブジェクトの情報を alarmInterval の間にサンプリングできます。 ・invalid（4）：alarmVariable に設定されたオブジェクトが存在しません。または，alarmInterval の間にサンプリングできませんでした。	

変更後

表 2-28　Alarm グループの実装仕様

項番	オブジェクト識別子	アクセス	実装仕様	実装有無
4	alarmInterval {alarmEntry 2}※1	R/W	[規格] 閾値と比較する間隔（単位：秒）。設定できる範囲は 1～（2^{32}-1） [実装] 本装置では GET のみ可能。※2	●
5	alarmVariable {alarmEntry 3}※1	R/W	[規格] サンプリングする MIB のオブジェクト識別子。 [実装] 本装置では GET のみ可能。	●
6	alarmSampleType {alarmEntry 4}※1	R/W	[規格] 値を閾値と比較する方法を指定します。 ・absoluteValue（1） ・deltaValue（2） [実装] 本装置では GET のみ可能。	●
8	alarmStartupAlarm {alarmEntry 6}※1	R/W	[規格] 最初にアラームを生成するタイミング。 ・risingAlarm（1） ・fallingAlarm（2） ・rising Or fallingAlarm（3） [実装] 本装置では GET のみ可能。	●
9	alarmRisingThreshold {alarmEntry 7}※1	R/W	[規格] サンプリングした統計に対する上方閾値。 [実装] 本装置では GET のみ可能。※2	●
10	alarmFallingThreshold {alarmEntry 8}※1	R/W	[規格] サンプリングした統計に対する下方閾値。 [実装] 本装置では GET のみ可能。※2	●
11	alarmRisingEventIndex {alarmEntry 9}※1	R/W	[規格] 上方閾値を超えた場合に使用するイベントグループのインデックス番号。設定できる範囲は 0～65535。 [実装] 本装置では GET のみ可能。	●
12	alarmFallingEventIndex {alarmEntry 10}※1	R/W	[規格] 下方閾値を超えた場合に使用するイベントグループのインデックス番号。設定できる範囲は 0～65535。 [実装] 本装置では GET のみ可能。	●
13	alarmOwner {alarmEntry 11}※1	R/W	[規格] エントリを構成する実態およびリソースを割り当てたオーナー。 [実装] 本装置では GET のみ可能。	●
14	alarmStatus {alarmEntry 12}	R/W	[規格] エントリの状態を示します。 [実装] 本装置では GET のみ可能。	●

2.10.5 Event グループ

変更

表 2-29　Event グループの実装仕様

変更前

表 2-29　Event グループの実装仕様

項番	オブジェクト識別子	アクセス	実装仕様	実装有無
4	eventDescription {eventEntry 2}※1	R/W	[規格] このリストの説明。最大 127 文字の文字列。 [実装] 79 文字以内の文字列。	●
5	eventType {eventEntry 3}※1	R/W	[規格] イベント通知方法。 ・none（1） ・log（2） ・snmp-trap（3） ・log-and-trap（4） [実装] 規格に同じ。	●
6	eventCommunity {eventEntry 4}※1	R/W	[規格] eventType に SNMP 通知を含む指定をしたときの送信先のコミュニティ名。最大 127 文字の文字列。 [実装] eventType に SNMP 通知を含む指定をしたときの送信先のコミュニティ名。最大 60 文字の文字列。	●
8	eventOwner {eventEntry 6}※1	R/W	[規格] このエンティティを構成する実態およびリソースを割り当てるオーナー。最大 127 文字。 [実装] 24 文字以内の文字列を読み書きできます。	●
9	eventStatus {eventEntry 7}	R/W	[規格] このエントリの状態。 ・valid（1） ・createRequest（2） ・underCreation（3） ・invalid（4） [実装] このエントリに追加するときは，まず，createRequest（2）を Set します。エントリ内の MIB に Set を行い，最後に valid（1）を Set します。 削除するときは，invalid（4）を Set します。createRequest（2）を Set した後で，Get すると，underCreation（3）を応答し，valid（1）を Set した後で Get すると，valid（1）を応答します。※2 すでにエントリがある場合は，いったん invalid（4）を Set してエントリを削除してから追加してください。	●

変更後

表 2-29　Event グループの実装仕様

項番	オブジェクト識別子	アクセス	実装仕様	実装有無
4	eventDescription {eventEntry 2}※1	R/W	[規格] このリストの説明。最大 127 文字の文字列。 [実装] 79 文字以内の文字列。本装置では GET のみ可能。	●
5	eventType {eventEntry 3}※1	R/W	[規格] イベント通知方法。 ・none（1） ・log（2） ・snmp-trap（3） ・log-and-trap（4） [実装] 本装置では GET のみ可能。	●
6	eventCommunity {eventEntry 4}※1	R/W	[規格] eventType に SNMP 通知を含む指定をしたときの送信先のコミュニティ名。最大 127 文字の文字列。 [実装] eventType に SNMP 通知を含む指定をしたときの送信先のコミュニティ名。最大 60 文字の文字列。本装置では GET のみ可能。	●
8	eventOwner {eventEntry 6}※1	R/W	[規格] このエンティティを構成する実態およびリソースを割り当てるオーナー。最大 127 文字。 [実装] 本装置では GET のみ可能。	●
9	eventStatus {eventEntry 7}	R/W	[規格] このエントリの状態。 ・valid（1） ・createRequest（2） ・underCreation（3） ・invalid（4） [実装] 本装置では GET のみ可能。	●

3　プライベート MIB

3.2 axsFdb グループ(MAC アドレステーブルグループ MIB)

追加

表 3-6　axsFdb グループの実装仕様

表 3-6　axsFdb グループの実装仕様

項番	オブジェクト識別子	SYNTAX	アクセス	実装仕様	実装有無
5	axsFdbCounterCounts {axsFdbCounterEntry 3}	Counter32	R/O	このポートで学習している MAC アドレステーブルエントリ数。 本装置では固定値（0）を返す。	●

3.14 axsManagementMIB グループ(装置の状態/情報の変更を行う)

3.14.1 axsFdbClearMIB グループ(MAC アドレステーブル Clear 用 MIB)

削除

3.14.1 axsFdbClearMIB グループ(MAC アドレステーブル Clear 用 MIB)

(1) 識別子

```
axsMib          OBJECT IDENTIFIER ::= {axsEx 1}
オブジェクト ID 値　1.3.6.1.4.1.21839.2.2.1

axsManagementMIB    OBJECT IDENTIFIER ::= {axsMib 803}
オブジェクト ID 値　1.3.6.1.4.1.21839.2.2.1.803

axsOperationCommand OBJECT IDENTIFIER ::= {axsManagementMIB 51}
オブジェクト ID 値　1.3.6.1.4.1.21839.2.2.1.803.51
```

(2) 実装仕様

axsFdbClearMIB グループの実装仕様を次の表に示します。

表 3-41　axsFdbClearMIB グループの実装仕様

項番	オブジェクト識別子	SYNTAX	アクセス	実装仕様	実装有無
1	axsFdbClearMIB {axsOperationCommand 1}	NOT-ACCESSIBLE	NA	MAC アドレステーブル情報をクリアするための MIB グループ。	●
2	axsFdbClearSet {axsFdbClearMIB 1}	INTEGER	R/W	MAC アドレステーブル clear 情報。 ・初期値（0） ・clear 処理中（1） ・clear 失敗（2） ・clear 成功（3） Set を行う場合，1 を設定する。※	●
3	axsFdbClearReqTime {axsFdbClearMIB 2}	TimeTicks	R/O	最近に MAC アドレステーブル情報のクリア要求を受付けた時間（sysUpTime）。	●
4	axsFdbClearSuccessTime {axsFdbClearMIB 3}	TimeTicks	R/O	MAC アドレステーブル情報のクリアが行われた最新の時間（sysUpTime）。	●

3.15 icmp グループ(HP プライベート MIB)

削除

3.15. icmp グループ(HP プライベート MIB)

（1）識別子

```
hp OBJECT IDENTIFIER ::= {enterprises 11}
nm OBJECT IDENTIFIER ::= {hp 2}

icmp OBJECT IDENTIFIER ::= {nm 7}
```

オブジェクト ID 値　1.3.6.1.4.1.11.2.7

（2）実装仕様

icmp グループの実装仕様を次の表に示します。

表 3-42　icmp グループの実装仕様

項番	オブジェクト識別子	SYNTAX	アクセス	実装仕様	実装有無
1	icmpEchoReq {icmp 1}	INTEGER	R/O	ICMP Echo Reply を受信するのに要した時間（単位：ミリ秒）。 INDEX {PacketSize，TimeOut，IPAddress} ・PacketSize：32～2048 ・TimeOut：1～60（Second） ・IP Address：対象 IP アドレス ICMP Echo Reply を正しく受信しなかった場合，次に示す値を応答します。 ・-1：内部エラー ・-2：タイムアウト ・-3：ICMP Echo Reply の値不正 ・-4：送信パケットサイズエラー ・-5：設定タイムアウト値不正	●