



最初にお読みください

CentreCOM® GS908M V2-4PS リリースノート

この度は、CentreCOM GS908M V2-4PS（以下、特に記載がないかぎり、「本製品」と表記します）をお買いあげいただき、誠にありがとうございました。

このリリースノートは、取扱説明書とコマンドリファレンスの補足や、ご使用前にご理解いただきたい注意点など、お客様に最新の情報をお知らせするものです。

最初にこのリリースノートをよくお読みになり、本製品を正しくご使用ください。

1 ファームウェアバージョン 2.4.0

2 本バージョンで追加された項目

ファームウェアバージョン 2.3.3 から 2.4.0 へのバージョンアップにおいて、以下の機能が追加されました。

2.1 ハードウェアパケットフィルター機能

 **参照** 「コマンドリファレンス」 / 「クラシファイア」

ハードウェア (ASIC) レベルで入力パケットをフィルタリング (許可・拒否) するハードウェアパケットフィルター機能をサポートしました。フィルタリング条件はヘッダー情報に基づいてパケットを分類するクラシファイアによって定義し、送信元 MAC アドレス、始点・終点 IP アドレス、プロトコル (ARP のみ) を使用できます。条件に一致したパケットに対しては、許可 (permit) または破棄 (deny) の処理が指定できます。

ハードウェアパケットフィルター機能の設定、情報の表示をするには、新規追加された以下のコマンドを使用します。

- CREATE ACL
- SET ACL
- DESTROY ACL
- PURGE ACL
- SHOW ACL
- SHOW ACL COUNTER
- RESET ACL COUNTER

コマンドの解説および設定に関する注意事項については、本リリースノートの「6.4 ハードウェアパケットフィルター機能」を参照してください。

3 本バージョンで仕様変更された項目

ファームウェアバージョン 2.3.3 から 2.4.0 へのバージョンアップにおいて、以下の仕様変更が行われました。

3.1 PoE 最大供給電力 90W に対応

 [「取扱説明書」](#)

 [「コマンドリファレンス」](#) / [「PoE」](#)

装置全体の PoE 最大供給電力を 75W から 90W に拡張しました。これにともない本製品の仕様の一部および MIB ファイルの poeswitch.mib が更新されました。なお、仕様変更の詳細については本リリースノートの「6.2 PoE 最大供給電力 90W 対応にともなう仕様変更」を参照してください。

4 本バージョンで修正された項目

ファームウェアバージョン 2.3.3 から 2.4.0 へのバージョンアップにおいて、以下の項目が修正されました。

- 4.1 SHOW DEBUG コマンド実行時に、本製品宛て Ping のタイムアウトやスパニングツリープロトコル (STP/RSTP/MSTP) のトポロジーチェンジが発生する場合がありますが、これを修正しました。

5 本バージョンでの制限事項

ファームウェアバージョン 2.4.0 には、以下の制限事項があります。

5.1 SNMP

 [「コマンドリファレンス」](#) / [「運用・管理」](#) / [「SNMP」](#)

- SNMP マネージャーのタイムアウトによって、同時に 5 個以上の SNMP マネージャーから ifEntry を Get できない場合があります。SNMP マネージャーのタイムアウト値を長く設定するようにしてください。
- SHOW INTERFACE コマンドで表示される ifMTU の値および SNMP で取得可能な ifMTU の値が正しくありません。9196 と表示されますが、正しくは 9194 です。

5.2 RADIUS サーバー

 [「コマンドリファレンス」](#) / [「運用・管理」](#) / [「認証サーバー」](#)

- 802.1X 認証有効時、SET RADIUS コマンドの DEAD-ACTION パラメーターで PERMIT を設定しても、RADIUS サーバーからの応答がないときに、通信ができなくなる場合があります。
- RADIUS アカウンティング機能有効時に、RADIUS サーバーから Access-Reject パケットを受信すると、本製品から Failed 属性が付加された Accounting-Request パケットが送信されます。
- ポート認証で RADIUS サーバーを 2 台登録し、かつ 2 台の RADIUS サーバーの共有パスワード (Secret 値) を異なる文字列に設定すると、認証に成功しない場合があります。ポート認証で 2 台の RADIUS サーバーを利用する場合は、Secret 値を同じ文字列に設定してください。

5.3 スイッチング

 [「コマンドリファレンス」](#) / [「スイッチング」](#)

- ポートを無効に設定しているとき、ハードウェアの仕様により、パケットを受信した際の LINK/ACT LED の点灯動作がポート範囲によって以下のように異なります。ポート 1～8 では点灯し、ポート 9 以降では点滅します。

- SFP ポートで通信モードやポートトランキングを設定すると、該当ポートの通信ができなくなる可能性があります。
該当ポートのフローコントロールを無効に設定することで、この現象を回避できます。

5.4 ポートトランキング

 **参照** 「コマンドリファレンス」 / 「スイッチング」

トランクグループを以下のいずれかの条件で複数作成し、512 個以上の MAC アドレスが使用される通信が発生している状態で、トランクポートの追加と削除を繰り返し実施すると、本製品がリポートすることがあります。

- トランクグループの所属ポートに 512 個以上のスイッチフィルタが登録されている
- トランクポートの通信モードがポート本来の通信モードと異なる設定になっている

5.5 IGMP Snooping

 **参照** 「コマンドリファレンス」 / 「IGMP Snooping」

- IGMP Snooping 有効時、IGMP パケットの通信中にグループの所属 VLAN を変更すると、IGMP Snooping 用のテーブルから変更前の VLAN 情報が削除されません。
- IGMP Snooping 有効時、メンバーが存在するポートをミラーポートに設定しても、IGMP Snooping 用のテーブルから該当ポートの情報が削除されません。
- IGMP Snooping と、EPSR アウエアまたはスバニングツリープロトコル併用時、経路の切り替えが発生したときにマルチキャストグループの登録がクリアされないため、切り替え前に登録されたルーターポートが残ったままになります。
なお、EPSR アウエアについては、CREATE EPSR コマンドの DELETEDEMCAST オプションで、リングトポロジーチェンジ発生時にマルチキャストグループのエントリを FDB から削除する設定が可能です。
- マルチキャストグループをスタティック登録するには、あらかじめ SET IGMP Snooping コマンドの ROUTERPORT パラメーターでルーターポートを設定する必要があります。このとき指定するポートが複数の VLAN に所属していた場合、ADD IGMP Snooping MCGROUP コマンドの NUMBER パラメーターで同時に複数のマルチキャストを登録する際に、学習可能なマルチキャストグループの最大数を超える設定をしてしまうと、「Warning: 52 addresses were not able to be added from multicast group address (224.1.1.13)」のようなエラーが表示され、その後、DELETE IGMP Snooping コマンド、SHOW IGMP Snooping コマンドを実行するが、SHOW CONFIG コマンドに DYNAMIC パラメーターを指定して実行するとリポートが発生します。この現象を回避するには、以下を参考にグループ数の最大を超えないように設定してください。
 - マルチキャストグループの最大数はデフォルトで 64 個だが、SET IGMP Snooping コマンドの NUMBERMULTICASTGROUPS パラメーターにより変更することが可能
 - ルーターポートが複数の VLAN に所属する場合、VLAN の数だけエントリ数を消費する

5.6 スバニングツリー

 **参照** 「コマンドリファレンス」 / 「スバニングツリープロトコル」

本製品の実装では、トポロジーチェンジ発生時にエッジポートに設定されたポートの FDB が消去されます。

5.7 Web GUI

 **「コマンドリファレンス」 / 「Web GUI」**

Web GUI でマルチプル VLAN(Protected Port 版) のポート設定を行う際、グループ番号の設定変更とタグなし / タグ付きの設定変更を同時に行うことができますが、個別に変更するようにしてください。

グループ番号の変更とタグなし→タグ付きの変更を同時に行った場合、該当ポートがタグなしとしてデフォルト VLAN にも追加されます。

6 マニュアルの補足・誤記訂正

最新マニュアル（取扱説明書、コマンドリファレンス）の補足事項および誤記訂正です。

6.1 オートファンコントロール

 **「取扱説明書」 77 ページ**

ファームウェアバージョン 2.3.2 から、動作時温度（外気温度）に応じたファンの回転を低速回転 / 高速回転の 2 段階に変更しました。ファンが低速回転 / 高速回転を開始する外気温度の目安は以下のとおりです。

条件	低速回転開始	高速回転開始
全標準ポート使用時（100%負荷）	15℃	40℃
全標準ポート + SFP ポート使用時（100%負荷）	15℃	40℃

6.2 PoE 最大供給電力 90W 対応にともなう仕様変更

 **「取扱説明書」 13、40、41、58、76、77 ページ**

 **「コマンドリファレンス」 / 「PoE」**

ファームウェアバージョン 2.4.0 から、装置全体の PoE 最大供給電力を 75W から 90W に拡張し、以下の仕様に変更されました。

- PoE 供給電力により下記の仕様差分があります。

PoE 供給電力	75W 時	90W 時
最大入力電流（実測値）	1.3A	1.6A
平均消費電力	58W（最大 110W）	66W（最大 130W）
平均発熱量	210kJ/h（最大 400kJ/h）	240kJ/h（最大 470kJ/h）
動作保証温度	0～50℃※ 1	0～45℃※ 2

※ 1 PoE 供給電力 75W までの動作保証温度

※ 2 PoE 供給電力 75W を超えて 90W までの動作保証温度

- 動作時温度に応じたファンの回転数を次のとおり変更しました。

	バージョン 2.3.3 まで	バージョン 2.4.0 から
低速回転	3000rpm	4000rpm
高速回転	5000rpm	5000rpm

- SET POE GUARDBAND コマンドで設定する PoE 電源最大供給電力のガードバンドの上限を 70W から 85W に変更しました。

6.3 ファンアラーム

 **「取扱説明書」 77 ページ**

 **「コマンドリファレンス」 / 「運用・管理」 / 「システム」**

本製品のファン回転には低速回転（4000rpm） / 高速回転（5000rpm）の2段階があり、それぞれ75%未満の回転時を異常状態として warning アラームを発行する仕様になっていますが、FAN Low(warning) から FAN High(warning) へ移行する場合とその逆の場合で、アラーム発行の動作が異なります。

FAN Low(warning) から FAN High(warning) へ移行する場合は、warning 状態は継続されますが、一度 recover アラームが発行された後、再度 warning アラームが発行されます。

FAN High(warning) から FAN Low(warning) へ移行する場合は、warning アラームは発行されず、warning の状態が引き継がれたままとなります。

6.4 ハードウェアパケットフィルター機能

 **「コマンドリファレンス」 / 「クラシファイア」**

ファームウェアバージョン 2.4.0 から、ハードウェア（ASIC）レベルで入力パケットをフィルタリング（許可・拒否）するハードウェアパケットフィルター機能をサポートしました。フィルタリング条件はヘッダー情報に基づいてパケットを分類するクラシファイアによって定義し、送信元 MAC アドレス、始点・終点 IP アドレス、プロトコル（ARP のみ）を使用できます。条件に一致したパケットに対しては、許可（permit）または破棄（deny）の処理が指定できます。クラシファイアの詳細についてはコマンドリファレンス「クラシファイア」を参照してください。

- ハードウェアパケットフィルターは、複数のエントリーをリストとして保持する「アクセスコントロールリスト（ACL）」から構成されます。エントリーは、クラシファイア（汎用パケットフィルター）とアクション、および適用対象のスイッチポート（入力ポート）で構成されます。パケット受信時のフィルター処理の大きな流れとしては、受信したパケットがエントリーにマッチするかどうか、ACL のエントリー ID の番号順に調べ、条件にマッチした場合は、残りの条件は調べずにその条件のアクションを実行し、エントリーにマッチしないパケットは出力します。
- ACL の仕様は、次のとおりです。
 - ・ 最大エントリー数は 64 個
 - ・ 同一ポートに複数のエントリーを割り当てることができる（ただし、同じクラシファイアを含むエントリーを、同一ポートに割り当ててはできない）
 - ・ 同一エントリーを複数ポートに割り当てることができる
 - ・ 1 ポートに割り当てられるクラシファイアの数、128 個まで（ポリシーベース QoS とハードウェアパケットフィルター機能合わせて）
 - ・ 同一のクラシファイアを、ポリシーベース QoS とハードウェアパケットフィルター機能の両方で使用可能
- ACL 設定時の注意事項は、次のとおりです。
 - ・ スイッチ本体（CPU）宛てのパケットに対し、ハードウェアパケットフィルター機能は動作する
 - ・ ハードウェアパケットフィルターと DHCP Snooping を併用した場合、DHCP パケットにはハードウェアパケットフィルターのフィルタリングは優先されず、DHCP Snooping による DHCP パケットの通信が許可される

- ACL からエントリーを削除しても、クラシファイアは削除されず、ACL とクラシファイアの関連付けが削除される。クラシファイアを削除するには、DESTROY CLASSIFIER コマンドを使用する
 - ハードウェアパケットフィルターでの ACL のエントリーにクラシファイアを割り当てた後、クラシファイアの設定を変更することはできない。クラシファイアの設定を変更するには、設定を解除してから行う
- ACL にエントリーを追加するのは CREATE ACL コマンドで、ACL エントリーの設定を変更するのは SET ACL コマンドで行います。

コマンド

```
CREATE ACL=0..255 [DESCRIPTION=string] [ACTION={DENY|PERMIT}]  
[CLASSIFIERLIST={rule-list|NONE}] [PORTLIST={port-  
list|ALL|NONE}]  
  
SET ACL=0..255 [DESCRIPTION=string] ACTION={DENY|PERMIT}  
CLASSIFIERLIST={rule-list|NONE} PORTLIST={port-  
list|ALL|NONE}
```

パラメーター

ACL: 作成・変更するエントリーの ID。エントリーを作成するとき、ID は連番でなくてもかまわない。

DESCRIPTION: エントリーの説明 (1～31 文字。空白を含む場合はダブルクォートで囲む)。

ACTION: パケットがクラシファイアに一致したときのアクション。PERMIT (許可)、DENY (破棄) から選択する。エントリー作成時のデフォルトは DENY。

CLASSIFIERLIST: ACL に対応づけるクラシファイアの ID を指定する (1～9999。ハイフン、カンマを使った複数指定も可能)。エントリー作成時のデフォルトは NONE

PORTLIST: ACL を割り当てるポートを指定する (1～。ハイフン、カンマを使った複数指定も可能)。エントリー作成時のデフォルトは NONE

備考・注意事項

作成したエントリーの順番を変えるときは、エントリーを削除し、作成し直す必要がある。

CREATE/SET CLASSIFIER コマンドで ACL に対応づけるクラシファイアを作成 / 設定するときに指定できるパラメーターは、MACSADDR/MACSMASK/PROTOCOL (ARP のみ指定可) /IPSADDR/IPDADDR。それ以外のパラメーターを設定したクラシファイアを ACL に関連付けた場合の動作はサポート対象外となる。

コマンド例

- ポート 6 で送信元 MAC アドレスが 00-00-f4-33-22-11 のパケットを破棄
CREATE CLASSIFIER=1 MACSADDR=00-00-f4-33-22-11
CREATE ACL=1 ACTION=DENY CLASSIFIERLIST=1 PORTLIST=6
- すべてのポートで 192.168.20.100 のみ双方向の通信を許可
CREATE CLASSIFIER=1 IPDADDR=192.168.20.100/32
CREATE CLASSIFIER=2 IPSADDR=192.168.20.100/32

```
CREATE CLASSIFIER=3 PROTOCOL=ARP
CREATE CLASSIFIER=4
CREATE ACL=1 ACTION=PERMIT CLASSIFIERLIST=1 PORTLIST=ALL
CREATE ACL=2 ACTION=PERMIT CLASSIFIERLIST=2 PORTLIST=ALL
CREATE ACL=3 ACTION=PERMIT CLASSIFIERLIST=3 PORTLIST=ALL
CREATE ACL=4 ACTION=DENY CLASSIFIERLIST=4 PORTLIST=ALL
```

- ACL エントリーの削除は DESTROY ACL コマンドで、ACL の設定を工場出荷時の状態に戻すのは PURGE ACL コマンドで行います。

コマンド

```
DESTROY ACL=0..255
```

```
PURGE ACL
```

パラメーター

ACL: 削除するエントリーの ID。

- ACL エントリーの表示は SHOW ACL コマンドで行います。

コマンド

```
SHOW ACL [= {id-list} | ALL ]
```

パラメーター

ACL: 表示するエントリーの ID (0 ~ 255)。ハイフン、カンマを使った複数指定も可能)。省略時および ALL を指定した場合は、すべてのエントリー情報が表示される。

入力・出力・画面例

```
Manager > show acl

-----
ACL ID ..... 1
Description .....
Action ..... Deny
Classifier List ..... 1
Port List ..... 8
Is Active ..... Yes
```

ACL ID	エントリーの ID
Description	エントリーの説明
Action	パケットがクラシファイアに一致したときのアクション。Permit または Deny
Classifier List	クラシファイアの ID
Port List	エントリーを割り当てるポート
Is Active	エントリーがポートに割り当てられている (Yes) または、割り当てられていない (No)

- ACL に割り当てられているクラシファイアごとのカウンターの表示は SHOW ACL COUNTER コマンドで行います。

コマンド

SHOW ACL[={id-list|ALL}] COUNTER

パラメーター

ACL: 表示するエントリーの ID (0 ~ 255。ハイフン、カンマを使った複数指定も可能)。省略時および ALL を指定した場合は、すべてのエントリー情報が表示される。

入力・出力・画面例

```
Manager > show acl counter
```

ACL	Classifier	Hit Counter
1 ACL 1	1 Classifier 1	334412
2 ACL 2	2 Classifier 2	1349
3 ACL 3	3 Classifier 3	1394055485
4 ACL 4	4 Classifier 4	4348500

ACL	ACL ID と CREATE ACL コマンドで設定したエントリーの説明を表示。設定されていない場合、"ACL id" フォーマットで表記
Classifier	クラシファイア ID と CREATE CLASSIFIER コマンドで設定したクラシファイアの説明を表示。設定されていない場合、"Classifier id" フォーマットで表記
Hit Counter	フィルターにマッチした数を表示

- 指定された ACL に割り当てられているクラシファイアのカウンターのリセットは RESET ACL COUNTER コマンドで行います。

コマンド

RESET ACL[={id-list|ALL}] COUNTER

パラメーター

ACL: カウンターをリセットするエントリーの ID (0 ~ 255。ハイフン、カンマを使った複数指定も可能)。省略時および ALL を指定した場合は、すべての ACL に割り当てられているクラシファイアのカウンターのリセットする。

6.5 ポリシーベース QoS の最大帯域



「コマンドリファレンス」 / 「QoS」 / 「ポリシーベース QoS」

コマンドリファレンスの「最大帯域（帯域制限）」についての記載に誤りがありました。下記のとおり訂正して、お詫びいたします。

誤：

Note - 実際に制限される帯域は、MAXBANDWIDTH パラメーターで設定された最大帯域幅より高いレートとなる場合があります。トラフィックのフレームサイズが小さいほど誤差が大きくなり、最大 15Mbps 程度の誤差が発生します。

正：

Note - 本機能はネットワークの帯域幅ではなく、実際に転送するフレームに対する L2 ヘッダーを含むデータの転送速度の帯域を制限します。

MAXBANDWIDTH パラメーターで設定される最大帯域幅にはイーサネットフレームのプリアンブルなどのオーバーヘッドは含まれないため、トラフィックのフレームサイズが小さいほど誤差が大きくなり、設定値に対して最大 1.5 倍程度の誤差が発生します。

6.6 SET SWITCH PORT コマンド

 **参照** 「コマンドリファレンス」 / 「スイッチング」

コマンドリファレンスの SET SWITCH PORT コマンドの SPEED パラメーターについての記載に一部誤りがありました。下記のとおり訂正して、お詫びいたします。

誤：

GS908M V2 の SFP ポートおよび GS916M V2、GS924M V2 のコンポポートでは AUTONEGOTIATE または 1000MFULL のみ設定可能。GS908M V2-4PS の SFP ポートでは AUTONEGOTIATE、100MFULL または 1000MFULL を設定可能。

正：

GS908M V2 の SFP ポートでは AUTONEGOTIATE または 1000MFULL のみ設定可能。GS916M V2、GS924M V2 のコンポポートおよび GS908M V2-4PS の SFP ポートでは AUTONEGOTIATE、100MFULL または 1000MFULL を設定可能。

6.7 SHOW SWITCH PORT コマンド

 **参照** 「コマンドリファレンス」 / 「スイッチング」

コマンドリファレンスの SHOW SWITCH PORT コマンドで表示される Port Type(Combo Actual) についての記載に誤りがありました。下記のとおり訂正して、お詫びいたします。

誤：

ポートの種類。コンボ（共用）ポートの場合は、コンポポートの設定により、次のように表示。FIBERAUTO 設定時はリンクしているメディア、FIBER 設定時は 1000Base-X SFP、COPPER 設定時は 10/100/1000BASE-T

正：

ポートの種類。コンボ（共用）ポートの場合は、コンポポートの設定により、次のように表示。FIBERAUTO 設定時はリンクしているメディア、FIBER 設定時は 100Base-X SFP（100MFull 設定時）、1000Base-X SFP（Autonegotiate 設定時）、COPPER 設定時は 10/100/1000BASE-T

6.8 トランクグループに所属するポートの VLAN 設定変更

 **参照** 「コマンドリファレンス」 / 「スイッチング」

ファームウェアバージョン 2.3.2 から、トランクグループに所属するポートの VLAN 設定を変更することが可能になりました。

6.9 LDF 検出

 **参照** 「コマンドリファレンス」 / 「スイッチング」

- LDF のデフォルト送信間隔は 120 秒です。LDF の検出時間を短くしたいときは、SET SWITCH LOOPDETECTION コマンドの INTERVAL パラメーターで送信間隔を短く設定してください。LDF 検出機能の効果を最大にするには、送信間隔を最小値の 1 秒に設定する必要があります。ただし、送信間隔を短くするとソフトウェア処理に負荷がかかり、本製品宛て通信の応答時間など、他の機能の動作性能が低下する可能性があります。

- 対向機器のポート間でループが発生したような場合、対向機器のフローコントロール機能などにより、送信した LDF を本製品が受信できない可能性があります。その場合、LDF 検出によるループガード機能は動作しません。

6.10 EPSR リングポートと LDF の併用

参照 「コマンドリファレンス」/「スイッチング」/「EPSRアウェア」

ファームウェアバージョン 2.3.2 から、EPSR リングポートと LDF 検出機能の併用が可能になりました。

6.11 ポート認証

参照 「コマンドリファレンス」/「ポート認証」

- ポート認証機能において、SET AUTHENTICATION コマンドの DEAD-ACTION パラメーターに PERMIT を指定し、RADIUS サーバーからの応答がないときに通信を許可するよう設定する場合は、下記の条件を満たすように各パラメーターを設定してください。

SERVERTIMEOUT > $\text{TIMEOUT} \times (\text{RETRANSMITCOUNT} + 1) \times \text{RADIUS サーバー数}$

SERVERTIMEOUT SET PORTAUTH PORT コマンドのパラメーター。デフォルト 30 秒 (MAC ベース認証ポートでは 30 秒固定)

TIMEOUT SET AUTHENTICATION コマンドのパラメーター。デフォルト 6 秒

RETRANSMITCOUNT SET AUTHENTICATION コマンドのパラメーター。デフォルト 3 回

RADIUS サーバー数 ADD RADIUSSERVER SERVER コマンドで登録した RADIUS サーバーの数

特に RADIUS サーバーを 2 台登録する場合は、各パラメーターがデフォルトのままだと条件を満たさないため、条件を満たすように設定を変更する必要があります。

- ポート認証機能でゲスト VLAN やダイナミック VLAN を使用し、Supplicant が DHCP サーバーから IP アドレスを取得する場合は、認証前の VLAN において DHCP サーバーのリースタイムを短く設定する必要があります。

6.12 リンクダウンをともなわない認証ポートの移動

参照 「コマンドリファレンス」/「ポート認証」

ファームウェアバージョン 2.3.2 から、802.1X 認証、WEB 認証において、リンクダウンをともなわない認証ポートの移動が可能になりました。

6.13 Web GUI

参照 「コマンドリファレンス」/「Web GUI」/「マネージメント」

Internet Explorer 7 以上を使用し、コンフィグファイルやファームウェアを転送する場合の注意事項に、Internet Explorer 9 に関して以下のとおり補足します。

- 「Internet Explorer 7 以上を使用する場合の注意」の Note を下記のように変更します。
変更前：
Note - 本設定は、Internet Explorer 7 ではデフォルト有効に、Internet Explorer 8 ではデフォルト無効になっています。
変更後：
Note - 本設定は、Internet Explorer 7 ではデフォルト有効に、Internet Explorer 8 / 9 ではデフォルト無効になっています。
- 「Internet Explorer 8 を使用する場合の注意」の見出し名を「Internet Explorer 8 / 9 を使用する場合の注意」に変更し、最初の説明文を下記のように変更します。

変更前：

Internet Explorer 8 で SmartScreen フィルター機能を有効にしていると、設定ファイルの取得に時間がかかる場合があります。この現象を回避するには、以下の方法を実行してください。

変更後：

Internet Explorer 8 / 9 で SmartScreen フィルター機能を有効にしていると、設定ファイルの取得に時間がかかる場合があります。この現象を回避するには、以下の方法を実行してください。

7 未サポートコマンド (機能)

以下のコマンド (パラメーター) はサポート対象外ですので、あらかじめご了承ください。

```
SET HTTP SERVER PORT
SET SYSTEM LANG
SET SYSTEM FAN
RESET PORTAUTH PORT
LOAD METHOD=TFTP FILE=filename SERVER=ipadd BOOT
SET IGMPSPNOOPING HOSTSTATUS
SET MLDSNOOPING HOSTSTATUS
SHOW DHCPSPNOOPING DATABASE NVS
SHOW DHCPSPNOOPING HWFILTER
```

8 最新マニュアルについて

最新の取扱説明書「CentreCOM GS900M V2 シリーズ 取扱説明書」(613-001184 Rev.B)、コマンドリファレンス「CentreCOM GS900M V2 シリーズ コマンドリファレンス 2.3.2」(613-001180 Rev.E) は弊社ホームページに掲載されています。

本リリースノートは、これらの最新マニュアルに対応した内容になっていますので、お手持ちのマニュアルが上記のものでない場合は、弊社 Web ページで最新の情報をご覧ください。

<http://www.allied-telesis.co.jp/>