J613-M0019-04 Rev.E 060327

Allied Telesis

CentreCOM® 8724SL/8748SL リリースノート

この度は、CentreCOM 8724SL/8748SL（以下、CentreCOM を省略）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（J613-M0019-00 Rev.A）とコマンドリファレンス（J613-M0019-01 Rev.D）の補足や、ご使用の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　ソフトウェアバージョン　2.7.3-09

2　重要：2.6.1 pl12 以前からバージョンアップするときの注意事項

ソフトウェアバージョン **2.6.1 pl12** 以前から **2.7.3-09** にバージョンアップすると、最初の再起動時に「設定なし」の状態で起動する場合があります。

このようなときは、バージョンアップ後にコンソールからログインし、SET CONFIG コマンドで起動時設定ファイルを指定しなおした後、本製品を再起動してください。例えば、バージョンアップ前に mynet.cfg という設定ファイルを使用していた場合は、次のようにします。

```
SET CONFIG=mynet.cfg
RESTART SWITCH
```

また、リモートからバージョンアップを行うときは、バージョンアップ後アクセス不能に陥ることを避けるため、次の手順にしたがってバージョンアップを行ってください。

1. バージョン **2.6.1 pl12** 以前で動作している本製品にログインします。
2. 次のコマンドを実行し、Boot configuration file: に表示されるファイル名をメモします。

   ```
   SHOW CONFIG
   ```

3. 次のコマンドを実行し、現在の設定を boot.cfg に保存します。boot.cfg は、「設定なし」で起動したときに自動実行される特殊なファイルです。

   ```
   CREATE CONFIG=boot.cfg
   ```

4. ログアウトします。
5. 「バージョンアップ手順書」の指示にしたがって、**2.7.3-09** にバージョンアップします。
6. バージョン **2.7.3-09** で動作している本製品にログインします。
7. 次のコマンドを実行します。xxxx には手順 2 でメモしたファイル名を指定します。

   ```
   SET CONFIG=xxxx
   ```

8. 手順 3 で作成した boot.cfg を削除します。

   ```
   DELETE FILE=boot.cfg
   ```

9. 以上です。

3 本バージョンで追加された機能

ソフトウェアバージョン **2.7.3-06** から **2.7.3-09** 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。

3.1 追加コマンド：ENABLE/DISABLE SWITCH FILTER VLANSECURE

参照 「コマンドリファレンス」/「スイッチング」/「ポート」

ポートセキュリティー機能において、ルーティングパケットおよび本体宛のパケットに対するポートセキュリティー動作の有効 / 無効を設定するコマンドが追加されました。デフォルトは有効です。

ENABLE SWITCH FILTER VLANSECURE

ルーティングパケットおよび本体宛のパケットにおいてポートセキュリティーの動作が有効となります。

DISABLE SWITCH FILTER VLANSECURE

ルーティングパケットおよび本体宛のパケットにおいてポートセキュリティーの動作が無効となります。

備考

本コマンドで動作に影響があるのは、ADD SWITCH FILTER コマンドで ACTION=FORWARD パラメーターを指定した場合のみになります。

4 本バージョンで修正された項目

ソフトウェアバージョン **2.7.3-06** から **2.7.3-09** 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 SSH サーバー有効時、大量の TCP Syn パケットを受信すると SSH サーバー機能が停止していましたが、これを修正しました。

4.2 MAC アドレスフィルターを 300 件登録したポートをリセットすると、CPU 使用率が 100% になっていましたが、これを修正しました。

4.3 スパニングツリープロトコルとスタティックエントリーの併用時、BPDU が正常に受信できないため、ポートの状態が Blocking にならず Forwarding となっていましたが、これを修正しました。

4.4 ポートセキュリティー使用時、フォワーディングデータベースが更新されない場合がありましたが、これを修正しました。

4.5 ルーティングパケットと本体（CPU）宛てのパケットに対して、フォワーディングデータベース（FDB）のスタティックエントリーが機能しませんでしたが、これを修正しました。

4.6 ADD SWITCH L3FILTER ENTRY コマンドで EPORT パラメーターを指定した場合、フィルター対象パケットの終点 IP アドレスが L3 テーブルに登録されていないと、NODROP アクションが機能しませんでしたが、これを修正しました。

4.7 ソフトウェア IP フィルターにおいて特定パラメーターを設定した場合、エントリーの設定順序によってスループットに差が出る場合がありましたが、ロジックの最適化を行い、設定順序に依存せず、より高速となるよう動作を改善しました。

4.8 ハードウェア IP フィルターの動作に問題がありましたが、これを修正しました。

4.9 ADD SWITCH L3FILTER ENTRY コマンドでフィルタリング条件に IPORT、EPORT パラメーターの両方を指定（または EPORT のみ指定）した場合、条件にマッチしない場合でもフィルター処理されてしまうことがありましたが、これを修正しました。

4.10 RESET PORTAUTH PORT コマンドに SUPPLICANTMAC パラメーターを指定して実行すると、対象 Supplicant 情報ばかりではなく、ポート上のすべての Supplicant の MAC アドレスを FDB から削除していましたが、これを修正しました。

4.11 RIP バージョン 2 使用時、ネットワークアドレスが同じでサブネットマスクの異なる複数の経路情報を持っている場合、優先度の最も高い（Preference 値が最も小さい）経路だけを通知していましたが、これを修正しました。

4.12 AS External LSA Type が正しく設定されませんでしたが、これを修正しました。

4.13 ADD BGP コマンドの CONFEDERATIONPEER パラメーターをコンフィグに設定すると、リブート時にエラーになっていましたが、これを修正しました。

4.14 IP ルートフィルターに、制限を超える 100 以上のフィルターが追加できていましたが、これを修正しました。

4.15 ADD/SET IP FILTER コマンドで OPTIONS パラメーターを指定した場合、フィルターが正しく動作しませんでしたが、これを修正しました。

4.16 IP フィルター関連のログメッセージが不適切でしたが、これを修正しました。

4.17 UDP ブロードキャストパケットの転送機能を有効にした場合、パケットの宛先 MAC アドレスに本製品自身の MAC アドレスをセットするようなディレクティドブロードキャストパケットを転送するよう修正しました。

4.18 特定のネットワーク宛の経路が複数ある環境で、IPv6 ルートテーブルの情報が更新された後、メトリックが小さいパスを使用しませんでしたが、これを修正しました。

4.19 IPv6 の Neighbour をスタティック登録していても、他のポートから NA パケットを受信すると Neighbour キャッシュのポート番号が書き換えられていましたが、これを修正しました。

4.20 IGMP Snooping 使用時、複数のメンバーが存在するマルチキャストグループから 1 つのメンバーが脱退すると、SHOW IGMPSNOOPING コマンドで表示される Entry timeout が更新されていましたが、これを修正しました。

4.21 Protected VLAN と VRRP を併用したインターフェースにおいて、FDB が重複して登録されていましたが、これを修正しました。

4.22 Protected VLAN と VRRP を併用したインターフェースにおいて、VRRP の状態が Backup から Master に移行したインターフェースでの通信が行えなくなっていましたが、これを修正しました。

4.23 CREATE VRRP コマンドで ADOPTVRIP パラメーターを ON に設定している場合に、マスタールーターからバーチャルルーター宛ての通信ができませんでしたが、これを修正しました。

また以下の 項目は、ソフトウェアバージョン **2.7.3-06** のリリースノートに制限事項として記載されていましたが、実際には **2.7.3-06** で修正済みでした。お詫びして訂正いたします。

4.24 MIB-II の ifInErrors が正しくカウントアップされませんでしたが、これを修正しました。

4.25 SET SWITCH L3FILTER ENTRY コマンドの実行時、変更したエントリーと既存のエントリーの間に矛盾が生じた場合、変更したエントリーが無条件に削除されていましたが、これを修正しました。

4.26 802.1X Multi-Supplicant モードの Authenticator ポートに対して DISABLE SWITCH PORT コマンドを実行しても、認証済み Supplicant のスイッチフィルターエントリーが削除されないという現象において、残ったエントリーを手動で削除するとリブートしていましたが、リブートしないよう修正しました。

4.27 TRACE コマンドの実行完了前に次の TRACE を実行すると、本製品がリブートすることがありましたが、これを修正しました。

4.28 マルチホーミングした IP インターフェース上にスタティック ARP エントリーを登録する場合、存在しない論理インターフェースを ADD IP ARP コマンドの INTERFACE パラメーターに指定すると、システムがリブートしていましたが、これを修正しました。

4.29 IGMP 有効時、Non-Querier のときでも、Leave メッセージを受信すると Refresh タイマーを更新していましたが、これを修正しました。

4.30 MLD Snooping において、IGMP Query、RIP などの IPv4 のルーターパケットを受信した際に、内部テーブルの All Group エントリーにその受信ポートを追加していましたが、これを修正しました。

4.31 ファイアウォールにおいて不正な ACK 番号を持つ TCP セグメントに対しても ACK を返していましたが、これを修正しました。

4.32 本製品を DHCP サーバーとして使用している場合、Mac OS X など一部の OS を搭載したコンピューターがスリープ状態から復帰するときに IP アドレスを取得できない場合がありましたが、これを修正しました。

5 本バージョンでの制限事項

ソフトウェアバージョン **2.7.3-09** には、以下の制限事項があります。

5.1 認証サーバー

参照 「コマンドリファレンス」/「運用・管理」/「認証サーバー」

Supplicant が RADIUS 認証を受けた後、Authenticator が START 属性を持つ Accounting-Request メッセージを RADIUS サーバーに送信しません。

5.2 ログ

参照 「コマンドリファレンス」/「運用・管理」/「ログ」

○ SET LOG OUTPUT コマンドで PERMANENT ログの設定を変更すると、既存のログが削除されます。

○ DESTINATION=NVS のログ出力先定義に対し、SET LOG OUTPUT コマンドで MESSAGES パラメーター（保存件数）を変更すると、すでに NVS 上に保存されていたメッセージがすべて消去されます。

○ PERMANENT ログの最大格納メッセージ数はデフォルト設定では 20 ですが、新たに作り直すと最大格納メッセージ数が 50 に変わります。

5.3 SNMP

参照 「コマンドリファレンス」/「運用・管理」/「SNMP」

○ イーサネット MIB の dot3StatsFrameTooLongs が正しくカウントアップされません。

○ ブロードキャスト受信時に、VLAN インターフェースの ifInDiscards がカウントされます。

○ topologyChange トラップと newRoot トラップが送信されません。

○ dot3StatsCarrierSenseErrors の値が取得できません。

○ プライベート MIB の instRelMajor、instRelMinor、instRelInterim の値を取得できません。

5.4 SET TTY コマンドの PAGE パラメーター

参照「コマンドリファレンス」/「運用・管理」/「ターミナルサービス」

SET TTY コマンドの PAGE パラメーターに OFF を指定した場合、この設定変更を CREATE CONFIG コマンドでファイルに正しく保存できません。

5.5 Telnet セッション数の制限

参照「コマンドリファレンス」/「運用・管理」/「ターミナルサービス」

SET TELNET コマンドの MAXSESSIONS パラメーター（同時に確立可能な Telnet セッション数）が正しく動作しません。実際には、指定した値 +2 として扱われます。たとえば、MAXSESSIONS=3 と設定した場合、MAXSESSIONS=5 として動作します。

5.6 フローコントロール

参照「コマンドリファレンス」/「スイッチング」/「ポート」

DISABLE SWITCH PORT FLOW コマンドでフローコントロールを無効にした後、CREATE CONFIG コマンドで設定を保存し、SET CONFIG コマンドで保存したファイルを起動時設定ファイルに指定すると、システム再起動時にエラーが表示され、フローコントロールが無効になりません。設定ファイルを EDIT コマンドで開き、「flow=jamming,pause」の部分を「flow=pause」に修正するか、再起動トリガーを使用して対処してください。

5.7 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」/「ポート」

○ CREATE SWITCH TRUNK コマンドで複数のトランクグループを作成後、設定を保存して再起動すると、トランクグループの設定が作成時と異なる順序で読み込まれるため、表示上の順序が変更されます。なお、動作には問題ありません。

○ ポートトランキングと IGMP Snooping の併用時、マスターポートがリンクダウンすると SHOW IGMPSNOOPING コマンドで表示される Entry timeout 値が更新されます。これは表示だけの問題であり、動作には影響ありません。
（「マスターポート」はトランクグループ内で最初にリンクアップしたポートを示します）

○ ポートトランキングと DVMRP の併用時、マルチキャストデータの転送ができなくなることがあります。

○ CREATE SWITCH TRUNK コマンドの PORT パラメーターでトランクポートを指定した場合、指定ポートがマルチプル VLAN（Private VLAN）の同一グループ所属であるかのチェックが行われません。これを回避するため、マルチプル VLAN とポートトランキングを併用するときは、先にトランクグループを作成してから、トランクグループをマルチプル VLAN に割り当ててください。

5.8 ポートセキュリティー

参照「コマンドリファレンス」/「スイッチング」/「ポート」

ポートセキュリティーがオンのポートで受信したパケットの VLAN ID が、ポートの所属 VLAN と一致しない場合でも、アドレスを FDB に登録します。

5.9 LACP（IEEE802.3ad）

参照「コマンドリファレンス」/「スイッチング」/「LACP (IEEE802.3ad)」

LACP によって自動生成されたトランクグループのメンバーポートに対して CREATE SWITCH TRUNK コマンドを実行すると、通信ができなくなります。

5.10 バーチャル LAN

参照「コマンドリファレンス」/「スイッチング」/「バーチャル LAN」

Protected VLAN のポートをミラーリングポートに設定すると、Protected VLAN のポート間で通信ができてしまいます。

5.11 スパニングツリープロトコル

参照「コマンドリファレンス」/「スイッチング」/「スパニングツリープロトコル」

○ スパニングツリープロトコル（STP）有効時に ADD VLAN PORT コマンドを実行すると、VLAN 内のすべてのポートにおいて、STP のポートステータスが初期化されます。

○ Rapid モードで非ルートブリッジとして動作している場合、ポートが Discarding 状態から Forwarding 状態に遷移するときのフォワードディレイタイムとして、ルートブリッジの値ではなく自身の設定値を使用します。

○ タグ付きポート上で LACP とスパニングツリープロトコル（STP）を併用した場合、SHOW STP PORT コマンドによるポート情報が正しく表示されません。なお、これは表示だけの問題であり、動作には影響ありません。

○ スパニングツリープロトコル（STP）有効時に Topology Change が発生すると、すべてのポートから ARP エントリーが削除されます。

○ Topology change が起きた後、FDB が正常に登録されないことがあります。（通信の動作に影響はありません。）

5.12 ハードウェア IP フィルター

参照「コマンドリファレンス」/「スイッチング」/「ハードウェア IP フィルター」

○ 8748SL では、ポート 25 ～ 48 とポート 49 で受信したパケットに対して、ハードウェア IP フィルターの SENDNONUNICASTTOPORT、SENDEPORT アクションが機能しません。

○ ADD SWITCH L3FILTER MATCH コマンドで IMPORT=False、または EMPORT=False を指定すると、IMPORT=True、EMPORT=True の設定で動作します。False で動作させたい場合は、IMPORT、EMPORT パラメーターを指定しないでください (デフォルトで False の設定になります)。

○ ADD IP FILTER ENTRY コマンドで複数の IP フィルターを登録する場合、設定が適用されずエラーが出力されることがあります。この場合は、IP フィルターの入力順序を変更して登録してください。

○ ADD SWITCH L3FILTER ENTRY コマンドで EMPORT と ACTION=NODROP のパラメーターを指定したとき、条件にマッチしたパケットの送信先 ARP が登録されていない場合、ARP 解決（ARP Request 送信）をすべきですが、行われません。

5.13 ポート認証

参照「コマンドリファレンス」/「スイッチング」/「ポート認証」

○ 802.1X Multi-Supplicant モードの Authenticator ポートでは、Port Status が authorised でも IGMP Query パケットがフラッディングされません。

○ DISABLE PORTAUTH コマンドを実行しても、認証済み Supplicant のスイッチフィルターエントリーが削除されません。

○ ENABLE/SET PORTAUTH PORT コマンドの SERVERTIMEOUT パラメーターが正しく動作しません。これは、SET RADIUS コマンドの TIMEOUT パラメーターと RETRANSMITCOUNT パラメーターの設定が優先されているためです。SET RADIUS コマンドで TIMEOUT × (RETRANSMITCOUNT + 1) の値を SERVERTIMEOUT より大きく設定した場合は、SERVERTIMEOUT の設定が正しく機能します。

○ 802.1X Multi-Supplicant モードの Authenticator ポートに対して DISABLE SWITCH PORT コマンドを実行しても、認証済み Supplicant のスイッチフィルターエントリーが削除されません。（残ったエントリーは手動で削除できます。）

○ RADIUS サーバーによってダイナミック VLAN を割り当てられた Supplicant がリンクダウン、ログオフなどで存在しなくなった場合、プライベート MIB である AuthPreAuthVlan、AuthPostAuthVlan が不正な値を返します。

5.14 IP 統計情報

参照「コマンドリファレンス」/「IP」

ファイアウォール有効時、SHOW IP INTERFACE COUNTER コマンドで表示される受信パケットカウンター（ifInPkts、ifInBcastPkts、ifInUcastPkts、ifInDiscards）に、実際の受信パケット数の 2 倍の値が表示されます。

5.15 ICMP メッセージ

参照「コマンドリファレンス」/「IP」

ICMP Host Unreachable メッセージの送信に時間がかかることがあります。

5.16 TRACE コマンド

参照「コマンドリファレンス」/「IP」

SET TRACE コマンドで値を設定し、SHOW TRACE コマンドで表示すると、設定した値が正しく表示されない場合があります。

5.17 ADD IP ROUTE コマンド

参照「コマンドリファレンス」/「経路制御」

ADD IP ROUTE コマンドで METRIC1 パラメーターに値を指定し、METRIC2 パラメーターには値を指定しない場合、METRIC2 パラメーターに省略時の 1 が設定されず、METRIC1 パラメーターで指定した値が設定されます。

5.18 OSPF

参照「コマンドリファレンス」/「IP」/「経路制御（OSPF)」

○ OSPF インターフェースの IP アドレスを変更すると、その後 IP アドレスを元に戻しても OSPF の隣接関係が回復しません。

○ IP ルートテーブルにデフォルトルートがなくても、SET OSPF コマンドで DEFROUTE=ON を指定した場合は、デフォルトルートを LSA として追加します。

○ ADD OSPF STUB または ADD OSPF HOST コマンドがすでに設定されている状態で同一コマンドを再入力すると、OSPF の Hello パケットの送受信が行われなくなります。この場合は、RESET OSPF コマンド、RESET OSPF INTERFACE コマンド、DISABLE / ENABLE OSPF コマンドのいずれかを入力するか、設定ファイルを保存後再起動してください。

○ メトリックが等しくない複数の経路が存在する場合、LSDB 上は各経路のメトリックが等しくないにもかかわらず、IP ルートテーブルには同一メトリックの経路として反映されるため、意図しない経路へのトラフィックが発生し、最適な経路が選択されない場合があります。

○ ASBR の OSPF インターフェースに設定されているネットマスク値と ADD OSPF RANGE コマンドの MASK パラメーターで指定するネットマスク値が異なっていると、ABR から受信した ASBR サマリー LSA の情報が経路表に反映されない場合があります。
使用する OSPF インターフェースに設定されているネットマスク値で ADD OSPF RANGE コマンドの MASK パラメーターの指定を行ってください。

○ SET OSPF コマンドで DEFROUTE パラメータが OFF の状態でも、スイッチはデフォルトルート (0.0.0.0) を External Route としてインポートします。

○ AS external デフォルトルートの TYPE を変更し、RESET OSPF コマンドを実行すると、デフォルトルートが LSA から消去されます。

5.19 BGP-4

参照「コマンドリファレンス」/「IP」/「経路制御（BGP-4)」

○ ADD BGP PEER コマンド、SET BGP PEER コマンドの EHOPS パラメーターが機能しません。

○ プライベート AS フィルターを有効にすると、自身のプライベート AS 番号まで削除してしまいます。

○ 経路情報を E-BGP に再通知するときに、以下の条件において MED 属性が付加されたまま UPDATE メッセージが送信されます。
- ADD/SET BGP PEER コマンドの INROUTEMAP パラメーターで適用されたルートマップによって MED 属性が付加された場合
- ADD/SET BGP IMPORT コマンドの ROUTEMAP パラメーターで適用されたルートマップによって MED 属性が付加された場合

○ SET BGP PEER コマンドの MAXPREFIX パラメーターを設定した場合、最大プレフィックス数を超えてセッションが終了したにもかかわらず、TCP Syn パケットを送出し続けます。

○ ADD BGP AGGREGATE コマンドによって集約経路エントリーを設定した場合、設定したプレフィックスよりも具体的でない（マスクが短い）BGP 経路も通知されてしまうことがあります。

○ ADD IP ROUTEMAP コマンドおよび ADD IP COMMUNITYLIST コマンドにおいて、BGP コミュニティーの指定のとき、「asn:xxx」形式で AS 番号（asn）に 0 を指定すると、コマンドがエラーになり正常に登録されません。
単一の 32 ビット整数値（= asn × 65536 + xxx）で指定すると正常に登録できます。

5.20 DNS サーバーアドレスの動的取得

参照「コマンドリファレンス」/「IP」/「名前解決」

ADD IP DNS コマンドの INTERFACE パラメーターで、DNS サーバーアドレスを DHCP で動的に取得するよう設定していないにもかかわらず、DNS サーバーアドレスが動的に取得されます。

5.21 DNS キャッシュ

参照「コマンドリファレンス」/「IP」/「名前解決」

DNS キャッシュ機能のキャッシュサイズを 1 に設定した場合、最初のキャッシュエントリーがエージングも上書きもされずに残り続けます。キャッシュサイズを 1 に設定しないでください。

5.22 ARP

参照「コマンドリファレンス」/「IP」/「ARP」

○ Gratuitous ARP パケットの受信時、受信インターフェースと異なるネットワークの IP アドレスであっても、そのアドレスを ARP キャッシュに登録します。

○ ARP テーブルからスタティックエントリーを削除すると本製品から ARP Request が送信されますが、Reply を受信しても該当ホストのエントリーが ARP テーブルに登録されません。

5.23 IPv6

参照「コマンドリファレンス」/「IPv6」

○ IPv6 において、インターフェースがダウンした場合、Lifetime フィールドが 0 のルーター通知（RA）パケットが送信されません。

○ ルーター通知（RA）において、SET IPV6 PREFIX コマンドでパラメーターに ONLINK=NO を指定して実行すると、プレフィックス情報オプションの L フラグだけでなく、A フラグ（AUTONOMOUS パラメーター）もオフになってしまいます。

○ IPv6 のループ構成でポイズンリバースが動作しません。

○ ADD IPV6 PREFIX コマンドを、IPv6 インターフェースと同じ IPv6 アドレス / プレフィックス長を指定して実行した場合、コマンドが反映されません。これを回避するには、EDIT コマンドで直接設定ファイルに記入するか、再起動トリガーを使用して起動直後に同コマンドを実行させるかしてください。

○ SET IPV6 INTERFACE コマンドで PREFERRED と VALID の値を INFINITE に変更しても、RA パケットに反映されません。これを反映させるには、コンフィグを保存して再起動を行ってください。

○ 存在しない link-local アドレス宛ての ICMP Request を受信すると、本体がリブートすることがあります。

5.24 RIPng

参照「コマンドリファレンス」/「IPv6」/「経路制御（RIPng）」

RIPng においてトリガーアップデートが動作しません。

5.25 SET IPV6 PREFIX コマンド

参照「コマンドリファレンス」/「IPv6」/「近隣探索」

SET IPV6 PREFIX コマンドの設定をした場合、コマンド入力直後は正しく機能しますが、CREATE CONFIG コマンドで設定を保存しても同コマンドが書き込まれません。これを回避するには、EDIT コマンドで直接設定ファイルに記入するか、再起動トリガーを使用して起動直後に同コマンドを実行させるかしてください。

5.26 DVMRP

参照「コマンドリファレンス」/「IP マルチキャスト」/「DVMRP」

○ DVMRP が有効で、IGMP Snooping が無効のとき、マルチキャストデータがフラッディングされません。

○ DVMRP とタグ VLAN の併用時、マルチキャストデータが正常にルーティングされないことがあります。

5.27 PIM

参照「コマンドリファレンス」/「IP マルチキャスト」/「PIM」

○ （PIM-DM/PIM-SM）マルチキャストデータの通信負荷が高いと、PIM パケットを処理できず、マルチキャスト通信が途絶えることがあります。これを避けるには、次のようなハードウェア IP フィルターを設定し、PIM パケットを優先的に処理させるようにしてください。

```
ADD SWITCH L3FILTER MATCH=DIP DCLASS=HOST
ADD SWITCH L3FILTER=1 ENTRY DIP=224.0.0.13 PRIO=5 AC=SENDC
```

○ PIM-SM 関連のログと SNMP トラップを有効にしていても（SET PIM LOG コマンド）、PIM インターフェース削除時のログとトラップが生成されません。

○ （PIM-SM）PIM インターフェースでメンバーからの IGMP Leave メッセージを受信しても、該当インターフェースが下流インターフェースのエントリーから削除されないため、マルチキャストパケットがフラッディングされます。

○ （PIM-DM/PIM-SM）PIM モジュール有効時、同一インターフェース上で 1000 グループ程度のマルチキャストを転送すると CPU 負荷が 100%になる、または本製品がリブートすることがあります。

○ （PIM-SM）DR でないインターフェースにおいて、マルチキャストグループが登録されている状態で IGMP Report を受信すると、PIM Join メッセージを送信します。

○ （PIM-SM）すべてのポートがリンクダウンしている状態で ADD PIM BSRCANDIDATE を実行すると、Warning メッセージが表示されます。

5.28 IGMP Snooping

参照「コマンドリファレンス」/「IP マルチキャスト」/「IGMP Snooping」

○ SET IGMPSNOOPING ROUTERMODE コマンドでパラメーターに NONE を指定しても、224.0.0.1 および 224.0.0.2 からのマルチキャストパケットを受信した場合には All Group を作成します。All Group を作成しない場合は、DISABLE IP IGMP ALLGROUP コマンドを使用してください。

○ IGMP Snooping 機能において、メンバーの存在しないグループ宛てのパケットが転送されることがあります。

○ IP の設定がされていないと、Leave メッセージを受信したときに受信ポートをグループから削除します。

5.29 PIM（IPv6 マルチキャスト）

参照「コマンドリファレンス」/「IPv6 マルチキャスト」/「PIM」

同一送信元 IP アドレスからのマルチキャストを受信すると、受信したインターフェースはそのインターフェースすべてのポートにフラッディングしてしまいます。

5.30 MLD Snooping

参照「コマンドリファレンス」/「IPv6 マルチキャスト」/「MLD Snooping」

ポートトランキングと MLD Snooping の併用時、非マスターポートで受信した IPv6 マルチキャストパケットをマスターポートから送信するため、ループが発生します。

（「マスターポート」はトランクグループ内で最初にリンクアップしたポート、「非マスターポート」はそれ以外のポートを示します）

5.31 IPX

参照「コマンドリファレンス」/「IPX」/「IPX インターフェース」

IPX インターフェースの構成ポートがすべてリンクダウンしても、SHOW IPX CIRCUIT コマンドの表示項目 Link State に反映されません（表示上は「up」のまま）。このようなときは、いったんケーブルを抜き差しすると正しく表示されるようになります。

5.32 ファイアウォール

参照「コマンドリファレンス」/「ファイアウォール」

○ PUBLIC 側で受信したパケットを破棄した場合、SHOW FIREWALL POLICY コマンドの COUNTER オプションで表示される Total Packets Received カウンターが 2 ずつカウントされます。

○ ファイアウォールポリシーにアクセスリストを登録する場合、IP アドレスリストよりルール番号の大きい MAC アドレスリストは有効になりません。MAC アドレスリストのルール番号は IP アドレスリストのルール番号よりも小さくなるように設定してください。

○ ADD FIREWALL POLICY コマンドでダイナミック ENAT の PUBLIC インターフェースに IP と LIST を指定したルールを設定した場合、エラーメッセージが表示されます。その場合は、ADD FIREWALL POLICY コマンドで MAC アドレスリストを追加し、SET FIREWALL POLICY コマンドで IP アドレスを設定してください。

○ FTP サーバーの制御用コネクションポートが 21 以外のとき、FTP データの通信に対して NAT が機能しません。

○ PUBLIC 側から PRIVATE 側に対して FTP 通信を行った場合、SHOW FIREWALL SESSION コマンドで不要なセッションが表示されることがあります。これは表示だけの問題であり、動作には影響ありません。

○ PUBLIC 側インターフェースにルール NAT（エンハンスト、リバース、ダブルのいずれか）を設定した場合、PUBLIC 側から PRIVATE 側への FTP 通信が正常に行えないことがあります。

○ ファイアウォールを無効にしても、SHOW FIREWALL POLICY COUNTER コマンドで表示される「Number of active session」の値がクリアされません。これは表示だけの問題であり、動作には影響ありません。

○ SMTP プロキシーにてメールの転送を自ドメインのみに制限した場合でも、Windows プロンプトの Telnet でメールを送信すると自ドメイン以外のメールも転送することがあります。

○ Smurf AMP 攻撃を受信しても、SHOW FIREWALL POLICY コマンドの COUNTER オプションで表示されるカウンターがカウントされません。

○ 攻撃検出機能（SET FIREWALL POLICY ATTACK コマンド）によって攻撃を検出したとき、検出されたパケットが許可されているにも関わらず、SHOW FIREWALL EVENT コマンドの出力では Deny Event（拒否イベント）に表示されます。

○ SHOW FIREWALL EVENT コマンドで表示されるイベント情報は、内部テーブルがいっぱいになると古い情報から削除されます。このとき、攻撃開始のイベント情報が削

除されてしまうと、攻撃の終了を検出しても、攻撃終了のイベントを通知しなくなります。

○ ファイアウォール有効時、TCP コネクションキュー内に確立したセッションが残ってしまいます。

○ ファイアウォール有効時、RTSP パケット（ポート番号：554）を許可するようルールを設定しても、パケットが転送されません。これを回避するには、RTSP のポート番号を変更してください。

○ ファイアウォール NAT を使用している環境で、PRIVATE 側へ traceroute を実行すると、PUBLIC インターフェースからの返答パケットに対しても、NAT により PRIVATE 側の IP アドレスへ変換されてしまいます。

○ ファイアウォール NAT を使用している環境で、PRIVATE 側へ traceroute を実行すると、PRIVATE 側から返信される ICMP Reply（Time-to-live exceeded）の Inner Header の PRIVATE 側アドレスが、PUBLIC 側の IP アドレスに変換されません。

5.33 VRRP

参照「コマンドリファレンス」/「VRRP」

○ SET VRRP コマンドで ADOPTVRIP=ON に設定した場合、本製品から送信される ICMP Reply の始点アドレスが実インターフェースアドレスを使用するため、Windows XP ではタイムアウトが発生し、通信ができません。（Windows 2000 などの OS では問題なく通信できます。）

○ VRRP のインターフェースのリンクアップ / リンクダウンのトラップを送出すると、それ以降トラップが送出されなくなります。これを回避するには、以下のいずれかの処置を行ってください。

- ADD IP ARP コマンドでスタティックエントリーを追加します。
- VRRP を有効にしているインターフェースを常にリンク状態にします。
- トラップホストまたは本製品から PING を定期的に実行します。

5.34 DHCP サーバー

参照「コマンドリファレンス」/「VRRP」

クライアント 1 に IP アドレスを割り当てた際、クライアント 2 から同一の IP アドレスの要求があると、クライアント 1 に対して DHCPNAK を送信してしまいます。

6 取扱説明書・コマンドリファレンスの補足・誤記訂正

同梱の取扱説明書、および「CentreCOM 8724SL/8748SL コマンドリファレンス 2.7 (Rev.D)」の補足事項です。

6.1 HTTP サーバー（サポート対象外）

参照「コマンドリファレンス」/「運用・管理」/「システム」

本製品はデフォルトで HTTP サーバー（サポート対象外）が有効になっているため、IP 有効時は TCP ポート 80 番がオープンしています。セキュリティーを重視する場合は、DISABLE HTTP SERVER コマンドを実行して、HTTP サーバーを無効にしてください。

6.2 DESTINATION=ROUTER のログ出力先定義

参照「コマンドリファレンス」/「運用・管理」/「ログ」

DESTINATION=ROUTER のログ出力先定義を使用するときは、ログの送信側と受信側で同一ファームウェア（ファイル名とバージョンが同じもの）を使用してください。それ以外の構成はサポート対象外とさせていただきますのでご注意ください。

6.3 送信元アドレスがマルチキャストアドレスのフレーム

受信した Ethernet フレームの送信元アドレスがマルチキャストアドレスだった場合、このフレームは転送されずに破棄されます。

6.4 スイッチポートの統計カウンター（8748SL のみ）

8748SL では、ポートグループ「1 ～ 24、50」と「25 ～ 48、49」をまたぐパケットは、SHOW SWITCH PORT COUNTER コマンドで表示される ifOutUcastPkts、ifOutErrors、DropEvents カウンターにカウントされません。

6.5 1000Mbps ポートのフラッディングレート

リンクしている 10/100Mbps ポートの数によって、拡張モジュールの 1000Mbps ポートのブロードキャスト、マルチキャストの転送率が下がる場合があります。

6.6 ポート帯域制限機能の受信レート上限値と TCP 通信のスループット

参照「コマンドリファレンス」/「スイッチング」/「ポート」

スイッチポートに受信レート上限値（INGRESSLIMIT）を設定している場合、同ポートを経由した TCP の通信では、TCP データのスループットが設定した上限値よりも低くなります（低下の度合いは通信状況に依存します）。これは TCP プロトコルの特性として、帯域制限機能によって破棄されたパケットの再送処理などが発生するためです。また、TCP 以外においても、同様の再送処理を行うプロトコルではこの現象が発生する可能性があります。

6.7 フォワーディングデータベース

参照「コマンドリファレンス」/「スイッチング」/「フォワーディングデータベース」

1 回目のエージアウトでは、すべてのダイナミックエントリーがフォワーディングデータベースから削除されない場合があります。ただし、2 回目以降のエージアウトではすべてのダイナミックエントリーが削除されます。

6.8 ハードウェア IP フィルター

参照「コマンドリファレンス」/「スイッチング」/「ハードウェア IP フィルター」

○ IPv6 ルーティングを有効にしている場合、ルーティング対象の IPv6 パケットに対して、Ethertype = 0x86DD（IPv6）の条件を持つハードウェア IP フィルターエントリーがマッチしません。ルーティング対象の IPv6 パケットをフィルタリングするには、IPv6 フィルターを使用してください。ルーティング対象でない（スイッチングされる）IPv6 パケットには、前述のハードウェア IP フィルターがマッチします。

○ IPX ルーティングを有効にしている場合、ルーティング対象の IPX パケットに対しては、SENDMIRROR 以外のアクションが機能しません。また、SENDMIRROR アクションと EPORT パラメーターは併用できません。ルーティング対象の IPX パケットをフィルタリングするには、IPX トラフィックフィルターを使用してください。なお、ルーティング対象でない（スイッチングされる）IPX パケットには、すべてのアクションが機能します（ただし、IP パケットを前提としている MOVETOSTOPRIO、SETTOS、MOVEPRIOTOTOS、SETIPDSCP アクションは使用不可）。

○ フレームタイプ 802.3 raw の IPX パケットにマッチさせるため、DSAP / SSAP = 0xFFFF の条件を持つフィルターエントリーを作成した場合、このエントリーはフレームタイプ Ethernet 2 の IPX パケットにもマッチします。

6.9 ポート認証

参照「コマンドリファレンス」/「スイッチング」/「ポート認証」

ポート認証（802.1X 認証、MAC ベース認証）を有効にしたポートでは、ポートトランキング、スパニングツリープロトコル、ポートセキュリティーを使用できません。また、802.1X 認証の Authenticator ポートと MAC ベース認証ポートをタグ付きに設定することはできません。

6.10 IP マルチキャストのハードウェア処理

参照「コマンドリファレンス」/「IP マルチキャスト」/「概要」

スイッチ間をタグ付きポートで接続している場合、タグ付きポートを通過する IP マルチキャストパケットは、最初に ADD IP INTERFACE コマンドを実行した VLAN の VID を持つものだけがハードウェア処理の対象となり、他の VID を持つパケットはソフトウェア処理となります。ソフトウェア処理される場合のパフォーマンスは「ワイヤースピード÷ VLAN 数」となります。タグ VLAN 環境で IP マルチキャストを使用するときは、タグ付きポートに割り当てる VLAN 数を 3 つまでにすることをおすすめします。

7 未サポートコマンド（機能）

以下のコマンド（機能）はサポート対象外ですので、あらかじめご了承ください。

○ **以下の機能別キーワードを含む全コマンド**
ENABLE の後に [?] キーを押すと表示される機能別キーワードです。

ACC, APPLETALK, BRI, CLASSIFIER, ETH, FRAMERELAY, GARP, GRE, GUI, PIM6, IPSEC, ISAKMP, ISDN, L2TP, LAPB, LAPD, LDAP, LOADBALANCER, LB, LPD, MIOX, PKI, PRI, Q931, RSVP, SA, SERVICE, SSL, STAR, STARTUP, STT, SYN, TPAD, TACACS, VLANRELAY, X25C, X25T, TDM, DS3, VOIP

○ 以下のコマンド（パラメーター）
太字はコマンド名、細字は該当コマンドのパラメーター名です。

COPY

DUMP

START PKT
STOP PKT
SET PKT
SHOW SYSTEM TEMPERATURE

TRACE [ADDRONLY]

PING [APPLEADDR ¦ OSIADDRESS] [SAPPLEADDRESS ¦ SOSIADDRESS]
SET PING [APPLEADDR ¦ OSIADDRESS] [SAPPLEADDRESS ¦ SOSIADDRESS]
PURGE PING TOTALLY

SHOW SWITCH SOCK
SHOW SWITCH MEMORY
SHOW SWITCH SWTABLE
SET SWITCH SOCK
SET SWITCH PORT [MULTICASTMODE] [SPEED={10MHAUTO ¦ 10MFAUTO ¦ 100MHAUTO ¦ 100MFAUTO ¦ 1000MHAUTO ¦ 1000MFAUTO ¦ 1000MHALF}]
ENABLE/DISABLE SWITCH BIST

CREATE/DESTROY IP POOL
SHOW IP POOL
ADD/DELETE IP ROUTE FILTER [PROTOCOL={STATIC ¦ INTERFACE}]
ADD/DELETE/SET IP FILTER PRIORITY
ADD/DELETE IP EGP
ENABLE/DISABLE IP EGP
SHOW IP EGP
ADD/SET IP RIP [NEXTHOP]
ADD/DELETE IP SA
SHOW IP SA
SET IP ARP [DLCI] [CIRCUIT]
SET IP RIP NEWIPADDRESS
SET IP FLOW
SHOW IP FLOW
SHOW IP CACHE
SHOW IP ROUTE [CACHE]

SHOW IP ROUTE TEMPLATE
SHOW IP ROUTE MULTICAST
ENABLE/DISABLE IP FOFILTER
ENABLE/DISABLE IP MULTICASTSWITCHING
ENABLE/DISABLE IP SRCROUTE
ADD/DELETE/SET IP ROUTE BLACKHOLE

ADD/DELETE DVMRP [DLC]
ADD/DELETE DVMRP INTERFACE [DLC]
SET DVMRP [DLC]
SET DVMRP INTERFACE [DLC]

ADD/DELETE IPV6 FILTER [PRIORITY]
ADD/DELETE IPV6 INTERFACE [PRIORITYFILTER]
SET IPV6 FILTER [PRIORITY]
SET IPV6 INTERFACE [PRIORITYFILTER]
ENABLE/DISABLE IPV6 MLD
ENABLE/DISABLE IPV6 FLOW
ADD/SET IPV6 INTERFACE [TYPE=ANYCAST]

CREATE FIREWALL POLICY DYNAMIC
ADD/DELETE FIREWALL POLICY DYNAMIC
ADD/DELETE FIREWALL POLICY PROXY
ADD/DELETE FIREWALL POLICY SPAMSOURCES
ADD/DELETE FIREWALL POLICY HTTPFILTER
SET FIREWALL POLICY SMTPDOMAIN
SET FIREWALL POLICY ATTACK
ENABLE/DISABLE FIREWALL POLICY SMTPRELAY
ENABLE/DISABLE FIREWALL POLICY HTTPCOOKIES

CREATE QOS
ADD/DELETE QOS
SET QOS PORT
SET QOS POLICY
SET QOS TRAFFICCLASS
SET QOS FLOWGROUP
SHOW QOS POLICY
SHOW QOS TRAFFICCLASS
SHOW QOS FLOWGROUP

CREATE/DESTROY PPP [AUTHMODE] [BAPMODE] [CBMODE] [CBDELAY] [COPY] [DEBUGMAXBYTES] [DESCRIPTION] [FRAGMENT] [FRAGOVERHEAD] [LOGIN] [MAXLINKS] [MRU] [NULLFRAGTIMER] [NUMBER] [TYPE]
ADD/DELETE PPP [AUTHENTICATION] [CBDELAY] [CBMODE] [CBNUMBER] [CBOPERATION] [COMPALGORITHM] [COMPRESSION] [CONFIGURE]

[MODEM] [NUMBER] [PREDCHECK] [RESTART] [STACCHECK] [TERMINATE] [TYPE]
ADD/DELETE/SET PPP ACSERVICE
ADD/DELETE/SET PPP TEMPLATE
ENABLE/DISABLE PPP TEMPLATE
ADD/DELETE PPP MAXSESSIONS
ADD/DELETE PPP ACRADIUS
ADD/DELETE PPP VLAN
ENABLE/DISABLE PPP ACCESSCONCENTRATOR
ACTIVATE PPP RXPKT

ADD/DELETE/SET PIM INTERFACE [SRCAPABLE]
SHOW PIM [STATEREFRESH]
ADD/SET PIM BSRCANDIDATE [HASHMASKLENGTH]

SET BOOTP MAXHOPS

ENABLE/DISABLE DHCP [BOOTP]

ENABLE/DISABLE BGP DAMPING
CREATE/SET BGP DAMPING PARAMETERSET
ADD IP ROUTEMAP [MATCH TAG]

8　コマンドリファレンスについて

最新のコマンドリファレンス**「CentreCOM 8724SL/8748SL コマンドリファレンス 2.7 (J613-M0019-01 Rev.D)」**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、上記のコマンドリファレンスに対応した内容になっていますので、お手持ちのコマンドリファレンス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。

※パーツナンバー**「J613-M0019-01 Rev.D」**は、コマンドリファレンスの全ページ（左下）に入っています。

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