Cisco Nexus 5000 シリーズおよび Cisco Nexus 2000 シリーズ リリース ノート、リリース 4.0(1a)N2(1a)

Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Release Notes, Release 4.0(1a)N2(1a)

最新リリース：4.0(1a)N2(1a)
OL-16601-01-J I0

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。米国サイト掲載ドキュメントとの差異が生じる場合があるため、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このドキュメントでは、Cisco Nexus 5000 シリーズ スイッチおよび Cisco Necus 2000 シリーズ Fabric Extender の機能、警告、および制限事項について説明します。このドキュメントは、「関連資料」（P.32）に示されたドキュメントと併せて使用してください。

（注） リリース ノートは、制限や警告に関する新しい情報によって更新される場合があります。Cisco Nexus 5000 シリーズおよび Cisco Nexus 2000 シリーズの最新バージョンのリリース ノートについては、次の Web サイトを参照してください。
http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/release/notes/Nexus_5000_Release_Notes.html

（注） 表 1 に、このドキュメントのオンライン変更履歴を示します。

表 1　オンライン変更履歴

Part Number	リビジョン	日付	説明
OL-16601-01	A0	2008 年 6 月 3 日	リリース ノートを作成。
OL-16601-01	B0	2008 年 6 月 16 日	リリース 4.0(0)N1(1a) の情報を追加。
OL-16601-01	C0	2008 年 6 月 30 日	Cisco Fabric Manager リリース 3.4(1a) の情報を追加。
OL-16601-01	D0	2008 年 7 年 22 日	リリース 4.0(0)N1(1a) の情報を追加。
OL-16601-01	E0	2008 年 8 月 13 日	リリース 4.0(0)N1(2) の情報を追加。
OL-16601-01	F0	2008 年 9 月 29 日	リリース 4.0(0)N1(2a) の情報を追加。
OL-16601-01	G0	2008 年 12 月 3 日	リリース 4.0(1a)N1(1) の情報を追加。
OL-16601-01	H0	2009 年 2 月 26 日	リリース 4.0(1a)N2(1) の情報を追加。
OL-16601-01	I0	2009 年 4 月 30 日	リリース 4.0(1a)N2(1a) の情報を追加。

内容

このドキュメントの構成は、次のとおりです。

はじめに

ここでは、次の内容について説明します。

Cisco Nexus 5000 シリーズ スイッチ

Cisco Nexus 5000 シリーズ スイッチは、ラインレート、低遅延、ロスレス 10 ギガビット イーサネット、Cisco Data Center Ethernet、および Fibre Channel over Ethernet（FCoE）に対応したデータセンター アプリケーション向けのスイッチのファミリで構成されています。Cisco Nexus 5000 シリーズには、Cisco Nexus 5020 スイッチと Cisco Nexus 5010 スイッチが含まれます。

Cisco Nexus 5000 シリーズ スイッチのハードウェアについては、次のトピックで説明します。

- 「Cisco Nexus 5010 スイッチ」（P.3）

Cisco Nexus 5020 スイッチ

Cisco Nexus 5020 スイッチは、56 ポートのスイッチです。10 ギガビット イーサネット、Cisco Data Center Ethernet、FCoE、およびファイバ チャネルに対応した 2 ラック ユニット（2 RU）スイッチで、1.04 テラビット/秒（Tbps）のスループットを非常に低遅延で実現します。

このスイッチは、次のような特徴を備えています。

- 10 ギガビット イーサネット、Cisco Data Center Ethernet、および FCoE Small Form Factor Pluggable Plus（SFP+; 拡張着脱可能小型フォーム ファクタ）の固定ポート 40 個。40 個の固定ポートのうち 16 個は、ギガビット イーサネットと 10 ギガビット イーサネットの両方をサポートします。デフォルトは 10 ギガビット イーサネットです。
- 拡張モジュール スロット 2 個。これらは 10 ギガビット イーサネット、Cisco Data Center Ethernet、および FCoE SFP+ のポートを最大 12 個追加、ファイバ チャネル スイッチのポートを最大 16 個追加、またはその両方の組み合わせをサポートするように設定可能です。
- シリアル コンソール ポートおよびアウトオブバンド 10/100/1000 Mbps イーサネット管理ポート。
- 1+1 のホットプラグ可能な冗長電源。
- 4+1 のホットプラグ可能な冗長ファン モジュール。これらによって前面から背面へと確実に冷却されます。

Cisco Nexus 5020 スイッチの詳細については、『*Cisco Nexus 5000 シリーズ ハードウェア インストレーション ガイド*』を参照してください。

Cisco Nexus 5010 スイッチ

Cisco Nexus 5010 スイッチは、28 ポートのスイッチです。10 ギガビット イーサネット、Cisco Data Center Ethernet、FCoE、およびファイバ チャネルに対応した 1 RU スイッチで、500 Gbps を超えるスループットを非常に低遅延で実現します。このスイッチは、次のような特徴を備えています。

- 10 ギガビット イーサネット、Cisco Data Center Ethernet、および FCoE SFP+ の 固定ポート 20 個。20 個の固定ポートのうち 8 個は、ギガビット イーサネットと 10 ギガビット イーサネットの両方をサポートします。
- 拡張モジュール スロット 1 個。これは 10 ギガビット イーサネット、Cisco Data Center Ethernet、および FCoE SFP+ のポートを最大 6 個追加、ファイバ チャネル スイッチのポートを最大 8 個追加、または 10 ギガビット イーサネット、Cisco Data Center Ethernet、および FCoE SFP+ の 4 個の追加ポートと、ファイバ チャネル スイッチの 4 個の追加ポートの組み合わせをサポートするように設定可能です。
- シリアル コンソール ポートおよびアウトオブバンド 10/100/1000 Mbps イーサネット管理ポート。
- 1+1 のホットプラグ可能な冗長電源。
- 1+1 のホットプラグ可能な冗長ファン モジュール。これらによって前面から背面へと確実に冷却されます。

Cisco Nexus 5010 スイッチの詳細については、『*Cisco Nexus 5000 シリーズ ハードウェア インストレーション ガイド*』を参照してください。

（注） Cisco Nexus 5020 スイッチと N5K-M1404 および N5K-M1600 Gatos Expansion Module（GEM）では、リリース 4.0(0)N1(1) 以降のイメージが使用されます。Cisco 5010 スイッチと N5K-M1008 GEM では、リリース 4.0（1a）N1（1）以降のイメージが使用されます。

Cisco Nexus 2000 シリーズ Fabric Extender

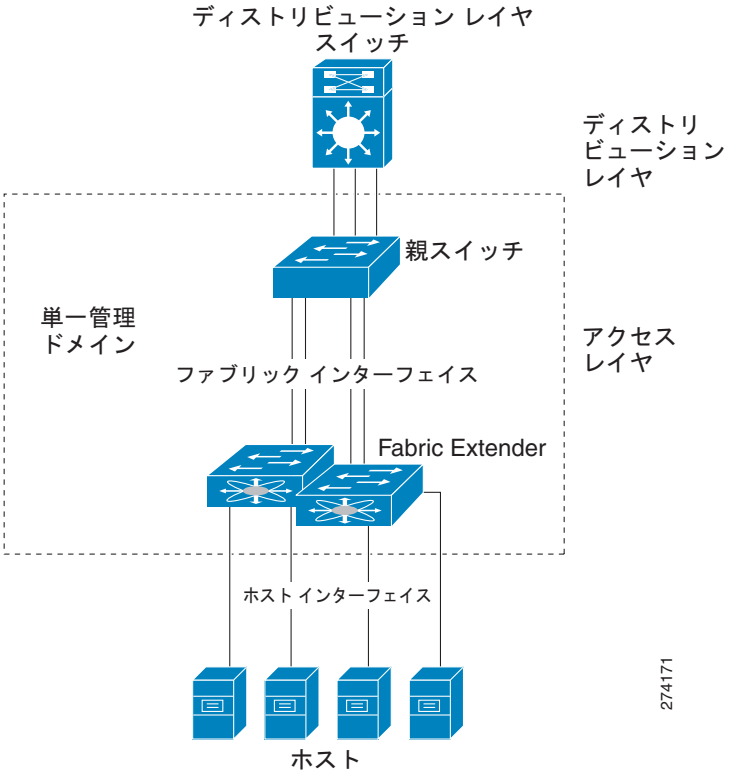
Cisco Nexus 2000 シリーズ Fabric Extender は、Cisco Nexus 5000 シリーズ スイッチと連動して高密度かつ低コストのサーバ集約を実現する、拡張性と柔軟性が高いサーバ ネットワーキング ソリューションです。

ファブリック エクステンダ は、多数の 1 ギガビット イーサネット、10 ギガビット イーサネット、統合ファブリック、ラック、およびブレード サーバ環境の間で規模を調整することで、データセンターのアーキテクチャと運用を簡略化するように設計されています。

ファブリック エクステンダ は、その親スイッチと統合されるため、ゼロタッチのプロビジョニングと自動設定が可能になります。この統合により、セキュリティや Quality Of Service（QoS）などの親 Nexus 5000 シリーズ スイッチと同じ機能を使用して、図 1 に示すように単一の管理ポイントから多数のサーバおよびホストをサポートできるようになります。Fabric Extender とその親スイッチを使用すると、マルチパス、ループフリーの大規模なアクティブ-アクティブ トポロジをイネーブルにできるため、ファブリック エクステンダ とその親スイッチの間に Spanning Tree Protocol（STP; スパニング ツリー プロトコル）は必要はありません。

Fabric Extender は、直接サーバに接続するように設計されているため、デフォルトですべての Fabric Extender ホスト ポートがエッジ ポートになります。また、Fabric Extender ホスト ポートでは、デフォルトで BPDU ガードと BPDU フィルタもイネーブルになります。

図 1　　単一の管理ドメイン



ここでは、2148T Fabric Extender について説明します。内容は次のとおりです。

- 「Cisco Nexus 2148T Fabric Extender」（P.5）

Cisco Nexus 2148T Fabric Extender

Cisco Nexus 2000 シリーズの最初の製品は、ラックマウント用に設計された 1 RU シャーシの Nexus 2148T Fabric Extender です。このシャーシは、冗長性のあるホットスワップ可能なファンと電源をサポートします。

Cisco Nexus 2148T Fabric Extender は、すべてのトラフィックを 10 ギガビット イーサネット ファブリック アップリンク経由で Cisco Nexus 5000 シリーズの親スイッチに転送し、Cisco Nexus 5000 シリーズ スイッチで確立されたポリシーによってすべてのトラフィックを検査できるようにします。Nexus 2148T にソフトウェアは含まれていません。ソフトウェアは、Cisco Nexus 5000 シリーズの親スイッチからダウンロードされて、アップグレードされます。

Nexus 2148T には、サーバまたはホストへのダウンリンク接続用に 48 個の 1 ギガビット イーサネット ホスト インターフェイスが搭載されています。また、親スイッチへのアップリンク接続用に SFP+ インターフェイス アダプタが付いた 4 個の 10 ギガビット イーサネット ファブリック インターフェイスが搭載されています。

Cisco NX-OS リリース 4.0(1a)N2(1) の新機能と変更された機能

このリリースには、次の新機能や変更された機能が含まれています。

- Cisco Nexus 2000 シリーズ Fabric Extender（Part Number N2K-C2148T-1GE）のサポート
- ポート ベースの CoS 割り当て
- STP ブリッジ保証

これらの機能の詳細については、「関連資料」（P.32）に示された Cisco Nexus 5000 シリーズと Cisco Nexus 2000 シリーズのドキュメンテーションを参照してください。

Cisco NX-OS リリース 4.0(0)N ベースのリリースのアップグレード/ダウングレード問題

ここでは、Cisco Nexus 5000 シリーズ スイッチで Cisco NXOS 4.0(0)N ベースのリリースからアップグレードしたり、これらのリリースにダウングレードしたりすると発生する可能性がある問題について説明します。また、これらの変更点の一部について、設定構文の違いの例を示します。

ここでは、次の内容について説明します。

EtherChannel のアップグレード/ダウングレードの変更点

次の表に、EtherChannel メンバーのセキュリティ Access Control List（ACL; アクセス コントロール リスト）の変更点を示します。

リリース	説明
4.0(0)N ベースのリリース	メンバー ポートで設定可能です（ただし、ポートが EtherChannel のメンバーである場合は使用されません）。
4.0(1a)N ベースのリリースとそれ以降のリリース	メンバー ポートで設定できません。すべてのメンバー ポートが EtherChannel の設定に従います。
アップグレード	メンバー ポートの ACL 設定（存在する場合）は失われて、EtherChannel の設定が保持されます。ポートが EtherChannel のメンバーである場合、動作に影響はありません。 メンバー ポートが EtherChannel とは別個の場合、物理インターフェイスで ACL 設定を再作成する必要があります。
ダウングレード	問題はありません。

次の表に、インターフェイス レベルの QoS サービス ポリシーの変更点を示します。

リリース	説明
4.0(0)N ベースのリリース	インターフェイス レベルの QoS サービス ポリシーは、EtherChannel に対応していません。QoS は、メンバー単位のポート設定に厳密に従います。インターフェイス レベルでサポートされるサービス ポリシーは、出力キュー スケジューリング ポリシーだけです。
4.0(1a)N ベースのリリースとそれ以降のリリース	メンバー ポートで設定できません。すべてのメンバー ポートが EtherChannel の設定に従います。
アップグレード	変更された出力スケジューリング ポリシーを持つメンバー ポートが存在し、EtherChannel が明示的に設定されている場合は、ポートの出力スケジューリング設定が失われます。EtherChannel には、デフォルトの出力スケジューリング ポリシーが存在します。
ダウングレード	この機能は、ダウングレード後に再設定する必要があります。再設定しないと、EtherChannel の出力キュー スケジューリング設定はダウングレード後に失われます。

次の表に、優先度フロー制御設定の変更点を示します。

リリース	説明
4.0(0)N ベースのリリース	優先度フロー制御は、インターフェイス レベルの設定です。この CLI オプションは、DCBX ネゴシエーションの結果を上書きするために使用されます。優先度フロー制御機能は、EtherChannel を認識しません。メンバー単位のポート設定に厳密に従います。
4.0(1a)N ベースのリリースとそれ以降のリリース	メンバー ポートで設定できません。すべてのメンバー ポートが EtherChannel の設定に従います。

アップグレード	変更された優先度フロー制御設定を持つメンバー ポートが存在し、EtherChannel が明示的に設定されている場合は、ポート設定が失われます。EtherChannel には、優先度フロー制御のデフォルト設定が存在します。
ダウングレード	この機能は、ダウングレード後に再設定する必要があります。再設定しないと、EtherChannel の優先度フロー制御設定は失われます。

次の表に、イーサネット負荷分散コマンド構文の変更点を示します。

リリース	説明

4.0(0)N ベースのリリース	チャネルグループ バンドルで負荷分散方式を設定するには、次のコマンドを使用します。
	`switch(config)# port-channel load-balance ethernet source-destination-?`
	`  source-destination-ip    Source & Destination IP address`
	`  source-destination-mac   Source & Destination MAC address`
	`  source-destination-port  Source & Destination TCP/UDP port`
	注 このリリースでは、キーワード **source-destination** が使用されます。

4.0(1a)N ベースのリリースとそれ以降のリリース	チャネルグループ バンドルで負荷分散方式を設定するには、次のコマンドを使用します。
	`switch(config)# port-channel load-balance ethernet source-dest-?`
	`  source-dest-ip    Source & Destination IP address`
	`  source-dest-mac   Source & Destination MAC address`
	`  source-dest-port  Source & Destination TCP/UDP port`
	注 このリリースでは、キーワード **source-dest** が使用されます。

アップグレード	負荷分散設定が失われます。
ダウングレード	この機能は、ダウングレード後に再設定する必要があります。再設定しないと、EtherChannel の負荷分散設定は失われます。

イーサネット インターフェイスが EtherChannel に参加すると、次のインターフェイス レベルのパラメータがディセーブルになります。

```
  bandwidth              Set bandwidth informational parameter
  delay                  Specify interface throughput delay
  duplex                 Enter the port duplex mode
  flowcontrol            Configure interface flowcontrol
  ip                     Configure IP features
  ipv6                   Configure IPv6 features
  mac                    MAC configuration commands
  priority-flow-control  Configure interface priority-flowcontrol
  service-policy         Configure QoS service policy
  spanning-tree          Spanning Tree Subsystem
  speed                  Enter the port speed
  storm-control          Configure Interface storm control
```

ファイバ チャネル ポートのシャットダウン

次の表に、インターフェイスの **shutdown** コマンド構文の変更点を示します。

リリース	説明
4.0(0)N ベースのリリース	**system default switchport shutdown** コマンドで、すべてのファイバ チャネル ポート（物理または仮想）がデフォルトでシャットダウンされます。
4.0(1a)N ベースのリリースとそれ以降のリリース	**system default switchport shutdown** コマンドで、すべてのイーサネット ポートの管理状態がダウンに設定されるようになりました。ファイバ チャネル ポートをシャットダウン状態に設定するには、**system default switchport shutdown san** コマンドを使用します。
アップグレード	ファイバ チャネル ポートではなく、イーサネット ポートがデフォルトでシャットダウン状態になります。
ダウングレード	この機能は、ダウングレード後に再設定する必要があります。再設定しないと、スイッチは **system default switchport shutdown san** コマンドに無効のフラグを付けます。

スイッチド ポート アナライザ

次の表に、Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）セッションの変更点を示します。

リリース	説明
4.0(0)N ベースのリリース	デフォルトでは、オープン状態でセッションが保持されます。セッションを閉じるには、次のコマンドを使用します。 `switch(config)# monitor session session-number suspend`
4.0(1a)N ベースのリリースとそれ以降のリリース	デフォルトでは、シャット状態でセッションが保持されます。セッションを開くには、次のコマンドを使用します。 `switch(config)# no monitor session session-number shut` **注** コマンドの構文も変更され、**suspend** キーワードが **shut** に変更されています。
アップグレード	SPAN セッションはアップグレード後、シャット状態になります。
ダウングレード	SPAN セッションで特定の **shut** または **no-shut** コマンドを実行しない場合、SPAN セッションはダウングレード後、非一時停止状態になります。

FCoE モデルと関連する設定の変更点

以前の Cisco NX-OS 4.0(0)N ベースのリリースでは、FCoE モデルのインターフェイス上でイーサネットと FCoE が同時に存在することが可能であり、仮想インターフェイス、仮想イーサネット、Virtual Fibre Channel（VFC; 仮想ファイバ チャネル）は、互いに影響を与えませんでした。たとえば、仮想イーサネット インターフェイスがエラー ディセーブルであっても、VFC インターフェイスは動作できました。

Cisco NX-OS 4.0(1a)N ベースのリリースとそれ以降のリリースでは、将来 T11 FCoE Initialization Protocol（FIP）との上位互換性が実現されるように CLI 実装が変更されました。この新しい FCoE モデルでは、次の点が変更されています。

- FCoE トラフィックはイーサネットを通過し、イーサネット STP がポート ステータスを制御する。

- VSAN の FCoE トラフィックは、FCoE がイネーブルな単一専用の VLAN 経由で転送される。

  CLI 実装では VLAN および VSAN 間のマッピングが必要ですが、FCoE フレームでタグ付けを解除するか、プライオリティ タグを付ける必要があります。FCoE VLAN は、FCoE フレームで転送する必要はありません。これは、FIP ベースの FCoE がサポートされたると、将来のリリースで変更されます。

仮想インターフェイスの変更点については、次のトピックで説明します。

- 「仮想インターフェイス グループ」（P.9）
- 「仮想イーサネット インターフェイス」（P.9）
- 「仮想ファイバ チャネル インターフェイス」（P.9）
- 「VSAN および VLAN 間のマッピング」（P.10）

仮想インターフェイス グループ

以前の Cisco NX-OS 4.0(0)N ベースのリリースでは、次の例に示すように仮想インターフェイス グループを使用して、仮想インターフェイスを物理イーサネット インターフェイスにバインドできました。

```
switch# configure terminal
switch(config)# interface vig 1
switch(config-if)# bind interface ethernet 1/1
```

仮想インターフェイス グループは、Cisco NX-OS 4.0(1a)N ベースのリリースとそれ以降のリリースで廃止されました。

仮想イーサネット インターフェイス

Cisco NX-OS 4.0(1a)N ベースのリリースとそれ以降のリリースでは、仮想イーサネット インターフェイスがサポートされません。仮想イーサネット インターフェイスで以前に設定されたすべてのイーサネット機能は、バインドされたイーサネット インターフェイスで設定する必要があります。

仮想イーサネット インターフェイスと同じ動作を保つには、イーサネット インターフェイスで次の設定ステートメントを明示的に設定する必要があります。

```
spanning-tree bpduguard enable
spanning-tree port type edge trunk
```

仮想イーサネット インターフェイスで以前に設定された他のすべての機能（ACL、SPAN など）は、バインドされたイーサネット インターフェイスに適用する必要があります。

仮想ファイバ チャネル インターフェイス

以前の Cisco NX-OS 4.0(0)N ベースのリリースでは、仮想ファイバ チャネル インターフェイスが仮想インターフェイス グループに追加され、そのグループによって物理イーサネット インターフェイスにバインドされていました。

Cisco NX-OS 4.0(1a)N ベースのリリースとそれ以降のリリースでは、各仮想ファイバ チャネル インターフェイスは、FCoE がイネーブルな物理イーサネット インターフェイスに直接バインドされます。この変更によって、次の例に示すように **interface vfc** コマンドが簡略化されます。

```
switch# configure terminal
switch(config)# interface vfc 1
switch(config-if)# bind interface ethernet 1/1
```

仮想ファイバ チャネル インターフェイスをバインドするイーサネット インターフェイスは、次のように設定する必要があります。

- トランク ポートにする（**switchport mode trunk** コマンドを使用）。
- 仮想ファイバ チャネルの VSAN に対応する FCoE VLAN が、許可される VLAN に含まれる。FCoE VLAN は、トランク ポートのネイティブ VLAN として設定する必要があります。
- イーサネット インターフェイスを、PortFast として設定する（**spanning-tree port type edge trunk** コマンドを使用）。

VSAN および VLAN 間のマッピング

以前の Cisco NX-OS 4.0(0)N ベースのリリースでは、FCoE にスイッチで定義された VLAN との依存関係がありませんでした。

Cisco NX-OS 4.0(1a)N ベースのリリースとそれ以降のリリースでは、各仮想ファイバ チャネル インターフェイスは単一の VSAN とだけ関連付けられます。仮想ファイバ チャネル インターフェイスが関連付けられた VSAN は、次の例に示すように FCOE がイネーブルな専用 VLAN にマッピングする必要があります。

```
switch# configure terminal
switch(config)# vlan 200
switch(config-vlan)# fcoe vsan 2
switch(config-vlan)# exit
switch(config)# interface ethernet 1/1
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk native vlan 1
switch(config-if)# switchport trunk allowed vlan 1,200
switch(config-if)# exit
switch(config)# interface vfc 1
switch(config-if)# bind interface ethernet 1/1
switch(config-if)# exit
switch(config)# vsan database
switch(config-vsan)# vsan 2 interface vfc 1
```

（注） FCoE VLAN は、FCoE トラフィック専用に予約されています。FCoE 以外のイーサネット フォワーディングには使用できません。

仮想インターフェイス設定の変更点の例

ここでは、次の内容について説明します。

- 「Cisco NX-OS 4.0(0)N ベースのリリースの設定」（P.11）
- 「Cisco NX-OS 4.0(1a)N ベースのリリースとそれ以降のリリースで変換された設定」（P.11）

Cisco NX-OS 4.0(0)N ベースのリリースの設定

```
interface vig 1
bind interface Ethernet 1/1

interface vethernet 1/1
switchport access vlan 2

interface vfc 1/1
no shutdown

vsan database
vsan 1 interface vfc 1/1
```

Cisco NX-OS 4.0(1a)N ベースのリリースとそれ以降のリリースで変換された設定

```
vlan 101
fcoe vsan 1

interface Ethernet 1/1
switchport mode trunk
switchport trunk native vlan 2
switchport trunk allowed vlan 2,101
spanning-tree bpduguard enable
spanning-tree port type edge trunk

interface vfc 1
no shutdown

vsan database
vsan 1 interface vfc 1
```

Cisco NX-OS 4.0(0)N ベースのリリースからのアップグレード

Cisco Nexus 5000 シリーズ スイッチを Cisco NX-OS 4.0(0)N ベースのリリースからアップグレードする場合、適用される CLI に以前のリリースとの互換性がないため、仮想ファイバ チャネルと仮想イーサネット インターフェイスのすべての設定が失われます。このため、アップグレードを実行する前に、startup-config ファイルをバックアップすることを推奨します。スイッチに FCoE 設定がある場合は、新しい FCoE CLI を使用して FCoE を再設定する必要があります。または、シスコのカスタマー サポートに問い合わせて、アップグレードして設定を新しい形式に変換できます。

Cisco NX-OS リリース 4.0(0)N ベースのリリースへのダウングレード

Cisco NX-OS リリース 4.0(0)N ベースのリリースにダウングレードすると、FCoE 設定が失われます。このため、Cisco NX-OS 4.0(0)N ベースのリリースの元の設定をバックアップしておくことを推奨します。バックアップした startup-config は、ダウングレード後、元の設定を復元するために使用できます。

FCoE 設定のダウングレード手順

Cisco NX-OS 4.0(0)N ベースのリリースへのダウングレード後に FCoE 設定を復元するには、次の手順に従います。

ステップ 1 **install all** コマンドを使用して、スイッチを Cisco NX-OS 4.0(0)N ベースのイメージにダウングレードします。

ステップ 2 ダウングレードが完了したら、**write erase** コマンド、**reload** コマンドの順に使用してスイッチの設定をクリアします。

ステップ 3 **feature fcoe** コマンドと **copy running startup** コマンドを実行して、スイッチを再設定します。NPV モードで動作しているスイッチの場合は、**npv enable** コマンドを使用します。**reload** コマンドを使用して、スイッチをリロードします。

ステップ 4 **copy** *4.0(0)N based image-config* **running-config** コマンドを使用して、アップグレード前の設定を復元します。

制限事項

ここでは、Nexus 5000 シリーズ スイッチおよび Cisco Nexus 2000 シリーズ Fabric Extender リリース 4.0(1a)N2(1a) における制限事項について説明します。

- BPDU フィルタは、イネーブルな場合、イーサネット ポートでの BPDU の転送と受信を停止します。Nexus 2000 Fabric Extender のホスト側のポートでは、BPDU フィルタが常にイネーブルになります。BPDU フィルタをディセーブルにする設定は、サポートされません。
- 大規模な設定では、一部の Cisco Nexus 2000 シリーズ Fabric Extender で、**reload** コマンドの発行後オンラインになるまでに最大 3 分かかることがあります。最大許容数の Cisco Nexus 2000 シリーズ Fabric Extender が Cisco Nexus 5000 シリーズ スイッチに接続されており、すべてのホスト側ポートが接続されて、ホスト側の各インターフェイスに大きい設定がある（インターフェイスごとに最大許容数の ACE をサポートする）場合は、大規模な設定と呼ばれます。
- Cisco Nexus 2000 Fabric Extender では、VLAN トランク経由の PVLAN を使用した異なるスイッチへの接続はサポートされません。PVLAN トランクはスイッチ間のリンクだけに使用されますが、FEX ポートはサーバへの接続だけに使用されます。VLAN トランクとして設定された Fabric Extender ポートの一部として、分離されたセカンダリ VLAN を作成する設定は有効ではないため、分離されたセカンダリ VLAN 上のすべてのフレームは FEX への送信から除外されます。
- 出力スケジューリングは、ドロップ / 非ドロップ クラス間でサポートされません。各 Fabric Extender のホスト ポートでは、ドロップ トラフィックと非ドロップ トラフィックは同時にサポートされません。各 Fabric Extender のホスト ポートでは、ドロップ トラフィックと非ドロップ トラフィックのいずれかをサポートできます。
- イーサネット SPAN の宛先に向かうトラフィックには、常にタグが付けられます。SPAN の宛先は、アクセス モードとトランク モードのいずれかにできます。また、SPAN ソース ポートのフレームには、タグを付けたりタグ付けを解除したりできます。フレームがシステムを通過すとき、常に内部タグが付けられます。SPAN ソースで表示されていた、フレームにもともとタグが付けられていたか、タグ付けが解除されていたかという情報は、SPAN の宛先では保持されません。SPAN の宛先ポートから送信されるスパンされたトラフィックには、常に VLAN タグが付けられます。SPAN の宛先から送信されるとき、適切な VLAN タグがフレームに適用されます。唯一の例外は、フレームが無効な VLAN 上で SPAN ソース ポートから入力される場合です。この場合、スパンされるフレームには **vlan 0** が適用されます。
- 4.0(0)N ベースのリリースから 4.0(1a)N ベースのリリースとそれ以降のリリースにアップグレードしたり、4.0(0)N ベースのリリースにダウングレードしたりすると、RADIUS および AAA のスタートアップ コンフィギュレーションが失われます。アップグレードまたはダウングレード前にスタートアップ コンフィギュレーションをブートフラッシュ メモリに保存し、アップグレードまたはダウングレード後にそれをブートフラッシュ メモリから復元してください。

- スパンされる FCoE フレームでは、元の SMAC フィールドと DMAC フィールドが保持されません。フレームが宛先にスパンされると、イーサネット ヘッダーが変更されます。変更されたヘッダー フィールドは、SPAN の宛先で監視されるときに表示されます。
- イーサネット SPAN の宛先ポート上でスパンされる FCoE フレームの CoS 値は、SPAN FCoE ソース フレームの CoS 値とは一致しません。キャプチャされた SPAN FCoE フレームの CoS 値は無視してください。
- 不良な CRC や無効な SOF と EOF を持つイーサネットおよびファイバ チャネル フレームは、ドロップされません。Cisco Nexus 5000 シリーズ スイッチは、カットスルー スイッチング モードで動作するため、フレームは完全に受信される前にシステムを通過します。イーサネットおよびファイバ チャネル CRC はフレームで上書きされて、EOF コードは EOFa に設定されます。ダウンストリーム スイッチまたは宛先端末で、不良フレームがドロップされます。
- ファイバ チャネルがスイッチでイネーブルになっていなくても、class-fcoe は削除できません。
- 単一の VLAN 上で複数タイプの VACL はサポートされません。NX-OS ソフトウェアでは、VLAN に適用された単一タイプの VACL（MAC、IPv4、または IPv6 のいずれか）だけサポートされます。VACL が VLAN に適用されると、新しい VACL のタイプが異なる場合は既存の VACL が置き換えられます。たとえば、VLAN で MAC VACL が設定されている場合は、同じ VLAN で IPv6 VACL が設定され、IPv6 VACL が適用されて MAC VACL が削除されます。
- MAC ACL は非 IP パケットにだけ適用されます。MAC ACL に **match eth type = ipv4** ステートメントがある場合でも、IP パケットには一致しません。この状況に対処するには、Ethertype が Ipv4 または Ipv6 に一致する MAC ACL を使用する代わりに、IP ACL を使用して IP トラフィックにアクセス コントロールを適用します。
- ポートから 100 Kbps 未満の速度でトラフィックが送信される場合は、バッファの消耗を避けるため 10 秒間エラー ディセーブルになります。一方、送信速度が 100 Kbps を超える場合は、10 秒間以内のエラー ディセーブルにならないことがあります。これによって入力バッファが消耗され、フレームが破棄される可能性があります。このため、**shut** コマンドを使用して、低速送信ポートをディセーブルにしてください。
- Cisco Nexus 5000 シリーズ ハードウェアのマルチキャスト ストーム制御機能では、IP、非 IP、登録、未登録の各マルチキャスト トラフィックが区別されません。すべてのマルチキャスト トラフィックは、設定時に単一のマルチキャスト ストーム制御ポリサーの対象となります。
- 設定には複数の **boot kickstart** ステートメントを使用できません。
- ファイバ チャネル ポートを備えた拡張モジュールを削除し、ケーブルがそのまま接続されている場合は、次の FCP_ERRFCP_PORT エラーが表示されます。

```
2008 May 14 15:55:43 switch %KERN-3-SYSTEM_MSG: FCP_ERRFCP_PORT:
gat_fcp_isr_ip_fcmac_sync_intr@424, jiffies = 0x7add9a:Unknown intr src_id 42 - kernel
2008 May 14 15:55:43 switch %KERN-3-SYSTEM_MSG: FCP_ERRFCP_PORT:
gat_fcp_isr_ip_fcmac_sync_intr@424, jiffies = 0x7add9a:Unknown intr src_id 41 - kernel
```

これらは情報目的のメッセージにすぎないため、機能性が失われることはありません。

Fabric Extender ポートにおける SPAN 制限

- Fabric Extender（FEX）のポートは、1 セッションだけの tx ソースとして設定できます。

  同じ FEX 上の 2 つのポートが tx ソースとしてイネーブルになっている場合は、それらのポートを同じセッションに含める必要があります。FEX ポートを tx ソースとして設定したが、同じ FEX に属する別のポートが異なる SPAN セッションの tx ソースとしてすでに設定されている場合は、CLI にエラーが表示されます。

  次の例では、FEX 100 上のインターフェイス Ethernet100/1/1 は、すでに SPAN セッション 1 で tx ソースとして設定されています。

```
swor28(config-monitor)# show running-config monitor
      version 4.0(1a)N2(1)
      monitor session 1
          source interface Ethernet100/1/1 tx
          destination interface Ethernet1/37
          no shut
```

インターフェイス Ethernet100/1/2 を tx ソースとして別の SPAN セッション（セッション 2）に追加した場合は、次のエラーが表示されます。

```
swor28(config)# monitor session 2
swor28(config-monitor)# source interface ethernet 100/1/2 tx
ERROR: Eth100/1/2: Ports on a fex can be tx source in one session only
swor28(config-monitor)#
```

- FEX ポートが tx 送信元として設定されると、tx 送信元ポートがメンバーとなっているすべての VLAN のマルチキャスト トラフィックが SPAN で処理されます。FEX ポートは、IGMP スヌーピングによってフィルタ処理されないマルチキャスト パケットだけを送信します。たとえば、FEX ポート 100/1/1 ～ 12 が VLAN 11 で設定されており、スイッチ ポート 1/5 がマルチキャスト グループ内の VLAN 11 でマルチキャスト トラフィックを送信し、FEX ポート 100/1/3 ～ 12 に接続されたホストがマルチキャスト トラフィックの受信を待機している場合（IGMP 経由）、そのマルチキャスト トラフィックは FEX ポート 100/1/3 ～ 12 から送信されますが、100/1/1 ～ 2 からは送信されません。

  SPAN Tx をポート 100/1/1 で設定した場合、マルチキャスト トラフィックはポート 100/1/1 から送信されませんが、SPAN の宛先はそのマルチキャスト トラフィックを受信します。これは、仕様上の制限が原因です。

- FEX ポートが SPAN rx ソースと tx ソースの両方として設定されている場合、そのポートから送信されるブロードキャスト フレーム、非 IGMP レイヤ 2 マルチキャスト フレーム、および不明なユニキャスト フレームが、SPAN の宛先で 2 回（1 回は入力パスで、もう 1 回は出力パスで）検出されることがあります。出力パスでは、受信されたポートと同じポートから送信されることがないように、フレームが FEX によってフィルタ処理されます。たとえば、FEX ポート 100/1/1 が VLAN 11 で設定されていて、SPAN rx ソースおよび tx ソースとしても設定されており、ブロードキャスト フレームがそのポートで受信される場合は、フレームがポート 100/1/1 から再送信されない場合でも、SPAN の宛先でフレーム 2 つのコピーが認識されます。
- FEX ポートは、SPAN の宛先として設定できません。スイッチ ポートだけを SPAN の宛先として設定および使用できます。

警告

ここでは、次の内容について説明します。

未解決の警告

ここでは、このリリースの未解決の警告について説明します。

- CSCsx67695

  症状：GEM ポートにシステム ポリシーと一致するインターフェイス ポリシー設定がある場合、GEM がスイッチから削除されると、システム ポリシーが新しいポリシーに変更されます。GEM がスイッチに挿入されると、GEM ポートのインターフェイス ポリシーと新しいシステム ポリシーの間に不一致が発生する可能性があります（新しいシステム ポリシーに、古いシステム ポリシーにあったシステム クラスが存在しない場合があります）。この不一致のエラーは報告されません。

  回避策：GEM ポートのインターフェイス ポリシーを削除してインターフェイス ポリシーを修正し、GEM ポートに再適用します。

- CSCsx68778

  症状：インターフェイスの範囲下でコマンドを設定できません。

  回避策：一度に 1 つの FEX の HIF ポート下でコマンドを設定します。

- CSCsx60187

  症状：複数の Switched Virtual Interface（SVI; スイッチ仮想インターフェイス）に重複する IP アドレスが設定されます。

  回避策：複数の SVI に同じ IP アドレスを設定しないでください。

- CSCsx35870

  症状：PVLAN の作成および削除の前に、多数の VLAN が作成および削除されると、CLI がタイムアウトします。イーサネット ポート マネージャ（ethpm）と SPAN マネージャまたは PVLAN マネージャとの通信がタイムアウトしたことを示す、syslog がシステムによって記録されます。この結果、一部の PVLAN インターフェイスがエラー ディセーブルになります。FEX ポートは PVLAN のメンバーとして設定され、それらの一部は通常の VLAN のメンバーになります。

  回避策：エラー ディセーブルになったインターフェイスで、**shut** および **no shut** を実行します。

- CSCsx39481

  タイトル：**vlan intf delete** の後、その ipv6 アドレスを別のインターフェイスに追加できません。

  症状：ipv6 アドレスを含むアップ VLAN インターフェイスの削除後に、同じ ipv6 アドレスを別の VLAN インターフェイスに追加できません。この問題は ipv6 アドレスだけで発生します。IPV4 アドレスでこの問題は発生しません。

  回避策：削除した VLAN インターフェイスを戻して IPv6 アドレスを削除してから、VLAN インターフェイスをもう一度削除します。その後、同じ IPv6 アドレスを別の VLAN インターフェイスに追加します。

- CSCsx54086

  症状：ソース VLAN がモニタ セッション用に設定されており、4.0(1a)N2(1) からダウングレードされた場合、ソース VLAN の設定が失われます。この影響として、ダウングレード後にソース VLAN トラフィックが正常にスパンされないことがあります。

  回避策：ダウングレード後、モニタ セッションのソース VLAN 設定を再設定します。

- CSCsx54270

  症状：4.0(1a)N2(1) にアップグレードするとき、**system qos service-policy** 設定ですべての CoS 値が非ドロップ クラスにマッピングされると、サービス ポリシーの適用に失敗します。この影響として、アップグレード後にトラフィックが正常に動作しなくなることがあります。

回避策：アップグレード後、ポリシー マップを再設定して非ドロップ クラスに少なくとも 1 つの CoS を含め、ポリシー マップを **system qos service-policy** 設定に再び適用します。

- CSCsx40562

  症状：**system qos service-policy** 設定で 4 つのユーザ QoS クラスがすべて設定されていない場合、802.1p CoS 値が 3 より大きい ACL ドロップ トラフィックが、スパンされないことがあります。

  回避策：4 つのユーザ QoS クラス（**class-default** と **class-fcoe** を除く）をすべて **system qos service-policy** の下で設定し、すべての ACL ドロップ トラフィックをスパンします。

- CSCsw21301

  症状：Cisco NX-OS ではオフライン設定がサポートされません。FEX インターフェイスの作成は、ファブリック インターフェイスの設定後、FEX がオンラインになれば実行できます。ファイルから設定を復元すると、FEX インターフェイスはまだ作成されていない期間に、インターフェイス設定が適用されて失敗します。

  回避策：システム設定を設定ファイル（ローカルにコピーするか、tftp 経由で取得されたファイル）から復元する必要がある場合は、設定の FEX インターフェイスの部分（存在する場合）を別のファイルに分離できます。まず、メイン ファイルをコピーしてから FEX がオンラインになるのを待ち、個別の FEX インターフェイス設定ファイルをコピーします。あるいは、2 回コピーすることも可能です。

- CSCsv52871

  症状：複数の FEX ホスト ポートの FEX アップリンクが、非ドロップ クラスのトラフィックで輻輳すると、FEX ホストで実行される一時停止が均等でなくなります。この結果、一部の FEX ホスト ポートから送信されるトラフィックのスループットが、他のポートよりも良くなります。

  回避策：ありません。

- CSCsx24526

  症状：FEX ホスト ポートが輻輳すると、8 ポートのうち同じブロック内の輻輳していないポートで、一部のトラフィックが失われます。損失量は、輻輳しているポートの原因となっているソースの数によって異なります。

  回避策：ありません。

- CSCsv93263

  症状：Cisco NX-OS ではオフライン設定がサポートされません。FEX インターフェイスの作成は、ファブリック インターフェイスの設定後、FEX がオンラインになれば実行できます。ファイルから設定を復元すると、FEX インターフェイスはまだ作成されていない期間に、インターフェイス設定が適用されて失敗します。

  回避策：システム設定を設定ファイル（ローカルにコピーするか、tftp 経由で取得されたファイル）から復元する必要がある場合は、設定の FEX インターフェイスの部分（存在する場合）を別のファイルに分離できます。まず、メイン ファイルをコピーしてから FEX がオンラインになるのを待ち、個別の FEX インターフェイス設定ファイルをコピーします。あるいは、2 回コピーすることも可能です。

- CSCsv81694

  症状：同じ MAC アドレスが動的に学習されているポートがフラップしている場合、自動学習静的 MAC エントリが削除されます。静的 MAC アドレスは、ハードウェアだけでなくソフトウェアからも削除されます。

  回避策：CLI を使用して静的 MAC エントリを再び追加します。

- CSCsu01188

  症状：ギガビット イーサネットまたは 10 ギガビット イーサネットの SFP が削除または挿入されると、トラップが送信されません。

回避策：ありません。

- CSCsv56881

  症状：インバンド管理用の各 SVI に、異なる IP アドレスを設定する必要があります。IPv6 にはエラー チェック機能があり、管理者が 2 つの SVI 間で重複する IPv6 アドレスを入力すると、重複するアドレスが原因でソフトウェアのコマンドが失敗します。同様のエラー チェックは、SVI の IPv4 アドレス設定にも存在します。

  回避策：重複する IPv4 アドレスまたは IPv6 アドレスを設定しないでください。

- CSCsv24214

  症状：Cisco Nexus 5000 シリーズ スイッチで実行されるイメージを、4.0(1a)N1 イメージから 4.0(0)N1(1) イメージまたは 4.0(0)N1(1a) イメージにダウングレードすると、起動設定が復元されません。これは、問題 CSCsq74395 が原因であり、4.0(0)N1(2) および 4.0(0)N1(2a) で解決されました。

  回避策：ダウングレード後、起動設定を実行設定に手動でコピーして、システムをリブートします。

- CSCsv02866

  症状：**show interface ethernet transceiver details** コマンドにより、DOM がサポートされる 1 G SFP の無効なキャリブレーションが表示されることがあります。

  回避策：ありません。

- CSCsv10783

  症状：**show startup-config** コマンドにより、チャネル グループの適切なモードが表示されません。チャネル グループの現在のモードが表示されます。適切なモードは保存されており、その後リロードすると、チャネル グループで適切なモードが設定されます。**show startup-config** では、起動用に保存されたモードではなく、常に現在のモードが表示されます。その後リロードすると、適切なモードが設定されます。これは show コマンドだけの問題です。

  回避策：ありません。

- CSCsv00989

  症状：**show interface ethernet transceiver details** コマンドにより、DOM に対応した 1 G SFP にすべてゼロの値が表示されることがあります。

  回避策：ありません。

- CSCsu48008

  症状：仮想ファイバ チャネル（VFC）インターフェイスがダウンしたとき、**fcIfOperStatusCause** MIB オブジェクトによって正しい理由が報告されません。

  回避策：**show interface vfc x** コマンドを使用して、CLI から OperStatus を取得します。

- CSCsu77946

  症状：コンフィギュレーション セッション内で、PACL で統計をイネーブルにして 252 を超える ACES を ACL に追加し、インターフェイスに適用すると、統計カウンタが消費されたときにエラー メッセージが生成されます。統計キーワードは削除しようとしても、削除されません。この結果、ACL をインターフェイスに適用できなくなります。この問題は、コンフィギュレーション セッションで設定に失敗した場合だけ発生します。

  回避策：ACL のサイズを小さくして（252 未満の ACES）、ACL をインターフェイスに再び適用します。統計キーワードは残ってハードウェア リソースを消費します。

- CSCsu93313

  症状：コンフィギュレーション セッション内で、合計 1023 の TCAM エントリを持つ 125 の一意の VACL が作成されます。verify コマンドは失敗し、次のメッセージが表示されます。

```
d2-switch-2(config)# configure session 30
Config Session started, Session ID is 1
d2-switch-2(config-s)# verify
Failed to start Verification: Message Timed Out
d2-switch-2(config-s)# commit
Failed to complete Verification: no free label
```

  この問題は大規模な VACL 設定で発生します。Cisco Nexus 5000 シリーズ スイッチが一度この状態になると、その後の VACL 設定は失敗します。

  回避策：リロードして設定を回復します。

- CSCsv19979

  症状：SD モードに設定された FC ポートが、速度を手動で設定するまでアップになりません。ポートはエラー ディセーブルの状態になり、SD としてオンラインにするには、速度を手動で 2 G または 4 G に設定するしかありません。

  回避策：速度を手動で 2 G または 4 G に設定します。

- CSCsv00402

  症状：Cisco NX-OS 4.0(1a)N1 リリースから以前のソフトウェア リリースにダウングレードすると、EtherChannel 経由で設定された静的 IGMP エントリがダウングレード後に失われます。

  回避策：以前のリリースにダウングレードし、スイッチをリロードしてから、EtherChannel 経由で設定した静的 IGMP グループを再設定します。または、**copy startup running** を実行して起動設定をリロードすることも可能です。その後 **copy running startup** を実行し、静的 IGMP エントリが起動設定に正しく追加されるようにします。

- CSCsr20499

  症状：設定ファイルから設定を実行設定に復元すると、ACL マネージャでメモリ リークが発生することがあります。リークのサイズは、ACL 設定のサイズと復元が行われた回数に関連しています。ACL 設定が非常に大きく、復元が何回も行われた場合は、スイッチがリブートすることがあります。

  回避策：ありません。

- CSCsq64251

  症状：ログイン時にユーザ名を入力して誘導要求の認証が開始された場合、Terminal Access Controller Access Control Plus（TACACS+）に失敗します。スイッチへの誘導要求を認証する構文は、**username@**(*TACACS+ サーバの IP アドレスまたは名前*) です。

  回避策：誘導要求の認証に RADIUS を使用します。

- CSCsq76688

  症状：Cisco Discovery Protocol（CDP; シスコ検出プロトコル）保持期間のポートをシャットダウンしても、CDP の隣接デバイスが削除されません。

  回避策：ありません。

- CSCsl62545

  症状：ファンが正しく動作していても、Device Manager 上のファン LED がオレンジ色になります。

  回避策：ありません。

- CSCsr28868

  症状：FCoE 機能がディセーブルな場合、Ethertype/length フィールドに 00 00 のタグが付けられていないイーサネット パケットが無効なパケットとして処理され、不良なイーサネット CRC が設定されて転送されます。

  回避策：ありません。

- CSCsr35452

  症状：MDS ファブリックで **ntp peer** コマンドが設定されており、CFS を使用して配布される場合、Nexus 5000 シリーズ スイッチは **VRF 管理**の代わりに間違った VRF 名 **AC** をコマンドに付加します。

  回避策：**ntp server** コマンドを使用して、ファブリック間で時間を同期します。

- CSCsr36661

  症状：IGMP グループ メンバーシップがプライベート VLAN（PVLAN）ホスト ポートを使用して静的に構成されると、ハードウェアが正しくプログラミングされます。ただし、スイッチのリロード後に、PVLAN ホスト ポートのメンバーシップ情報がプログラミングされません。

  回避策：プライベート VLAN の関連付けを削除して、もう一度追加します。

- CSCsr64291

  症状：複数の入力トラフィックが原因でポートが輻輳すると、厳密な優先度スケジューリングが設定されていても、ユーザ定義の QoS クラスにマッピングされたトラフィックが、非常に低速（1 秒あたりのフレーム数が少ない）で破棄されることがあります。

  回避策：ありません。

- CSCsr68690

  症状：ジャンボ フレームまたは大きいフレームを伝送するポートで出力 SPAN が設定されると、スパンされるフレームが 2384 バイトに丸められます。

  回避策：ありません。

- CSCsl21529

  症状：**show interface** コマンドの出力に間違った MTU 値が表示されます。Cisco Nexus 5000 シリーズ スイッチでは、クラス ベースの MTU だけがサポートされます。インターフェイス単位レベルの MTU 設定はサポートされません。スイッチでは、ジャンボ フレームがデフォルトでサポートされます。ただし、**show interface** コマンドの出力には、現在のところ間違った MTU 値である 1500 バイトが表示されます。

  回避策：ありません。

- CSCsm03765

  症状：CISCO-IP-IF-MIB での Set 操作はサポートされません。SNMP を使用して mgmt0 の IP アドレスは設定できません。

  回避策：CLI を使用して mgmt0 の IP アドレスを設定します。

- CSCsm16222

  症状：CFS では、ロール設定の配布がサポートされません。**show cfs application** コマンドを入力すると、登録されたアプリケーションが表示されます。

  回避策：CFS に登録されていない機能は、スイッチでローカル設定する必要があります。

- CSCsl73766

  症状：CFS では、RADIUS 設定の配布がサポートされません。**show cfs application** コマンドを入力すると、登録されたアプリケーションが表示されます。

回避策：CFS に登録されていない機能は、スイッチでローカル設定する必要があります。

- CSCso25966

  症状：Catalyst 6500 スイッチと Cisco Nexus 5000 シリーズ スイッチの間で LACP ポート チャネルが設定され、ポート チャネルの両側の設定が一致しない場合、Catalyst 6500 LACP ポートがエラー ディセーブル状態に変わることがあります。

  回避策：設定を修正してポート チャネルの両方のピア スイッチで一致するようにし、Catalyst 6500 ポート チャネル インターフェイスで **shut** および **no shut** 操作を実行します。

- CSCso27446

  症状：Cisco Nexus 5000 シリーズ スイッチの mgmt0 インターフェイスに **shutdown** コマンドを発行してもリンクはダウンせず、リンクがダウンしたことがリモート エンドに示されません。

  回避策：ありません。

- CSCso46345

  症状：Cisco Nexus 5000 シリーズ スイッチで実行されている NX-OS ソフトウェアの現在のバージョンでは、Brocade i10K の interop モード 4 がサポートされません。i10k v9.2.0.8 は、interop モード 1 および 4 で、SAN-OS 3.2(2c) および 3.2(3) の MDS によってサポートされます。

  回避策：ありません。

- CSCso74872

  症状：2 つの SNMP ウォークが同時に開始すると、それらのいずれかが失敗して次のエラーが表示されます。

  ```
  OID not increasing
  ```

  この問題は 1 つの SNMP ウォークでは発生しません。

  回避策：永続的なエラーではありません。ウォークを再開すると、他の SNMP ウォークが進行中でなければ問題は発生しません。

- CSCso84269

  症状：起動後にリロードが実行されて設定の変更がない場合、スイッチに次の警告が表示されることがあります。

  ```
  'WARNING: There is unsaved configuration!!!'
  ```

  回避策：**copy running startup** コマンドを入力します。問題は解消します。

- CSCsq10026

  症状：着脱可能小型フォーム ファクタ（SFP）がイーサネット ポートにない場合、**show interface** コマンドの出力に帯域幅が 1 Gbps と表示されます。SFP が取り付けられると、帯域幅が正しく表示されます（10 Gbps）。

  回避策：ありません。

- CSCsq17571

  症状：SNMP ユーザが Virtual Interface Group（VIG; 仮想インターフェイス グループ）、Virtual Ethernet（VEth; 仮想イーサネット）または VFC インターフェイスを作成または削除すると、**show accounting log** コマンドによって表示されるアカウンティング ログが更新されません。

  回避策：設定に CLI を使用すると、アカウンティング ログが更新されます。

- CSCsq35527

  症状：スイッチで IGMP スヌーピングがイネーブルになっていて、スイッチが STP ルートであり、STP トポロジの変更が生じると、IP マルチキャスト トラフィックの収束に時間がかかることがあります。この間、IP マルチキャスト トラフィックに影響が及ぶ可能性があります。

回避策：IGMP ルータで短いクエリ間隔を設定し、このトポロジでの IP マルチキャスト トラフィックの収束にかかる時間を短くします。

- CSCsq35728

  症状：SAN ポート チャネルが作成されると、次の syslog メッセージが表示されます。

  ```
  2008 May 20 06:09:13 switch %PORT_CHANNEL-3-MSG_SEND_FAILURE: failed to send
  MAP_PARAM_FROM_CHANNEL to sap 45: Broken pipe"
  ```

  機能性は失われないため、このメッセージは無視できます。

  回避策：ありません。

- CSCso01268

  症状：モジュールがホットスワップされると、次のエラー メッセージが表示されます。

  ```
  2005 Jan  1 00:08:23 switch %KERN-4-SYSTEM_MSG: SI-VDC map entry <0, 0x0> does not
  exist! - kernel"
  ```

  機能性は失われないため、このメッセージは無視できます。

  回避策：ありません。

- CSCsq57558

  症状：Enhanced Inter Switch Link（EISL; 拡張スイッチ間リンク）のカプセル化は、ファイバ チャネルの SPAN の宛先ポートでサポートされません。EISL のカプセル化が SPAN の宛先（SD）ポートで設定されると、SD ポートから送信されるパケットに VFT ヘッダーが追加されます。VFT ヘッダーには、さまざまな VSAN のトラフィックを区別する際に役立つ VSAN 情報が含まれています。これは、ファイバ チャネルのどの SPAN ソースにも当てはまります。デフォルトでは、EISL のカプセル化が追加されず、パケットは VFT ヘッダーなしで送信されます。SPAN ソース ポートのタイプと関係はありません。Cisco Nexus 5000 シリーズ スイッチの場合は、**switchport encap** EISL コマンドの効果がありません。

  回避策：SPAN ファイバ チャネル トラフィックに対して、イーサネットの SPAN の宛先ポートを使用します。イーサネットの SPAN の宛先ポートから送信される FCoE パケットでは、イーサネット VLAN タグ内に VSAN 情報が含められます。

- CSCsq90423

  症状：EISL のカプセル化は、NPV モードのファイバ チャネルの SPAN の宛先ポートでサポートされません。EISL のカプセル化が SPAN の宛先（SD）ポートで設定されると、SD ポートから送信されるパケットに VFT ヘッダーが追加されます。VFT ヘッダーには、さまざまな VSAN のトラフィックを区別する際に役立つ VSAN 情報が含まれています。これは、ファイバ チャネルのどの SPAN ソースにも当てはまります。デフォルトでは、EISL のカプセル化が追加されず、パケットは VFT ヘッダーなしで送信されます。SPAN ソース ポートのタイプと関係はありません。Cisco Nexus 5000 シリーズ スイッチの場合は、**switchport encap** EISL コマンドの効果がありません。

  回避策：SPAN ファイバ チャネル トラフィックに対して、イーサネットの SPAN の宛先ポートを使用します。イーサネットの SPAN の宛先ポートから送信される FCoE パケットでは、イーサネット VLAN タグ内に VSAN 情報が含められます。

- CSCsw79515

  症状：Cisco Nexus 2000 シリーズ Fabric Extender の電源が次々に何度も再投入された場合、Cisco Nexus 5000 シリーズ スイッチと Cisco Nexus 2000 シリーズ Fabric Extender の間の一部のリンクが、エラー ディセーブル状態になることがあります。

  回避策：数秒後にファブリック ポートが回復します。ユーザの操作は必要ありません。

- CSCsv93278

  症状：**logging server vrf** コマンドが、管理 VRF 以外で機能しません。管理 VRF 経由で syslog を送信する必要がある場合、機能性に影響はありません。

  回避策：ありません。

- CSCsv93922

  症状：モジュロ（%）演算子を Cisco Nexus 2000 シリーズ Fabric Extender の記述で使用した場合、**show fex <fex-id>** コマンドによって次のエラー メッセージが表示されます。

  ```
  ERROR: bad format: non escaped % not followed by 's'.
  ```

  回避策：Cisco Nexus 2000 シリーズ Fabric Extender の記述から、モジュロ（%）演算子を削除します。

- CSCsv95478

  症状：Cisco Nexus 2000 シリーズ Fabric Extender の pinning redistribute コマンドが、yes または no 操作によるユーザ プロンプトを待機しません。

  回避策：ありません。

- CSCsw66216

  症状：メンバーの FEX ファブリック ポートがチャネルグループに追加または削除されると、Cisco Nexus 5000 シリーズ スイッチと Cisco Nexus 2000 シリーズ Fabric Extender がポート チャネル転送設定の更新を完了するまで、フレームが数秒間失われることがあります。これは、設定を変更するために新しいポート チャネル メンバーのポートに再配布される、既存のトラフィックに影響を与えます。

  回避策：ありません。

- CSCsw64952

  症状：Cisco Nexus 5000 シリーズ スイッチに 3000 を超える STP インスタンスがあり、ブリッジ保証設定で 1 秒の STP hello タイムが使用されている場合、STP が収束しないことがあります。

  回避策：ブリッジ保証モードで、2 秒の STP hello タイムを使用します。

- CSCsv15775

  症状：Cisco Nexus 2000 シリーズ Fabric Extender のポートで、プライオリティ タグが付いたフレームが受信されると、それらのフレームがドロップされて、ポートのネイティブまたはデフォルトの VLAN で転送されなくなります。MAC アドレスは学習されません。

  回避策：ありません。

- CSCsv65911

  症状：show running-config を発行しても、RMON アラーム設定が表示されません。これは表示の問題にすぎません。copy running-config startup-config によって設定は正しく保存され、リロード後に正しく復元されます。

  回避策：ありません。

- CSCsw14619

  症状：changing FEX pinning max-links によって、ユーザに yes または no が要求されません。

  回避策：ありません。

- CSCsw27089

  症状：ポート チャネル インターフェイスで **switchport mode fex-fabric** または **fex associate** 設定を削除すると、FEX がオフラインになり、警告メッセージが表示されません。

  回避策：ありません。

- CSCsw44921

  症状：FEX ファブリック ポートを **switchport mode fex-fabric** から **switchport mode trunk** に変更しても、警告メッセージが表示されません。

  回避策：ありません。

- CSCsu93674

  症状：**fex associate** 設定を削除しても、FEX がオフラインになる可能性があることを示す警告が表示されません。

  回避策：ありません。

解決済みの警告 — Cisco NX-OS リリース 4.0(1a)N2(1a)

ここでは、このリリースの解決済みの警告について説明します。

- CSCsz00155

  症状：リンク ピアによって大量にフロー制御されていると、Nexus 5000 または Nexus 2000 イーサネット ポートからのトラフィックの送信が遅くなります。この状況が一定期間続く場合、輻輳がシステム内の他のポートに広がって、他のポートでテール ドロップが発生する可能性があります。

  回避策：送信が遅いポートをシャットダウンします。

- CSCsv13371

  症状：インターフェイス リセット カウンタが更新されません。

  回避策：ありません。

- CSCsx39376

  症状：AES プライバシ パスワードを使用して作成されたユーザが、そのプライバシ パスワードを使用せずにログインした場合、ユーザはどの通常ユーザも削除できません。システムがタイムアウトするだけです。

  回避策：ありません。

- CSCsw39639

  症状：特定のインターフェイス名（Ethernet 1/1 など）を参照するルールをロール定義 CLI に入力すると、コマンドがハングすることがあります。Ctrl+C キーを押すと、CLI プロンプトに戻れます。

  回避策：ロール定義 CLI では、特定のインターフェイスを参照するルールを設定しないでください。

- CSCsw83134

  症状：セッションが長時間開いている場合、telnet プロセスが大量の CPU を消費することがあります。

  回避策：ありません。

- CSCsx33608

  症状：**allowed vlan list** 設定のないアクセス ポートまたはトランク ポートが多数システムに存在し、ユーザが次々と **shut** および **no-shut vlan** を実行した場合、メッセージをキューに入れるスペースがないことを示す syslogs が表示されることがあります。

  ```
  %$ VDC-1 %$ %KERN-2-SYSTEM_MSG: mts_is_q_space_available(): NO SPACE.  This condition
  is temporary and will recover as buffers are drained.
  ```

回避策：VLAN のシャットダウンとシャットダウン解除の間に、数秒の間隔を開けます。

- CSCsx83103

  症状：フォワーディング プロセスが頻繁にビジー状態になり、システム状態のチェックにハートビートを使用して応答できないため、システムがリセットされます。次の場合は、STP モードが PVRST から MST（またはその逆）に変わります。

  - STP インスタンスの数が多い（3000 を超える）。
  - 複数のインターフェイス上にある多数の VLAN 間で、MAC アドレスが学習されている。

  回避策：これらの状況で STP モードが変わる前に、次のコマンドを使用してダイナミック MAC アドレス テーブルをクリアします。

  ```
  clear mac-address-table dynamic
  ```

  この問題は必ず発生するわけではなく、これらの状況において問題が発生する場合があります。

- CSCsy01547

  症状：FEX に設定されたシリアル番号が FEX の実際のシリアル番号と一致しない場合、FEX がオフラインになります。シリアル番号の設定が削除されて、ファブリック ポートを **shut** または **no-shut** する必要がある場合、FEX がオンラインに戻らない可能性があります。

  回避策：ファブリック ポートで **shut** または **no-shut** を実行すると、FEX がオンラインに戻ります。

- CSCsy24194

  症状：SNMPv3 トラップを設定すると、**debug snmp all** を設定したときにクラッシュが発生することがあります。

  回避策：SNMPv2 トラップだけを使用してください。

解決済みの警告 — Cisco NX-OS リリース 4.0(1a)N2(1)

ここでは、このリリースの解決済みの警告について説明します。

- CSCsv70815

  症状：デフォルトの VRF が、VRF 設定のシステム デフォルトになっています。管理者によって VRF 設定が指定されない場合は、VRF を使用するアプリケーション（TACACS+ など）がデフォルト VRF 値を引き次ぐのが理想的です。ただし、デフォルトの VRF が設定されていないと、TACACS+ は適切に設定されません。

  回避策：

  Cisco Nexus 5000 シリーズ スイッチでは、考えられる 2 つの VRF（デフォルト VRF と管理 VRF）がサポートされます。TACACS+ サービスを使用するときは必要な VRF を設定してください。必要な VRF は、次のいずれかの設定を使用して設定できます。

  ```
  aaa group server tacacs+ t1
      server 10.193.149.54
      use-vrf management

  aaa group server tacacs+ t2
  server 20.1.1.2
  use-vrf default
  ```

- CSCsv55655

  症状：Cisco Nexus 5000 のイーサネット ポートは、**speed 1000** コマンドを使用して 1 G モードで動作するように設定されると、フロー制御設定をアドバタイズおよび自動ネゴシエートしません。この結果、リンク ピアは Cisco Nexus 5000 シリーズ スイッチの機能について学習せず、そのエンドでフロー制御をイネーブルにしません。

  回避策：リンク ピアでオートネゴシエーションをディセーブルにし、フロー制御をイネーブルにしてフロー制御がリンク上で機能するようにします。

- CSCsv52513

  症状：VLAN インターフェイス 1 は SVI デーモンによりデフォルトで内部に作成されるため、この VLAN インターフェイスは CLI から削除できません。

  回避策：ありません。

- CSCsu50589

  症状：RADIUS 設定内（RADIUS サーバなど）で無効な IP アドレスが設定された場合、RADIUS 設定を操作すると、**show running-configuration** または **copy running to startup** などのコンソールでタイムアウトが発生します。

  回避策：RADIUS 設定に有効な IP アドレスを設定します。

- CSCsu66201

  症状：ネーム サーバの IP アドレスに到達できない場合、TACACS デーモンによるサーバ名の解決が停止します。停止中は、**show running-config** や **copy running-config startup-config** などの一般的なコマンドを含む TACACS コマンドが処理されません。

  回避策：ネーム サーバの IP アドレスへのネットワーク接続を修正します。

- CSCso65934

  症状：設定モードでインターフェイス名を指定すると、仮想インターフェイスが作成されます。インターフェイスが存在しない場合は、システムによってインターフェイスが作成されて、インターフェイス設定モードに入ります。ユーザ ロールによってそのインターフェイスへの接続が禁止されている場合、インターフェイスは作成されますが、この CLI が拒否され、ユーザがインターフェイス設定モードに入りません。同様に、ユーザが仮想インターフェイスにアクセスできない場合は、**no interface** コマンドを使用してインターフェイスを削除できます。

  回避策：ありません。

- CSCso82992

  症状：ロールのロール スコープの削除および挿入に失敗することがあり、次のエラーが表示されます。

  ```
  entry already exists
  ```

  この問題は、次の手順を実行すると発生します。

  - ロールのすべてのロール スコープを削除する。
  - 同じロールの新しいロール スコープを挿入する。

  回避策：これらの手順をもう一度繰り返します。

解決済みの警告 — Cisco NX-OS リリース 4.0(1a)N1(1)

ここでは、このリリースの解決済みの警告について説明します。

- CSCso91286

  症状：TACACS+ 認証を使用して、Access Control System（ACS; アクセス コントロール システム）を使用する AAA ユーザを認証すると、Cisco Nexus 5000 シリーズ スイッチによって ACS で指定されたユーザとロールのバインディング情報が無視されます。ユーザはデフォルト ロールでログインします。新しいユーザのデフォルト ロールは network-operator です。管理者ユーザの場合は、network-admin になります。

  回避策：ロールのバインディングを適用するには、ユーザとロールのバインディングを Cisco Nexus 5000 シリーズ スイッチでローカル設定する必要があります。

- CSCsu32247

  症状：Cisco Nexus 5000 シリーズ スイッチは、起動時に Power On Self Test（POST; 電源投入時自己診断テスト）を実行して、ASIC のハードウェア整合性を検証します。ファイバ チャネル ポートが HBA に接続されると、HBA ドライバが LOS をアサートし、ASIC のいずれかに関して POST により誤った障害が報告される可能性があります。この結果、GEM 上の ASIC により提供されるすべてのポートが hwFailure とマーク付けされます。

  回避策：次の手順を実行して、起動時に POST をバイパスします。

```
switch(config)# diagnostic bootup level bypass
switch(config)# copy running-config startup-config
switch(config)# reload
```

- CSCsv05115

  症状：Cisco Nexus 5000 シリーズ スイッチで CFS コールホームがイネーブルな場合、接続された MDS で CFS コールホームのコミットが実行されると、スイッチがクラッシュします。

  回避策：ありません。

- CSCsv30392

  症状：Cisco Nexus 5020 スイッチがバージョン 4.0(0)N1(2) の場合、Pktmgr のメモリ リークが発生します。この結果、レイヤ 2 のループがしらばく生じてから、STP の機能が停止します。冗長接続を切断すると、No buffer space available メッセージが原因でスイッチを管理できなくなります。

  条件：Cisco Nexus 5020 スイッチが、2 つの 6500 スイッチが存在する三角形トポロジで設定されていて、Cisco Nexus 5020 スイッチにコード バージョン 4.0(0)N1(2) がロードされています。ループを停止するには、冗長リンクをシャットダウンする必要があります。

  回避策：切断状態を修正するには、SVI を設定しないでください。

- CSCso99821

  症状：PVLAN が、一時停止せずに連続して作成および削除された場合、イーサネット インターフェイスを設定できず、リブートが必要になることがあります。

  回避策：PVLAN の作成と削除の間で一時停止し、複数の PVLAN 操作を同時に実行しないでください。または、PVLAN インターフェイスが作成される前に PVLAN を作成し、PVLAN が削除される前にスイッチ ポート PVLAN をインターフェイスから削除することも可能です。

- CSCsr52118

  症状：VLAN で削除、追加、シャットダウン、またはシャットダウン解除操作を実行すると、ポート チャネル インターフェイスがフォワーディング プレーンで VLAN メンバーシップを失うことがあります。この結果、ポートはその VLAN であらゆるフォワーディング操作に加わらなくなります。この動作は、スイッチ ポートのアクセス VLAN 設定が削除および再追加された VLAN と一致する、アクセス ポート チャネルに当てはまります。削除または再追加された VLAN がポート チャネルのネイティブ VLAN と一致する場合は、この動作がトランク ポート チャネルに発生することがあります。

  回避策：ポート チャネルで **shutdown** コマンドまたは **no shutdown** コマンドを入力します。

- CSCsr39670

  症状：スイッチでは SNMP 通知がイネーブルですが、電源モジュールおよびファン モジュールのトラップが受信されません。

  回避策：ありません。

- CSCsr47531

  症状：VSAN が SPAN ソースとして設定されると、全メンバー ポートからのトラフィックは SPAN の宛先ポートにスパンされます。スイッチがリブートされると、VSAN SPAN ソースがダウン状態のままになります。

  回避策：SPAN セッションの VSAN ソースを削除して追加します。

解決済みの警告 — Cisco NX-OS リリース 4.0(0)N1(2a)

- CSCsu08988

  症状：**no telnet server enable** コマンドを実行して Nexus 5020 スイッチをリロードしないと、Telnet アクセスを使用できません。

  回避策：コマンドが startup-config に保存されている場合でも、リロード後に **no telnet server enable** コマンドをもう一度実行します。さらに、SVI にフィルタを適用して、信頼できるホストだけがシステムと通信できるようにすることも可能です。

- CSCsu32247

  症状：Nexus 5000 シリーズ スイッチは、起動時に電源投入時自己診断テスト（POST）を実行して、ASIC のハードウェア整合性を検証します。ファイバ チャネル ポートが Host Bus Adapter（HBA; ホスト バス アダプタ）に接続されると、HBA ドライバが信号損失を引き起こし、ASIC のいずれかに関して POST により誤った障害が報告される可能性があります。この結果、GEM 上の ASIC によって提供されるすべてのポートが、ハードウェア障害とマーク付けされます。

  回避策：：HBA を FC 拡張モジュールに接続しないでください。

- CSCsu40126

  症状：Cisco Nexus 5000 シリーズ スイッチが、N-Port Virtualization（NPV; N ポート仮想化）モードで動作するように設定されると、サーバ ポート経由で受信された LOGO が正しく処理されません。この結果、スイッチのファイバ チャネル ID が古くなります。

  回避策：すべてのサーバ ポートで **shut** および **no shut** コマンド操作を実行し、NPV スイッチでその古い状態をクリアします。

- CSCsm66194 および CSCsr66209

  症状：次のような状況下で Cisco Nexus 5000 シリーズ スイッチが NPV モードで動作している場合、使用可能なすべての境界ポート間でログインのバランスが均等にならないことがあります。

  - スイッチがリロードされる。
  - NPIV がディセーブルになっており、NPV コアスイッチで再度イネーブルにされる。
  - NPV コアスイッチがリロードされる。
  - 新しい NP リンクが追加される。

  回避策：ログインのバランスを取り直すすべてのサーバ ポートで、**shut** および **no shut** コマンド操作を実行します。

- CSCsu25775

  症状：Cisco Nexus 5020 シリーズ スイッチを 110 V 電源に接続すると、次の問題が発生します。

- 起動時、syslog に警告が表示される。ハードウェアでは 110 V 入力がサポートされますが、オペレーティング システムが警告メッセージを間違ってログに記録する。
- show environment power コマンドで、使用可能な電源が間違って負の値で表示される。

回避策：重大な問題ではなく、システムは 110 V 電源入力で通常どおり動作します。syslog メッセージが表示されないようにする回避策はありません。

解決済みの警告 — Cisco NX-OS リリース 4.0(0)N1(2)）

ここでは、このリリースの解決済みの警告について説明します。

- CSCsq61505

  症状：Cisco NX-OS リリース 4.0(0)N1(1) または 4.0(0)N1(1a) から Cisco NX-OS リリース 4.0(0)N1(2) へのアップグレード時に、問題が検出されます。

  回避策：ありません。

- CSCsq67305

  症状：スイッチが N ポート仮想化（NPV）モードで動作しているとき、NP モードのアップリンク インターフェイスのいずれかで **shutdown** または **no shutdown** コマンドを入力すると、アクティブなファイバ チャネル リンクでトラフィックが中断されます。中断は、ポートのインターフェイス モードを F から NP に変更するか、NP から F に変更しても発生します。NP モード ポートと同じ VSAN 内のすべての F モード ポートで、トラフィックが中断されます。

  回避策：メンテナンス ウィンドウでは、NP モードのファイバ チャネル インターフェイスの、インターフェイス状態またはインターフェイス モードだけを変更します。

- CSCso56749

  症状：現在のソフトウェアでは、スーパーバイザは送信元のフレームをデータの制御に基づいて個別にタグ付けできません。フレームは常に CoS 0 で送信されます。

  回避策：ありません。

- CSCso91286

  TACACS+ 認証を使用して、アクセス コントロール システム（ACS）を使用する AAA ユーザを認証すると、ACS で指定されたバインディング情報が無視されます。

  症状：TACACS+ 認証を使用して、ACS を使用する AAA ユーザを認証すると、Cisco Nexus 5000 シリーズ スイッチによって ACS で指定されたユーザとロールのバインディング情報が無視されます。ユーザは network-operator（新規ユーザの場合）および network-admin のデフォルト ロールでログインしています。

  回避策：ロールのバインディングを適用するには、ユーザとロールのバインディングを Cisco Nexus 5000 シリーズ スイッチでローカル設定します。

- CSCsq23027

  症状：電源投入時自己診断テスト（POST）ルーチンで、物理ループバック障害がたびたび報告されます。これは、前面ポートの POST ルーチンでときどき発生する問題です。システムの起動時に、ポートがループバック テストに失敗することがあります。

  回避策：スイッチをリロードし、ハードウェアの不具合であることを確認します。

- CSCsq27576

  症状：FC-SP 認証は E/TE ポートを介したスイッチでしかサポートされません。ネイティブ ファイバ チャネル（FC）および FCoE の発信側および送信先での認証は、サポートされません。

回避策：ありません。

- CSCsq32710

  症状：ユーザ定義のロールが設定された SNMP ユーザが、ファイバ チャネル インターフェイスを取得できません。

  回避策：network-admin や network-operator など、定義済みロールのいずれかをスイッチで使用します。

- CSCsq37899

  症状：出力ポリシー マップから class-fcoe または class-default を削除すると、どちらかのクラスに **priority** キーワードが設定されている場合、**show policy-map** コマンドと **show running-config terminal** コマンドに矛盾が生じます。

  回避策：**class-fcoe** および **class-default** のデフォルトの帯域幅の割合は 50% です。出力ポリシーからこれらのクラスを削除する前に、ポリシー マップ内の他のクラスが 50% を超えていないことを確認してください。あるいは、最小帯域幅を class-fcoe または class-default に割り当てる場合は、これらのクラスの帯域幅を 0% に設定します。

- CSCsq39683

  症状：トラフィックが存在するファイバ チャネル リンクにより、次のような syslog エラーが生成されることがあります。

  ```
  2008 May 21 15:08:55 switch %KERN-3-SYSTEM_MSG: FCP_ERRFCP_PORT:
  gat_fcp_isr_process_blk_intr@1441, jiffies = 0xb1cec:ISR threshold reached, reg_block
  = 0x8, num_regs = 6, idx = 0, src_bit = 11 - kernel
  ```

  機能性は失われないため、これらのメッセージは無視できます。

  回避策：ありません。

- CSCso83662

  症状：さまざまなポートから送信されたすべての STP および PVRST フレームで、1 つのグローバル MAC アドレスが使用されます。この結果、複数のリンクが接続されたピア スイッチを、矛盾した MAC が通過する可能性があります。

  回避策：ありません。

解決済みの警告 — Cisco NX-OS リリース 4.0(0)N1(1a)

ここでは、このリリースの解決済みの警告について説明します。

- CSCsq53614

  症状：2 つの Cisco Nexus 5000 シリーズ スイッチ間で設定されたイーサネット ポート チャネルによって、DCBX プロセスでメモリ リークが発生します。このリークにより、最終的には DCBX プロセスがクラッシュし、システムがリブートします（数日かかります）。この問題が発生するのは、Cisco Nexus 5000 シリーズ スイッチ間のイーサネット ポート チャネルだけです。Catalyst 6500 シリーズ スイッチを使用するポート チャネルでは、この問題は発生しません。

  回避策：ポート チャネルのメンバーである各イーサネット インターフェイスで次の設定を入力して、ポート チャネル メンバーにおける Link Layer Discovery Protocol（LLDP）の送受信をディセーブルにします。

  ```
  Interface Ethernet 1/1
      no lldp receive
      no lldp transmit
  ```

- CSCsq36609

症状：SPAN ソースとして設定されている仮想イーサネット インターフェイスまたは仮想ファイバ チャネル インターフェイスで、インターフェイスの管理状態を変更するとメモリ リークが発生します。また、SPAN セッションを削除および追加しても、メモリ リークが発生します。最終的に、このメモリ リークによってスイッチがリブートします。

回避策：仮想イーサネット インターフェイスと仮想ファイバ チャネル インターフェイスを、SPAN ソースとして使用しないようにします。また、SPAN セッションを削除および追加しないようにします。

解決済みの警告 — Cisco NX-OS リリース 4.0(0)N1(1)

これは、Nexus 5000 シリーズ スイッチ用の Cisco NX-OS の最初のリリースでした。このリリースに解決済みの警告はありません。

Cisco Fabric Manager

Cisco Fabric Manager リリース 3.4(1a) 以降、Nexus 5000 シリーズ スイッチは Fabric Manager によりサポートされています。

FCoE を使用して Cisco Nexus 5000 シリーズ スイッチを展開する場合は、Fabric Manager を Display FCoE モードで運用する必要があります。Display FCoE モードでは、追加のツリー ノード、メニュー項目、ツールバー ボタンと、トポロジ ノードおよび FCoE に関連するリンクが表示されます。Display FCoE モードへ変換するには、server.properties ファイルを編集して display FCoE プロパティを true に設定します。

Fabric Manager の詳細については、『*Cisco Nexus 5000 Series Switch Fabric Manager Software Configuration Guide, Release 4.0*』を参照してください。

次のセクションは、Cisco Nexus 5000 シリーズ スイッチの Fabric Manager サポートに適用されます。

- 「制限事項」（P.30）
- 「警告」（P.31）

制限事項

ここでは、Cisco Nexus 5000 シリーズ スイッチの管理に関連した Cisco Fabric Manager の制限事項について説明します。

イーサネットの設定

物理イーサネット インターフェイスは、Fabric Manager または Device Manager を使用して設定できません。物理イーサネット インターフェイスは、CLI コマンドを使用して設定する必要があります。

SPAN

Device Manager を使用して、イーサネット インターフェイスまたは仮想イーサネット インターフェイスを SPAN ソース ポートとして設定したり、イーサネット インターフェイスを宛先ポートとして設定したりできません。回避策として、CLI コマンドを使用して SPAN を設定してください。

ゾーン分割

Edit Local Full Zone Database ツールでは、メンバーをゾーンに追加する [Switch Port WWN] 方式を使用して仮想ファイバ チャネル インターフェイスを指定する必要があります。[Add Members to Zone] ダイアログ ボックスでは、仮想ファイバ チャネル インターフェイスの [Switch & Port] 方式と [Domain & Port] 方式がサポートされません。

警告

ここでは、Cisco Nexus 5000 シリーズ スイッチの管理に関連した Cisco Fabric Manager の警告について説明します。

未解決の警告

- CSCq57019

  症状：Fabric Manager の N ポート仮想化（NPV）ウィザードには、NPV モードで動作している Cisco Nexus 5000 シリーズ スイッチがリストされません。

  回避策：ありません。

- CSCsq06170

  症状：Fabric Manager で、2 つの電源が搭載された Cisco Nexus 5000 シリーズ スイッチの電源が 1 つしか表示されません。

  回避策：Device Manager を使用します。[Physical] メニューの [Power Supplies] メニュー項目を使用すると、正しい情報が表示されます。

- CSCso82992

  症状：Device Manager で [Roles] ダイアログ ボックスを使用するとき、すでにロール スコープが定義されているロールのロール スコープを編集して、[Apply] ボタンをクリックすると、エラー メッセージ ダイアログ ボックスにエントリがすでに存在すると表示されます。

  回避策：[Apply] ボタンをもう一度クリックすると、変更内容が保存されます。

- CSCsq23436

  症状：NPV モードの Cisco Nexus 5000 シリーズ スイッチでは、負荷分散機能とトラフィック エンジニアリング機能がサポートされませんが、Fabric Manager はこれらの機能の設定をディセーブルにしません。[Switches] > [NPV] 情報ペインの、[Load Balancing] タブにこの機能をイネーブルにするチェックボックスがあり、[Traffic Engineering] タブにトラフィック エンジニアリング セッションを作成するダイアログ ボックスがあります。

  回避策：Cisco Nexus 5000 シリーズ スイッチでは、これらの設定オプションを無視してください。

- CSCsq14828

  症状：Cisco Nexus 5000 シリーズ スイッチまで FCoE 接続を使用する発信側のフロー統計またはイーサネット インターフェイス統計が、Web クライアントに表示されません。

  回避策：Fabric Manager の [Flow Statistics] を使用すると、フロー統計が正しく表示されます。Device Manager では、イーサネット インターフェイス統計が正しく表示されます。

- CSCsq32710

  症状：ユーザ定義のロールを使用して Cisco Nexus 5000 シリーズ スイッチにログインした場合、SNMP を使用してファイバ チャネル インターフェイスを取得できません。

  回避策：CLI コマンドを使用して情報を取得できます。

関連資料

Nexus 5000 シリーズのドキュメンテーションは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps9670/tsd_products_support_series_home.html

関連する Cisco Nexus 5000 シリーズのドキュメンテーションは、次のとおりです。

- *Cisco Nexus 5000 シリーズ スイッチ CLI ソフトウェア コンフィギュレーション ガイド*
- *Cisco Nexus 5000 シリーズ スイッチ Fabric Manager ソフトウェア コンフィギュレーション ガイド*
- *Cisco Nexus 5000 Series System Messages Reference*
- *Cisco Nexus 5000 Series MIB Quick Reference*
- *Cisco Nexus 5000 シリーズ コマンド リファレンス*
- *Cisco Nexus 5000 シリーズ ハードウェア インストレーション ガイド*

Cisco Nexus 2000 シリーズのドキュメンテーションは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps10110/tsd_products_support_series_home.html

関連する Cisco Nexus 2000 シリーズのドキュメンテーションは、次のとおりです。

- *Cisco Nexus 2000 Series Hardware Installation Guide*
- *Cisco Nexus 2000 Series CLI Software Configuration Guide*

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。
