



Cisco NCS 5500 シリーズ ルータ (IOS XR リリース 7.0.2) リリース ノート

[ネットワーク コンバージェンス システム 5500 シリーズルータ](#) 2

[このリリースで導入された新しいハードウェア](#) 2

[このリリースで導入された新しいソフトウェア機能](#) 3

[サポートされるハードウェア](#) 7

[リリース 7.0.2 パッケージ](#) 7

[ソフトウェア バージョンの特定](#) 8

[不具合](#) 8

[ファームウェアのサポートの特定](#) 9

[特記事項](#) 10

[Cisco IOS XR ソフトウェアのアップグレード](#) 11

[関連資料](#) 11

[通信、サービス、およびその他の情報](#) 11

[Full Cisco Trademarks with Software License](#) 13

改訂：2020年6月11日

ネットワーク コンバージョン システム 5500 シリーズ ルーター



(注) 強化された製品ドキュメントのエクスペリエンスを提供する、まったく新しいポータルである [コンテンツ ハブ](#) をご確認ください。

- ファセット検索を使用すると、自分に最も関連性の高いコンテンツを見つけることができます。
- カスタマイズした PDF を作成して、すぐに参照できるようにします。
- コンテキストベースの推奨事項を活用することができます。

パーソナライズされたドキュメントエクスペリエンスを実現するには、content.cisco.com のコンテンツハブから開始してください。

コンテンツ ハブでの体験のフィードバックをお送りください。

ネットワーク コンバージョン システム 5500 シリーズ ルーターは、コア、ピアリング、および WAN トランスポートの導入に対して、プログラマブルで高容量な、モジュール式の答えを提供します。Cisco IOS XR ソフトウェアの最新バージョンを実行する 5500 シリーズは、セグメントルーティング、高度な転送機能セット、プログラム可能なネットワーク管理をサポートしています。

このルーターシリーズの特長：

- 高パフォーマンス、高密度の 100 GE セントリック導入
- 冗長ルートプロセッサ、ファブリックカード、電源モジュール、およびシステムコントローラのオプション
- ワット/Gbps 単位での最適化された電力消費を特に重視
- アプリケーション ホスティング対応インフラストラクチャ
- YANG モデルベースの API を使用したプログラマビリティ

Cisco IOS XR オペレーティングシステムの最新リリースでは、64 ビットの Linux ベースのオペレーティングシステムを使用した Cisco IOS XR のアーキテクチャが開かれ、ネットワークの運用コストを削減をしながら、より優れた俊敏性、自動化、シンプルさを実現します。

このリリースで導入された新しいハードウェア

このリリースでは次のハードウェアが導入されています。

- NC57-24DD : Cisco NCS 5500 シリーズ 24 ポート 400 GE ベースラインカードが、第 2 世代ファブリックカード (NC55-5508-FC2/NC55-5516-FC2) およびファントレイ (NC55-5508-FAN2/NC55-5516-FAN2) が搭載された Cisco

NCS 5508 および Cisco NCS 5516 シャーシでサポートされています。詳細については、『Hardware Installation Guide for Cisco NCS 5500 Series Modular Routers』を参照してください。

詳細については、「[400GE Line Cards Data Sheet](#)」を参照してください。

- NC57-18DD-SE : Cisco NCS 5500 シリーズ 18 ポート 400 GE スケールラインカードが、第 2 世代ファブリックカード (NC55-5508-FC2/NC55-5516-FC2) およびファントレイ (NC55-5508-FAN2/NC55-5516-FAN2) が搭載された Cisco NCS 5508 および Cisco NCS 5516 シャーシでサポートされています。詳細については、『Hardware Installation Guide for Cisco NCS 5500 Series Modular Routers』を参照してください。

詳細については、「[400GE Line Cards Data Sheet](#)」を参照してください。

- QDD-400G-CU1M、QDD-400G-CU2M、QDD-400G-FR4-S、QDD-400G-DR4-S、QDD-400G-LR8 : これらの光モジュールが、NC57-24DD および NC57-18DD-SE ラインカードでサポートされています。詳細については、「[TMG compatibility matrix tool](#)」を参照してください。
- CFP2-WDM-DS100-HL、CFP2-WDM-DETS-1HL=、CFP2-WDM-DS-1HL= : Cisco NCS 5500 固定ポートおよびモジュラポートルータは、Cisco CFP2 DCO 着脱可能光モジュール (CFP2-WDM-DS100-HL、CFP2-WDM-DETS-1HL=、CFP2-WDM-DS-1HL) をサポートしています。詳細については、「[TMG compatibility matrix tool](#)」を参照してください。

このリリースで導入された新しいソフトウェア機能

このリリースの拡張機能を使用すると、ラインカード NC57-24DD および NC57-18DD-SE で使用可能な機能が、Cisco IOS XR リリース 6.5.1 で使用可能な機能と同等になります。

ただし、NC57-24DD および NC57-18DD-SE での次の機能のサポートは、今後の IOS XR リリースで予定されています。

- BVI
- EVPN
- ERSPAN
- DHCP リレー
- レイヤ 2
- L2 OAM
- 合法的傍受
- mLDP エッジ
- タイミング
- P2MP エッジ
- スマート ライセンス
- qos-group が入力ポリシーマップを使用して設定されている場合、QoS DSCP 保存ビットはサポートされません

IS-IS の SRv6 フレキシブルアルゴリズム

IPv6 を介したセグメントルーティング (SRv6) フレキシブルアルゴリズムを使用すると、オペレータは、独自のニーズに応じて IGP 最短パス計算をカスタマイズできます。オペレータは、リンクコストベースの SPF よりも優れた転送を実現するために、カスタムの SR プレフィックス SID を割り当てることができます。結果として、フレキシブルアルゴリズムにより、IGP から到達可能なあらゆる宛先へのトラフィック エンジニアリングに基づくパスを IGP で自動的に計算できます。

SR アーキテクチャでは、パスの計算方法を定義するアルゴリズムにプレフィックス SID が関連付けられます。フレキシブルアルゴリズムにより、ユーザが定義したメトリックタイプと制約の組み合わせに基づいて IGP でパスを計算する、ユーザ定義のアルゴリズムを実現できます。

SRv6 のトポロジに依存しないループフリー代替ノードと共有リスクリンクグループの保護

この機能は、IS-IS プロトコル用の IPv6 を介したセグメントルーティング (SRv6) を使用した、トポロジに依存しないループフリー代替 (TI-LFA) ノードの保護と共有リスクリンクグループ (SRLG) の保護のサポートを導入します。

- TI-LFA ノード保護機能は、ノード障害からの保護を提供します。ネイバー ノードはコンバージェンス後のバックアップパスの計算中に除外されます。
- TI-LFA SRLG 保護機能は、保護されているリンクの SRLG を除外するコンバージェンス後のバックアップパスを見つけようとしています。SRLG を保護リンクと共有するすべてのローカルリンクは、コンバージェンス後のバックアップパスの計算中に除外されます。

SRv6 マイクロループ回避

IPv6 を介したセグメントルーティング (SRv6) のマイクロループ回避機能により、IS-IS などのリンクステートルーティングプロトコルを使用して、トポロジ変更後のネットワーク コンバージェンス中に発生するマイクロループを防止または回避することができます。

マイクロループは、トポロジの変更 (リンクダウン、リンクアップ、またはメトリック変更イベント) 後にネットワークで発生する短いパケットループです。マイクロループは、ネットワーク内の異なるノードの非同時コンバージェンスによって引き起こされます。ノードが収束し、まだ収束していないネイバー ノードにトラフィックを送信すると、これら2つのノード間でトラフィックがループし、パケット損失、ジッター、および順不同パケットが発生する可能性があります。新しいトポロジでマイクロループが発生する可能性がある場合、ノードが計算した場合、ノードはセグメントのリストを使用して宛先へのループフリーパスを作成します。RIB 更新遅延タイマーの有効期限が切れた後、明示パスは通常の転送パスに置き換えられます。

SRv6 OAM : SID 検証

この機能は、IPv6 データプレーン (SRv6) を使用して、セグメントルーティングネットワークでの運用、管理、保守 (OAM) を強化します。

最短パスに沿ってリモート IPv6 プレフィックスに対して ping を実行してトレースする既存の OAM メカニズムは、SRv6 ネットワークに変更を加えることなく引き続き機能します。

ただし、従来の IPv6 OAM を使用して、リモート SRv6 SID 機能に対して ping を実行することやトレースすることはできません。この機能は、リモート SRv6 SID をターゲットとする ping の実行とトレースルートの操作を強化します。SRv6 対応ルータは、END.OP（パントを使用する OAM エンドポイント）と呼ばれる新しい SRv6 OAM SID を割り当てるようになりました。

ターゲットリモート SID には次のものが含まれます。

- END
- END.DT4/END.DX4（SRv6 を介した L3 サービスにより使用されます）
- END.DX2（SRv6 を介した L2 サービスにより使用されます）

BGP-LS レポートの SRv6 SID 情報

BGP-LS は、ノード、リンク、プレフィックスを使用してドメインのトポロジをレポートするために使用されます。この機能により、SRv6 セグメント識別子（SID）のネットワーク層到達性情報（NLRI）をレポートできるようになります。

SRv6 をサポートするために、次の NLRI が BGP-LS プロトコルに追加されました。

- ノード NLRI : SRv6 機能、SRv6 MSD タイプ
- リンク NLRI : End.X、LAN End.X、SRv6 MSD タイプ
- プレフィックス NLRI : SRv6 ロケータ
- SRv6 SID NLRI（ノードに関連付けられた SID の場合） : エンドポイント機能、BGP-EPE ピアノード/設定および Opaque

SRv6 サービス : L3VPN VPNv4 アクティブ-アクティブ冗長性

この機能は、L3VPN 展開の CE デバイスに対するアクティブ-アクティブ接続を提供します。CE デバイスは、1 つの LACP LAG ポートを介して冗長 PE に接続するレイヤ 2 またはレイヤ 3 のデバイスにすることができます。

SRv6 サービス : SRv6 サービス TLV タイプ 5 のサポート

IOS XR 6.6.1 は、IETF ドラフト [draft-dawra-idr-srv6-vpn-04](#) をサポートしています。SRv6 サービス SID 情報は SRv6-VPN SID TLV（TLV タイプ 4）で伝送されます。この SID TLV は、SRv6 SID 構造と一致しません。

IOS XR 7.0.2 以降のリリースでは、この不一致に対処するために、この実装は新しい SRv6 サービス TLV（TLV タイプ 5/6）および SRv6 SID 構造 サブ-サブ TLV が定義される [draft-ietf-bess-srv6-services-00](#) に準拠しています。

この機能は、2 つの TLV タイプ間の後方互換性を確保するためにも提供されています。

SRv6 サービス : BGP グローバル IPv4

この機能は、End.DT4 SRv6 機能を PE ノード（[draft-ietf-bess-srv6-services](#)）で実装することで SRv6 ベースの BGP サービスのサポートを拡張し、インターネット（IPv4）サービスを含めることができます。

起動時の IS-IS の最大メトリック

この機能により、IS-IS は、BGP がコンバージするか、指定された起動タイマーが期限切れになるまで、起動フェーズ中に最大メトリックをアダバタイズできます。

起動時にルータが最大メトリックで設定されている場合、IS-IS は、IS-IS リンクおよびルータから発信されたプレフィックスの最大メトリックをアダバタイズします。この設定により、ネイバルルータはラストリゾートの中継ノードとしてこのルータを使用します。最大メトリックは、ルーティングテーブルがコンバージしていない場合に、起動フェーズでのみアダバタイズされます。起動タイマーが期限切れになるか、BGP コンバージ信号が受信されると、通常のメトリックがアダバタイズされます。デフォルトルート、SRv6 ロケータ、または再配布されるプレフィックスの最大メトリックを設定できます。

ナローメトリックの場合、最大メトリック値は 63 です。ワイドメトリックの場合、最大メトリック値は 16777214 です。

SRv6 サービス : EVPN VPWS : オールアクティブ マルチホーミング

SRv6 を介した EVPN VPWS オールアクティブ マルチホーミングは、SRv6 ネットワークを介したオールアクティブ マルチホーミング機能を使用して、ELINE (P2P) サービスを提供します。

オールアクティブ マルチホーミングは、カスタマーエッジ (CE) デバイスを 2 台以上のプロバイダーエッジ (PE) デバイスに接続し、ロードバランシングと冗長接続を提供します。オールアクティブ マルチホーミングにより、すべての PE がマルチホームデバイスとの間でトラフィックを転送できます。

SRv6 サービス : EVPN VPWS : 入力 L2 フレームに基づく IPv6 フローラベル計算

この機能を使用すると、入力 EVPN VPWS PE が、着信イーサネットフレームの L2 フィールドおよび L3 フィールドに基づいて、最も外側の IPv6 ヘッダーのフローラベルフィールドを計算できます。

SRv6 サービス : EVPN VPWS : IPv6 QoS トラフィック クラス マーキング

この機能により、入力 EVPN VPWS PE が最上位の VLAN ヘッダーの CoS 値を、最も外側の IPv6 ヘッダーのトラフィック クラス (TC) フィールドにコピーできます。この機能により、IPv6 ネットワークでのトラフィックの優先順位付けが可能になります。

この機能を有効にするには、**hw-module profile segment-routing srv6 encapsulation traffic-class propagate** コマンドを使用します。このコマンドは、設定を有効にするためにルータをリロードする必要があります。

疑似回線を介した SPAN

(PW-SPAN と呼ばれる) 疑似回線トラフィックミラーリングは、既存の SPAN ソリューションの追加機能です。既存の SPAN ソリューションは、宛先インターフェイスで、または GRE トンネルまたは RSPAN を使用してモニタされます。PW-SPAN では、トラフィックミラーリングの宛先ポートは、物理ポートではなく疑似回線として設定されます。この場合、送信元ポートで指定したトラフィックは、中央への疑似回線にミラーリングされます。送信元ポートで指定されたトラフィックを疑似回線を介して中央の場所にミラーリングすることで、コストのかかるネットワークトラフィック分析ツールを一元化できます。

この機能の詳細については、『*Interface and Hardware Component Configuration Guide for Cisco NCS 5500 Series Routers*』の「*Configuring Traffic Mirroring*」の章を参照してください。

VRF リークを使用したブリッジポート間の MAC モビリティ

VRF リークを使用したブリッジポート間の MAC モビリティ機能は、VRF リーク機能によりブリッジポート間の EVPN MAC モビリティをサポートします。送信元とターゲットの両方の VRF が同じルータ上にある場合、ターゲット VRF 内の VM が移行されると、移行された VM に到達するためにこの機能が送信元 VRF 内のホストをサポートします。

この機能の詳細については、『*L2VPN and Ethernet Services Configuration Guide for Cisco NCS 5500 Series Routers*』および『*L2VPN and Ethernet Services Configuration Guide for Cisco NCS 560 Series Routers*』の「*Configure EVPN IRB*」の章を参照してください。

サポートされるハードウェア

サポート対象の光学部品、ハードウェア、および注文情報の完全なリストについては、『*Cisco NCS 5500 Series Data Sheet*』を参照してください。

Cisco NCS 5500 シリーズ ルータを設置するには、『*Hardware Installation Guide For Cisco NCS 5500 Series Router*』を参照してください。

リリース 7.0.2 パッケージ

次の表に、Cisco IOS XR ソフトウェアの機能セットのマトリックス（パッケージ）および関連付けられているファイル名を示します。

表 1: Cisco NCS 5500 シリーズ ルータ向けリリース 7.0.2 パッケージ

複合パッケージ		
フィーチャセット	ファイル名	説明
Cisco IOS XR IP ユニキャストルーティングのコアバンドル	ncs5500-mini-x	次を含む基本のイメージコンテンツが含まれています。 <ul style="list-style-type: none">• ホスト オペレーティング システム• システム管理者のブートイメージ• IOS XR のブートイメージ• BGP パッケージ
個別にインストール可能なオプションパッケージ		
フィーチャセット	ファイル名	説明
Cisco IOS XR Manageability パッケージ	ncs5500-mgbl-3.0.0.0-r702.x86_64.rpm	拡張マークアップ言語 (XML) パーサ、テレメトリ、Netconf、gRPC および HTTP サーバパッケージ。

Cisco IOS XR MPLS パッケージ	ncs5500-mpls-2.1.0.0-r702.x86_64.rpm ncs5500-mpls-te-rsvp-2.2.0.0-r702.x86_64.rpm	MPLS と MPLS トラフィック エンジン アリング (MPLS-TE) RPM。
Cisco IOS XR セキュリティ パッケージ	ncs5500-k9sec-3.1.0.0-r702.x86_64.rpm	暗号化、復号化、セキュア シェル (SSH)、セキュア ソケット レイヤ (SSL)、および公開キー インフラ ストラクチャ (PKI) をサポート
Cisco IOS XR ISIS パッケージ	ncs5500-isis-1.2.0.0-r702.x86_64.rpm	ISIS をサポート
Cisco IOS XR OSPF パッケージ	ncs5500-ospf-2.0.0.0-r702.x86_64.rpm	OSPF をサポート
合法的傍受 (LI) パッケージ	ncs5500-li-1.0.0.0-r702.x86_64.rpm	LI ソフトウェアイメージを格納
マルチキャスト パッケージ	ncs5500-mcast-1.0.0.0-r702.rpm	マルチキャストのサポート

ソフトウェアバージョンの特定

ルータで実行されているソフトウェアバージョンを確認するには、EXEC モードで **show version** コマンドを使用します。

```
RP/0/RP0/cpu 0: router# show version
Cisco IOS XR Software, Version 7.0.1
Cisco IOS XR Software, Version 7.0.2
Copyright (c) 2013-2020 by Cisco Systems, Inc.
```

```
Build Information:
Built By      : <username>
Built On     : Wed Mar 11 08:33:25 PDT 2020
Built Host   : iox-ucs-027
Workspace    : /auto/srcarchive17/prod/7.0.2/ncs5500/ws
Version    : 7.0.2
Location    : /opt/cisco/XR/packages/
Label       : 7.0.2
```

```
cisco NCS-5500 () processor
System uptime is 1 day 15 minutes
```

不具合

注意事項では、Cisco IOS XR ソフトウェアリリースの予期しない動作について説明します。重大度 1 の注意事項が最も重大度の高い注意事項で、重大度 2 の注意事項は重大度が低くなります。

NCS 5500 シリーズ ルータに固有の注意事項

注意事項では、Cisco IOS XR ソフトウェアリリースでの予期しない動作について説明します。これらの注意事項は、NCS 5500 シリーズ ルータに固有です。

不具合 ID	タイトル
CSCvt42370	ルータのリロード/アップグレード後の BVI での入力 IPv6 ACL による IPv6 トラフィックドロップ
CSCvt38319	TCAM キー形式が変更されると、ノードのリロード後もリロード要求がログに記録される
CSCvt24508	アップグレード/リロード後に 4x10 ブレークアウトが動作しない

ファームウェアのサポートの特定

EXEC モードで **show hw-module fpd** コマンドを使用して、ハードウェアのコンポーネントとそれらの現在の FPD バージョンおよびステータスを表示します。ハードウェアのステータスは **CURRENT** である必要があります。実行中とプログラム済みのバージョンは同じである必要があります。

(RP/0/RP0/CPU0) #show hw-module fpd

Location	Card type	HWver	FPD device	FPD Versions		
				ATR	Status	Running Programd
0/2	NC55-36X100G-S	0.4	MIFPGA		CURRENT	0.07 0.07
0/2	NC55-36X100G-S	0.4	Bootloader		CURRENT	1.14 1.14
0/2	NC55-36X100G-S	0.4	IOFPGA		CURRENT	0.11 0.11
0/2	NC55-36X100G-S	0.4	SATA		CURRENT	5.00 5.00
0/4/1	NC55-MPA-1TH2H-S	1.0	MPAFPGA		CURRENT	0.53 0.53
0/4/2	NC55-MPA-2TH-HX-S	0.1	MPAFPGA		CURRENT	0.53 0.53
0/4	NC55-MOD-A-S	1.0	MIFPGA		CURRENT	0.13 0.13
0/4	NC55-MOD-A-S	1.0	Bootloader		CURRENT	1.02 1.02
0/4	NC55-MOD-A-S	1.0	DBFPGA		CURRENT	0.14 0.14
0/4	NC55-MOD-A-S	1.0	IOFPGA		CURRENT	0.09 0.05
0/5	NC55-18H18F	1.0	MIFPGA		CURRENT	0.03 0.03
0/5	NC55-18H18F	1.0	Bootloader		CURRENT	1.14 1.14
0/5	NC55-18H18F	1.0	IOFPGA		CURRENT	0.22 0.22
0/5	NC55-18H18F	1.0	SATA		CURRENT	5.00 5.00
0/6/2	NC55-MPA-12T-S	0.1	MPAFPGA		CURRENT	0.27 0.27
0/6	NC55-MOD-A-SE-S	0.201	MIFPGA		CURRENT	0.13 0.13
0/6	NC55-MOD-A-SE-S	0.201	Bootloader		CURRENT	1.02 1.02
0/6	NC55-MOD-A-SE-S	0.201	DBFPGA		CURRENT	0.14 0.14
0/6	NC55-MOD-A-SE-S	0.201	IOFPGA		CURRENT	0.09 0.05
0/7/1	NC55-MPA-12T-S	0.1	MPAFPGA		CURRENT	0.27 0.27
0/7/2	NC55-MPA-12T-S	0.1	MPAFPGA		CURRENT	0.27 0.27
0/7	NC55-MOD-A-S		MIFPGA		NOT READY	
0/7	NC55-MOD-A-S	0.302	Bootloader		CURRENT	1.02 1.02
0/7	NC55-MOD-A-S	0.302	DBFPGA		CURRENT	0.14 0.14
0/7	NC55-MOD-A-S	0.302	IOFPGA		CURRENT	0.09 0.05
0/7	NC55-MOD-A-S	0.302	SATA		CURRENT	5.00 5.00
0/9	NC55-36X100G-A-SE	0.303	MIFPGA		CURRENT	0.03 0.03
0/9	NC55-36X100G-A-SE	0.303	Bootloader		CURRENT	0.14 0.14
0/9	NC55-36X100G-A-SE	0.303	DBFPGA		CURRENT	0.14 0.14
0/9	NC55-36X100G-A-SE	0.303	IOFPGA		CURRENT	0.26 0.21
0/9	NC55-36X100G-A-SE	0.303	SATA		CURRENT	5.00 5.00
0/13	NC55-6X200-DWDM-S	2.3	CFP2_PORT_2		NEED UPGD	5.23 5.23
0/13	NC55-6X200-DWDM-S	0.0	DENALI0		CURRENT	13.48 13.48
0/13	NC55-6X200-DWDM-S	0.0	DENALI1		CURRENT	13.48 13.48
0/13	NC55-6X200-DWDM-S	0.0	DENALI2		CURRENT	13.48 13.48

0/13	NC55-6X200-DWDM-S	0.0	MORGOTH	CURRENT	5.26	5.26
0/13	NC55-6X200-DWDM-S	0.0	MSFPGA0	CURRENT	2.22	2.22
0/13	NC55-6X200-DWDM-S	0.0	MSFPGA1	CURRENT	2.22	2.22
0/13	NC55-6X200-DWDM-S	0.0	MSFPGA2	CURRENT	2.22	2.22
0/13	NC55-6X200-DWDM-S	0.502	Bootloader	CURRENT	1.14	1.14
0/13	NC55-6X200-DWDM-S	0.502	IOFPGA	CURRENT	0.14	0.11
0/13	NC55-6X200-DWDM-S	0.502	SATA	CURRENT	5.00	5.00
0/RP0	NC55-RP-E	1.0	Bootloader	CURRENT	1.21	1.21
0/RP0	NC55-RP-E	1.0	IOFPGA	CURRENT	0.23	0.23
0/RP0	NC55-RP-E	1.0	OMGFPGA	CURRENT	0.48	0.48
0/RP1	NC55-RP-E	1.0	Bootloader	CURRENT	1.21	1.21
0/RP1	NC55-RP-E	1.0	IOFPGA	CURRENT	0.23	0.23
0/RP1	NC55-RP-E	1.0	OMGFPGA	CURRENT	0.48	0.48
0/FC0	NC55-5516-FC	0.216	Bootloader	CURRENT	1.75	1.75
0/FC0	NC55-5516-FC	0.216	IOFPGA	CURRENT	0.26	0.23
0/FC1	NC55-5516-FC	0.216	Bootloader	CURRENT	1.75	1.75
0/FC1	NC55-5516-FC	0.216	IOFPGA	CURRENT	0.26	0.23
0/FC2	NC55-5516-FC	0.216	Bootloader	CURRENT	1.75	1.75
0/FC2	NC55-5516-FC	0.216	IOFPGA	CURRENT	0.26	0.23
0/FC3	NC55-5516-FC	0.216	Bootloader	CURRENT	1.75	1.75
0/FC3	NC55-5516-FC	0.216	IOFPGA	CURRENT	0.26	0.23
0/FC4	NC55-5516-FC	0.216	Bootloader	CURRENT	1.75	1.75
0/FC4	NC55-5516-FC	0.216	IOFPGA	CURRENT	0.26	0.26
0/FC5	NC55-5516-FC	0.216	Bootloader	CURRENT	1.75	1.75
0/FC5	NC55-5516-FC	0.216	IOFPGA	CURRENT	0.26	0.23
0/PM3	NC55-PWR-3KW-2HV	0.2	DT-LogicMCU	CURRENT	3.01	3.01
0/PM3	NC55-PWR-3KW-2HV	0.2	DT-PrimMCU	CURRENT	3.00	3.00
0/PM3	NC55-PWR-3KW-2HV	0.2	DT-SecMCU	CURRENT	3.01	3.01
0/PM6	NC55-PWR-3KW-2HV	0.2	DT-LogicMCU	CURRENT	3.01	3.01
0/PM6	NC55-PWR-3KW-2HV	0.2	DT-PrimMCU	CURRENT	3.00	3.00
0/PM6	NC55-PWR-3KW-2HV	0.2	DT-SecMCU	CURRENT	3.01	3.01
0/SC0	NC55-SC	1.5	Bootloader	CURRENT	1.74	1.74
0/SC0	NC55-SC	1.5	IOFPGA	CURRENT	0.10	0.10
0/SC1	NC55-SC	1.5	Bootloader	CURRENT	1.74	1.74
0/SC1	NC55-SC	1.5	IOFPGA	CURRENT	0.10	0.10



(注) 製造業者が出荷したボード上の FPD バージョンが、IOS XR に統合された FPD パッケージ以降のバージョンである場合があります。

特記事項

- ブリッジドメイン (2 X BD) と GRE トンネルの合計数は、1518 を超えないようにする必要があります。ここで、1518 の数値は、多次元のスケール値を表しています。
- オフライン診断機能は、NCS 5500 プラットフォームではサポートされていません。したがって、**hw-module service offline location** コマンドは機能しません。ただし、**(sysadmin)# hw-module shutdown location** コマンドを使用して LC をダウンさせることができます。
- スマートライセンスの評価期間が終了したことを示す警告メッセージが、1 時間ごとにコンソールに表示されます。ただし、デバイス上の機能には影響ありません。この問題は、柔軟な消費ライセンスモデルが有効になっていないルータで発生します。メッセージの反復表示を停止するには、デバイスをスマート ライセンシング サーバに登録し、柔軟な消費モデルを有効にします。後で新しい登録トークンをロードします。

スマート ライセンシング サーバにデバイスを登録するには、[デバイスの登録とアクティブ化リンク](#)に記載されている手順に従ってください。

柔軟な消費ライセンスモデルを有効にしない場合は、CSCvk45026 SMUをインストールして、反復メッセージを停止します。

Cisco IOS XR ソフトウェアのアップグレード

Cisco IOS XR ソフトウェアは、モジュール型パッケージからインストールおよびアクティブ化され、関係のないプロセスに影響を与えることなく、特定の機能またはソフトウェアのパッチをインストール、アップグレード、またはダウングレードできます。ソフトウェアパッケージは、サポートされているすべてのカードタイプ、または単一のカード（ノード）でアップグレードまたはダウングレードできます。

アップグレードドキュメント ([NCS5500_Upgrade_Downgrade_MOP_7.0.2.pdf](#)) は、ソフトウェアイメージとともに入手できます。

ソフトウェアアップグレードを開始する前に、**admin** モードで **show install health** コマンドを使用します。このコマンドは、システムのすべての関連パラメータのステータスが、システムを中断せずにソフトウェアアップグレードの準備ができていないかどうかを検証します。

関連資料

最新の Cisco Network Convergence System 5500 シリーズのマニュアルは、次の URL にあります。

<http://www.cisco.com/c/en/us/support/routers/network-convergence-system-5500-series/tsd-products-support-series-home.html>

Cisco IOS XR システムのエラーメッセージ (SEM) が記載されたドキュメントは、次の URL にあります。

https://www.cisco.com/c/en/us/td/docs/ios_xr_sw/error/message/ios-xr-sem-guide.html

実稼働ソフトウェアメンテナンスの更新 (SMU)

実稼働 SMU は、正式に要求され、開発され、テストされ、リリースされた SMU です。実稼働の SMU は、ライブネットワーク環境での使用を目的としており、Cisco TAC と関連する開発チームによって正式にサポートされています。ソフトウェアの推奨事項またはバグ検索ツールを通して特定されるソフトウェアのバグは、実稼働 SMU 要求の根拠とはなりません。

実稼働 SMU タイプの詳細については、『[IOS XR Software Maintenance Updates \(SMUs\)](#)』ガイドの「[Production SMU Types](#)」の項を参照してください。

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、[Cisco Profile Manager](#) でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、[シスコ サービス](#)にアクセスしてください。
- サービス リクエストを送信するには、[シスコ サポート](#)にアクセスしてください。

- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、[Cisco Marketplace](#) にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、[Cisco Press](#) にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、[Cisco Warranty Finder](#) にアクセスしてください。

Cisco バグ検索ツール

[Cisco バグ検索ツール](#) (BST) は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

【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、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、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。

©2008 Cisco Systems, Inc. All rights reserved.

Cisco, Cisco Systems, およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。

本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R)

この資料の記載内容は2008年10月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255 (フリーコール、携帯・PHS含む)

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>