CHAPTER 1

概要

この章では、NX-OS ソフトウェアの概要を説明します。内容は、次のとおりです。

- ソフトウェアの互換性（p.1-1）
- サービサビリティ（p.1-4）
- 管理性（p.1-6）
- トラフィックのルーティング、フォワーディング、および管理（p.1-7）
- QoS（Quality Of Service）（p.1-8）
- ネットワーク セキュリティ（p.1-9）
- ライセンス（p.1-10）
- サポートされる標準（p.1-11）

ソフトウェアの互換性

Cisco NX-OS ソフトウェアは、Cisco IOS ソフトウェアのバリアントを実行するシスコ製品との相互運用が可能です。また、Cisco NX-OS ソフトウェアは、サポート対象として「サポートされる標準」（p.1-11）に記載されているネットワーキング標準に準拠したネットワーキング OS とも相互運用できます。

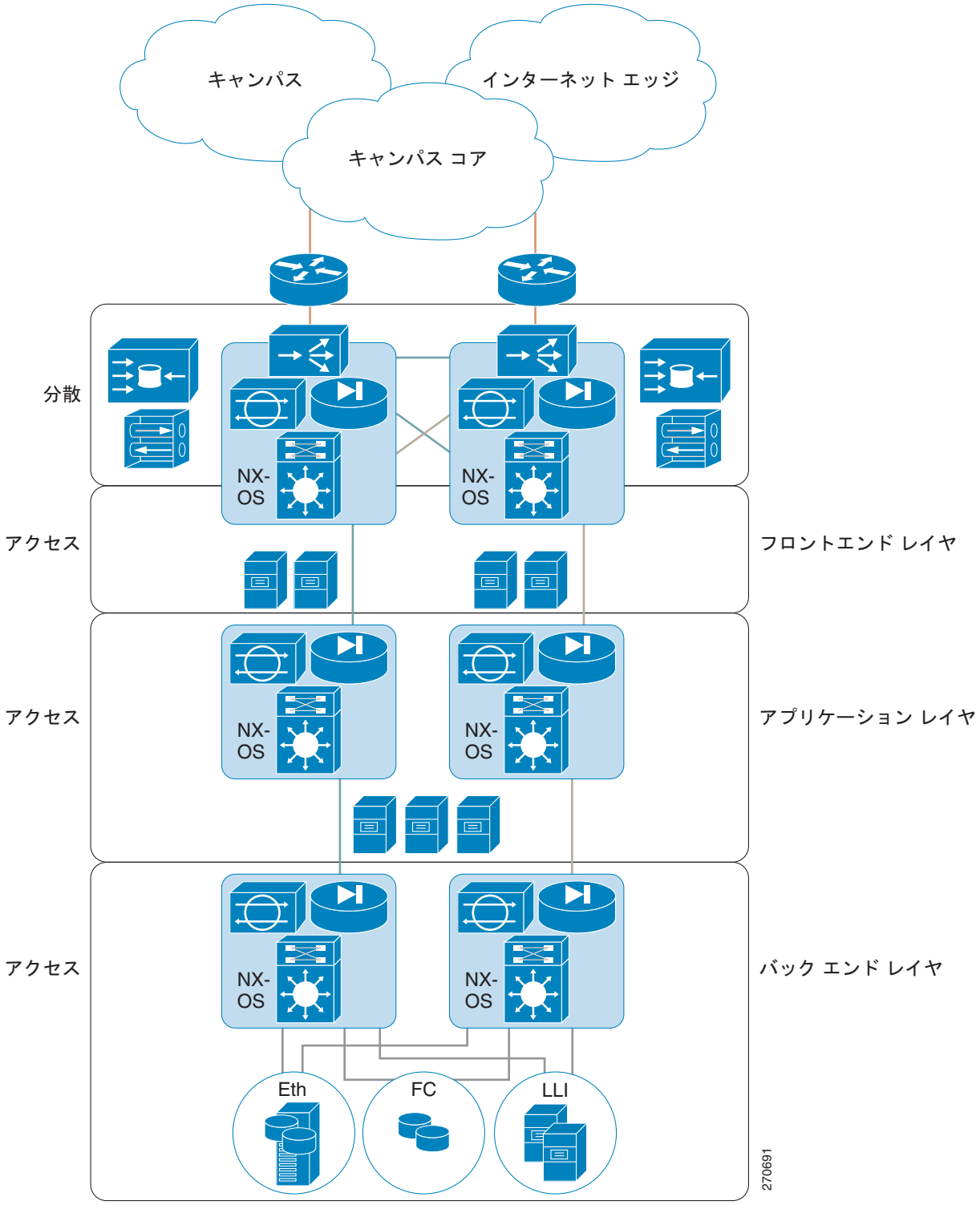
ここでは、次の内容について説明します。

- データセンター全体に共通のソフトウェア（p.1-2）
- モジュラ式のソフトウェア設計（p.1-3）
- Virtual Device Context（VDC; 仮想デバイス コンテキスト）（p.1-3）

データセンター全体に共通のソフトウェア

Cisco NX-OS ソフトウェアは、統合 OS として、LAN およびレイヤ 4 ～ 7 のネットワーク サービスなど、データセンター ネットワークの全領域において実行できるように設計されています（図 1-1 を参照）。

図 1-1　データセンター内の Cisco NX-OS



モジュラ式のソフトウェア設計

Cisco NX-OS ソフトウェアは、対称型マルチプロセッサ（SMP）、マルチコア CPU、分散データ モジュール プロセッサ上の分散マルチスレッド処理をサポートします。Cisco NX-OS ソフトウェアは、ハードウェア テーブル プログラミングのような大量の演算処理を要するタスクを、データ モジュールに分散された専用のプロセッサにオフロードします。モジュール化されたプロセスは、それぞれ別の保護メモリ領域内でオンデマンドに生成されます。機能がイネーブルになったときにのみ、プロセスが開始されてシステム リソースが割り当てられます。これらのモジュール化されたプロセスはリアルタイム プリエンプティブ スケジューラによって制御されるため、重要な機能が適切なタイミングで実行されます。

Virtual Device Context（VDC; 仮想デバイス コンテキスト）

Cisco NX-OS ソフトウェアには、システムおよびハードウェア リソースをセグメント化して仮想コンテキストを作成し、仮想デバイスをエミュレートする機能があります。各 virtual device context（VDC）には、固有のソフトウェア プロセス、専用のハードウェア リソース（インターフェイス）、および独立した管理環境があります。VDC は、それぞれ独立したネットワークを 1 つの共通インフラストラクチャに集約するための手段です。物理的に独立したネットワークの管理境界と障害分離の特性が維持される一方で、運用コストの面でインフラストラクチャの単一化による多くのメリットが期待できます。詳細については、『*Cisco NX-OS Virtual Device Context Configuration Guide*』Release 4.0 を参照してください。

サービサビリティ

Cisco NX-OS ソフトウェアには、デバイスがネットワークのトレンドやイベントに対応できるサービサビリティ機能が組み込まれています。これらの機能は、ネットワーク プランニングおよび応答時間の短縮に役立ちます。

ここでは、次の内容について説明します。

- Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）（p.1-4）
- Ethanalyzer（p.1-4）
- Call Home（p.1-4）
- オンライン診断（p.1-4）
- Embedded Event Manager（EEM）（p.1-5）
- NetFlow（p.1-5）

Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）

SPAN 機能を使用すると、外部アナライザが接続された SPAN の終点ポートに、セッションに負担をかけずに SPAN セッション トラフィックが送信されるようになり、ポート（SPAN ソース ポートと呼びます）間のすべてのトラフィックを分析できるようになります。SPAN の詳細については、『*Cisco NX-OS System Management Configuration Guide*』Release 4.0 を参照してください。

Ethanalyzer

Ethanalyzer は、Wireshark（旧称 Ethereal）オープン ソース コードに基づく Cisco NX-OS プロトコル アナライザ ツールです。Ethanalyzer は、パケットのキャプチャとデコード用の Wireshark のコマンド ライン バージョンです。ネットワークのトラブルシューティングおよびコントロール プレーン トラフィックの分析を実行するために Ethanalyzer を使用できます。Ethanalyzer の詳細については、『*Cisco NX-OS Troubleshooting Guide*』Release 4.0 を参照してください。

Call Home

Call Home は、ハードウェア コンポーネントとソフトウェア コンポーネントを継続的に監視し、重要なシステム イベントを E メールで通知する機能です。さまざまなメッセージ フォーマットが用意されており、ポケットベル サービス、標準の E メール、および XML ベースの自動解析アプリケーションに対応します。アラートをグループ化する機能があり、宛先プロファイルのカスタマイズも可能です。この機能を利用すると、たとえばネットワーク サポート技術者を直接ポケットベルで呼び出したり、E メール メッセージを Network Operations Center（NOC; ネットワーク オペレーション センター）に送信したり、Cisco AutoNotify サービスを使用して直接 Cisco Technical Assistance Center（TAC）でケースを生成したりすることができます。Call Home の詳細については、『*Cisco NX-OS System Management Configuration Guide*』Release 4.0 を参照してください。

オンライン診断

Cisco Generic Online Diagnostics（GOLD; 汎用オンライン診断）では、ハードウェアおよび内部データ パスが設計どおりに稼働していることを確認します。Cisco GOLD には、起動時診断、継続的監視、オンデマンドおよびスケジュールによるテストなどの機能セットがあります。GOLD を使用することで、迅速な障害分離と継続的なシステム監視が可能になります。GOLD の設定の詳細については、『*Cisco NX-OS System Management Configuration Guide*』Release 4.0 を参照してください。

Embedded Event Manager（EEM）

Cisco EEM は、ネットワーク イベントの発生に応じて動作をカスタマイズするのに役立つデバイスおよびシステムの管理機能です。EEM の設定の詳細については、『*Cisco NX-OS System Management Configuration Guide*』Release 4.0 を参照してください。

NetFlow

Cisco NX-OS に実装された NetFlow では、バージョン 5 およびバージョン 9 のエクスポートに加えて、Flexible NetFlow 構成モデル、およびハードウェア ベースの Sampled NetFlow がサポートされており、スケーラビリティが拡張されています。NetFlow の詳細については、『*Cisco NX-OS System Management Configuration Guide*』Release 4.0 を参照してください。

管理性

ここでは、次の内容について説明します。

- Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）（p.1-6）
- 構成の検証とロールバック（p.1-6）
- Role-Based Access Control（RBAC; ロールベース アクセス コントロール）（p.1-6）
- Connectivity Management Processor（CMP; 接続管理プロセッサ）（p.1-6）
- Cisco NX-OS デバイス コンフィギュレーション方式（p.1-6）

Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）

Cisco NX-OS ソフトウェアは、SNMP バージョン 1、2、および 3 に準拠しています。多くの MIB（Management Information Base; 管理情報ベース）がサポートされます。SNMP の詳細については、『*Cisco NX-OS System Management Configuration Guide*』Release 4.0 を参照してください。

構成の検証とロールバック

Cisco NX-OS ソフトウェアは、構成をコミットする前に構成の整合性や、必要なハードウェア リソースが使用可能かどうかを検証することができます。つまり、デバイスをあらかじめ構成しておいて、検証済みの構成を後で適用することができます。また、構成にはチェックポイントが組み込まれるため、必要に応じて、問題のない構成にロールバックすることができます。ロールバックの詳細については、『*Cisco NX-OS System Management Configuration Guide*』Release 4.0 を参照してください。

Role-Based Access Control（RBAC; ロールベース アクセス コントロール）

RBAC では、ユーザにロールを割り当てることで、デバイス操作のアクセスを制限できます。アクセスが必要なユーザだけにアクセスを許可するように、カスタマイズすることが可能です。RBAC の詳細については、『*Cisco NX-OS Security Configuration Guide*』Release 4.0 を参照してください。

Connectivity Management Processor（CMP; 接続管理プロセッサ）

Cisco NX-OS ソフトウェアは、CMP を使用したプラットフォームのリモート管理をサポートしています。CMP により、アウトオブバンド アクセス チャネルを通して NX-OS コンソールへのアクセスが可能になります。CMP の詳細については、『*Cisco Nexus 7000 Series Connectivity Management Processor Configuration Guide*』を参照してください。

Cisco NX-OS デバイス コンフィギュレーション方式

Secure Shell（SSH; セキュア シェル）セッションまたは Telnet セッションから CLI（コマンドライン インターフェイス）を使用してデバイスを設定できます。SSH では、デバイスへのセキュアな接続が提供されます。CLI コンフィギュレーション ガイドおよびコマンド リファレンスは、機能ごとに構成されています。詳細については、『*Cisco NX-OS configuration guides*』および『*Cisco NX-OS command references*』を参照してください。SSH および Talent の詳細については、『*Cisco NX-OS Security Configuration Guide*』Release 4.0 を参照してください。

また、XML 管理インターフェイスを使用してデバイスを構成できます。これは、CLI を補完する NETCONF プロトコルに基づくプログラム的な方式です。詳細については、『*Cisco NX-OS XML Management Interface User Guide*』Release 4.0 を参照してください。

トラフィックのルーティング、フォワーディング、および管理

ここでは、次の内容について説明します。

- イーサネット スイッチング（p.1-7）
- IP ルーティング（p.1-7）
- IP サービス（p.1-8）
- IP マルチキャスト（p.1-8）

イーサネット スイッチング

Cisco NX-OS ソフトウェアは、高密度、高パフォーマンスのイーサネット システムをサポートし、次のイーサネット スイッチング機能を提供します。

- IEEE 802.1D-2004 Rapid Spanning Tree Protocol（RSTP; 高速スパニング ツリー プロトコル）および多重スパニング ツリー プロトコル（802.1w および 802.1s）
- IEEE 802.1Q VLAN およびトランク
- 16,000 サブスクライバ VLAN
- IEEE 802.3ad リンク アグリゲーション
- プライベート VLAN
- シャーシ間プライベート VLAN
- アグレッシブ モードと標準モードの Unidirectional Link Detection（UDLD; 単一方向リンク検出）

詳細については、『*Cisco NX-OS Interfaces Configuration Guide*』Release 4.0 および『*Cisco NX-OS Layer 2 Switching Configuration Guide*』Release 4.0 を参照してください。

IP ルーティング

Cisco NX-OS ソフトウェアは、IP バージョン 4（IPv4）、IP バージョン 6（IPv6）、および次のルーティング プロトコルをサポートしています。

- OSPF プロトコル バージョン 2（IPv4）および 3（IPv6）
- Intermediate System-to-Intermediate System（IS-IS）プロトコル
- Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）
- Enhanced IGRP（EIGRP）
- RIP バージョン 2（RIPv2）

これらのプロトコルの NX-OS への実装は、最新の標準に完全に準拠しており、4 バイト自律システム番号（ASN）やインクリメンタル SPF などに対応しています。すべてのユニキャスト プロトコルで、ノンストップ フォワーディング グレースフル リスタート（NSF-GR）がサポートされます。すべてのプロトコルで、すべてのインターフェイス タイプ（イーサネット インターフェイス、VLAN インターフェイスおよびサブインターフェイス、ポート チャネル、トンネル インターフェイス、ループバック インターフェイスなど）がサポートされます。

IP サービス

Cisco NX-OS ソフトウェアでは、次の IP サービスを使用できます。

- Virtual Routing and Forwarding（VRF）
- DHCP Helper
- Hot-Standby Routing Protocol（HSRP）
- Gateway Load Balancing Protocol（GLBP）
- Enhanced Object Tracking（拡張オブジェクト追跡）
- Policy-Based Routing（PBR; ポリシーベース ルーティング）
- IPv4 ではすべてのプロトコルに対するユニキャスト グレースフル リスタート、IPv6 では OPSFv3 に対するユニキャスト グレースフル リスタート。

詳細については、『*Cisco NX-OS Unicast Routing Configuration Guide*』Release 4.0 を参照してください。

IP マルチキャスト

NX-OS リリース 4.0 は、次のマルチキャスト プロトコルおよび機能を備えています。

- PIM Version 2（PIMv2）
- Source Specific Multicast (SSM)
- PIM 希薄モード（IPv4 および IPv6 に対する Any-Source Multicast [ASM]）

（注）　Cisco NX-OS ソフトウェアは、PIM dense mode（PIM DM; PIM 稠密モード）はサポートしていません。

- 双方向 PIM（Bidir PIM）
- Anycast rendezvous point（Anycast-RP）
- IPv4 および IPv6 対応マルチキャスト NSF
- Bootstrap Router（BSR; ブートストラップ ルータ）を使用した RP 検出：Auto-RP およびスタティック
- Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）バージョン 1、2、3 ルータ ロール
- IGMPv2 ホスト モード
- IGMP スヌーピング
- Multicast Listener Discovery（MLD）プロトコル バージョン 2（IPv6）
- Multicast Source Discovery Protocol（MSDP）（IPv4 のみ）

詳細については、『*Cisco NX-OS Multicast Routing Configuration Guide*』Release 4.0 を参照してください。

QoS（Quality Of Service）

Cisco NX-OS ソフトウェアは、分類、マーキング、キューイング、ポリシング、スケジューリングなどの QoS 機能をサポートしています。Modular QoS CLI（MQC）がすべての QoS 機能をサポートします。MQC を使用すると、シスコのさまざまなプラットフォームで構成を統一することができます。詳細については、『*Cisco NX-OS Quality of Service Configuration Guide*』Release 4.0 を参照してください。

ネットワーク セキュリティ

ここでは、次の内容について説明します。

- Cisco TrustSec（p.1-9）
- その他のネットワーク セキュリティ機能（p.1-9）

Cisco TrustSec

Cisco TrustSec セキュリティは、データ機密性と完全性を実現しており、128 ビット Advanced Encryption Standard（AES; 高度暗号化規格）暗号化を使用した標準の IEEE 802.1AE リンク層での暗号化をサポートしています。リンク層での暗号化によって、エンドツーエンドのデータ プライバシーが保証されるとともに、暗号化されたパスに沿ってセキュリティ サービス デバイスを挿入することが可能になります。Cisco TrustSec は、IP アドレスではなくセキュリティ グループ タグに基づく SGACL（セキュリティ グループ アクセス コントロール リスト）を使用します。SGACL は、トポロジに依存しないため、ポリシーをシンプルにして管理を容易にします。詳細については、『*Cisco NX-OS Security Configuration Guide*』Release 4.0 を参照してください。

その他のネットワーク セキュリティ機能

Cisco TrustSec に加えて、Cisco NX-OS リリース 4.0 は次のセキュリティ機能を備えています。

- プロトコル準拠を調べるためのデータ パス Intrusion Detection System（IDS; 侵入検知システム）
- Control Plane Policing（CoPP）
- Message-Digest Algorithm 5（MD5）ルーティング プロトコル認証
- Dynamic Address Resolution Protocol（ARP; アドレス解決プロトコル）検査（DAI）、DHCP スヌーピング、IP ソース ガードなどのシスコの統合セキュリティ機能
- Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）
- RADIUS および TACACS+
- SSH プロトコル バージョン 2
- SNMPv3
- ポート セキュリティ
- IEEE 802.1x 認証
- レイヤ 2 Cisco Network Admission Control（NAC）LAN ポート IP
- 名前付き ACL（ポート ベース ACL [PACL]、VLAN ベース ACL [VACL]、およびルータ ベース ACL [RACL]）によってサポートされる、MAC アドレスおよび IPv4 アドレスに基づいたポリシー
- トラフィック ストーム制御（ユニキャスト、マルチキャスト、およびブロードキャスト）
- Unicast RPF

詳細については、『*Cisco NX-OS Security Configuration Guide*』Release 4.0 を参照してください。

ライセンス

Cisco NX-OS ライセンス機能により、その機能に対応する適切なライセンスをインストールすれば、デバイスでプレミアム機能を利用できるようになります。ライセンス パッケージに含まれていない機能は Cisco NX-OS ソフトウェアにバンドルされており、無料で提供されます。

各デバイスのライセンスを購入してインストールしてください。

（注）　例外的に Cisco TrustSec 機能は、ライセンスをインストールしなくてもイネーブルにできます。Cisco NX-OS ソフトウェアには、機能を試した後でライセンスを購入できる猶予期間があります。Cisco TrustSec 機能を有効にするには、Advanced Services ライセンス パッケージをインストールしてください。

NX-OS のライセンスの詳細については、『*Cisco NX-OS Licensing Guide*』Release 4.0 を参照してください。

ライセンスの問題のトラブルシューティングに関する詳細は、『*Cisco NX-OS Troubleshooting Guide*』Release 4.0 を参照してください。

サポートされる標準

表 1-1 に、IEEE 準拠標準を示します。

表 1-1　IEEE への準拠

標準	説明
802.1D	MAC ブリッジ
802.1s	多重スパニングツリー プロトコル
802.1w	高速スパニング ツリー プロトコル
802.1AE	MAC セキュリティ（リンク層暗号化）
802.3ad	LACP によるリンク集約
802.3ab	1000BaseT（銅線 10/100/1000 イーサネット）
802.3ae	10 ギガビット イーサネット
802.1Q	VLAN タギング
802.1p	イーサネット フレームのサービス タギング のクラス
802.1X	ポート ベースのネットワーク アクセス コントロール

表 1-2 に、RFC 準拠標準を示します。

表 1-2　RFC 準拠

標準	説明
BGP	
RFC 1997	BGP コミュニティ アトリビュート
RFC 2385	TCP MD5 シグネチャ オプションによる BGP セッションの保護
RFC 2439	BGP ルート フラップ ダンピング
RFC 2519	ドメイン間ルート アグリゲーションのフレームワーク
RFC 2858	BGP-4 のためのマルチプロトコル拡張
RFC 3065	BGP のための自律システム連合
RFC 3392	BGP-4 によるケイパビリティ アドバタイズメント
RFC 4271	BGP バージョン 4
RFC 4273	BGP4 MIB - BGP-4 のための管理対象オブジェクトの定義
RFC 4456	BGP ルート リフレクション
RFC 4486	BGP 中止通知メッセージのサブコード
RFC 4724	BGP のためのグレースフル リスタート メカニズム
RFC 4893	4 オクテット AS 番号空間に対する BGP のサポート
IETF ドラフト	最適パス遷移回避（draft-ietf-idr-avoid-transition-05.txt）
IETF ドラフト	ピア テーブル オブジェクト（draft-ietf-idr-bgp4-mib-15.txt）
IETF ドラフト	動的ケイパビリティ（draft-ietf-idr-dynamic-cap-03.txt）
OSPF	
RFC 2370	OSPF Opaque LSA オプション
RFC 2328	OSPF バージョン 2
RFC 2740	IPv6 のための OSPF（OSPF バージョン 3）
RFC 3101	OSPF Not-So-Stubby-Area（NSSA）オプション
RFC 3137	OSPF スタブ ルータ アドバタイズメント

表 1-2　RFC 準拠 （続き）

標準	説明
RFC 3509	OSPF エリア境界ルータの代替実装
RFC 3623	グレースフル OSPF リスタート
RFC 4750	OSPF バージョン 2 MIB
RIP	
RFC 1724	RIPv2 MIB 拡張
RFC 2082	RIPv2 MD5 認証
RFC 2453	RIP バージョン 2
IS-IS	
RFC 1142 （OSI 10589）	OSI 10589 IS-IS ドメイン間ルーティング交換プロトコル
RFC 1195	TCP/IP 環境およびデュアル環境におけるルーティングのための OSI IS-IS の使用
RFC 2763	IS-IS のための動的ホスト名交換メカニズム
RFC 2966	2 レベル IS-IS によるドメイン全体へのプレフィクス配布
RFC 2973	IS-IS メッシュ グループ
RFC 3277	IS-IS 過渡的ブラックホール回避
RFC 3373	IS-IS ポイントツーポイント隣接関係確立のための 3 ウェイ ハンドシェイク
RFC 3567	IS-IS 暗号化認証
RFC 3847	IS-IS のためのリスタート シグナリング
IETF ドラフト	インターネット ドラフト：リンクステート ルーティング プロトコルにおける LAN 経由ポイントツーポイント オペレーション （draft-ietf-isis-igp-p2pover-lan-06.txt）
IP サービス	
RFC 768	UDP
RFC 783	TFTP
RFC 791	IP
RFC 792	ICMP
RFC 793	TCP
RFC 826	ARP
RFC 854	Telnet
RFC 959	FTP
RFC 1027	プロキシ ARP
RFC 1305	NTP v3
RFC 1519	CIDR
RFC 1542	BootP リレー
RFC 1591	DNS クライアント
RFC 1812	IPv4 ルータ
RFC 2131	DHCP Helper
RFC 2338	VRRP
RFC 2784	Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）

表 1-2　RFC 準拠 （続き）

標準	説明
IP マルチキャスト	
RFC 2236	IGMP バージョン 2
RFC 2710	IPv6 のための Multicast Listener Discovery（MLD）
RFC 3376	IGMP バージョン 3
RFC 3446	PIM および MSDP を使用したエニーキャスト ランデブー ポイント（Anycast-RP）メカニズム
RFC 3569	SSM の概要
RFC 3618	MSDP
RFC 3810	IPv6 のための MLD バージョン 2（MLDv2）
RFC 4601	ASM - 希薄モード（PIM-SM）：プロトコル仕様（改訂）
RFC 4607	IP のための SSM
RFC 4610	PIM を使用した Anycast-RP
IETF ドラフト	mtrace 要求を処理するための mtrace サーバ機能（draft-ietf-idmr-traceroute-ipm-07.txt）
IETF ドラフト	Bi-directional Protocol Independent Multicast（BIDIR-PIM; 双方向プロトコル独立マルチキャスト）（draft-ietf-pim-bidir-09.txt）