QoS：NBAR コンフィギュレーション ガイド

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/

【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。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

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.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

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:http://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.(1110R)

© 2017 Cisco Systems, Inc. All rights reserved.

目 次

最初にお読みください 1

NBAR を使用したネットワーク トラフィックの分類 3

機能情報の確認 4

NBAR を使用したネットワーク トラフィックの分類に関する制約事項 4

NBAR を使用したネットワーク トラフィックの分類に関する情報 6

NBAR の機能 6

NBAR の利点 7

NBAR と HTTP トラフィックの分類 8

URL、ホスト、または MIME による HTTP トラフィックの分類 8

HTTP ヘッダー フィールドを使用した HTTP トラフィックの分類 9

HTTP ヘッダーと URL、ホスト、または MIME タイプの分類の組み合わせによる HTTP トラフィックの特定 10

NBAR と Citrix ICA トラフィックの分類 10

発行済みアプリケーション名による Citrix ICA トラフィックの分類 11

Citrix ICA クライアント モード 11

ICA タグ番号による Citrix ICA トラフィックの分類 12

Citrix ICA Packet Tagging 12

NBAR と RTP ペイロード タイプの分類 13

NBAR とカスタム プロトコルおよびアプリケーションの分類 14

NBAR DNS ベースの分類 15

NBAR とダイナミック PDLMs を使用した分類 16

NBAR がサポートするプロトコル 17

NBAR プロトコル パック 17

NBAR とピアツーピア ファイル共有アプリケーションの分類 17

NBAR 多段階分類 18

NBAR の拡張性 19

インターフェイス拡張性 19

フロー拡張性 20
フロー テーブルのサイジング 20
NBAR Protocol Discovery 21
NBAR Protocol Discovery MIB 21
NBAR とマルチパケットの分類 21
VRF インターフェイス上の NBAR 22
NBAR と IPv6 22
IPv6 に対する NBAR のサポート 22
GETVPN に対する NBAR のサポート 23
CAPWAP に対する NBAR のサポート 23
NBAR の設定プロセス 24
NBAR の再起動 25
DNS ベースの分類の設定方法 25
DNS ベースの分類の有効化と無効化 25
DNS ベースの分類のための DNS ガードの有効化と無効化 26
NBAR を使用したネットワーク トラフィックの分類方法 27
カテゴリの使用に適合する属性ベースのプロトコルの設定について 27
SRND の使用に適合する属性ベースのプロトコルの設定について 27
属性：traffic-class 28
属性：business-relevance 29
カテゴリとサブカテゴリを使用した属性ベースのプロトコル一致の設定 30
SRND を使用した属性ベースのプロトコル一致の設定 32
SRND 設定：典型的なクラスマップ、ポリシーマップ 33
Cisco ソフトウェアの NBAR を使用したネットワーク トラフィックの分類の設定例 35
例：HTTP ヘッダー フィールドを使用した HTTP トラフィックの分類 35
例：HTTP ヘッダーおよび URL、Host、または MIME タイプの分類の組み合わせによる HTTP トラフィックの識別 36
例：NBAR とカスタム プロトコルおよびアプリケーションの分類 36
例：NBAR とピアツーピア ファイル共有アプリケーションの分類 36
例：属性ベースのプロトコル一致の設定 37
例：SRND 設定 - アプリケーションをビジネス関連（business-relevant）と再分類する 39

例：組み込みプロトコルのカスタマイズ 39
その他の参考資料 40
NBAR を使用したネットワーク トラフィックの分類の機能情報 41
用語集 45
NBAR プロトコル パック 49
機能情報の確認 49
NBAR プロトコル パックの前提条件 50
NBAR プロトコル パックの制約事項 50
NBAR プロトコル パックについて 50
プロトコル パックの概要 50
SSL unique-name サブ分類 51
RTP 動的ペイロード タイプのサブ分類 52
NBAR2 プロトコル パック 9.0.0 内の QoS とレポート用の新しいカテゴリとサブカテゴリ 52
NBAR2 プロトコル パック 9.0.0 でサポートされるカテゴリとサブカテゴリ 52
NBAR プロトコル パックのロード方法 55
NBAR プロトコル パックのロード 55
NBAR プロトコル パックの設定例 57
例：NBAR プロトコル パックのロード 57
例：ロードされた NBAR プロトコル パックの確認 57
例：NBAR 分類情報の表示 58
例：SSL セッションの分類 60
例：RTP 動的ペイロード タイプの分類 60
NBAR プロトコル パックに関する追加情報 60
NBAR プロトコル パックの機能情報 61
Protocol Discovery のイネーブル化 63
機能情報の確認 63
Protocol Discovery のイネーブル化の前提条件 64
Protocol Discovery のイネーブル化に関する制限事項 64
Protocol Discovery に関する情報 65
Protocol Discovery の概要 65
インターフェイス拡張性 66

Protocol Discovery のイネーブル化方法 66
インターフェイスでの Protocol Discovery のイネーブル化 66
Protocol Discovery の統計情報のレポート 68
Protocol Discovery の設定例 69
例：インターフェイスでの Protocol Discovery のイネーブル化 69
例：Protocol Discovery の統計情報のレポート 70
その他の参考資料 71
Protocol Discovery のイネーブル化の機能情報 72
自動トラフィック分析とプロトコル生成 73
auto-custom の前提条件 73
auto-custom の制限 74
背景：NBAR2 auto-learn を使用した自動トラフィック分析 74
auto-custom を使用したカスタム プロトコルの自動生成 74
自動カスタム モードの有効化および無効化 76
作成する自動生成 NBAR プロトコルの最大数の設定 76
自動カスタム プロトコルを再生成する時間間隔の設定 77
自動カスタム データのクリア 78
自動カスタム機能で作成された自動生成 NBAR プロトコルの表示 79
自動カスタム プロトコルの NBAR Protocol Discovery 情報の表示 80
Configuring NBAR Using the MQC 81
機能情報の確認 81
MQC を使用した NBAR の設定の前提条件 82
NBAR の粗粒分類に関する情報 82
NBAR と MQC の機能 82
NBAR と match protocol コマンド 83
MQC を使用して NBAR を設定する方法 84
DSCP ベースのレイヤ 3 カスタム アプリケーションの設定 84
未分類トラフィックと不明トラフィックの管理 85
トラフィック ポリシーの設定 87
トラフィック ポリシーのインターフェイスまたはサブインターフェイスへの適用 89
MCQ を使用した NBAR の確認 91

未知および未分類のトラフィック管理の確認 92
DSCP ベースのレイヤ 3 カスタム アプリケーションの設定例 93
例：トラフィック クラスの設定 93
例：トラフィック ポリシーの設定 94
例：トラフィック ポリシーのインターフェイスまたはサブインターフェイスへの適用 94
例：NBAR のプロトコルからポートへのマッピングの確認 95
例：任意の IP ポートの L3 カスタム 95
次の作業 95
その他の参考資料 95
Configuring NBAR Using the MQC の機能情報 97
DSCP ベースのレイヤ 3 カスタム アプリケーション 101
機能情報の確認 101
DSCP ベースのレイヤ 3 カスタム アプリケーションの制約事項 102
DSCP ベースのレイヤ 3 カスタム アプリケーションの概要 102
NBAR2 auto-learn の設定方法 102
DSCP ベースのレイヤ 3 カスタム アプリケーションの設定 102
DSCP ベースのレイヤ 3 カスタム アプリケーションの設定例 103
例：DSCP ベースのレイヤ 3 カスタム アプリケーション 103
例：任意の IP ポートの L3 カスタム 104
DSCP ベースのレイヤ 3 カスタム アプリケーションに関する追加情報 104
DSCP ベースのレイヤ 3 カスタム アプリケーションの機能情報 105
トランスポート階層に基づく MQC 107
機能情報の確認 107
トランスポート階層に基づく MQC の制限事項 108
トランスポート階層に基づく MQC に関する情報 108
トランスポート階層に基づく MQC の概要 108
トランスポート階層に基づく MQC の設定方法 109
トランスポート階層に基づく MQC の設定 109
トランスポート階層に基づく MQC の確認 111
トランスポート階層に基づく MQC の設定例 112
例：トランスポート階層に基づく MQC の設定 112

例：トランスポート階層に基づく MQC の設定の確認 112
その他の参考資料 113
トランスポート階層に基づく MQC の機能情報 113
NBAR の分類と属性 115
機能情報の確認 115
NBAR2 カスタム プロトコルに関する情報 116
NBAR の分類と属性 116
NBAR2 カスタム プロトコルの概要 117
NBAR2 カスタム プロトコルの設定方法 118
NBAR 属性のカスタマイズ 118
NBAR2 カスタム プロトコルの設定例 120
例：属性のカスタム値の追加 120
例：属性のカスタム値に関する情報の表示 120
例：プロファイルの作成およびプロファイルの属性の設定 121
例：属性プロファイルのプロトコルへの適用 122
NBAR2 カスタム プロトコルに関する追加情報 122
NBAR の分類と属性の機能情報 122
Flexible NetFlow により抽出したフィールドの報告 125
機能情報の確認 125
Flexible NetFlow 経由で抽出したフィールドのレポートに関する情報 126
Subapplication テーブルのフィールド 126
Flexible NetFlow 経由で抽出したフィールドのレポート方法 126
Subapplication テーブルのフィールドのレポート 126
Flexible NetFlow 経由で抽出したフィールドをレポートするための設定例 127
例：Subapplication フィールドのレポート 127
その他の参考資料 127
Reporting Extracted Fields Through Flexible NetFlow の機能情報 129
NBAR プロトコル パック自動更新 131
NBAR プロトコル パック自動更新の導入 132
プロトコル パック自動更新のための送信元サーバのセットアップ 134
プロトコル パック自動更新のためのプロトコル パック サーバの設定 135
プロトコル パック自動更新の設定ファイル 136

プロトコル パック自動更新の有効化 141
プロトコル パック自動更新の無効化 142
自動更新によるプロトコル パック更新の即時開始 142
プロトコル パック自動更新情報の表示 143
ルータでのローカル プロトコル パック自動更新の設定 144
プロトコル パック自動更新サブモード コマンド 145
NBAR2 カスタム プロトコル 147
機能情報の確認 147
カスタム プロトコルの作成の前提条件 148
カスタム プロトコルの作成に関する情報 148
NBAR とカスタム プロトコル 148
MQC と NBAR カスタム プロトコル 149
IP アドレスおよびポートベースのカスタム プロトコル 149
カスタム NBAR プロトコルの比較：単一のネットワーク プロトコルに基づく場合と複数のネットワーク プロトコルに基づく場合 150
カスタム プロトコルの制限 150
カスタム プロトコルの作成方法 151
単一のネットワーク プロトコルに基づいたカスタム NBAR プロトコルの定義 151
例 152
複数のネットワーク プロトコルに基づいたカスタム NBAR プロトコルの定義 153
カスタム プロトコルを使用するためのトラフィック クラスの設定 154
トラフィック ポリシーの設定 156
トラフィック ポリシーのインターフェイスへの適用 158
カスタム プロトコル情報の表示 160
IP アドレスおよびポートベースのカスタム プロトコルの設定 161
カスタム プロトコルの作成の設定例 162
例：カスタム プロトコルの作成 162
例：カスタム プロトコルを使用するためのトラフィック クラスの設定 162
例：トラフィック ポリシーの設定 163
例：トラフィック ポリシーのインターフェイスへの適用 163
例：カスタム プロトコル情報の表示 163
例：IP アドレスおよびポートベースのカスタム プロトコルの設定 164

その他の参考資料 164
NBAR2 カスタム プロトコルの機能情報 165
NBAR2 プロトコル パック ヒットレス アップグレード 167
機能情報の確認 167
NBAR2 プロトコル パック ヒットレス アップグレードの制約事項 168
NBAR2 プロトコル パック ヒットレス アップグレードに関する情報 168
NBAR2 PP ヒットレス アップグレードの概要 168
NBAR2 プロトコル パック ヒットレス アップグレードのメリット 169
NBAR2 プロトコル パック ヒットレス アップグレードに関する追加情報 169
NBAR2 プロトコル パック ヒットレス アップグレードの機能情報 170
NBAR の Web ベース カスタム プロトコル 173
機能情報の確認 173
NBAR の Web ベース カスタム プロトコルの制限事項 174
NBAR の Web ベース カスタム プロトコルに関する情報 174
NBAR の Web ベース カスタム プロトコルの概要 174
NBAR の Web ベース カスタム プロトコル一致の定義方法 174
Web ベースのカスタム プロトコル一致の定義 174
NBAR の Web ベース カスタム プロトコルの設定例 175
例：Web ベースのカスタム プロトコル一致の定義 175
NBAR の Web ベース カスタム プロトコルに関する追加情報 176
NBAR の Web ベース カスタム プロトコルの機能情報 176
NBAR2 HTTP ベースの可視性ダッシュボード 179
機能情報の確認 179
NBAR2 HTTP ベースの可視性ダッシュボードに関する情報 180
NBAR2 HTTP ベースの可視性ダッシュボードの概要 180
NBAR2 HTTP ベースの可視性ダッシュボードの設定方法 180
NBAR2 HTTP ベースの可視性ダッシュボードの設定 180
NBAR2 HTTP ベースの可視性ダッシュボードの設定例 181
例：NBAR2 HTTP ベースの可視性ダッシュボード 181
NBAR2 HTTP ベースの可視性ダッシュボードへのアクセス 181
可視性ダッシュボードへのアクセス 181
NBAR2 HTTP ベースの可視性ダッシュボードに関する追加情報 182

NBAR2 HTTP ベースの可視性ダッシュボードの機能情報 182

NBAR の粗粒分類 185

機能情報の確認 185

NBAR の粗粒分類に関する情報 186

NBAR の粗粒分類の概要 186

簡易分類 186

先頭パケットによる分類 186

粗粒モードの制限 186

細粒モードと粗粒モードの比較 187

NBAR の粗粒分類の設定方法 187

NBAR 分類モードの設定 187

アプリケーション統計情報を使用した Performance Monitor コンテキストの設定 188

NBAR の粗粒分類の設定例 190

例：NBAR 分類モードの設定 190

例：アプリケーション統計情報プロファイルによる Performance Monitor コンテキストの設定 190

例：アプリケーション統計情報プロファイルを使用した Performance Monitor コンテキストの設定と細粒 NBAR 分類モード強制設定 191

例：NBAR 分類モードの確認 191

NBAR の粗粒分類に関する追加資料 191

NBAR の粗粒分類の機能情報 192

SSL カスタム アプリケーション 193

機能情報の確認 193

SSL カスタム アプリケーションに関する情報 194

SSL カスタム アプリケーションの概要 194

SSL unique name サブ分類 194

SSL カスタム アプリケーションの設定方法 197

SSL カスタム アプリケーションの設定 197

SSL カスタム アプリケーションの設定例 198

例：SSL カスタム アプリケーション 198

SSL カスタム アプリケーションに関する追加情報 198

SSL カスタム アプリケーションの機能情報 199

選択的アプリケーションのための細粒 NBAR 201

機能情報の確認 201

選択的アプリケーションのための細粒 NBAR に関する情報 202

選択的アプリケーションのための細粒 NBAR の概要 202

選択的アプリケーションのための細粒 NBAR の設定方法 202

選択的アプリケーションのための細粒 NBAR の設定 202

選択的アプリケーションのための細粒 NBAR の設定例 203

例：選択的アプリケーションのための細粒 NBAR 203

例：選択的アプリケーションのための細粒 NBAR の確認 204

選択的アプリケーションのための細粒 NBAR に関する追加情報 204

選択的アプリケーションのための細粒 NBAR の機能情報 204

DNS 名に基づく NBAR カスタム アプリケーション 207

機能情報の確認 207

DNS 名に基づく NBAR カスタム アプリケーションの前提条件 208

DNS 名に基づく NBAR カスタム アプリケーションの制限事項 208

DNS 名に基づく NBAR カスタム アプリケーションに関する情報 208

DNS 名に基づく NBAR カスタム アプリケーションの概要 208

DNS 名に基づく NBAR カスタム アプリケーションの設定方法 209

DNS 名に基づく NBAR カスタム アプリケーションの設定 209

DNS 名に基づく NBAR カスタム アプリケーションの設定例 210

例：DNS 名に基づく NBAR カスタム アプリケーションの設定 210

DNS 名に基づく NBAR カスタム アプリケーションに関する追加情報 210

DNS 名に基づく NBAR カスタム アプリケーションの機能情報 211

NBAR2 auto-learn 213

機能情報の確認 213

NBAR2 auto-learn の概要 214

NBAR2 auto-learn の設定方法 215

NBAR2 auto-learn の設定 215

auto-learn の上位ホストまたはポートの表示 216

auto-learn の上位ソケットの表示 217

NBAR2 auto-learn のホスト/ポート統計のクリア 218

NBAR2 auto-learn のホスト/ポスト統計と非アクティブ ホスト/ポートのクリア 218

NBAR2 auto-learn の設定例 219
例：ホストの auto-learn の設定 219
例：auto-learn データの表示 219
NBAR2 auto-learn に関する追加情報 221
NBAR2 auto-learn の機能情報 221
DNS-AS 223
はじめに 223
DNS-AS の利用 224
事前定義のプロトコルとカスタマイズされたプロトコル 226
分類とトラフィック ポリシー 226
効率的な中央集中型設定 227
DNS-AS と SDN コントローラの機能の比較 227
進化するネットワークとネットワーク トラフィックに対応する NBAR2 227
カスタム プロトコル機能との比較 228
DNS-AS メカニズム 229
DNS-AS のセットアップ 231
DNS-AS サーバのセットアップ 231
DNS-AS ルータのセットアップ 233
ネットワークへの新しいアプリケーションの導入 233
制約事項 233
DNS-AS CLI コマンド 234
DNS-AS の有効化と設定 234
ルータがクエリするための DNS-AS サーバの設定 236
トラステッド ドメインの設定 237
DNS-AS の有効化 237
DNS-AS の無効化 238
DNS-AS 用インターフェイスでの NBAR の有効化 239
DNS-AS のモニタリング 240
DNS-AS クライアント統計情報の表示 241
DNS-AS カスタム アプリケーション データの表示 241
DNS-AS カスタム アプリケーション データの表示：詳細 242
受信および送信カウントのクリア 243

auto-learn テーブルのクリア 243
DNS-AS 学習のクリアと再開 244
アクティブな DNS サーバの表示 244
DNS-AS auto-learn データの表示 245
保留中の DNS クエリの表示 246
保留中の DNS クエリ統計情報のクリア 246
DNS-AS のトラブルシューティング 247

第 1 章

最初にお読みください

Cisco IOS XE 16 に関する重要な情報

有効な 2 つのリリースとしての Cisco IOS XE リリース 3.7.0E（Catalyst スイッチ用）および Cisco IOS XE リリース 3.17S（アクセスおよびエッジ ルーティング用）が、1 つのバージョンの統合されたリリース（Cisco IOS XE 16）へと展開（マージ）されています。これにより、スイッチングおよびルーティング ポートフォリオの広範なアクセスおよびエッジ製品が盛り込まれた 1 つのリリースが実現しました。

（注） 技術構成ガイドの機能情報の表に、機能の導入時期を記載しています。その他のプラットフォームでその機能がサポートされた時期については示されていない場合があります。特定の機能が使用しているプラットフォームでサポートされているかどうかを判断するには、製品のランディング ページに掲載された技術構成ガイドを参照してください。技術的構成ガイドが製品のランディング ページに表示される場合は、その機能がお使いのプラットフォームでサポートされていることを示します。

第 2 章

NBAR を使用したネットワーク トラフィックの分類

Network-Based Application Recognition（NBAR）は、多様なプロトコルとアプリケーションを認識および分類する分類エンジンです。NBAR がプロトコルまたはアプリケーションを認識して分類したら、そのアプリケーション、またはプロトコルが分類されたトラフィックに適切な Quality of Service（QoS）を適用するようにネットワークを設定できます。

このモジュールでは、NBAR を使用したネットワーク トラフィックの分類の概要について説明します。

- 機能情報の確認，4 ページ
- NBAR を使用したネットワーク トラフィックの分類に関する制約事項，4 ページ
- NBAR を使用したネットワーク トラフィックの分類に関する情報，6 ページ
- NBAR の設定プロセス，24 ページ
- NBAR の再起動，25 ページ
- DNS ベースの分類の設定方法，25 ページ
- NBAR を使用したネットワーク トラフィックの分類方法，27 ページ
- Cisco ソフトウェアの NBAR を使用したネットワーク トラフィックの分類の設定例，35 ページ
- その他の参考資料，40 ページ
- NBAR を使用したネットワーク トラフィックの分類の機能情報，41 ページ
- 用語集，45 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

NBAR を使用したネットワーク トラフィックの分類に関する制約事項

NBAR は次のアプリケーションをサポートしません。

- 非 IP トラフィック。
- マルチプロトコル ラベル スイッチング（MPLS）ラベル付きパケットNBAR は IP パケットのみを分類します。ただし、トラフィックが MPLS に渡される前に、NBAR を使用して IP トラフィックを分類することができます。NBAR で分類したパケットで、モジュラ QoS CLI（MQC）を使用して IP Diffserv コード ポイント（DSCP）フィールドを設定します。これによって、MPLS が MPLS ヘッダー内の MPLS Experimental（EXP）設定に DSCP 設定をマッピングできるようにします。
- NBAR の処理。設計上、NBAR の処理は In-Service Software Upgrade（ISSU）の際に一時的に無効化されます。次の syslog メッセージは、ISSU が完了した後の NBAR 分類の再起動を示します。「%NBAR_HA-5-NBAR_INFO: NBAR sync DONE!」
- マルチキャスト パケット分類
- ステートフル プロトコルによる非対称フロー。
- NBAR を実行するデバイスから送信されるか、そのデバイスに送信されるパケット。

（注） NBAR のコンテキストでは、非対称フローとは、ロード バランシングの実装や、パケットが異なるルータを経由して異なる方向に流れる非対称ルーティングなどの理由により、異なるパケットが異なるデバイスを経由するフローのことです。

NBAR は次の論理インターフェイスでサポートされません。

- ダイヤラ インターフェイス
- ダイナミック仮想トンネル インターフェイス（DVTI）などのダイナミック トンネル

- Fast EtherChannel
- デバイスで終端する IPv6 トンネル
- MPLS
- オーバーレイ トランスポート仮想化（OTV）オーバーレイ インターフェイス

（注） いくつかのリンクで NBAR によるカプセル化がサポートされていない場合、デバイスの他のインターフェイスにNBARを適用し、入力の分類を実行することができます。たとえば、LAN インターフェイスで NBAR を設定し、WAN リンクの出力トラフィックを分類することができます。

次の仮想インターフェイスは、Cisco IOS イメージによってはサポートされています。

- 総称ルーティング カプセル化（GRE）
- Protocol Discovery モードおよび MQC モードでの IPsec IPv4 トンネル（トンネリングされた IPv6 を含む）
- Protocol Discovery モードでの IPSec IPv6 トンネル（MQC モードではサポートされません）
- Protocol Discovery モードでのマルチポイント GRE/Dynamic マルチポイント VPN（DMVPN）

（注） NBARがトンネリングされたインターフェイスで有効化されている場合、NBARはより多くの CPU パワーを必要とします。

Protocol Discoveryがトンネル インターフェイスと、トンネル インターフェイスが設定された物理インターフェイスの両方で有効化されている場合、トンネル インターフェイスに指定されたパケットは両方のインターフェイスでカウントされます。物理インターフェイスでは、パケットはカプセル化に基づいて分類され、カウントされます。トンネル インターフェイスでは、パケットはレイヤ 7 プロトコルに基づいて分類され、カウントされます。

すべてのプロトコルに対して、プロトコルごとにサブ分類の20の組み合わせのみを設定することができます。**match protocol** *protocol-name variable-field-name value* コマンドを使用して、サブ分類の組み合わせを定義することができます。

NBAR を使用したネットワーク トラフィックの分類に関する情報

NBAR の機能

NBAR は、多様なプロトコルとアプリケーションを認識および分類する分類エンジンです。たとえば、ダイナミック TCP/UDP ポート割り当てを使用する Web ベースや他の分類が困難なアプリケーションとプロトコルなどです。

プロトコルまたはアプリケーションが NBAR に認識および分類されると、そのアプリケーションまたはそのプロトコルによるトラフィックに適した QoS を適用するようにネットワークを設定できるようになります。QoS は、MQC を使用して適用されます。

（注） MQC の詳細については、「MQC を使用した QoS 機能の適用」モジュールを参照してください。

NBAR は、レイヤ 4 ～レイヤ 7 のアプリケーションとプロトコルを識別する分類機能をいくつか導入しています。これらの分類機能は、次のとおりです。

- スタティックに割り当てられた TCP および UDP ポート番号。
- 非 TCP および非 UDP IP プロトコル。
- ダイナミックに割り当てられた TCP および UDP ポート番号。このような分類にはステートフルインスペクションが必要です。つまり、パケット分類時に複数パケットにわたるプロトコルを検査する機能です。
- サブポートの分類またはディープパケットインスペクションに基づく分類（つまり、パケットを検査するための分類）。

（注） アクセス コントロール リスト（ACL）は、スタティック ポート プロトコルの分類にも使用できます。ただし、NBAR は設定が容易で、ACL の使用時には利用できない分類の統計情報を提供できます。

NBAR には Protocol Discovery 機能があり、インターフェイス上で動作しているアプリケーションプロトコルを簡単に検出できます。Protocol Discovery の詳細については、「Protocol Discovery のイネーブル化」モジュールを参照してください。

（注） NBARはアプリケーション別またはプロトコル別にネットワーク トラフィックを分類します。ただし、ネットワーク トラフィックはNBAR を使用しなくても分類できます。NBAR を使用せずにネットワークを分類する方法については、「ネットワーク トラフィックの分類」モジュールを参照してください。

NBAR には、プロトコルをロードする簡単な方法を提供し、NBAR がネットワーク トラフィックを分類するために追加のプロトコルを認識できるようにするプロトコル パック機能が組み込まれています。プロトコル パックは、一緒に開発され、パックされたプロトコルのセットです。デバイスに新しいプロトコル パックをロードすることにより、デバイス上にすでに存在しているデフォルトの IOS プロトコル パックを置き換えることができます。

NBAR の利点

ネットワーク トラフィックの識別と分類は、QoS を実装するうえで重要な最初のステップです。ネットワーク管理者は、ネットワーク上で動作しているアプリケーションとプロトコルの数とタイプを識別してからの方が、より効率的にネットワーキング環境に QoS を実装できます。

NBAR を使用すれば、ネットワーク管理者は、さまざまなタイプのプロトコルと、各プロトコルによって生成されるトラフィックの量を確認できます。NBAR がこの情報を収集したら、ユーザはトラフィックをクラスに整理することができます。これらのクラスを使用して、さまざまなレベルのサービスをネットワーク トラフィックに提供できます。その結果、ネットワーク トラフィックに対して適切なレベルのネットワーク リソースが提供され、ネットワーク管理を改善できます。

NBAR は、Cisco Application Visibility and Control（AVC）でも使用されます。AVC を使用して、NBAR は、より適切な QoS とポリシングを通してアプリケーション パフォーマンスを向上させ、使用されているネットワークに関する可視性を高めます。

AVC ライセンスを使用すると、次の NBAR 機能がサポートされます。

- 一時的な IPv6 トンネル内部の分類
- カスタム プロトコル
- プロトコル属性のカスタマイズ
- フィールド抽出
- プロトコル パックの更新

NBAR と HTTP トラフィックの分類

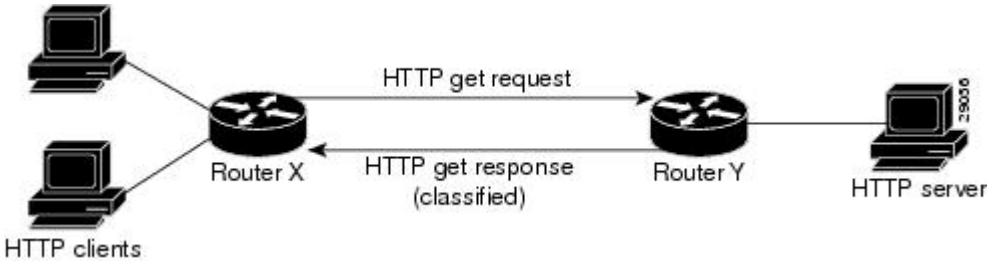
URL、ホスト、または MIME による HTTP トラフィックの分類

NBAR は、パケットの TCP/UDP ポート番号以外の部分を確認することでアプリケーション トラフィックを分類できます。これはサブポート分類と呼ばれます。NBAR は、TCP/UDP ペイロード自体を検査して、その内容（トランザクション識別子、メッセージ タイプ、その他の同様のデータなど）に基づいてパケットを分類します。

URL、ホスト、または Multipurpose Internet Mail Extension（MIME）タイプによる HTTP トラフィックの分類は、サブポート分類の一例です。NBAR は、正規表現照合を使用して、要求の URL またはホスト フィールド内のテキストによって HTTP トラフィックを分類します。NBAR での HTTP クライアント要求のマッチングは、GET、PUT、HEAD、POST、DELETE、OPTIONS、CONNECT、および TRACE など、ほとんどの HTTP 要求方式をサポートします。NBAR エンジンは、指定した一致文字列を正規表現に変換します。

下の図に、デバイス Y が NBAR 対応デバイスである NBAR を含むネットワーク トポロジを示します。

図 *1*：*NBAR* 対応デバイスを含むネットワーク トポロジ



分類する URL を指定する場合は、**match** ステートメントに www.*hostname.domain* に続く URL の部分のみを含めます。たとえば、www.cisco.com/latest/whatsnew.html という URL の場合、**match** ステートメントに /latest/whatsnew.html のみを含めます（例：**matchprotocolhttpurl/latest/whatsnew.html**）。

ホスト指定は URL 指定と同じです。NBAR は、HTTP パケット内のホスト フィールド コンテンツで正規表現一致を実行し、そのホストからのすべてのパケットを分類します。たとえば、www.cisco.com/latest/whatsnew.html という URL の場合、www.cisco.com のみを含めます。

MIME タイプ マッチングの場合、MIME タイプには、ユーザが指定したテキスト文字列を含めることができます。Internet Assigned Numbers Authority（IANA）がサポートする MIME タイプの一覧については、次の URL を参照してください。

http://www.iana.org/assignments/media-types/

MIME タイプでマッチングすると、次の HTTP トランザクションまで、NBAR は MIME タイプとすべての後続パケットを含むパケットのマッチングを実行します。

永続 HTTP がある場合、NBAR は URL とホスト分類をサポートします。NBAR は、パイプライン処理された要求に含まれるパケットを分類しません。パイプライン処理された要求の場合、前の要求にサービスが提供される前に、複数の要求がサーバにパイプラインで送信されます。パイプライン処理された要求は、下位分類と、トランスポート プロトコルとして HTTP を使用するトンネル化プロトコルではサポートされません。

HTTP トラフィックの NBAR 拡張検査機能を使用すると、NBAR は不明な TCP ポートをスキャンし、それらのポートを通過する HTTP トラフィックを識別することができます。HTTP トラフィックの分類は既知で定義済みの TCP ポートに限定されなくなりました。

リリースによっては、常時接続の HTTP トランザクションでの NBAR URI 抽出の有効化機能が、以前のリリースでサポートされていたように最初のトランザクションのURLだけでなく、トランザクションごとの URL フィールドの抽出とエクスポートをサポートします。複数のトランザクションを有効にするには、「拡張 Web 分類」を含むプロトコル パックをインストールする必要があります。拡張 Web 分類プロトコル パックをインストールすると、Flexible NetFlow 内の **match connection transaction-id** コマンド設定が複数の HTTP トランザクションを追跡します。HTTP トランザクションの追跡の詳細については、『*Cisco IOS Flexible NetFlow Configuration Guide*』を参照してください。

（注） NBAR は、トランザクションごとの分類とエクスポート用の重要な追加のタスクを実行します。これらのタスクは、パフォーマンスに影響を与えるため、エクスポート レートが上昇する可能性があります。

HTTP ヘッダー フィールドを使用した HTTP トラフィックの分類

NBAR では、HTTP ヘッダー フィールド内の情報を使用して HTTP トラフィックを分類できる拡張機能が導入されています。

HTTP はクライアント/サーバ モデルを使用して動作します。HTTP クライアントは、HTTP サーバに要求メッセージを送信することで接続を開きます。HTTP サーバは HTTP クライアントに対して応答メッセージを返します（通常、この応答メッセージは、HTTP クライアントからの要求メッセージで要求されたリソースです）。HTTP サーバは応答の送信後に接続を閉じ、トランザクションは完了します。

HTTP ヘッダー フィールドは、HTTP 要求メッセージと応答メッセージに関する情報を提供するために使用されます。HTTP には多数のヘッダー フィールドがあります。HTTP ヘッダーの詳細については、RFC 2616『*Hypertext Transfer Protocol-HTTP/1.1*』のセクション 14 を参照してください。この RFC は次の URL で入手できます。

http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html

NBAR は次の HTTP ヘッダーフィールドを分類できます。

- （クライアントからサーバへの）要求メッセージの場合、NBAR を使用して次の HTTP ヘッダー フィールドを識別できます。
  - User-Agent
  - Referrer

- From

- （サーバからクライアントへの）応答メッセージの場合、NBAR を使用して次の HTTP ヘッダー フィールドを識別できます。
  - Server
  - Location
  - Content-Base
  - Content-Encoding

NBAR 内では、**matchprotocolhttpc-header-field** コマンドは、NBAR 識別要求メッセージを指定するために使用されます（コマンドの **c-header-field** 部分の「c」はクライアントを示しています）。**matchprotocolhttps-header-field** コマンドは、応答メッセージを指定するために使用されます（コマンドの **s-header-field** 部分の「s」はサーバを示しています）。

（注） **matchprotocolhttp** コマンド内の **c-header-field** キーワード、**s-header-field** キーワード、および関連引数は使用できなくなりました。同じ機能は、個別のキーワードと引数を使用して実行できます。詳細については、『*Quality of Service Solutions Command Reference*』の **matchprotocolhttp** コマンドの構文を参照してください。

（注） c-header-field は、user-agent、referrer、または from-header フィールドの値に含まれる単一値に基づいて下位分類を実行します。s-header-field は、server、location、content-encoding、または content-base ヘッダー フィールドの値に含まれる単一値に基づいて下位分類を実行します。これらのヘッダー フィールド値に相関関係はありません。そのため、c-header フィールドと s-header フィールドは、HTTP 下位分類の目的とニーズに基づいて、user-agent、referrer、from、server、content-base、content-encoding、および location パラメータで置き換えられます。

HTTP ヘッダーと URL、ホスト、または MIME タイプの分類の組み合わせによる HTTP トラフィックの特定

URL、Host、MIME タイプ、および HTTP ヘッダーの組み合わせは、NBAR 設定時に使用できます。この組み合わせによって、ネットワーク要件に基づく特定の HTTP トラフィックの分類がさらに柔軟になります。

NBAR と Citrix ICA トラフィックの分類

NBAR は、Citrix Independent Computing Architecture（ICA）トラフィックを分類し、Citrix トラフィックのサブポート分類を実行できます。分類には、発行済みアプリケーション名または ICA タグ番号が使用されます。

発行済みアプリケーション名による Citrix ICA トラフィックの分類

NBAR は、Citrix ICA Master ブラウザ宛ての発行済みアプリケーションに対する Citrix ICA クライアント要求をモニタできます。クライアントが発行済みアプリケーションを要求した後、Citrix ICA マスター ブラウザは空きメモリが最も多いサーバにクライアントを転送します。Citrix ICA クライアントは、アプリケーションの接続をその Citrix ICA サーバに接続します。

（注） Citrix でトラフィックをモニタして発行済みアプリケーション名で分類するには、マスター ブラウザで Server Browser モードを使用します。

Server Browser モードでは、NBAR がトラフィックをステートフルに追跡およびモニタし、**matchprotocolcitrix** コマンドで指定された発行済みアプリケーション名の正規表現検索をパケット コンテンツに対して実行します。発行済みアプリケーション名は、**matchprotocolcitrix** コマンドの **app** キーワードと *application-name-string* 引数を使用して指定します。**matchprotocolcitrix** コマンドの詳細については、『Quality of Service Solutions Command Reference』を参照してください。

指定したアプリケーションを伝送するためにトリガーされた Citrix ICA セッションはキャッシュされ、トラフィックは発行済みアプリケーション名によって適切に分類されます。

Citrix ICA クライアント モード

Citrix ICA クライアントは多様なモードで設定できます。NBAR は、操作のすべてのモードで Citrix アプリケーションを区別できる訳ではありません。そのため、ネットワーク管理者は Citrix 管理者と協力して、NBAR が Citrix トラフィックを適切に分類できるようにする必要があります。

Citrix 管理者は、Citrix アプリケーションを個別にまたは Published Desktop モードで発行するように Citrix を設定できます。Published Desktop モードの動作では、クライアントの発行済みデスクトップ内のすべてのアプリケーションが同じ TCP セッションを使用します。そのため、アプリケーションの区別は不可能であり、NBAR では（ポート 1494 を確認して）集約としてのみ Citrix アプリケーションを分類できます。

NBAR の使用時は、Citrix ICA クライアントに Published Application モードを使用することを推奨します。Published Application モードでは、Citrix 管理者が Citrix クライアントをシームレス モードと非シームレス（ウィンドウ）モードのどちらかの動作で設定できます。非シームレス モードでは、各 Citrix アプリケーションが個別の TCP 接続を使用するため、NBAR は発行済みアプリケーションの名前に基づいてアプリケーションを区別するために使用できます。

シームレス モード クライアントは、セッション共有または非セッション共有という 2 つのサブモードのいずれかで動作します。シームレス セッション共有モードでは、すべてのクライアントが同じ TCP 接続を共有するため、NBAR はアプリケーションを区別できません。シームレス共有モードは、一部のソフトウェア リリースでデフォルトで有効になります。シームレス非セッション共有モードでは、各クライアントの各アプリケーションが個別の TCP 接続を使用します。シームレス非セッション共有モードの場合、NBAR はアプリケーションを区別できます。

（注） Citrix ICA セキュア モードでは NBAR は適切に動作します。パイプライン処理された Citrix ICA クライアント要求はサポートされません。

ICA タグ番号による Citrix ICA トラフィックの分類

アプリケーションが開かれるたびに、Citrix は TCP セッションを 1 つずつ使用します。TCP セッションでは、同じセッションに多様な Citrix トラフィックが混在している可能性があります。たとえば、印刷トラフィックとインタラクティブ トラフィックが混在し、特定のアプリケーションで中断や遅延が発生する可能性があります。

多くのユーザは、印刷がバックグラウンド プロセスで処理され、高い優先度のトラフィックの処理を妨げないことを望みます。この印刷の優先度に対応するために、Citrix ICA プロトコルは、パケットの ICA タグ番号に基づいて Citrix ICA トラフィックを識別する機能を備えています。Citrix ICA トラフィックの識別、タグ付け、および優先順位付けの機能は、ICA Priority Packet Tagging と呼ばれます。ICA Priority Packet Tagging を使用すると、Citrix ICA トラフィックは、パケットの ICA タグによって high、medium、low、および background に分類されます。

ICA トラフィックの priority タグ番号を使用し、トラフィックの優先順位を決定すると、QoS 機能を実装してトラフィックの処理方法を決定できます。たとえば、QoS トラフィック ポリシングを設定して、特定の優先順位でパケットを送信またはドロップできます。

Citrix ICA Packet Tagging

Citrix クライアントとサーバ間の最初のネゴシエーションが完了した後に、Citrix ICA タグが Citrix ICA パケットの先頭の 2 バイトに追加されます。

パケットの先頭 2 バイト（バイト 1 およびバイト 2）には、バイト カウントと ICA priority タグ番号が含まれます。バイト 1 には下位バイト カウントが含まれ、バイト 2 の先頭 2 ビットには priority タグが含まれます。その他の 6 ビットには、上位バイト カウントが含まれます。

ICA priority タグ値には、0 ～ 3 の数を指定できます。数値はパケットの優先順位を示し、0 が最も高い優先順位で、3 が最も低い優先順位です。

パケットの ICA タグ番号によって Citrix トラフィックに優先順位を付けるには、**matchprotocolcitrix** コマンドの **ica-tag** キーワードと *ica-tag-value* 引数を使用してタグ番号を指定する必要があります。**matchprotocolcitrix** コマンドの詳細については、『Quality of Service Solutions Command Reference』を参照してください。

次の表に、さまざまな Citrix トラフィックとそれぞれのプライオリティ タグに関する情報を示します。

表 *1*：*Citrix ICA Packet Tagging*

プライオリティ	ICA ビット（10 進数）	仮想チャネルの例
High	0	ビデオ、マウス、およびキーボード画面の更新

プライオリティ	ICA ビット（10 進数）	仮想チャネルの例
Medium	1	プログラム ネイバーフッド、クリップボード、音声マッピング、およびライセンス管理
Low	2	クライアント共通機器（COM）ポート マッピングとクライアント ドライブ マッピング
Background	3	自動クライアント更新、クライアント プリンタ マッピング、および相手先商標製造会社（OEM）チャネル

NBAR と RTP ペイロード タイプの分類

Real-time Transport Protocol（RTP）は、マルチメディア データ ストリームのパケット形式です。メディアオンデマンドやインタラクティブ サービス（インターネットテレフォニーなど）に使用できます。RTP はデータ部分とコントロール部分で構成されます。コントロール部分は Real-Time Transport Control Protocol（RTCP）と呼ばれます。RTCP は NBAR がサポートする個別のプロトコルです。注意が必要なのは、NBAR RTP Payload Type Classification（RTP ペイロード タイプ分類）機能では RTCP パケットを識別しない点と、RTCP パケットは奇数ポートで実行され、RTP パケットは偶数ポートで実行される点です。

RTP のデータ部分はシン プロトコルであり、タイミングの再構築、損失の検出、セキュリティとコンテンツの識別を含む、連続媒体（オーディオやビデオ）などのアプリケーションのリアルタイム プロパティをサポートします。RTP は、RFC 1889（*ATransportProtocolforReal-TimeApplications*）と RFC 1890（*RTPProfileforAudioandVideoConferenceswithMinimalControl*）で規定されています。

RTP ペイロード タイプとは、パケットの中で RTP によって送信されるデータです。たとえば、オーディオ サンプルや圧縮されたビデオ データなどです。

NBAR RTP Payload Type Classification 機能を使用すると、リアルタイム オーディオ/ビデオ トラフィックをステートフルに識別できるだけではなく、オーディオコーデックとビデオコーデックに基づいて区別することで、より粒度の細かい QoS を提供することもできます。そのため、RTP Payload Type Classification 機能は、RTP ヘッダーに対するディープ パケット インスペクションを実行して RTP パケットを分類します。

NBAR を使用した RTP の分類の詳細については、NBAR RTP ペイロード分類を参照してください。

NBAR とカスタム プロトコルおよびアプリケーションの分類

NBAR では、カスタム プロトコルを使用してカスタム アプリケーションを識別できます。カスタム プロトコルは、スタティック ポートベースのプロトコルとアプリケーションをサポートしますが、現在のところ、NBAR はサポートしていません。カスタム プロトコルを作成することで、NBAR が認識するプロトコルおよびアプリケーション タイプのセットに追加できます。

カスタム プロトコルによって NBAR Protocol Discovery 機能を拡張し、追加のスタティック ポート アプリケーションを分類およびモニタできます。それによって、NBAR はサポートしていないスタティック ポート トラフィックを分類できるようになります。

カスタム プロトコルを定義したら、それらと NBAR Protocol Discovery および MQC を組み合わせて使用して、トラフィックを分類できます。

NBAR はカスタム プロトコルの使用をサポートし、カスタム プロトコルに静的な TCP ポート番号と UDP ポート番号をマップできます。

カスタム プロトコルには次の 2 種類があります。

- 事前定義のカスタム プロトコル
- ユーザ定義のカスタム プロトコル

NBAR には、事前定義のカスタム プロトコルとアプリケーションに関連する次のような特徴があります。

- カスタム プロトコルには、custom-xx（xx は数値）という名前を付ける必要があります。
- NBAR を使用して 10 のカスタム アプリケーションを割り当てることができ、各カスタム アプリケーションでは、最大 16 の TCP ポートと最大 16 の UDP ポートをそれぞれ個別のカスタム プロトコルにマップすることができます。各カスタム プロトコルのリアルタイム統計情報を Protocol Discovery を使用してモニタできます。
- カスタム プロトコルの作成時に変数を作成したら、**matchprotocol** コマンドを使用して、カスタム プロトコルの特定の値に基づいてトラフィックを分類できます。

NBAR には、ユーザ定義のカスタム プロトコルとアプリケーションに関連する次のような特徴があります。

- 特定のオフセットで特定のマッチング ストリング パターンについてペイロードを検査する機能。
- ユーザが自分のカスタム プロトコル アプリケーションの名前を定義できる機能。これにより、ユーザ指定のプロトコルを NBAR がサポートするプロトコルとして、Protocol Discovery、Protocol Discovery MIB、および **matchprotocol** コマンドで使用できるようになります。
- ユーザの希望によって、トラフィックの方向ごと（つまり、双方向のトラフィックではなく、発信元方向または宛先方向のトラフィック）に指定されたカスタムプロトコルを NBAR で検査する機能。

- CLI によって、カスタム アプリケーションを設定したユーザは、個々のポートではなくポートの範囲を指定できるようになります。
- **variable** キーワード、*field-name* 引数、および *field-length* 引数が **ipnbarcustom** コマンドに追加されました。
- カスタム ホストと URL 署名を追加可能にする **http** キーワード グループ。

この追加のキーワードおよび追加引数を使用すると、同じポート番号に基づいて複数のカスタム プロトコルを作成できます。

（注） ユーザ定義のカスタム プロトコルを定義すると NBAR 機能が再起動しますが、事前定義のカスタム プロトコルを定義しても NBAR 機能は再起動しません。

NBAR DNS ベースの分類

NBAR は、ユーザがアプリケーション サーバとの接続を開始したときに交換される DNS トランザクション情報を使用することにより、トラフィック分類を促進することができます。この方式には、フローの先頭パケットに基づいてフローを分類できるという大きなメリットがあります。

たとえば、ブラウザで Web ベースのアプリケーションを開くと、ブラウザはまず DNS サーバと通信してそのアプリケーションの関連サーバの IP アドレスを要求します。DNS トランザクションは要求と応答で構成されます。応答には、Web ベース アプリケーション用のサーバの IP アドレスが含まれています。

NBAR はこのトランザクションからの情報を使用して、Web ベースのアプリケーションと関連サーバの IP アドレスを正しく関連付けることができます。そうすれば、NBAR は、フローの先頭パケットから、その IP アドレスを含むトラフィックを特定できるようになります。

サポートされるプラットフォーム

この機能は、Cisco IOS XE リリース 3.17S 以降の IOS XE Denali 16.x を含む Cisco IOS XE が動作しているプラットフォームでサポートされます。

利点

NBAR は複数の方式をトラフィックの分類に適用します。これには、socket-cache のように先頭パケットに基づいてソケットを分類するものが含まれます。DNS ベースの分類機能は、他の NBAR 方式と連動してトラフィック分類を向上させます。この機能は、特に、非対称サーバ/クライアント間フローを含む特定のタイプのトラフィックだけでなく、何らかの方法で暗号化されたトラフィックにも役に立ちます。

他の NBAR 分類方式による補完

一般に、NBAR エンジンは、さまざまな戦略を駆使して、可能な限り最も粒度の細かいトラフィックの分類を提供します。先頭パケット分類は、DNS ベースの分類や socket-cache などの複数の方

式で採用されています。その他の分類方式の中には、分類の粒度をさらに細かくするものがあります。

制限事項

- DNS トランザクション情報による識別では不十分な場合があります。このような場合、NBAR は、可能な限り、他の方式を使用してトラフィックを分類します。たとえば、この方式は、汎用のホストやサービス集約でうまく機能しません（汎用のホストやサービス集約では、大量のサービスが単一サーバの IP アドレス経由でホストされていても、同じホスト名を使用する場合と、複数の異なるホスト名を使用する場合があります）。
- NBAR が一部のトラフィックの DNS トランザクション データにアクセスできない場合もあります。たとえば、ネットワーク トポロジに、NBAR によってモニタされていない接続を介してアクセスされるローカル DNS サーバが含まれている場合です。このような場合は、DNS ベースの分類が使用できません。

DNS ベースの分類の制限または無効化

DNS ベースの分類は無効にすることができます（DNS ベースの分類の有効化と無効化, （25 ページ）を参照）。

通常は、DNS Guard 機能をデフォルトの有効状態のままにすることをお勧めします。そうすれば、完全な DNS トランザクション（要求、応答）が利用可能な場合にのみ動作するように DNS ベースの分類を制限できます。ただし、特殊なケースでは、この機能を無効にすることができます（DNS ベースの分類のための DNS ガードの有効化と無効化, （26 ページ）を参照）。

関連機能

NBAR には、DNS ベースの分類機能に加え、場合によってはトラフィックの先頭パケット分類を提供できる機能も備わっています

カスタマイズされたサーバ指定：この機能は、NBAR をサポートするすべてのプラットフォームで動作します。これには、DNS ベースの分類方式をサポートしないものも含まれます。この機能は、DNS トランザクション方式よりも限定的です。カスタマイズされたサーバ指定では、DNS トランザクション情報を使用して識別する特定のドメインをユーザが設定する必要があります。

カスタマイズされたサーバ指定は、指定されたドメインの他の NBAR 分類方式より優先的に使用されるため、どうしても必要な場合以外は使用しないでください。設定コマンドを含むこの機能の詳細については、「DNS 名に基づく NBAR カスタム アプリケーション」を参照してください。

NBAR とダイナミック PDLMs を使用した分類

ダイナミック Packet Description Language Modules（PDLMs）を使用すれば、特定のシスコ リリースへのアップグレードやデバイスのリロードをすることなく、NBAR に対する新しいプロトコルのサポートや、既存のプロトコル サポートの機能強化ができます。サポートが NBAR に対するプロトコルの機能強化に関するものの場合は、PDLMs のモジュール バージョンを既存のバージョンより新しくする必要があります。今後のシスコ リリースに、これらの新しいプロトコルのサポートが組み込まれます。

（注） ASR 1006 冗長ハードウェア セットアップを使用している場合は、PDLMs を両方のルート プロセッサ（RP）上でロードする必要があります。

ダイナミック PDLMs は、プラットフォーム固有で、ソフトウェア ファミリ識別子（SFI）が組み込まれています。他のプラットフォームのダイナミック PDLMs は、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータではロードできません。

NBAR がサポートするプロトコル

matchprotocol（NBAR）コマンドは、NBAR でサポートされるプロトコルに基づいてトラフィックを分類するために使用されます。NBAR は、次のタイプのプロトコルを分類できます。

- 非 UDP および非 TCP IP プロトコル
- スタティックに割り当てられたポート番号を使用する TCP および UDP プロトコル
- スタティックに割り当てられたポート番号を使用し、さらにステートフルインスペクションを必須とする TCP および UDP プロトコル
- ダイナミックに割り当てられたポート番号を使用するため、ステートフルインスペクションを必須とする TCP および UDP プロトコル

プロトコル パックでサポートされるプロトコルのリストを表示するには、『NBAR Protocol Library』を参照してください。

NBAR プロトコル パック

NBAR プロトコル パックは、デバイス上にすでに存在しているベース IOS イメージを置き換えることなく NBAR でサポートされるプロトコルを更新するための簡単な方法を提供します。プロトコル パックは、一緒に開発され、パックされたプロトコルのセットです。NBAR プロトコル パックのロード方法については、『QoS：NBAR コンフィギュレーション ガイド』を参照してください。プロトコル パックでサポートされるプロトコルのリストを表示するには、『NBAR Protocol Library』を参照してください。

NBAR とピアツーピア ファイル共有アプリケーションの分類

次のアプリケーションは、NBAR でサポートされる最も一般的なピアツーピア ファイル共有アプリケーションです。

- BitTorrent
- DirectConnect
- eDonkey
- eMule

- FastTrack
- KazaA（および KazaA Lite と KazaA Lite Resurrection）
- Win MX
- POCO

DirectConnect プロトコルと eDonkey P2P プロトコルは、リリースに応じて次の下位分類をサポートします。

- eDonkey は、次の下位分類オプションをサポートします。
  - ファイル転送
  - 検索ファイル名
  - テキスト チャット
- KazaA、FastTrack、および Gnuetella は、ファイル転送下位分類をサポートします。

Gnutella ファイル共有は、Cisco IOS XE リリース 2.5 で NBAR を使用して分類可能になりました。

Gnutella プロトコルを使用するアプリケーションは、Bearshare、Gnewtellium、Gnucleus、Gtk-Gnutella、Limewire、Mutella、Phex、Qtella、Swapper、および Xolo です。Gnutella プロトコルを使用するアプリケーションからのトラフィックは、それぞれのアプリケーションとしてではなく、Gnutella として分類されます。

NBAR 多段階分類

NBAR は、URL、ホストと MIME タイプによる HTTP 分類や、FTP、TFTP などのようなステートフルなネットワーク プロトコルを多数サポートします。NBAR は、アクセス コントロール リスト（ACL）を使用して分類可能なプロトコルなどのスタティック ポート プロトコルを分類します。

多段階分類は、未知の分類の代わりに、一時的な分類として基礎となるプロトコルをレポートします。たとえば、以前のリリースでは、HTTP 応答パケットで署名が検出される Video-over-HTTP などのケースをサポートするために、HTTP 経由の再帰分類で HTTP フローの先頭パケットを未知としてレポートできました。これは、以下の影響を与えます。

- Protocol Discovery：分類の低下。
- パケットベースの Flexible NetFlow（FNF）：分類の低下。
- QoS：分類の遅延。
- パフォーマンス：より多くのパケットが処理されるため。
- 分類プロセスの途中のエージングした短いフローは、分類結果を出力せずに停止しますが、部分的に分類されました。

NBAR 多段階分類以前は、NBAR が、最終分類決定に至るまでは未知の分類結果をレポートしました。NBAR 多段階分類は、最新の分類決定を返します。この分類は、メディア パーティション分割（MP）再帰分類パスから基礎となるプロトコルを公開するようにデータ パスを変更します。最終分類が使用可能になるまで「未知」を返し続ける代わりに、その時点の（一時的な）分類決定を返します。

NBAR 多段階分類には次のような特長があります。

下位非互換性

システムに AOL Instant Messenger（AIM）と BitTorrent の基礎となるプロトコルである SOCKet Secure（SOCKS）などのプロトコルを照合するポリシーが設定されている場合は、他のすべてのプロトコルが失敗したとき（Protocol Discovery、FNF、および Modular QoS CLI（MQC）のいずれかを経由して他のプロトコルも有効になっている場合）に、このポリシーが AIM または BitTorrent フローの先頭パケットを SOCKS として照合します。多段階分類では、基礎となるプロトコルをブロックしながら、それ以外のプロトコルを許可することはできません。

トラフィックの並べ替え

トラフィック フローの分類ごとに異なる優先順位が設定されている場合は、フローが別々の出力キューに転送されます。多段階分類では、単一のトラフィック フローに対して複数の分類決定が下される場合があります。トラフィックが優先順位付けされた分類に基づく場合は、基礎となるプロトコルを優先することをお勧めします（たとえば、HTTP は Video-over-HTTP より優先されます）。

Performance Routing（PfR）

PfR は、NBAR からの分類をチェックしてルーティング決定を下すときに、それが最終分類かどうかを考慮します。それが最終分類ではない場合、ルーティング決定は行われません。そのようにすると、トラフィック フローが複数のパスに分断され、「未知の」分類が発生する可能性があるためです。

NBAR クライアントがユーザに分類が途中かどうかを伝達します。

NBAR の拡張性

インターフェイス拡張性

リリースによって、Protocol Discovery を有効にできるインターフェイスの数に制限はありません。

次の表に、Protocol Discovery でサポートされるインターフェイスとリリース番号の詳細を示します。

表 *2*：リリースと *Protocol Discovery* インターフェイスのサポート

リリース	**Protocol Discovery** でサポートされるインターフェイスの数
Cisco IOS XE リリース 2.5	128
Cisco IOS XE リリース 2.6	256

リリース	Protocol Discovery でサポートされるインターフェイスの数
Cisco IOS XE リリース 2.7	32
Cisco IOS XE リリース 3.2S 以降のリリース	32

フロー拡張性

双方向フローの数とサポートされているプラットフォームの数はすべてのリリースで同じです。クイック エージングに基づいてアクティブ フローの数を削減する方式が使用できます。

クイック エージングは、次の条件下で発生します。

- TCP フローが確立状態に到達しない。
- パケット数が 5 未満の UDP フローが、指定されたクイック エージング タイムアウト以内に分類されない。
- フローが、指定されたクイック エージング タイムアウト以内に分類されない。

クイック エージング方式は、NBAR の動作に必要なフローの数をネットワーク動作に応じて 3 倍以上削減します。

シスコ クラウド サービス ルータ 1000V シリーズ デバイスは、フロー拡張性に関して ESP5 と同じ動作を示します。

フロー テーブルのサイジング

ip nbar resources flow max-sessions コマンドは、フロー テーブルで許可されるデフォルトの最大フロー セッション数をオーバーライドするオプションを提供します。NBAR 機能を備えたデバイスのパフォーマンスは、フローテーブルに設定されたメモリ サイズとフロー数によって異なります。フロー数を変更可能にする柔軟性があるので、デバイスのキャパシティに応じてシステムのパフォーマンスを向上できます。NBAR フロー統計情報を確認するには、**show ip nbar resources flow** コマンドを使用します。

次の表に、プラットフォームの詳細とフロー サイズの制限を示します。

表 *3*：プラットフォームとフロー サイズの詳細

プラットフォーム	フローの最大数	フローのデフォルト数	メモリの上限（プラットフォーム メモリの 70 %）
ESP5/ASR1001/CSR	750,000	500,000	179 MB
ESP10	1,650,000	1,000,000	358 MB
ESP20/ESP40/ASR1002-X	3,500,000	1,000,000	716 MB

プラットフォーム	フローの最大数	フローのデフォルト数	メモリの上限（プラットフォーム メモリの 70 %）
ESP100	10,000,000	3,000,000	2.1 GB

メモリへの影響を軽減するためのフローの推奨数は 50,000 であり、このような設定で十分です。

（注） システム全体のメモリ使用率が 90 % に達すると、フロー エントリの総数は増えなくなります。

NBAR Protocol Discovery

NBAR には、Protocol Discovery という機能が含まれます。Protocol Discovery は、インターフェイスを通過するプロトコル パケットを検出するための簡単な方法を提供します。Protocol Discovery の詳細については、「Protocol Discovery のイネーブル化」モジュールを参照してください。

NBAR Protocol Discovery MIB

NBAR Protocol Discovery MIB は、Simple Network Management Protocol（SNMP）による次の新機能を提供することで、NBAR Protocol Discovery の機能を拡張します。

- インターフェイスごとの Protocol Discovery 機能をイネーブルまたはディセーブルにします。
- Protocol Discovery の統計情報を表示します。
- 帯域幅の使用状況別にプロトコルを一覧表示する複数の top-n テーブルを設定および表示します。
- しきい値を超えたときに違反についてレポートし、通知を送信する特定の NBAR 対応プロトコルまたはアプリケーションのトラフィックに基づいて、しきい値を設定します。

NBAR Protocol Discovery MIB の詳細については、「Network-Based Application Recognition Protocol Discovery Management Information Base」モジュールを参照してください。

NBAR とマルチパケットの分類

リリースに応じて、NBAR は、大量のマルチパケット署名を同時に検索する機能を提供します。この新しいテクニックは、さまざまな新しいプロトコルに対してサポートされます。また、このテクニックは、他のプロトコルのパフォーマンスや正確さを向上させます。新しい署名に対するサポートに伴って、マルチパケット分類機能は次のように NBAR の動作を変更します。

1. NBAR 分類では、プロトコルに応じて 1 つのフロー内に 1 ～ 15 のペイロード パケットが必要です。再送信されたパケットはこの計算にカウントされません。

2. NBAR は、ペイロード パケットを含まないフローを分類することも、分類用のペイロード パケットが 15 個存在していてもシーケンス番号が間違っている TCP ペイロード パケットを分類することもありません。
3. TCP 再送信パケットは、マルチパケット エンジン モジュールでは分類に対して有効なパケットとしてカウントされません。このようなタイプのパケットは、十分な数の有効なパケット ペイロードが蓄積されるまで、分類を遅らせる可能性があります。
4. NBAR では、静的署名しか存在しないペイロード パケットは、シングルパケット プロトコルとマルチパケット プロトコルが処理され、失敗した後で分類されます。そのため、最大 15 のパケット ペイロードが、最後の（静的な）分類決定が下されるまで、未知として分類される可能性があります。
5. 上記の制限があるので、カスタムプロトコルを使用することにより先頭パケットの分類を強制し、ポートベースの分類でのペイロードや正しいシーケンス番号の存在を無視させることができます。

VRF インターフェイス上の NBAR

リリースに応じて、VRF インターフェイス上の NBAR IPv4 および IPv6 分類がサポートされます。

（注） VRF インターフェイス上で NBAR が有効になっている場合、「app」下位分類を使用した Citrix プロトコルの分類は VRF インターフェイス上で保証されません。

NBAR と IPv6

リリースに応じて、次のタイプの分類がサポートされます。

- NBAR は、IPv6 パケット用のスタティック ポートベースの分類と IP プロトコル ベースの分類を提供します。
- NBAR は、MQC モードではなく、Protocol Discovery モードで IPv6 分類をサポートします。
- NBAR は、必ず、固定 IPv6 ヘッダー内のネクスト ヘッダー フィールドを読み取って、IPv6 パケットのペイロードで使用されるトランスポート層プロトコルを決定します。IPv6 パケットに 1 つ以上の拡張ヘッダーが含まれている場合、NBAR は最後の IPv6 拡張ヘッダーにスキップし、実際のプロトコルタイプを読み取りません。代わりに、NBAR はそのパケットを IPv6 拡張ヘッダー パケットとして分類します。

IPv6 に対する NBAR のサポート

リリースに応じて、NBAR は次のタイプの分類をサポートします。

- ネイティブ IPv6 分類。

- IPv4 と Teredo 経由でトンネル化された IPv6 内部の IPv6 トラフィック フローの分類。
- Protocol Discovery モードと MQC モードでの IPv6 分類。
- スタティックでステートフルな分類。
- IPv6 上で NBAR ベースのフィールドを使用した Flexible NetFlow。

NBAR は、IPv6 in IPv4（6-to-4、6rd、および ISATAP）と Teredo トンネル分類をサポートします。**ip nbar classification tunneled-traffic** コマンドは、トンネル トラフィック分類を有効にするために使用されます。トンネル トラフィック分類が有効になっている場合は、NBAR が IPv4 トラフィック内で伝送される IPv6 パケットのアプリケーション分類を実行します。**ip nbar classification tunneled-traffic** コマンドが無効になっている場合は、トンネル IPv6 パケットが IPv4 パケットとして処理されます。

NBAR は、IPv6 フィールドのキャプチャをサポートし、IPv6 トラフィック ベースのフロー モニタの作成を可能にします。**ipv6 flow monitor** コマンドを有効にすると、モニタがインターフェイスにバインドされ、NBAR 分類が IPv6 トラフィック タイプに適用され、Flexible NetFlow が IPv6 トラフィック フロー内のアプリケーション ID をキャプチャします。

GETVPN に対する NBAR のサポート

NBAR は Group Encrypted Transport VPN（GETVPN）をサポートします。入力 QoS が暗号マップ モードになっている場合は、入力 QoS が暗号化されたトラフィックに対して動作します。

後方互換モードに戻すには、グローバル コンフィギュレーション モードで **ip nbar disable classification encrypted-app** コマンドを使用します。

（注） GETVPN は現在 AVC と FNF でサポートされません。

CAPWAP に対する NBAR のサポート

CAPWAP（Control And Provisioning of Wireless Access Points）は、ワイヤレス トラフィック内で使用されるプロトコルで、アプリケーション トラフィックにポイントツーポイント カプセル化（トンネル）を提供します。CAPWAP トラフィックにはデータと制御の 2 つのタイプがあります。

NBAR は、CAPWAP トンネル内のアプリケーション トラフィックの NBAR 分類を可能にする CAPWAP 認識モードを提供します。

分類動作：CAPWAP 認識無効/有効

CAPWAP 認識モードはデフォルトでは無効です。すべての CAPWAP トラフィックが、トンネル内のアプリケーション トラフィックの詳細なしに「capwap-data」または「capwap-control」として報告されます。

CAPWAP 認識が有効になっている場合：

- CAPWAP 制御トラフィック：NBAR は「capwap-control」として報告します。
- CAPWAP データ トラフィック：NBAR はトンネル内の特定のアプリケーション トラフィックに関して報告します。

CAPWAP トラフィック タイプ	NBAR CAPWAP 認識有効	NBAR CAPWAP 認識無効
制御トラフィック	NBAR はトラフィックを「capwap-control」として報告します。	NBAR はトラフィックを「capwap-control」として報告します。
データ トラフィック	NBAR は CAPWAP トンネル内のアプリケーション トラフィックを報告します。	NBAR はトラフィックを「capwap-data」として報告します。

要件

CAPWAP トンネル内のアプリケーション トラフィックの NBAR 認識には以下が必要です。

- Cisco IOS XE プラットフォーム
- Cisco IOS XE 3.17 以降
- プラットフォーム上で NBAR が有効になっていること

使用法

CAPWAP 機能はデフォルトでは無効です。この機能を有効にするには、ip nbar classification tunneled-traffic capwap CLI を使用します。無効にするには、no ip nbar classification tunneled-traffic capwap を使用します。

```
device# config terminal
device(config)# ip nbar classification tunneled-traffic capwap
```

NBAR の設定プロセス

NBAR は次の 2 つの方法で設定できます。

- MQC を使用した NBAR の設定
- Protocol Discovery のイネーブル化

NBAR 設定の詳細については、『QoS：NBAR コンフィギュレーション ガイド』を参照してください。

NBAR の再起動

NBAR は、次の状況で再起動します。

- CLI を介したカスタム プロトコルの追加
- PDLM のロード
- RP スイッチオーバー
- FP スイッチオーバー
- プロトコル パックのインストール
- リンケージの変更

再起動には、NBAR を非アクティブ化し、再度アクティブ化することが含まれます。この間、すべてのパケットは NBAR により「未知」として分類されます。NBAR が再度アクティブ化されると、分類が有効化されます。

（注） Protocol Discovery の統計情報は、RP スイッチオーバーにより失われます。

DNS ベースの分類の設定方法

次の手順では、NBAR DNS ベースの分類の設定方法について説明します。これには、機能全体の有効化/無効化と DNS Guard の有効化/無効化が含まれます。

背景情報については、NBAR DNS ベースの分類, （15 ページ）を参照してください。

DNS ベースの分類の有効化と無効化

NBAR2 は DNS ベースの分類と呼ばれるトラフィック分析メカニズムを採用しており、DNS クエリ/応答トラフィックを分析することによって、アプリケーションのネットワーク アドレスを学習します。これにより NBAR は、フローの先頭パケット（「first in flow」（FIF）とも呼ばれる）からアプリケーショントラフィックを分類できます。DNS ベースの学習とも呼ばれるこのメカニズムは、シスコが提供する NBAR2 プロトコル パック内のプロトコルで記述されるアプリケーションに適用されます。

このメカニズムはデフォルトで有効になります。このメカニズムが原因でトラフィックの誤分類が生じた場合は、この機能の無効化が役立つことがあります。無効にするには、コマンドの **no** 形式を使用します。

手順の概要

1. **configureterminal**
2. [**no**] **ipnbarclassificationdnslearning**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**] **ipnbarclassificationdnslearning** 例： `Device(config)#no ip nbar classification dns learning`	DNS ベースの分類メカニズムを有効または無効にします。この例では、機能を無効にします。 デフォルト：enabled

DNS ベースの分類のための DNS ガードの有効化と無効化

DNS ベースの分類メカニズムは、アプリケーションのネットワーク アドレスを学習するために DNS 要求/応答トラフィックを分析します。正常に分析されたら、NBAR が、フロー内の先頭パケットからアプリケーション トラフィックを分類できます。機能はデフォルトで有効になりますが、誤分類を引き起こす可能性がある特異な状況においては、完全に無効にすることができます（DNS ベースの分類の有効化と無効化, （25 ページ）を参照してください）。

一般的な用途では、完全な DNS トランザクション（要求、応答）が使用可能な場合にのみ、トラフィックの誤分類を防ぐために、DNS ベースの分類を適用することをお勧めします。DNS ガード機能によって、この制御が有効になります。

- **Enabled**：DNS ベースの分類は、DNS 要求と応答の両方を分析できる場合にのみ機能します。
- **Disabled**：DNS ベースの分類に DNS 要求は必要なく、DNS 応答のみを使用して、アプリケーションのネットワーク アドレスを学習します。無効にするには、コマンドの **no** 形式を使用します。

このメカニズムはデフォルトで有効になります。

手順の概要

1. **configureterminal**
2. [**no**] **ipnbarclassificationdnslearningguard**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**] **ipnbarclassificationdnslearningguard** 例： `Device(config)#no ip nbar classification dns learning guard`	DNS ガードを有効または無効にします。この例では、機能を無効にします。 デフォルト：enabled

NBAR を使用したネットワーク トラフィックの分類方法

NBAR は、属性ベースのプロトコル照合を設定するための 2 つのアプローチを提供します。

- **カテゴリとサブカテゴリ**へのトラフィックのグループ化（カテゴリとサブカテゴリを使用した属性ベースのプロトコル一致の設定，（30 ページ）を参照）

  SRND を使用しないポリシー実装に役立ちます。この方式の欠点は、ポリシー内で定義されたカテゴリ/サブカテゴリとトラフィックとの間のマッピングを追跡することが困難になる可能性があることです。

- Solution Reference Network Design（**SRND**）モデルの使用（SRND を使用した属性ベースのプロトコル一致の設定，（32 ページ）を参照）

  SRND ベースのポリシーの設定を簡素化します。カテゴリ/サブカテゴリ モデルは SRND 実装をサポートできますが、このモデルを使用する方がシンプルかつ効率的です。

カテゴリの使用に適合する属性ベースのプロトコルの設定について

SRND を使用しないポリシー実装に役立ちます。この方式の欠点は、ポリシー内で定義されたカテゴリ/サブカテゴリとトラフィックとの間のマッピングを追跡することが困難になる可能性があることです。手順の詳細については、カテゴリとサブカテゴリを使用した属性ベースのプロトコル一致の設定，（30 ページ）を参照してください。

SRND の使用に適合する属性ベースのプロトコルの設定について

NBAR カテゴリ/サブカテゴリ モデルは、SRND 実装をサポートできます。ただし、IOS 15.5(3)T および IOS XE 3.16S 以降のリリースでは、SRND ポリシー実装に対して、より効率的な SRND 固有のモデルの使用が推奨されています。

SRND 固有のモデルは、SRND ベースのポリシーに適合するプロトコルを設定するための 2 つの属性（traffic-class と business-relevance）を提供します。SRND ベースのポリシーを使用した運用向けに提供される属性は、SRND 実装の一環でのみ使用できます。

背景：SRND ポリシー モデル

Solution Reference Network Design（SRND）ポリシー モデルは、QoS のためのトラフィックの優先順位付けを簡素化します。このモデルは、アプリケーションに基づいてトラフィックを定義する 12 のクラスを提供します。トラフィックのクラスごとに固有の QoS キューに入れることができます。これらのクラスのうち：

- 10 のクラスは、VoIP、ビデオ、会議などの 10 種類の一般に認められたテクノロジーで動作するビジネス関連アプリケーションに適用されます。
- 1 つのクラスは、テクノロジーが不明なビジネス関連アプリケーションに適用されます。
- 1 つのクラスは、非ビジネス関連アプリケーションに適用されます。

アプリケーションを再分類する柔軟性

NBAR が SRND モデルで運用するために提供している 12 のクラスには、ほとんどの企業に適切なデフォルト値が含まれています。ただし、必要に応じて、NBAR は、特定のアプリケーションをビジネス関連または非ビジネス関連として簡単に再分類できるようにします。（Skype VoIP アプリケーションの再分類の例：例：SRND 設定 - アプリケーションをビジネス関連（business-relevant）と再分類する，（39 ページ）を参照してください）。

属性：traffic-class

traffic-class 属性は、VoIP、ビデオ、会議などのトラフィックの一般的なカテゴリを指定します。次の表で、**traffic-class** の 10 の値について説明します。

表 *4*：***traffic-class*** の値

値	説明
voip-telephony	VoIP テレフォニー（ベアラーのみ）トラフィック
broadcast-video	ブロードキャスト TV、ライブ イベント、ビデオ監視
real-time-interactive	高解像度インタラクティブ ビデオ アプリケーション
multimedia-conferencing	デスクトップ ソフトウェア マルチメディア コラボレーション アプリケーション

値	説明
multimedia-streaming	ビデオ オン デマンド（VoD）ストリーミング ビデオ
network-control	ネットワーク コントロールプレーン トラフィック
signaling	IP 音声およびビデオ テレフォニーをサポートするシグナリング トラフィック
ops-admin-mgmt	ネットワーク運用、管理者および管理トラフィック
transactional-data	インタラクティブ データ アプリケーション
bulk-data	非インタラクティブ データ アプリケーション

属性：business-relevance

business-relevance 属性は、アプリケーションが組織のビジネス活動に関係があると見なされるかどうかを指定します。デフォルト値は一般的な使用状況とビジネス関連性を反映しており、値は組織固有の要件に合わせてカスタマイズできます。

次の表で、business-relevance の値について説明します。

表 *5*：*business-relevance* の値

値	説明
business-relevant	組織のビジネス活動にとって不可欠なアプリケーション
default	組織のビジネス活動に使用されるアプリケーション
business-irrelevant	組織のビジネス活動に関係しないアプリケーション

カテゴリとサブカテゴリを使用した属性ベースのプロトコル一致の設定

手順の概要

1. **enable**
2. **configureterminal**
3. **class-map** [**type**] [**match-all** |**match-any**] *class-map-name*
4. **matchprotocolattributeapplication-group***application-group* [*application-name*]
5. **matchprotocolattributecategory***application-category* [*application-name*]
6. **matchprotocolattributeencrypted** {**encrypted-no** | **encrypted-unassigned** | **encrypted-yes**} [*application-name*]
7. **matchprotocolattributesub-category***application-category* [*application-name*]
8. **matchprotocolattributetunnel** {**tunnel-no** | **tunnel-unassigned** | **tunnel-yes**} [*application-name*]
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map** [**type**] [**match-all** |**match-any**] *class-map-name* 例： `Device(config)# class-map cmap1`	指定したクラスとパケットの照合に使用されるクラスマップを作成し、QoS クラスマップ モードを開始します。 • クラス マップの名前を入力します。
ステップ 4	**matchprotocolattributeapplication-group***application-group* [*application-name*] 例： `Device(config-cmap)# match protocol attribute application-group skype`	指定されたアプリケーション グループを一致基準として設定します。 • （任意）アプリケーション グループではなくアプリケーションを一致基準として設定するには、*application-name* 引数を使用します。この設定は、**matchprotocolattributeapplication-group***application-group*

	コマンドまたはアクション	目的
		ではなく **matchprotocol***application-name* として保存されます。
ステップ 5	**matchprotocolattributecategory***application-category* [*application-name*] 例： `Device(config-cmap)# match protocol attribute category email`	指定されたカテゴリを一致基準属性として設定します。 • （任意）アプリケーション カテゴリではなく特定のアプリケーションを一致基準として設定するには、*application-name* 引数を使用します。この設定は、**matchprotocolattributecategory***application-category* ではなく **matchprotocol***application-name* として保存されます。
ステップ 6	**matchprotocolattributeencrypted** {**encrypted-no** | **encrypted-unassigned** | **encrypted-yes**} [*application-name*] 例： `Device(config-cmap)# match protocol attribute encrypted encrypted-yes`	指定された暗号化ステータスを一致基準として設定します。 • （任意）指定された暗号化ステータス内のアプリケーションを一致基準として設定するには、*application-name* 引数を使用します。この設定は、**matchprotocolattributeencrypted** {**encrypted-no** | **encrypted-unassigned** | **encrypted-yes**} ではなく **matchprotocol***application-name* として保存されます。
ステップ 7	**matchprotocolattributesub-category***application-category* [*application-name*] 例： `Device(config-cmap)# match protocol attribute sub-category client-server`	指定されたサブカテゴリを一致基準属性として設定します。 • （任意）サブカテゴリではなく特定のアプリケーションを一致基準として設定するには、*application-name* 引数を使用します。この設定は、**matchprotocolattributesub-category***application-category* ではなく **matchprotocol***application-name* として保存されます。
ステップ 8	**matchprotocolattributetunnel** {**tunnel-no** | **tunnel-unassigned** | **tunnel-yes**} [*application-name*] 例： `Device(config-cmap)# match protocol attribute tunnel tunnel-yes`	指定された暗号化ステータスを一致基準として設定します。 • （任意）指定されたトンネル ステータス内のアプリケーションを一致基準として設定するには、*application-name* 引数を使用します。この設定は、**matchprotocolattributetunnel** {**tunnel-no** | **tunnel-unassigned** | **tunnel-yes**} ではなく **matchprotocol***application-name* として保存されます。

	コマンドまたはアクション	目的
ステップ 9	**end** 例： `Device(config-cmap)# end`	QoS クラスマップ モードを終了し、特権 EXEC モードに戻ります。

SRND を使用した属性ベースのプロトコル一致の設定

手順の概要

1. **enable**
2. **configureterminal**
3. **class-map** [**type**] [**match-all** |**match-any**] *class-map-name*
4. **matchprotocolattributetraffic-class***traffic-class-option*
5. **matchprotocolattributebusiness-relevance***business-relevance-option*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**class-map** [**type**] [**match-all** |**match-any**] *class-map-name* 例： `Device(config)# class-map cmap1`	指定したクラスとパケットの照合に使用されるクラスマップを作成し、QoS クラスマップ モードを開始します。 • クラスマップの名前を入力します。

	コマンドまたはアクション	目的
ステップ 4	**matchprotocolattributetraffic-class***traffic-class-option* 例： `Device(config-cmap)# match protocol attribute traffic-class voip-telephony`	指定されたトラフィック クラスを一致基準として設定します。 • *traff-class-option* に設定できる値：voip-telephony、broadcast-video、real-time-interactive、multimedia-conferencing、multimedia-streaming、network-control、signaling、ops-admin- mgmt、transactional-data、bulk-data
ステップ 5	**matchprotocolattributebusiness-relevance***business-relevance-option* 例： `Device(config-cmap)# match protocol attribute business-relevance business-relevant`	指定されたカテゴリを一致基準属性として設定します。 • *business-relevance-option* に設定できる値：business-relevant、default、business-irrelevant
ステップ 6	**end** 例： `Device(config-cmap)# end`	QoS クラスマップ モードを終了し、特権 EXEC モードに戻ります。

SRND 設定：典型的なクラスマップ、ポリシーマップ

次のセクションは、SRND 実装の class-map と policy-map の一般的な例を示しています。traffic-class と business-relevance 属性がどのように 12 クラスの SRND QoS モデルに対応するかを説明します。

クラスマップ

```
class-map match-all VOICE
    match protocol attribute traffic-class voip-telephony
    match protocol attribute business-relevance business-relevant

class-map match-all BROADCAST-VIDEO
    match protocol attribute traffic-class broadcast-video
    match protocol attribute business-relevance business-relevant

class-map match-all INTERACTIVE-VIDEO
    match protocol attribute traffic-class real-time-interactive
    match protocol attribute business-relevance business-relevant

class-map match-all MULTIMEDIA-CONFERENCING
    match protocol attribute traffic-class multimedia-conferencing
    match protocol attribute business-relevance business-relevant

class-map match-all MULTIMEDIA-STREAMING
```

```
    match protocol attribute traffic-class multimedia-streaming
    match protocol attribute business-relevance business-relevant

class-map match-all SIGNALING
    match protocol attribute traffic-class signaling
    match protocol attribute business-relevance business-relevant

class-map match-all NETWORK-CONTROL
    match protocol attribute traffic-class network-control
     match protocol attribute business-relevance business-relevant

class-map match-all NETWORK-MANAGEMENT
    match protocol attribute traffic-class ops-admin-mgmt
    match protocol attribute business-relevance business-relevant

class-map match-all TRANSACTIONAL-DATA
    match protocol attribute traffic-class transactional-data
    match protocol attribute business-relevance business-relevant

class-map match-all BULK-DATA
    match protocol attribute traffic-class bulk-data
    match protocol attribute business-relevance business-relevant

class-map match-all SCAVENGER
    match protocol attribute business-relevance business-irrelevant
```

ポリシーマップ

```
policy-map 12-cls-marking

class VOICE
    set dscp ef

class BROADCAST-VIDEO
    set dscp cs5

class INTERACTIVE-VIDEO
    set dscp cs4

class MULTIMEDIA-CONFERENCING
    set dscp af41

class MULTIMEDIA-STREAMING
    set dscp af31

class SIGNALING
    set dscp cs3

class NETWORK-CONTROL
    set dscp cs6

class NETWORK-MANAGEMENT
    set dscp cs2

class TRANSACTIONAL-DATA
    set dscp af21

class BULK-DATA
    set dscp af11

class SCAVENGER
    set dscp cs1

class class-default
    set dscp default
```

Cisco ソフトウェアの NBAR を使用したネットワーク トラフィックの分類の設定例

例：HTTP ヘッダー フィールドを使用した HTTP トラフィックの分類

次に、User-Agent、Referer、または From フィールドに「somebody@cisco.com」を含む要求メッセージが、NBAR によって分類される例を示します。通常、「somebody@cisco.com」のような形式の項目は、HTTP 要求メッセージの From ヘッダー フィールドで見られます。

```
Device(config)# class-map match-all class1
Device(config-cmap)# match protocol http from "somebody@cisco.com"
```

次に、User-Agent、Referer、または From フィールドに「http://www.cisco.com/routers」を含む要求メッセージが、NBAR によって分類される例を示します。通常、「http://www.cisco.com/routers」のような形式の項目は、HTTP 要求メッセージの Referer ヘッダー フィールドで見られます。

```
Device(config)# class-map match-all class2
Device(config-cmap)# match protocol http referer "http://www.cisco.com/routers"
```

次に、User-Agent、Referer、または From フィールドに「CERN-LineMode/2.15」を含む要求メッセージが、NBAR によって分類される例を示します。通常、「CERN-LineMode/2.15」のような形式の項目は、HTTP 要求メッセージの User-Agent ヘッダー フィールドで見られます。

```
Device(config)# class-map match-all class3
Device(config-cmap)# match protocol http user-agent "CERN-LineMode/2.15"
```

次に、Content-Base（使用可能な場合）、Content-Encoding、Location、または Server ヘッダー フィールドに「CERN/3.0」を含む応答メッセージが、NBAR によって分類される例を示します。通常、「CERN/3.0」のような形式の項目は、応答メッセージの Server ヘッダー フィールドで見られます。

```
Device(config)# class-map match-all class4
Device(config-cmap)# match protocol http server "CERN/3.0"
```

次に、Content-Base（使用可能な場合）、Content-Encoding、Location、または Server ヘッダー フィールドに「http://www.cisco.com/routers」を含む応答メッセージが、NBAR によって分類される例を示します。通常、「http://www.cisco.com/routers」のような形式の項目は、応答メッセージの Content-Base（使用可能な場合）または Location ヘッダー フィールドで見られます。

```
Device(config)# class-map match-all class5
Device(config-cmap)# match protocol http location "http://www.cisco.com/routers"
```

次に、Content-Base（使用可能な場合）、Content-Encoding、Location、または Server ヘッダー フィールドに「gzip」を含む応答メッセージが、NBAR によって分類される例を示します。通常、「gzip」のような形式の項目は、応答メッセージの Content-Encoding ヘッダー フィールドで見られます。

```
Device(config)# class-map match-all class6
Device(config-cmap)# match protocol http content-encoding "gzip"
```

例：HTTP ヘッダーおよび URL、Host、または MIME タイプの分類の組み合わせによる HTTP トラフィックの識別

次に、HTTP ヘッダー フィールドと URL を組み合わせてトラフィックを分類する例を示します。この例では、User-Agent フィールド「CERN-LineMode/3.0」、Server フィールド「CERN/3.0」、ホスト名「cisco.com」、および URL「/routers」を含むトラフィックが NBAR を使用して分類されます。

```
Device(config)# class-map match-all c-http
Device(config-cmap)# match protocol http user-agent "CERN-LineMode/3.0"
Device(config-cmap)# match protocol http server "CERN/3.0"
Device(config-cmap)# match protocol http host cisco*
Device(config-cmap)# match protocol http url /routers
```

例：NBAR とカスタム プロトコルおよびアプリケーションの分類

次のカスタム プロトコル LAYER4CUSTOM の例では、6700 の宛先ポートまたは送信元ポートを持つ TCP パケットを検索します。

```
Device# configure terminal
Device(config)# ip nbar custom LAYER4CUSTOM  transport tcp id 14
Device(config-custom)# port 6700
```

ポート以外のオプションを表示するには、次のようにします。

```
Device# configure terminal
Device(config)# ip nbar custom LAYER4CUSTOM  transport tcp id 14
Device(config-custom)# ?
Custom protocol commands:
  direction  Flow direction
  dscp       DSCP in IPv4 and IPv6 packets
  exit       Exit from custom configuration mode
  ip         ip address
  ipv6       ipv6 address
  no         Negate a command or set its defaults
  port       ports
```

例：NBAR とピアツーピア ファイル共有アプリケーションの分類

matchprotocolgnutellafile-transfer*regular-expression* および **matchprotocolfasttrackfile-transfer***regular-expression* コマンドは、トラフィック クラスの Gnutella および FastTrack 分類の有効化に使用します。特定の Gnutella または FastTrack トラフィックの識別に正規表現変数が使用されることを示すために、**file-transfer** キーワードが使用されます。すべての FastTrack または Gnutella トラフィックをトラフィック クラスで分類するには、*regular-expression* 変数を「*」で表現できます。

次の例では、すべての FastTrack トラフィックはクラス マップ nbar に分類されます。

```
Device(config)# class-map match-all nbar
Device(config-cmap)# match protocol fasttrack file-transfer "*"
```

同様に、次の例ではすべての Gnutella トラフィックはクラス マップ nbar に分類されます。

```
Device(config)# class-map match-all nbar
Device(config-cmap)# match protocol gnutella file-transfer "*"
```

また、正規表現のワイルドカード文字は、特定の Gnutella および FastTrack トラフィックの識別にも使用できます。これらの正規表現一致を使用して、ファイル名の拡張子またはファイル名に含まれる特定の文字列に基づいてマッチングを実行します。

次に、拡張子が .mpeg の Gnutella ファイルすべてをクラス マップ nbar に分類する例を示します。

```
Device(config)# class-map match-all nbar
Device(config-cmap)# match protocol gnutella file-transfer "*.mpeg"
```

次に、文字「cisco」を含む Gnutella トラフィックのみを分類する例を示します。

```
Device(config)# class-map match-all nbar
Device(config-cmap)# match protocol gnutella file-transfer "*cisco*"
```

同じ例を FastTrack トラフィックに使用できます。

```
Device(config)# class-map match-all nbar
Device(config-cmap)# match protocol fasttrack file-transfer "*.mpeg"
```

または

```
Device(config)# class-map match-all nbar
Device(config-cmap)# match protocol fasttrack file-transfer "*cisco*"
```

例：属性ベースのプロトコル一致の設定

matchprotocolattributes コマンドは、さまざまな属性をアプリケーション認識の一致基準として設定するのに使用します。

次の例では、電子メールに関連するアプリケーション カテゴリが一致基準として設定されます。

```
Device# configure terminal
Device(config)# class-map mygroup
Device(config-cmap)# match protocol attribute category email
```

次の例では、Skype グループのアプリケーションが一致基準として設定されます。

```
Device# configure terminal
Device(config)# class-map apps
Device(config-cmap)# match protocol attribute application-group skype-group
```

次の例では、暗号化アプリケーションが一致基準として設定されます。

```
Device# configure terminal
Device(config)# class-map my-class
Device(config-cmap)# match protocol encrypted encrypted-yes
```

次の例では、クライアント/サーバサブカテゴリのアプリケーションが一致基準として設定されます。

```
Device# configure terminal
Device(config)# class-map newmap
Device(config-cmap)# match protocol attribute sub-category client-server
```

次の例では、トンネル アプリケーションが一致基準として設定されます。

```
Device# configure terminal
Device(config)# class-map mygroup
Device(config-cmap)# match protocol attribute tunnel tunnel-yes
```

次に、すべての属性の詳細を表示する **showipnbarattribute** コマンドの出力例を示します。

```
Device# show ip nbar attribute

      Name :  category
      Help :  category attribute
      Type :  group
    Groups :  email, newsgroup, location-based-services, instant-messaging, netg
      Need :  Mandatory
   Default :  other

      Name :  sub-category
      Help :  sub-category attribute
      Type :  group
    Groups :  routing-protocol, terminal, epayment, remote-access-terminal, nen
      Need :  Mandatory
   Default :  other

      Name :  application-group
      Help :  application-group attribute
      Type :  group
    Groups :  skype-group, wap-group, pop3-group, kerberos-group, tftp-group, bp
      Need :  Mandatory
   Default :  other

      Name :  tunnel
      Help :  Tunnelled applications
      Type :  group
    Groups :  tunnel-no, tunnel-yes, tunnel-unassigned
      Need :  Mandatory
   Default :  tunnel-unassigned

      Name :  encrypted
      Help :  Encrypted applications
      Type :  group
    Groups :  encrypted-yes, encrypted-no, encrypted-unassigned
      Need :  Mandatory
   Default :  encrypted-unassigned
```

次に、プロトコルの詳細を表示する **showipnbarprotocol-attribute** コマンドの出力例を示します。

```
Device# show ip nbar protocol-attribute

           Protocol Name :  ftp
                category :  file-sharing
            sub-category :  client-server
       application-group :  ftp-group
                  tunnel :  tunnel-no
               encrypted :  encrypted-no

           Protocol Name :  http
                category :  browsing
            sub-category :  other
       application-group :  other
                  tunnel :  tunnel-no
               encrypted :  encrypted-no

           Protocol Name :  egp
                category :  net-admin
            sub-category :  routing-protocol
       application-group :  other
                  tunnel :  tunnel-no
               encrypted :  encrypted-no

           Protocol Name :  gre
                category :  net-admin
            sub-category :  tunneling-protocols
       application-group :  other
                  tunnel :  tunnel-yes
               encrypted :  encrypted-no
```

例：SRND設定-アプリケーションをビジネス関連（business-relevant）と再分類する

Skype はコンシューマ VoP 製品であり、一般的にビジネスでは使用されません。SRND 固有のプロトコル マッピングでは、デフォルトで Skype は business-irrelevant と分類されます。ただし、一部の組織では Skype はビジネス クリティカルなアプリケーションとして使用されることがあります。この例では、Skype を business-relevant と再分類する方法が示されます。

1. Skype の現在のプロトコル属性を表示します。結果は（最後の 2 行で）、Skype が VoIP テレフォニー技術として分類され、business-irrelavant であることを示します。

```
show ip nbar protocol-attribute skype
encrypted           encrypted-yes
tunnel              tunnel-no
category            voice-and-video
sub-category        consumer-multimedia-messaging
application-group   skype-group
p2p-technology      p2p-tech-yes
traffic-class       voip-telephony
business-relevance  business-irrelevant
```

   この段階で、Skype は標準のデフォルト SRND class-map 設定の一部である SCAVENGER class-map に一致します。

```
class-map match-all SCAVENGER
    match protocol attribute business-relevance business-irrelevant
```

2. Skype の business-relevance の値を business-relevant に変更します。

```
ip nbar attribute-map demo
    attribute business-relevance business-relevant
ip nbar attribute-set skype demo
```

   この段階で、Skype は標準のデフォルト SRND class-map 設定の一部である VOIP-TELEPHONY class-map に一致します。

```
class-map match-all VOIP-TELEPHONY
    match protocol attribute traffic-class voip-telephony
    match protocol attribute business-relevance business-relevant
```

3. Skype が business-relevant と分類されていることを確認します。新しい値は次の結果の最後の行に示されています。

```
show ip nbar protocol-attribute skype
encrypted           encrypted-yes
tunnel              tunnel-no
category            voice-and-video
sub-category        consumer-multimedia-messaging
application-group   skype-group
p2p-technology      p2p-tech-yes
traffic-class       voip-telephony
business-relevance  business-relevant
```

例：組み込みプロトコルのカスタマイズ

NBAR 組み込みプロトコル（Cisco プロトコル パックに付属）をカスタマイズして、ユーザ指定のドメインを追加で含めると、組み込みプロトコルの範囲が拡大されます。プロトコルに関連付

けられたポリシーは、ユーザ指定のドメインにも適用されます。次に、myOffice365 というカスタマイズ設定で、組み込みの office365 プロトコルを拡張して「*uniqueOffice365」に一致するドメインを含める例を示します。

次の例では、電子メールに関連するアプリケーション カテゴリが一致基準として設定されます。

```
Device# configure terminal
Device(config)# ip nbar custom myOffice365 dns domain-name "*uniqueOffice365" extends
office365
```

その他の参考資料

ここでは、Protocol Discovery のイネーブル化に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
QoS コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Quality of Service Solutions Command Reference*』
NBAR に関する概念と情報	「NBAR を使用したネットワーク トラフィックの分類」モジュール
MQC を使用した NBAR の設定	「Configuring NBAR Using the MQC」モジュール
アプリケーション認識モジュール（PDLM とも呼ばれます）の追加	「Adding Application Recognition Modules」モジュール
カスタム プロトコルの作成	「カスタム プロトコルの作成」モジュール

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

NBAR を使用したネットワーク トラフィックの分類の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *6*：*NBAR* を使用したネットワーク トラフィックの分類の機能情報

機能名	リリース	機能情報
Additional PDL Support for NBAR	Cisco IOS XE リリース 3.1S	Additional PDL Support for NBAR 機能は、その他の PDL をサポートします。 この機能については、次の項を参照してください。NBAR と HTTP トラフィックの分類
Enable NBAR URI Extraction for HTTP Transactions for Persistent Connections	Cisco IOS XE リリース 3.9S	Enable NBAR URI Extraction for HTTP Transactions for Persistent Connections 機能は、トランザクション単位での URL フィールドの抽出とエクスポートをサポートします。 この機能については、次のセクションで説明しています。URL、ホスト、または MIME による HTTP トラフィックの分類。
Enhanced NBAR	Cisco IOS XE リリース 3.2S	Enhanced NBAR 機能は、Cisco IOS XE リリース 3.2S 用の追加の PDL を提供します。 この機能については、次のセクションで説明しています。NBAR がサポートするプロトコル

機能名	リリース	機能情報
NBAR Classification Enhancements for IOS-XE3.5	Cisco IOS XE リリース 3.5S	NBAR Classification Enhancements 機能は、ネイティブの IPv6 の分類、および IPv4 を介したトンネル化 IPv6 内のフローの分類に対応する分類を追加で提供します。 この機能については、次のセクションで説明しています。IPv6 に対する NBAR のサポート 次のコマンドが導入または変更されました：**ipnbarclassificationtunneled-traffic**、**option**（FNF）。
NBAR PDLM Supported in ASR 1000 リリース 2.5	Cisco IOS XE リリース 2.5 Cisco IOS XE リリース 3.1S Cisco IOS XE リリース 3.3S	この機能は、Cisco IOS XE リリース 2.5 に統合されました。このリリースでは、NBAR でサポートされるプロトコルが追加されました。 この機能については、次のセクションで説明しています。NBAR がサポートするプロトコル 次のコマンドが変更されました：**matchprotocol**(NBAR)。
NBAR Protocols	Cisco IOS XE リリース 2.3	この機能は、Cisco IOS XE リリース 2.3 に統合されました。このリリースでは、NBAR でサポートされるプロトコルが追加されました。 この機能については、次のセクションで説明しています。NBAR がサポートするプロトコル 次のコマンドが変更されました：**matchprotocol**(NBAR)。

機能名	リリース	機能情報
NBAR Real-time Transport Protocol Payload Classification	Cisco IOS XE リリース 2.1	この機能は、Cisco ASR 1000 シリーズのアグリゲーションサービスルータで導入されました。 この機能については、次のセクションで説明しています。 NBAR がサポートするプロトコル
NBAR Static IPv4 IANA Protocols Pack1	Cisco IOS XE リリース 3.1S	この機能は、Cisco ASR 1000 シリーズのアグリゲーションサービスルータで導入されました。 この機能については、次のセクションで説明しています。 NBAR がサポートするプロトコル
NBAR VRF-Aware	Cisco IOS XE リリース 3.3S	この機能は、Cisco ASR 1000 シリーズのアグリゲーションサービスルータで導入されました。 この機能については、次のセクションで説明しています。 NBAR の拡張性
NBAR 多段階分類	Cisco IOS XE リリース 3.7S	この機能は、Cisco ASR 1000 シリーズのアグリゲーションサービスルータで導入されました。この機能については、次のセクションで説明しています。 NBAR Multi-stage Classification

機能名	リリース	機能情報
NBAR2: Add/Rename Static Attributes	Cisco IOS XE リリース 3.11S	カスタム値を使用すれば、プロトコルのグループ化に基づいて属性に名前を付けることができます。application-group、category、および sub-category の各属性にカスタム値を作成できます。 この機能については、「NBAR の分類と属性」を参照してください。 次のコマンドが導入または変更されました：**ip nbar attribute**、**show ip nbar attribute-custom**、および **show ip nbar category**。
NBAR2 GETVPN (Cryptomap) Support	Cisco IOS XE リリース 3.11S	この機能は、Cisco ASR 1000 シリーズのアグリゲーションサービスルータで導入されました。 この機能に関する詳細については、次の項を参照してください。 GETVPN に対する NBAR のサポート，（23 ページ）
CAPWAP に対する NBAR のサポート	Cisco IOS XE リリース 3.17S	CAPWAP（Control And Provisioning of Wireless Access Points）は、ワイヤレス トラフィック内で使用されるプロトコルで、アプリケーション トラフィックにポイントツーポイント カプセル化（トンネル）を提供します。NBAR は、CAPWAP トンネル内のアプリケーション トラフィックの NBAR 分類を可能にする CAPWAP 認識モードを提供します。 この機能に関する詳細については、次の項を参照してください。CAPWAP に対する NBAR のサポート

機能名	リリース	機能情報
NBAR DNS ベースの分類	Cisco IOS XE リリース 3.17S	この機能で、ユーザがアプリケーション サーバとの接続を開始するときに交換されるDNSトランザクション情報を使用することによって、トラフィックの分類を改善できます。この方式には、フローの先頭パケットに基づいてフローを分類できるという大きなメリットがあります。 この機能については、次のセクションで説明しています。NBAR DNS ベースの分類
組み込みプロトコルのカスタマイズ	Cisco IOS XE Denali 16.3	NBAR 組み込みプロトコル（Cisco プロトコル パックに付属）をカスタマイズして、ユーザ指定のドメインを追加で含めると、組み込みプロトコルの範囲が拡大されます。プロトコルに関連付けられたポリシーは、ユーザ指定のドメインにも適用されます。 この機能については、次のセクションで説明しています。組み込みプロトコルのカスタマイズ

用語集

暗号化：暗号化は、データの外観が変わるように、特定のアルゴリズムをデータに適用することです。暗号化によって、情報を見る権限がなければ理解できないデータになります。

HTTP：Hypertext Transfer Protocol。Web ブラウザと Web サーバがファイル（テキスト ファイルやグラフィック ファイルなど）の転送に使用するプロトコル。

IANA：Internet Assigned Numbers Authority。インターネット アーキテクチャ委員会（IAB）に属するインターネット学会（ISOC）の後援を受けて運営されている組織。IANA は IP アドレス空間の割り当ておよびドメイン名の割り当ての権限を InterNIC および他の組織に委任しています。また、自律システム番号など、TCP/IP スタックで使用される割り当て済みプロトコル ID のデータベースを維持しています。

LAN：Local-area Network（ローカルエリア ネットワーク）。比較的狭い地理的領域（最大で数千メートル）を対象とする高速で低エラーのデータ ネットワーク。LAN は、1 つの建物または他の地理的に制限された領域にあるワークステーション、周辺機器、およびその他のデバイスを接続します。LAN 規格は、オープン システム インターコネクション（OSI）モデルの物理およびデータリンク層でのケーブル配線とシグナリングを規定します。イネーブル、FDDI、およびトークンリングは、LAN テクノロジーで幅広く使用されています。

MIME：Multipurpose Internet Mail Extension。電子メールで、テキスト以外のデータ（つまり、プレーン ASCII コードでは表現できないデータ）を転送するための規格。たとえば、バイナリ、外国語テキスト（ロシア語や中国語など）、オーディオ、ビデオなどのデータです。MIME は RFC 2045『*Multipurpose Internet Mail Extension*（*MIME*）*Part One*：*Format of Internet Message Bodies*』で定義されています。

MPLS：Multiprotocol Label Switching（マルチプロトコル ラベル スイッチング）。ラベルを使用して IP トラフィックを転送するスイッチング方式です。このラベルによって、ネットワーク内のルータおよびスイッチが、事前に確立された IP ルーティング情報に基づくパケットの転送先を指示されます。

MQC：Modular Quality of Service Command-Line Interface（モジュラ QoS コマンドライン インターフェイス）。トラフィック クラスを定義し、トラフィック ポリシー（ポリシー マップ）を作成および設定し、そのポリシー マップをインターフェイスにアタッチできる CLI です。ポリシー マップは、適切な Quality of Service（QoS）をネットワーク トラフィックに適用するために使用されます。

ProtocolDiscovery：NBAR に含まれる機能。Protocol Discovery には、インターフェイスで動作しているアプリケーション プロトコルを検出できる機能が用意されています。

QoS：Quality of Service。転送システムのパフォーマンスの尺度の 1 つであり、転送品質とサービスのアベイラビリティを反映したものです。

RTCP：RTP Control Protocol。IPv6 Real-Time Transport Protocol（RTP）接続の QoS をモニタし、進行中のセッションに関する情報を伝送するプロトコルです。

ステートフルプロトコル：接続時に決まる TCP および UDP ポート番号を使用するプロトコル。

スタティックプロトコル：定義済み（事前に決まっている）TCP および UDP ポートを通信に使用するプロトコル。

サブポート分類：パケット ペイロードに含まれる情報（つまり、TCP または UDP のポート番号以外で検出される情報）によるネットワーク トラフィックの分類。

TCP：Transmission Control Protocol。信頼できる全二重方式データ送信を可能にする接続指向のトランスポート層プロトコル。TCP は TCP/IP プロトコル スタックの一部です。

トンネリング：トンネリングは、任意の標準ポイントツーポイント カプセル化スキームの実装に必要なサービスを提供するために設計されたアーキテクチャです。

UDP：User Datagram Protocol。TCP/IP プロトコル スタックのコネクションレス型トランスポート層プロトコルです。UDP は、確認応答や配信保証なしでデータグラムを交換する単純なプロトコルです。エラー処理と再送信は、他のプロトコルで処理する必要があります。UDP は、RFC 768『*User Datagram Protocol*』で定義されています。

WAN：Wide-Area Network（広域ネットワーク）。広範な地理的領域に分散するユーザにサービスを提供し、多くの場合、共通の通信事業者が提供する送信デバイスを使用するデータ通信ネットワークです。

第 3 章

NBAR プロトコル パック

NBAR プロトコル パックは、デバイス上にすでに存在しているベース IOS イメージを置き換えることなく NBAR でサポートされるプロトコルを更新するための簡単な方法を提供します。プロトコル パックは、一緒に開発され、パックされたプロトコルのセットです。NBAR プロトコル パックのロード方法については、『QoS：NBAR コンフィギュレーション ガイド』を参照してください。プロトコルパックでサポートされるプロトコルのリストを表示するには、『NBAR Protocol Library』を参照してください。

- 機能情報の確認，49 ページ
- NBAR プロトコル パックの前提条件，50 ページ
- NBAR プロトコル パックの制約事項，50 ページ
- NBAR プロトコル パックについて，50 ページ
- NBAR プロトコル パックのロード方法，55 ページ
- NBAR プロトコル パックの設定例，57 ページ
- NBAR プロトコル パックに関する追加情報，60 ページ
- NBAR プロトコル パックの機能情報，61 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

NBAR プロトコル パックの前提条件

プロトコルパックは、リブート後のエラーを回避するために、ローカルディスクにコピーする必要があります。

（注） NBAR エンジンに完全に適合する NBAR プロトコル パックをロードし、シスコ ソフトウェアの最新のリビルドもロードすることを強くお勧めします。

NBAR プロトコル パックの制約事項

デバイスごとに 1 つのプロトコル パックのみサポートされています。

NBAR プロトコル パックについて

プロトコル パックの概要

NBAR プロトコル パックは、デバイスのシスコ ソフトウェアを置き換えることなく、デバイスの NBAR プロトコル サポートを更新するソフトウェア パッケージです。NBAR プロトコル パックには、NBAR にサポートされる一連の署名が含まれています。

プロトコル パックには次の特長があります。

- ロードが容易。
- 高いバージョンのプロトコル パックにアップグレードしたり、低いバージョンのプロトコル パックに戻したりするのが容易。
- 必要なプロトコルのセットのみを提供。

Cisco は、ユーザの使用しているシスコ イメージがライセンスを受けているか受けていないかに応じて、2 つの異なるプロトコル パック（標準プロトコル パックと高度なプロトコル パック）を提供します。

シスコは、プロトコル パックを作成し、シスコのツールとプロセスを使用して新しいプロトコル パックを作成する組織（「パブリッシャ」）に特定の ID 番号を提供します。プロトコル パックを作成する組織が、そのパックを所有します。

シスコは、デバイス上のライセンスを受けたシスコイメージに対して高度なプロトコルパックを基本プロトコルパックとして提供します。高度なプロトコルパックには、リリースで利用可能なプロトコル記述言語（PDL）ファイルの完全なセットが含まれます。高度なプロトコル パックでは、NAME フィールドが「高度なプロトコル パック」である PDLM のみをロードできます。

シスコは、デバイス上のライセンスを受けていないシスコイメージに対して標準プロトコルパックを基本プロトコルパックとして提供します。標準プロトコルパックでは、機能が制限されています。カテゴリと属性、フィールド抽出およびトンネリングされた分類などの一部の機能はサポートされていません。標準プロトコルパックでは、NAME フィールドが「標準プロトコルパック」である PDLM のみをロードできます。

プロトコルパックでサポートされるプロトコルのリストを表示するには、『NBAR Protocol Library』を参照してください。

NBAR の分類ファイルには、プロトコル パックで利用可能な各プロトコルの共通名、説明、下層のプロトコルなどの情報が含まれています。**showipnbarprotocol-packactivetaxonomy**、**showipnbarprotocol-packinactivetaxonomy** および **showipnbarprotocol-packloadedtaxonomy** コマンドを使用して、アクティブ、非アクティブおよびすべてのロードされたプロトコル パックそれぞれの分類ファイルを参照してください。

NBAR 分類ファイルは一般に、1000 以上のプロトコルの情報が含まれ、分類ファイル サイズは 2 MB 以下です。**show ip nbar protocol-pack**[**active** | **inactive** | **loaded**] taxonomy コマンドからの出力を、たとえば **show ip nbar protocol-pack active taxonomy** | **redirect harddisk:***nbar_taxonomy.xml* のようなリダイレクト出力修飾子を使用して、ファイルにリダイレクトすることを推奨します。

SSL unique-name サブ分類

NBAR2 プロトコル パック 7.0.0 では、「unique-name」と呼ばれる新しいサブ分類がセキュア ソケット レイヤ（SSL）に対して導入されました。unique-name パラメータは、グローバルで既知ではないか、まだ NBAR にサポートされていないサーバの SSL セッションに一致させるのに使用することができます。unique-name は、SNI（Server Name Indication）フィールドが存在する場合はクライアント リクエスト内の SNI フィールドに一致するか、サーバの応答の第 1 の証明書内の共通名（CN）フィールドに一致します。

NBAR2 プロトコル パック 7.0.0 はまた、ハンドシェイクを使用する SSL セッションではなく、session-id を使用する SSL セッションをサポートします。

（注） SSL サブ分類パラメータは、組み込みの署名よりも優先されます。したがって、ユーザ定義の unique-name が Facebook などの既知のアプリケーションに一致する場合、組み込みのプロトコルには一致せず、設定されたサブ分類を持つ SSL に一致します。

（注） 他のサブ分類機能と同じように、分類の結果（たとえば Protocol Discovery で見られたような）には変更はなく、SSL のままです。ただし、クラス マップと一致するフローは、それらに対して設定された QoS および Performance Monitor などのサービスを受け取ります。一致の詳細な統計情報を表示するには、ポリシー マップのカウンタを参照してください。

SSL の詳細については、http://tools.ietf.org/html/rfc6101 を参照してください。

RTP 動的ペイロード タイプのサブ分類

NBAR2 プロトコル パック 7.0.0 により、Real-time Transport Protocol（RTP）オーディオおよび RTP ビデオの既存のサブ分類パラメータは、動的ペイロード タイプ（PT）を使用する RTP フローを検出するように強化されました。動的 PT は、RTP RFC で定義されている 96 から 127 のダイナミック レンジの PT であり、各セッションに対して SIP や RTSP などのシグナリング プロトコルによりオンラインで選択されます。このプロトコル パックでは、SIP を使用して開始された RTP セッションのみが動的ペイロード タイプにより一致します。

（注） RTP 音声/ビデオのサブ分類パラメータは本質的に汎用で、汎用 RTP トラフィックでのみ一致します。ms-lync-audio、cisco-jabber-audio、facetime および cisco-phone などのさらに具体的な分類は RTP と一致せず、さらにオーディオ/ビデオのサブ分類とも一致しません。

NBAR2 プロトコル パック 9.0.0 内の QoS とレポート用の新しいカテゴリとサブカテゴリ

NBAR2 プロトコル パック 9.0.0 では、QoS 設定を容易にし、AVC レポートをより意味のあるものにする新しいカテゴリとサブカテゴリが追加されました。そのため、多数のプロトコルのカテゴリとサブカテゴリの割り当てが、エンタープライズ ネットワークでのそれらの分類をより正確に反映するように更新されました。

新しいカテゴリでは、カテゴリに基づいてレポート内でより細かい粒度が利用できます。

新しいサブカテゴリは、さらに粒度の細かいレポートの生成に使用できるうえ、Cisco SRND QoS モデルに従って QoS ポリシーを実装するときに非常に役に立ちます。新しいサブカテゴリによって、アプリケーションがビジネスやコンシューマだけではなく、さまざまなメディア タイプにも分割されるため、特定のサブカテゴリを必要な SRND サービス クラスにマップして QoS を適用する MQC クラス マップの構築が容易になります。SRND の詳細については、http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSIntro_40.html#wp61104 を参照してください。

また、MQC クラス マップを変更するのではなく、属性マップを使用して特定のアプリケーションをデフォルトの割り当てとは別のサブカテゴリに再割り当てすることによっても、QoS 定義のカスタマイズがさらに容易になります。

プロトコルとそれらのマッピングの完全なリストについては、プロトコル ブック内の特定のプロトコルを参照するか、**show ip nbar attribute category** コマンドまたは **show ip nbar attribute sub-category** コマンドを使用します。

NBAR2 プロトコル パック 9.0.0 でサポートされるカテゴリとサブカテゴリ

NBAR2 プロトコル パック 9.0.0 でサポートされるカテゴリのリストを以下に示します。

- アノニマイザー
- バックアップおよびストレージ
- ブラウジング
- ビジネスおよび生産性ツール
- データベース
- 電子メール
- 電子決済
- ファイル共有
- ゲーム
- 産業用プロトコル
- インスタント メッセージング
- インターネット セキュリティ
- プロセス間 RPC
- Layer 3 over IP
- ロケーションベースのサービス
- ネット管理者
- ニュースグループ
- その他
- ソーシャルネットワーク
- ソフトウェア アップデート
- トロイの木馬
- 音声とビデオ

NBAR2 プロトコル パック 9.0.0 でサポートされるサブカテゴリのリストを以下に示します。

- 認証サービス
- バックアップ システム
- コンシューマ オーディオ ストリーミング
- コンシューマ クラウド ストレージ
- コンシューマ マルチメディア メッセージング
- コンシューマ ビデオ ストリーミング
- コンシューマ Web ブラウジング

- 制御とシグナリング
- デスクトップ仮想化
- エンタープライズ クラウド データ ストレージ
- エンタープライズ データセンター ストレージ
- エンタープライズ データセンター ストレージ
- エンタープライズ マルチメディア会議
- エンタープライズ リアルタイム アプリケーション
- エンタープライズ リッチメディア コンテンツ
- エンタープライズ ソフトウェア導入ツール
- エンタープライズ トランザクション アプリケーション
- エンタープライズ ビデオ ブロードキャスト
- エンタープライズ音声コラボレーション
- ファイル転送
- ネーミング サービス
- ネットワーク管理
- OS アップデート
- その他
- p2p ファイル転送
- p2p ネットワーキング
- リモート アクセス端末
- ルーティング プロトコル
- トンネリング プロトコル

（注） この更新では、一般的に使用されない一部のカテゴリとサブカテゴリの削除や名前の変更を行いました。一部の値はサブカテゴリからカテゴリに移動され、カテゴリ レベルでより細かい粒度が用意されました。そのため、プロトコルがインストールされたときに、削除された値または名前が変更された値に基づく一致を含む既存のクラスマップは自動的に削除されますが、コマンドは置き換えられません。削除された値と名前が変更された値を示す次のリストを参照して、既存のポリシーがどれも変更の影響を受けないことを確認してください。

次のカテゴリが NBAR2 プロトコル パック 9.0.0 で削除されました。

- インターネット プライバシー
- ストリーミング

次のサブカテゴリが NBAR2 プロトコル パック 9.0.0 で削除されました。

- クライアント サーバ
- 商用メディア配信
- データベース
- 電子決済
- ファイル共有
- インターネット プライバシー
- プロセス間 RPC
- ライセンス マネージャ
- ネットワーク プロトコル
- リッチ メディア HTTP コンテンツ
- ストレージ
- ストリーミング
- 端末
- 音声 - ビデオ - チャット - コラボレーション

NBAR プロトコル パックのロード方法

NBAR プロトコル パックのロード

手順の概要

1. **enable**
2. **configureterminal**
3. **ipnbarprotocol-pack***protocol-pack*[**force**]
4. **exit**
5. **showipnbarprotocol-pack**{protocol-pack | **active**} [**detail**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipnbarprotocol-pack***protocol-pack*[**force**] 例： `Device(config)# ip nbar protocol-pack harddisk:defProtoPack`	プロトコル パックをロードします。 • 基本のプロトコル パック バージョンとは異なる、より低いバージョンのプロトコル パックを指定し、ロードするには、**force** キーワードを使用します。これによりさらに、より低いバージョンのプロトコル パックでサポートされないコンフィギュレーションがすべて削除されます。
ステップ 4	**exit** 例： `Device(config)# exit`	特権 EXEC モードに戻ります。
ステップ 5	**showipnbarprotocol-pack**{protocol-pack | **active**} [**detail**] 例： `Device(config)# show ip nbar protocol-pack active`	プロトコル パック情報を表示します。 • このコマンドを使用して、ロードされたプロトコル パックのバージョン、パブリッシャ、その他の詳細を確認します。 • 指定されたプロトコル パックの情報を表示するには、*protocol-pack* 引数を使用します。 • アクティブなプロトコル パックの情報を表示するには、**active** キーワードを使用します。 • 詳細なプロトコル パックの情報を表示するには、**detail** キーワードを使用します。

NBAR プロトコル パックの設定例

例：NBAR プロトコル パックのロード

次の例は、ハードディスクから defProtoPack という名前の NBAR プロトコル パックをロードする方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# ip nbar protocol-pack harddisk:defProtoPack
Device(config)# exit
```

次に、NBAR プロトコル パックの基本イメージ バージョンに戻す例を示します。

```
Device> enable
Device# configure terminal
Device(config)# default ip nbar protocol-pack
Device(config)# exit
```

次の例は、**force** キーワードを使用して、低いバージョンのプロトコルパックをロードする方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# ip nbar protocol-pack harddisk:olddefProtoPack force
Device(config)# exit
```

例：ロードされた NBAR プロトコル パックの確認

次に、**showipnbarprotocol-pack active** コマンドで表示される、デバイスでライセンスされたシスコ イメージのデフォルトで提供されるプロトコル パックに関する情報の出力例を示します。

```
Device# show ip nbar protocol-pack active

ACTIVE protocol pack:
Name:                           Advanced Protocol Pack
Version:                        1.0
Publisher:                      Cisco Systems Inc.
NBAR Engine Version:            14
```

次に、**show ip nbar protocol-pack active detail** コマンドで出力される、デバイスでライセンスされたシスコ イメージのデフォルトで提供されるアクティブ プロトコル パックに関する詳細情報の例を示します。

```
Device# show ip nbar protocol-pack active detail

ACTIVE protocol pack:
Name:                           Advanced Protocol Pack
Version:                        1.0
Publisher:                      Cisco Systems Inc.
NBAR Engine Version:            14
Protocols:
base                            Mv: 4
```

```
ftp                                Mv: 5
http                               Mv: 18
static                             Mv: 6
socks                              Mv: 2
nntp                               Mv: 2
tftp                               Mv: 2
exchange                           Mv: 3
vdolive                            Mv: 1
sqlnet                             Mv: 2
netshow                            Mv: 3
sunrpc                             Mv: 3
streamwork                         Mv: 2
citrix                             Mv: 11
fasttrack                          Mv: 3
gnutella                           Mv: 7
kazaa2                             Mv: 11
```

次に、**showipnbarprotocol-pack** コマンドで出力される、指定されたデバイス ロケーションに存在する拡張プロトコル パックのプロトコル パック情報の例を示します。

```
Device# show ip nbar protocol-pack disk:0ppsmall_higherversion

Name:                              Advanced Protocol Pack
Version:                           2.0
Publisher:                         Cisco Systems Inc.
NBAR Engine Version:               14
Creation time:                     Mon Jul 16 09:29:34 UTC 2012
```

次に、**showipnbarprotocol-pack** コマンドで出力される、指定されたディスク ロケーションに存在するプロトコル パックの詳細な情報の例を示します。

```
Device# show ip nbar protocol-pack disk:0ppsmall_higherversion detail

Name:                              Advanced Protocol Pack
Version:                           2.0
Publisher:                         Cisco Systems Inc.
NBAR Engine Version:               14
Creation time:                     Mon Jul 16 09:29:34 UTC 2012
Protocol Pack contents:
iana                       Mv: 1
base                       Mv: 4
tftp                       Mv: 2
```

次に **showipnbarprotocol-pack** コマンドで出力される、デバイスでライセンスされていないシスコ イメージのアクティブ プロトコル パックに関する情報の例を示します。

```
Device# show ip nbar protocol-pack active

ACTIVE protocol pack:
Name:                              Standard Protocol Pack
Version:                           1.0
Publisher:                         Cisco Systems Inc.
```

例：NBAR 分類情報の表示

次に、**showipnbarprotocol-packactivetaxonomy** コマンドで出力される、アクティブ プロトコル パックのプロトコルに関する情報の例を示します。

```
Device# show ip nbar protocol-pack active taxonomy

Protocol Pack Taxonomy for Advanced Protocol Pack:
<?xml version="1.0"?>
```

```
<NBAR2-Taxonomy>
  <protocol>
    <name>active-directory</name>
    <engine-id>7</engine-id>
    <enabled>true</enabled>
    <selector-id>473</selector-id>
    <help-string>Active Directory Traffic</help-string>
    <global-id>L7:473</global-id>
    <common-name>Active Directory</common-name>
    <static>false</static>
    <attributes>
      <category>net-admin</category>
      <application-group>other</application-group>
      <p2p-technology>false</p2p-technology>
      <tunnel>false</tunnel>
      <encrypted>false</encrypted>
      <sub-category>network-management</sub-category>
    </attributes>
    <ip-version>
      <ipv4>true</ipv4>
      <ipv6>true</ipv6>
    </ip-version>

<references>http://www.microsoft.com/en-us/server-cloud/windows-server/active-directory.aspx</references>

    <id>1194</id>
    <underlying-protocols>cifs,ldap,ssl,ms-rpc</underlying-protocols>
    <long-description-is-final>true</long-description-is-final>
    <long-description>a directory service created by Microsoft for Windows domain networks,
 responsible for authenticating and authorizing all users and computers within a network
of Windows domain type, assigning and enforcing security policies for all computers in a
network and installing or updating software on network computers</long-description>
    <pdl-version>1</pdl-version>
    <uses-bundling>false</uses-bundling>
  </protocol>
  <protocol>
    <name>activesync</name>
    <engine-id>7</engine-id>
    <enabled>true</enabled>
    <selector-id>490</selector-id>
    <help-string>Microsoft Activesync protocol </help-string>
    <global-id>L7:490</global-id>
    <common-name>ActiveSync</common-name>
    <static>false</static>
    <attributes>
      <category>business-and-productivity-tools</category>
      <application-group>other</application-group>
      <p2p-technology>false</p2p-technology>
      <tunnel>false</tunnel>
      <encrypted>true</encrypted>
      <sub-category>client-server</sub-category>
    </attributes>
    <ip-version>
      <ipv4>true</ipv4>
      <ipv6>true</ipv6>
    </ip-version>
    <references>http://msdn.microsoft.com/en-us/library/dd299446(v=exchg.80).aspx</references>

    <id>1419</id>
    <underlying-protocols>http</underlying-protocols>
    <long-description-is-final>true</long-description-is-final>
    <long-description>ActiveSync is a mobile data synchronization technology and protocol
based on HTTP, developed by Microsoft. There are two implementations of the technology: one
 which synchronizes data and information with handheld devices with a specific desktop
computer, and another technology, commonly known as Exchange ActiveSync (or EAS), which
provides push synchronization of contacts, calendars, tasks, and email between
ActiveSync-enabled servers and devices.</long-description>
    <pdl-version>1</pdl-version>
    <uses-bundling>false</uses-bundling>
  </protocol>
  .
  .
```

```
.
.
```

例：SSL セッションの分類

次に、**unique-name** を使用して、「finance.cisco.com」というサーバ名の SSL ベースのサービスが一致する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# class-map match-any cisco-finance
Device(config-cmap)# match protocol ssl unique-name finance.cisco.com
```

例：RTP 動的ペイロード タイプの分類

次に、静的および動的 PT の両方を含む RTP オーディオ フローを検出する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# class-map match-any generic-rtp-audio
Device(config)# match protocol rtp audio
```

NBAR プロトコル パックに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS LAN スイッチング コマンド	『Cisco IOS LAN Switching Command Reference』
Cisco IOS QoS 構成情報	『*QoS Configuration Guide*』

標準および RFC

標準/RFC	マニュアル タイトル
RFC 3551	『RTP Profile for Audio and Video Conferences with Minimal Control』
RFC 6101	『The Secure Sockets Layer (SSL) Protocol Version 3.0』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

NBAR プロトコル パックの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *7*：*NBAR* プロトコル パックの機能情報

機能名	リリース	機能情報
NBAR プロトコル パック	Cisco IOS XE リリース 3.3S	この機能は、Cisco ASR 1000 シリーズのアグリゲーション サービス ルータで導入されました。 NBAR プロトコル パック機能を使用すると、開発済みのプロトコルのセットを 1 つにまとめたプロトコル パックを簡単に設定できます。 次のコマンドが導入または変更されました：**defaultipnbarprotocol-pack**、**ipnbarprotocol-pack**、**showipnbarprotocolpack**。

機能名	リリース	機能情報
NBAR2 Protocol Pack 7.0.0	Cisco IOS XE リリース 3.9S	この機能は、Cisco ASR 1000 シリーズのアグリゲーションサービスルータで導入されました。 この機能については、次のセクションで説明しています。SSL unique-name サブ分類, （*51 ページ*）および RTP 動的ペイロード タイプのサブ分類, （*52 ページ*）。
NBAR2: Integrate NBAR Taxonomy into the Router	Cisco IOS XE リリース 3.11S	NBAR 分類法には、プロトコルパックで使用可能なすべてのプロトコルの共通の名前、説明、基となるプロトコルなどの情報が含まれます。 次のコマンドが導入または変更されました：**show ip nbar protocol-pack**。
NBAR2 Protocol Pack 9.0.0	Cisco IOS XE リリース 3.13S	この機能は、Cisco ASR 1000 シリーズのアグリゲーションサービスルータで導入されました。 この機能については、次のセクションで説明しています。NBAR2 プロトコル パック 9.0.0 内の QoS とレポート用の新しいカテゴリとサブカテゴリ, （*52 ページ*）。

第 4 章

Protocol Discovery のイネーブル化

Network-Based Application Recognition（NBAR）には、Protocol Discovery という機能が含まれます。Protocol Discovery は、インターフェイス経由で渡されるアプリケーション プロトコル パケットを簡単に検出できる方法を提供します。NBAR を設定するときの最初の作業は Protocol Discovery をイネーブルにすることです。

このモジュールでは、Protocol Discovery 機能のイネーブル化に関する概念と作業について説明します。

- 機能情報の確認，63 ページ
- Protocol Discovery のイネーブル化の前提条件，64 ページ
- Protocol Discovery のイネーブル化に関する制限事項，64 ページ
- Protocol Discovery に関する情報，65 ページ
- Protocol Discovery のイネーブル化方法，66 ページ
- Protocol Discovery の設定例，69 ページ
- その他の参考資料，71 ページ
- Protocol Discovery のイネーブル化の機能情報，72 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

Protocol Discovery のイネーブル化の前提条件

Protocol Discovery をイネーブルにする前に、「NBAR を使用したネットワーク トラフィックの分類」モジュールの説明を参照してください。

Protocol Discovery のイネーブル化に関する制限事項

NBAR Protocol Discovery は次をサポートしません。

- ステートフル プロトコルによる非対称フロー。

（注） NBAR のコンテキストでは、非対称フローとは、ロード バランシングの実装や、パケットが異なるルータを経由して異なる方向に流れる非対称ルーティングなどの理由により、フローの異なるパケットが異なるルータを経由するフローのことです。

- NBAR の処理。設計上、NBAR の処理は In-Service Software Upgrade（ISSU）の際に一時的に無効化されます。次の syslog メッセージは、ISSU が完了した後の NBAR 分類の再起動を示します。

"%NBAR_HA-5-NBAR_INFO: NBAR sync DONE!"

- マルチキャスト パケット分類
- マルチプロトコル ラベル スイッチング（MPLS）ラベル付きパケットNBAR は IP パケットのみを分類します。ただし、トラフィックが MPLS に渡される前に、NBAR を使用して IP トラフィックを分類することができます。NBAR で分類したパケットで、モジュラ Quality of Service（QoS）CLI（MQC）を使用して IP Diffserv コードポイント（DSCP）フィールドを設定します。これによって、MPLS が MPLS ヘッダー内の MPLS Experimental（EXP）設定に DSCP 設定をマッピングできるようにします。
- 非 IP トラフィック。
- NBAR を実行するルータから送信されるか、そのルータに送信されるパケット。

NBAR は次の論理インターフェイスでサポートされません。

- ダイヤラ インターフェイス
- ダイナミック仮想トンネル インターフェイス（DVTI）などのダイナミック トンネル
- Fast EtherChannel
- デバイスで終端する IPv6 トンネル
- MPLS
- オーバーレイ トランスポート仮想化（OTV）オーバーレイ インターフェイス

（注） いくつかのリンクで NBAR によるカプセル化がサポートされていない場合、デバイスの他のインターフェイスにNBARを適用し、入力の分類を実行することができます。たとえば、LAN インターフェイスで NBAR を設定し、WAN リンクの出力トラフィックを分類することができます。

次の仮想インターフェイスは、Cisco IOS イメージによってはサポートされています。

- 総称ルーティング カプセル化（GRE）
- Protocol Discovery モードおよび MQC モードでの IPsec IPv4 トンネル（トンネリングされた IPv6 を含む）
- Protocol Discovery モードでの IPSec IPv6 トンネル（MQC モードではサポートされません）
- Protocol Discovery モードでのマルチポイント GRE/Dynamic マルチポイント VPN（DMVPN）

（注） NBARがトンネリングされたインターフェイスで有効化されている場合、NBARはより多くの CPU パワーを必要とします。

Protocol Discoveryがトンネル インターフェイスと、トンネル インターフェイスが設定された物理インターフェイスの両方で有効化されている場合、トンネル インターフェイスに指定されたパケットは両方のインターフェイスでカウントされます。物理インターフェイスでは、パケットはカプセル化に基づいて分類され、カウントされます。トンネル インターフェイスでは、パケットはレイヤ 7 プロトコルに基づいて分類され、カウントされます。

（注） トンネリングまたは暗号化が使用されている WAN リンクの出力トラフィックを分類するためには、NBAR を使用できません。そのため、ルータの他のインターフェイス（LAN リンクなど）でNBARを設定して入力の分類を実行してから、トラフィックを WAN リンクに切り替える必要があります。

Protocol Discovery に関する情報

Protocol Discovery の概要

NBAR の Protocol Discovery 機能は、適切な QoS 機能を適用できるように、インターフェイスをパススルーするアプリケーション プロトコルの検出を容易にします。

NBARは、ネットワークで現在動作しているプロトコルとアプリケーションを判断します。Protocol Discovery は、適切な QoS 機能を適用できるように、インターフェイス上で動作しているアプリケーション プロトコルの検出を容易にします。Protocol Discovery を使用すると、NBAR でサポー

トされるすべてのプロトコル トラフィックを検出し、そのプロトコルに関連付けられた統計情報を取得できます。

Protocol Discovery は、有効なインターフェイスに関する次のプロトコル別の統計情報を保持します。

- 入力パケットとバイトの合計数
- 出力パケットとバイトの合計数
- 入力ビット レート
- 出力ビット レート

これらの統計情報は、クラスと、各トラフィック クラスのトラフィック ポリシー（ポリシー マップとも呼ばれる）を定義するときに使用できます。トラフィック ポリシー（ポリシー マップ）は、特定の QoS の特性と機能をトラフィック クラスに適用するために使用されます。

インターフェイス拡張性

リリースによっては、Protocol Discoveryを有効にできるインターフェイスの数に制限があります。

次の表に、Protocol Discovery でサポートされるインターフェイスとリリース番号の詳細を示します。

表 *8*：リリースと *Protocol Discovery* インターフェイスのサポート

リリース	**Protocol Discovery でサポートされるインターフェイスの数**
Cisco IOS XE リリース 2.5 より前のリリース	無制限
Cisco IOS XE リリース 2.5	128
Cisco IOS XE リリース 2.6	256
Cisco IOS XE リリース 2.7	32
Cisco IOS XE リリース 3.2S 以降	32

Protocol Discovery のイネーブル化方法

インターフェイスでの Protocol Discovery のイネーブル化

インターフェイスで Protocol Discovery を有効にするには、次の作業を行います。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***typenumber* [*name-tag*]
4. **ipnbarprotocol-discovery** [**ipv4** | **ipv6**]
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***typenumber* [*name-tag*] 例： `Router(config)# interface fastethernet1/1/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。 • インターフェイス タイプとインターフェイス番号を入力します。
ステップ 4	**ipnbarprotocol-discovery** [**ipv4** | **ipv6**] 例： `Router(config-if)# ip nbar protocol-discovery`	特定のインターフェイス上で NBAR が認識するすべてのプロトコルについて、トラフィックを検出するように NBAR を設定します。 • （任意）**ipv4** キーワードを入力して IPv4 パケットの Protocol Discovery 統計情報収集を有効にするか、**ipv6** キーワードを入力して IPv6 パケットの Protocol Discovery 統計情報収集を有効にします。 • 次のいずれかのキーワードを指定すると、指定した IP バージョンのみの Protocol Discovery 統計情報収集が可能になります。どちらのキーワードも指定しなかった場合は、IPv4 と IPv6 の両方の統計情報収集が有効になります。 • 指定したキーワードのみの統計情報収集が有効になるため、このコマンドの **no** 形式を使用してキーワードを無効にする必要はありません。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Router(config-if)# end`	（任意）インターフェイス コンフィギュレーション モードを終了します。

Protocol Discovery の統計情報のレポート

インターフェイスごとに Protocol Discovery 統計情報のサポートを表示するには、次の作業を行います。

手順の概要

1. **enable**
2. **showpolicy-mapinterface***typenumber*
3. **showipnbarprotocol-discovery** [**interface***typenumber*] [**stats** {**byte-count** | **bit-rate** | **packet-count**| **max-bit-rate**}] [**protocol***protocol-name* | **top-n***number*]
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showpolicy-mapinterface***typenumber* 例： `Router# show policy-map interface FastEthernet 1/1/1`	（任意）指定したインターフェイスのすべてのポリシーマップについて、パケットとクラスの統計情報を表示します。 • インターフェイス タイプとインターフェイス番号を入力します。
ステップ 3	**showipnbarprotocol-discovery** [**interface***typenumber*] [**stats** {**byte-count**	**bit-rate**	**packet-count**| **max-bit-rate**}] [**protocol***protocol-name*	**top-n***number*]	NBAR Protocol Discovery 機能によって収集された統計情報を表示します。 • （任意）表示される統計情報を最適化するには、キーワードおよび引数を入力します。各キーワードの詳細

	コマンドまたはアクション	目的
	例： `Router# show ip nbar protocol-discovery interface Fastethernet1/1/1`	については、『Cisco IOS Quality of Service Solutions Command Reference』の **showipnbarprotocol-discovery** コマンドを参照してください。
ステップ 4	**exit** 例： `Router# exit`	（任意）特権 EXEC モードを終了します。

Protocol Discovery の設定例

例：インターフェイスでの Protocol Discovery のイネーブル化

次の設定例では、ファストイーサネットインターフェイス 1/1/1 で Protocol Discovery が有効です。

```
Router> enable
Router# configure terminal
Router(config)# interface fastethernet1/1/1
Router(config-if)# ip nbar protocol-discovery
Router(config-if)# end
```

次の設定例では、IPv6 パケットのファストイーサネットインターフェイス 1/1/2 で Protocol Discovery が有効です。

```
Router> enable
Router# configure terminal
Router(config)# interface fastethernet1/1/2
Router(config-if)# ip nbar protocol-discovery ipv6
Router(config-if)# end
```

次の設定例では、IPv6パケットのファストイーサネットインターフェイス1/1/2でProtocol Discoveryが有効です。その後、IPv4 パケットの Protocol Discovery を有効にしますが、**ipv6** キーワードの **no** 形式は必要ありません。

```
Router> enable
Router# configure terminal
Router(config)# interface fastethernet1/1/2
Router(config-if)# ip nbar protocol-discovery ipv6
Router(config-if)# ip nbar protocol-discovery ipv4
Router(config-if)# end
```

例：Protocol Discovery の統計情報のレポート

次に、ファストイーサネットインターフェイス 2/0/1 のアクティブなプロトコルの上位 5 個について、**showipnbarprotocol-discovery** コマンドの出力例を示します。

```
Router# show ip nbar protocol-discovery top-n 5

 FastEthernet2/0/1
                            Input                     Output
                            -----                     ------
  Protocol                  Packet Count              Packet Count
                            Byte Count                Byte Count
                            30sec Bit Rate (bps)      30sec Bit Rate (bps)
                            30sec Max Bit Rate (bps)  30sec Max Bit Rate (bps)
---------------------------- ------------------------- -------------------------
   rtp                      3272685                   3272685
                            242050604                 242050604
                            768000                    768000
                            2002000                   2002000
   gnutella                 513574                    513574
                            118779716                 118779716
                            383000                    383000
                            987000                    987000
   ftp                      482183                    482183
                            37606237                  37606237
                            121000                    121000
                            312000                    312000
   http                     144709                    144709
                            32351383                  32351383
                            105000                    105000
                            269000                    269000
   netbios                  96606                     96606
                            10627650                  10627650
                            36000                     36000
                            88000                     88000
   unknown                  1724428                   1724428
                            534038683                 534038683
                            2754000                   2754000
                            4405000                   4405000
   Total                    6298724                   6298724
                            989303872                 989303872
                            4213000                   4213000
                            8177000                   8177000
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
QoS コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Quality of Service Solutions Command Reference*』
NBAR に関する概念と情報	「NBAR を使用したネットワーク トラフィックの分類」モジュール
MQC	「Applying QoS Features Using the MQC」モジュール

標準

規格	タイトル
新しい規格または変更された規格はサポートされていません。また、既存の規格に対するサポートに変更はありません。	--

MIB

MIB	MIB のリンク
新しい MIB または変更された MIB はサポートされていません。また、既存の MIB に対するサポートに変更はありません。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Protocol Discovery のイネーブル化の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *9*：*Protocol Discovery* のイネーブル化の機能情報

機能名	リリース	機能情報
Protocol Discovery	Cisco IOS XE 2.1、Cisco IOS XE 3.3S	この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。 この機能に関する詳細については、次の各項を参照してください。 次のコマンドが導入されました：**ipnbarprotocoldiscovery**、**showipnbarprotocoldiscovery**。

第 5 章

自動トラフィック分析とプロトコル生成

NBAR には、一般的なネットワーク トラフィックと未知のネットワーク トラフィックを分析して最も頻繁に使用されているホストとポートを特定する auto-learn 機能が組み込まれています。このデータを使用して、auto-custom 機能は、トラフィックの識別を容易にするための一時的な NBAR プロトコルを自動的に生成することができます。

- auto-custom の前提条件，73 ページ
- auto-custom の制限，74 ページ
- 背景：NBAR2 auto-learn を使用した自動トラフィック分析，74 ページ
- auto-custom を使用したカスタム プロトコルの自動生成，74 ページ
- 自動カスタム モードの有効化および無効化，76 ページ
- 作成する自動生成 NBAR プロトコルの最大数の設定，76 ページ
- 自動カスタム プロトコルを再生成する時間間隔の設定，77 ページ
- 自動カスタム データのクリア，78 ページ
- 自動カスタム機能で作成された自動生成 NBAR プロトコルの表示，79 ページ
- 自動カスタム プロトコルの NBAR Protocol Discovery 情報の表示，80 ページ

auto-custom の前提条件

auto-custom 機能を使用するには、auto-learn が有効になっている必要があります。

NBAR Customized Assistance Based on SSL or HTTP を参照してください。

auto-custom の制限

デフォルト

auto-custom 機能はデフォルトでは無効です。

サポートされる環境

auto-custom 機能は次の環境をサポートします。

- 単一コレクタを備えた単一ルータ
- コレクタなしの単一ルータ

この機能は、単一コレクタで動作している複数のルータが存在する環境をサポートしません。

背景：NBAR2 auto-learn を使用した自動トラフィック分析

NBAR2 auto-learn 機能（NBAR2 auto-learn，（213 ページ）を参照）と auto-custom 機能は連動します。NBAR2 auto-learn は、一般的な HTTP/SSL または未知に分類されたトラフィックを分析します。一般的な HTTP/SSL トラフィックでは、トラフィック内のパケット ヘッダー フィールドからホスト名を抽出して、一般的なトラフィック上に出現する「トップ ホスト」を追跡します。未知のトラフィックでは、サーバ側のポートを特定して、未知のトラフィック上に出現する「トップ ポート」と「トップ ソケット」を追跡します。

auto-learn によって生成された結果は、auto-custom 機能で、分類が困難なトラフィックに対するアプリケーションの可視性を高めるため、トラフィックの分類を向上させるカスタム NBAR プロトコルを自動的に作成するために使用できます。たとえば、トップホストは、カスタムプロトコルの作成で使用される「候補」ホストを提供します。

auto-custom を使用したカスタム プロトコルの自動生成

auto-custom 機能は、auto-learn の結果を使用して、一般的なネットワーク トラフィックと未知のネットワーク トラフィックの NBAR 分類を改善し、カスタム NBAR プロトコルを自動的に生成します。

自動生成された NBAR プロトコルによって分類されたトラフィックのレポート形式

自動生成された NBAR プロトコルは、ホスト名またはポート番号に基づいてトラフィックをレポートします。

- 一般的なトラフィックの場合は、プロトコルは、最も頻繁に出現するホストに対して生成され、ホスト名に基づいて名前が付けられます。ホスト名がなくホストアドレスのみを含むト

ラフィックについては、NBAR は可能な場合に DNS ルックアップを使用して対応するホスト名を提供します。

例：abcd.com、efgh.net

- 未知のトラフィックの場合は、プロトコルは、最も頻繁に出現するポートに対して生成され、ポート番号またはソケット（サーバ側の IP とポート）とトラフィック タイプ（TCP または UDP）に基づいて名前が付けられます。

  ポートの例：Port_80_TCP、Port_443_UDP

  ソケットの例：72.163.4.162:256_TCP

トラフィック フローのサンプリングに基づく自動生成

auto-learn メカニズムは、分析するトラフィック フローをサンプリングすることにより、一般的なトラフィックと未知のトラフィックに関するデータを収集します。すべてのフローが分析されるわけではありません。各フローの分析ではなくサンプリングを使用する理由は、ハードウェア リソースの制約によるものです。auto-learn 分析にハードウェア リソースを使用できるかどうかは、デバイスが処理しているネットワーク トラフィックの量に主に依存します。

一般的なトラフィックの場合は、サンプリング レートは動的で、システム負荷に応じて自動的に調整されます。未知のトラフィックの場合は、デフォルトのサンプリング レートは 128 です。これは、このメカニズムによって 128 の未知のトラフィックごとに 1 フローをサンプリングされることを意味します。この値は手動で設定できます。

auto-custom 機能は auto-learn によって収集されたデータに依存するため、auto-learn によって実行されるフローサンプリングはauto-customによるプロトコルの自動生成に影響を与える可能性があります。ただし、ほとんどのユースケースで、ネットワーク トラフィックの構成が正確にサンプリングに反映されます。

他の機能によって自動生成された NBAR プロトコルの使用

auto-custom によって自動生成された NBAR アプリケーション プロトコルは、ネットワーク トラフィックのレポート機能を強化し、アプリケーションの可視性を向上させます。ただし、任意の時点で存在する自動生成されたプロトコルは、最新のネットワーク トラフィックの構成によって決定されるため、本質的に動的で一時的です。

この動的な特性のために、auto-custom プロトコルは一部の機能にしか適用できません。一般に、auto-custom プロトコルは、アプリケーションの可視性を向上させますが、セキュリティ（ファイアウォール）や QoS ポリシーには影響しません。

auto-custom プロトコルの影響を受ける機能：

- NBAR Protocol Discovery
- アプリケーションの可視性（FNF、パフォーマンス モニタ、ezPM、MACE など）

auto-custom プロトコルの影響を受けない機能：

- MQC/QoS
- WAAS

- Performance Routing（PfR）
- NAT

自動カスタム モードの有効化および無効化

次のいずれか一方または両方の自動カスタム モードを有効または無効にします。

- top-hosts
- top-ports

手順の概要

1. **configureterminal**
2. [**no**] **ipnbarauto-custom** {**top-ports** | **top-hosts**}
3. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**] **ipnbarauto-custom** {**top-ports** | **top-hosts**} 例： `Device(config)# ip nbar auto-custom top-hosts`	自動カスタムモードを有効または無効にします。top-ports オプションと top-hosts オプションを使用すると、コマンドがそれぞれの自動カスタム モードに適用されます。
ステップ 3	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了します。

作成する自動生成 NBAR プロトコルの最大数の設定

auto-custom で自動生成するプロトコルの最大数を設定します。自動生成されたプロトコルは出現時刻に関係なく、最近のネットワーク トラフィックの状態によって判別され、本質的に動的かつ非永続的になります。

手順の概要

1. **configureterminal**
2. **ipnbarauto-custom** {**top-hosts** | **top-ports**} **max-protocols***number*
3. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipnbarauto-custom** {**top-hosts** | **top-ports**} **max-protocols***number* 例： `ip nbar auto-custom top-hosts max-protocols 30`	auto-learn メカニズムによって収集された top-hosts または top-ports のリストから生成する自動カスタム プロトコルの最大数を設定します。 top-hosts のデフォルト：10 top-ports のデフォルト：10
ステップ 3	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了します。

自動カスタム プロトコルを再生成する時間間隔の設定

自動カスタムによって、汎用トラフィックの場合は「top-hosts」のリスト、不明データの場合は「top-ports」のリストをリロードする時間間隔を設定します。これらのリストは auto-learn メカニズムによって提供されます。リストをリロードした後、auto-custom メカニズムは、そのデータに基づいて新しいカスタム プロトコル セットを生成します。これには、最新のネットワーク トラフィックが反映されます。このメカニズムにより、自動カスタム プロトコルのリストは動的になり、汎用および不明のネットワーク トラフィックの状態によって変化します。

手順の概要

1. **configureterminal**
2. **ipnbarauto-custom** {**top-hosts** | **top-ports**} **time-interval***minutes*
3. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipnbarauto-custom** {**top-hosts** | **top-ports**} **time-interval***minutes* 例： `ip nbar auto-custom top-hosts time-interval 10`	自動カスタムによって、汎用トラフィックの場合は「top-hosts」のリスト、不明データの場合は「top-ports」のリストをリロードする時間間隔を設定します。 デフォルト：30 分
ステップ 3	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了します。

自動カスタム データのクリア

手順の概要

1. **configureterminal**
2. **clearipnbarauto-custom** {**top-hosts** | **top-ports**} {**stats** | **restart**}
3. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**clearipnbarauto-custom** {**top-hosts** | **top-ports**} {**stats** | **restart**} 例： `clear ip nbar auto-custom top-ports restart`	自動カスタム データをクリアします。 top-ports オプションと top-hosts オプションを使用すると、コマンドがそれぞれの自動カスタムモードに適用されます。 stats：カウンタのみをクリアします。 restart：カウンタをクリアし、現在のすべての自動カスタム プロトコルを削除します。

	コマンドまたはアクション	目的
ステップ 3	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了します。

自動カスタム機能で作成された自動生成 NBAR プロトコルの表示

手順の概要

1. **showipnbarauto-custom** [**top-hosts** | **top-ports**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**showipnbarauto-custom** [**top-hosts** | **top-ports**] 例： `show ip nbar auto-custom`	自動カスタムメカニズムで作成された自動生成NBARプロトコルを表示します。任意で、top-hosts または top-ports のプロトコルのみを指定できます。 • 出力の最初の部分は、generic トラフィックから取得された、ホスト名に基づいたプロトコルを示しています。 • 出力の 2 番目の部分は、unknown トラフィックから取得された、ポート番号 + トラフィック タイプ（TCP または UDP）に基づいたプロトコルを示しています。

```
# show ip nbar auto-custom
Top-hosts:
 Max number of protocols   :10
 Interval (min)            :30
 ---------------------------------------------------------------------------------------------------
 | Id  | Protocol name          | Underlying | Auto-learn value                | Age (min) | Status |
 |     |                        | protocol   |                                 |           |        |
 ---------------------------------------------------------------------------------------------------
 |    1|m.abc-demo.com          |http        |m.abc-demo.com                   |         80|Dynamic |
 |    2|hwcdn.def-demo.com      |http        |hwcdn.def-demo.com               |         80|Dynamic |
 |    3|ec.def-demo.com         |http        |ec.def-demo.com                  |         80|Dynamic |
 |    4|payroll.demo.com        |ssl         |payroll.demo.com                 |         80|Dynamic |
 |    5|ec-media.demo.com       |http        |ec-media.demo.com                |         50|Dynamic |
 |    6|TrustedSourceServer_IMQ |ssl         |TrustedSourceServer_IMQA01       |         20|Dynamic |
 |    7|go.microsoft.com        |http        |go.microsoft.com                 |         20|Dynamic |
 |    8|ping.chartbeat.net      |http        |ping.chartbeat.net               |         20|Dynamic |
 ---------------------------------------------------------------------------------------------------

Top-ports:
 Max number of protocols   :40
 Interval (min)            :1
 -----------------------------------------------------------------------------------------------------------
```

```
| Id  | Protocol name          |              Auto-learn value                    | Age (min) | Status |
-------------------------------------------------------------------------------------------------------
|    1|Port_256_TCP            |Port_256_TCP                                      |          0|Dynamic |
|    2|72.163.4.162:256_TCP    |72.163.4.162:256_TCP                              |          0|Dynamic |
-------------------------------------------------------------------------------------------------------
```

自動カスタム プロトコルの NBAR Protocol Discovery 情報の表示

手順の概要

1. **showipnbarprotocol-discoverystatauto-custom**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**showipnbarprotocol-discoverystatauto-custom** 例： `show ip nbar protocol-discovery stats auto-custom`	自動カスタム プロトコルのディスカバリ統計情報を表示します。

```
# show ip nbar protocol-discovery stats auto-custom

 Ethernet0/0

 Last clearing of "show ip nbar protocol-discovery" counters 1d05h

                            Input                    Output
                            -----                    ------
   ------------------------ ------------------------ ------------------------
www.abcdef-demo.com          152        0
Total                        152                      0
```

第 6 章

Configuring NBAR Using the MQC

Protocol Discovery をイネーブルにすると、モジュラ Quality of Service（QoS）コマンドライン インターフェイス（CLI）（MQC）を使用して、Network-Based Application Recognition（NBAR）を設定できます。MQC はトラフィック クラスとトラフィック ポリシー（ポリシー マップ）を使用して、NBAR に認識されるトラフィックおよびアプリケーションのクラスに QoS 機能を適用します。

このモジュールでは、MQC を使用して NBAR を設定する際の概念と作業について説明します。

- 機能情報の確認，81 ページ
- MQC を使用した NBAR の設定の前提条件，82 ページ
- NBAR の粗粒分類に関する情報，82 ページ
- MQC を使用して NBAR を設定する方法，84 ページ
- DSCP ベースのレイヤ 3 カスタム アプリケーションの設定例，93 ページ
- 次の作業，95 ページ
- その他の参考資料，95 ページ
- Configuring NBAR Using the MQC の機能情報，97 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

MQC を使用した NBAR の設定の前提条件

- MQC を使用して NBAR を設定する前に、「NBAR を使用したネットワーク トラフィックの分類」モジュールの説明を参照してください。
- 適用可能な場合、Protocol Discovery をイネーブルにし、ネットワークに使用されるプロトコルおよびアプリケーションに関する統計情報の取得に使用します。MQC を使用するときに、この情報が必要になります。

（注） この前提条件では、ネットワークで使用しているプロトコルとアプリケーションに関するこの情報をまだ持っていないと仮定しています。

NBAR の粗粒分類に関する情報

NBAR と MQC の機能

MQC を使用して NBAR を設定するには、トラフィック クラスを定義し、トラフィック ポリシー（ポリシーマップ）を設定してから、そのトラフィック ポリシーを適切なインターフェイスに適用します。これら 3 つの作業は MQC を使用して実現できます。MQC とは、コマンドライン インターフェイスで、トラフィック クラスの定義、トラフィック ポリシーの作成および設定（ポリシー マップ）、およびトラフィック ポリシーのインターフェイスへのアタッチが行えます。

MQC では、**class-map** コマンドを使ってトラフィック クラスを定義します（トラフィック クラスはその後、トラフィック ポリシーに関連付けられます）。トラフィック クラスの目的は、トラフィックを分類することです。

MQC を使用した NBAR の設定は、次の作業から構成されます。

- **class-map** コマンドを使用したトラフィック クラスの定義
- トラフィック クラスを 1 つまたは複数の QoS 機能と関連付けてトラフィック ポリシーを作成（**policy-map** コマンドを使用）
- **service-policy** コマンドを使用した、トラフィック ポリシーのインターフェイスへの適用

トラフィック クラスには、3 つの主要な要素が含まれています。それらは、名前、1 つ以上の **match** コマンド、およびトラフィック クラス内に複数の **match** コマンドが存在する場合にこれらの **match** コマンドを評価する方法（**match-all** または **match-any**）に関する手順です。トラフィック クラスの名前は、**class-map** コマンド ラインで指定します。たとえば、CLI でトラフィック クラスを設定するときに **class-map cisco** コマンドを入力すると、トラフィック クラスの名前は「cisco」になります。

match コマンドは、パケット分類のためのさまざまな基準を指定するために使用します。パケットは、matchコマンドで指定された基準に合っているかどうかを判断するためにチェックされます。指定された基準に合っていれば、パケットはクラスのメンバーと見なされ、トラフィック ポリシーで設定された QoS 仕様に従って転送されます。一致基準を満たさないパケットは、デフォルトのトラフィック クラスのメンバーとして分類されます。

（注） NBAR の場合は、**match protocol** コマンドがNBAR と match protocol コマンド, （83 ページ）の説明に従って一致基準の指定に使用されます。

NBAR と match protocol コマンド

NBARは、ネットワークに使用される特定のネットワーク プロトコルとネットワーク アプリケーションを認識します。NBARによってプロトコルまたはアプリケーションが認識されると、MQCを使用して、そのプロトコルまたはアプリケーションに関連付けられているパケットをクラスにグループ化できます。これらのクラスは、パケットが特定の基準に準拠しているかどうかに基づいてグループ化されます。

NBAR の場合、NBAR に認識される特定のプロトコルまたはアプリケーションにパケットが一致するかどうかという基準です。MQC を使用すると、1 つのネットワーク プロトコル（citrix など）を使用するネットワーク トラフィックを 1 つのトラフィック クラスに配置し、異なるネットワーク プロトコル（gnutella など）に一致するトラフィックを別のトラフィック クラスに配置できます。その後、各クラス内のネットワーク トラフィックには、トラフィック ポリシー（ポリシー マップ）を使用して適切な QoS 処理を適用できます。

トラフィックの分類に使用する基準を指定するには、**matchprotocol** コマンドを使用します。下の表に、使用可能な **matchprotocol** コマンドの一部と対応するプロトコルまたは NBAR で認識およびサポートされるトラフィック タイプを示します。

（注） NBAR でサポートされるプロトコル タイプの完全なリストについては、「NBAR を使用したネットワーク トラフィックの分類」モジュールを参照してください。

表 *10* : ***match protocol*** コマンドと対応するプロトコルまたはトラフィック タイプ

match protocol コマンド[1]	プロトコル タイプ
matchprotocol(NBAR)	NBAR がサポートするプロトコル タイプ
matchprotocolcitrix	Citrix プロトコル
matchprotocolfasttrack	FastTrack ピアツーピア トラフィック
matchprotocolgnutella	Gnutella ピアツーピア トラフィック

match protocol コマンド[1]	プロトコル タイプ
matchprotocolhttp	Hypertext Transfer Protocol
matchprotocolrtp	Real-Time Transport Protocol トラフィック
matchprotocolunknown [final]	すべての未知または未分類のトラフィック

[1] Cisco IOS の match protocol コマンドはリリースによって異なる可能性があります。詳細については、お使いの Cisco IOS Release のコマンド マニュアルを参照してください。

MQC を使用して NBAR を設定する方法

DSCP ベースのレイヤ 3 カスタム アプリケーションの設定

手順の概要

1. **enable**
2. **configureterminal**
3. **ipnbarcustom***name***transport** {**tcp** | **udp** | **udp-tcp** }**id***id*
4. **dscp***dscp-value*
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipnbarcustom***name***transport** {**tcp** | **udp** | **udp-tcp** }**id***id* 例： `Device(config)# ip nbar custom mycustom transport tcp id 100`	TCP、UDP、または TCP と UDP の両方と照合するようにトランスポート プロトコルを指定し、カスタム コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**dscp***dscp-value* 例： `Device(config-custom)# dscp ef`	DiffServ コード ポイント（DSCP）値を指定します。 （注） 2 つのカスタム アプリケーションに同じフィルタが存在する場合は、設定の順序に従って優先順位が設定されます。
ステップ 5	**exit** 例： `Device(config-custom)# exit`	カスタム コンフィギュレーション モードを終了します。

未分類トラフィックと不明トラフィックの管理

一部のプロトコルでは、NBAR 分類のために、複数のパケットを分析する必要があります。そのため、この分類が実行されるまでの間に送信されたパケットは、**unknown** と見なされます。**unknown final** は、一時的に分類されたパケットを除外し、NBAR 分類プロセス完了後に不明と判別されたパケットのみを含めます。

デフォルトでは、不明トラフィックと一致しないすべてのトラフィックが、MQC の場合と同様に、デフォルト クラスと一致します。

はじめる前に

NBAR が完全に設定されていること（つまり、Protocol Discovery およびその他）を確認します。NBAR が一部のプロトコル セットのみを照合するように設定されている場合は、すべての非アクティブ プロトコルが未分類トラフィック、つまり不明トラフィックと見なされます。

手順の概要

1. **enable**
2. **configureterminal**
3. **class-map** [**match-all** | **match-any**] **unknown**
4. **matchprotocolunknown[final]**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**class-map** [**match-all** | **match-any**] **unknown** 例： `Device(config)# class-map match-all my-unknown`	不明なトラフィックを新しいクラスと照合するために使用するクラス マップを作成し、クラスマップ コンフィギュレーション モードを開始します。
ステップ 4	**matchprotocolunknown[final]** 例： `Device(config-cmap)# match protocol unknown final`	不明なトラフィックを照合するように NBAR を設定します。 • **unknown** キーワードは、未分類のトラフィックを表します。 • **unknown final** は、NBAR によって不明と判別されたトラフィックを表します。
ステップ 5	**end** 例： `Device(config-cmap)# end`	（任意）特権 EXEC モードに戻ります。

この時点で、次のタスクを設定できます。

1. トラフィック ポリシーの設定
2. トラフィック ポリシーのインターフェイスまたはサブインターフェイスへの適用

トラフィック ポリシーの設定

ユーザが指定した基準に一致するトラフィックは特定のクラスに分類できます。また、そのクラスをポリシー マップに含めると、ユーザが定義した特定の QoS 処理が実行されます。

トラフィック ポリシーを設定するには、次の手順を実行します。

（注） **bandwidth** コマンドは手順 トラフィック ポリシーの設定 に記載されています。**bandwidth** コマンドは、QoS 機能の Class-Based Weighted Fair Queuing（CBWFQ）を設定します。CBWFQ は、設定できる QoS 機能の単なる一例です。使用する QoS 機能に適したコマンドを使用してください。Cisco IOS リリース 12.2(18)ZY の場合、Supervisor 32/Programmable Intelligent Services Accelerator（PISA）を搭載した Catalyst 6500 シリーズ スイッチで CBWFQ はサポートされません。

（注） Cisco IOS リリース 12.2(18)ZY の場合、既存のトラフィック ポリシーがすでにインターフェイスに適用されているときには、そのトラフィック ポリシー（ポリシーマップ）を変更できません。インターフェイスからポリシー マップを削除するには、**service-policy** コマンドの **no** 形式を使用します。

>

手順の概要

1. **enable**
2. **configureterminal**
3. **policy-map***policy-map-name*
4. **class** {*class-name* | **class-default**}
5. **bandwidth** {*bandwidth-kbps*| **remainingpercent***percentage*| **percent***percentage*}
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy-map***policy-map-name* 例： `Device(config)# policy-map policy1`	1 つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、policy-map コンフィギュレーションモードを開始します。 • ポリシー マップの名前を入力します。
ステップ 4	**class** {*class-name* | **class-default**} 例： `Device(config-pmap)# class class1`	作成または変更するポリシーのクラス名を指定し、ポリシーマップ クラス コンフィギュレーション モードを開始します。 • 特定のクラス名または **class-default** キーワードを入力します。
ステップ 5	**bandwidth** {*bandwidth-kbps*| **remainingpercent***percentage*| **percent***percentage*} 例： `Device(config-pmap-c)# bandwidth percent 50` 例：	（任意）ポリシーマップに属するクラスに割り当てる帯域幅を指定または変更します。 • kbps の数値、帯域幅の相対的な割合、または帯域幅合計の絶対値として、帯域幅の合計を入力します。 （注） **bandwidth** コマンドは、QoS 機能の Class-Based Weighted Fair Queuing（CBWFQ）を設定します。CBWFQ は、設定できる QoS 機能の単なる一例です。使用する QoS 機能に適したコマンドを使用してください。 （注） Cisco IOS リリース 12.2(18)ZY の場合、Supervisor 32/PISA を搭載する Catalyst 6500 シリーズ スイッチでは、CBWFQ はサポートされません。
ステップ 6	**end** 例： `Device(config-pmap-c)# end`	（任意）特権 EXEC モードに戻ります。

トラフィックポリシーのインターフェイスまたはサブインターフェイスへの適用

ポリシー マップの作成した後の次の手順は、トラフィック ポリシー（ポリシー マップとも呼ばれます）をインターフェイスまたはサブインターフェイスに適用する作業です。トラフィック ポリシーは、インターフェイスまたはサブインターフェイスの入力方向または出力方向に適用できます。

（注） 実際のネットワークの要件によっては、ATM PVC、フレームリレー データリンク接続識別子（DLCI）、または他のインターフェイス タイプにトラフィック ポリシーを適用する必要があります。

トラフィック ポリシー（ポリシーマップ）をインターフェイスに適用するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***typenumber* [*name-tag*]
4. **pvc** [*name*] *vpi*/*vci* [**ilmi**| **qsaal**| **smds**|**l2transport**]
5. **exit**
6. **service-policy** {**input** | **output**}*policy-map-name*
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface***typenumber* [*name-tag*] 例： `Device(config)# interface ethernet 2/4`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。 • インターフェイス タイプとインターフェイス番号を入力します。
ステップ 4	**pvc** [*name*] *vpi*/*vci* [**ilmi**| **qsaal**| **smds**|**l2transport**] 例： `Device(config-if)# pvc cisco 0/16`	（任意）名前を ATM PVC に作成または割り当て、ATM 相手先固定接続（PVC）でカプセル化を指定し、ATM 仮想回線コンフィギュレーション モード開始します。 • PVC 名、ATM ネットワーク仮想パス ID、およびネットワーク仮想チャンネル ID を入力します。 （注） この手順は、ポリシー マップを ATM PVC に適用する場合にのみ必要です。ポリシーマップを ATM PVC に適用しない場合は、トラフィック ポリシーのインターフェイスまたはサブインターフェイスへの適用 に進みます。
ステップ 5	**exit** 例： `Device(config-atm-vc)# exit`	（任意）インターフェイス コンフィギュレーション モードに戻ります。 （注） この手順は、ポリシー マップを ATM PVC に適用しており、トラフィック ポリシーのインターフェイスまたはサブインターフェイスへの適用 を完了している場合にのみ必要です。ポリシーマップを ATM PVC に適用しない場合は、トラフィック ポリシーのインターフェイスまたはサブインターフェイスへの適用 に進みます。
ステップ 6	**service-policy** {**input** | **output**}*policy-map-name* 例： `Device(config-if)# service-policy input policy1`	ポリシーマップ（トラフィック ポリシー）を入力または出力インターフェイスに適用します。 • **input** または **output** キーワードを指定し、ポリシー マップ名を入力します。 （注） ポリシー マップは、入力デバイスまたは出力デバイスで設定できます。また、入力方向または出力方向のインターフェイスにも適用できます。ポリシー マップを適用する方向（入力または出力）とデバイス（入力または出力）は、ネットワーク構成によって異なります。**service-policy** コマンドを使用してポリシーマップをインターフェイスに適用する場合は、ネットワーク構成に適したデバイスおよびインターフェイスの方向を選択してください。 （注） **service-policy** コマンドを使用すると、次のような 2 つのメッセージが表示されることがあります。 `%PISA-6-NBAR_ENABLED: feature accelerated on input direction of: [`*interface name and type*

	コマンドまたはアクション	目的
		] %PISA-6-NBAR_ENABLED: feature accelerated on output direction of: [*interface name and type* この両方のメッセージが表示されても、**input** または **output** キーワードで指定した方向のみで NBAR が有効化されます。
ステップ 7	**end** 例： `Device(config-if)# end`	（任意）特権 EXEC モードに戻ります。

MCQ を使用した NBAR の確認

トラフィック クラスおよびトラフィック ポリシー（ポリシー マップ）を作成した後は、予定どおりの結果になることを確認できます。つまり、トラフィックが適切に分類されること、および目的の QoS 処理が適用されることを確認できます。また、プロトコルからポートへのマッピングが適切であることを確認できます。

NBAR のトラフィック クラス、トラフィック ポリシー、およびプロトコルからポートへのマッピングを確認するには、次の手順を実行します。

手順の概要

1. **showclass-map** [*class-map-name*]
2. **showpolicy-map** [*policy-map*]
3. **showpolicy-mapinterface***typenumber*
4. **showipnbarport-map** [*protocol-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**showclass-map** [*class-map-name*] 例： `Device# show class-map`	（任意）すべてのクラスマップとその一致条件を表示します。 • （任意）特定のクラス マップの名前を入力します。

	コマンドまたはアクション	目的
ステップ 2	**showpolicy-map** [*policy-map*] 例： `Device# show policy-map`	（任意）指定したサービス ポリシー マップの全クラスの設定、またはすべての既存ポリシー マップに関する全クラスの設定を表示します。 • （任意）特定のポリシー マップの名前を入力します。
ステップ 3	**showpolicy-mapinterface***typenumber* 例： `Device# show policy-map interface Fastethernet 6/0`	（任意）指定したインターフェイスのすべてのポリシー マップについて、パケットとクラスの統計情報を表示します。 • インターフェイス タイプとインターフェイス番号を入力します。
ステップ 4	**showipnbarport-map** [*protocol-name*] 例： `Device# show ip nbar port-map`	（任意）NBAR に現在使用されているプロトコルからポートへのマッピングを表示します。 • （任意）プロトコル名を入力します。

未知および未分類のトラフィック管理の確認

不明トラフィックと未分類トラフィックの管理を確認するには、次の手順を実行します。

手順の概要

1. **show ip nbar protocol-id unknown**
2. **show ip nbar link-age unknown**
3. **show ip nbar protocol-attribute unknown**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**show ip nbar protocol-id unknown**
	
	例：
	
	`Device# show ip nbar protocol-id unknown`
	
	`Protocol Name id type`
	`---`
	`unknown 1 L7 STANDARD`
		（任意）不明トラフィックと未分類トラフィックのプロトコル分類 ID が表示されます。

	コマンドまたはアクション	目的

ステップ 2	**show ip nbar link-age unknown**
	
	例：
	
	`Device# show ip nbar link-age unknown`
	
	`Protocol  Link Age (seconds)`
	`unknown  60`
		（任意）不明トラフィックと未分類トラフィックのプロトコルリンク期間経過が表示されます。

ステップ 3	**show ip nbar protocol-attribute unknown**
	
	例：
	
	`Device# show ip nbar protocol-attribute unknown`
	
	`Protocol Name : unknown`
	`encrypted : encrypted-no`
	`tunnel : tunnel-no`
	`category : other`
	`sub-category : other`
	`application-group : other`
	`p2p-technology : p2p-tech-no`
		（任意）不明トラフィックと未分類トラフィックの設定済み属性のリストが表示されます。

DSCP ベースのレイヤ 3 カスタム アプリケーションの設定例

例：トラフィック クラスの設定

次の例では、cmap1 というクラスが設定されました。citrix プロトコルに一致するすべてのトラフィックは、cmap1 クラスに配置されます。

```
Device> enable
Device# configure terminal
Device(config)# class-map cmap1
Device(config-cmap)# match protocol citrix
Device(config-cmap)# end
```

例：トラフィック ポリシーの設定

次の例では、policy1 というトラフィック ポリシー（ポリシー マップ）が設定されました。policy1 には class1 というクラスが含まれ、class1 では CBWFQ がイネーブルです。

```
Device> enable
Device# configure terminal
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# bandwidth percent 50
Device(config-pmap-c)# end
```

（注） 上記の例では、Class-Based Weighted Fair Queuing（CBWFQ）を有効化するために **bandwidth** コマンドが使用されます。CBWFQ は、ポリシー マップで適用できる QoS 機能の一例です。使用する QoS 機能に適したコマンドを使用してください。Cisco IOS リリース 12.2(18)ZY の場合、Supervisor 32/PISA を搭載する Catalyst 6500 シリーズ スイッチでは、CBWFQ はサポートされません。

例：トラフィック ポリシーのインターフェイスまたはサブインターフェイスへの適用

次の例では、policy1 というトラフィック ポリシー（ポリシー マップ）が、インターフェイスの入力方向のイーサネット インターフェイス 2/4 に適用されました。

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 2/4

Device(config-if)# service-policy input policy1
Device(config-if)# end
```

例：NBAR のプロトコルからポートへのマッピングの確認

次の出力は、**showipnbarport-map** コマンドの出力例です。このコマンドは、NBAR に現在使用されているプロトコルからポートへのマッピングを表示します。この表示を使用して、マッピングが正しいことを確認します。

```
Device# show ip nbar port-map
port-map bgp      udp 179
port-map bgp      tcp 179
port-map cuseeme  udp 7648 7649
port-map cuseeme  tcp 7648 7649
port-map dhcp     udp 67 68
port-map dhcp     tcp 67 68
```

ipnbarport-map コマンドを使用した場合は、**showipnbarport-map** コマンドによって、プロトコルに割り当てられたポートが表示されます。

noipnbarport-map コマンドを使用した場合は、**showipnbarport-map** コマンドによって、デフォルトポートが表示されます。特定のプロトコルのマッピングのみを表示するには、**showipnbarport-map** コマンドで *protocol-name* 引数を指定します。

例：任意の IP ポートの L3 カスタム

```
Device> enable
Device# configuration terminal
Device (config)# ip nbar custom mycustom transport udp-tcp
Device(config-custom)# dscp ef
Device (config-custom)# exit
```

次の作業

アプリケーション認識モジュール（パケット記述言語モジュールまたは PCLM としても知られる）をネットワークに追加するには、『アプリケーション認識モジュールの追加』モジュールを参照してください。

カスタム プロトコルに基づいてネットワーク トラフィックを分類するには、『カスタム プロトコルの作成』モジュールを参照してください。

その他の参考資料

ここでは、MQC を使用した NBAR の設定に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
QoS コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Quality of Service Solutions Command Reference*』
Catalyst 6500 シリーズ スイッチの QoS の特性と機能	『*Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide*, Release 12.2ZY』の「Configuring PFC QoS」の章
MQC、トラフィック ポリシー（ポリシー マップ）、およびトラフィック クラス	「Applying QoS Features Using the MQC」モジュール
CBWFQ	「Configuring Weighted Fair Queueing」モジュール
NBAR に関する概念と情報	「NBAR を使用したネットワーク トラフィックの分類」モジュール
Protocol Discovery のイネーブル化に関する情報	「Enabling Protocol Discovery」モジュール
アプリケーション認識モジュール（PDLM とも呼ばれます）の追加に関する情報	「Adding Application Recognition Modules」モジュール
カスタム プロトコルの作成	「カスタム プロトコルの作成」モジュール

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

Configuring NBAR Using the MQC の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *11*：*Configuring NBAR Using the MQC* の機能情報

機能名	リリース	機能情報
NBAR MQC Support for Pre-resolved and Unknown Applications	IOS リリース 15.5(1)T IOS XE リリース 3.14S	NBAR MQC Support for Pre-resolved and Unknown Applications 機能は、MQC を使用したすべての不明トラフィックおよび未分類トラフィックの照合をサポートします。 次のコマンドが変更されました：**class-map**、**match protocol**
QoS：DirectConnect PDLM	12.4(4)T	DirectConnect プロトコルおよび Packet Description Language Module（PDLM）をサポートします。DirectConnect プロトコルは、MQC を使用してトラフィックを分類するときに認識できるようになります。 以下の項では、QoS：DirectConnect PDLM 機能に関する情報を提供します。

機能名	リリース	機能情報
QoS：Skype Classification	12.4(4)T	Skype プロトコルをサポートします。Skype プロトコルは、MQC を使用してトラフィックを分類するときに認識できるようになります。 （注） シスコは、現在 Skype Version 1 のみをサポートします。 以下の項では、QoS：Skype Classification 機能に関する情報を提供します。
NBAR--BitTorrent PDLM	12.4(2)T	BitTorrent PDLM とプロトコルをサポートします。BitTorrent プロトコルは、MQC を使用してトラフィックを分類するときに認識できるようになります。 NBAR–BitTorrent PDLM 機能については、以下のセクションで説明しています。
NBAR--Citrix ICA Published Applications	12.4(2)T	Citrix Independent Computing Architecture（ICA）が発行したアプリケーション名とタグ番号に基づいて、NBAR がトラフィックを分類できるようにします。 NBAR–Citrix ICA Published Application 機能については、以下のセクションで説明しています。
NBAR--Multiple Matches Per Port	12.4(2)T	TCP または UDP ポートの特定のアプリケーションのトラフィック ストリーム内で、属性の値を NBAR が区別できる機能を提供します。 NBAR–Multiple Matches Per Port 機能については、以下のセクションで説明しています。

機能名	リリース	機能情報
NBAR Extended Inspection for HTTP Traffic	12.3(4)T	NBAR は不明な TCP ポートをスキャンし、そのルータを通過する HTTP トラフィックを識別できます。 以下の項では、NBAR Extended Inspection for HTTP Traffic 機能に関する情報を示します。
NBAR Real-Time Transport Protocol Payload Classification	12.2(15)T	リアルタイム オーディオおよびビデオトラフィックのステートフル識別をイネーブルにします。 以下の項では、NBAR Real-Time Transport Protocol Payload Classification 機能に関する情報を提供します。
NBAR--Network-Based Application Recognition	12.2(18)ZYA	Supervisor 32/Programmable Intelligent Services Accelerator（PISA）を搭載した Catalyst 6500 シリーズ スイッチで NBAR と Firewall Service Module（FWSM）機能を統合します。NBAR で認識されるプロトコルが増えました。 以下の項では、NBAR 機能に関する情報を提供します。 次のコマンドが変更されました：**matchprotocol(NBAR)**。
NBAR--Network-Based Application Recognition (Hardware Accelerated NBAR)	12.2(18)ZY	Supervisor 32/Programmable Intelligent Services Accelerator（PISA）を搭載した Catalyst 6500 シリーズ スイッチで NBAR 機能を有効にします。 NBAR--Network-Based Application Recognition（Hardware Accelerated NBAR）機能については、次のセクションで説明しています。

第 7 章

DSCP ベースのレイヤ3カスタム アプリケーション

Network-Based Application Recognition（NBAR）は、カスタム プロトコルを使用した顧客固有のアプリケーションと NBAR でサポートされていないアプリケーションの識別をサポートします。IP アドレスおよびポートベースのカスタム プロトコルには、特定の TCP または UDP トランスポートを使用した IP サブネットまたは IP アドレス リストのサポートが含まれます。DSCP ベースのレイヤ 3 カスタム アプリケーション機能は、顧客がトラフィック内の DiffServ コード ポイント（DSCP）値を使用することにより、レイヤ 3 またはレイヤ 4 カスタム アプリケーションに属しているトラフィックを識別できるようにする機能強化です。

- 機能情報の確認，101 ページ
- DSCP ベースのレイヤ 3 カスタム アプリケーションの制約事項，102 ページ
- DSCP ベースのレイヤ 3 カスタム アプリケーションの概要，102 ページ
- NBAR2 auto-learn の設定方法，102 ページ
- DSCP ベースのレイヤ 3 カスタム アプリケーションの設定例，103 ページ
- DSCP ベースのレイヤ 3 カスタム アプリケーションに関する追加情報，104 ページ
- DSCP ベースのレイヤ 3 カスタム アプリケーションの機能情報，105 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

DSCP ベースのレイヤ 3 カスタム アプリケーションの制約事項

「DSCP ベースのレイヤ 3 カスタム アプリケーション」機能は、Differentiated Services Code Point（DSCP）分類をフローのプロパティとして扱い、フローの先頭パケットの DSCP 値のみを確認します。フローのさまざまなパケットを特定し、それらにポリシーを適用するには、**match dscp** コマンドを使用します。

DSCP ベースのレイヤ 3 カスタム アプリケーションの概要

Network-Based Application Recognition（NBAR）は、カスタム プロトコルを使用した顧客固有のアプリケーションと NBAR でサポートされていないアプリケーションの識別をサポートします。IP アドレスおよびポートベースのカスタム プロトコルには、特定の TCP または UDP トランスポートを使用した IP サブネットまたは IP アドレス リストのサポートが含まれます。DSCP ベースのレイヤ 3 カスタム アプリケーション機能は、顧客がトラフィック内の DiffServ コード ポイント（DSCP）値を使用することにより、レイヤ 3 またはレイヤ 4 カスタム アプリケーションに属しているトラフィックを識別できるようにする機能強化です。カスタムプロトコルトランスポートを定義するには、**ip nbar custom transport** コマンドのキーワードと引数を使用します。

NBAR2 auto-learn の設定方法

DSCP ベースのレイヤ 3 カスタム アプリケーションの設定

手順の概要

1. **enable**
2. **configureterminal**
3. **ipnbarcustom***name***transport** {**tcp** | **udp** | **udp-tcp** }**id***id*
4. **dscp***dscp-value*
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**ipnbarcustom***name***transport** {**tcp** | **udp** | **udp-tcp** }**id***id* 例： `Device(config)# ip nbar custom mycustom transport tcp id 100`	TCP、UDP、または TCP と UDP の両方と照合するようにトランスポート プロトコルを指定し、カスタム コンフィギュレーション モードを開始します。
ステップ 4	**dscp***dscp-value* 例： `Device(config-custom)# dscp ef`	DiffServ コード ポイント（DSCP）値を指定します。 （注） 2 つのカスタム アプリケーションに同じフィルタが存在する場合は、設定の順序に従って優先順位が設定されます。
ステップ 5	**exit** 例： `Device(config-custom)# exit`	カスタム コンフィギュレーション モードを終了します。

DSCP ベースのレイヤ 3 カスタム アプリケーションの設定例

例：DSCP ベースのレイヤ 3 カスタム アプリケーション

```
Device> enable
Device# configuration terminal
Device (config)# ip nbar custom mycustom transport tcp id 100
Device(config-custom)# dscp ef
Device (config-custom)# exit
```

例：任意の IP ポートの L3 カスタム

```
Device> enable
Device# configuration terminal
Device (config)# ip nbar custom mycustom transport udp-tcp
Device(config-custom)# dscp ef
Device (config-custom)# exit
```

DSCP ベースのレイヤ 3 カスタム アプリケーションに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
QoS コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『Cisco IOS Quality of Service Solutions Command Reference』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

DSCP ベースのレイヤ 3 カスタム アプリケーションの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *12*：*DSCP* ベースのレイヤ *3* カスタム アプリケーションの機能情報

機能名	リリース	機能情報
L3 custom any IP/Port	Cisco IOS XE 3.16S	NBAR では、カスタム プロトコルを使用して、顧客特定のアプリケーションおよび NBAR でサポートされないアプリケーションを識別できます。IP アドレスおよびポートベースのカスタム プロトコルには、特定の TCP または UDP または TCP と UDP のトランスポートを使用した IP サブネットまたは IP アドレス リストのサポートが含まれます。DSCP ベースのレイヤ 3 カスタム アプリケーション機能は、顧客がトラフィック内の DSCP 値を使用してレイヤ 3 またはレイヤ 4 のカスタム アプリケーションに属するトラフィックを識別できる拡張機能です。 L3 custom any IP/Port 機能は、ユーザが UDP/TCP 以外または UDP と TCP の両方の転送で L3 または L4 カスタム アプリケーションを設定できる拡張機能です。 次のコマンドが導入または変更されました： **ip nbar custom**

第 8 章

トランスポート階層に基づく MQC

トランスポート階層（TPH）に基づく MQC 機能は、TPH を使用して、HTTP 経由の電子メールアプリケーションのように最後に分類されたプロトコルにのみ従うのではなく、特定の基礎となるプロトコルに従ってポリシーを適用できるようにします。クラス マップ内で設定された新しい MQC フィルタは、階層内のこのプロトコルを含むすべてのトラフィックを照合します。

- 機能情報の確認，107 ページ
- トランスポート階層に基づく MQC の制限事項，108 ページ
- トランスポート階層に基づく MQC に関する情報，108 ページ
- トランスポート階層に基づく MQC の設定方法，109 ページ
- トランスポート階層に基づく MQC の設定例，112 ページ
- その他の参考資料，113 ページ
- トランスポート階層に基づく MQC の機能情報，113 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

トランスポート階層に基づく MQC の制限事項

- 「トランスポート階層に基づく MQC」機能は、DNS、HTTP、RTP および SSL のみでサポートされます。
- 同じ class-map に ptotocol と in-app-hierarchy の match を追加することはできません。
- match protocol attribute tunnel が設定されている場合、異なる class-map 上であっても、match protocol http in-app-hierarchy および match protocol rtp in-app-hierarchy はサポートされません。

トランスポート階層に基づく MQC に関する情報

トランスポート階層に基づく MQC の概要

トランスポート階層（TPH）に基づく MQC 機能は、NBAR が TPH を使用して、最後に分類されたプロトコルにのみ従うのではなく、特定の基礎となるプロトコルに従ってポリシーを適用できるようにします。特定のアプリケーションの TPH は、そのアプリケーションが配信されるプロトコルのスタックです。たとえば、アプリケーションが HTTP 経由で転送されながら、HTTP が TCP 上で動作します。

トランスポート階層（TPH）に基づく MQC 機能の設定前は、**match protocol***protocol-id* クラスマップフィルタを使用して最後に分類されたプロトコルにクラスマップフィルタを適用することしかできません。ただし、HTTP のすべてのトラフィックに QoS ポリシーを適用してから、HTTP 経由で動作するすべてのプロトコルをクラスマップに含めると、このようなユースケースの設定が非常に困難になります。この問題の解決策が、TPH を使用して、最後に分類されたプロトコルにのみ従うのではなく、特定の基礎となるプロトコルに従ってポリシーを適用する in-app-hierarchy クラスマップ フィルタです。たとえば、階層内に HTTP が存在する場合は、ルールの **match protocol***http* **in-app-hierarchy** が一致します。

トランスポート階層に基づく MQC の設定方法

トランスポート階層に基づく MQC の設定

手順の概要

1. **enable**
2. **configureterminal**
3. **class-map**[**match-all** | **match-any**] *class-map-name*
4. **matchprotocol***protocol-name***in-app-hierarchy**
5. **end**
6. **configureterminal**
7. **policy-map***policy-map-name*
8. **class** {*class-name* | **class-default** }
9. **end**
10. **configureterminal**
11. **interface***type number*
12. **service-policy** {**input** | **output**} *policy-map-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map**[**match-all** | **match-any**] *class-map-name* 例： `Device(config)# class-map match-all C1`	指定したクラスとパケットの照合に使用されるクラスマップを作成し、QoS クラスマップ モードを開始します。 • クラス マップの名前を入力します。

	コマンドまたはアクション	目的
ステップ 4	**matchprotocol***protocol-name***in-app-hierarchy** 例： `Device(config-cmap)# match protocol http in-app-hierarchy`	指定されたプロトコルに基づいて、クラスマップの一致基準を設定します。トランスポート階層にプロトコルが存在する場合は、キーワード **in-app-hierarchy** が照合されます。 *protocol-name* に指定できる値：DNS、HTTP、RTP、SSL
ステップ 5	**end** 例： `Device(config-cmap)# end`	クラスマップ モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 7	**policy-map***policy-map-name* 例： `Device(config)# policy-map P1`	ポリシーマップの名前を指定して、ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 8	**class** {*class-name* | **class-default** } 例： `Device(config-pmap)# class C1`	作成するポリシーのクラス名を指定し、ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 9	**end** 例： `Device(config-cmap)# end`	クラスマップ モードを終了し、特権 EXEC モードに戻ります。
ステップ 10	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 11	**interface***type number* 例： `Device(config)# interface GigabitEthernet 0/0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 12	**service-policy** {**input** | **output**} *policy-map-name* 例： `Device(config-if)# service-policy input P1`	インターフェイスの入力方向または出力方向にアタッチするポリシー マップの名前を指定します。

トランスポート階層に基づく MQC の確認

トランスポート階層機能に基づいて MQC 機能を確認するには、次の手順を実行します。

手順の概要

1. **enable**
2. **showpolicy-mapinterface***typenumber*
3. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	（任意）特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showpolicy-mapinterface***typenumber* 例： `Device# show policy-map interface GigabitEthernet0/0/1`	指定したインターフェイスのすべてのサービス ポリシーに設定されたすべてのクラスのパケット統計情報を表示します。 • インターフェイスタイプとインターフェイス番号を入力します。
ステップ 3	**exit** 例： `Device# exit`	（任意）特権 EXEC モードを終了します。

トランスポート階層に基づく MQC の設定例

例：トランスポート階層に基づく MQC の設定

次に、トランスポート階層機能に基づいた MQC の設定例を示します。

```
Device> enable
Device# configure terminal
Device(config)# class-map match-all C1
Device(config-cmap)# match protocol http in-app-hierarchy
Device(config-cmap)# match protocol youtube
Device(config-cmap)# end
Device# configure terminal
Device(config)# policy-map P1
Device(config-pmap)# class C1
Device(config-cmap)# end
Device# configure terminal
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# service-policy input P1
```

P1 というトラフィック ポリシーを設定します。たとえば、P1 に、QoS 帯域幅制限を設定する C1 というクラスを含めます。トランスポートが HTTP の YouTube が最終分類になるすべてのトラフィックは、C1 クラスに配置されます。Youtube の他の可能なトランスポート（DNS、SSL、RTSP など）は、このクラス マップに一致しません。

例：トランスポート階層に基づく MQC の設定の確認

次は、**showpolicy-mapinterface** コマンドのサンプル出力です。

```
Device#  show policy-map interface GigabitEthernet0/0/1

GigabitEthernet0/0/1
  Service-policy input: P1

Class-map: C1 (match-all)
      17 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: protocol http in-app-hierarchy
      Match: protocol youtube

    Class-map: class-default (match-any)
      3 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
QoS コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『Cisco IOS Quality of Service Solutions Command Reference』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

トランスポート階層に基づく MQC の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *13*：トランスポート階層に基づく *MQC* の機能情報

機能名	リリース	機能情報
トランスポート階層に基づく MQC	Cisco IOS XE 3.14S	トランスポート階層に基づく MQC 機能を使用すると、Transport Hierarchy によって、最後に分類されたプロトコルのみに従うのではなく、基になる特定のプロトコルに従ってポリシーを適用できます。クラスマップ内で設定できる新しい MQC フィルタが導入されます。 次のコマンドが変更されました。 **match protocol**
Transport Hierarchy による DNS のサポート	Cisco IOS XE Denali 16.3	**match protocol** CLI は、DNS、HTTP、SSL、および RTP の各プロトコル タイプに従って照合できます。例：**match protocol dns in-app-hierarchy**

第 9 章

NBAR の分類と属性

NBAR の分類と属性機能は、application-group、category、sub-category、encrypted、tunnel などの静的に割り当てられた属性に基づいてプロトコルまたはアプリケーションを照合するメカニズムを提供します。プロトコルとアプリケーションをさまざまなグループに分類することにより、レポート作成や Quality of Service（QoS）ポリシーの適用が容易になります。

- 機能情報の確認，115 ページ
- NBAR2 カスタム プロトコルに関する情報，116 ページ
- NBAR2 カスタム プロトコルの設定方法，118 ページ
- NBAR2 カスタム プロトコルの設定例，120 ページ
- NBAR2 カスタム プロトコルに関する追加情報，122 ページ
- NBAR の分類と属性の機能情報，122 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

NBAR2 カスタム プロトコルに関する情報

NBAR の分類と属性

NBAR の分類と属性機能は、特定の属性に基づいてプロトコルまたはアプリケーションを照合するメカニズムを提供します。プロトコルとアプリケーションをさまざまなグループに分類することにより、それらに対する QoS ポリシーの適用などのグループ アクションのレポートや実行が容易になります。属性は、プロトコルまたはアプリケーションごとに静的に割り当てられ、トラフィックには依存しません。次の属性が **match protocol attribute** コマンドを使用した一致基準の設定に使用できます。

- **application-group**：**application-group** キーワードは、条件に基づいてグループ化したアプリケーションの設定を可能にします。たとえば、Yahoo-Messenger、Yahoo-VoIP-messenger、および Yahoo-VoIP-over-SIP は、yahoo-messenger-group の下にまとめてグループ化されます。
- **category**：**category** キーワードは、各プロトコルについて、最初の分類レベルの条件に基づいてグループ化されたアプリケーションの設定を可能にします。類似したアプリケーションが 1 つのカテゴリにまとめてグループ化されます。たとえば、電子メール カテゴリには、Internet Mail Access Protocol（IMAP）、Simple Mail Transfer Protocol（SMTP）、Lotus Notes などのすべての電子メール アプリケーションが含まれます。
- **sub-category**：**sub-category** キーワードは、一致基準としての各プロトコルの分類の 2 つ目のレベルに基づいてグループ化されたアプリケーションを設定するオプションを提供します。たとえば、clearcase、dbase、rda、mysql、その他のデータベース アプリケーションはデータベース グループにグループ化されます。
- **encrypted**：**encrypted**キーワードは、一致基準としてのプロトコルが暗号化プロトコルなのかどうかに基づいてグループ化されたアプリケーションを設定するオプションを提供します。アプリケーションは、その暗号化ステータスと非暗号化ステータスに基づいてまとめてグループ化されます。NBAR が値を指定しないプロトコルは、未割り当ての暗号化グループに分類されます。
- **tunnel**：**tunnel** キーワードは、プロトコルが他のプロトコルのトラフィックをトンネルするかどうかに基づいてプロトコルを設定するオプションを提供します。NBAR が値を指定しないプロトコルは、未割り当てのトンネル グループに分類されます。たとえば、レイヤ 2 トンネリング プロトコル（L2TP）などです。
- **p2p-technology**：**p2p（ピアツーピア）-technology** 属性は、プロトコルが p2p テクノロジーを使用するかどうかを指定するオプションを提供します。

（注） 属性ベースのプロトコル照合設定は、レポートまたは Protocol Discovery 情報内の分類の粒度に影響しません。

application-group、category、および sub-category の各属性にカスタム値を作成できます。カスタム値を使用すれば、プロトコルのグループ化に基づいて属性に名前を付けることができます。application-group、category、および sub-category の各属性にカスタム値を追加するには、それぞれ **ip nbar attribute application-group custom application-group-name**、**ip nbar attribute category custom category-name**、および **ip nbar attribute sub-category custom sub-category-name** コマンドを使用します。

動的に作成されたカスタム属性値は、**ip nbar attribute-map** コマンドを使用する際の属性マップの作成に使用したり、**match protocol attribute** コマンドを使用する際のクラスマップの一致基準の設定に使用したりできます。

show ip nbar attribute-custom コマンドの出力には、属性に対して定義可能なカスタム値の数と、現在定義されているカスタム値が表示されます。**show ip nbar attribute** コマンドは、NBAR で使用されるカスタム属性を含むすべての属性を表示します。

カスタム値を削除するには、**no ip nbar attribute** コマンドを使用します。

NBAR2 カスタム プロトコルの概要

Network-Based Application Recognition（NBAR）は、カスタム プロトコルを使用したカスタム アプリケーションの識別をサポートします。カスタム プロトコルは、NBAR でサポートされないスタティック ポートベースのプロトコルとアプリケーションをサポートします。

カスタムプロトコルの詳細については、「カスタムプロトコルの作成」モジュールを参照してください。

NBAR2 カスタム プロトコルの設定方法

NBAR 属性のカスタマイズ

手順の概要

1. **enable**
2. **configureterminal**
3. **ip nbar attribute-map** *profile-name*
4. [**attributecategory** *category-name*]
5. [**attributesub-category** *sub-category-name*]
6. [**attributeapplication-group** *application-group-name*]
7. [**attributetunnel** *tunnel-info*]
8. [**attributeencrypted** *encrypted-info*]
9. [**attributetraffic-class** *traffic-class*]
10. [**attributebusiness-relevance** *business-relevance*]
11. [**attributep2p-technology** *p2p-technology-info*]
12. **ip nbar attribute-set** *protocol-name profile-name*
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nbar attribute-map** *profile-name* 例： `Device(config)# ip nbar attribute-map actdir-attrib`	指定した名前で属性プロファイルを作成し、属性マップ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	[**attributecategory** *category-name*] 例： `Device(config-attribute-map)# attribute category net-admin`	アプリケーショングループ属性の属性値をプロファイルに追加します。
ステップ 5	[**attributesub-category** *sub-category-name*] 例： `Device(config-attribute-map)# attribute sub-category network-management`	サブカテゴリ属性の属性値をプロファイルに追加します。
ステップ 6	[**attributeapplication-group** *application-group-name*] 例： `Device(config-attribute-map)# attribute application-group other`	アプリケーショングループ属性の属性値をプロファイルに追加します。
ステップ 7	[**attributetunnel** *tunnel-info*] 例： `Device(config-attribute-map)# attribute tunnel no`	トンネル属性の属性値をプロファイルに追加します。
ステップ 8	[**attributeencrypted** *encrypted-info*] 例： `Device(config-attribute-map)# attribute encrypted no`	暗号化属性の属性値をプロファイルに追加します。
ステップ 9	[**attributetraffic-class** *traffic-class*] 例： `Device(config-attribute-map)# attribute traffic-class multimedia-conferencing`	トラフィッククラス属性の属性値をプロファイルに追加します。
ステップ 10	[**attributebusiness-relevance** *business-relevance*] 例： `Device(config-attribute-map)# attribute business-relevance business-relevant`	ビジネス関連属性の属性値をプロファイルに追加します。

	コマンドまたはアクション	目的
ステップ 11	[**attributep2p-technology** *p2p-technology-info*] 例： `Device(config-attribute-map)# attribute p2p-technology no`	p2p テクノロジー属性の属性値をプロファイルに追加します。
ステップ 12	**ip nbar attribute-set** *protocol-name profile-name* 例： `Device(config-attribute-map)# ip nbar attribute-set active-directory actdir-attrib`	指定されたプロファイルの属性値を指定されたプロトコルに追加します。
ステップ 13	**end** 例： `Device(config-attribute-map)# end`	特権 EXEC モードに戻ります。

NBAR2 カスタム プロトコルの設定例

例：属性のカスタム値の追加

次に、アプリケーション グループ属性、カテゴリ属性、およびサブカテゴリ属性のカスタム値を追加する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip nbar attribute application-group custom Home_grown_finance_group "our
finance tools network traffic"
Device(config)# ip nbar attribute category custom dc_backup_category "Data center backup
traffic"
Device(config)# ip nbar attribute sub-category custom hr_sub_category "HR custom applications
 traffic"
Device(config)# exit
```

例：属性のカスタム値に関する情報の表示

次の **showipnbarattribute-custom** コマンドの出力例では、定義可能なカスタム値の数と、属性に現在定義されているカスタム値が表示されています。

```
Device# show ip nbar attribute-custom

                  Name :  category
```

```
                 Help :  category attribute
   Custom Groups Limit :  1
 Custom Groups Created :  dc_backup_category

                 Name :  sub-category
                 Help :  sub-category attribute
   Custom Groups Limit :  1
 Custom Groups Created :  hr_sub_category

                 Name :  application-group
                 Help :  application-group attribute
   Custom Groups Limit :  1
 Custom Groups Created :  Home_grown_finance_group
```

次の **showipnbarattribute category** コマンドの出力例では、カテゴリ属性に関する詳細が表示されています。

```
Device# show ip nbar attribute category

      Name :  category
      Help :  category attribute
      Type :  group
    Groups :  newsgroup
           :  instant-messaging
           :  net-admin
           :  trojan
           :  email
           :  file-sharing
           :  industrial-protocols
           :  business-and-productivity-tools
           :  internet-privacy
           :  social-networking
           :  layer3-over-ip
           :  obsolete
           :  streaming
           :  location-based-services
           :  voice-and-video
           :  other
           :  gaming
           :  browsing
           :  dc_backup_category
   Need :  Mandatory
   Default :  other
```

例：プロファイルの作成およびプロファイルの属性の設定

次に、Network News Transfer Protocol（NNTP）用に設定した属性がある属性プロファイルを作成する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip nbar attribute-map nntp-attrib
Device(config-attribute-map)# attribute category newsgroup
Device(config-attribute-map)# attribute application-group nntp-group
Device(config-attribute-map)# attribute tunnel tunnel-no
Device(config-attribute-map)# attribute encrypted encrypted-yes
Device(config-attribute-map)# attribute p2p-technology p2p-tech-no
Device(config-attribute-map)# end
```

次に、上記の設定を確認する例を示します。

```
Device> enable
Device# show ip nbar attribute-map nntp-attrib
Device# Profile Name :  nntp-attrib
            category :  newsgroup
```

```
   application-group :  nntp-group
           encrypted :  encrypted-yes
Device# end
```

例：属性プロファイルのプロトコルへの適用

次に、属性プロファイルをアプリケーション通信プロトコル（ACP）のプロトコルに設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip nbar attribute-set acp test-profile
Device(config)# exit
```

NBAR2 カスタム プロトコルに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS LAN スイッチング コマンド	『Cisco IOS LAN Switching Command Reference』
Cisco IOS QoS 構成情報	『*QoS Configuration Guide*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

NBAR の分類と属性の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを

示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *14*：*NBAR2* カスタム プロトコルの機能情報

機能名	リリース	機能情報
NBAR の分類と属性	Cisco IOS XE リリース 3.4S	この機能は、Cisco ASR 1000 シリーズ アグリゲーション サービスルータに導入されました。 次のコマンドが導入または変更されました：**ip nbar custom**
NBAR2 カスタム プロトコル	Cisco IOS XE リリース 3.8S	NBAR2 カスタム プロトコル機能は、プロトコルの属性プロファイルを設定し、プロファイルをプロトコルにマップします。 次のコマンドが導入または変更されました：**ip nbar attribute-map**、**ip nbar attribute-set**。

第 10 章

Flexible NetFlow により抽出したフィールドの報告

「Flexible NetFlow により抽出したフィールドの報告」機能により、Network Based Application Recognition（NBAR）は Subapplication テーブル フィールドを Flexible NetFlow によりコレクタに送信することができます。

- 機能情報の確認，125 ページ
- Flexible NetFlow 経由で抽出したフィールドのレポートに関する情報，126 ページ
- Flexible NetFlow 経由で抽出したフィールドのレポート方法，126 ページ
- Flexible NetFlow 経由で抽出したフィールドをレポートするための設定例，127 ページ
- その他の参考資料，127 ページ
- Reporting Extracted Fields Through Flexible NetFlow の機能情報，129 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

Flexible NetFlow 経由で抽出したフィールドのレポートに関する情報

Subapplication テーブルのフィールド

optionsub-application-table コマンドを使用して、オプション テーブルを周期的にコレクタに送信し、それによりコレクタがフロー レコードで提供される NBAR サブアプリケーション タグ、サブアプリケーション名およびサブアプリケーションの説明をアプリケーション ID にマッピングできるようにします。

Flexible NetFlow 経由で抽出したフィールドのレポート方法

Subapplication テーブルのフィールドのレポート

手順の概要

1. **enable**
2. **configureterminal**
3. **flowexporter***exporter-name*
4. **optionsub-application-table**
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**flowexporter***exporter-name* 例： `Device(config)# flow exporter EXPORTER-1`	Flexible NetFlow フローエクスポータ コンフィギュレーション モードを開始します。
ステップ 4	**optionsub-application-table** 例： `Device(config-flow-exporter)# option sub-application-table`	オプション テーブルが定期的に送信されます。このオプションテーブルを使用して、コレクタはフロー レコードに記録されている NBAR サブアプリケーション タグ、サブアプリケーション名、およびサブアプリケーションの説明をアプリケーション ID にマッピングします。
ステップ 5	**exit** 例： `Device(config-flow-exporter)# exit`	Flexible NetFlow フローエクスポータ コンフィギュレーションモードを終了して、グローバル コンフィギュレーションモードに戻ります。

Flexible NetFlow 経由で抽出したフィールドをレポートするための設定例

例：Subapplication フィールドのレポート

次の例では、オプション テーブルの定期的な送信を有効化し、コレクタが、NBAR サブアプリケーションタグ、サブアプリケーション名、およびフロー レコードで提供されたサブアプリケーションの説明をアプリケーション ID にマッピングできるようにする方法を示します。

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# option sub-application-table
```

その他の参考資料

ここでは、MQC を使用した NBAR の設定に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
QoS コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Quality of Service Solutions Command Reference*』
Catalyst 6500 シリーズ スイッチの QoS の特性と機能	『*Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide*, Release 12.2ZY』の「Configuring PFC QoS」の章
MQC、トラフィック ポリシー（ポリシー マップ）、およびトラフィック クラス	「Applying QoS Features Using the MQC」モジュール
CBWFQ	「Configuring Weighted Fair Queueing」モジュール
NBAR に関する概念と情報	「NBAR を使用したネットワーク トラフィックの分類」モジュール
Protocol Discovery のイネーブル化に関する情報	「Enabling Protocol Discovery」モジュール
アプリケーション認識モジュール（PDLM とも呼ばれます）の追加に関する情報	「Adding Application Recognition Modules」モジュール
カスタム プロトコルの作成	「カスタム プロトコルの作成」モジュール

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

Reporting Extracted Fields Through Flexible NetFlow の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *15*：***Reporting Extracted Fields Through Flexible NetFlow*** の機能情報

機能名	リリース	機能情報
Flexible NetFlow により抽出したフィールドの報告	Cisco IOS XE リリース 3.7	Reporting Extracted Fields Through Flexible NetFlow 機能を使用すると、NBAR が Flexible NetFlow 経由で Subapplication テーブル フィールドをコレクタへ送信できます。 次のコマンドが導入または変更されました：**option (Flexible NetFlow)**。

第 11 章

NBAR プロトコル パック自動更新

シスコでは、NBAR2 トラフィックの認識機能を継続的に改善するために、長寿命に指定された Cisco IOS リリース用の NBAR2 プロトコル パックの定期更新を提供しています。プロトコル パック自動更新機能は、最新の互換性のあるプロトコル パックを使用した任意の数の参加ルータの更新に役立ちます。

利点

- **自動化**：新しいプロトコル パックが入手可能になったら、そのプロトコル パックのインストール ファイルをそれぞれのルータから到達可能なサーバにダウンロードし、単純な設定ファイル内でファイル パスを指定します。自動更新が有効になっているネットワーク内のルータがサーバを定期的にチェックします。新しいプロトコル パックが入手可能で互換性がある場合は、ルータが自動的にプロトコル パック ファイルをダウンロードしてインストールします。
- **中央集中型システム管理**：プロトコル パック自動更新は、強力なツールをネットワーク管理者に提供します。管理者は、1 つの中央集中型設定ファイルを使用して、任意の数のデバイス上でのプロトコル パックの導入を制御できます。

プロトコル パック自動更新のセットアップ

プロトコル パック自動更新をセットアップするには、自動更新に参加する各ルータ上でのいくつかの簡単な手順と、中央集中型アクティビティを管理するための 2 台のサーバ（または両方の役割を実行する 1 台のサーバ）のセットアップが必要です。詳細については、NBAR プロトコル パック自動更新の導入，（132 ページ）を参照してください。

デバイス OS のアップグレード時

原則として、プロトコル パックのインストール ファイルは、特定の Cisco IOS リリースを実行している特定のプラットフォーム タイプとしか互換性がありません。そのため、プロトコル パック自動更新に参加しているルータの OS をアップグレードした場合は、新しいリリースをサポートするために新しいプロトコル パックのインストール ファイルをダウンロードしてプロトコル パック自動更新設定に追加する必要があります。これには、後述する、プロトコル パック サー

バ上での新しいファイルの保存と、新しくダウンロードしたファイルを追加するための設定ファイルの更新が含まれます。

ルータを新しいメジャー リリースにアップグレードした後、**show ip nbar version** コマンドを使用して NBAR ソフトウェア バージョンを表示します。次の例では、NBAR ソフトウェア バージョンが 23 になっています。

```
ASR1004#show ip nbar version

NBAR software version:  23
NBAR minimum backward compatible version:  21

Loaded Protocol Pack(s):

Name:                           Advanced Protocol Pack
Version:                        14.0
Publisher:                      Cisco Systems Inc.
NBAR Engine Version:            23
State:                          Active
```

NBAR ソフトウェア バージョンが変更された場合は、最新の互換性のあるプロトコル パックがリリースに使用できるかどうかを確認します。該当する場合は、プロトコル パック自動更新で使用する新しいプロトコル パックのインストール ファイルをダウンロードします。

（注） プロトコルパックのリリースについては、NBAR2 Protocol Library ページを参照してください。

- NBAR プロトコル パック自動更新の導入，132 ページ
- プロトコル パック自動更新のための送信元サーバのセットアップ，134 ページ
- プロトコル パック自動更新のためのプロトコル パック サーバの設定，135 ページ
- プロトコル パック自動更新の設定ファイル，136 ページ
- プロトコル パック自動更新の有効化，141 ページ
- プロトコル パック自動更新の無効化，142 ページ
- 自動更新によるプロトコル パック更新の即時開始，142 ページ
- プロトコル パック自動更新情報の表示，143 ページ
- ルータでのローカル プロトコル パック自動更新の設定，144 ページ

NBAR プロトコル パック自動更新の導入

要素

プロトコルパック自動更新を使用するには、2 つのサーバまたは両方の機能を提供する 1 つのサーバと、任意の数の参加するルータが必要です。

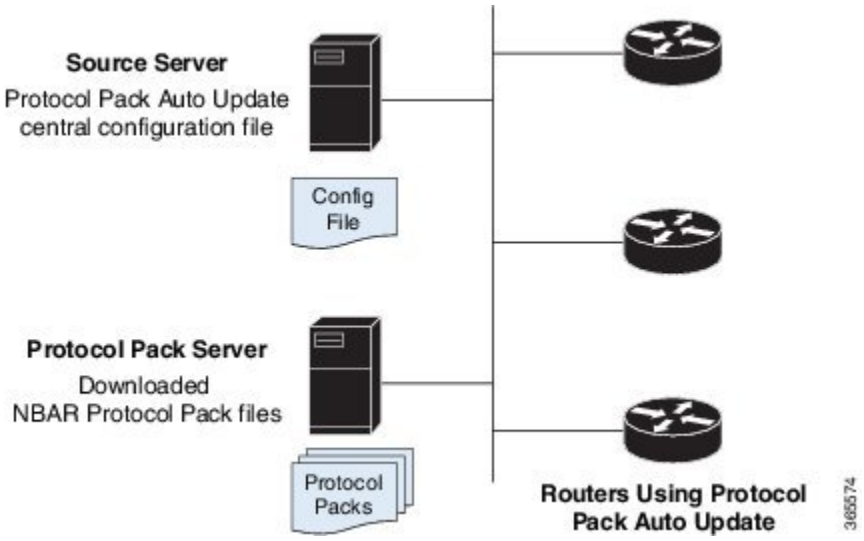
- **プロトコル パック サーバ**には次が含まれます。

- ダウンロードしたプロトコル パックのインストール用ファイル。プロトコル パック自動更新に参加する各ルータの最新プロトコル パックをダウンロードします。

- **送信元サーバ**には次が含まれます。
  - プロトコル パック自動更新の設定についての詳細を指定する設定ファイル（NBAR_PROTOCOL_PACK_DETAILS.json）：プロトコル パック サーバの場所、プロトコル パック ファイルの場所およびプロトコル パック自動更新の設定。
  - プロトコル パック自動更新のログ ファイル。

- **ルータ**：プロトコル パック自動更新が有効にされた 1 つ以上の参加するルータ（プロトコル パック自動更新の有効化，（141 ページ）を参照してください）。

図 *2*：プロトコル パック自動更新



導入手順

1. **プロトコル パック サーバ**を設定します。このサーバは、参加するルータから到達可能である必要があります。全ての参加するルータの最新プロトコルパック ファイルをダウンロードし、サーバにファイルを保存します。（『NBAR2 プロトコル パックのライブラリ』を参照してください）。設定ファイルで指定できるように、ファイルの場所を記録します。

   プロトコル パック自動更新のためのプロトコル パック サーバの設定，（135 ページ）を参照してください。

2. **送信元サーバ**を設定します。このサーバは、参加するルータから到達可能である必要があります。サーバで、JSON 形式の設定ファイルを作成します。

   プロトコル パック自動更新のための送信元サーバのセットアップ，（134 ページ）を参照してください。

（注） 単一サーバは、**プロトコル パック サーバ**と**送信元サーバ**の両方の機能を実行できます。

3 参加するルータ上で、プロトコルパック自動更新を有効にし、送信元サーバの場所と設定ファイルを含むディレクトリのパスを指定します。

プロトコル パック自動更新の有効化，（141 ページ）およびプロトコル パック自動更新の設定ファイル，（136 ページ） を参照してください。

例：

```
Device#configure terminal
Device(config)#ip nbar protocol-pack-auto-update
Device(config-pp-auto-update)#source-server tftp://10.20.300.400/NbarAutoUpdate
Device(config-pp-auto-update)#exit
```

4 （オプション）必要に応じて、個々のルータ上でプロトコル パック自動更新 CLI コマンドを使用し、設定ファイルで指定された設定をローカルで上書きします。

ルータでのローカル プロトコル パック自動更新の設定，（144 ページ）を参照してください。

5 新しいプロトコル パック リリースが利用可能になった場合、それを**プロトコル パック サーバ**にダウンロードし、その場所を**送信元サーバ**の設定ファイルに追加します。

（注） ルータを新しいメジャー リリースにアップグレードした後、**show ip nbar version** コマンドを使用して NBAR ソフトウェア バージョンを表示します。NBAR ソフトウェア バージョンが変更されている場合、新しいバージョンをサポートするプロトコル パックをダウンロードします。ファイルをプロトコル パック サーバに保存し、新しいプロトコル パック ファイルの場所を含むように設定ファイルを更新します。

プロトコルパック自動更新のための送信元サーバのセットアップ

プロトコル パック自動更新のために**送信元サーバ**をセットアップするには、次の手順を実行します。（プロトコル パック自動更新のためのプロトコル パック サーバの設定，（135 ページ）も参照してください）。

（注） 単一サーバは、プロトコル パック サーバと送信元サーバの両方の機能を実行できます。

1 サーバは、すべての参加するルータから到達可能なネットワークの場所に設定します。

2 サーバのディレクトリ（たとえば、/NbarAutoUpdate）内に、NBAR_PROTOCOL_PACK_DETAILS.json という名前の JSON ファイルを作成します。これは、JSON 形式のコンフィギュレーション ファイルであり、参加しているルータ上のプロトコル パック自動更新機能を制御します。

プロトコル パック自動更新の設定ファイル，（136 ページ）を参照してください。

3 サーバのネットワークの場所、およびコンフィギュレーション ファイルが含まれているディレクトリのパスをメモしておきます。参加しているルータ上の**送信元サーバ**を指定するときに、この場所を使用します。パスにコンフィギュレーション ファイル名を含めないでください。

例：tftp://10.20.300.400/NbarAutoUpdate

プロトコル パック自動更新のためのプロトコル パック サーバの設定

プロトコル パック自動更新のために**プロトコル パック サーバ**を設定するには、次の手順を実行します。（プロトコルパック自動更新のための送信元サーバのセットアップ，（134ページ）も参照してください）。

（注） 単一サーバは、**プロトコル パック サーバ**と**送信元サーバ**の両方の機能を実行できます。

1 サーバは、すべての参加するルータから到達可能なネットワークの場所に設定します。

2 IP アドレスやディレクトリ構造などプロトコル パック サーバの詳細は、インストールによって異なります。これらの詳細は、設定ファイルで指定されます。プロトコル パック サーバ上で、プロトコル パック ファイルを保存するベース ディレクトリとして次のような直感的なパスを作成します。

```
/NbarAutoUpdate/pp_server/
```

3 プロトコルパック自動更新に参加するルータに必要なプロトコルパック ファイルをダウンロードします。サーバに保存します。

次に示すように、プロトコル パック ファイルは 1 つのディレクトリまたは各プラットフォーム タイプ（ASR、ISR、CSR など）ごとに別々のディレクトリに保存することができます。

- **単一のディレクトリ**（この例では、各プラットフォーム タイプに対して 1 つのプロトコル パック ファイルがあります）：

  tftp://<Protocol-Pack-Server-address>/NbarAutoUpdate/pp_server/pp-adv-asr1k-155-3.S2-23-20.0.0.pack

  tftp://<Protocol-Pack-Server-address>/NbarAutoUpdate/pp_server/pp-adv-isrg2-155-3.M2-23-19.1.0.pack

  tftp://<Protocol-Pack-Server-address>/NbarAutoUpdate/pp_server/pp-adv-csr1000v-155-3.S2-23-21.0.0.pack

- **各プラットフォームごとに別々のディレクトリ**：

  tftp://<Protocol-Pack-Server-address>/NbarAutoUpdate/pp_server/**asr**/pp-adv-asr1k-155-3.S2-23-20.0.0.pack

  tftp://<Protocol-Pack-Server-address>/NbarAutoUpdate/pp_server/**isr**/pp-adv-isrg2-155-3.M2-23-19.1.0.pack

  tftp://<Protocol-Pack-Server-address>/NbarAutoUpdate/pp_server/**csr**/pp-adv-csr1000v-155-3.S2-23-21.0.0.pack

4 サーバのネットワークの場所、プロトコル パック ファイルのベース ディレクトリへのパス、およびダウンロードされた各プロトコル パック ファイルへのパスを書き留めます。

5 設定ファイルを作成する際には、プロトコル パック サーバの詳細とプロトコル パック ファイルの場所を指定します。

プロトコル パック自動更新の設定ファイル，（136 ページ）を参照してください。

プロトコル パック自動更新の設定ファイル

プロトコルパック自動更新の設定ファイル（NBAR_PROTOCOL_PACK_DETAILS.json）は**送信元サーバ**（プロトコルパック自動更新のための送信元サーバのセットアップ，（134ページ）を参照してください）に保存され、次を指定します：

- プロトコル パック サーバ（ダウンロードしたプロトコル パック ファイルを含むサーバ）の場所。
- プロトコル パック サーバ上のダウンロードされた各プロトコル パック ファイルの場所。
- 各プロトコル パック ファイルの NBAR ソフトウェア バージョン。

  （各プロトコル パック インストール用ファイルは、NBAR ソフトウェア バージョンによって示される NBAR2 の特定のバージョンで稼働します。詳細については以下を参照してください）
- 参加ルータがプロトコルパック サーバの更新を確認するスケジュールを設定してください。

例

設定ファイルの例：

```
{
  "nbar_auto_update_config": {
    "protocol-pack-server": "tftp://10.20.200.1/NbarAutoUpdate/pp_server/",
    "update-window":0,
    "force-upgrade":true,
    "clear-previous":true,
    "schedule": {
      "weekly": 6,
      "hh": 02,
      "mm": 30
    },
  },
  "nbar_pp_files": {
    "ISR": {
      "23":"isr/pp-adv-isrg2-155-3.M2-23-18.0.0.pack",
      "23":"isr/pp-adv-isrg2-155-3.M2-23-19.1.0.pack"
    },
    "ASR": {
      "23":"asr/pp-adv-asr1k-155-3.S2-23-19.1.0.pack",
      "23":"asr/pp-adv-asr1k-155-3.S2-23-20.0.0.pack"
    },
    "CSR": {
      "23":["csr/pp-adv-csr1000v-155-3.S2-23-19.1.0.pack"]
      "23":["csr/pp-adv-csr1000v-155-3.S2-23-21.0.0.pack"]
     },
    }
}
```

設定ファイルのファイル形式とファイル名

設定ファイル形式は、JSON です。必要なファイル名は次のとおりです。

NBAR_PROTOCOL_PACK_DETAILS.json

プロトコル パック サーバの場所とベース ディレクトリ

IPアドレスやディレクトリ構造などプロトコルパック サーバの詳細は、インストールによって異なります。これらの詳細は、設定ファイルで指定されます。プロトコルパック サーバ上で、プロトコル パック ファイルを保存するベース ディレクトリとして直感的なパスを作成します。推奨パスは次の通りです。 **/NbarAutoUpdate/pp_server/**。

設定ファイルの **protocol-pack-server** セクションでプロトコル パック サーバの場所を指定します。ディレクトリが推奨の /NbarAutoUpdate/pp_server であり、アドレスが 10.20.200.1 であるサーバの場合、設定ファイルには次の行が含まれます（パスの最後に「/」を含む）。

```
"protocol-pack-server":"tftp://10.20.200.1/NbarAutoUpdate/pp_server/"
```

プロトコル パック ファイルの場所

設定ファイルは、プロトコルパック サーバに保存されている、ダウンロードされた各プロトコルパック ファイルの場所を指定します。参加ルータはこれらのパスを使用して、プロトコルパック ファイルを自動でダウンロードし、インストールします。

各プロトコル パック ファイルの場所は、プロトコル パック サーバの場所とベース ディレクトリ、および設定ファイルの nbar_pp_files セクションで定義されているプロトコル パック ファイルのパスを組み合わせることにより指定されます。

たとえば、プロトコル パック サーバの場所とベース ディレクトリが

tftp://10.20.200.1/NbarAutoUpdate/pp_server/

であり、ファイルの場所が

asr/pp-adv-asr1k-155-3.S2-23-20.0.0.pack

である場合、ファイルの完全パスは次の通りです。

```
tftp://10.20.200.1/NbarAutoUpdate/pp_server/asr/pp-adv-asr1k-155-3.S2-23-20.0.0.pack
```

プロトコル パックの場所の整理

プロトコルパック ファイルは1つのディレクトリまたは各プラットフォーム タイプ（ASR、ISR、CSR など）ごとに別々のディレクトリに保存することができます。

（プロトコルパック自動更新のためのプロトコルパック サーバの設定, （135 ページ）を参照）。

isr と **asr** ディレクトリに保存された4つのプロトコル パック ファイルの、設定ファイル セクションの例：

```
"nbar_pp_files": {
  "ISR": {
    "23":"isr/pp-adv-isrg2-155-3.M2-23-18.0.0.pack",
    "23":"isr/pp-adv-isrg2-155-3.M2-23-19.1.0.pack"
  },
  "ASR": {
    "23":"asr/pp-adv-asr1k-155-3.S2-23-19.1.0.pack",
    "23":"asr/pp-adv-asr1k-155-3.S2-23-20.0.0.pack"
```

```
    },
  }
```

異なるバージョンの NBAR2 を実行している同じタイプのルータ

同じプラットフォーム タイプ（ISR など）のルータは、異なるバージョンの NBAR2 を使用している可能性があります。たとえば、2 つの Cisco ISR 4451 ルータがあり、一方は Cisco IOS XE 3.13 で稼働しており、もう一方は 3.16 で稼働している場合があります。設定ファイルでは、両方の NBAR バージョンに対してプロトコル パックのインストール用ファイルを指定する必要があります。

各プロトコル パック ファイルに対して指定される NBAR ソフトウェアのバージョン

各プロトコル パックのインストール用ファイルは、特定の NBAR ソフトウェア バージョンとのみ互換性があります。互換性のある NBAR ソフトウェアのバージョンは通常、インストール用ファイル名に示されます。たとえば、次のプロトコル パック 20.0.0 のインストール用ファイルは、NBAR バージョン 23 と互換性があります。これは、ファイル名に含まれる「23」によって示されます。 pp-adv-asr1k-155-3.S2-**23**-20.0.0.pack

プロトコルパックの自動更新用設定ファイルの、プロトコルパックのインストール用ファイルの場所を指定する各行は、適合する NBAR ソフトウェアのバージョンも示しています。プロトコル パックのインストール用ファイルの場所を追加する際は、そのファイルに適切な NBAR ソフトウェアのバージョンを指定する必要があります。

ヒント インストール済み OS の現在の NBAR ソフトウェアのバージョンを表示するには、ルータ上で **show ip nbar version** コマンドを使用します。

次の例は、NBAR ソフトウェアのバージョン 23 で動作するプロトコル パック 20.0.0 ファイルを指定する設定ファイルの抜粋です。「23」で始まる行は、指定されたファイルが NBAR ソフトウェアのバージョン 23 を使用するルータに適用されることを示しています。また、それに続くファイル名にも「23」が含まれており、ソフトウェアのバージョン 23 で動作することを示しています。

```
"23":"asr/pp-adv-asr1k-155-3.S2-23-20.0.0.pack"
```

設定ファイルのパラメータ

次のパラメータが設定ファイル NBAR_PROTOCOL_PACK_DETAILS.json で使用されます。プロトコル パック自動更新を使用する各ルータは、ローカル CLI コマンドを使用してこれらのパラメータを上書きすることができます。

パラメータ	説明
protocol-pack-server	（必須） プロトコル パック サーバの場所。 例：tftp://10.20.200.1/NbarAutoUpdate/pp_server/

パラメータ	説明
nbar_pp_files	（必須） 様々なプラットフォームとNBARバージョン向けのプロトコル パック ファイルの場所を指定します。NBARソフトウェアのバージョン番号によって特定されます。
schedule {**daily** | **weekly**: | **monthly**:} [*day*] {**hh**: *hh*, **mm**: *mm*}	NBAR プロトコル パック自動更新のアップグレード間隔をスケジュールします。参加するルータは、スケジュールされた時間に定期的に更新を確認します。 • monthly：月の日付 • weekly：曜日（0 ～ 6） • hh：時間（24 時間） • mm：分 実際の実行時間は update-window オプションに依存します。 デフォルト：毎日 00:00
update-window	NBARプロトコルパック自動更新が機能するメンテナンス期間（分単位）。メンテナンス ウィンドウは、schedule パラメータによって設定された時間に従ってスケジュールされます。 デフォルト：60
clear-previous	enable：クールダウン期間後に不要なプロトコル パック ファイルを削除します。 disable：どのファイルも削除しないように機能を設定します。 デフォルト：enable
force-upgrade	enable：新しいプロトコル パックの更新が「強制」フラグ付きで適用されます。 disable：新しいプロトコルパックの更新が「強制」フラグ付きでは適用されません。 デフォルト：disable

設定ファイル：最小例

最小の設定ファイルの例には、トップレベルの nbar_auto_update_config と、必須フィールドのみが含まれます。スケジュールは設定されないため、ルータはデフォルトの確認スケジュール（毎日 00:00）を使用します。例では、3 つのプラットフォーム タイプそれぞれに 1 つのプロトコル パック ファイルを指定し、「other」に 1 つ指定しています。どの場合も、プロトコル パックは NBAR ソフトウェア バージョン 23 を使用します。これは、各行においてファイル名の前に指定される必要があります。

```
{
  "nbar_auto_update_config":{
  "protocol-pack-server":"tftp://10.20.200.1/NbarAutoUpdate/pp_server/"
  },
  "nbar_pp_files":{
    "ISR":{"23":"/pp-adv-isrg2-155-3.M2-23-19.1.0.pack"},
    "ASR":{"23":"/pp-adv-asr1k-155-3.S2-23-20.0.0.pack"},
    "CSR":{"23":"/pp-adv-csr1000v-155-3.S2-23-21.0.0.pack"}
  }
}
```

設定ファイル：典型的な例

典型的な設定ファイルの例には、トップレベルの nbar_auto_update_config と、必須およびオプションのフィールドが含まれます。この例では、次のようになります。

- プロトコル パック TFTP サーバには、推奨の /NbarAutoUpdate/pp_server/ ディレクトリが含まれています。
- 2 つのプロトコル パックのバージョンが各プラットフォームに指定されています（たとえば、ASR プラットフォームに対して 19.1.0 および 20.0.0）。
- プロトコルパック ファイルはすべて、各ファイル名の前の「23」で示されているように（この数字は、プロトコルパックのインストール用ファイルそのもののファイル名に含まれている「23」に一致）、NBAR ソフトウェアのバージョン 23 を実行している Cisco IOS バージョンに適用されます。
- "schedule" セクションは、更新スケジュールを毎週土曜日の 2:30 AM に指定しています。参加するルータは、利用可能な更新をスケジュールされた時間に確認します。

  "weekly" の値「6」により、土曜日であることが示されています。（曜日の番号は 0 から 6 で、0 が日曜日、6 が土曜日を意味します）

  更新時間 2:30 AM は、"hh" と "mm" の値により示されています。

```
{
  "nbar_auto_update_config": {
    "protocol-pack-server": "tftp://10.20.200.1/NbarAutoUpdate/pp_server/",
    "update-window":0,
    "force-upgrade":true,
    "clear-previous":true,
    "schedule": {
      "weekly": 6,
      "hh": 02,
      "mm": 30
    },
  },
  "nbar_pp_files": {
    "ISR": {
      "23":"isr/pp-adv-isrg2-155-3.M2-23-18.0.0.pack",
      "23":"isr/pp-adv-isrg2-155-3.M2-23-19.1.0.pack"
```

```
    },
    "ASR": {
      "23":"asr/pp-adv-asr1k-155-3.S2-23-19.1.0.pack",
      "23":"asr/pp-adv-asr1k-155-3.S2-23-20.0.0.pack"
    },
    "CSR": {
      "23":["csr/pp-adv-csr1000v-155-3.S2-23-19.1.0.pack"]
      "23":["csr/pp-adv-csr1000v-155-3.S2-23-21.0.0.pack"]
     },
    }
}
```


プロトコル パック自動更新の有効化

ルータでプロトコル パック自動更新を有効にするには、次の操作を実行する必要があります。

- 機能を有効にする
- 使用する**送信元サーバ**を指定するか、すでに指定されていることを確認する

手順の概要

1. **configureterminal**
2. **ipnbarprotocol-pack-auto-update**
3. **source-server***server*
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device#configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**ipnbarprotocol-pack-auto-update**
	
	例：
	`Device(config)#ip nbar protocol-pack-auto-update`
	`Device(config-auto-pp-update)#`
		NBAR プロトコル パック自動更新を有効にします。

ステップ 3	**source-server***server* 例： `Device(config-auto-pp-update)#source-server tftp://10.20.300.400/NbarAutoUpdate`	（**送信元サーバ**がまだ指定されていない場合にのみ必要） **送信元サーバ**の場所と、プロトコル パック自動更新コンフィギュレーション ファイル NBAR_PROTOCOL_PACK_DETAILS.json が含まれているディレクトリを指定します。

	コマンドまたはアクション	目的
ステップ 4	**exit** 例： `Device(config-auto-pp-update)#exit`	グローバル コンフィギュレーション モードを終了します。

プロトコル パック自動更新の無効化

ルータでプロトコル パック自動更新を無効にします。

手順の概要

1. **configureterminal**
2. **noipprotocol-pack-auto-update**
3. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**noipprotocol-pack-auto-update** 例： `Device(config)# no ip nbar protocol-pack-auto-update`	NBAR プロトコル パック自動更新を無効にします。
ステップ 3	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了します。

自動更新によるプロトコル パック更新の即時開始

プロトコル パック自動更新メカニズムを使用してプロトコル パック更新をすぐに開始します。

手順の概要

1. **configureterminal**
2. **ipnbarprotocol-pack-auto-updatenow**
3. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipnbarprotocol-pack-auto-updatenow** 例： `Device(config)# ip nbar protocol-pack-auto-update now`	自動更新メカニズムを使用してプロトコル パックの更新を開始します。
ステップ 3	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了します。

プロトコル パック自動更新情報の表示

プロトコルパック自動更新設定、コピーされたファイル、およびプロトコルパック自動更新を使用する個別のルータの統計情報を表示します。

手順の概要

1. **showipnbarprotocol-pack auto-update**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**showipnbarprotocol-pack auto-update** 例： `Device# show ip nbar protocol-pack-auto-update`	プロトコル パック自動更新設定、コピーされたファイル、および統計情報を表示します。

次の例は、このコマンドの出力で提供される情報を示しています。

```
Device# show ip nbar protocol-pack-auto-update

NBAR Auto-Update:
=================

Configuration:
=============
force-upgrade               : (Default)  Enabled
clear-previous              : (Default)  Enabled
update-window               : (Default)  30
source-server               :                 tftp://10.20.200.1/NbarAutoUpdate/
protocol-pack-directory     : (Default)  harddisk:
schedule                    : (Default)  03:22

Copied files:
==========
File            : harddisk:/NbarAutoUpdate/AsrNbarPP
Copied          : *11:29:11.000 UTC Mon Jan 5 2015


Last run result: SUCCESS
Last auto-update run                      : *11:29:12.000 UTC Mon Jan 5 2015
Last auto-update success                  : *11:29:12.000 UTC Mon Jan 5 2015
Last auto-update successful update        : *11:29:12.000 UTC Mon Jan 5 2015

Last auto-update server-config update     : *16:15:13.000 UTC Mon Jan 5 2015
Success count                              : 3
Failure count                              : 0
Success rate                               : 100 percent

Next AU maintenance estimated to run at   : *17:15:13.000 UTC Mon Jan 5 2015
Next AU update estimated to run at        : *03:41:00.000 UTC Tue Jan 6 2015
```

ルータでのローカル プロトコル パック自動更新の設定

ルータでローカル プロトコル パック自動更新を設定するには、ここで説明するコマンドのサブモードを使用します。ルータでローカル設定を行うと、一元化されたコンフィギュレーションファイルで指定された設定が上書きされます。

手順の概要

1. **configureterminal**
2. **ipnbarprotocol-pack-auto-update**
3. 1 つ以上のサブモード コマンドを使用します。作業が完了したら、**exit** を使用してコマンド サブモードを終了します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device#configure terminal`	グローバルコンフィギュレーションモードを開始します。

ステップ 2	**ipnbarprotocol-pack-auto-update**
	
	例：
	`Device(config)#ip nbar protocol-pack-auto-update`
	`Device(config-auto-pp-update)#`
		プロトコルパック自動更新設定のサブモードを開始します。サブモードの開始は、プロンプトで「(config-auto-pp-update)」を含めるように変更されることからわかります。

ステップ 3	1 つ以上のサブモードコマンドを使用します。作業が完了したら、**exit** を使用してコマンドサブモードを終了します。	プロトコル パック自動更新サブモード コマンド，（145 ページ）を参照してください。

プロトコル パック自動更新サブモード コマンド

プロトコルパック自動更新サブモードコマンドは、ルータ上のローカル自動更新設定を構成します。コマンド サブモードの開始方法については、ルータでのローカル プロトコル パック自動更新の設定，（144 ページ）を参照してください。

作業が完了したら、exit を使用してコマンド サブモードを終了します。

コマンド	説明
clear-previous {**enable** | **disable**}	**enable**：クールダウン期間後に不要なプロトコル パック ファイルを削除します。 **disable**：どのファイルも削除しないように機能を設定します。 デフォルト：enable
force-upgrade {**enable** | **disable**}	**enable**：新しいプロトコルパックの更新が「強制」フラグ付きで適用されます。 **disable**：新しいプロトコルパックの更新が「強制」フラグ付きでは適用されません。 デフォルト：Disable

コマンド	説明
protocol-pack-directory*directory*	新しいプロトコル パック ファイルを保存するローカル ディレクトリ。 デフォルト：空き容量が最も多いファイル システム
schedule {**daily** | **weekly** | **monthly**} [*day*] [*hh:mm*]	NBAR プロトコル パック自動更新のアップグレード間隔をスケジュールします。実際の実行時間はupdate-windowオプションに依存します。 デフォルト：毎日 00:00
update-window*minutes*	NBARプロトコルパック自動更新が機能するメンテナンス期間（分単位）。メンテナンス期間は、schedule オプションで設定された時間に基づいて発生します。 範囲：0 ～ 60 デフォルト：60

例：更新期間のオーバーライド

次のコマンドは、更新期間を 10 分に設定して、プロトコル パック自動更新設定ファイルで指定された設定をオーバーライドします。

```
Device# configure terminal
Device(config)# ip nbar protocol-pack-auto-update
Device(config-auto-pp-update)# update-window 10
```

第 12 章

NBAR2 カスタム プロトコル

Network-Based Application Recognition（NBAR）は、カスタム プロトコルを使用したカスタム アプリケーションの識別をサポートします。カスタム プロトコルは、NBAR でサポートされないスタティック ポートベースのプロトコルとアプリケーションをサポートします。

- 機能情報の確認，147 ページ
- カスタム プロトコルの作成の前提条件，148 ページ
- カスタム プロトコルの作成に関する情報，148 ページ
- カスタム プロトコルの作成方法，151 ページ
- カスタム プロトコルの作成の設定例，162 ページ
- その他の参考資料，164 ページ
- NBAR2 カスタム プロトコルの機能情報，165 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

カスタム プロトコルの作成の前提条件

カスタムプロトコルを作成する前に、「NBAR を使用したネットワーク トラフィックの分類」モジュールの説明を参照してください。

カスタム プロトコルの作成に関する情報

NBAR とカスタム プロトコル

NBAR では、カスタムプロトコルを使用してカスタムアプリケーションを識別できます。カスタムプロトコルは、スタティック ポートベースのプロトコルとアプリケーションをサポートしますが、現在のところ、NBAR はサポートしていません。

（注） NBAR がサポートするプロトコルの一覧については、「NBAR を使用したネットワーク トラフィックの分類」モジュールを参照してください。

NBAR はカスタム プロトコルの使用をサポートし、カスタム プロトコルに静的な TCP ポート番号と UDP ポート番号をマップできます。

初期段階で、カスタムプロトコルおよびアプリケーションに関連する次の機能が NBAR に含まれていました。

- カスタム プロトコルには、custom-xx（xx は数値）という名前を付ける必要があります。
- NBAR を使用して 10 のカスタム アプリケーションを割り当てることができ、各カスタム アプリケーションでは、最大 16 の TCP ポートと最大 16 の UDP ポートをそれぞれ個別のカスタム プロトコルにマップすることができます。各カスタム プロトコルのリアルタイム統計情報を Protocol Discovery を使用してモニタできます。

NBAR には、ユーザ定義のカスタム プロトコルとアプリケーションに関連する次のような特徴があります。

- 特定のオフセットで特定のマッチング ストリング パターンについてペイロードを検査する機能。
- ユーザが自分のカスタム プロトコル アプリケーションの名前を定義できる機能。これにより、ユーザ指定のプロトコルを NBAR がサポートするプロトコルとして、Protocol Discovery、Protocol Discovery MIB、**matchprotocol** コマンド、および **ipnbarport-map** コマンドで使用できるようになります。
- トラフィックの方向ごと（つまり、双方向のトラフィックではなく、発信元方向または宛先方向のトラフィック）に指定されたカスタム プロトコルを NBAR で検査する機能。

- CLI によって、カスタム アプリケーションを設定したユーザは、個々のポートではなくポートの範囲を指定できるようになります。
- カスタム ホストと URL 署名を追加可能にする **http/dns/ssl** キーワード グループ。

（注） ユーザ定義のカスタム プロトコルを定義すると NBAR 機能が再起動しますが、事前定義のカスタム プロトコルを定義しても NBAR 機能は再起動しません。

MQC と NBAR カスタム プロトコル

NBAR は、プロトコルまたはアプリケーションによってネットワーク トラフィックを認識および分類します。カスタム プロトコルを作成することによって、NBAR が認識するプロトコルとアプリケーションのセットを拡張できます。カスタム プロトコルによって NBAR Protocol Discovery 機能を拡張し、追加のスタティック ポートアプリケーションを分類およびモニタできます。それによって、NBAR はサポートしていないスタティック ポート トラフィックを分類できるようになります。カスタムプロトコルを定義するには、**ipnbarcustom** コマンドのキーワードと引数を使用します。ただし、カスタム プロトコルの定義後に、トラフィック クラスを作成し、NBAR がトラフィックを分類するときにカスタム プロトコルを使用するようにトラフィック ポリシー（ポリシーマップ）を設定する必要があります。トラフィック クラスを作成し、トラフィック ポリシーを設定するには、モジュラ Quality of Service（QoS）コマンドライン インターフェイス（CLI）（MQC）の機能を使用します。MQC とは、コマンドライン インターフェイスで、トラフィック クラスの定義、トラフィック ポリシーの作成および設定（ポリシーマップ）、およびトラフィック ポリシーのインターフェイスへのアタッチが行えます。NBAR と MQC の機能の詳細については、「MQC を使用した NBAR の設定」モジュールを参照してください。

IP アドレスおよびポートベースのカスタム プロトコル

IP アドレスおよびポートベースのカスタム プロトコルには、特定の TCP または UDP トランスポートを使用した IP サブネットまたは IP アドレス リストのサポートが含まれます。これにより、Network-Based Application Recognition（NBAR）は、IP アドレスに基づいてトラフィックを認識し、指定された IP アドレスとの間のトラフィックにアプリケーション ID を関連付けることができます。カスタム プロトコル トランスポートを定義するには、**ip nbar custom transport** コマンドのキーワードと引数を使用します。

IP アドレスおよびポートベースのカスタムプロトコルオプションをサポートするために、カスタム コンフィギュレーション モード（config-custom）が **ip nbar custom transport** コマンドで導入されました。このモードは、最大 8 つの個別の IP アドレス、サブネット IP アドレス、およびサブネットマスク長を指定するオプションをサポートします。また、8 つのポートのリストまたはポート範囲の開始と終了を指定することもできます。

IP アドレスベースのカスタム アプリケーションは、SYN パケットから分類を取得します。

カスタム NBAR プロトコルの比較：単一のネットワーク プロトコルに基づく場合と複数のネットワーク プロトコルに基づく場合

（注） この説明では、「プロトコル」という語を 2 つの方法で使用しています。1 つはトラフィックの識別に使用される NBAR プロトコルとして、もう 1 つはネットワーク プロトコル（HTTP、SSL など）として使用しています。

NBAR が提供するもの：

- 単一のネットワーク プロトコルに基づくカスタム NBAR プロトコル

  指定されたパターンに従って単一のトラフィック タイプ（HTTP、SSL など）を識別するのに役立ちます。

  構文：ip nbar custom <protocol_name> <traffic_type> <criteria>

- 複数のネットワーク プロトコルに基づくカスタム NBAR プロトコル（「複合」カスタム NBAR プロトコルと呼ばれる）

  複数のネットワーク プロトコル用の署名を使用してトラフィックを特定するのに役立ちます。現在、この複合方式は、特定のサーバに関連付けられたすべての HTTP、SSL、および DNS トラフィックを特定するオプションの「server-name」（CLI 構文内の <composite_option> の値）を提供しています。

  単一のプロトコルを使用して、指定されたパターンに従って複数のトラフィック タイプ（HTTP、SSL など）を識別するのに役立ちます。

  構文：ip nbar custom <protocol_name> composite <composite_option> <criteria>

使用例：複数のネットワーク プロトコルに基づくカスタム NBAR プロトコル

- 目的：abc_example.com サーバに関連付けられたすべての HTTP、SSL、および DNS トラフィックを特定します。
- 推奨方式：複合カスタム NBAR プロトコルを使用します。
- CLI：`ip nbar custom abc_example_custom composite server-name *abc_example`

カスタム プロトコルの制限

カスタム プロトコルには次の制限が適用されます。

- NBAR は、最大 120 個のカスタム プロトコルをサポートします。この最大数には単一署名プロトコルや複合プロトコルを含む、すべてのカスタム プロトコルが含まれます。
- 同じターゲット正規表現の 2 つのカスタム プロトコルを定義することはできません。

たとえば、ip nbar custom 1abcd http url www.abcdef.com を設定したら、次は設定できません。

ip nbar custom 2abcd http url www.abcdef.com

これを行おうとするとエラーになります。

- カスタム プロトコルを定義する正規表現の最大長：30 文字

カスタム プロトコルの作成方法

単一のネットワーク プロトコルに基づいたカスタム NBAR プロトコルの定義

カスタム プロトコルによって NBAR Protocol Discovery 機能を拡張し、追加の静的ポート アプリケーションを分類およびモニタできます。それによって、NBARはサポートしていないスタティック ポート トラフィックを分類できるようになります。

この手順では、単一のネットワーク プロトコル（HTTP、SSL など）に基づいてカスタム NBAR プロトコルを作成します。

（注） NBAR は、最大 120 個のカスタム プロトコルをサポートします。この最大数には単一署名プロトコルや複合プロトコルを含む、すべてのカスタム プロトコルが含まれます。

カスタム プロトコルを定義するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ipnbarcustom***protocol-name* [*offset* [*formatvalue*]] [**variable***field-namefield-length*] [*source* | *destination*] [**tcp** | **udp**] [**range***startend* | *port-number*]
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipnbarcustom***protocol-name* [*offset* [*formatvalue*]] [**variable***field-namefield-length*] [*source* | *destination*] [**tcp** | **udp**] [**range***startend* | *port-number*] 例： `Router(config)# ip nbar custom app_sales1 5 ascii SALES source tcp 4567`	NBAR Protocol Discovery 機能を拡張し、追加の静的ポート アプリケーションを分類および監視できます。または、NBAR はサポートしていない静的ポート トラフィックを分類できるようになります。 • 単一のネットワーク プロトコルに基づいてトラフィックを識別するカスタム NBAR プロトコルを作成します。 • 指定されたパターンに従って単一のトラフィック タイプ（HTTP、SSL など）を識別するのに役立ちます。 • カスタム プロトコル名とその他の任意のキーワードと引数を入力します。
ステップ 4	**end** 例： `Router(config)# end`	（任意）グローバル コンフィギュレーション モードを終了します。

例

次のカスタム プロトコル LAYER4CUSTOM の例では、6700 の宛先ポートまたは送信元ポートを持つ TCP パケットを検索します。

```
Device# configure terminal
Device(config)# ip nbar custom LAYER4CUSTOM  transport tcp id 14
Device(config-custom)# port 6700
```

ポート以外のオプションを表示するには、次のようにします。

```
Device# configure terminal
Device(config)# ip nbar custom LAYER4CUSTOM  transport tcp id 14
Device(config-custom)# ?
Custom protocol commands:
  direction  Flow direction
  dscp       DSCP in IPv4 and IPv6 packets
  exit       Exit from custom configuration mode
  ip         ip address
  ipv6       ipv6 address
  no         Negate a command or set its defaults
  port       ports
```

複数のネットワーク プロトコルに基づいたカスタム NBAR プロトコルの定義

カスタム プロトコルによって NBAR Protocol Discovery 機能を拡張し、追加の静的ポート アプリケーションを分類およびモニタできます。それによって、NBARはサポートしていないスタティック ポート トラフィックを分類できるようになります。

この手順では、複数のネットワーク プロトコルに基づいてカスタムNBARプロトコルを作成します。

（注） この説明では、「プロトコル」という語を 2 つの方法で使用しています。1 つはトラフィックの識別に使用される NBAR プロトコルとして、もう 1 つはネットワーク プロトコル（HTTP、SSL など）として使用しています。

（注） NBAR は、最大 120 個のカスタム プロトコルをサポートします。この最大数には単一署名プロトコルや複合プロトコルを含む、すべてのカスタム プロトコルが含まれます。

コンポジット署名カスタム プロトコルを定義するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ipnbarcustom***protocol-name***compositeserver-name***server-name*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ipnbarcustom***protocol-name***compositeserver-name***server-name* 例： `Router(config)# ip nbar custom abc_example_custom composite server-name *abc_example`	NBAR Protocol Discovery 機能を拡張し、追加の静的ポートアプリケーションを分類および監視できます。または、NBAR はサポートしていない静的ポートトラフィックを分類できるようになります。 • 複数のネットワーク プロトコルの署名を使用してトラフィックを識別するカスタム NBAR プロトコルを作成します。 現在、*composite-option* の唯一のオプションは server-name です。これは、特定のサーバに関連付けられているすべての HTTP、SSL、および DNS トラフィックを識別します。 • 単一のプロトコルを使用して、指定されたパターンに従って複数のトラフィック タイプ（HTTP、SSL など）を識別するのに役立ちます。 この例の目的は、abc_example.com サーバに関連付けられているすべての HTTP、SSL、および DNS トラフィックを識別することです。
ステップ 4	**end** 例： `Router(config)# end`	（任意）グローバル コンフィギュレーション モードを終了します。

カスタム プロトコルを使用するためのトラフィック クラスの設定

トラフィック クラスを使用し、ユーザが指定した基準に基づいて、パケットをグループに分類できます。たとえば、NBAR が認識するプロトコル タイプまたはアプリケーションに基づいて、パケットに一致するようにトラフィック クラスを設定できます。この場合、カスタムプロトコルに基づいて一致するようにトラフィック クラスを設定します。

カスタムプロトコルを使用するようにトラフィック クラスを設定するには、次の手順を実行します。

（注） **matchprotocol** コマンドは手順 4 に記載されています。*protocol-name* 引数の場合は、一致基準として使用するプロトコル名を入力します。カスタム プロトコルの場合は、**ipnbarcustom** コマンドの *name* 引数に指定されたプロトコルを使用します。（「カスタム プロトコルの定義」タスクの手順 3 を参照してください。）

手順の概要

1. **enable**
2. **configureterminal**
3. **class-map** [**match-all** | **match-any**] *class-map-name*
4. **matchprotocol***protocol-name*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map** [**match-all**	**match-any**] *class-map-name* 例： `Router(config)# class-map cmap1`	指定したクラスとパケットのマッチングに使用されるクラスマップを作成し、クラスマップ コンフィギュレーション モードを開始します。 • クラス マップの名前を入力します。
ステップ 4	**matchprotocol***protocol-name* 例： `Router(config-cmap)# match protocol app_sales1`	指定のプロトコルに基づいてトラフィックを照合するように NBAR を設定します。 • *protocol-name* 引数の場合は、一致基準として使用するプロトコル名を入力します。カスタム プロトコルの場合は、**ipnbarcustom** コマンドの *name* 引数に指定されたプロトコルを使用します。（「カスタムプロトコルの定義」タスクの手順 3 を参照してください。）

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Router(config-cmap)# end`	（任意）クラスマップ コンフィギュレーション モードを終了します。

例

次の例では、カスタム プロトコルの作成中に **variable** キーワードが使用され、変数フィールド内のさまざまな値をさまざまなトラフィック クラスに分類するようにクラスマップが設定されています。具体的には、次の例では、変数 scid 値 0x15、0x21、および 0x27 は、クラスマップ active-craft に分類され、scid 値 0x11、0x22、および 0x25 はクラス マップ passive-craft に分類されます。

```
Router(config)#
 ip nbar custom ftdd 23 variable scid 1 tcp range 5001 5005

Router(config)#
class-map active-craft
Router(config-cmap)# match protocol ftdd scid 0x15
Router(config-cmap)# match protocol ftdd scid 0x21
Router(config-cmap)# match protocol ftdd scid 0x27

Router(config)#
class-map passive-craft
Router(config-cmap)# match protocol ftdd scid 0x11
Router(config-cmap)# match protocol ftdd scid 0x22
Router(config-cmap)# match protocol ftdd scid 0x25
```

トラフィック ポリシーの設定

ユーザが指定した基準に一致するトラフィックは、特定のクラスに分類されます。そのクラスをポリシー マップに含めると、そのクラスのトラフィックは特定の QoS 処理を受けられるようになります。

トラフィック ポリシーを設定するには、次の手順を実行します。

（注） **bandwidth** コマンドは手順 5 に記載されています。**bandwidth** コマンドは、QoS 機能の Class-Based Weighted Fair Queuing（CBWFQ）を設定します。CBWFQ は、設定できる QoS 機能の単なる一例です。使用する QoS 機能に適したコマンドを使用してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **policy-map***policy-map-name*
4. **class** {*class-name* | **class-default**}
5. **bandwidth** {*bandwidth-kbps*| **remaining percent** *percentage*| **percent** *percentage*}
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy-map***policy-map-name* 例： `Router(config)# policy-map policy1`	1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、policy-map コンフィギュレーション モードを開始します。 • ポリシー マップの名前を入力します。
ステップ 4	**class** {*class-name*	**class-default**} 例： `Router(config-pmap)# class class1`	作成または変更するポリシーのクラス名を指定し、ポリシーマップ クラス コンフィギュレーション モードを開始します。 • 特定のクラス名または **class-default** キーワードを入力します。
ステップ 5	**bandwidth** {*bandwidth-kbps*| **remaining percent** *percentage*| **percent** *percentage*} 例： `Router(config-pmap-c)# bandwidth percent 50`	（任意）ポリシー マップに属するクラスに割り当てる帯域幅を指定または変更します。 • kbps の数値、帯域幅の相対的な割合、または帯域幅合計の絶対値として、帯域幅の合計を入力します。 （注） **bandwidth** コマンドは、QoS 機能の Class-Based Weighted Fair Queuing（CBWFQ）を設定します。CBWFQ は、設定できる QoS 機能の単なる一例です。使用する QoS 機能に適したコマンドを使用してください。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Router(config-pmap-c)# end`	（任意）ポリシー マップ クラス コンフィギュレーション モードを終了します。

トラフィック ポリシーのインターフェイスへの適用

トラフィック ポリシー（ポリシー マップ）を作成した後の次の手順は、ポリシー マップをインターフェイスに適用することです。ポリシー マップは、入力方向または出力方向のインターフェイスに適用できます。

（注） ネットワークのニーズにより、ポリシー マップをサブインターフェイス、ATM PVC、フレームリレー DLCI、または他のタイプのインターフェイスにアタッチする必要がある場合もあります。

トラフィック ポリシーをインターフェイスに適用するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***typenumber* [*name-tag*]
4. **pvc** [*name*] *vpi* / *vci* [**ilmi**| **qsaal**| **smds**| **l2transport**]
5. **exit**
6. **service-policy** {**input** | **output**} *policy-map-name*
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***typenumber* [*name-tag*] 例： `Router(config)# interface ethernet 2/4`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。 • インターフェイスタイプとインターフェイス番号を入力します。
ステップ 4	**pvc** [*name*] *vpi* / *vci* [**ilmi**| **qsaal**| **smds**| **l2transport**] 例： `Router(config-if)# pvc cisco 0/16`	（任意）名前を ATM PVC に作成または割り当て、ATM 相手先固定接続（PVC）でカプセル化を指定し、ATM 仮想回線コンフィギュレーション モード開始します。 • PVC 名、ATM ネットワーク仮想パス ID、およびネットワーク仮想チャンネル ID を入力します。 （注） この手順は、ポリシー マップを ATM PVC に適用する場合にのみ必要です。ポリシー マップを ATM PVC に適用しない場合は、トラフィック ポリシーのインターフェイスへの適用 に進みます。
ステップ 5	**exit** 例： `Router(config-atm-vc)# exit`	（任意）インターフェイス コンフィギュレーション モードに戻ります。 （注） この手順は、ポリシーマップを ATM PVC に適用しており、トラフィック ポリシーのインターフェイスへの適用 を完了している場合にのみ必要です。ポリシー マップを ATM PVC に適用しない場合は、トラフィックポリシーのインターフェイスへの適用 に進みます。
ステップ 6	**service-policy** {**input** | **output**} *policy-map-name* 例： `Router(config-if)# service-policy input policy1`	ポリシー マップを入力または出力インターフェイスに適用します。 • ポリシー マップの名前を入力します。 （注） ポリシーマップは、入力または出力ルータで設定できます。また、入力方向または出力方向のインターフェイスにも適用できます。ポリシー マップを適用する方向（入力または出力）と、ルータ（入力または出力）は、ネットワーク構成に応じて変わります。**service-policy** コマンドを使用してポリシーマップをインターフェイスに適用する場合、ネットワーク構成に適したルータおよびインターフェイスの方向を選択してください。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： `Router(config-if)# end`	（任意）特権 EXEC モードに戻ります。

カスタム プロトコル情報の表示

カスタムプロトコルを作成し、カスタムプロトコルに基づいてトラフィックを照合した後、**show ip nbar port-map** コマンドを使用してカスタム プロトコルに関する情報を表示できます。

カスタム プロトコル情報を表示するには、次の手順を実行します。

手順の概要

1. **enable**
2. **showipnbarport-map**[*protocol-name*]
3. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showipnbarport-map**[*protocol-name*] 例： `Router# show ip nbar port-map`	NBAR に現在使用されているプロトコルからポートへのマッピングを表示します。 • （任意）プロトコル名を入力します。
ステップ 3	**exit** 例： `Router# exit`	（任意）特権 EXEC モードを終了します。

IP アドレスおよびポートベースのカスタム プロトコルの設定

手順の概要

1. **enable**
2. **configureterminal**
3. **ip nbar custom** *name* **transport {tcp | udp} {id** *id* **} ip address** *ip-address* **| subnet** *subnet-ip subnet-mask***}| ipv6 address {***ipv6-address* **| subnet** *subnet-ipv6 ipv6-prefix***} | port {***port-number* **| range** *start-range end-range***} | direction {any | destination | source}**
4. **ip nbar custom** *name* **transport {tcp | udp} {id** *id***}**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	**ip nbar custom** *name* **transport {tcp	udp} {id** *id* **} ip address** *ip-address* **| subnet** *subnet-ip subnet-mask***}| ipv6 address {***ipv6-address* **| subnet** *subnet-ipv6 ipv6-prefix***}	port {***port-number* **| range** *start-range end-range***}	direction {any	destination	source}**
						
						例：
						
						`Device(config)# ip nbar custom mycustom transport tcp id 100`
						`Device(config-custom)# ip address 10.2.1.1`
							カスタム コンフィギュレーション モードで IP アドレスとポートベースのカスタム プロトコル オプションを指定します。

ステップ 4	**ip nbar custom** *name* **transport {tcp	udp} {id** *id***}**
		
		例：
		
		`Device(config)# ip nbar custom mycustom transport tcp id 100`
		`Device(config-custom)#`
			TCP または UDP をトランスポート プロトコルとして設定し、カスタム コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config-custom)# end`	（任意）カスタム コンフィギュレーション モードを終了します。

カスタム プロトコルの作成の設定例

例：カスタム プロトコルの作成

次のカスタム プロトコル app_sales1 の例では、4567 の送信元ポートを持つ TCP パケット、および最初のペイロード パケットに「SALES」という用語を含むパケットを識別します。

```
Router> enable
Router# configure terminal
Router(config)# ip nbar custom app_sales1 5 ascii SALES source tcp 4567
Router(config)# end
```

例：カスタム プロトコルを使用するためのトラフィック クラスの設定

次の例では、cmap1 というクラスが設定されました。カスタム プロトコル app_sales1 に一致するすべてのトラフィックは、cmap1 クラスに配置されます。

```
Router> enable
Router# configure terminal
Router(config)# class-map cmap1
Router(config-cmap)# match protocol app_sales1
Router(config-cmap)# end
```

例：トラフィック ポリシーの設定

次の例では、policy1 というトラフィック ポリシー（ポリシー マップ）が設定されました。policy1 には class1 というクラスが含まれ、class1 では CBWFQ がイネーブルです。

```
Router> enable
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth percent 50
Router(config-pmap-c)# end
```

（注） 上記の例では、Class-Based Weighted Fair Queuing（CBWFQ）を有効化するために **bandwidth** コマンドが使用されます。CBWFQ は、トラフィック ポリシー（ポリシー マップ）で適用できる QoS 機能の一例です。使用する QoS 機能に適したコマンドを使用してください。

例：トラフィック ポリシーのインターフェイスへの適用

次の例では、policy1 というトラフィック ポリシー（ポリシー マップ）が、インターフェイスの入力方向のイーサネット インターフェイス 2/4 に適用されました。

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 2/4

Router(config-if)# service-policy input policy1
Router(config-if)# end
```

例：カスタム プロトコル情報の表示

次に、**show ip nbar port-map** コマンドの出力例を示します。このコマンドは、NBAR に現在使用されているプロトコルからポートへのマッピングを表示します。この表示を使用して、マッピングが正しいことを確認します。

```
Router# show ip nbar port-map
port-map bgp      udp 179
port-map bgp      tcp 179
port-map cuseeme  udp 7648 7649
port-map cuseeme  tcp 7648 7649
```

```
port-map dhcp     udp 67 68
port-map dhcp     tcp 67 68
```

ip nbar port-map コマンドが使用されている場合、**show ip nbar port-map** コマンドを使用すると、プロトコルに割り当てられているポートが表示されます。

no ip nbar port-map コマンドが使用されている場合、**show ip nbar port-map** コマンドを使用すると、デフォルト ポートが表示されます。表示を特定のプロトコルに限定するには、**show ip nbar port-map** コマンドの *protocol-name* 引数を使用します。

例：IP アドレスおよびポートベースのカスタム プロトコルの設定

次に、グローバル コンフィギュレーション モードからカスタム コンフィギュレーション モードを開始し、サブネット IP アドレスおよびそのマスク長を設定する例を示します。

```
Device(config)#  ip nbar custom mycustom transport tcp id 100
Device(config-custom)# ip subnet 10.1.2.3 22
```

その他の参考資料

ここでは、カスタム プロトコルの作成に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
QoS コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Quality of Service Solutions Command Reference*』
MQC、トラフィック ポリシー（ポリシー マップ）、およびトラフィック クラス	「Applying QoS Features Using the MQC」モジュール
NBAR に関する概念と情報	「NBAR を使用したネットワーク トラフィックの分類」モジュール
Protocol Discovery のイネーブル化に関する情報	「Enabling Protocol Discovery」モジュール
MQC を使用した NBAR の設定	「Configuring NBAR Using the MQC」モジュール
アプリケーション認識モジュール（PDLM とも呼ばれます）の追加	「Adding Application Recognition Modules」モジュール

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

NBAR2 カスタム プロトコルの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *16*：*NBAR2* カスタム プロトコルの機能情報

機能名	リリース	機能情報
NBAR2 カスタム プロトコル	Cisco IOS XE リリース 3.8S	この機能は、Cisco ASR 1000 シリーズ アグリゲーション サービスルータに導入されました。 次のコマンドが導入または変更されました：**ip nbar custom**
NBAR2 Custom Protocol Enhancements Ph II	Cisco IOS XE リリース 3.12S	NBAR2 Custom Protocol Enhancements Phase II 機能を使用すると、特定の TCP または UDP 転送で IP サブネットまたは IP アドレスのリストがサポートされます。 次のコマンドが導入または変更されました：**ip nbar custom**

第 13 章

NBAR2 プロトコル パック ヒットレス アップグレード

NBAR2 プロトコル パック ヒットレス アップグレード機能は、デバイス上の現在の分類設定に影響を与えることなく、ユーザが Network-Based Application Recognition（NBAR）プロトコル パックをシームレスにアップグレードしたり、NBAR 設定を変更したりできるようにします。

- 機能情報の確認，167 ページ
- NBAR2 プロトコル パック ヒットレス アップグレードの制約事項，168 ページ
- NBAR2 プロトコル パック ヒットレス アップグレードに関する情報，168 ページ
- NBAR2 プロトコル パック ヒットレス アップグレードに関する追加情報，169 ページ
- NBAR2 プロトコル パック ヒットレス アップグレードの機能情報，170 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

NBAR2 プロトコル パック ヒットレス アップグレードの制約事項

「NBAR2 プロトコル パック ヒットレス アップグレード」機能は以前の設定が不要となるまで 2 つの設定を維持するため、追加のメモリが必要となります。

NBAR2 プロトコル パック ヒットレス アップグレードに関する情報

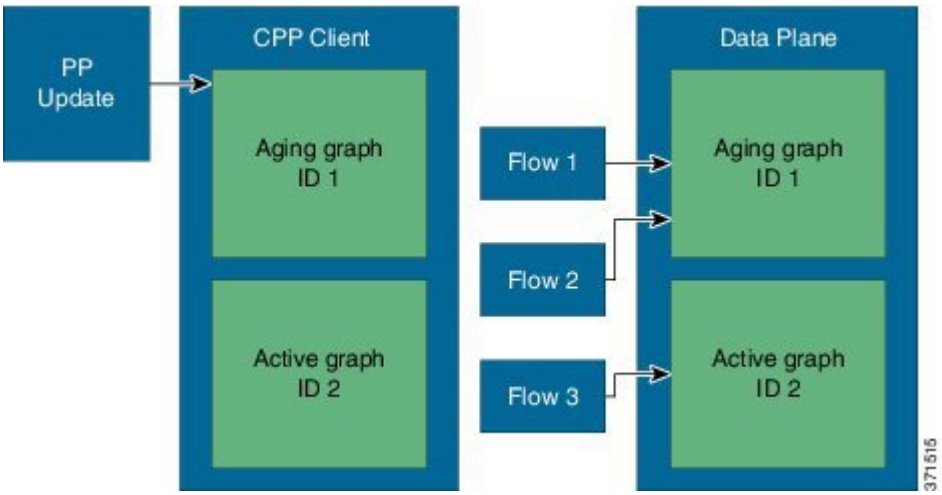
NBAR2 PP ヒットレス アップグレードの概要

ヒットレスアップグレードは、サービスダウンタイムを引き起こすことなく、NBARエンジン上で NBAR2 プロトコル パック（PP）のコンポーネントをアップグレードする方式です。以前の Cisco IOS ソフトウェア リリースでは、NBAR は、データ パスに転送されるコントロール プレーン クライアント上で 1 つの設定グラフしか保持できませんでした。Cisco IOS XE リリース 3.12S 以降では、NBAR は、一度に複数の設定グラフを保持できます。新しい設定の変更が加えられると、新しい設定グラフがコントロールプレーンクライアント上で作成されます。新しいグラフはデータ プレーンにダウンロードされ、すべての新しいフローが新しいグラフに転送されます。

分類されていたフローからパケットが到着すると、正しい設定グラフ（フローの作成時にアクティブだったグラフ）に転送されます。

次の図に、設定またはプロトコル パックの更新後の NBAR システムの状態を示します。

図 *3*：グラフのエージング



上の図では、新しいグラフが作成されると、古いグラフはエージング状態に移行します。エージングした状態では、グラフに関連付けられたフローだけがそのグラフで参照されます。フローがエージング タイムまで分類されなかった場合は、NBAR から不明としてレポートされます。

（注） メモリには制限があるため、NBAR システム内の並列存在グラフとエージング グラフの数を制限することが重要です。現在、すべてのプラットフォームで同時に保持できる設定は2つまでです。

NBAR のステータスを確認するには、**show platform software nbar statistics** コマンドを使用します。

NBAR2 プロトコル パック ヒットレス アップグレードのメリット

NBAR2 プロトコル パック ヒットレス アップグレードには、次のようなメリットがあります。

- プロトコル アップグレード中に分類されたフローに関する情報が消失しない
- 新しいフローに影響しない
- 進行中のフローに影響しない

NBAR2 プロトコル パック ヒットレス アップグレードに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
NBAR プロトコル パック	『*QoS*：*NBAR* コンフィギュレーション ガイド』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

NBAR2 プロトコル パック ヒットレス アップグレードの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *17* : ***NBAR2*** プロトコル パック ヒットレス アップグレードの機能情報

機能名	リリース	機能情報
NBAR2プロトコルパック ヒットレス アップグレード	Cisco IOS XE リリース 3.12S	NBAR2 プロトコル パック ヒットレス アップグレード機能を使用すると、デバイスの現在の分類設定に影響を及ぼさずにNBARプロトコルパックまたはNBAR設定をシームレスにアップグレードできます。 Cisco IOS XE リリース 3.12S では、Cisco ASR 1000 シリーズ ルータのサポートが追加されました。

第 14 章

NBAR の Web ベース カスタム プロトコル

NBAR の Web ベース カスタム プロトコル機能は、HTTP URL とホスト名のいずれかまたは両方に基づいて照合するカスタム プロトコルを定義するメカニズムを提供します。

- 機能情報の確認，173 ページ
- NBAR の Web ベース カスタム プロトコルの制限事項，174 ページ
- NBAR の Web ベース カスタム プロトコルに関する情報 ，174 ページ
- NBAR の Web ベース カスタム プロトコル一致の定義方法，174 ページ
- NBAR の Web ベース カスタム プロトコルの設定例，175 ページ
- NBAR の Web ベース カスタム プロトコルに関する追加情報，176 ページ
- NBAR の Web ベース カスタム プロトコルの機能情報，176 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

NBAR の Web ベース カスタム プロトコルの制限事項

カスタム プロトコルの一致に定義された HTTP URL とホスト名は一意である必要があります。プロトコル名の長さは 4 文字以上で、プロトコル名のプレフィクスは他のプロトコル名のプレフィクスと異なっている必要があります。

NBAR の Web ベース カスタム プロトコルに関する情報

NBAR の Web ベース カスタム プロトコルの概要

NBAR の Web ベース カスタム プロトコル機能は、HTTP URL とホスト名のいずれかまたは両方に基づいてトラフィックを照合するカスタム プロトコルを定義するメカニズムを提供します。

全部で 120 のカスタム プロトコルを HTTP URL とホスト名のいずれかまたは両方に基づいて照合するように定義できます。Web ベースのカスタム プロトコルを照合する場合は、HTTP URL とホスト名の両方が定義されたカスタム プロトコルの優先順位が最も高く、次に HTTP URL だけが定義されたプロトコルが、最後にホスト名だけが定義されたプロトコルが続きます。Web ベースのサブプロトコルの照合は、どのタイプの Web ベースのカスタム プロトコルの照合より優先されます。たとえば、**match protocol** *http url http-url* コマンドは、同じ URL 設定のカスタム プライオリティより優先されます。

NBAR の Web ベース カスタム プロトコル一致の定義方法

Web ベースのカスタム プロトコル一致の定義

手順の概要

1. **enable**
2. **configureterminal**
3. **ip nbar custom** *custom-protocol-name* **http** {**host** *host-name* | **url** *http-url* [**host** *host-name*]} [**id** *selector-id*]
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nbar custom** *custom-protocol-name* **http** {**host** *host-name* | **url** *http-url* [**host** *host-name*]} [**id** *selector-id*] 例： `Router(config)# ip nbar custom app_sales1 http url www.example.com`	Web ベースのカスタム プロトコル照合を定義します。 • カスタムプロトコル名とその他の任意のキーワードと引数を入力します。 （注） カスタム プロトコルを追加するには、**ip nbar custom** コマンドを使用します。プロトコルを有効にするには、**match protocol** コマンドまたは **ip nbar protocol discovery** コマンドを使用します。
ステップ 4	**end** 例： `Router(config)# end`	（任意）グローバル コンフィギュレーション モードを終了します。

NBAR の Web ベース カスタム プロトコルの設定例

例：Web ベースのカスタム プロトコル一致の定義

次に、HTTP URL に基づくカスタム プロトコルを照合する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# ip nbar custom app_sales1 http url www.example.com
```

次に、ホスト名の一部に「example」という文字列を含むカスタムプロトコルを照合する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# ip nbar custom app_sales1 http host *example*
```

NBAR の Web ベース カスタム プロトコルに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
カスタム プロトコル	「*Creating a Custom Protocol*」モジュール

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

NBAR の Web ベース カスタム プロトコルの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *18* : ***NBAR*** の ***Web*** ベース カスタム プロトコルの機能情報

機能名	リリース	機能情報
NBAR の Web ベース カスタム プロトコルの拡張性	Cisco IOS XE リリース 3.13S	NBAR の Web ベース カスタム プロトコルの拡張機能を使用すると、HTTP ホスト名や URL に基づいてカスタム プロトコル照合を定義できます。 次のコマンドが導入または変更されました。 **ip nbar custom**。

第 15 章

NBAR2 HTTP ベースの可視性ダッシュボード

NBAR2 HTTP ベースの可視性ダッシュボード機能は、ネットワーク上のトラフィックをグラフ表示する機能を提供します。

- 機能情報の確認，179 ページ
- NBAR2 HTTP ベースの可視性ダッシュボードに関する情報，180 ページ
- NBAR2 HTTP ベースの可視性ダッシュボードの設定方法，180 ページ
- NBAR2 HTTP ベースの可視性ダッシュボードの設定例，181 ページ
- NBAR2 HTTP ベースの可視性ダッシュボードへのアクセス，181 ページ
- NBAR2 HTTP ベースの可視性ダッシュボードに関する追加情報，182 ページ
- NBAR2 HTTP ベースの可視性ダッシュボードの機能情報，182 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

NBAR2HTTPベースの可視性ダッシュボードに関する情報

NBAR2 HTTP ベースの可視性ダッシュボードの概要

NBAR HTTP ベースの可視性ダッシュボード機能は、ネットワーク上のトラフィックの可視性を高め、ネットワーク要件をより正確に把握することができます。

ルータ上で NBAR HTTP ベースの可視性ダッシュボード機能を有効にすると、1 分ごとに NBAR 検出データを収集してデータベースに格納する定期タスクが作成されます。この機能は、ウィンドウ サイズである定義済みの期間（過去 24 時間など）の統計情報を表示するためのオプションも提供します。ウィンドウサイズ（2時間、24時間、および48時間）に基づいてWebアプリケーションが作成されます。このアプリケーションには、デバイス上の HTTP サーバ ユーティリティ オプションを使用してアクセスできます。このWebアプリケーションは、インタラクティブチャートやウィンドウ サイズごとの帯域幅グラフなどの NBAR データのグラフィカル表示を支援します。

HTTP ベースの可視性ダッシュボードを使用するには、Protocol Discovery 機能を有効にする必要があります（Protocol Discovery のイネーブル化, （63 ページ）を参照してください）。

NBAR2 HTTP ベースの可視性ダッシュボードの設定方法

NBAR2 HTTP ベースの可視性ダッシュボードの設定

はじめる前に

HTTP ベースの可視性ダッシュボードを使用するには、Protocol Discovery 機能を有効にする必要があります（Protocol Discovery のイネーブル化, （63 ページ）を参照してください）。

手順の概要

1. **enable**
2. **configureterminal**
3. **ip nbar http-services**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nbar http-services** 例： `Device(config)# ip nbar http-services`	NBAR ディスカバリ データを毎分収集して 48hr データベースに格納する定期タスクを実行するように、HTTP サービスを設定します。

NBAR2 HTTP ベースの可視性ダッシュボードの設定例

例：NBAR2 HTTP ベースの可視性ダッシュボード

例：**NBAR2 HTTP** サービスの有効化

```
Device> enable
Device# configure terminal
Device(config)# ip nbar http-services
Device(config)# end
```

NBAR2HTTPベースの可視性ダッシュボードへのアクセス

可視性ダッシュボードへのアクセス

ダッシュボードにアクセスするには、ルータにアクセス可能なブラウザで次のいずれかを入力します。

- http://<Router-IP-address>/flash/nbar2/home.html
- http://<Router-Hostname>/flash/nbar2/home.html（ルータのホスト名が定義されている場合）

例：

```
http://192.168.0.1/flash/nbar2/home.html
```

NBAR2HTTPベースの可視性ダッシュボードに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS QoS 構成情報	『QoS Configuration Guide』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

NBAR2 HTTP ベースの可視性ダッシュボードの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *19*：***NBAR2 HTTP*** ベースの可視性ダッシュボードの機能情報

機能名	リリース	機能情報
NBAR2 HTTP ベースの可視性ダッシュボード	Cisco IOS XE リリース 3.16S	NBAR2 HTTP ベースの可視性ダッシュボード機能は、ネットワーク上のトラフィックをグラフ表示する機能を提供します。 次のコマンドが変更または導入されました：**ip nbar http-services**。

第 16 章

NBAR の粗粒分類

NBAR は、粗粒と細粒という 2 つのレベルのアプリケーション認識を提供します。Cisco IOS XE リリース 3.14S のデフォルトでは、NBAR はその完全なアプリケーション認識機能を提供する細粒モードで動作します。粗粒モードでは、ディープ パケット インスペクションを最小限に抑えることにより、パフォーマンス メリットを提供し、メモリ リソースの需要を削減します。

- 機能情報の確認，185 ページ
- NBAR の粗粒分類に関する情報，186 ページ
- NBAR の粗粒分類の設定方法，187 ページ
- NBAR の粗粒分類の設定例，190 ページ
- NBAR の粗粒分類に関する追加資料，191 ページ
- NBAR の粗粒分類の機能情報，192 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

NBAR の粗粒分類に関する情報

NBAR の粗粒分類の概要

NBAR は、粗粒と細粒という 2 つのレベルのアプリケーション認識を提供します。デフォルトでは、NBAR はその完全なアプリケーション認識機能を提供する細粒モードで動作します。デフォルトの NBAR 細粒モードは、細粒モードと粗粒モードが別々に導入される以前の NBAR の機能とパフォーマンスと等価です。これは、既存の設定に対する完全な後方互換性を提供します。

粗粒モードでは、ディープパケットインスペクションを最小限に抑えることにより、パフォーマンスメリットを提供し、メモリリソースの需要を削減します。このモードは、完全な細粒分類を必要としないシナリオで使用できます。細粒モードは、パケット単位レポートが必要な場合に使用することをお勧めします。特定のパケット単位レポートが必要ない場合は、粗粒モードを使用します。その方が、パフォーマンスとメモリのメリットが得られます。

簡易分類

粗粒モードでは、ディープパケットインスペクションを最小化する分類の簡易モードを使用します。NBAR は、以前のパケットに対して下された分類決定をキャッシュして、同じサーバからの以降のパケットを同様に分類します。

先頭パケットによる分類

ほとんどのフローにはペイロードインスペクションが実行されないため、IP 同期（SYN）パケットの場合であっても、先頭パケットに基づいて分類されます。その結果、ポリシーはペイロードに依存することなくフロー全体に適用されます。

粗粒モードの制限

粗粒モードには、メトリック レポート詳細において次の制限があります。

フィールド抽出と下位分類：部分的にしかサポートされません。粗粒モードでは、フィールド抽出と下位分類のレポート結果の精度が低く、サンプリングされる可能性があります。

粒度：キャッシングが粒度の低下につながる可能性があります。たとえば、NBAR は、より具体的な **ms-office-web-apps** としてではなく、**ms-office-365** として一部のトラフィックを分類する可能性があります。

回避的アプリケーション：BitTorrent、eMule、Skype などの回避的アプリケーションの分類は、デフォルトの NBAR である細粒モードより非効率です。そのため、これらのアプリケーションに対するブロッキングやスロットリングが機能しない可能性があります。

細粒モードと粗粒モードの比較

粗粒モードには、メトリック レポート詳細において次の制限があります。

	細粒モード	粗粒モード
分類	最大限のディープ パケット インスペクション	簡易分類 以前の同様のパケットに基づく一部の分類
パフォーマンス	低速	高速
メモリ リソース	メモリ需要が高い	メモリ需要が低い
下位分類	完全サポート	部分サポート
フィールド抽出	完全サポート	部分サポート
最適な用途	パケット単位ポリシー 例： 特定の URL を検索するクラスマップ	特定のパケット単位操作に関する要件がない場合

NBAR の粗粒分類の設定方法

NBAR 分類モードの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nbar classification granularity coarse-grain**
4. **exit**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nbar classification granularity coarse-grain** 例： `Device(config)# ip nbar classification granularity coarse-grain`	NBAR の粗粒分類モードを設定します。
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

アプリケーション統計情報を使用した Performance Monitor コンテキストの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **performance monitor context** *context-name* **coarse-grain***profile-name*
4. **traffic-monitor application-client-server-stats**
5. **exit**
6. **interface** *type slot/port/number*
7. **performance monitor context** *context-name*
8. **end**
9. **show ip nbar classification granularity**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**performance monitor context** *context-name* **coarse-grain***profile-name* 例： `Device (config)# performance monitor context xyz profile application-statistics`	Performance Monitor コンフィギュレーション モードを開始し、アプリケーション統計プロファイルを使用してコンテキストを作成します。 （注） アプリケーション統計プロファイルを使用して Easy Performance Monitor（ezPM）ポリシーを設定すると、Network Based Application Recognition（NBAR）の粗粒分類モードが暗黙的に呼び出されます。ただし、NBAR の細粒分類モードを設定する必要がある場合は、アプリケーション統計プロファイルを使用して Performance Monitor コンテキストを設定した後で、**ip nbar classification granularity fine-grain** コマンドを使用します。
ステップ 4	**traffic-monitor application-client-server-stats** 例： `Device(config-perf-mon)# traffic-monitor application-client-server-stats`	指定されたメトリックを監視するようにトラフィック監視を設定します。
ステップ 5	**exit** 例： `Device(config-perf-mon)# exit`	Performance Monitor コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 6	**interface** *type slot/port/number* 例： `Device(config)# interfcace 0/2/2`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**performance monitor context** *context-name* 例： `Device (config-if)# performance monitor context xyz`	インターフェイス上の指定の Performance Monitor コンテキストを設定します。

	コマンドまたはアクション	目的
ステップ 8	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show ip nbar classification granularity** 例： `Device# show ip nbar classification granularity`	現在設定されている NBAR 分類モードを表示します。

NBAR の粗粒分類の設定例

例：NBAR 分類モードの設定

次に、NBAR の粗粒分類モードの設定例を示します。

```
Device> enable
Device# configure terminal
Device (config)# ip nbar classification granularity coarse-grain
Device (config)# end
```

例：アプリケーション統計情報プロファイルによるPerformanceMonitor コンテキストの設定

次に、アプリケーション統計情報プロファイルを使用して Easy Performance Monitor（ezPM）を設定し、おおまかな NBAR 分類モードを起動する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# performance monitor context xyz profile application-statistics
Device(config-perf-mon)# traffic-monitor application-client-server-stats
Device(config-perf-mon)# exit
Device(config)# interface gigabitEthernet 0/2/2
Device(config-if)# performance monitor context xyz
Device(config-if)# end
```

例：アプリケーション統計情報プロファイルを使用した Performance Monitor コンテキストの設定と細粒 NBAR 分類モード強制設定

次の例では、アプリケーション統計情報プロファイルを使用した ezPM ポリシーの設定方法と粗粒 NBAR 分類モードの強制設定方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# performance monitor context xyz profile application-statistics
Device(config-perf-mon)# traffic-monitor application-client-server-stats
Device(config-perf-mon)# exit
Device(config)# interface gigabitEthernet 0/2/2
Device(config-if)# performance monitor context xyz
Device(config-if)# end
Device (config)# ip nbar classification granularity fine-grain
```

例：NBAR 分類モードの確認

次の例は、現在設定されている NBAR 分類モードを確認する方法を示しています。

```
Device # show ip nbar classification granularity

NBAR classification granularity mode: coarse-grain
```

NBAR の粗粒分類に関する追加資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
AVC 構成	「AVC Configuration」モジュール

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

NBAR の粗粒分類の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *20*：*NBAR* の粗粒分類の機能情報

機能名	リリース	機能情報
NBAR の粗粒分類	Cisco IOS XE リリース 3.14S	Network Based Application Recognition（NBAR）は、粗粒と細粒の 2 つのレベルのアプリケーション認識機能を提供します。デフォルトでは、NBAR はその完全なアプリケーション認識機能を提供する細粒モードで動作します。粗粒モードでは、ディープ パケット インスペクションを最小限に抑えることにより、パフォーマンス メリットを提供し、メモリ リソースの需要を削減します。 次のコマンドが導入または変更されました： **ip nbar classification granularity** および **show ip nbar classification granularity**。

第 17 章

SSL カスタム アプリケーション

SSL カスタム アプリケーション機能を使用すれば、サーバ名（Client Hello 拡張内に存在する場合）またはサーバからクライアントに送信された証明書内の共通名を使用して、HTTP over Secure Socket Layer（HTTPS）などのセキュア ソケット レイヤ（SSL）経由の任意のプロトコルに対して動作するアプリケーションをカスタマイズすることができます。

- 機能情報の確認，193 ページ
- SSL カスタム アプリケーションに関する情報，194 ページ
- SSL カスタム アプリケーションの設定方法，197 ページ
- SSL カスタム アプリケーションの設定例，198 ページ
- SSL カスタム アプリケーションに関する追加情報，198 ページ
- SSL カスタム アプリケーションの機能情報，199 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

SSL カスタム アプリケーションに関する情報

SSL カスタム アプリケーションの概要

SSL カスタム アプリケーション機能を使用すれば、サーバ名（Client Hello 拡張内に存在する場合）またはサーバからクライアントに送信された証明書内の共通名を使用して、HTTP over Secure Socket Layer（HTTPS）などのセキュア ソケット レイヤ（SSL）経由の任意のプロトコルに対して動作するアプリケーションをカスタマイズすることができます。

HTTP over Secure Socket Layer（HTTPS）は、セキュア通信のための通信プロトコルです。HTTPS は、HTTP を SSL プロトコルの上に階層化した結果です。

SSL 下位分類では、パケットの後ろの方で出現するルールが適用されます。たとえば、サーバ名「finance.example.com」に対して「finance」のルールと example.com の別のルールが存在する場合は、「example.com」のルールが適用されます。

SSL unique name サブ分類

SSL unique-name パラメータは、グローバルで既知ではないか、まだ NBAR にサポートされていないサーバの SSL セッションに一致させるのに使用されます。unique-name は、SNI（Server Name Indication）フィールドが存在する場合はクライアント リクエスト内の SNI フィールドに一致するか、サーバの応答の第 1 の証明書内の共通名（CN）フィールドに一致します。

この機能はまた、ハンドシェイクを使用する SSL セッションではなく、session-id を使用する SSL セッションをサポートします。

サーバ名は HTTPS URL そのものの一部として使用できます。たとえば、URL https://www.facebook.com の場合、サーバ名は www.facebook.com です。ただし、証明書はブラウザにあります。ユーザは HTTPS アイコンをクリックして証明書情報を確認できます。

次の 2 つの図は、ユーザが Wireshark ツールを使用して確認できる、サーバ名と共通名の場所を示しています。

次の図は、SNI フィールドの場所を強調表示しています。

図 *4*：***Server Name Indication*** フィールド

```
⊟ Secure Sockets Layer
  ⊟ TLSv1 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 183
    ⊟ Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 179
        Version: TLS 1.0 (0x0301)
      ⊞ Random
        Session ID Length: 0
        Cipher Suites Length: 72
      ⊞ Cipher Suites (36 suites)
        Compression Methods Length: 2
      ⊞ Compression Methods (2 methods)
        Extensions Length: 65
      ⊟ Extension: server_name
          Type: server_name (0x0000)
          Length: 21
        ⊟ Server Name Indication extension
            Server Name list length: 19
            Server Name Type: host_name (0)
            Server Name length: 16
            Server Name: www.facebook.com
      ⊟ Extension: renegotiation_info
          Type: renegotiation_info (0xff01)
          Length: 1
        ⊞ Renegotiation Info extension
      ⊟ Extension: elliptic_curves
          Type: elliptic_curves (0x000a)
          Length: 8
          Elliptic Curves Length: 6
        ⊞ Elliptic curves (3 curves)
      ⊟ Extension: ec_point_formats
          Type: ec_point_formats (0x000b)
          Length: 2
          EC point formats Length: 1
        ⊞ Elliptic curves point formats (1)
      ⊟ Extension: SessionTicket TLS
```

353870

次の図は、CN フィールドの場所を強調表示しています。

図 *5* : ***Common Name*** フィールド

```
⊟ Secure Sockets Layer
  ⊟ TLSv1 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 1892
    ⊟ Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 1888
        Certificates Length: 1885
      ⊟ Certificates (1885 bytes)
          Certificate Length: 976
        ⊟ Certificate (id-at-commonName=www.facebook.com,id-at-organizationName=
          ⊟ signedCertificate
              version: v3 (2)
              serialNumber : 0x3c08cfeebe9febc42bb13ee03d620bdf
            ⊞ signature (shaWithRSAEncryption)
            ⊞ issuer: rdnSequence (0)
            ⊞ validity
            ⊟ subject: rdnSequence (0)
              ⊟ rdnSequence: 5 items (id-at-commonName=www.facebook.com,id-at-or
                ⊞ RDNSequence item: 1 item (id-at-countryName=US)
                ⊞ RDNSequence item: 1 item (id-at-stateOrProvinceName=California
                ⊞ RDNSequence item: 1 item (id-at-localityName=Palo Alto)
                ⊞ RDNSequence item: 1 item (id-at-organizationName=Facebook, Inc
                ⊟ RDNSequence item: 1 item (id-at-commonName=www.facebook.com)
                  ⊟ RelativeDistinguishedName item (id-at-commonName=www.faceboo
                      Id: 2.5.4.3 (id-at-commonName)
                    ⊟ DirectoryString: printableString (1)
                        printableString: www.facebook.com
            ⊞ subjectPublicKeyInfo
            ⊞ extensions: 7 items
          ⊞ algorithmIdentifier (shaWithRSAEncryption)
            Padding: 0
            encrypted: 0d8867ee01442a9146620f6728cc299befe7babcae72cdcf...
          Certificate Length: 903
        ⊟ Certificate (id-at-organizationalUnitName=www.verisign.com/CPS Incorp.
          ⊟ signedCertificate
```

SSL カスタム アプリケーションの設定方法

SSL カスタム アプリケーションの設定

手順の概要

1. **enable**
2. **configureterminal**
3. **ip nbar custom** *custom-protocol-name* **sslunique-name** *regex* **id** *selector-id*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nbar custom** *custom-protocol-name* **sslunique-name** *regex* **id** *selector-id* 例： `Device (config)# ip nbar custom name ssl unique-name www.example.com id 11`	SSL ベースのカスタム プロトコル照合を定義し、正規表現形式でホスト名を指定します。 （注） このコマンドで設定されたホスト名は、Client Hello 拡張機能の Server Name Indication（SNI）フィールド、またはサーバからクライアントに送信されるデジタル証明書内の Common Name（CN）フィールドに格納されます。
ステップ 4	**end** 例： `Router(config)# end`	（任意）グローバル コンフィギュレーション モードを終了します。

SSL カスタム アプリケーションの設定例

例：SSL カスタム アプリケーション

次に、SSL カスタム アプリケーションを設定する例を示します。このコマンドで設定されたホスト名は、Client Hello 拡張機能の Server Name Indication（SNI）フィールド、またはサーバからクライアントに送信されるデジタル証明書内の Common Name（CN）フィールドに格納されます。

```
Device> enable
Device# configuration terminal
Device(config)# ip nbar custom name ssl unique-name  www.example.com id  11
Device(config)# exit
```

SSL カスタム アプリケーションに関する追加情報

SSL カスタム アプリケーションに関する関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
SSL の小分類	「NBAR プロトコル パック」モジュール

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

SSL カスタム アプリケーションの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *21*：*SSL* カスタム アプリケーションの機能情報

機能名	リリース	機能情報
SSL カスタム アプリケーション	Cisco IOS XE リリース 3.15S	SSL カスタム アプリケーション機能を使用すれば、サーバ名（Client Hello 拡張内に存在する場合）またはサーバからクライアントに送信された証明書内の共通名を使用して、HTTP over Secure Socket Layer（HTTPS）などのセキュア ソケット レイヤ（SSL）経由の任意のプロトコルに対して動作するアプリケーションをカスタマイズすることができます。 次のコマンドが導入または変更されました。 **ip nbar custom**。

第 18 章

選択的アプリケーションのための細粒NBAR

デフォルトでは、NBARはその完全なアプリケーション認識機能を提供する細粒モードで動作します。パケット単位のレポートが必要なときに使用される細粒モードは、トラブルシューティングに有効です。細粒モードは、重要なアプリケーションのためにNBARで詳細なレイヤ7メトリックを抽出する必要がある場合にのみ使用することをお勧めします。選択的アプリケーションのための細粒NBAR機能を使用すれば、顧客は、詳細なレイヤ7メトリックのコレクションを含む重要なアプリケーションの動的なモニタリングができます。この機能は、他のアプリケーションが粗粒モードで動作しているときの特定のアプリケーションの速度低下のトラブルシューティングに役立つため、システムのパフォーマンスへの影響を防ぐことができます。

- 機能情報の確認，201 ページ
- 選択的アプリケーションのための細粒 NBAR に関する情報，202 ページ
- 選択的アプリケーションのための細粒 NBAR の設定方法，202 ページ
- 選択的アプリケーションのための細粒 NBAR の設定例，203 ページ
- 選択的アプリケーションのための細粒 NBAR に関する追加情報，204 ページ
- 選択的アプリケーションのための細粒 NBAR の機能情報，204 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

選択的アプリケーションのための細粒 NBAR に関する情報

選択的アプリケーションのための細粒 NBAR の概要

NBAR は、粗粒と細粒という 2 つのレベルのアプリケーション認識を提供します。デフォルトでは、NBAR はその完全なアプリケーション認識機能を提供する細粒モードで動作します。デフォルトの NBAR 細粒モードは、細粒モードと粗粒モードが別々に導入される以前の NBAR の機能とパフォーマンスと等価です。これは、既存の設定に対する完全な後方互換性を提供します。

パケット単位のレポートが必要なときに使用される細粒モードは、トラブルシューティングに有効です。細粒モードは、重要なアプリケーションのために NBAR で詳細なレイヤ 7 メトリックを抽出する必要がある場合にのみ使用することをお勧めします。選択的アプリケーションのための細粒 NBAR 機能を使用すれば、顧客は、詳細なレイヤ 7 メトリックのコレクションを含む重要なアプリケーションの動的なモニタリングができます。この機能は、他のアプリケーションが粗粒モードで動作しているときの特定のアプリケーションの速度低下のトラブルシューティングに役立つため、システムのパフォーマンスへの影響を防ぐことができます。

選択的アプリケーションのための細粒 NBAR の設定方法

選択的アプリケーションのための細粒 NBAR の設定

手順の概要

1. **enable**
2. **configureterminal**
3. **ip nbar classification granularity fine-grain protocol** *protocol-name*
4. **exit**
5. **show ip nbar classification granularity protocol** *protocol-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nbar classification granularity fine-grain protocol** *protocol-name* 例： `Device(config)# ip nbar classification granularity fine-grain protocol 3pc`	NBARの細粒分類モードを設定し、アプリケーションを表すプロトコル名を指定します。
ステップ 4	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 5	**show ip nbar classification granularity protocol** *protocol-name* 例： `Device(config)# show ip nbar classification granularity protocol 3pc`	現在設定されている NBAR 分類モードを表示します。

選択的アプリケーションのための細粒 NBAR の設定例

例：選択的アプリケーションのための細粒 NBAR

次に、NBAR の細分分類モードを設定し、アプリケーションを表すプロトコル名を選択する例を示します。

```
Device> enable
Device# configuration terminal
Device(config)# ip nbar classification granularity fine-grain protocol 3cp
Device(config)# exit
```

例：選択的アプリケーションのための細粒 NBAR の確認

次の例は、現在設定されているプロトコルの分類の詳細度を確認する方法を示しています。

```
Device # show ip nbar classification granularity protocol 3pc

Protocol                  Force mode
-------------------------------------
3pc                       fine-grain
```

選択的アプリケーションのための細粒 NBAR に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
AVC 構成	「AVC Configuration」モジュール

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

選択的アプリケーションのための細粒 NBAR の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *22*：選択的アプリケーションのための細粒 *NBAR* の機能情報

機能名	リリース	機能情報
選択的アプリケーションのための細粒 NBAR	Cisco IOS XE リリース 3.15S	デフォルトでは、NBARはその完全なアプリケーション認識機能を提供する細粒モードで動作します。パケット単位のレポートが必要なときに使用される細粒モードは、トラブルシューティングに有効です。細粒モードは、重要なアプリケーションのために NBAR で詳細なレイヤ7メトリックを抽出する必要がある場合にのみ使用することをお勧めします。選択的アプリケーションのための細粒NBAR機能を使用すれば、顧客は、詳細なレイヤ7メトリックのコレクションを含む重要なアプリケーションの動的なモニタリングができます。この機能は、他のアプリケーションが粗粒モードで動作しているときの特定のアプリケーションの速度低下のトラブルシューティングに役立つため、システムのパフォーマンスへの影響を防ぐことができます。 次のコマンドが導入または変更されました。 **ip nbar custom**。

第 19 章

DNS 名に基づく NBAR カスタム アプリケーション

DNS 名に基づく NBAR カスタム アプリケーション機能は、ドメイン ネーム システム（DNS）のホスト名に基づいてアプリケーションをカスタマイズするメカニズムを提供します。

- 機能情報の確認，207 ページ
- DNS 名に基づく NBAR カスタム アプリケーションの前提条件，208 ページ
- DNS 名に基づく NBAR カスタム アプリケーションの制限事項，208 ページ
- DNS 名に基づく NBAR カスタム アプリケーションに関する情報，208 ページ
- DNS 名に基づく NBAR カスタム アプリケーションの設定方法，209 ページ
- DNS 名に基づく NBAR カスタム アプリケーションの設定例，210 ページ
- DNS 名に基づく NBAR カスタム アプリケーションに関する追加情報，210 ページ
- DNS 名に基づく NBAR カスタム アプリケーションの機能情報，211 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

DNS 名に基づく NBAR カスタム アプリケーションの前提条件

ドメイン名に関する基本的な知識が必要です。

DNS 名に基づく NBAR カスタム アプリケーションの制限事項

ドメイン ネーム システム（DNS）を使用するには、ネットワークに DNS ネーム サーバが必要です。

DNS は UDP タイプのメッセージだけを読み取ることができ、53 の送信元ポートを持つ応答パケットだけを考慮します。

DNS 名に基づく NBAR カスタム アプリケーションに関する情報

DNS 名に基づく NBAR カスタム アプリケーションの概要

Network-Based Application Recognition（NBAR）は、一連のプロトコルおよびアプリケーション タイプに基づいて、ネットワーク トラフィックを認識および分類します。カスタムプロトコルを作成することによって、NBAR が認識するプロトコルとアプリケーション タイプのセットに追加します。

DNS ホスト名の署名を指定するには、簡易な正規表現形式の **ip nbar custom***custom1 dns domain-name regular-expression id* コマンドを使用します。この署名を DNS サーバが DNS テンプレートにプッシュします。DNS ベースの分類は、直接応答として抽出された IP アドレスが将来の分類ルックアップ用にルックアップ テーブル（LUT）に追加された場合にのみ機能します。

次のタイプのドメインがサポートされます。

- A
- AAAA
- CNAME

ip nbar custom myDns dns domain-name*example* コマンドを定義すると、式「example」と一致するドメイン名の DNS トラフィックがデバイスに到着します。NBAR は、テーブル内の式「example」とドメイン名が一致するドメインの対応する IP アドレス A.B.C.D を保存します。IP アドレスが A.B.C.D の TCP または UDP トラフィックが到着すると、myDns プロトコルとして分類されます。

DNS 名に基づく NBAR カスタム アプリケーションの設定方法

DNS 名に基づく NBAR カスタム アプリケーションの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nbar custom** *custom-name* **dns** *domain-name regular-expression* **id** *1*
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nbar custom** *custom-name* **dns** *domain-name regular-expression* **id** *1* 例： `Device(config)# ip nbar custom cust1 dns dns-name *example.com id 1`	DNS 名に基づく NBAR カスタム アプリケーションを設定します。 （注） 完全なドメイン名またはその一部を正規表現で指定できます。例：表現「*example」は、「example」という語を含むすべてのドメインと一致します。
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

DNS 名に基づく NBAR カスタム アプリケーションの設定例

例：DNS 名に基づく NBAR カスタム アプリケーションの設定

```
Device> enable
Device# configure terminal
Device(config)#  ip nbar custom custom1 dns domain-name *example id 11
Device(config)# exit
```

DNS 名に基づく NBAR カスタム アプリケーションに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

DNS 名に基づく NBAR カスタム アプリケーションの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *23*：*DNS* 名に基づく *NBAR* カスタム アプリケーションの機能情報

機能名	リリース	機能情報
DNS 名に基づく NBAR カスタム アプリケーション	Cisco IOS XE リリース 3.15S	NBAR Custom Applications Based on Domain Name Service (DNS) Name 機能は、DNS ホスト名に基づいてアプリケーションをカスタマイズするためのメカニズムを提供します。 次のコマンドが導入または変更されました。 **ip nbar custom**。

第 20 章

NBAR2 auto-learn

NBAR2 auto-learn は、それ以外の方法では NBAR2 プロトコルで認識されないトラフィックの分類を改善します。一般的な HTTP または SSL トラフィックでは、NBAR2 がパケット ヘッダー フィールドからホスト名を特定できます。未知のトラフィックでは、最も多く出現するサーバ側のポートとソケットを追跡できます。これらのメカニズムは、他の一般的なまたは未知のトラフィックをより適切に分類するためのカスタム プロトコルの作成を容易にします。

（注） NBAR2 auto-learn は、以前は、「NBAR Customized Assistance Based on SSL or HTTP」と呼ばれていました。

- 機能情報の確認，213 ページ
- NBAR2 auto-learn の概要，214 ページ
- NBAR2 auto-learn の設定方法，215 ページ
- NBAR2 auto-learn の設定例，219 ページ
- NBAR2 auto-learn に関する追加情報，221 ページ
- NBAR2 auto-learn の機能情報，221 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

NBAR2 auto-learn の概要

ネットワーク トラフィックの一部を NBAR2 メカニズムで明確に特定することが困難な場合があります。このようなトラフィックは、**一般的な** HTTP または SSL としてまたは**未知**として分類されます。この場合は、トラフィックに関する有益な情報がほとんど得られません。

NBAR2 auto-learn は、一般的な HTTP/SSL または未知に分類されたトラフィックを分析します。

- 一般的な HTTP/SSL トラフィックでは、トラフィック内のパケット ヘッダー フィールドからホスト名を抽出して、一般的なトラフィック上に出現する「トップ ホスト」を追跡します。これは、トラフィック量が特に多いホストを意味します。トップ ホストのリストは、トラフィック量の多い順に並べられます。トラフィック量が最大のホストがリストの一番上に表示されます。
- 未知のトラフィックでは、サーバ側のポートを特定して、未知のトラフィック上に出現する「トップ ポート」と「トップ ソケット」を追跡します。これは、トラフィック量が特に多いポートとソケットを意味します。トップ ポートとソケットのリストは、トラフィック量の多い順に並べられます。トラフィック量が最大のポートとソケットがリストの一番上に表示されます。

一般的なトラフィックの「トップ ホスト」のリストと未知のトラフィックの「トップ ポート」/「トップ ソケット」のリストは、トラフィックをより適切に特定して分類するプロトコルの作成においてカスタム プロトコル メカニズムを支援するために使用できます。たとえば、トップ ホストは、カスタム プロトコルの作成で使用される「候補」ホストを提供します。

メカニズムの詳細

NBAR は、組み込み NBAR2 プロトコルが認識しないトラフィックを特定するカスタム プロトコルの作成をサポートします。

- **一般的な** HTTP または SSL トラフィックでは、NBAR2 auto-learn が次のいずれかから関連ホスト名を抽出できます。
  - Client Hello 拡張内のサーバ名フィールド
  - クライアントがサーバに送信するデジタル証明書内の共通名フィールド
- **未知の**トラフィックでは、サーバ側のポート番号を抽出できます。

例

たとえば、NBAR2 がエンタープライズ メール サーバのトラフィックを分類できない場合は、トラフィックが SSL としてのみ分類されます。この機能は、トラフィックをより明確に特定するカスタム プロトコルの作成を支援し、メール サーバ トラフィックのレポートを充実させることができます。

NBAR2 auto-learn の設定方法

NBAR2 auto-learn の設定

- HTTP または SSL の汎用トラフィックの場合、NBAR2 auto-learn は、最も頻繁に出現したホスト（「top hosts」）のリストを収集します。不明トラフィックの場合、この機能は、最も頻繁に出現したサーバ側ポート（「top ports」）とソケット（「top sockets」）のリストを収集します。この情報は、カスタム プロトコルの作成を促進するために、自動カスタム メカニズムに取り込まれることがあります。
- パフォーマンスを最適化するため、このシステムでは汎用トラフィックと不明トラフィックのすべてのフローを追跡するのではなく、特定のサンプル レートを使用してフローをサンプリングします。デフォルトでは、NBAR2 は top hosts を分析するために、トラフィック基づいて動的にサンプル レートを設定します。サンプル レートの設定については、NBAR2 auto-learn の設定, （215 ページ）を参照してください。
- デフォルトでは、top hosts の追跡が有効になり、top ports と top sockets の追跡が無効になります。
- 「top sockets」の auto-learn は、「top ports」が有効化または無効化されると、自動的に有効または無効になります。

手順の概要

1. **enable**
2. **configureterminal**
3. **ipnbarclassificationauto-learn** { **top-hosts** | **top-ports** }
4. **ipnbarclassificationauto-learn** { **top-hosts** | **top-ports** } **sample-rate***rate*
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 3	**ipnbarclassificationauto-learn** { **top-hosts** | **top-ports** }
	
	例：
	`Device (config)# ip nbar classification auto-learn top-hosts`
	`Device (config)# ip nbar classification auto-learn top-ports`
		top-hosts：汎用として分類されるトラフィックの分析を有効にして、汎用トラフィックの top hosts のリストを生成します。
		
		top-ports：不明として分類されるトラフィックの分析を有効にして、不明トラフィックで出現するサーバ側の top ports と top sockets のリストを生成します。

ステップ 4	**ipnbarclassificationauto-learn** { **top-hosts** | **top-ports** } **sample-rate***rate* 例： `Device (config)# ip nbar classification auto-learn top-ports sample-rate 5`	（任意）この機能のフロー サンプリング レートを設定します。パフォーマンスを最適化するため、このメカニズムではすべての汎用トラフィックと不明トラフィックを追跡するのではなく、特定のサンプル レートを使用してフローをサンプリングします。数字が小さい場合、精度は向上しますが、より多くのルータ リソースが必要となります。 *rate* の値が 1 である場合、このメカニズムでは、汎用トラフィック（**top-hosts**）または不明トラフィック（**top-ports**）のすべてのフローをサンプリングします。 **top-hosts** のデフォルト：NBAR2 はトラフィックに基づいてレートを動的に設定します。 **top-ports** のデフォルト：128
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了します。

auto-learn の上位ホストまたはポートの表示

手順の概要

1. **showipnbarclassificationauto-learn** { **top-hosts** | **top-ports** } *number_of_entries* [**detailed**]

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**showipnbarclassificationauto-learn** { **top-hosts** | **top-ports** } *number_of_entries* [**detailed**]
	
	例：
	`Device (config)# show ip nbar classification auto-learn top-hosts 10 detailed`
	
	`Device (config)# show ip nbar classification auto-learn top-ports 25`
		汎用トラフィック内の上位ホストまたは不明なトラフィック内の上位サーバ側ポートの統計情報を表示します。
		
		number_of_entries：表示するエントリの最大数。指定できる値：1 ～ 100
		
		detailed：それぞれのバイト、フロー、パケット カウントなど、その他の情報を指定します。

auto-learn の上位ソケットの表示

auto-learn のコンテキストで、ソケットとはサーバ側のソケット アドレス（IP アドレスとポート）を指します。

（注） top-ports を有効または無効にすると、auto-learn top-sockets 機能が自動的に有効または無効になります。

手順の概要

1. **showipnbarclassificationauto-learntop-sockets***number_of_entries* [**detailed**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**showipnbarclassificationauto-learntop-sockets***number_of_entries* [**detailed**] 例： `Device (config)# show ip nbar classification auto-learn top-sockets 100 detailed`	不明なトラフィック内の上位ソケットの統計情報を表示します。 *number_of_entries*：表示するエントリの最大数。指定できる値：1 ～ 100 **detailed**：それぞれのバイト、フロー、パケット カウントなど、その他の情報を指定します。

NBAR2 auto-learn のホスト/ポート統計のクリア

この手順は、汎用または不明と分類されたトラフィックのために NBAR2 auto-learn 機能によって作成されるホスト、ポート、およびソケットのリストに対して機能します。

このコマンドは、ホスト（**top-hosts** オプション）、またはポートとソケット（**top-ports** オプション）のために収集された統計データ（バイト、パケット、フローなど）をクリアしますが、最近トラフィックが検出されなかった古いホスト/ポート/ソケットはクリアしません。これを **clear ip nbar classification auto-learn top-hosts restart**（統計をクリアし、古いホスト/ポート/ソケットもクリアする）と比較してください。

手順の概要

1. **clearipnbarclassificationauto-learn** { **top-hosts** | **top-ports** } **statistics**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**clearipnbarclassificationauto-learn** { **top-hosts** | **top-ports** } **statistics** 例： `Device# clear ip nbar classification auto-learn top-hosts statistics`	ホスト（**top-hosts** オプション）またはポートとソケット（**top-ports** オプション）のために収集された統計データをクリアします。

NBAR2auto-learnのホスト/ポスト統計と非アクティブホスト/ポートのクリア

この手順は、汎用または不明と分類されたトラフィックのために NBAR2 auto-learn 機能によって作成されるホスト、ポート、およびソケットのリストに対して機能します。

この手順は、ホスト（**top-hosts** オプション）、またはポートとソケット（**top-ports** オプション）のために収集された統計データ（バイト、パケット、フローなど）をクリアし、さらに最近のトラフィックが検出されなかった古いホスト/ポート/ソケットをクリアします。これを **clear ip nbar classification auto-learn top-hosts statistics**（統計はクリアするが、ホスト/ポート/ソケットはクリアしない）と比較してください。

手順の概要

1. **clearipnbarclassificationauto-learn** { **top-hosts** | **top-ports** } **restart**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**clearipnbarclassificationauto-learn** { **top-hosts** | **top-ports** } **restart** 例： `Device# clear ip nbar classification auto-learn top-hosts restart`	ホスト（**top-hosts** オプション）またはポート（**top-ports** オプション）のために収集された統計データをクリアし、さらに最近トラフィックが検出されなかった古いホスト/ポート/ソケットをクリアします。

NBAR2 auto-learn の設定例

例：ホストの auto-learn の設定

```
Device> enable
Device# configuration terminal
Device (config)# ip nbar classification auto-learn top-hosts
Device (config)# exit
```

例：auto-learn データの表示

上位のホスト

show ip nbar classification auto-learn top-hosts コマンドの出力（**detailed** オプションなし）。

```
Device#show ip nbar classification auto-learn top-hosts 10

Total bytes:         23.236 M
Total packets:       31.816 K
Total flows:         229
Sample rate last:    1
Sample rate average: 1
Sample rate min:     1
Sample rate max:     1
--------------------------------------------------------------------------------
  #|Host                                     |Byte%|Flow%|Pkt% |Type |Field
--------------------------------------------------------------------------------
  1|images1.xyz.com                          | 37% | 34% | 38% |http |host
  2|res.cloudinary.com                       | 34% |  3% | 25% |http |host
  3|mail.cisco.com                           | 27% | 62% | 35% |ssl  |host
  4|10.210.20.19                             | <1% | <1% | <1% |http |host
```

上位のホスト - 詳細

show ip nbar classification auto-learn top-hosts コマンドの出力（**detailed** オプション付き）。

```
Device# show ip nbar classification auto-learn top-hosts 10 detailed
Total bytes:         23.236 M
Total packets:       31.816 K
Total flows:         229
Sample rate last:    1
Sample rate average: 1
Sample rate min:     1
Sample rate max:     1
-----------------------------------------------------------------------------------------------

  #|Host                 |Byte count |Byte%|Flow count |Flow%|Pkt count  |Pkt% |Type |Field
-----------------------------------------------------------------------------------------------

  1|site.xyz.com          |8.707 M    | 37% |79         | 34% |12.239 K   | 38% |http |host

  2|res.cloudinary.com    |8.045 M    | 34% |7          |  3% |8.162 K    | 25% |http |host

  3|mail.cisco.com        |6.363 M    | 27% |142        | 62% |11.315 K   | 35% |ssl  |host

  4|10.210.20.19          |120.111 K  | <1% |1          | <1% |100        | <1% |http |host
```

上位のソケット

auto-learn のコンテキストで、ソケットとはサーバ側のソケットアドレス（IP アドレスとポート）を指します。

（注） top-ports を有効または無効にすると、auto-learn top-sockets 機能が自動的に有効または無効になります。

show ip nbar classification auto-learn top-sockets コマンドの出力（見やすくなるよう修正済み）。

```
Device#show ip nbar classification auto-learn top-sockets 100 detailed
Total bytes:  398.747 K
Total packets:         1.611 K
Total flows:           1.109 K
Sample rate last:    1
Sample rate average: 1
Sample rate min:     1
Sample rate max:     1
-----------------------------------------------------------------------------------------------
 #|Port  |IP              |Byte count |Byte%|Flow |Flow%|Pkt   |Pkt% |Traffic |Asymmetric
  |      |                |           |     |count|     |count |     |Type    |byte
  |      |                |           |     |     |     |      |     |        |count
-----------------------------------------------------------------------------------------------
 1|80    |173.38.201.172  | 81.776 K  | 20% |  4  | <1% | 90   |  5% |TCP     |0
 2|80    |173.38.201.174  | 74.555 K  | 18% |  4  | <1% | 84   |  5% |TCP     |0
 3|123   |10.56.129.33    | 42.672 K  | 10% |889  | 80% |889   | 55% |UDP     |N/A
 4|443   |47.88.68.98     |  1.472 K  | <1% |  3  | <1% | 10   | <1% |TCP     |0
 5|1080  |10.56.217.8     |  1     K  | <1% |  1  | <1% |  1   | <1% |TCP     |0
 6|63699 |10.210.20.123   | 213       | <1% |  1  | <1% |  1   | <1% |TCP     |0
 7|443   |171.70.124.118  | 37        | <1% |  1  | <1% |  1   | <1% |TCP     |0
 8|37814 |10.210.20.122   | 14        | <1% |  1  | <1% |  2   | <1% |TCP     |0
 9|443   |140.205.195.83  | 12        | <1% |  1  | <1% |  2   | <1% |TCP     |0
10|443   |10.61.25.91     |  7        | <1% |  1  | <1% |  1   | <1% |TCP     |0
```

NBAR2 auto-learn に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
QoS コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『Cisco IOS Quality of Service Solutions Command Reference』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

NBAR2 auto-learn の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *24*：*NBAR Customization Assistance Based on SSL or HTTP* の機能情報

機能名	リリース	機能情報
NBAR2 auto-learn （従来の名称は「NBAR Customization Assistance based on SSL or HTTP」）	Cisco IOS XE リリース 3.16S、Cisco IOS リリース 15.5(3)T	カスタム プロトコルを作成して、汎用トラフィックまたは不明トラフィックの分類機能の改善を支援します。 次のコマンドが導入または変更されました：**ip nbar classification auto-learn top-hosts**、**ip nbar classification auto-learn top-ports**、**ip nbar classification auto-learn top-ports sample-rate**、**show ip nbar classification auto-learn top-hosts**、**show ip nbar classification auto-learn top-ports**、**clear ip nbar classification auto-learn top-ports restart**、**clear ip nbar classification auto-learn top-hosts**、**clear ip nbar classification auto-learn top-ports statistics**

第 21 章

DNS-AS

DNS-AS（DNS as Authoritative Source）は、カスタム アプリケーション分類情報の中央集中型制御を可能にします。

このモジュールでは、DNS-AS の設定と使用に関する概念とタスクについて説明します。

- はじめに，223 ページ
- DNS-AS メカニズム，229 ページ
- DNS-AS のセットアップ，231 ページ
- ネットワークへの新しいアプリケーションの導入，233 ページ
- 制約事項，233 ページ
- DNS-AS CLI コマンド，234 ページ
- DNS-AS のトラブルシューティング，247 ページ

はじめに

DNS-AS（DNS as Authoritative Source）は、Cisco NBAR2 と共に機能することにより、カスタム アプリケーション分類情報の中央集中型制御を可能にします。NBAR2 が分類情報（アプリケーション名、ID、トラフィック クラス、ビジネスとの関連性などのメタデータ）を使用することにより、特定のアプリケーションのネットワーク トラフィックを認識し、ネットワーク トラフィック ポリシーのレポート作成とポリシーの適用の両方に有用なパラメータを割り当てることによってトラフィックを分類します。

分類メタデータには組織のニーズとポリシーの目的が反映される

企業によって、ネットワーク トラフィック ポリシーを手段にしたトラフィックのレポートとシェーピングに関する要件が異なります。これは、組織内部で使用されているローカル アプリケーションが異なるためと、広く使用されているアプリケーションのビジネスとの関連性が組織によって異なるためです。

そのため、ネットワーク トラフィックがトラフィック ポリシーによってどのようにレポートされ、シェーピングされるかを判断するには、多くの場合、アプリケーション分類情報のカスタマイズが役立ちます。

DNS インフラストラクチャの活用

DNS-AS は、汎用的に利用可能な DNS クエリ/応答インフラストラクチャを活用して、組織内のローカル DNS サーバからエンタープライズ ネットワーク内のルータにアプリケーション分類情報を伝達できるようにします。ローカル DNS サーバは、DNS データとカスタム分類データの両方の「信頼すべき情報源」として機能します。

DNS-AS は柔軟かつ単純なので、他の方法では設定が困難なトラフィック レポートおよびシェーピング機能を活用可能にします。

DNS-AS の利用

セットアップ

DNS-AS のセットアップには、エンタープライズ ネットワーク内のローカル DNS サーバとルータ上の設定手順が含まれます。

ローカル DNS サーバは、特定の「信頼されたドメイン」サイト/アプリケーションに関する分類情報で設定されます。これにより、ネットワーク管理者は、エンタープライズ イントラネットで使用されているようなこれらのローカルなサーバ ベースのアプリケーションのトラフィックをネットワークで処理する方法を制御することができます。

ルータは、DNS-AS によって制御される「信頼されたドメイン」（サイト/アプリケーション）の DNS トラフィックを検出するように設定されます。

分類情報の伝達

設定が完了すると、DNS サーバは、「信頼されたドメイン」アプリケーションに関する分類情報を提供できます。

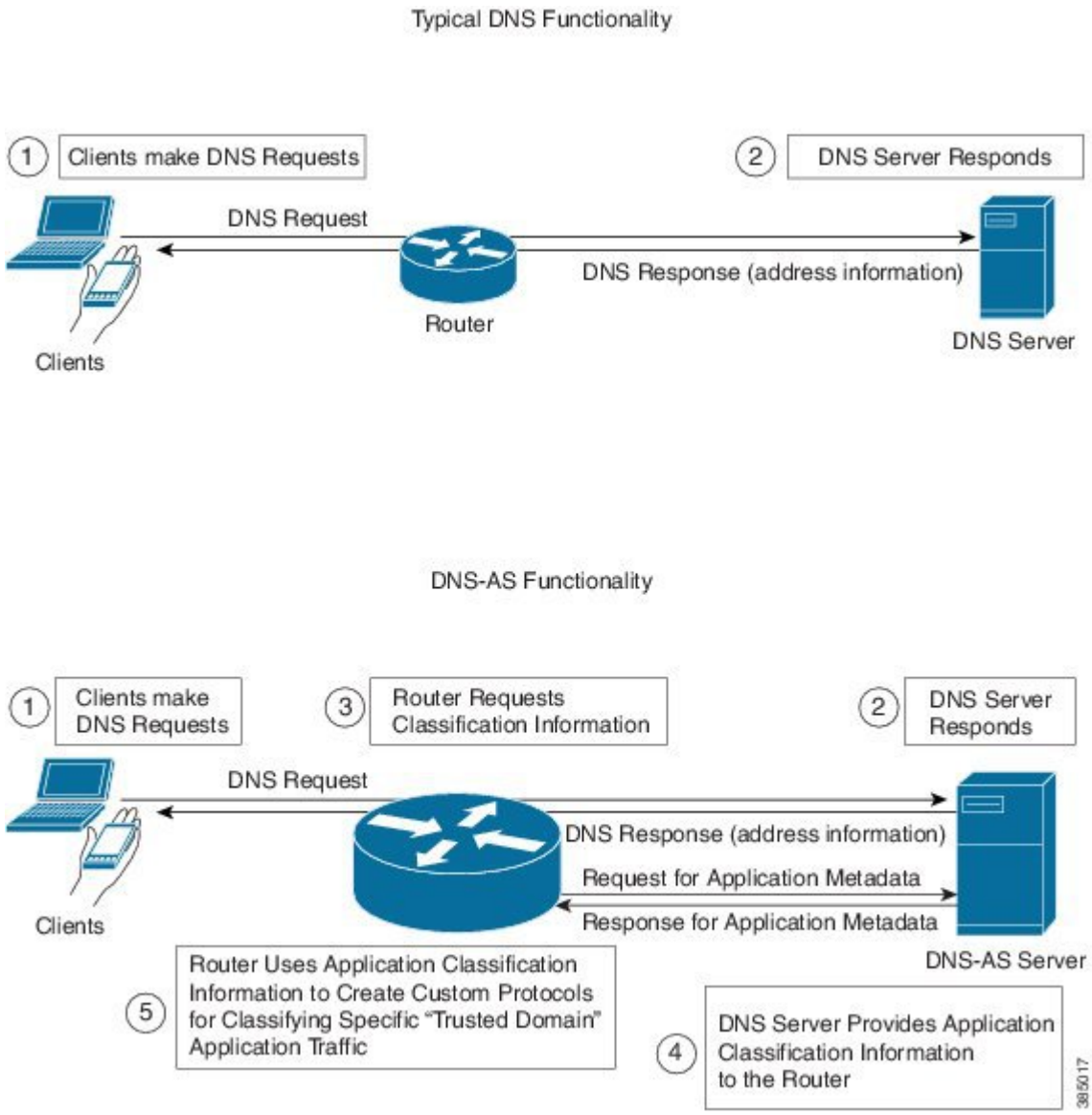
ネットワーク内のクライアントが DNS 要求を発行した場合は、DNS 応答が通常どおり送信されます。要求が「信頼されたドメイン」アプリケーションに関連している場合は、ルータがローカル DNS サーバにアプリケーションを問い合わせます。DNS サーバは、ネットワーク アドレス データと関連分類情報をルータに送信します。

分類情報の使用

情報を受信したルータ上では、NBAR2 がその情報を使用してトラフィックを分類するカスタム プロトコルを自動的に作成します。

トラフィック分類は、トラフィックのレポート作成などのアプリケーションの可視性機能に影響を与えるとともに、QoS トラフィック シェーピング ポリシーの使用などのアプリケーション制御にも影響を与えます。

図 *6*：*DNS-AS* 機能



プライオリティ

カスタム アプリケーション プロトコルは標準の Cisco NBAR2 プロトコル パック プロトコルより優先されるため、DNS-AS を使用してアプリケーション分類メタデータを設定することにより、プロトコル パック プロトコルをオーバーライドすることができます。

事前定義のプロトコルとカスタマイズされたプロトコル

NBAR2 プロトコル パック内の事前定義のプロトコルは、ほとんどのネットワーク トラフィックの識別と分類に使用できます。

企業のイントラネット内のサイトやアプリケーションなどのプロトコル パックでカバーされないローカル アプリケーションの場合は、DNS-AS がトラフィックを制御するための中央集中型メカニズムを提供します。

分類とトラフィック ポリシー

アプリケーション分類とトラフィック ポリシーは、関連性がありますが、別個のものです。DNS-AS は分類情報を提供しますが、トラフィック ポリシーを直接制御するわけではありません。

アプリケーションの分類を制御するものは次のとおりです。

- シスコが提供するプロトコル パック
- ユーザ定義のプロトコル
- 自動生成されたカスタム プロトコル
- カスタム プロトコルを間接的に作成する DNS-AS 指定のアプリケーション メタデータ

トラフィック ポリシーを定義するものは次のとおりです。

- ルータ上のポリシーの直接設定
- トラフィック ポリシーを提供する SDN などのネットワーク コントローラ

次の表に、アプリケーションの分類を制御可能なプロトコルのタイプ別の違いを示します。

表 *25*：アプリケーション分類を制御するプロトコル タイプ

プロトコル タイプ	送信元
NBAR2 プロトコル パック プロトコル	シスコが提供
手動で定義されたカスタム プロトコル	ルータ上でユーザが定義
DNS-AS を使用して自動的に定義されたカスタム プロトコル	ユーザ定義 • DNS-AS サーバで設定されたアプリケーション メタデータ • ルータで設定された信頼されたドメイン

効率的な中央集中型設定

DNS-AS を使用するメリットは設定の効率性です。DNS-AS は、エンタープライズ ネットワーク全体でのアプリケーション分類の制御に役立ちますが、その設定タスクのほとんどはネットワーク内で動作しているローカル DNS-AS サーバ上で処理されます。

次のような設定タスクがあります。

- **アプリケーション メタデータの設定**：DNS-AS サーバのセットアップ中の各「信頼されたドメイン」アプリケーション用のメタデータの定義。任意の時点でのメタデータの変更。
- **信頼されたドメインの設定**：信頼されたドメインは、ネットワーク内の個々のルータ上で設定されます。

適応性

中央集中型設定は、ローカル アプリケーションの変化への対応を容易にします。たとえば、ローカルアプリケーションを処理しているサーバのIPアドレスが変化した場合やアプリケーションのメタデータ属性（application-class や business-relevance など）が変化した場合は、ローカル DNS-AS サーバ上で変更を設定すれば、その更新がネットワーク全体のルータに伝達されます。

DNS-AS と SDN コントローラの機能の比較

DNS-AS と SDN コントローラは、使用された場合、どちらもネットワーク上の広範囲にわたって動作します。SDN コントローラはネットワーク内のデバイスにトラフィック ポリシーを提供するのに対して、DNS-AS はアプリケーション一致メタデータを提供します。

進化するネットワークとネットワーク トラフィックに対応するNBAR2

エンドツーエンドの暗号化を使用したアプリケーション

今日のネットワーク アプリケーションの多くは、HTTP などの一般的なトランスポート経由のクリア テキストで動作します。これらのアプリケーションは、ディープ パケット インスペクション（DPI）というリソースを大量に消費する方式を使用して識別できます。ただし、エンドツーエンドの暗号化を使用して通信しているネットワーク アプリケーションの数が増えるほど、DPI による識別が困難になります。

クラウドに移行するエンタープライズ ネットワーキング

エンタープライズ ネットワークのトレンドはクラウドへの移行です。独自の本格的なエンタープライズネットワークを運用する代わりに、組織は、ネットワーク インフラストラクチャをクラウド サービス プロバイダーに移行しつつあります。こうした会社は縮小された内部ネットワークで、世界中のあらゆる場所に設置されたさまざまなネットワーク デバイスを制御しなければならない場合があります。クラウドサービスプロバイダーによって管理されるこれらのデバイスは、直接管理統制下にあるとは限りません。

NBAR の柔軟性と俊敏性

DNS-AS などの Cisco NBAR2 機能は、エンタープライズ ネットワーキングのトレンドの変化に対応するように進化し続けています。エンドツーエンドの暗号化とクラウドへの移行によって、Application Visibility and Control を提供するタスクは複雑化しますが、NBAR が以下を目指すことに変わりはありません。

- ネットワーク設定の簡素化
- 規模に応じた俊敏性

カスタム プロトコル機能との比較

DNS-AS 設定プロセスは、NBAR2 **カスタム プロトコル**機能を使用して組織に関連する特定のアプリケーション用のプロトコルを作成する方法といくつかの点で似ていますが、DNS-AS は個々のアプリケーションに対してルータ単位では動作しません。

また、DNS-AS は、ネットワーク内の大量のデバイスによるカスタム アプリケーションの処理を再設定する場合に、より簡単な手段を提供します。

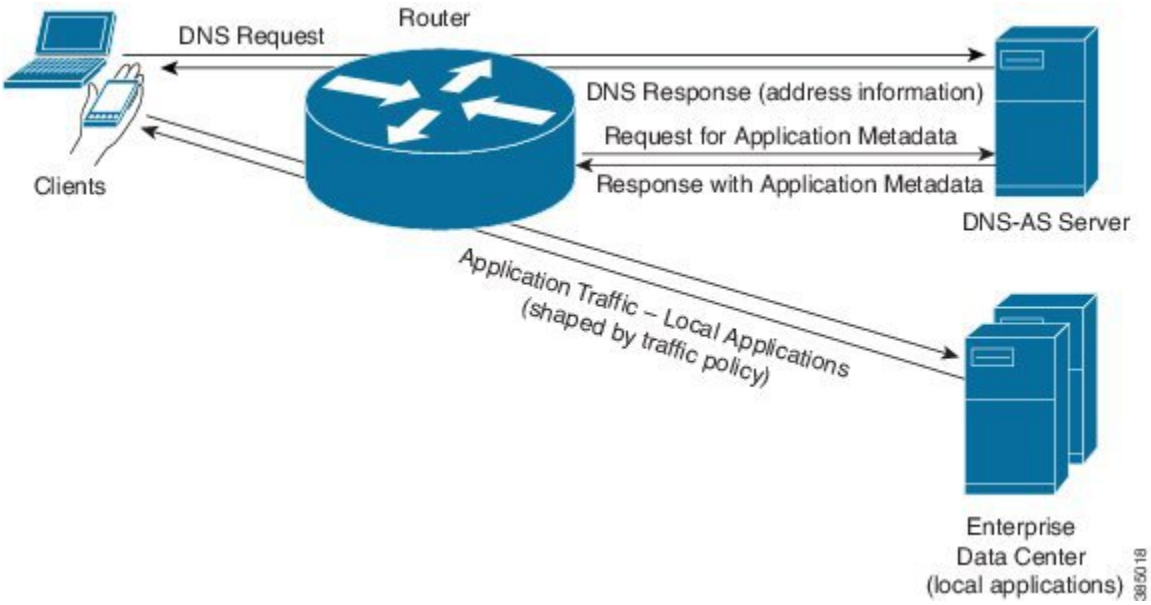
- **カスタム プロトコル**機能を使用している場合は、カスタム アプリケーションのいずれかの属性が変化した場合やアプリケーションをホストしているサーバが変化した場合に、ネットワーク内のルータごとにカスタムアプリケーションプロトコルを更新する必要があります。数百台のルータを含むネットワークでは、このプロセスは現実的ではありません。
- **DNS-AS** を使用している場合は、DNS サーバ上の 1 回の再設定によって、ネットワーク内のすべてのルータに情報が伝達されます。

DNS-AS メカニズム

基本的なトポロジ

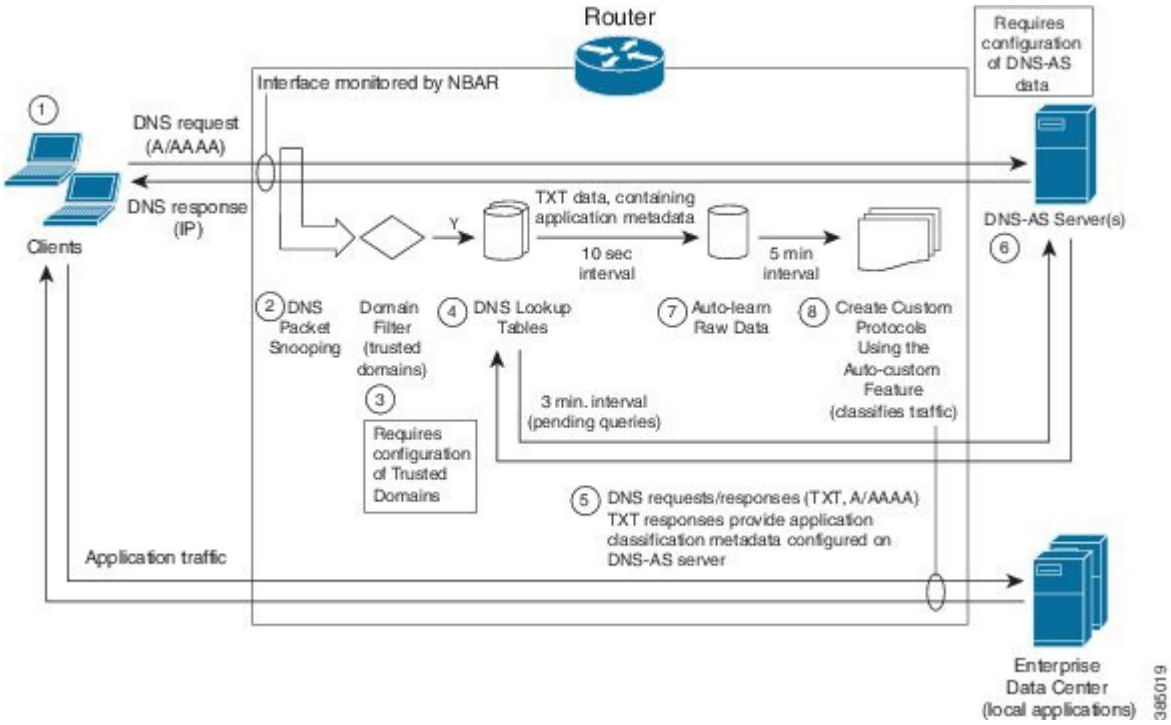
次の図に、DNS-AS サーバがエンタープライズ ネットワーク内のクライアント（ユーザ デバイス）、ルータ、およびデータセンター（ローカル アプリケーションをホストしている）とどのように連動するかを示します。

図 **7**：トポロジ



メカニズムの詳細

図 *8*：メカニズムの詳細



1.クライアント（ネットワーク内の PC）が、信頼されたドメインとして定義されたドメインに対する要求を発行します。要求は、クライアントが接続されているルータに転送されます。

例：ブラウザが StaffOnly.XYZ.com を要求します。

2.ルータ上で動作している NBAR2 は（NBAR2 がアクティブになっているインターフェイス上で）DNS パケット スヌーピングを使用して、ネットワーク内のクライアントからの DNS 要求をモニタします。ルータは、DNS 要求内の情報を、次のステップであるデータ分析に渡します。

3.ドメイン フィルタ メカニズムにより、設定されたテキスト正規表現と照合することによって信頼されたドメインに対する DNS 要求を識別します。

正規表現の例：*staffonly.xyz.com

4。前のステップで識別された信頼されたドメインごとに、ルータが DNS-AS サーバに送信される「TXT」DNS 要求を準備します。ルータは、短いパフォーマンス最適化インターバルでこれらの「保留中の」要求を収集します。

5.ルータ サーバが「TXT」DNS 要求を DNS-AS サーバに送信します。

6.DNS-AS サーバが「TXT」応答を送信します。「TXT」応答に「CISCO-CLS」プレフィックス付きの情報が含まれている場合は、ルータが A 要求（IPv4 アドレスを要求する）または AAAA 要求（IPv6 アドレスを要求する）を送信します。DNS-AS サーバがその要求に対する A または AAAA 応答を送信します。

7.ルータが短いインターバルでアプリケーション分類データを含む「auto-learn raw データ」応答を収集します。

8.auto-learn raw データを使用して、NBAR が関連ドメイン用のカスタム アプリケーション プロトコルを作成します。注：カスタム アプリケーション プロトコルは、標準の Cisco NBAR2 プロトコル パック プロトコルより優先されます。

DNS-AS サーバは常に最新バージョンを提供する

ルータが後で過去に問い合わせたドメインに対して新しい要求を発行すると、DNS-AS サーバは最新バージョンのメタデータを送信します。そのため、メタデータが変更されていた場合、ルータは新しいバージョンを受信することになります。

DNS-AS のセットアップ

DNS-AS には、次のようなローカル DNS サーバとルータ上の設定が必要です。

- DNS-AS サーバのセットアップ, （231 ページ）
- DNS-AS ルータのセットアップ, （233 ページ）

DNS-AS サーバのセットアップ

エンタープライズ ネットワーク内のローカル DNS サーバで、「信頼されたドメイン」ごとにアプリケーション分類情報を設定します。これは、アプリケーション メタデータがクエリされたときにサーバがルータに伝達する情報です。ルータがアプリケーションに関する TXT クエリを送信すると、DNS サーバが TXT 応答で関連メタデータを送信します。

アプリケーション メタデータ フィールド

アプリケーション メタデータは DNS-AS サーバ上で設定されます。ネットワーク内の個々のルータが、カスタムプロトコルを作成し、それに応じてアプリケーショントラフィックを処理するメタデータを適用します。

次の表に、DNS-AS 機能によって処理されるアプリケーションに指定可能なメタデータ フィールドの説明を示します。DNS-AS 機能を使用して指定されたカスタマイズされたアプリケーション メタデータは、ルータにインストールされた NBAR2 プロトコル パックで提供されるメタデータより優先されます。

表 *26*：メタデータ フィールド

フィールド	必須/オプション	使用方法
Application name （app-name）	必須	インストールされたプロトコルパックに**含まれている**アプリケーションの場合：アプリケーションに対して指定されたカスタマイズされたメタデータがプロトコルパックで指定されたメタデータより優先されます。 インストールされたプロトコルパックに**含まれていない**アプリケーションの場合：新しいカスタムプロトコルが作成されます。
Application ID （app-id）	任意	指定しなかった場合は、NBAR2 がアプリケーション ID を生成します。 既存のアプリケーションには無効です。 （注） 新しいアプリケーションを指定するときにこのフィールドを含めることをお勧めします。これにより、ネットワーク内のカスタマイズされたアプリケーションにユニバーサル ID 番号が提供されます。ユニバーサル ID 番号は、トラフィックデータコレクタがネットワーク内のさまざまなデバイスから受信した DNS-AS カスタムアプリケーション分類データを集約できるようにします。
Traffic class （app-traffic-class）	任意	このフィールドが指定され、business-relevance フィールドが指定されなかった場合は、NBAR2 が自動的に business-relevance フィールドに「business-relevant」の値を割り当てます。 （注） 新しいアプリケーションを指定するときにこのフィールドを含めることを強くお勧めします。traffic-class が指定されなかった場合、そのアプリケーションはデフォルトの traffic-class 値を使用します。
Business relevance （business）	任意	ビジネスとの関連性

DNS-AS ルータのセットアップ

ネットワーク内で動作しているシスコ ルータで、次のように、DNS-AS 機能をアクティブにし、使用する DNS-AS サーバと「信頼されたドメイン」を設定します。

ステップ 1：ネットワーク内のルータ上で DNS-AS をアクティブにする

ネットワーク内のルータで、DNS-AS をアクティブにします。

```
avc dns-as client enable
```

ステップ 2：使用する DNS-AS サーバを指定する

分類メタデータに対する TXT 要求を使用してクエリする DNS-AS サーバを指定します。

```
ip name-server vrf <name> <address>
```

詳細については、ルータがクエリするための DNS-AS サーバの設定，（236 ページ）を参照してください。

ステップ 3：ネットワーク内のルータ上で信頼されたドメインを設定する

ネットワーク内のルータで、「信頼されたドメイン」を設定します。DNS-AS 機能は、信頼されたドメインとして設定されたアプリケーションのみに影響します。

ルータが信頼されたドメインの DNS トラフィックを検出すると、TXT 要求/応答を使用して、ローカル DNS-AS サーバにアプリケーション分類メタデータを要求して受信します。

ネットワーク内のクライアントから送信された DNS 要求内で検出されたドメイン名と照合するテキスト正規表現を入力することで、信頼されたドメインを設定します。上の例の **StaffOnly.XYZ.com** の場合は、正規表現が次のようになります。

```
*staffonly.xyz
```

詳細については、トラステッド ドメインの設定，（237 ページ）を参照してください。

ネットワークへの新しいアプリケーションの導入

組織のネットワークに新しいローカルアプリケーションを導入する場合は、DNS-AS サーバのセットアップとルータの「信頼されたドメイン」セットアップに新しいアプリケーションを追加するための DNS-AS のセットアップ手順を確認してください。

制約事項

DNS-AS の使用には、次の制限が適用されます。

- IPv4 DNS サーバのみがサポートされます。
- ネットワーク内のすべての DNS サーバ全体で、最大 50 の DNS-AS カスタム アプリケーションがサポートされます。

（注） NBAR2 は全部で 120 のカスタム プロトコルをサポートします。DNS-AS によって生成されたカスタム プロトコルが合計に加算されます。

- 最大 2 つの VRF がサポートされます。
- VRF あたり最大 2 台のサーバがサポートされます。
- NBAR は、NBAR が設定されたインターフェイス上の DNS トラフィックに対してのみ DNS パケットスヌーピングを実行します。
- DNS-AS カスタム アプリケーション プロトコルには、IPv4 アドレスと IPv6 アドレスのどちらかを含めることができますが、両方を含めることはできません。
- DNS-AS を使用して既存のアプリケーションをカスタマイズする場合は、「app-id」フィールドを TXT レコードから除外するか、既存のアプリケーションの「app-id」と同じにする必要があります。
- NBAR2 プロトコル パックに含まれていないアプリケーションの場合は、「app-name」フィールドをすべての DNS-AS サーバのすべての TXT レコードで一意にする必要があります。

DNS-AS CLI コマンド

DNS-AS の設定とモニタには、ネットワーク内のルータ上で複数の CLI を使用します。

次の項を参照してください。

- DNS-AS の有効化と設定, （234 ページ）
- DNS-AS のモニタリング, （240 ページ）

DNS-AS の有効化と設定

次の参照表に、DNS-AS 設定コマンドの要約を示します。

表 *27*：コンフィギュレーション コマンド

CLI	説明
ip name-server vrf*nameaddress*	DNS サーバを設定します。 他のルータ機能に使用する場合、このCLIは、複数の VRF と VRF ごとに最大 6 つの IP アドレスをサポートできます。ただし、DNS-AS は、2 つの VRF と VRF ごとに設定された最初の 2 つのサーバしかサポートしません。 使用上の注意： • CLI の実行時点で特定の VRF が定義されている必要はありません。 • 複数のサーバの設定が冗長性または VRF のために使用されます。 • 設定直後に、DNS-AS が、設定されたサーバに設定の順番で優先順位を付けます。ルータを再起動すると、DNS-AS が VRF 名を使用してアルファベット順に優先順位を付けます。 • **show avc dns-as client name-server brief** コマンドを使用して設定を表示できます。これは、DNS-AS機能が使用しているサーバを示します。
1. **avc dns-as client trusted-domains** 2.**domain***regular-expression*	正規表現をフィルタとして使用して信頼されたドメインを設定します。 使用上の注意： 最大50の信頼されたドメインを設定できます。 例： `Device(config)#`**avc dns-as client trusted-domains** `Device(config-trusted-domains)#`**domain *staffonly.xyz.com** `Device(config-trusted-domains)#`**exit**
avc dns-as client enable	DNS-AS を有効にします。

CLI	説明
1. **interface***interface* 2. **avc dns-as learning**	インターフェイス上でNBARを有効にします。 DNS-AS 機能は、NBAR によってモニタされるインターフェイス上でのみアクティブになります。NBAR が NBAR 機能で使用されるインターフェイス上でアクティブになっている場合は、そのインターフェイスも DNS-AS に対してモニタされます。 例： `Device#`**config terminal** `Device(config)#`**interface gig 0/0/0** `Device(config-if)#`**avc dns-as learning** `Device(config-if)#`**exit**

ルータがクエリするための DNS-AS サーバの設定

DNS-AS サーバを設定するには、ルータで次の手順を実行します。設定されている DNS サーバを表示する方法については、アクティブな DNS サーバの表示, （244 ページ）を参照してください。

手順の概要

1. **configureterminal**
2. **ipname-servervrf***nameaddress*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device#`**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipname-servervrf***nameaddress* 例： この例では、MANAGEMENT と呼ばれる DNS サーバを指定します。 `Device(config)#`**ip name-server vrf MANAGEMENT 10.56.56.56**	DNS サーバを指定します。

トラステッド ドメインの設定

DNS-AS 機能は、トラステッド ドメインのリストで設定されたアプリケーションでのみ動作します。

ドメイン名と一致する正規表現を指定することによって、トラステッド ドメインを設定します。たとえば、**www.cisco.com** や **developer.cisco.com** を含めたすべての Cisco.com トラフィックを設定するには、***cisco.com** と指定します。

トラステッド ドメインを指定すると、パケット アナライザ アプリケーション（オープン ソースの Wireshark アプリケーションなど）を使用して、トラステッド アプリケーションの DNS 要求パケットを検査するときに役立つことがあります。ドメイン名はパケットに表示され、有効な正規表現の作成に使用できます。

新しいトラステッド ドメインを設定するには、ルータで次の手順を実行します。

手順の概要

1. **configureterminal**
2. **avcdns-asclienttrusted-domains**
3. **domain***regular-expression*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device#`**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**avcdns-asclienttrusted-domains** 例： `Device(config)#`**avc dns-as client trusted-domains**	トラステッド ドメイン コンフィギュレーション モードを開始します。
ステップ 3	**domain***regular-expression* 例： `Device(config-trusted-domains)#`**domain *staffonly.xyz.com**	正規表現でドメインを指定します。

DNS-AS の有効化

DNS-AS 機能を有効にするには、ルータで次の手順を実行します。

手順の概要

1. **configureterminal**
2. **avcdns-asclientenable**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device#`**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**avcdns-asclientenable** 例： `Device(config)#`**avc dns-as client enable**	DNS-AS 機能を有効にします。

DNS-AS の無効化

DNS-AS 機能を無効にするには、ルータで次の手順を実行します。

手順の概要

1. **configureterminal**
2. **noavcdns-asclientenable**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device#`**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**noavcdns-asclientenable** 例： `Device(config)#`**no avc dns-as client enable**	DNS-AS 機能を無効にします。

DNS-AS 用インターフェイスでの NBAR の有効化

DNS-AS を使用するときには、ネットワーク内の各ルータがネットワーク内のクライアントからの DNS トラフィックをスヌーピングし、DNS-AS プロセスの次のステップ（ドメイン フィルタ）へデータを転送する必要があります。

ルータで DNS 要求をモニタするには、ルータがクライアントからの DNS 要求を受信するインターフェイスで NBAR を有効にする必要があります。ルータは一般的に、NBAR が有効化されているすべてのインターフェイスで DNS トラフィックをモニタします。

多くの CLI で、インターフェイス上の NBAR を有効化できます。DNS-AS を使用するときには、次の手順を使用して、DNS-AS 学習用のインターフェイスで NBAR を有効化します。

（注） インターフェイスですでに NBAR が有効化されている場合、このタスクは冗長になります。たとえば、IP Protocol Discovery がインターフェイスにすでに有効になっている場合、この手順は不要です。ただし、このような冗長状態でも、明確にするために、この手順を実行することをお勧めします。

手順の概要

1. **configureterminal**
2. **interface***interface*
3. **avcdns-aslearning**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device#`**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***interface* 例： `Device(config)#`**interface gig 0/0/0**	特定のインターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**avcdns-aslearning** 例： `Device(config-if)#`**avc dns-as learning**	前のステップで指定したインターフェイスで NBAR を有効にします。

DNS-AS のモニタリング

次の参照表に、DNS-AS モニタリング コマンドの要約を表示します。

表 *28*：モニタリング コマンド

CLI	説明
show avc dns-as client statistics	サーバごとの受信/送信カウンタを表示します。
show avc dns-as client binding-table	DNS-AS カスタムアプリケーションデータを表示します。
show avc dns-as client binding-table detailed	DNS-AS カスタムアプリケーションデータをレコード形式で表示します。
clear avc dns-as client statistics	受信/送信カウンタをクリアします。
show avc dns-as client name-server brief	設定された DNS サーバを表示します。
show ip nbar classification auto-learn dns-as<*1-100*>	auto-learn テーブルを表示します。 数値は、テーブルに表示されるエントリの数を示します。
clear ip nbar classification auto-learn dns-as-client statistics	auto-learn テーブルをクリアします。
clear ip nbar classification auto-learn dns-as restart	すべての DNS-AS 学習を再起動します。すべてのデータベースがクリアされます。
show ip nbar classification auto-learn dns-as pending-queries	保留中のクエリを表示します。
clear ip nbar classification auto-learn dns-as pending-queries	保留中のクエリ統計情報をクリアします。 **使用上の注意**： この CLI を実行しても、保留中のクエリの挿入は起こりません。
show ip nbar protocol-discovery stats packet-count	DNS-AS によって生成されたカスタムプロトコルを含む、すべての NBAR プロトコルのパケット カウントを表示します。

DNS-AS クライアント統計情報の表示

DNS-AS クライアント統計情報を表示するには、次の手順を実行します。結果はサーバごとに表示され、実行中のパケット数の合計が表示されます。

使用方法：

- DNS-AS を無効にすると、統計情報がリセットされます。
- 場合によっては、トラフィック ボリュームが異常に高いことが原因で、統計情報を取得できないことがあります。その場合は、一部の統計情報について「エラー」が表示されます。

手順の概要

1. **showavcdns-as client statistics**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**showavcdns-as client statistics** 例： Device#**show avc dns-as client statistics** csi-mcp-asr1k-02#show avc dns-as client statistics Server details: vrf-id = 2 vrf-name = MNG ip = 10.56.196.50 AAAA Query Error packets 0 AAAA Query TX packets 0 AAAA Response RX packets 0 TXT Query Error packets 0 TXT Query TX packets 50 TXT Response RX packets 50 A Query Error packets 0 A Query TX packets 50 A Response RX packets 50 Total Drop packets 0 Server details: vrf-id = 5 vrf-name = vrf2 ip = 10.56.196.51 AAAA Query Error packets 0 AAAA Query TX packets 0 AAAA Response RX packets 0 TXT Query Error packets 0 TXT Query TX packets 0 TXT Response RX packets 0 A Query Error packets 0 A Query TX packets 0 A Response RX packets 0 Total Drop packets 0	サーバあたりのクライアント統計情報を表示します。

DNS-AS カスタム アプリケーション データの表示

binding table format で DNS-AS カスタム アプリケーション データを表示するには、次の手順を実行します。コマンドの **detailed** 形式も参照してください。この形式では、**record format** で同じ情

報が表示されるため、別のアプリケーションへのデータのパイピングが可能になります。DNS-AS カスタム アプリケーション データの表示：詳細，（242 ページ）を参照してください。

含まれる情報は次のとおりです。

- DNS-AS を使用してカスタマイズできるプロトコルの最大数。
- カスタマイズ間隔：ルータが新しいカスタムプロトコルを作成するまでに auto-learn raw データを収集する時間間隔。デフォルト：5 分
- バインディングテーブルに現在保存されているプロトコルのテーブル。VRF 名、サーバ IP、期間経過、メタデータ、TTL、およびデータの期限が切れるまでの時間が表示されます。

プロトコルがこのテーブルに到達するまでの時間

DNS-AS プロセスにはレート リミッタが組み込まれており、遅延を短時間に抑えて全体的なパフォーマンスを最適化します。プロトコルがバインディング テーブルに表示されるまでの時間に影響する主要な間隔は次のとおりです（デフォルトでは合計約 8 分）。

- ルータが DNS 要求を DNS サーバに次に送信する前のレート リミッタ（デフォルト：3 分）。
- ルータが DNS サーバから DNS 応答を受信した後のレート リミッタ（デフォルト：10 分）。
- 収集した raw データがカスタムプロトコルの生成に使用される前のレート リミッタ（デフォルト：5 分）。

手順の概要

1. **showavcdns-asclientbinding-table**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**showavcdns-asclientbinding-table** 例： `Device#`**show avc dns-as client binding-table**	カスタム アプリケーション データが取り込まれたバインディング テーブルを表示します。

DNS-AS カスタム アプリケーション データの表示：詳細

DNS-AS カスタム アプリケーション データをレコード形式で表示するには、この手順を実行します。これにより、出力を別のアプリケーションにパイピングすることができます。

この手順では、DNS-AS カスタム アプリケーション データの表示，（241 ページ）の手順で説明しているコマンドと同じコマンドを使用しますが、**detailed** キーワードも指定します。

show avc dns-as client binding-table detailed

次の例では、UNIX 系環境で sec コマンドを使用して、xyz ドメインの出力を選択します。このコマンド出力は sec にパイピングされ、**staffonly** のフィルタが実行されます。

```
Device#show avc dns-as client binding-table detailed | sec staffonly
Protocol-name        : staffonly
 VRF                 : MNG
 Host                : staffonly.xyz.com
 Age[min]            : 17
 TTL[min]            : 1440
 Time to Expire[min] : 1420
 TXT Record          : app-name:staffonly|app-class:BULK-DATA
 IP                  : 10.2.3.10
```

受信および送信カウントのクリア

DNS-AS クライアント統計情報の送受信カウンタをクリアするには、この手順を実行します。

手順の概要

1. **clearavcdns-asclientstatistics**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**clearavcdns-asclientstatistics** 例： Device#**clear avc dns-as client statistics**	送受信カウンタをクリアします。

auto-learn テーブルのクリア

auto-learn の raw データをクリアするには、次の手順を実行します。

auto-learn の raw データは、一定間隔（デフォルトでは 5 分）でコントロール プレーンで収集されてから、データに基づいてカスタム プロトコルを作成するメカニズムに送信されます。クリアされてからすぐに（通常は 10 秒以内）、同じデータまたはデータのサブセットがデータ プレーンからコントロール プレーン内の auto-learn raw データ テーブルに再送されるときに、テーブルが再生成されます。このとき、データの TTL は一般的に 24 時間です。

一方、DNS-AS 学習のクリアと再開，（244 ページ）の手順を使用すると、作成された auto-learn raw データとカスタムプロトコルがクリアされます。

手順の概要

1. **clearipnbarclassificationauto-learndns-as-clientstatistics**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**clearipnbarclassificationauto-learndns-as-clientstatistics** 例： `Device#`**clear ip nbar classification auto-learn dns-as-client statistics**	auto-learn raw データをクリアします。

DNS-AS 学習のクリアと再開

生成された auto-learn raw データとカスタムプロトコルをクリアするには、このコマンドを使用します。すべてのデータベースがクリアされ、事前データなしで auto-learn プロセスが再開されます。

手順の概要

1. **clearipnbarclassificationauto-learndns-asrestart**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**clearipnbarclassificationauto-learndns-asrestart** 例： `Device#`**clear ip nbar classification auto-learn dns-as restart**	生成された auto-learn raw データとカスタムプロトコルをクリアします。

アクティブな DNS サーバの表示

DNS-AS と連携するように設定された DNS サーバを表示するには、次の手順を使用します。DNS サーバの設定については、ルータがクエリするための DNS-AS サーバの設定，（236 ページ）を参照してください。

手順の概要

1. **showavcdns-asclient name-serverbrief**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**showavcdns-asclient name-serverbrief** 例： `Device#`**show avc dns-as client name-server brief**	DNS-AS と連携するように設定された DNS サーバを表示します。

DNS-AS auto-learn データの表示

DNS-AS auto-learn raw データ リポジトリで収集されたデータを、カスタム プロトコルの作成に使用される前に表示するには、この手順を実行します。

auto-learn データをクリアする方法については、auto-learn テーブルのクリア，（243 ページ）を参照してください。

データがこのテーブルに到達するまでの時間

DNS-AS プロセスにはレート リミッタが組み込まれており、遅延を短時間に抑えて全体的なパフォーマンスを最適化します。データが auto-learn ステップに到達するまでの時間に影響する主要な間隔は次のとおりです（デフォルトでは合計約 3 分）。

- ルータが DNS 要求を DNS サーバに次に送信する前のレート リミッタ（デフォルト：3 分）。
- ルータが DNS サーバから DNS 応答を受信した後のレート リミッタ（デフォルト：10 分）。

手順の概要

1. **showipnbarclassificationauto-learndns-as-client**<*1-100*>**detailed**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**showipnbarclassificationauto-learndns-as-client**<*1-100*>**detailed** 例： `Device#`**show ip nbar classification auto-learn dns-as-client 100 detailed**	DNS-AS auto-learn raw データ リポジトリに収集されたデータを表示します。指定した数によって、テーブルに表示されるエントリの数が決まります。

保留中の DNS クエリの表示

ルータがまだDNSサーバに送信していないDNSクエリを表示するには、次の手順を使用します。レート リミッタは、累積された DNS クエリを DNS-AS サーバに送信する間隔を 3 分間に制限します。これにより、多くの同一要求で DNS-AS サーバを過負荷状態にすることなく、システムのパフォーマンスが最適化されます。

保留中のクエリ統計情報をクリアするには、保留中の DNS クエリ統計情報のクリア，（246 ページ）の手順を参照してください。

手順の概要

1. **showipnbarclassificationauto-learndns-aspending-queries**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**showipnbarclassificationauto-learndns-aspending-queries** 例： Device#**show ip nbar classification auto-learn dns-as pending-queries** AAAA queries pending inject 0 AAAA queries injected 0 TXT queries pending inject 0 TXT queries injected 50 A queries pending inject 0 A queries injected 50	保留中のクエリを表示します。

保留中の DNS クエリ統計情報のクリア

保留中のクエリ統計情報をクリアするには、次の手順を実行します。統計情報を表示するには、保留中の DNS クエリの表示，（246 ページ）の手順を参照してください。

手順の概要

1. **clearipnbarclassificationauto-learndns-as pending-queries**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**clearipnbarclassificationauto-learndns-as pending-queries** 例： `Device#`**clear ip nbar classification auto-learn dns-as pending-queries**	保留中のクエリ統計情報をクリアします。

DNS-AS のトラブルシューティング

DNS-AS のトラブルシューティングについては、『Cisco DNS-AS Troubleshooting』を参照してください。