Cisco Umbrella 統合

Cisco Umbrella 統合機能では、デバイスを介して DNS サーバーに送信されるドメインネームシステム（DNS）クエリを検証して、クラウドベースのセキュリティサービスを有効にすることができます。セキュリティ管理者は、完全修飾ドメイン名（FQDN）へのトラフィックを許可または拒否するポリシーを Cisco Umbrella ポータルに設定します。Cisco デバイスは、ネットワークエッジの DNS フォワーダとして機能し、DNS トラフィックを透過的にキャッチして Cisco Umbrella ポータルに DNS クエリを転送します。この機能は、Cisco IOS XE Denali 16.3 以降のリリースで使用できます。

- Cisco Umbrella 統合の制限 （1 ページ）
- Cisco Umbrella 統合の前提条件 （2 ページ）
- Cisco Umbrella Integration を使用したクラウドベースのセキュリティサービス （3 ページ）
- DNS パケットの暗号化 （3 ページ）
- Cisco Umbrella 統合のメリット （4 ページ）
- Cisco Umbrella Connector の設定 （4 ページ）
- Cisco Umbrella タグの登録 （5 ページ）
- Cisco デバイスをパススルーサーバーとして設定 （6 ページ）
- DNSCrypt、リゾルバ、および公開キー （6 ページ）
- Cisco Umbrella Connector の設定の確認 （7 ページ）
- Cisco Umbrella 統合のトラブルシューティング （9 ページ）
- 設定例 （9 ページ）
- Cisco Prime CLI テンプレートを使用した Cisco Umbrella Integration の展開 （9 ページ）
- Cisco Umbrella 統合の追加情報 （10 ページ）
- Cisco Umbrella 統合の機能情報 （11 ページ）

Cisco Umbrella 統合の制限

- アプリケーションまたはホストが、DNSを使用する代わりにIPアドレスを直接使用してドメイン名をクエリしている場合、ポリシーは適用されません。

- クライアントが Web プロキシに接続すると、DNS クエリはシスコデバイスをパススルーしません。この場合、コネクタはDNS要求を一切検出できず、Web サーバーへの接続は Cisco Umbrella ポータルからのすべてのポリシーをバイパスします。
- Cisco Umbrella の統合ポリシーによって DNS クエリがブロックされると、クライアントは Cisco Umbrella ブロックページにリダイレクトされます。これらのブロックページは、HTTPS サーバによって提供され、IP アドレス範囲は Cisco Umbrella ポータルによって定義されます。
- ユーザー認証とアイデンティティは、このリリースではサポートされません。
- リダイレクトされるレコードは、タイプ A、AAAA、および TXT クエリのみです。他のタイプのクエリはコネクタをバイパスします。Cisco Umbrella Connector は、悪意のあるトラフィックに関する既知の IP アドレスのリストを保持しています。Cisco Umbrella ローミングクライアントは、これらのアドレスが宛先のパケットを検出すると、各アドレスを Cisco Umbrella クラウドに転送して、さらに検査します。
- ホストの IPv4 アドレスのみが EDNS オプションで伝達されます。
- 最大 64 のローカルドメインを設定できます。許可されるドメイン名の長さは 100 文字です。

Cisco Umbrella 統合の前提条件

Cisco Umbrella 統合機能を設定するには、次の要件を満たしている必要があります。

- Cisco Umbrella を有効にするには、デバイスにセキュリティ K9 ライセンスが必要です。
- デバイスが Cisco IOS XE Denali 16.3 以降のソフトウェアイメージを実行している必要があります。
- Cisco Umbrella サブスクリプションライセンスが利用可能である必要があります。
- デバイスがデフォルトの DNS サーバーゲートウェイとして設定されており、DNS トラフィックがその Cisco デバイスを確実に通過する必要があります。
- Cisco Umbrella サーバへのデバイス登録に使用する通信は HTTPS 経由です。HTTPS 通信を行うには、ルータにルート証明書がインストールされている必要があります。この証明書をペーストする代わりに、次のリンクから証明書を直接ダウンロードすることができます。https://cacerts.digicert.com/DigiCertGlobalRootCA.crt.pem

Cisco Umbrella Integration を使用したクラウドベースのセキュリティサービス

Cisco Umbrella Integration 機能は、デバイスを介して DNS サーバーに送信される DNS クエリを検査する、クラウドベースのセキュリティサービスを提供します。ホストがトラフィックを開始し、DNS クエリを送信すると、デバイスの Cisco Umbrella コネクタは DNS クエリを横取りして検査します。ローカルドメインへの DNS クエリの場合は、DNS パケットを変更せずにエンタープライズ ネットワーク内の DNS サーバーにクエリを転送します。外部ドメインへの DNS クエリの場合は、クエリに拡張 DNS（EDNS）レコードを追加して Cisco Umbrella リゾルバに送信します。EDNS レコードには、デバイス識別子情報、組織 ID、およびクライアント IP アドレスが含まれています。Cisco Umbrella クラウドは、この情報に基づいて、DNS クエリにさまざまなポリシーを適用します。

DNS パケットの暗号化

Cisco デバイスから Cisco Umbrella 統合サーバーに送信される DNS パケットは、パケット内の EDNS 情報にユーザー ID、内部ネットワーク IP アドレスなどの情報が含まれている場合、暗号化する必要があります。DNS 応答が DNS サーバーから戻されると、デバイスはパケットを復号してからホストに転送します。

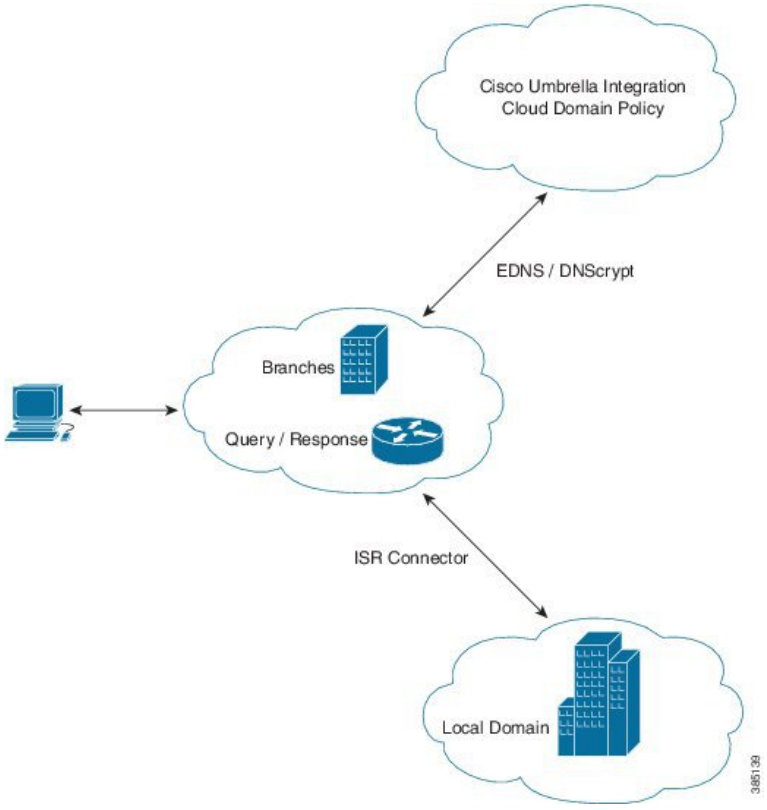
DNS パケットは、DNScrypt 機能が Cisco デバイスで有効化されている場合にのみ暗号化できます。

Cisco デバイスは次の Anycast 再帰型 Cisco Umbrella 統合サーバーを使用します。

- 208.67.222.222
- 208.67.220.220
- 2620:119:53::53
- 2620:119:35::35

次の図は、Cisco Umbrella 統合のトポロジを示します。

図 *1 : Cisco Umbrella* 統合のトポロジ



Cisco Umbrella 統合のメリット

Cisco Umbrella 統合により、DNS レベルでセキュリティとポリシーを適用できます。これにより、管理者は DNS トラフィックを分割して、目的の DNS トラフィックの一部を特定の DNS サーバ（エンタープライズ ネットワーク内にある DNS サーバ）に直接送信することができます。これにより、管理者は Cisco Umbrella 統合をバイパスできます。

Cisco Umbrella Connector の設定

Cisco Umbrella Connector を設定するには、次の手順を実行します。

- Cisco Umbrella 登録サーバーから API トークンを取得します。
- Cisco Umbrella 登録サーバとの間で HTTPS 接続を確立するために、ルート証明書を取得します。**crypto pki trustpool import terminal** コマンドを使用して、以下に示す DigiCert のルート証明書をデバイスにインポートします。

```
-----BEGIN CERTIFICATE-----
MIIDrzCCApegAwIBAgIQCDvgVpBCRrGhdWrJWZHHSjANBgkqhkiG9w0BAQUFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
```

```
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAeFw0wNjExMTAwMDAwMDBaFw0zMTExMTAwMDAwMDBaMGExCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j
b20xIDAeBgNVBAMTF0RpZ2lDZXJ0IEdsb2JhbCBSb290IENBMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4jvhEXLeqKTTo1eqUKKPC3eQyaKl7hLOllsB
CSDMAZOnTjC3U/dDxGkAV53ijSLdhwZAAIEJzs4bg7/fzTtxRuLWZscFs3YnFo97
nh6Vfe63SKMI2tavegw5BmV/Sl0fvBf4q77uKNd0f3p4mVmFaG5cIzJLv07A6Fpt
43C/dxC//AH2hdmoRBBYMql1GNXRor5H4idq9Joz+EkIYIvUX7Q6hL+hqkpMfT7P
T19sdl6gSzeRntwi5m3OFBqOasv+zbMUZBfHWymeMr/y7vrTC0LUq7dBMtoM1O/4
gdW7jVg/tRvoSSiicNoxBN33shbyTApOB6jtSj1etX+jkMOvJwIDAQABo2MwYTAO
BgNVHQ8BAf8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUA95QNVbR
TLtm8KPiGxvDl7I90VUwHwYDVR0jBBgwFoAUA95QNVbRTLtm8KPiGxvDl7I90VUw
DQYJKoZIhvcNAQEFBQADggEBAMucN6pIExIK+t1EnE9SsPTfrgT1eXkIoyQY/Esr
hMAtudXH/vTBH1jLuG2cenTnmCmrEbXjcKChzUyImZOMkXDiqw8cvpOp/2PV5Adg
06O/nVsJ8dWO41P0jmP6P6fbtGbfYmbW0W5BjfIttep3Sp+dWOIrWcBAI+0tKIJF
PnlUkiaY4IBIqDfv8NZ5YBberOgOzW6sRBc4L0na4UU+Krk2U886UAb3LujEV0ls
YSEY1QSteDwsOoBrp+uvFRTp2InBuThs4pFsiv9kuXclVzDAGySj4dzp30d8tbQk
CAUw7C29C79Fv1C5qfPrmAESrciIxpg0X40KPMbp1ZWVbd4=
-----END CERTIFICATE-----
```

- PEM インポートが正常に行われたことを確認します。証明書をインポートすると、メッセージが表示されます。

これはサンプル設定です。

```
enable
configure terminal
parameter-map type umbrella global
 token AABBA59A0BDE1485C912AFE472952641001EEECC

exit
```

Cisco Umbrella タグの登録

Cisco Umbrella タグを登録するには、次の手順を実行します。

1. 前の項で示したように Cisco Umbrella パラメータマップを設定します。
2. WAN インターフェイスで **umbrella out** を設定します。

```
interface gigabitEthernet 0/0/1
 umbrella out
```

3. LANインターフェイスで **umbrella in** を設定します。

```
interface gigabitEthernet 0/0/0.4
 umbrella in mydevice_tag
```

（注） Cisco デバイスの場合、ホスト名と umbrella タグは 49 文字以内で指定します。

4. **umbrella in mydevice_tag** コマンドを使用してタグと **umbrella in** を設定すると、デバイスによって Cisco Umbrella Integration ポータルにタグが登録されます。

5. デバイスが *api.opendns.com* を解決して登録プロセスを開始します。FQDN の解決を成功させるために、デバイスにネームサーバー（*ip name-server x.x.x.x*）とドメインルックアップ（*ip domain-lookup*）が設定されている必要があります。

（注） **umbrella in** コマンドを設定する前に、**umbrella out** コマンドを設定してください。登録は、ポート 443 が「オープン」状態にあり、既存のファイアウォールへのトラフィックのパススルーが許可される場合にのみ成功します。

Cisco デバイスをパススルーサーバーとして設定

ドメイン名を使用して、バイパスされるトラフィックを特定することができます。Cisco デバイスでは、正規表現形式でこれらのドメインを定義できます。デバイスによってキャッチされる DNS クエリが、設定済みの正規表現の 1 つにマッチすると、このクエリはバイパスされ、Cisco Umbrella クラウドにリダイレクトされずに、指定された DNS サーバーに送信されます。次の設定例は、目的のドメイン名と正規表現で regex parameter-map を定義する方法を示しています。

```
Device# configure terminal
Device(config)# parameter-map type regex dns_bypass
Device(config)# pattern www.fisco.com
Device(config)# pattern .*engineering.fisco.*

Attach the regex param-map with the openDNS global configuration as shown below:

Device(config)# parameter-map type umbrella global
Device(config-profile)# token AADDD5FF6E510B28921A20C9B98EEEFF
Device(config-profile)# local-domain dns_bypass
```

DNSCrypt、リゾルバ、および公開キー

- DNSCrypt
- リゾルバ IP
- 公開キー

上記のパラメータは、ラボで特定のテストを実行するときのみ変更することをお勧めします。これらのパラメータは今後の利用のために予約されています。これらのパラメータを変更すると、デバイスの正常な機能に影響が及ぶことがあります。

リゾルバ

次のコマンドは、DNS パケットのリダイレクションを Cisco デバイスから Cisco Umbrella クラウドに変更します。

- **resolver ipv4** *1.1.1.1*

- **resolver ipv4** *1.1.1.2*
- **resolver ipv6** *1234::1*
- **resolver ipv6** *2345::1*

この例では、すべての IPv4 DNS パケットが 1.1.1.1 または 1.1.1.2 にリダイレクトされ、IPv6 DNS パケットが 1234::1 または 2345::1 にリダイレクトされます。リゾルバのデフォルト値に戻すには、IP アドレスを削除する必要があります。リゾルバ IP アドレスを変更すると、次のメッセージが表示されます。

```
User configured would overwrite defaults
Defaults are restored when no more user configured are present
```

208.67.222.222 および **208.67.220.220** のデフォルト値を使用すると、すべての DNS パケットが Cisco Umbrella Anycast リゾルバにリダイレクトされます。デバイスは、すべてのリダイレクションに最初のデフォルトリゾルバ IP アドレスを使用します。Cisco デバイスは、3 つの連続する DNS クエリの応答を受信しない場合、別のリゾルバ IP アドレスに自動的に切り替えます。この動作は、IPv6 リゾルバ アドレスの場合も同じです。

（注） IPv6 リダイレクションは延期され、すべての IPV6 DNS パケットは Cisco Umbrella Anycast サーバーにリダイレクトされません。

公開キー

公開キーは、Cisco Umbrella Integration クラウドから DNSCrypt 証明書をダウンロードするために使用されます。この値は、**B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79**（Cisco Umbrella Integration Anycast サーバーの公開キー）に事前に設定されています。public-key に変更があり、このコマンドを変更する場合、デフォルト値に戻すときは変更されたコマンドを削除する必要があります。この値を変更すると、DNSCrypt 証明書のダウンロードは失敗することがあります。

DNSCrypt

DNSCrypt を無効化するには **no dnscrypt** コマンドを使用し、DNSCrypt を再度有効化するには **dnscrypt** コマンドを使用します。

DNSCrypt を使用する場合は、DNS 要求パケットサイズが 512 バイトよりも大きくなります。これらのパケットが中間デバイスで許可されていることを確認します。そうしないと、応答が目的の受信者に到達しない可能性があります。

Cisco Umbrella Connector の設定の確認

Cisco Umbrella Connector の設定を確認するには、次のコマンドを実行します。

```
Router# show umbrella config
Umbrella Configuration
==================
   Token:  AAC1A2555C11B2B798FFF3AF27C2FB8F001CB7B2
   OrganizationID: 1882034
   Local Domain Regex parameter-map name: NONE
   DNSCrypt: Enabled
   Public-key:
B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79

   UDP Timeout: 5 seconds
   Resolver address:
       1. 208.67.220.220
       2. 208.67.222.222
       3. 2620:119:53::53
       4. 2620:119:35::35
   Umbrella Interface Config:
       Number of interfaces with "opendns out" config: 1
         1. GigabitEthernet0/0/0
             Mode     :  OUT
             VRF      : global(Id: 0)
       Number of interfaces with "opendns in" config: 1
         1. GigabitEthernet0/0/1
             Mode      : IN
             Tag       : test
             Device-id : 010a6aef0b443f0f
             VRF       : global(Id: 0)

Device# show umbrella deviceid
Device registration details
Interface Name          Tag       Status   Device-id
GigabitEthernet0/0/1     guest  200 SUCCESS 010a7ba73bd216d1


Device#show umbrella dnscrypt
    DNSCrypt: Enabled
Public-key: B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79
Certificate Update Status:
Last Successful Attempt : 10:55:40 UTC Apr 14 2016
Last Failed Attempt : 10:55:10 UTC Apr 14 2016
Certificate Details:
Certificate Magic : DNSC
Major Version : 0x0001
Minor Version : 0x0000
Query Magic : 0x717744506545635A
Serial Number : 1435874751
Start Time : 1435874751 (22:05:51 UTC Jul 2 2015)
End Time : 1467410751 (22:05:51 UTC Jul 1 2016)
Server Public Key :
ABA1:F000:D394:8045:672D:73E0:EAE6:F181:19D0:2A62:3791:EFAD:B04E:40B7:B6F9:C40B
Client Secret Key Hash :
BBC3:409F:5CB5:C3F3:06BD:A385:78DA:4CED:62BC:3985:1C41:BCCE:1342:DF13:B71E:F4CF
Client Public key :
ECE2:8295:2157:6797:6BE2:C563:A5A9:C5FC:C20D:ADAF:EB3C:A1A2:C09A:40AD:CAEA:FF76
NM key Hash :
F9C2:2C2C:330A:1972:D484:4DD8:8E5C:71FF:6775:53A7:0344:5484:B78D:01B1:B938:E884
```

Cisco Umbrella 統合のトラブルシューティング

次のコマンドを使用して、Cisco Umbrella 機能の有効化に関連する問題のトラブルシューティングを行うことができます。

- **debug umbrella device-registration**
- **debug umbrella config**
- **debug umbrella dnscrypt**

OS に応じて、クライアントデバイスから次の 2 つのコマンドのいずれかを実行します。

- Windows マシンのコマンドプロンプトから **nslookup -type=txt debug.umbrella.com** コマンドを実行します
- Linux マシンのターミナルウィンドウまたはシェルから **nslookup -type=txt debug.umbrella.com** コマンドを実行します

```
nslookup -type=txt debug.opendns.com 8.8.8.8
Server: 8.8.8.8
Address: 8.8.8.8#53
Non-authoritative answer:
debug.opendns.com text = "server r6.mum1"
debug.opendns.com text = "device 010A826AAABB6C3D"
debug.opendns.com text = "organization id 1892929"
debug.opendns.com text = "remoteip 171.168.1.7"
debug.opendns.com text = "flags 436 0 6040 39FF000000000000000"
debug.opendns.com text = "originid 119211936"
debug.opendns.com text = "orgid 1892929"
debug.opendns.com text = "orgflags 3"
debug.opendns.com text = "actype 0"
debug.opendns.com text = "bundle 365396"
debug.opendns.com text = "source 72.163.220.18:36914"
debug.opendns.com text = "dnscrypt enabled (713156774457306E)"
```

設定例

次に、Cisco Umbrella 統合を有効にする例を示します。

Cisco Prime CLI テンプレートを使用した Cisco Umbrella Integration の展開

Cisco Prime CLI テンプレートを使用して、Cisco Umbrella Integration 環境をプロビジョニングできます。Cisco Prime CLI テンプレートを使用すると、Cisco Umbrella Integration 環境を簡単にプロビジョニングできます。

（注） Cisco Prime CLI テンプレートは、Cisco Prime バージョン 3.1 以降でのみサポートされています。

Cisco Prime CLI テンプレートを Cisco Umbrella Integration 環境のプロビジョニングに使用するには、次の手順を実行します。

ステップ 1 システムで実行されている Cisco IOS XE バージョンに対応する Cisco Prime テンプレートをダウンロードします。

ステップ 2 このファイルが圧縮されている場合は解凍します。

ステップ 3 Cisco Prime Web UI から、[設定（Configuration）] > [テンプレート（Templates）] > [機能とテクノロジー（Features and Technologies）] を選択し、次に [CLIテンプレート（ユーザー定義）（CLI Templates (User Defined)）] を選択します。

ステップ 4 [Import] をクリックします。

ステップ 5 テンプレートのインポート先フォルダを選択し、[テンプレートを選択（Select Templates）] をクリックして、先ほどダウンロードしたテンプレートを選択します。

ステップ 6 次の Cisco Umbrella Integration テンプレートが使用可能です。

- [Cisco Umbrella（Umbrella）]：このテンプレートは、デバイスの Cisco Umbrella Connector のプロビジョニングに使用します。
- [Cisco Umbrella クリーンアップ（Umbrella Cleanup）]：このテンプレートは、Cisco Umbrella Connector の削除に使用します。

Cisco Umbrella 統合の追加情報

関連資料

関連項目	マニュアル タイトル
IOS コマンド	『Cisco IOS Master Command List, All Releases』[英語]

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』[英語] • 『Cisco IOS Security Command Reference: Commands D to L』[英語] • 『Cisco IOS Security Command Reference: Commands M to R』[英語] • 『Cisco IOS Security Command Reference: Commands S to Z』[英語]

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/support

Cisco Umbrella 統合の機能情報

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 *1 : Cisco Umbrella* 統合の機能情報

機能名	リリース	機能情報
Cisco Umbrella 統合	Cisco IOS XE Everest リリース 16.6.1	Cisco Umbrella 統合機能により、Cisco デバイスを介して任意の DNS サーバに送信される DNS クエリを検査する、クラウドベースのセキュリティサービスを利用できるようになります。セキュリティ管理者は、完全修飾ドメイン名（FQDN）へのトラフィックを許可または拒否するポリシーを Cisco Umbrella クラウドに設定します。この機能は、Cisco ISR でのみサポートされます。

翻訳について
このドキュメントは、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。