CHAPTER 8

# FC-SP および DHCHAP の設定

この章は、次の項で構成されています。



## ファブリック認証の概要

Fibre Channel Security Protocol（FC-SP）機能は、スイッチ間およびホストとスイッチ間で認証を実行して、企業全体のファブリックに関するセキュリティ問題を解決します。Diffie-Hellman Challenge Handshake Authentication Protocol（DHCHAP）は、Cisco MDS 9000 ファミリ スイッチとその他のデバイス間で認証を行う FC-SP プロトコルです。DHCHAP は、CHAP プロトコルと Diffie-Hellman 交換を組み合わせて構成されています。

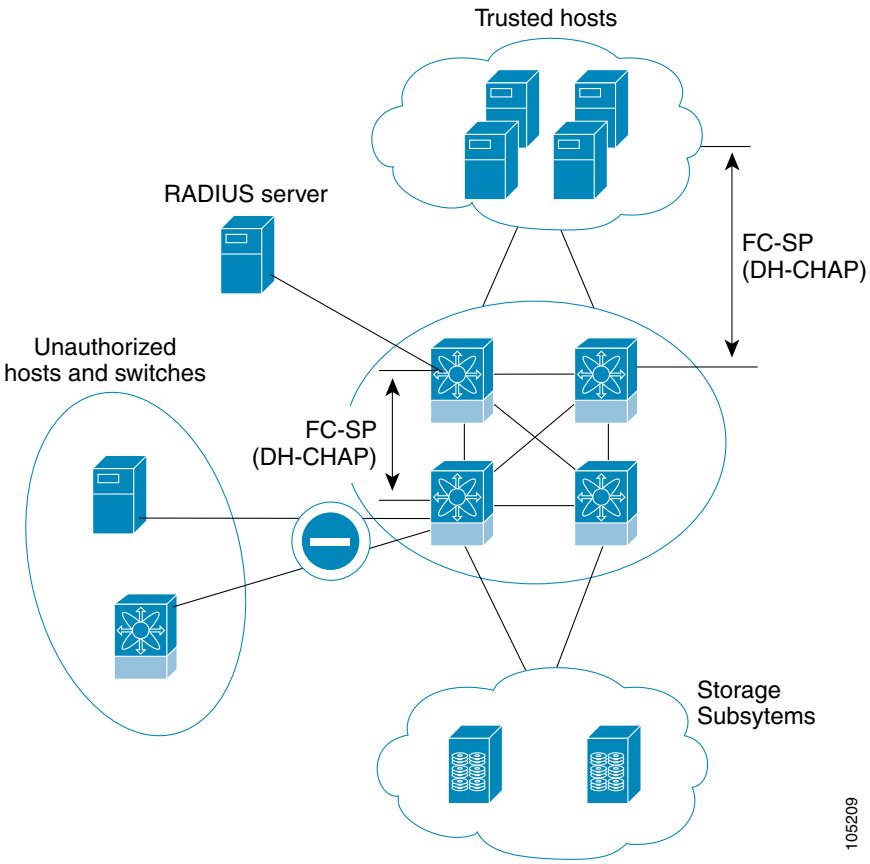
（注） Cisco NX-OS リリース 6.2(1) は Cisco MDS 9710 のみでファイバ チャネル セキュリティ プロトコル（FC-SP）機能をサポートしていません。Cisco MDS 9710 での FC-SP のサポートは、Cisco NX-OS リリース 6.2(9) 以降です。

VFC ポートを介して認証するには、FC-SP が通信にポート VSAN を使用する必要があります。したがって、認証メッセージを送受信するには、両方のピアでポート VSAN が同じで、かつアクティブになっている必要があります。

Cisco MDS 9000 ファミリのスイッチはすべて、スイッチ間またはスイッチとホスト間の認証をファブリック全体で実行できます。これらのスイッチおよびホスト認証は、各ファブリックでローカルまたはリモートで実行できます。ストレージ アイランドを企業全体のファブリックに統合して、移行すると、新しいセキュリティ問題が発生します。ストレージ アイランドを保護する方法が、企業全体のファブリックで必ずしも保証されなくなります。

たとえば、スイッチが地理的に分散しているキャンパス環境では、他のユーザが故意に、またはユーザ自身が偶然に、互換性のないスイッチに故意に相互接続することにより、スイッチ間リンク（ISL）分離やリンク切断が発生することがあります。Cisco MDS 9000 ファミリ スイッチでは、物理セキュリティに対するこのようなニーズに対応しています（図 8-1 を参照）。

*図 8-1　　スイッチおよびホストの認証*




(注)　ホスト スイッチ認証には、適切なファームウェアおよびドライバを備えたファイバ チャネル（FC）Host Bus Adapter（HBA）が必要です。

# DHCHAP

DHCHAP は、スイッチに接続しているデバイスを認証する認証プロトコルです。ファイバ チャネル認証を使用すると、信頼できるデバイスだけをファブリックに追加できるので、不正なデバイスのスイッチへのアクセスを防止できます。

(注)　この章では、FC-SP および DHCHAP という用語を共通の意味で使用しています。

DHCHAP は、必須のパスワードに基づくキー交換による認証プロトコルであり、スイッチ間およびホスト スイッチ間の認証をサポートします。DHCHAP はハッシュ アルゴリズムおよび DH グループをネゴシエートしてから、認証を実行します。また、MD5 および SHA-1 アルゴリズムベース認証をサポートします。

DHCHAP 機能の設定には、ENTERPRISE_PKG ライセンスが必要です（『*Cisco MDS 9000 Family NX-OS Licensing Guide*』を参照）。

ローカル パスワード データベースを使用して DHCHAP 認証を設定する手順は、次のとおりです。

**ステップ 1**　DHCHAP をイネーブルにします。
**ステップ 2**　DHCHAP 認証モードを識別して設定します。
**ステップ 3**　ハッシュ アルゴリズムおよび DH グループを設定します。
**ステップ 4**　ローカル スイッチおよびファブリックの他のスイッチの DHCHAP パスワードを設定します。
**ステップ 5**　再認証の DHCHAP タイムアウト値を設定します。
**ステップ 6**　DHCHAP の設定を確認します。

この項では、次のトピックについて取り上げます。



# 既存の Cisco MDS 機能との DHCHAP の互換性

ここでは、DHCHAP 機能および既存の Cisco MDS 機能の設定の影響について説明します。

- PortChannel インターフェイス：PortChannel に属しているポートに対して DHCHAP がイネーブルの場合、DHCHAP 認証は PortChannel レベルでなく、物理インターフェイス レベルで実行されます。
- FCIP インターフェイス：DHCHAP プロトコルは、物理インターフェイスの場合と同様に、FCIP インターフェイスと連携します。
- ポート セキュリティまたはファブリック バインディング：ファブリック バインディング ポリシーは、DHCHAP によって認証される ID に基づいて実行されます。

- VSAN：DHCHAP 認証は、VSAN 単位では実行されません。
- ハイ アベイラビリティ：DHCHAP 認証は既存の HA 機能とトランスペアレントに連携します。

# DHCHAP イネーブル化の概要

デフォルトでは、Cisco MDS 9000 ファミリの全スイッチで DHCHAP 機能はディセーブルに設定されています。

ファブリック認証用のコンフィギュレーション コマンドおよび確認コマンドにアクセスするには、DHCHAP 機能をイネーブルにする必要があります。この機能をディセーブルにすると、関連するすべての設定が自動的に廃棄されます。

# DHCHAP のイネーブル化

Cisco MDS スイッチの DHCHAP をイネーブルにする手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# feature fcsp` | このスイッチ上で DHCHAP をイネーブルにします。 |
| | `switch(config)# no feature fcsp` | このスイッチ上で DHCHAP をディセーブル（デフォルト）にします。 |

# DHCHAP 認証モードの概要

各インターフェイスの DHCHAP 認証ステータスは、DHCHAP ポート モードの設定によって変化します。

スイッチ内で DHCHAP 機能がイネーブルの場合には、各ファイバ チャネル インターフェイスまたは FCIP インターフェイスを次の 4 つの DHCHAP ポート モードのいずれかに設定できます。

- On：接続元デバイスが DHCHAP 認証をサポートしている場合、スイッチ初期化中に認証シーケンスが実行されます。接続元デバイスが DHCHAP 認証をサポートしていない場合には、リンクが分離状態になります。
- auto-Active：接続元デバイスが DHCHAP 認証をサポートしている場合、スイッチ初期化中に認証シーケンスが実行されます。接続元デバイスが DHCHAP 認証をサポートしていない場合には、ソフトウェアにより、初期化シーケンスの残りが実行されます。
- auto-Passive（デフォルト）：スイッチは DHCHAP 認証を開始しませんが、接続元デバイスが DHCHAP 認証を開始すれば、DHCHAP 認証に参加します。
- Off：スイッチは DHCHAP 認証をサポートしません。このようなポートに認証メッセージが送信された場合、開始元スイッチにエラー メッセージが戻されます。

（注）　DHCHAP ポート モードを off モード以外のモードに変更すると、再認証が実行されます。

（注）　VE リンクの DHCHAP ポート モードの変更には、両端のポート フラップが必要です。

表 8-1 に、さまざまなモードに設定した 2 台の Cisco MDS スイッチ間での認証動作について説明します。

*表 8-1　2 台の MDS スイッチ間の DHCHAP 認証ステータス*

| スイッチ番号 DHCHAP モード | スイッチ 1 の DHCHAP モード | | | |
|---|---|---|---|---|
| | **on** | **auto-active** | **auto-passive** | **off** |
| **on** | FC-SP 認証が実行されます。 | FC-SP 認証が実行されます。 | FC-SP 認証が実行されます。 | リンクがダウンになります。 |
| **auto-Active** | | | | FC-SP 認証は*実行されません。* |
| **auto-Passive** | | | FC-SP 認証は*実行されません。* | |
| **off** | リンクがダウンになります。 | FC-SP 認証は*実行されません。* | | |

# DHCHAP モードの設定

特定のインターフェイスに DHCHAP モードを設定する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# configure terminal` | 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 | `switch(config)# interface fc2/1-3`<br>`switch(config-if)#` | インターフェイスの範囲を選択し、インターフェイス コンフィギュレーション サブモードを開始します。 |
| ステップ 3 | `switch(config-if)# fcsp on` | 選択したインターフェイスの DHCHAP モードを on ステートに設定します。 |
| | `switch(config-if)# no fcsp on` | これら 3 つのインターフェイスを出荷時デフォルトの auto-passive に戻します。 |
| ステップ 4 | `switch(config-if)# fcsp auto-active 0` | 選択したインターフェイスの DHCHAP 認証モードを auto-active に変更します。0 は、ポートが再認証を実行しないことを表します。 |
| | `switch(config-if)# fcsp auto-active 120` | DHCHAP 認証モードを選択したインターフェイスの auto-active に変更し、最初の認証後に再認証を 2 時間（120 分）ごとにイネーブルにします。 |
| | `switch(config-if)# fcsp auto-active` | 選択したインターフェイスの DHCHAP 認証モードを auto-active に変更します。再認証はディセーブルになります（デフォルト）。 |

# DHCHAP ハッシュ アルゴリズムの概要

Cisco MDS スイッチは、DHCHAP 認証用のデフォルト ハッシュ アルゴリズム プライオリティ リスト（MD5 のあとに SHA-1）をサポートしています。

ヒント　ハッシュ アルゴリズムの設定を変更する場合は、ファブリック上の全スイッチに対して設定をグローバルに変更してください。

**注意**　fcsp dhchap 用の AAA 認証を有効にすると、AAA 認証に RADIUS または TACACS+ を使用する場合は、MD5 ハッシュ アルゴリズムを設定する必要があります。これは、RADIUS および TACACS+ のアプリケーションが他のハッシュ アルゴリズムをサポートしていないためです。

# DHCHAP ハッシュ アルゴリズムの設定

ハッシュ アルゴリズムを設定する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# configure terminal` | 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 | `switch(config)# fcsp dhchap hash sha1` | SHA-1 ハッシュ アルゴリズムだけを使用するように設定します。 |
| | `switch(config)# fcsp dhchap hash MD5` | MD5 ハッシュ アルゴリズムだけを使用するように設定します。 |
| | `switch(config)# fcsp dhchap hash md5 sha1` | DHCHAP 認証に対して、MD5 ハッシュ アルゴリズムを使用してから SHA-1 を使用するデフォルトのプライオリティ リストを定義します。 |
| | `switch(config)# no fcsp dhchap hash sha1` | 出荷時デフォルトのハッシュ アルゴリズム プライオリティ リスト（最初に MD5、次に SHA-1）に戻します。 |

# DHCHAP グループ設定の概要

FC-SP では、複数の DHCHAP グループがサポートされています。使用できるグループは、デフォルト リストから変更される可能性があります。リストは、優先順位の最も高いものから低いものへの順序で FC-SP ピアとネゴシエートするときに使用されるように設定されています。どちらの側も、受信したグループのリストとローカル グループのリストを比較し、優先度の最も高いグループが使用されます。各グループは設定コマンドで一度しか指定できません。

グループに関する詳細については、『*Cisco MDS 9000 Series NX-OS Command Reference Guide*』の fcsp dhchap コマンドを参照してください。

**ヒント**　DH グループの設定を変更する場合は、ファブリック内のすべてのスイッチの設定をグローバルに変更してください。

# DHCHAP グループの設定

DH グループ設定を変更する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# configure terminal` | 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 | `switch(config)# fcsp dhchap dhgroup 2 3 4` | DH グループ リストを使用するように指定します。リストは降順の優先度の順に指定されます。指定されないグループは DHCHAP により使用から除外されます。 |
| | `switch(config)# no fcsp dhchap dhgroup 2 3 4` | DHCHAP のデフォルトの順番に戻ります。 |

# DHCHAP パスワードの概要

DHCHAP 認証を実行する方向ごとに、接続デバイス間の共有シークレット パスワードが必要です。このパスワードを使用するには、DHCHAP に参加するファブリック上のすべてのスイッチで、次の 3 つの方法のいずれかを使用してパスワードを管理します。

- 方法 1: ファブリック上のすべてのスイッチに同じパスワードを使用します。これは最も簡単な方法です。新しいスイッチを追加する場合、このファブリック内では同じパスワードを使用してそのスイッチを認証します。したがって、ファブリック内のいずれかのスイッチに外部から不正アクセスを試みる場合、これは最も脆弱な方法です。
- 方法 2: ファブリック上のスイッチごとに異なるパスワードを使用して、このパスワード リストを維持します。新しいスイッチを追加する場合は、新規パスワード リストを作成して、この新規リストを使用してすべてのスイッチを更新します。いずれかのスイッチにアクセスすると、このファブリック上のすべてのスイッチに関するパスワード リストが生成されます。
- 方法 3: ファブリック上のスイッチごとに異なるパスワードを使用します。新しいスイッチを追加する場合は、ファブリック内の各スイッチに対応する複数の新規パスワードを生成して、各スイッチに設定する必要があります。いずれかのスイッチが被害にあっても、他のスイッチのパスワードは引き続き保護されます。この方法では、ユーザ側で大量のパスワード メンテナンス作業が必要になります。

(注)　パスワードはすべて 64 文字以内の英数字に制限されます。パスワードは変更できますが、削除はできません。

ヒント　スイッチが 6 台以上のファブリックでは、RADIUS または TACACS+ の使用をお勧めします。ローカル パスワード データベースを使用する必要がある場合には、方法 3 を使用し、Cisco MDS 9000 ファミリ Fabric Manager を使用して、パスワード データベースを管理します。

# ローカル スイッチの DHCHAP パスワードの設定

ローカル スイッチに DHCHAP パスワードを設定する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# fcsp dhchap password 0 mypassword` | ローカル スイッチのクリアテキスト パスワードを設定します。 |
| | `switch(config)# fcsp dhchap password 0 mypassword 30:11:bb:cc:dd:33:11:22` | 指定 WWN のデバイスで使用する、ローカル スイッチのクリア テキスト パスワードを設定します。 |
| | `switch(config)# no fcsp dhchap password 0 mypassword 30:11:bb:cc:dd:33:11:22` | 指定 WWN のデバイスで使用する、ローカル スイッチのクリア テキスト パスワードを削除します。 |
| | `switch(config)# fcsp dhchap password 7 sfsfdf` | ローカル スイッチに対して暗号化フォーマットで入力されるパスワードを設定します。 |
| | `switch(config)# fcsp dhchap password 7 sfsfdf 29:11:bb:cc:dd:33:11:22` | 指定 WWN のデバイスで使用する、ローカル スイッチに対して暗号化フォーマットで入力されるパスワードを設定します。 |
| | `switch(config)# no fcsp dhchap password 7 sfsfdf 29:11:bb:cc:dd:33:11:22` | 指定 WWN のデバイスで使用する、ローカル スイッチに対して暗号化フォーマットで入力されるパスワードを削除します。 |
| | `switch(config)# fcsp dhchap password mypassword1` | 接続するデバイスで使用する、ローカル スイッチのクリア テキスト パスワードを設定します。 |

Fabric Manager を使用してローカル スイッチに DHCHAP パスワードを設定する手順は、次のとおりです。

**ステップ 1**　[Switches] > [Security] を展開し、[FC-SP] を選択します。

[Information] ペインに、FC-SP の設定が表示されます。

**ステップ 2**　[Local Passwords] タブをクリックします。

**ステップ 3**　[Create Row] アイコンをクリックして、新しいローカル パスワードを作成します。

[Create Local Passwords] ダイアログボックスが表示されます。

**ステップ 4**　(任意)同じローカル パスワードを設定するスイッチをチェックします。

**ステップ 5**　スイッチの WNN を選択し、[Password] フィールドにパスワードを入力します。

**ステップ 6**　[Create] をクリックして、更新したパスワードを保存します。

# リモート デバイスのパスワード設定の概要

ファブリック内の他のデバイスのパスワードを、ローカル認証データベースに設定できます。他のデバイスは、スイッチ WWN やデバイス WWN といったデバイス名で表されます。パスワードは 64 文字に制限され、クリア テキスト（0）または暗号化テキスト（7）で指定できます。

（注）　スイッチ WWN は、物理スイッチを識別します。この WWN はスイッチの認証に使用されます。また、VSAN ノード WWN とは異なります。

# リモート デバイスの DHCHAP パスワードの設定

ファブリック内の別のスイッチのリモート DHCHAP パスワードをローカルで設定する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# fcsp dhchap devicename 00:11:22:33:44:aa:bb:cc password NewPassword` | スイッチ WWN デバイス名で表される、ファブリック上の他のスイッチのパスワードを設定します。 |
| | `switch(config)# no fcsp dhchap devicename 00:11:22:33:44:aa:bb:cc password NewPassword` | ローカル認証データベースから、このスイッチのパスワード エントリを削除します。 |
| | `switch(config)# fcsp dhchap devicename 00:11:55:66:00:aa:bb:cc password 0 NewPassword` | スイッチ WWN デバイス名で表される、ファブリック上の他のスイッチのクリア テキスト パスワードを設定します。 |
| | `switch(config)# fcsp dhchap devicename 00:11:22:33:55:aa:bb:cc password 7 asdflkjh` | スイッチ WWN デバイス名で表される、ファブリック内の他のスイッチの暗号化形式で入力されるパスワードを設定します。 |

# DHCHAP タイムアウト値の概要

DHCHAP プロトコルの交換中に、MDS スイッチが待機中の DHCHAP メッセージを指定インターバル内に受信しなかった場合、認証は失敗したと見なされます。この（認証が失敗したと見なされるまでの）時間は、20 ～ 1000 秒の範囲で設定できます。デフォルトは 30 秒です。

タイムアウト値を変更する場合には、次の要因について考慮してください。

- 既存の RADIUS および TACACS+ タイムアウト値。
- ファブリック内のすべてのスイッチに同じ値を設定する必要もあります。

# DHCHAP タイムアウト値の設定

DHCHAP タイムアウト値を構成する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# fcsp timeout 60` | 再認証タイムアウトを 60 秒に設定します。 |
| | `switch(config)# no fcsp timeout 60` | 出荷時デフォルトの 30 秒に戻します。 |

# DHCHAP AAA 認証の設定

認証オプションは個別に設定できます。認証を設定しない場合、デフォルトでローカル認証が使用されます。

AAA 認証を設定するには、第 4 章「外部 AAA サーバでのセキュリティ機能の設定」を参照し、その手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# aaa authentication dhchap default group TacacsServer1` | 認証に TACACS+ サーバ グループ（この例では、TacacsServer1）を使用する DHCHAP をイネーブルにします。 |
| | `switch(config)# aaa authentication dhchap default local` | ローカル認証用の DHCHAP をイネーブルにします。 |
| | `switch(config)# aaa authentication dhchap default group RadiusServer1` | 認証に RADIUS サーバ グループ（この例では、RadiusServer1）を使用する DHCHAP をイネーブルにします。 |

# プロトコル セキュリティ情報の表示

ローカル データベースの設定を表示するには、**show fcsp** コマンドを使用します（例 8-1 から 8-6 を参照）。

***例 8-1　FC インターフェイスの DHCHAP 設定の表示***

```
switch# show fcsp interface fc1/9

fc1/9:
        fcsp authentication mode:SEC_MODE_ON
        Status: Successfully authenticated
```

***例 8-2　FC インターフェイスの DHCHAP 統計情報の表示***

```
switch# show fcsp interface fc1/9 statistics

fc1/9:
        fcsp authentication mode:SEC_MODE_ON
        Status: Successfully authenticated
        Statistics:
        FC-SP Authentication Succeeded:5
```

```
        FC-SP Authentication Failed:0
        FC-SP Authentication Bypassed:0
```

*例 8-3　指定されたインターフェイスを介して接続されたデバイスの FC-SP WWN の表示*

```
switch# show fcsp interface fc 2/1 wwn

fc2/1:
        fcsp authentication mode:SEC_MODE_ON
        Status: Successfully authenticated
        Other device's WWN:20:00:00:e0:8b:0a:5d:e7
```

*例 8-4　ハッシュ アルゴリズムとローカル スイッチ用に設定された DHCHAP グループの表示*

```
switch# show fcsp dhchap
Supported Hash algorithms (in order of preference):
DHCHAP_HASH_MD5
DHCHAP_HASH_SHA_1

Supported Diffie Hellman group ids (in order of preference):
DHCHAP_GROUP_NULL
DHCHAP_GROUP_1536
DHCHAP_GROUP_1024
DHCHAP_GROUP_1280
DHCHAP_GROUP_2048
```

*例 8-5　DHCHAP ローカル パスワード データベースの表示*

```
switch# show fcsp dhchap database
DHCHAP Local Password:
        Non-device specific password:**********
        Password for device with WWN:29:11:bb:cc:dd:33:11:22 is ******
        Password for device with WWN:30:11:bb:cc:dd:33:11:22 is *********

Other Devices' Passwords:
        Password for device with WWN:00:11:22:33:44:aa:bb:cc is ***********
```

*例 8-6　デバイス WWN の ASCII 表記の表示*

```
switch# show fcsp asciiwwn 30:11:bb:cc:dd:33:11:22
Ascii representation of WWN to be used with AAA servers:Ox_3011bbccdd331122
```

ヒント　RADIUS サーバおよび TACACS+ サーバにスイッチ情報を設定する場合、デバイス WWN の ASCII 表記（例 8-6 で太字で表記）を使用してください。

# 設定例

ここでは、図 8-2 に示した例を設定する手順を示します。

*図 8-2　DHCHAP 認証の例*

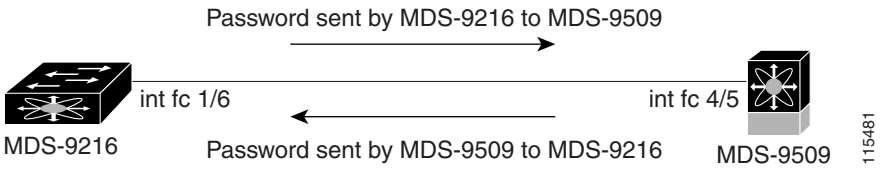



図 8-2 に示す認証設定を設定するには、次の手順を実行します。

**ステップ 1**　ファブリック内の MDS 9216 スイッチのデバイス名を取得します。ファブリック内の MDS 9216 スイッチは、スイッチ WWN によって識別されます。

```
MDS-9216# show wwn switch
Switch WWN is 20:00:00:05:30:00:54:de
```

**ステップ 2**　このスイッチで DHCHAP を明示的にイネーブルにします。

**（注）**　DHCHAP をディセーブルにすると、関連するすべての設定が自動的に廃棄されます。

```
MDS-9216(config)# feature fcsp
```

**ステップ 3**　このスイッチのクリア テキスト パスワードを設定します。このパスワードは、接続先デバイスで使用されます。

```
MDS-9216(config)# fcsp dhchap password rtp9216
```

**ステップ 4**　スイッチ WWN デバイス名で表される、ファブリック上の他のスイッチのパスワードを設定します。

```
MDS-9216(config)# fcsp dhchap devicename 20:00:00:05:30:00:38:5e password rtp9509
```

**ステップ 5**　目的のファイバ チャネル インターフェイスの DHCHAP モードをイネーブルにします。

**（注）**　DHCHAP ポート モードを off モード以外のモードに変更すると、再認証が実行されます。

```
MDS-9216(config)# interface fc 1/16
MDS-9216(config-if)# fcsp on
```

**ステップ 6**　DHCHAP ローカル パスワード データベースを表示して、このスイッチに設定されたプロトコル セキュリティ情報を確認します。

```
MDS-9216# show fcsp dhchap database
DHCHAP Local Password:
        Non-device specific password:*******
Other Devices' Passwords:
        Password for device with WWN:20:00:00:05:30:00:38:5e is *******
```

**ステップ 7**　ファイバ チャネル インターフェイスの DHCHAP 設定を表示します。

```
MDS-9216# show fcsp interface fc 1/6
fc1/6
        fcsp authentication mode:SEC_MODE_ON
        Status:Successfully authenticated
```

**ステップ 8**　接続先の MDS 9509 スイッチでこれらの手順を繰り返します。

```
MDS-9509# show wwn switch
Switch WWN is 20:00:00:05:30:00:38:5e
MDS-9509(config)# feature fcsp
MDS-9509(config)# fcsp dhchap password rtp9509
MDS-9509(config)# fcsp dhchap devicename 20:00:00:05:30:00:54:de password rtp9216
MDS-9509(config)# interface fc 4/5
MDS-9509(config-if)# fcsp on
MDS-9509# show fcsp dhchap database
DHCHAP Local Password:
        Non-device specific password:*******
Other Devices' Passwords:
        Password for device with WWN:20:00:00:05:30:00:54:de is *******
MDS-9509# show fcsp interface fc 4/5
Fc4/5
        fcsp authentication mode:SEC_MODE_ON
        Status:Successfully authenticated
```

これで、図 8-2 に示す設定例の DHCHAP 認証のイネーブル化と設定の作業が終わります。

# デフォルト設定

表 8-2 に、スイッチのすべてのファブリック セキュリティ機能のデフォルト設定を示します。

*表 8-2　デフォルトのファブリック セキュリティ設定値*

| パラメータ | デフォルト |
|---|---|
| DHCHAP 機能 | ディセーブル |
| DHCHAP ハッシュ アルゴリズム | 最初に MD5、次に SHA-1 のプライオリティ リストで DHCHAP 認証を実行 |
| DHCHAP 認証モード | auto-passive |
| DHCHAP グループのデフォルトの交換プライオリティ | 0、4、1、2、3 の順 |
| DHCHAP タイムアウト値 | 30 秒 |