CHAPTER 20

ファブリック セキュリティの設定

Cisco MDS SAN OS Release 1.3 の 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の認証を提供し、全社規模ファブリックのセキュリティ上の課題を克服します。Diffie-Hellman Challenge Handshake Authentication Protocol（DHCHAP）は、このリリースに実装されている FC-SP プロトコルであり、Cisco MDS 9000 ファミリー スイッチと他のデバイスとの間で認証を実行します。このプロトコルは、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。

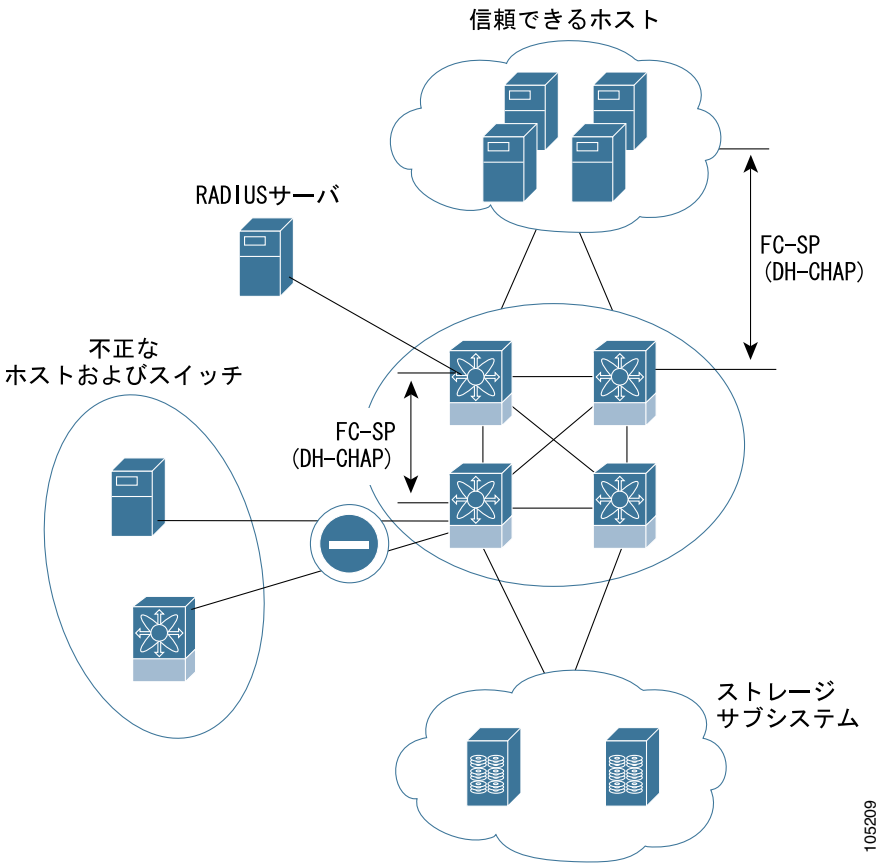
この章の内容は、次のとおりです。

- ファブリック認証の概要（p.20-2）
- DHCHAP の概要（p.20-3）
- 既存の Cisco MDS 機能との DHCHAP の互換性（p.20-3）
- DHCHAP 認証の設定（p.20-3）
- DHCHAP の設定（p.20-4）
- DHCHAP 認証モード（p.20-4）
- DHCHAP ハッシュ アルゴリズムの設定（p.20-6）
- DHCHAP グループの設定（p.20-7）
- DHCHAP パスワードの設定（p.20-7）
- 他のデバイスのパスワードの設定（p.20-9）
- DHCHAP タイムアウト値（p.20-9）
- プロトコル セキュリティ情報の表示（p.20-10）
- DHCHAP AAA 認証（p.20-11）
- コンフィギュレーション例（p.20-12）
- デフォルト設定値（p.20-14）

ファブリック認証の概要

Cisco MDS 9000 ファミリーの全スイッチで、1 台のスイッチから他のスイッチへ、またはスイッチからホストへ、ファブリック規模の認証を実行することができます。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に実行することも、リモートで実行することもできます。複数のストレージ アイランドを合併し全社規模のファブリックに移行するにつれ、セキュリティ上の新しい課題が生じます。ストレージ アイランドを保護するアプローチは、全社規模のファブリックでは常に保証されるとは限りません。たとえば、広い地域にスイッチが分散するキャンパス環境では、故意か偶発的かを問わず、互換性のないスイッチが相互接続され、その結果、ISL（スイッチ間リンク）が切り離されたり、リンクがダウンしたりする可能性があります。Cisco MDS 9000 ファミリー 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 20-1 を参照）。

図 20-1　スイッチとホストの認証



（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搭載したファイバ チャネル（FC）ホスト バス アダプタ（HBA）が必要です。

DHCHAP の概要

DHCHAP は、スイッチに接続しようとするデバイスを認証するための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がファブリックに追加され、権限のないデバイスによるスイッチ 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。このプロトコルは、MD5 アルゴリズムおよび SHA-1 アルゴリズムに基づく認証をサポートしています。

DHCHAP 機能を設定するには、ENTERPRISE_PKG ライセンスが必要です（第 3 章「ライセンスの入手とインストール」を参照）。

既存の Cisco MDS 機能との DHCHAP の互換性

ここでは、DHCHAP機能を既存のCisco MDS機能と一緒に設定した場合の影響について説明します。

- ポート チャネル インターフェイス — ポート チャネルに属するポートで DHCHAP をイネーブルにすると、DHCHAP 認証はポート チャネル レベルではなく、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と同じように、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 によって認証されたアイデンティティに基づいて実施されます。
- VSAN — DHCHAP 認証は、VSAN（仮想 SAN）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 機能に対してトランスペアレントに動作します。

DHCHAP 認証の設定

ローカル パスワード データベースを使用する DHCHAP 認証の設定手順は、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上の他のスイッチの 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。

DHCHAP の設定

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

ファブリック認証の設定および確認を行うコマンドにアクセスするには、DHCHAP 機能を明示的に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。

Cisco MDS スイッチで 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)# fcsp enable`	このスイッチ上で DHCHAP をイネーブルにします。
	`switch(config)# no fcsp enable`	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

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左右されます。

スイッチ上で DHCHAP 機能がイネーブルである場合、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 — 接続先デバイスが DHCHAP 認証をサポートしている場合、スイッチの初期化時にソフトウェアが認証シーケンスを実行します。接続先デバイスが DHCHAP 認証をサポートしていない場合、ソフトウェアはリンクを隔離ステートにします。
- auto-active — 接続先デバイスが DHCHAP 認証をサポートしている場合、スイッチの初期化時にソフトウェアが認証シーケンスを実行します。接続先デバイスが DHCHAP 認証をサポートしていない場合、ソフトウェアは残りの初期化シーケンスを続行します。
- auto-passive（デフォルト）— スイッチは DHCHAP 認証を開始しませんが、接続先デバイスが 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。このポートに認証メッセージが送信されると、発信側のスイッチにエラー 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。

表 20-1 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 20-1　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。*		

特定のインターフェイスで DHCHAP モード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)# interface fc2/1-3` `switch(config-if)#`	インターフェイス 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、ポートが認証を実行しないことを表します。
	`switch(config-if)# fcsp auto-active 120`	選択したポートの DHCHAP 認証モードを auto-active に変更し、初期化時の認証から 2 時間（120 分）ごとに再認証します。
	`switch(config-if)# fcsp auto-active`	選択したポートの DHCHAP 認証モードを auto-active に変更します。

DHCHAP ハッシュ アルゴリズムの設定

Cisco MDS スイッチは、DHCHAP 認証のためのデフォルトのハッシュ アルゴリズムのプライオリティ リストとして、最初に MD5、次に SHA-1 をサポートします。

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グローバルに変更してください。

注意　RADIUS および TACACS+ プロトコルは、CHAP 認証で常に MD5 を使用します。SHA-1 をハッシュ アルゴリズムとして使用すると、DHCHAP 認証用に RADIUS および TACACS+ がイネーブルになっていても、これらの AAA プロトコルが使用できなくなる可能性があります。

タイムアウト値を変更する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# 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 hash sha1`	SHA-1 ハッシュ アルゴリズムのみを使用するように設定します。
	`switch(config)# fcsp dhchap hash MD5`	MD5 ハッシュ アルゴリズムのみを使用するように設定します。
	`switch(config)# fcsp dhchap hash md5 sha1`	DHCHAP認証に使用するデフォルトのハッシュ アルゴリズムのプライオリティ リストとして、最初に MD5、次に SHA-1 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 グループの設定

Cisco MDS ファミリーの全スイッチで、規格に定められたすべての DHCHAP グループがサポートされます。0（Diffie-Hellman 交換を実行しないヌル DH グループ）、1、2、3、または 4 です。

ヒント　DH グループの設定を変更する場合は、ファブリック上の全スイッチに対してグローバルに変更してください。

DH グループの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# 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 group 2 3 4`	DH グループ 2、3、4 を、この順序で使用するようにプライオリティ リスト化します。
	`switch(config)# no fcsp dhchap group 0`	DHCHAP の出荷時デフォルトの順序（0、4、1、2、3）に戻します。

DHCHAP パスワードの設定

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。ファブリック上で DHCHAP に関与する全スイッチのパスワードを管理するために、次の 3 つのアプローチが考えられます。

- アプローチ 1 ― ファブリック上の全スイッチに同じパスワードを使用します（最も単純なアプローチ）。新しいスイッチを追加する場合、このファブリック上で同じパスワードを使用してそのスイッチを認証します。外部からファブリック上のいずれかのスイッチへの悪意あるアクセスが試みられる場合、これは最も脆弱なアプローチでもあります。
- アプローチ 2 ― スイッチごとに異なるパスワードを使用し、ファブリック上の各スイッチで、そのパスワード リストを維持します。新しいスイッチを追加する場合、新しいパスワード リストを作成し、そのリストですべてのスイッチを更新します。1 つのスイッチにアクセスすれば、ファブリック上の全スイッチのパスワード リストが得られます。
- アプローチ 3 ― ファブリック上の個々のスイッチに対し、それぞれ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、ファブリック上の各スイッチに対応する複数の新しい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。1 台のスイッチでセキュリティが破られても、他のスイッチのパスワードは引き続き保護されています。このアプローチを実施する場合、パスワード メンテナンスのために、かなりの手間が必要になります。

（注）　パスワードはすべて最大 64 文字の英数字とします。パスワードは変更できますが、削除することはできません。

ヒント　スイッチ数が 5 台より多いファブリックでは、RADIUS または TACACS+ を使用することを推奨します。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も、アプローチ 3 を使用し、Cisco MDS 9000 ファミリー Fabric Manager でパスワード データベースを管理することができます。

詳細は、『*Cisco MDS 9000 Family Fabric Manager Configuration Guide*』を参照してください。

ローカル スイッチの DHCHAP パスワードの設定

ローカル スイッチの 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**	指定した WWN を持つデバイスに使用されるローカル 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**	指定した WWN を持つデバイスに使用されるローカル 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 スイッチの暗号化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**	指定した WWN を持つデバイスに使用されるローカル スイッチの暗号化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**	指定した WWN を持つデバイスに使用されるローカル スイッチの暗号化パスワードを削除します。
	switch(config)# **fcsp dhchap password mypassword1**	任意の接続先デバイスに使用されるローカル スイッチのクリアテキスト パスワードを設定します。

他のデバイスのパスワードの設定

ファブリック上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、それぞれのデバイス名（スイッチ WWN またはデバイス WWN）で識別されます。パスワードは最大 64 文字であり、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、VSAN ノード WWN とは異なります。

ローカルでのデバイス名の設定

ファブリック上の他のスイッチのデバイス名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、ファブリック上の他のスイッチの暗号化パスワードを設定します。

DHCHAP タイムアウト値

DHCHAP プロトコル交換を実行するとき、MDS スイッチが一定の時間内に DHCHAP メッセージを受信できなかった場合、認証は失敗したとみなされます。この時間は、20（認証を実行しない）～ 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際、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
- ファブリック上の全スイッチに同じ値を設定する必要があります。

タイムアウト値の設定

DHCHAP タイムアウト値を設定する手順は、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 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。

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 20-1 ～ 20-6 を参照）。

例 20-1　FC インターフェイスに関する DHCHAP 設定の表示

```
switch# show fcsp interface fc1/9

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

例 20-2　FC インターフェイスに関する 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 20-3　特定のインターフェイス経由で接続したデバイスの 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 20-4　ローカル スイッチに設定済みのハッシュ アルゴリズムおよび 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 20-5　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:mypassword1
        Password for device with WWN:29:11:bb:cc:dd:33:11:22 is pjoalf
        Password for device with WWN:30:11:bb:cc:dd:33:11:22 is mypassword

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

例 20-6　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 20-6 に太字で示されている）を使用してください。

DHCHAP AAA 認証

個別に認証オプションを設定できます。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。

Cisco MDS 9000 ファミリー スイッチに認証を設定するには、**aaa authentication dhchap** コマンドを使用します。

Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）認証を設定する手順は、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)# aaa authentication dhchap default group TacacsServer1`	DHCHAP が TACACS+ サーバ グループ（この例では TacacsServer1）を認証に使用できるようにします。
	`switch(config)# aaa authentication dhchap default local`	DHCHAP をローカル認証でイネーブルにします。
	`switch(config)# aaa authentication dhchap default group RadiusServer1`	DHCHAP が RADIUS サーバ グループ（この例では RadiusServer1）を認証に使用できるようにします。

コンフィギュレーション例

ここでは、図 20-2 に示した例を設定する手順を示します。

図 20-2　DHCHAP 認証の例

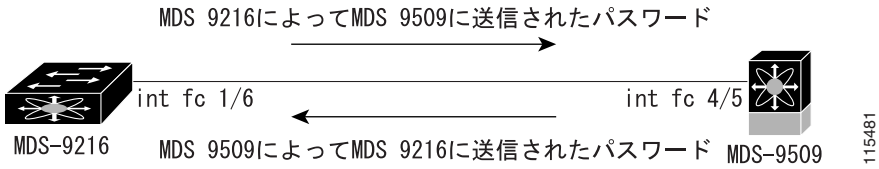


図 20-2 に表示されているように認証設定を設定する手順は、次のとおりです。

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 で表されます。

```
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)# fcsp enable
```

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:upt9216
Other Devices' Passwords:
        Password for device with WWN:20:00:00:05:30:00:38:5e is upt9509
```

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)# fcsp enable
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:upt9509
Other Devices' Passwords:
        Password for device with WWN:20:00:00:05:30:00:54:de is upt9216
MDS-9509# show fcsp interface fc 4/5
Fc4/5
        fcsp authentication mode:SEC_MODE_ON
        Status:Successfully authenticated
```

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

デフォルト設定値

表 20-2 に、スイッチのファブリック セキュリティ機能のデフォルト設定値を示します。

表 20-2　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 というプライオリティ リストで、DHCHAP 認証を実行します。
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