Cisco TrustSec ファイバ チャネル リンク暗号化の設定

この章では、Cisco TrustSec ファイバ チャネル（FC）リンクの暗号化機能の概要を示し、スイッチ間にリンク レベルの暗号化を設定する方法について説明します。

この章は、次の項目を取り上げます。

Cisco TrustSec FC リンク暗号化に関する用語

この章では、次に示す Cisco TrustSec FC リンク暗号化関連の用語を使用します。

- ガロア カウンタ モード（GCM）：機密保持とデータ発信元認証を行う操作のブロック暗号モード。
- ガロア メッセージ認証コード（GMAC）：データ発信元認証だけを行う操作のブロック暗号モード。GCM の認証限定バリアントです。
- セキュリティ アソシエーション（SA）：セキュリティ認定証を処理し、それらの認定証をスイッチ間にどのように伝播するかを制御する接続。SA には、salt やキーなどのパラメータが含まれます。
- キー：フレームの暗号化および復号化に使用する 128 ビットの 16 進数字列。デフォルト値は 0 です。
- Salt：暗号化および復号化の際に使用する 32 ビットの 16 進数字列。適切な通信を行うには、接続の両側に同じ salt を設定する必要があります。デフォルト値は 0 です。
- セキュリティ パラメータ インデックス（SPI）番号：ハードウェアに設定される SA を識別する 32 ビットの数字。有効な範囲は 256 ～ 65536 です。

AES 暗号化のサポート

Advanced Encryption Standard（AES）は、ハイ レベルなセキュリティを実現する対称暗号アルゴリズムであり、さまざまなキー サイズを受け入れることができます。

Cisco TrustSec FC リンク暗号化機能は、セキュリティ暗号用に 128 ビットの AES をサポートし、インターフェイスに AES-GCM または AES-GMAC のいずれかをイネーブルにします。AES-GCM モードではフレームの暗号化と認証が可能であり、AES-GMAC では 2 つのピア間で送受信されるフレームの認証だけが可能です。

Cisco TrustSec FC リンク暗号化の概要

Cisco TrustSec FC リンク暗号化は、Fibre Channel-Security Protocol（FC-SP）の拡張機能であり、既存の FC-SP アーキテクチャを使用してトランザクションの整合性と機密保持を実現します。セキュリティを保ち、望ましくないトラフィック傍受を防止するため、ピア認証機能に暗号化が追加されました。ピア認証は、Diffie-Hellman（DH）Challenge Handshake Authentication Protocol（DHCHAP）プロトコルを使用した FC-SP 標準に従って実装されます。

（注）　Cisco TrustSec FC リンク暗号化は現在、Cisco MDS スイッチ間に限りサポートされています。この機能は、カプセル化セキュリティ ペイロード（ESP）プロトコルをサポートしていないソフトウェア バージョンにダウングレードするとサポートされなくなります。

この項では、次のトピックについて取り上げます。

サポートされるモジュール

次のモジュールは、Cisco TrustSec FC リンク暗号化機能に対応しています。

- 2/4/8/10/16 Gbps 48 ポート アドバンスド ファイバ チャネル モジュール（DS-X9448-768K9）
- 8 Gbps 32 ポート拡張ファイバ チャネル スイッチング モジュール（DS-X9232-256K9）
- 8 Gbps 48 ポート拡張ファイバ チャネル スイッチング モジュール（DS-X9248-256K9）
- 1/2/4/8 Gbps 24 ポート ファイバ チャネル スイッチング モジュール（DS-X9224-96K9）
- 1/2/4/8 Gbps 48 ポート ファイバ チャネル スイッチング モジュール（DS-X9248-96K9）
- 1/2/4/8 Gbps 4/44 ポート ファイバ チャネル スイッチング モジュール（DS-X9248-48K9）
- 2/4/8/10/16 Gbps 96 ポート ファイバ チャネル スイッチング モジュール（DS-C9396S-K9）
- 24/10 ポート SAN 拡張モジュール（DS-X9334-K9）

Cisco TrustSec FC リンク暗号化のイネーブル化

Cisco MDS 9000 ファミリのすべてのスイッチの FC-SP 機能と Cisco TrustSec FC リンク暗号化機能は、デフォルトでディセーブルになります。

ファブリック認証および暗号化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、FC-SP 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。

Cisco MDS スイッチの FC-SP 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 モードに入ります。
ステップ 2	`switch(config)# feature fcsp`	FC-SP 機能をイネーブルにします。
	`switch(config)# no feature fcsp`	このスイッチの FC-SP 機能をディセーブル（デフォルト）にします。

Cisco TrustSec FC リンク暗号化機能を設定するには、ENTERPRISE_PKG ライセンスが必要です。詳細については、『*Cisco MDS 9000 Family NX-OS Licensing Guide*』を参照してください。

セキュリティ アソシエーションの設定

スイッチ間で暗号化を実行するには、セキュリティ アソシエーション（SA）を設定する必要があります。暗号化を実行するには、管理者があらかじめ手動で SA を設定する必要があります。SA には、キーや salt など、暗号化に必要なパラメータが含まれます。スイッチには、最大 2000 の SA を設定できます。

2 台のスイッチ間の SA を設定するには、次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 モードに入ります。
ステップ 2	`switch(config)# fcsp esp sa` *spi_number*	SA を設定するための SA サブモードを開始します。*spi_number* の範囲は 256 ～ 65536 です。
ステップ 3	`switch(config)# no fcsp esp sa` *spi_number*	スイッチ間の SA を削除します。[1]

1. 指定した SA が現在ポートにプログラムされている場合、このコマンドは SA が使用中であることを伝えるエラーを返します。

どのポートが SA を使用しているかを調べるには、**show running-config fcsp** コマンドを使用します。「実行中のシステム情報の表示」セクション（ 12-7 ページ）を参照してください。

（注）　Cisco TrustSec FC リンク暗号化は現在、on モードと off モードの DHCHAP だけでサポートされています。

セキュリティ アソシエーション パラメータの設定

キーや salt などの SA パラメータを設定する手順は、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 モードに入ります。
ステップ 2 ステップ 3	`switch(config)# fcsp esp sa spi_number`	SA を設定するための SA サブモードを開始します。 *spi_number* の範囲は 256 ～ 65536 です。
ステップ 4	`switch(config-sa)# key key`	SA のキーを設定します。*key* の最大サイズは 34 です。
ステップ 5	`switch(config-sa)# no key key`	SA からキーを削除します。
ステップ 6	`switch(config-sa)# salt salt`	SA の salt を設定します。有効な範囲は 0x0 ～ 0xffffffff です。
ステップ 7	`switch(config-sa)# no salt salt`	SA の salt が削除されます。

ESP の設定

この項では、次のトピックについて取り上げます。

- 入力および出力ポートでの ESP の設定（12-4 ページ）
- ESP モードの設定（12-5 ページ）

入力および出力ポートでの ESP の設定

SA が作成されると、ポートにカプセル化セキュリティ プロトコル（ESP）を設定する必要があります。同等のネットワーク間でパケットを暗号化および復号化する出力および入力ポートを指定する必要があります。出力 SA はどのキーまたはパラメータがスイッチから出るパケットの暗号化に使用されるかを指定します。入力 SA はどのキーまたはパラメータが特定のポートに入るパケットの復号化に使用されるかを指定します。

この項では、次のトピックについて取り上げます。

- 入力ポートでの ESP の設定（12-4 ページ）
- 出力ポートでの ESP の設定（12-5 ページ）

入力ポートでの ESP の設定

入力のハードウェアに SA を設定するには、次の手順を実行します。

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 fc x/y`	スロット *x* のポート *y* に FC インターフェイスを設定します。 (注)　ポート チャネルを選択すると、ポート チャネルのすべてのメンバの設定が適用されます。
ステップ 3	`switch(config-if)# fcsp esp manual`	ESP 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 4	`switch(config-if-esp)# ingress-sa spi_number`	入力のハードウェアに SA を設定します。
ステップ 5	`switch (config-if-esp)# no ingress-sa spi_number`	入力のハードウェアから SA を削除します。[1]

1. SA が入力ポートで設定されていない場合、このコマンドを実行すると、エラー メッセージが返されます。

出力ポートでの ESP の設定

出力のハードウェアに SA を設定するには、次の手順を実行します。

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 fc x/y`	スロット *x* のポート *y* に FC インターフェイスを設定します。 (注)　ポート チャネルを選択すると、ポート チャネルのすべてのメンバの設定が適用されます。
ステップ 3	`switch(config-if)# fcsp esp manual`	ESP 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 4	`switch(config-if-esp)# egress-sa spi_number`	出力のハードウェアに SA を設定します。
ステップ 5	`switch(config-if)# no fcsp esp manual`	入力と出力のハードウェアから SA を削除します。[1]

1. SA が出力ポートで設定されていない場合、このコマンドを実行すると、エラー メッセージが返されます。

(注)　インターフェイスの入力および出力ハードウェアに SA を適用するには、インターフェイスが admin shut モードである必要があります。

ESP モードの設定

GCM としてポートがメッセージ認証と暗号化を有効にする、または GMAC としてポートがメッセージ認証を有効にするように、ESP を設定します。

デフォルトの ESP モードは AES-GCM です。

この項では、次のトピックについて取り上げます。

- AES-GCM の設定（12-5 ページ）
- AES-GMAC の設定（12-6 ページ）

AES-GCM の設定

AES-GCM モードを設定するには、次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 ステップ 3 ステップ 4	`switch(config)# interface fc x/y`	スロット *x* のポート *y* に FC インターフェイスを設定します。 (注)　ポート チャネルを選択すると、ポート チャネルのすべてのメンバの設定が適用されます。
	`switch(config-if)# fcsp esp manual`	各ポートの ESP を設定するために ESP 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 5	`switch(config-if-esp)# mode gcm`	インターフェイスの GCM モードを設定します。

AES-GMAC の設定

AES-GMAC モードを設定するには、次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)# interface fc x/y`	スロット *x* のポート *y* に FC インターフェイスを設定します。 (注)　ポート チャネルを選択すると、ポート チャネルのすべてのメンバの設定が適用されます。
ステップ 3		
ステップ 4	`switch(config-if)# fcsp esp manual`	各ポートの ESP を設定するために ESP 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 5	`switch(config-if-esp)# mode gmac`	インターフェイスの GMAC モードを設定します。
ステップ 6	`switch(config-if-esp)# no mode gmac`	GMAC モードをインターフェイスから削除し、デフォルトの AES-GCM モードを適用します。

(注)　ESP モードが設定されるのは、入力または出力ハードウェアに SA が設定されている場合だけです。SA が設定されていない場合は、ESP がオフになり、カプセル化は行われません。

(注)　ポートを設定した後で ESP モードを変更した場合は、変更がシームレスでないため、常にポートのフラップが必要です。ただし、設定は拒否されません。

(注)　FC-SP ポート モードが有効で、ESP 対応のスイッチまたはブレードで使用可能な ISL だけが表示されます。

(注)　選択した ISL がイネーブルであれば、既存の ESP 設定を変更できます。

Cisco TrustSec FC リンク暗号化情報の表示

Fabric Manager または Device Manager では、**show** コマンドを使用して Cisco TrustSec FC リンク暗号化機能の情報を表示できます。

この項では、次のトピックについて取り上げます。

FC-SP のインターフェイス情報の表示

show fcsp interface コマンドを使用して、特定のインターフェイスのすべての FC-SP 関連情報を表示します。

```
switch# show fcsp interface fc7/41

fc7/41:
        fcsp authentication mode:SEC_MODE_OFF
        ESP is enabled
        configured mode is: GCM
        programmed ingress SA: 300, 303
        programmed egress SA: 300
        Status:FC-SP protocol in progress
```

実行中のシステム情報の表示

FC-SP に関連するすべての実行時の情報を表示するには、**show running-config fcsp** コマンドを使用します。ESP および設定されたインターフェイスに関するすべての詳細が表示されます。どのポートが SA を使用しているか調べるには、次のコマンドを使用します。

```
switch# show running-config fcsp
version 4.1(2)
feature fcsp
fcsp esp sa 300
  key 0x00000000000000000000000000123456
  salt 0x123456
fcsp esp sa 301
  key 0x00000000000000000000000000123456
  salt 0x1234567
fcsp esp sa 302
  key 0x00000000000000000000000000123456
  salt 0x123456

interface fc8/48
  fcsp off
  fcsp esp manual
    ingress-sa 300
    ingress-sa 301
    egress-sa 300
```

FC-SP インターフェイス統計情報の表示

インターフェイスに対し DHCHAP と ESP に関連するすべての統計情報を表示するには、**show fcsp interface statistics** コマンドを使用します。示されている ESP 統計情報はポート ASIC でサポートされている ESP により異なります。

```
switch# show fcsp interface fc3/31 statistics

fc7/41:
       fcsp authentication mode:SEC_MODE_ON
        ESP is enabled
        configured mode is: GMAC
        programmed ingress SA: 256, 257
        programmed egress SA: 256
        Status:Successfully authenticated
```

```
Authenticated using local password database
 Statistics:
 FC-SP Authentication Succeeded:17
 FC-SP Authentication Failed:3
 FC-SP Authentication Bypassed:0
 FC-SP ESP SPI Mismatched frames:0
 FC-SP ESP Auth failed frames:0
```

Cisco TrustSec FC リンク暗号化のベスト プラクティス

ベスト プラクティスとは、Cisco TrustSec FC リンク暗号化を適切に動作させるための推奨手順です。

この項では、次のトピックについて取り上げます。

- 一般的なベスト プラクティス（12-8 ページ）
- キーの変更に関するベスト プラクティス（12-8 ページ）

一般的なベスト プラクティス

ここでは、Cisco TrustSec FC リンク暗号化に関する一般的なベスト プラクティスを示します。

- Cisco TrustSec FC リンク暗号化が MDS スイッチ間だけでイネーブルであることを確認します。この機能は、E ポートまたは ISL だけでサポートされており、MDS 以外のスイッチを使用している場合はエラーが発生します。
- 接続にかかわるピアの設定が同一であることを確認します。設定に相違があると、「port re-init limit exceeded」というエラー メッセージが表示されます。
- スイッチ インターフェイスの入力および出力ハードウェアに SA を適用する前に、インターフェイスが admin shut モードであることを確認します。

キーの変更に関するベスト プラクティス

入力および出力ポートに SA を適用した後は、キーの設定を定期的に変更してください。トラフィックの中断を避けるには、キーを順番に変更する必要があります。

例として、2 つのスイッチ、Switch1 と Switch2 の間に作成されたセキュリティ アソシエーションについて考えます。SA は、次の例に示すように、入力および出力ポートに設定されます。

```
switch# config t
switch(config)# interface fc1/1
switch(config-if)# fcsp esp manual
switch(config-if)# ingress-sa 256
switch(config-if)# egress-sa 256
```

これらのスイッチのキーを変更するには、次の手順を実行します。

ステップ 1　Switch1 と Switch2 に新しい SA を追加します。

```
switch# config t
switch(config)# fcsp esp sa 257
switch(config-sa)# key 0xAC9EF8BC8DB2DBD2008D184F794E0C38
switch(config-sa)# salt 0x1234
```

ステップ 2　Switch1 に入力 SA を設定します。

```
switch# config t
switch(config)# interface fc1/1
switch(config-if)# fcsp esp manual
switch(config-if)# ingress-sa 257
```

ステップ 3　Switch2 に入出力 SA を設定します。

```
switch# config t
switch(config)# interface fc1/1
switch(config-if)# fcsp esp manual
switch(config-if)# ingress-sa 257
switch(config-if)# egress-sa 257
```

ステップ 4　Switch1 に出力 SA を設定します。

```
switch# config t
switch(config)# interface fc1/1
switch(config-if)# fcsp esp manual
switch(config-if)# egress-sa 257
```

ステップ 5　両方のスイッチから以前に設定された入力 SA を削除します。

```
switch# config t
switch(config)# interface fc1/1
switch(config-if)# fcsp esp manual
switch(config-if)# no ingress-sa 256
```