



データ暗号化の設定

- 機能情報の確認 (1 ページ)
- データ暗号化の設定の前提条件 (1 ページ)
- データ暗号化の設定に関する制約事項 (2 ページ)
- データの暗号化について (2 ページ)
- データ暗号化の設定方法 (2 ページ)
- データ暗号化の設定例 (3 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。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェアリリースに対応したリリース ノート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 には、<http://www.cisco.com/go/cfn> からアクセスします。Cisco.com のアカウントは必要ありません。

データ暗号化の設定の前提条件

- Cisco 1260、3500、3600、801、1140、1310、および1520シリーズのアクセスポイントは、Datagram Transport Layer Security (DTLS) のデータ暗号化をサポートします。
- デバイスを使用して、特定のアクセスポイントまたはすべてのアクセスポイントのDTLSデータ暗号化を有効化または無効化できます。
- シスコデバイスを使用するロシア人以外のお客様はデータDTLSライセンスは必要ありません。

データ暗号化の設定に関する制約事項

- 暗号化はデバイスおよびアクセスポイントの両方においてスループットを制限するため、多くのエンタープライズネットワークにおいて最大スループットが必要です。
- デバイスにデータ DTLS のライセンスがなく、デバイスに関連付けられているアクセスポイントで DTLS が有効になっている場合、データパスは暗号化されません。
- DTLS ライセンスがないイメージでは DTLS コマンドは使用できません。

データの暗号化について

デバイスにより、DTLS を使用してアクセスポイントとデバイスの CAPWAP コントロールパケット（および、オプションとして CAPWAP データパケット）の暗号化が可能です。DTLS は、標準化過程にある TLS に基づくインターネット技術特別調査委員会（IETF）プロトコルです。CAPWAP コントロールパケットとは、デバイスとコントローラとアクセスポイントの間で交換される管理パケットであり、CAPWAP データパケットは転送された無線フレームをカプセル化します。CAPWAP コントロールおよびデータパケットはそれぞれ異なる UDP ポートである 5246（コントロール）および 5247（データ）で送信されます。アクセスポイントが DTLS データ暗号化をサポートしない場合、DTLS はコントロールプレーンにのみ有効となり、データプレーンの DTLS セッションは確立されません。

データ暗号化の設定方法

データ暗号化の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	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 2	ap link-encryption 例： Device(config)# ap link-encryption	このコマンドを入力して、すべてのアクセスポイントまたは特定のアクセスポイントのデータ暗号化をイネーブルにします。デフォルト値は [disabled] です。 データ暗号化モードに変更するには、アクセスポイントをデバイスに再 join する必要があります。

	コマンドまたはアクション	目的
ステップ 3	end 例： Device(config)# end	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 4	show ap link-encryption 例： Device# show ap link-encryption	すべてのアクセス ポイントまたは特定のアクセス ポイントの暗号化の状態を表示します。このコマンドはまた、整合性チェックの失敗およびリプレイエラーの数を追跡する認証エラーを表示します。リレーエラーは、アクセス ポイントが同じパケットを受信する回数の追跡に役立ちます。
ステップ 5	show wireless dtls connections 例： Device# show wireless dtls connections	すべてのアクティブな DTLS 接続の概要を表示します。 (注) DTLSデータの暗号化に問題が生じた場合は、 debug dtls ap {all event trace} コマンドを入力して、すべての DTLS メッセージ、イベント、またはトレースをデバッグします。

関連トピック

[すべてのアクセス ポイントのデータ暗号化の状態の表示：例](#) (3 ページ)

データ暗号化の設定例

すべてのアクセス ポイントのデータ暗号化の状態の表示：例

次に、すべてのアクセス ポイントまたは特定のアクセス ポイントの暗号化の状態を表示する例を示します。このコマンドはまた、整合性チェックの失敗およびリプレイエラーの数を追跡する認証エラーを表示します。リレーエラーは、アクセス ポイントが同じパケットを受信する回数の追跡に役立ちます。

```
Device# show ap link-encryption
          Encryption  Dnstream  Upstream  Last
AP Name      State      Count      Count      Update
-----
3602a          Enabled      0          0      Never
```

次に、すべてのアクティブな DTLS 接続のサマリーを表示する例を示します。

すべてのアクセスポイントのデータ暗号化の状態の表示：例

```
Device# show wireless dtls connections
AP Name          Local Port  Peer IP      Peer Port    Ciphersuite
-----
3602a            Capwap_Ctrl 10.10.21.213 46075        TLS_RSA_WITH_AES_128_CBC_SHA
3602a            Capwap_Data 10.10.21.213 46075        TLS_RSA_WITH_AES_128_CBC_SHA
```