USB でのデータ保存

Universal Serial Bus（USB）ストレージ機能を使用すると、特定のモデルのシスコ製のルータで USB フラッシュ モジュールをサポートし、USB キー フォーム ファクタ（別名 USB eToken）で SmartCard テクノロジー（Aladdin Knowledge Systems 社製）を使用してルータへのセキュアなアクセスを提供できます。

USB eToken はセキュアなコンフィギュレーション配布を実現し、配置用にユーザによる Virtual Private Network（VPN; バーチャル プライベート ネットワーク）認証資格情報の保存を可能にします。USB フラッシュ ドライブを使用すると、イメージとコンフィギュレーションをルータ外に保存できます。

機能情報の入手方法

使用するソフトウェア リリースで、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。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「USB でのデータ保存の機能情報」（P.19）を参照してください。

プラットフォームのサポートと Cisco IOS および Catalyst OS 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。

この章の構成

USB にデータを保存する場合の前提条件

USB フラッシュ モジュールまたは eToken を使用する前に、次のシステム要件を満たしていなければなりません。

- Cisco 871 ルータ、Cisco 1800 シリーズ、Cisco 2800 シリーズ、あるいは Cisco 3800 シリーズ ルータ。
- サポートされているいずれかのプラットフォーム上で、少なくとも Cisco IOS Release 12.3(14)T イメージが稼動していること。
- シスコ対応の USB フラッシュまたは USB eToken。
- USB eToken サポートには k9 イメージが必要（ただし、USB フラッシュ サポートはすべてのイメージで利用可能です）。

USB にデータを保存する場合の制限事項

- USB eToken がサポートされるためには、ファイルをセキュアに保存できる 3DES（k9）Cisco IOS ソフトウェア イメージが必要です。
- USB ハブは現在、サポートされていません。そのため、サポートされるデバイスの数は、多くてもルータ シャーシで使用できる USB ポートの数までです。
- eToken または USB フラッシュからイメージを起動することはできません（ただし、eToken とフラッシュの両方からコンフィギュレーションを起動することはできます）。

USB へのデータ保存について

ルータで USB フラッシュ モジュールとセキュアな eToken を使用するには、次の概念を理解する必要があります。

- 「USB eToken と USB フラッシュの役割」（P.2）
- 「USB ストレージ ファイルシステム サポート」（P.4）
- 「USB にデータを保存する利点」（P.4）

USB eToken と USB フラッシュの役割

USB eToken と USB フラッシュ モジュールの両方を使用してファイル（ルータ コンフィギュレーションなど）を保存できます。次の項では、各デバイスの機能方法と各デバイス間の差異について説明します。

- 「USB eToken の動作の仕組み」（P.2）
- 「USB フラッシュの動作の仕組み」（P.3）
- 「eToken と USB フラッシュの機能的差異」（P.3）

USB eToken の動作の仕組み

SmartCard はプラスティック製の小型カードで、データの保存や処理を行うためのマイクロプロセッサやメモリが搭載されています。USB インターフェイスを備えた SmartCard が SmartCard eToken です。eToken では、記憶域の容量（32KB）内であれば、どのようなタイプのファイルでもセキュアに保存

できます。eToken に保存されたコンフィギュレーション ファイルに対する暗号化およびアクセスは、ユーザ PIN を介してだけ行えます。ルータにコンフィギュレーション ファイルをロードするには、ルータのコンフィギュレーション ファイルをセキュアに配布できるよう適切な PIN が設定されている必要があります。

eToken をルータに装着したら、その eToken にログインする必要があります。ログイン後は、ユーザ PIN（デフォルトは 1234567890）や、ログインが拒否されるようになるまで許容されるログイン試行の失敗回数（デフォルトは 15 回）など、さまざまなデフォルト設定を変更できます。eToken のアクセス方法および設定方法については、「eToken のアクセスと設定」を参照してください。

eToken へ正常にログインした場合は、**copy** コマンドを使用して、ルータから eToken へファイルをコピーできます。デフォルトでは、ルータから eToken を削除した後、関連付けられているすべての RSA キーが削除され、次回の Internet Key Exchange（IKE; インターネット キー エクスチェンジ）ネゴシエーション期間まで、IPSec トンネルは切断されません（デフォルトの動作を変更し、IPSec トンネルが切断されるまでの時間を指定する場合は、**crypto pki token removal timeout** コマンドを発行します）。

Aladdin Knowledge Systems 社製の eToken の詳細については、Aladdin 社の Web サイト http://www.aladdin.com/etoken/cisco/ を参照してください。

USB フラッシュの動作の仕組み

Cisco USB フラッシュ モジュールでは、ルータ構成と Cisco IOS ソフトウェア イメージの保存と配置ができます。Cisco USB フラッシュ モジュールには 64MB、128MB、256MB のバージョンがあります。

（注） USB フラッシュはルータの起動に必要なルータ コンパクト フラッシュの代わりになるものではありません。

USB フラッシュ モジュールをルータに挿入すると、スタートアップ コンフィギュレーションに **boot config** コマンドが含まれ、**boot config usbflash0: new-config** などの USB フラッシュ デバイスにある新しいコンフィギュレーションを指定している場合は、コンフィギュレーション ファイルを自動的に起動します。

eToken と USB フラッシュの機能的差異

eToken と USB フラッシュの両方がセカンダリ ストレージを提供しますが、各デバイスにはそれぞれ利点と制限事項があります。ニーズに合ったデバイスを検討する際に役立つよう、表 1 で eToken と USB フラッシュの機能的差異をハイライトしています。

表 1　eToken と USB フラッシュの機能的差異

機能	USB eToken	USB フラッシュ
アクセシビリティ	デジタル証明書、事前共有鍵、およびルータ設定を eToken からルータへセキュアに保存したり転送したりするためのものです。	USB フラッシュからルータのルータ構成とイメージを保存して配置するために使用します。
ストレージのサイズ	32KB	• 64MB • 128MB • 256MB

表 1　eToken と USB フラッシュの機能的差異 （続き）

機能	USB eToken	USB フラッシュ
ファイル タイプ	• 通常、IPSec VPN 用のデジタル証明書、事前共有鍵、およびルータ設定を保存する場合に使用します。 • eToken は Cisco IOS イメージを保存できません。	コンパクト フラッシュに保存できるファイル タイプを保存します。
セキュリティ	• ファイルに対する暗号化およびアクセスは、ユーザ PIN を介してだけ行えます。 • ファイルは、ノンセキュアなフォーマットでも保存できます。	ファイルは、ノンセキュアなフォーマットでだけ保存できます。
ブート設定	• ルータではブート時に、USB トークンに保存されている設定を使用できます。 • ルータではブート時に、eToken に保存されているセカンダリ設定を使用できます（セカンダリ設定を使用すると、ユーザは各自の IPSec 設定をロードできます）。	• **boot config** コマンドが発行される場合（**boot config usbflash0: new-config** など）は、コンフィギュレーション ファイルは自動的に USB フラッシュからルータに転送できます。

USB ストレージ ファイルシステム サポート

USB ストレージ デバイス容量は拡大しているため、DOSFS と usbflash コンポーネントを修正して、大容量 USB ストレージ デバイスを使用可能にしておく必要があります。USB ストレージ ファイルシステム サポート機能は USB フラッシュ デバイスの DOSFS サポートを拡張します。この機能を使用すると、大容量 USB ストレージ デバイスにデータを保存できます。

USB にデータを保存する利点

Cisco ルータでの USB フラッシュ ドライブと USB eToken サポートは次のアプリケーションに関する利点を提供します。

移動可能な証明書：配置する VPN クレデンシャルを外部デバイスに保存できます。

Aladdin eToken は SmartCard テクノロジーを使用して、デジタル証明書と IPSec VPN 導入用のコンフィギュレーションを保存できます。これにより、ルータにおいて RSA 公開鍵を生成し、少なくとも 1 つの IPSec トンネルを認証できるようになりました（ルータでは複数の IPSec トンネルを開始できるため、eToken には、必要に応じて複数の証明書を保存できるようになっています）。

VPN クレデンシャルを外部デバイスに保存すると、機密データが漏洩する危険性は低くなります。

ファイルをセキュアに配置するための PIN 設定

Aladdin eToken は、ユーザ設定 PIN 経由でのルータ上での暗号化をイネーブルにするために使用できるコンフィギュレーション ファイルを保存できます（つまり、デジタル証明書、事前共有鍵、および VPN は使用されません）。

軽減されるまたは不要になる手動での設定作業

eToken と USB フラッシュの両方がほとんど手作業なしにリモート ソフトウェア コンフィギュレーションとプロビジョニングを提供できます。設定は自動プロセスとして構成されます。つまり、いずれのデバイスも eToken または USB フラッシュがルータに挿入された後、ルータが起動するために使用できるブートストラップ設定を保存できます。さらにこのルータは、ブートストラップ設定によって TFTP サーバへ接続され、その TFTP サーバに保存されている設定に基づいて、すべてのルータ設定が行われます。

Cisco ルータで USB モジュールをセットアップおよび使用する方法

ここでは、USB モジュールをサポートするためのルータの設定手順について説明します。

外部 USB フラッシュ ドライブまたは eToken のコンフィギュレーションの保存

次の作業を使用して、USB フラッシュ ドライブ モジュールまたは eToken にコンフィギュレーション ファイルを保存します。

手順の概要

1. **enable**
2. **configure terminal**
3. **boot config** *file-system-prefix*:[*directory*/]*filename* [**nvbypass**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# 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 3	**boot config** *file-system-prefix*:[*directory*/]*filename* [**nvbypass**] **例：** `Router(config)# boot config usbflash0:`	USB フラッシュ ドライブまたはセキュアな eToken にスタートアップ コンフィギュレーション ファイルが保存されていることを指定します。 **（注）** USB フラッシュ ドライブを使用する場合は、**flash:** からブート ヘルパーが起動します。ブート ヘルパーは Cisco IOS イメージで **flash:** にあります。使用する Cisco IOS イメージは USB を認識する必要があります。

eToken のアクセスと設定

eToken を Cisco ルータに挿入した後、次に示す方法で eToken にログインする必要があります。

- 「eToken へのログイン」（P.6）（必須）

eToken にログインしたら、次に示す方法でユーザ PIN の変更やルータから eToken へのファイル コピーなどの管理作業を実行できます。

- 「eToken での管理者機能の設定」（P.8）（任意）

RSA キーと eToken の使用

- RSA キーは、eToken がルータへ正常にログインした後にロードされます。
- デフォルトの場合、新規に生成された RSA キーは、最後に装着された eToken に保存されます。再生成されたキーは、元の RSA キーが生成されたのと同じ場所に保存する必要があります。

eToken へのログイン

この作業を使用して、eToken に手動または自動でログインします。

自動ログイン

自動ログインを使用すると、ユーザやオペレータが介入することなく、ルータを完全な稼動状態に戻せます。PIN は、プライベート コンフィギュレーションに保存されるため、スタートアップ コンフィギュレーションや実行コンフィギュレーションには表示されません。

（注） 手動で生成されたスタートアップ コンフィギュレーションには、配置用に自動ログイン コマンドを指定できますが、手動で生成されたそのコンフィギュレーションをプライベート コンフィギュレーションに取り込むには、**copy system:running-config nvram: startup-config** コマンドを発行する必要があります。

手動ログイン

手動ログインは、PIN をルータ上に保存するのが適していない場合に使用できます。手動ログインは、権限の有無にかかわらず実行できます。また、手動ログインを実行すると、eToken 上のファイルおよび RSA キーが、Cisco IOS ソフトウェアで使用可能になります。セカンダリ コンフィギュレーション ファイルを設定する場合は、ログインを実行するユーザの権限がある場合にだけ手動ログインを実行できます。そのため、何らかの目的で、手動ログインを実行し、eToken 上にセカンダリ コンフィギュレーション ファイルを設定する場合は、権限をイネーブルにする必要があります。

手動ログインは、失われたルータ設定のリカバリを行う場合にも使用できます。通常 VPN を使用してコア ネットワークへ接続しているリモート サイトが存在する状況では、設定および RSA キーが失われた場合、eToken が備えているアウトオブバンド サービスが必要となります。eToken には、ブート設定、セカンダリ設定、および接続を認証するための RSA キーを保存できます。

また、初期導入時やハードウェア交換時に、ルータを現地の業者から調達したり、リモート サイトへ直送したりする場合にも、手動ログインが適しています。

自動ログインとは異なり、手動ログインを使用する場合は、ユーザが実際の eToken PIN を把握している必要があります。ユーザが物理的に eToken にアクセスできる場合は、Aladdin の Windows ベースのユーティリティを使用して、RSA キーとセカンダリ コンフィギュレーション ファイルを eToken からコピーできます。

手順の概要

1. **enable**
2. **crypto pki token** *token-name* [**admin**] **login** [*pin*]

   または

   configure terminal
3. **crypto pki token** *token-name* **user-pin** [*pin*]
4. exit
5. **show usbtoken**[**0-9**]**:***filename*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。

ステップ 2	**crypto pki token** *token-name* [**admin**] **login** [*pin*]
	
	例：
	`Router# crypto pki token usbtoken0 admin login 5678`
	
	または
	
	configure terminal
	
	例：
	`Router# configure terminal`
		手動で eToken にログインします。
		後でユーザ PIN を変更する場合は、**admin** キーワードを指定する必要があります。
		
		または
		ルータのモードを、eToken の自動ログインを設定できるグローバル コンフィギュレーション モードにします。

ステップ 3	**crypto pki token** *token-name* **user-pin** [*pin*] **例：** `Router(config)# crypto pki token usbtoken0 user-pin 1234`	（任意）ルータが自動的に起動時に USB eToken にログインできるように PIN を作成します。 **（注）** すでに手動ログインを設定している場合は、このコマンドを発行しないでください。
ステップ 4	**exit** **例：** `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 5	**show usbtoken**[**0-9**]:*filename* **例：** `Router#`	（任意）USB eToken がルータにログインしているかどうかを確認します。

eToken での管理者機能の設定

この作業を使用して、ユーザ PIN および eToken 上の失敗回数の上限などのデフォルト設定を変更します。

手順の概要

1. **enable**
2. **crypto pki token** *token-name* [**admin**] **change-pin** [*pin*]
3. **configure terminal**
4. **crypto pki token** {*token-name* | **default**} **removal timeout** [*minutes*]
5. **crypto pki token** {*token-name* | **default**} **max-retries** [*number*]
6. **exit**
7. **copy usbflash**[**0-9**]:*filename destination-url*
8. **show usbtoken**[**0-9**]:*filename*
9. **crypto pki token** *token-name* **logout**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**crypto pki token** *token-name* [**admin**] **change-pin** [*pin*] **例：** `Router# crypto pki token usbtoken0 admin change-pin`	（任意）USB eToken 上のユーザ PIN 番号を変更します。 • PIN が変更されない場合は、デフォルトの PIN（1234567890）が使用されます。 **（注）** PIN の変更後は、ログインの失敗回数を 0 にリセットする必要があります（**crypto pki token max-retries** コマンドを使用）。許容されるログインの失敗回数の上限は、15（デフォルト）に設定されています。
ステップ 3	**configure terminal** **例：** `Router# 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 4	**crypto pki token** {*token-name* | **default**} **removal timeout** [*seconds*] **例：** `Router(config)# crypto pki token usbtoken0 removal timeout 60`	（任意）eToken がルータから取り外されてから、eToken に保存されている RSA キーが削除されるまで、ルータが待機する時間を秒単位で設定します。 **（注）** このコマンドが発行されない場合は、eToken がルータから取り外された直後に、すべての RSA キーが削除される他、eToken に関連付けられている IPSec トンネルもすべて切断されます。
ステップ 5	**crypto pki token** {*token-name* | **default**} **max-retries** [*number*] **例：** `Router(config)# crypto pki token usbtoken0 max-retries 20`	（任意）eToken へのアクセスが拒否されるまでに許容されるログイン試行の連続失敗回数の上限を設定します。 • デフォルト値は 15 です。
ステップ 6	**exit** **例：** `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 7	`copy usbflash[0-9]:`*filename destination-url* **例：** `Router# copy usbflash0:`	ルータから eToken にファイルをコピーします。 • *destination-url*：サポートされているオプションのリストについては、**copy** コマンドに関するセクションを参照してください。
ステップ 8	**show usbtoken**[0-9]:*filename* **例：** `Router#`	（任意）USB eToken に関する情報を表示します。このコマンドを使用すると、USB eToken がルータにログインしているかどうかを確認できます。

ステップ 9	`crypto pki token` *token-name* `logout`
	
	例：
	`Router# crypto pki toke usbtoken0 logout`
		USB eToken からルータをログアウトします。
		（注） USB eToken に何らかのデータを保存する場合は、再度 eToken にログインする必要があります。

USB フラッシュ ドライブと eToken のトラブルシューティング

ここでは、次の各 Cisco IOS コマンドについて説明します。これらのコマンドは、USB フラッシュまたは USB eToken の使用中に発生し得る問題についてのトラブルシューティングに使用できます。

show file systems コマンド

ステップ 1 **show file systems** コマンドを使用すると、USB モジュールが USB ポートに差し込まれていることをルータが認識しているかどうかを判定できます。差し込まれている USB モジュールは、ファイル システムのリスト上に表示されます。これらのモジュールがリスト上に表示されない場合は、次のいずれかの問題が発生している可能性があります。

- USB モジュールとの接続の問題
- ルータ上で稼動している Cisco IOS イメージが USB モジュールをサポートしない
- USB モジュールそのもののハードウェア上の問題

ステップ 2 USB モジュールが以前に正常にフォーマットされている場合は、**show file systems** コマンドを使用します。Cisco ルータと互換性を持たせるには、USB フラッシュ モジュールを FAT16 形式でフォーマットする必要があります。これが当てはまらない場合は、**show file systems** コマンドを使用すると、互換性のないファイル システムであることを示すエラーが表示されます。

USB フラッシュ モジュールと USB eToken を示す **show file systems** コマンドのサンプル出力を次に示します。USB モジュールが現れるのはリストの最下行です。

```
Router# show file systems

File Systems:

     Size(b)     Free(b)      Type  Flags  Prefixes
           -           -    opaque     rw   archive:
           -           -    opaque     rw   system:
           -           -    opaque     rw   null:
           -           -   network     rw   tftp:
*  129880064    69414912      disk     rw   flash:#
      491512      486395     nvram     rw   nvram:
           -           -    opaque     wo   syslog:
           -           -    opaque     rw   xmodem:
           -           -    opaque     rw   ymodem:
           -           -   network     rw   rcp:
           -           -   network     rw   pram:
           -           -   network     rw   ftp:
           -           -   network     rw   http:
           -           -   network     rw   scp:
           -           -   network     rw   https:
           -           -    opaque     ro   cns:
    63158272    33037312  usbflash     rw   usbflash0:
       32768         858  usbtoken     rw   usbtoken1:
```

show usb device コマンド

ステップ 1 **show usb device** コマンドを使用すると、USB モジュールがシスコによりサポートされているかどうかを判別できます。モジュールがサポートされているかどうかを示す USB フラッシュと USB eToken の両方のサンプル出力が、次のサンプル出力例で強調表示されています。

次のサンプル出力は USB フラッシュ モジュールのものです。

```
Router# show usb device

Host Controller:1
Address:0x1
Device Configured:YES
Device Supported:YES
Description:DiskOnKey
Manufacturer:M-Sys
Version:2.0
Serial Number:0750D84030316868
Device Handle:0x1000000
USB Version Compliance:2.0
Class Code:0x0
Subclass Code:0x0
Protocol:0x0
Vendor ID:0x8EC
Product ID:0x15
Max. Packet Size of Endpoint Zero:64
Number of Configurations:1
Speed:Full
Selected Configuration:1
Selected Interface:0

Configuration:
    Number:1
    Number of Interfaces:1
    Description:
    Attributes:None
    Max Power:140 mA

    Interface:
        Number:0
        Description:
        Class Code:8
        Subclass:6
        Protocol:80
        Number of Endpoints:2

        Endpoint:
            Number:1
            Transfer Type:BULK
            Transfer Direction:Device to Host
            Max Packet:64
            Interval:0

        Endpoint:
            Number:2
            Transfer Type:BULK
            Transfer Direction:Host to Device
            Max Packet:64
            Interval:0
```

次のサンプル出力はサポートされている USB eToken のものです。

```
Router# show usb device
```

```
Host Controller:1
Address:0x11
Device Configured:YES
Device Supported:YES
Description:eToken Pro 4254
Manufacturer:AKS
Version:1.0
Serial Number:
Device Handle:0x1010000
USB Version Compliance:1.0
Class Code:0xFF
Subclass Code:0x0
Protocol:0x0
Vendor ID:0x529
Product ID:0x514
Max. Packet Size of Endpoint Zero:8
Number of Configurations:1
Speed:Low
Selected Configuration:1
Selected Interface:0

Configuration:
    Number:1
    Number of Interfaces:1
    Description:
    Attributes:None
    Max Power:60 mA

    Interface:
        Number:0
        Description:
        Class Code:255
        Subclass:0
        Protocol:0
        Number of Endpoints:0
```

show usb controllers コマンド

ステップ 1 **show usb controllers** コマンドを使用すると、USB フラッシュ モジュールにハードウェア上の問題があるかどうかを判別できます。**show usb controllers** コマンドの出力結果にエラーが表示された場合は、USB モジュールにハードウェア上の問題があると考えられます。

USB フラッシュ モジュールに対するコピー操作が正常に行われていることを確認する場合にも、この **show usb controllers** コマンドを使用できます。ファイルのコピーを実行した後で、**show usb controllers** コマンドを発行すると、データ転送が正常に行われたことを示す内容が表示されます。

次に示すのは、使用中の USB フラッシュ モジュールの **show usb controllers** コマンドによる出力例です。

```
Router# show usb controllers

Name:1362HCD
Controller ID:1
Controller Specific Information:
    Revision:0x11
    Control:0x80
    Command Status:0x0
    Hardware Interrupt Status:0x24
    Hardware Interrupt Enable:0x80000040
```

```
    Hardware Interrupt Disable:0x80000040
    Frame Interval:0x27782EDF
    Frame Remaining:0x13C1
    Frame Number:0xDA4C
    LSThreshold:0x628
    RhDescriptorA:0x19000202
    RhDescriptorB:0x0
    RhStatus:0x0
    RhPort1Status:0x100103
    RhPort2Status:0x100303
    Hardware Configuration:0x3029
    DMA Configuration:0x0
    Transfer Counter:0x1
    Interrupt:0x9
    Interrupt Enable:0x196
    Chip ID:0x3630
    Buffer Status:0x0
    Direct Address Length:0x80A00
    ATL Buffer Size:0x600
    ATL Buffer Port:0x0
    ATL Block Size:0x100
    ATL PTD Skip Map:0xFFFFFFFF
    ATL PTD Last:0x20
    ATL Current Active PTD:0x0
    ATL Threshold Count:0x1
    ATL Threshold Timeout:0xFF

Int Level:1
Transfer Completion Codes:
         Success              :920            CRC              :0
         Bit Stuff            :0              Stall            :0
         No Response          :0              Overrun          :0
         Underrun             :0              Other            :0
         Buffer Overrun       :0              Buffer Underrun :0
Transfer Errors:
         Canceled Transfers   :2              Control Timeout :0
Transfer Failures:
         Interrupt Transfer   :0              Bulk Transfer   :0
         Isochronous Transfer :0              Control Transfer:0
Transfer Successes:
         Interrupt Transfer   :0              Bulk Transfer   :26
         Isochronous Transfer :0              Control Transfer:894

USBD Failures:
         Enumeration Failures :0              No Class Driver Found:0
         Power Budget Exceeded:0

USB MSCD SCSI Class Driver Counters:
         Good Status Failures :3              Command Fail    :0
         Good Status Timed out:0              Device not Found:0
         Device Never Opened  :0              Drive Init Fail :0
         Illegal App Handle   :0              Bad API Command :0
         Invalid Unit Number  :0              Invalid Argument:0
         Application Overflow :0              Device in use   :0
         Control Pipe Stall   :0              Malloc Error    :0
         Device Stalled       :0              Bad Command Code:0
         Device Detached      :0              Unknown Error   :0
         Invalid Logic Unit Num:0

USB Aladdin Token Driver Counters:
         Token Inserted       :1              Token Removed   :0
         Send Insert Msg Fail :0              Response Txns   :434
         Dev Entry Add Fail   :0              Request Txns    :434
         Dev Entry Remove Fail:0              Request Txn Fail:0
```

```
         Response Txn Fail    :0                Command Txn Fail:0
         Txn Invalid Dev Handle:0

USB Flash File System Counters:
         Flash Disconnected   :0                Flash Connected :1
         Flash Device Fail    :0                Flash Ok        :1
         Flash startstop Fail :0                Flash FS Fail   :0

USB Secure Token File System Counters:
         Token Inserted       :1                Token Detached  :0
         Token FS success     :1                Token FS Fail   :0
         Token Max Inserted   :0                Create Talker Failures:0
         Token Event          :0                Destroy Talker Failures:0
         Watched Boolean Create Failures:0
```

dir コマンド

ステップ 1 **dir** コマンドと **usbflash[0-9]:** または **usbtoken[0-9]:** キーワードを使用して、USB フラッシュまたは USB eToken のすべてのファイル、ディレクトリ、および権限文字列を表示します。

次の出力例は、USB フラッシュに関するディレクトリ情報を表示したものです。

```
Router# dir usbflash0:

Directory of usbflash0:/

    1  -rw-    30125020  Dec 22 2032 05:31:32 +00:00  c3825-entservicesk9-mz.123-14.T

63158272 bytes total (33033216 bytes free)
```

次の出力例は、USB eToken に関するディレクトリ情報を表示したものです。

```
Router# dir usbtoken1:

Directory of usbtoken1:/

    2  d---           64  Dec 22 2032 05:23:40 +00:00  1000
    5  d---         4096  Dec 22 2032 05:23:40 +00:00  1001
    8  d---            0  Dec 22 2032 05:23:40 +00:00  1002
   10  d---          512  Dec 22 2032 05:23:42 +00:00  1003
   12  d---            0  Dec 22 2032 05:23:42 +00:00  5000
   13  d---            0  Dec 22 2032 05:23:42 +00:00  6000
   14  d---            0  Dec 22 2032 05:23:42 +00:00  7000
   15  ----          940  Jun 27 1992 12:50:42 +00:00  mystartup-config
   16  ----         1423  Jun 27 1992 12:51:14 +00:00  myrunning-config

32768 bytes total (858 bytes free)
```

次の出力例は、ルータにより認識されているすべてのデバイスについてのディレクトリ情報を表示したものです。

```
Router# dir all-filesystems

Directory of archive:/

No files in directory

No space information available
Directory of system:/

    2  drwx           0                    <no date>  its
```

```
  115  dr-x           0                    <no date>  lib
  144  dr-x           0                    <no date>  memory
    1  -rw-        1906                    <no date>  running-config
  114  dr-x           0                    <no date>  vfiles

No space information available
Directory of flash:/

    1  -rw-    30125020  Dec 22 2032 03:06:04 +00:00  c3825-entservicesk9-mz.123-14.T

129880064 bytes total (99753984 bytes free)
Directory of nvram:/

  476  -rw-        1947                    <no date>  startup-config
  477  ----          46                    <no date>  private-config
  478  -rw-        1947                    <no date>  underlying-config
    1  -rw-           0                    <no date>  ifIndex-table
    2  ----           4                    <no date>  rf_cold_starts
    3  ----          14                    <no date>  persistent-data

491512 bytes total (486395 bytes free)
Directory of usbflash0:/

    1  -rw-    30125020  Dec 22 2032 05:31:32 +00:00  c3825-entservicesk9-mz.123-14.T

63158272 bytes total (33033216 bytes free)
Directory of usbtoken1:/

    2  d---          64  Dec 22 2032 05:23:40 +00:00  1000
    5  d---        4096  Dec 22 2032 05:23:40 +00:00  1001
    8  d---           0  Dec 22 2032 05:23:40 +00:00  1002
   10  d---         512  Dec 22 2032 05:23:42 +00:00  1003
   12  d---           0  Dec 22 2032 05:23:42 +00:00  5000
   13  d---           0  Dec 22 2032 05:23:42 +00:00  6000
   14  d---           0  Dec 22 2032 05:23:42 +00:00  7000
   15  ----         940  Jun 27 1992 12:50:42 +00:00  mystartup-config
   16  ----        1423  Jun 27 1992 12:51:14 +00:00  myrunning-config

32768 bytes total (858 bytes free)
```

セキュアなトークン サポートの設定例

ここでは、次の設定例を示します。

- 「ログインして RSA キーを eToken に保存：例」（P.15）

ログインして RSA キーを eToken に保存：例

次に示すのは、eToken にログインして RSA キーを生成し、その RSA キーを eToken に保存する場合の設定例です。

```
! Configure the router to automatically log into the eToken
configure terminal
 crypto pki token default user-pin 0 1234567890
! Generate RSA keys and enroll certificates with the CA.
crypto pki trustpoint IOSCA
 enrollment url http://10.23.2.2
 exit
```

```
crypto ca authenticate IOSCA
Certificate has the following attributes:
       Fingerprint MD5:23272BD4 37E3D9A4 236F7E1A F534444E
      Fingerprint SHA1:D1B4D9F8 D603249A 793B3CAF 8342E1FE 3934EB7A

% Do you accept this certificate? [yes/no]:yes
Trustpoint CA certificate accepted.
crypto pki enroll
crypto pki enroll IOSCA
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.

Password:
Re-enter password:

% The subject name in the certificate will include:c2851-27.cisco.com
% Include the router serial number in the subject name? [yes/no]:no
% Include an IP address in the subject name? [no]:no
Request certificate from CA? [yes/no]:yes
% Certificate request sent to Certificate Authority
% The 'show crypto ca certificate IOSCA verbose' command will show the fingerprint.


*Jan 13 06:47:19.413:CRYPTO_PKI: Certificate Request Fingerprint MD5:E6DDAB1B
 0E30EFE6 54529D8A DA787DBA
*Jan 13 06:47:19.413:CRYPTO_PKI: Certificate Request Fingerprint SHA1:3B0F33B
7 57C02A10 3935042B C4B6CD3D 61039251
*Jan 13 06:47:21.021:%PKI-6-CERTRET:Certificate received from Certificate Authority
! Issue the write memory command, which will automatically save the RSA keys to the eToken
! instead of private NVRAM.
Router# write memory
Building configuration...
[OK]

*Jan 13 06:47:29.481:%CRYPTO-6-TOKENSTOREKEY:Key c2851-27.cisco.com stored on
Cryptographic Token eToken Successfully
```

次に示すのは、eToken から正常にロードされた保存済みクレデンシャルの **show crypto key mypubkey rsa** コマンドによる出力例です。eToken 上に保存されているクレデンシャルは、保護領域内に存在します。eToken 上にクレデンシャルを保存する場合、それらのファイルは /keystore というディレクトリに保存されます。ただし、キー ファイルは CLI からは非表示になります。

```
Router# show crypto key mypubkey rsa

% Key pair was generated at:06:37:26 UTC Jan 13 2005
Key name:c2851-27.cisco.com
 Usage:General Purpose Key
 Key is not exportable.
 Key Data:
  305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00E3C644 43AA7DDD
  732E0F4E 3CA0CDAB 387ABF05 EB8F22F2 2431F1AE 5D51FEE3 FCDEA934 7FBD3603
  7C977854 B8E999BF 7FC93021 7F46ABF8 A4BA2ED6 172D3D09 B5020301 0001
% Key pair was generated at:06:37:27 UTC Jan 13 2005
Key name:c2851-27.cisco.com.server
 Usage:Encryption Key
 Key is not exportable.
 Key Data:
  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00DD96AE 4BF912EB
  2C261922 4784EF98 2E70E837 774B3778 7F7AEB2D 87F5669B BF5DDFBC F0D521A5
```

```
56AB8FDC 9911968E DE347FB0 A514A856 B30EAFF4 D1F453E1 003CFE65 0CCC6DC7
21FBE3AC 2F8DEA16 126754BC 1433DEF9 53266D33 E7338C95 BB020301 0001
```

その他の関連資料

次の項に、USB 機能を使用したデータの保存に関する参考資料を示します。

関連資料

関連項目	参照先
ルータへの USB モジュールの接続	『*Cisco Access Router USB Flash Module and USB eToken Hardware Installation Guide*』
eToken および USB フラッシュのデータ シート	『*USB eToken and USB Flash Features Support*』
ファイル管理（ファイルのロード、コピー、および再起動）	『*Cisco IOS Configuration Fundamentals and Network Management Configuration Guide*』の「*File Management*」の項
デジタル証明書暗号化の設定	『*Cisco IOS Security Configuration Guide*』の「*Configuring Certification Authority Interoperability*」の章

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
なし	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

USB でのデータ保存の機能情報

表 2 に、このモジュールに記載されている機能および具体的な設定情報へのリンクを示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。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。

（注） 表 2 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していない限り、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 2　USB でのデータ保存の機能情報

機能名	リリース	機能情報
USB ストレージ	12.3(14)T	USB ストレージ機能は特定のモデルの Cisco ルータで USB フラッシュ モジュールをサポートし、USB キー フォーム ファクタ（別名 USB eToken）で SmartCard テクノロジー（Aladdin Knowledge Systems 社製）を使用してルータにセキュアなアクセスを提供します。 この機能に関する詳細については、次の各項を参照してください。 • 「USB へのデータ保存について」（P.2） • 「Cisco ルータで USB モジュールをセットアップおよび使用する方法」（P.5） • 「セキュアなトークン サポートの設定例」（P.15） 次のコマンドが導入または修正されました。**crypto pki token change-pin**、**crypto pki token login**、**crypto pki token logout**、**crypto pki token max-retries**、**crypto pki token removal timeout**、**crypto pki token secondary config**、**crypto pki token user-pin**、**debug usb**、**driver**、**show usb driver**、**show usb controllers**、**show usb device**、**show usb driver**、**show usb port**、**show usbtoken**、**show usb tree**、**boot config**、**copy**、**delete**、**dir**、**format**
USB ストレージ ファイルシステム サポート	12.2(33)SRE	USB ストレージ ファイルシステム サポート機能は USB フラッシュ デバイスの DOSFS サポートを拡張します。この機能を使用すると、大容量 USB ストレージ デバイスにデータを保存できます。 12.2(33)SRE では、この機能は Cisco 7200-NPE-G2 で導入されました。 この機能に関する詳細については、次の各項を参照してください。 • 「USB ストレージ ファイルシステム サポート」（P.4） 次のコマンドが導入または修正されました。**cd**, **verify**、**mkdir**、**fsck**