Kerberos の設定

Kerberos に関する情報

Kerberos は、マサチューセッツ工科大学（MIT）が開発した秘密キーネットワーク認証プロトコルであり、暗号化と認証にデータ暗号規格（DES）暗号アルゴリズムを使用します。Kerberos は、ネットワーク リソースの要求を認証するために設計されました。Kerberos は他の秘密キーシステムと同様に、ユーザーとサービスのセキュアな検証を実行する、信頼できるサードパーティの概念に基づいています。Kerberos プロトコルでは、この信頼できるサードパーティは、キー発行局（KDC）と呼ばれます。

Kerberos の主な用途は、ユーザと、そのユーザが使用するネットワーク サービスの身元が主張どおりであることを検証することです。この検証のために、信頼できる Kerberos サーバがユーザにチケットを発行します。有効期限のあるこれらのチケットは、ユーザの認定証キャッシュに保存されており、標準のユーザ名とパスワードの認証メカニズムの代わりに使用できます。

Kerberos の認定証スキームは、「シングル ログイン」という概念を表しています。この手順では、ユーザを 1 回認証することが必要で、ユーザ クレデンシャルが有効な間は（他のパスワードの暗号化を行わずに）セキュア認証が可能になります。

Cisco IOS XE ソフトウェアは Kerberos 5 をサポートするようになりました。そのため、Kerberos 5 をすでに配置している組織の場合、ルータ上で、他のネットワーク ホスト（UNIX サーバや PC など）ですでに使用している同じ Kerberos 認証データベースを使用できます。

次のネットワーク サービスは、Cisco IOS XE ソフトウェアの Kerberos 認証機能によってサポートされています。

- Telnet
- rlogin

- rsh
- rcp

（注） Kerberos クライアント サポートのシスコの実装は、MIT のコードから派生した CyberSafe が開発したコードに基づいています。そのため、シスコの Kerberos 実装は、CyberSafe Challenger 製の市販 Kerberos サーバおよび無料配布されている MIT のサーバ コードとの完全互換性テストに成功しています。

一般的な Kerberos 関連の用語と定義を下表に示します。

表 *1 : Kerberos* の用語

用語	定義
認証	ユーザやサービスが他のサービスに対して自分自身の身元を証明する手順。たとえば、クライアントがルータに対して認証したり、ルータが他のルータに対して認証したりすることができます。
許可	ネットワークまたはルータでユーザが持っている特権、および実行できるアクションをルータが判断する手段です。
クレデンシャル	認証チケット（チケット認可チケット（TGT）、サービス クレデンシャルなど）を表す総称。Kerberos クレデンシャルで、ユーザまたはサービスの ID を検証します。ネットワーク サービスがチケットを発行した Kerberos サーバを信頼することを決定すると、ユーザとパスワードを再入力する代わりにそのチケットを使用できます。クレデンシャルの有効期限は、8 時間がデフォルトの設定です。
インスタンス	Kerberos プリンシパルの承認レベル ラベル。ほとんどの Kerberos プリンシパルは、user@REALM という形式です（たとえば、smith@EXAMPLE.COM）。Kerberos インスタンスを指定した Kerberos プリンシパルは、user/instance@REALM という形式です（たとえば、smith/admin@EXAMPLE.COM）。Kerberos インスタンスは、認証が成功した場合のユーザーの承認レベルを指定するために使用できます。Kerberos インスタンスの認可マッピングを実装および実施するのは、各ネットワーク サービスのサーバ次第です。Kerberos レルム名は、大文字で指定する必要があります。
Kerberos 対応	Kerberos 証明書の基盤をサポートするように変更されたアプリケーションおよびサービス。

用語	定義
Kerberos レルム	Kerberos サーバーに登録されたユーザー、ホスト、およびネットワーク サービスで構成されるドメイン。Kerberos サーバーを信頼して、ユーザーまたはネットワーク サービスに対する別のユーザーまたはネットワーク サービスの ID を検証します。Kerberos レルムは、常に大文字にする必要があります。
Kerberos サーバ	ネットワーク ホスト上で稼働しているデーモン。ユーザーおよびネットワーク サービスはそれぞれ Kerberos サーバーに ID を登録します。ネットワーク サービスは Kerberos サーバーにクエリーを送信して、他のネットワーク サービスの認証を得ます。
キー発行局（KDC）	ネットワーク ホストで実行される Kerberos サーバとデータベース プログラム。
プリンシパル	Kerberos ID とも呼ばれ、Kerberos サーバに基づき、ユーザが誰であるか、サービスが何であるかを表します。
サービス認定証	ネットワーク サービスのクレデンシャル。この認定証は、KDC から発行されるとき、ネットワーク サービスと KDC で共有されるパスワード、およびユーザの TGT で暗号化されます。
SRVTAB	ネットワーク サービスが KDC と共有するパスワード。ネットワーク サービスは、SRVTAB（別名 KEYTAB）を使用することにより、暗号化されたサービス証明書を認証して解読します。
チケット認可チケット（TGT）	キー発行局（KDC）が認証済みユーザに発行する認定証。TGT を受け取ったユーザーは、KDC が示した Kerberos レルム内のネットワーク サービスに対して認証を得ることができます。

Kerberos クライアントのサポート操作

ここでは、Kerberos セキュリティ システムが、セキュリティ サーバとして機能する Cisco ルータと連携する方法について説明します。（便宜上または技術的な理由から）Kerberos は多様な方法でカスタマイズできますが、ネットワーク サービスにアクセスを試みるリモート ユーザは、3 レイヤのセキュリティを通過してからネットワーク サービスにアクセスする必要があります。

境界ルータに対する認証

ここでは、リモート ユーザがネットワークにアクセスを試みるときに通過する必要があるセキュリティの第 1 レイヤについて説明します。Kerberos 認証プロセスの第 1 段階は、ユーザが境界ルータに対して自身を認証することです。次のプロセスでは、ユーザが境界ルータに対して認証する方法について説明します。

1. リモート ユーザは、会社サイトのルータに対して PPP 接続を開きます。

2. ルータは、ユーザに対してユーザ名とパスワードの入力を求めます。
3. ルータは、そのユーザに関する KDC の TGT を要求します。
4. KDC は、（他の情報も含まれますが）ユーザの ID を含む暗号化済み TGT をルータに送信します。
5. ルータは、ユーザが入力したパスワードを使用して、TGT の復号化を試行します。復号化に成功すると、リモート ユーザはルータに対して認証されます。

PPP セッションの開始、および境界ルータに対する認証に成功するリモートユーザは、ファイアウォール内にいますが、ネットワーク サービスにアクセスするには KDC に対して直接認証する必要があります。これは、KDC から発行された TGT はルータに保存され、ユーザが物理的にルータにログインしない限り、追加の認証には役立ちません。

KDC からの TGT の取得

ここでは、境界ルータに対して認証されたリモート ユーザが、KDC に対して自身を認証する方法について説明します。

リモートユーザが境界ルータに対して認証すると、そのユーザは技術的にはネットワークの一部になります。つまり、ネットワークは、そのリモートユーザとユーザのマシンまたはネットワークを含むように拡張されます。ただし、リモート ユーザーがネットワーク サービスに対するアクセス権を得るには、KDC から TGT を取得する必要があります。次のプロセスでは、リモート ユーザーが KDC に対して認証する方法について説明します。

1. リモート サイトにあるワークステーションを使用するリモート ユーザーは、KINIT プログラム（Kerberos プロトコルに付属するクライアント ソフトウェアの一部）を起動します。
2. KINIT プログラムは、ユーザの ID を検索し、KDC から TGT を要求します。
3. KDC は TGT を作成します。TGT には、ユーザーの ID、KDC の ID、および TGT の有効期限が含まれます。
4. KDC は、ユーザーのパスワードをキーとして使用して、TGT を暗号化し、その TGT をワークステーションに送信します。
5. KINIT プログラムは暗号化された TGT を受信すると、ユーザーにパスワード（KDC でそのユーザー用に定義されているパスワード）の入力を求めます。
6. ユーザーが入力したパスワードを使用して KINIT プログラムが TGT を復号化できる場合、ユーザーは KDC に対して認証され、KINIT プログラムはユーザーの認定証キャッシュに TGT を保存します。

この時点で、ユーザーは TGT を持っており、KDC と安全に通信できます。その TGT を使用して、ユーザーは他のネットワーク サービスに対して認証できます。

ネットワーク サービスに対する認証の取得

次のプロセスでは、TGT を持つリモート ユーザーが、特定の Kerberos レルム内でネットワーク サービスに対して認証する方法について説明します。ここでは、ユーザーはリモート ワークステーション（Host A）上にあり、Host B にログインしようとしているとします。

1. Host A 上のユーザーは、Host B に対して Kerberos 化アプリケーション（Telnet など）を開始します。
2. Kerberos 化アプリケーションはサービス認定証要求を構築し、KDC に送信します。サービス認定証要求には、（他の情報も含まれますが）ユーザーの ID と目的のネットワーク サービスの ID が含まれます。TGT は、サービス認定証要求を暗号化するために使用されます。
3. KDC は、Host A 上のユーザーに対して発行された TGT を使用して、サービス認定証要求を復号化しようとします。KDC がパケットを復号化できる場合、要求の発行元が Host A 上の認証済みユーザーであると確認されます。
4. KDC は、サービス認定証要求に含まれるネットワーク サービス ID を記録します。
5. KDC は、Host A 上のユーザーの代理で、適切なネットワーク サービスのサービス認定証を Host B に構築します。サービス認定証には、クライアントの ID および必要なネットワーク サービスの ID が含まれます。
6. 次に、KDC はサービス認定証の暗号化を 2 回実行します。まず、認定証に指定されたネットワーク サービスと共有する SRVTAB を使用して認定証を暗号化します。次に、ユーザー（この場合は Host A 上のユーザー）の TGT を使用して結果のパケットを暗号化します。
7. KDC は、2 回暗号化された認定証を Host A に送信します。
8. Host A は、ユーザーの TGT を使用してサービス認定証の復号化を試行します。Host A がサービス認定証を復号化できる場合、その認定証の発行元が KDC であると確認されます。
9. Host A はサービス認定証を目的のネットワーク サービスに送信します。認定証は、まだ KDC とネットワーク サービスに共有されている SRVTAB で暗号化されています。
10. ネットワーク サービスは、SRVTAB を使用してサービス認定証の復号化を試行します。
11. ネットワーク サービスが認定証を復号化できる場合、その認定証の発行元が KDC であると確認されます。ネットワーク サービスは、ユーザーから間接的に送信されたデータでも、KDC から送信された復号化できるデータであれば、常に信頼します。これは、ユーザーがまず KDC で認証されているためです。

この時点で、ユーザーは Host B のネットワーク サービスに認証されます。このプロセスは、ユーザーが Kerberos レルムのネットワーク サービスにアクセスするときは毎回繰り返されます。

Kerberos を設定する方法

通信と相互認証を行う Kerberos レルムのホストと KDC について、相互に識別する必要があります。そのために、KDC 上の Kerberos データベースにホストのエントリを追加し、KDC が生成する SRVTAB ファイルを Kerberos レルムのすべてのホストに追加します。また、KDC データベースにユーザのエントリも作成します。

ここでは、Kerberos 認証済みのサーバ クライアント システムを設定する方法について説明します。内容は次のとおりです。

このセクションは、KDC 認識された UNIX ホストで Kerberos 管理プログラムをインストールし、データベースを初期化して、Kerberos レルム名とパスワードを選択していることを前提とします。これらのタスクの実行に関する手順については、Kerberos ソフトウェアに付属のマニュアルを参照してください。

（注） KDC のホスト名または IP アドレス、KDC で照会のために監視するポート番号、およびサービスを提供する Kerberos レルムの名前を書き留めます。この情報は、ルータの設定で必要になります。

Kerberos コマンドによる KDC の設定

Kerberos レルムで KDC として動作するようにホストを設定した後は、レルムのすべてのプリンシパルの KDC データベースに対してエントリを作成する必要があります。プリンシパルは、Cisco ルータおよびホスト上のネットワーク サービスの場合、またはユーザの場合があります。

Kerberos コマンドで KDC データベースにサービスを追加するには（また、既存のデータベース情報を変更するには）、以下の項のタスクを実行します。

（注） すべての Kerberos コマンド例は、オリジナルの MIT 実装の Kerberos 5 Beta 5 に基づいています。それよりも新しいバージョンでは、やや異なるインターフェイスを使用しています。

KDC データベースへのユーザーの追加

KDC にユーザーを追加し、そのユーザーの特権インスタンスを作成するには、KDC を実行するホストのルートになるために **su** コマンドを実行します。また、kdb5_edit プログラムを使用して、特権 EXEC モードで次のコマンドを使用します。

手順の概要

1. Router# **ank***username@REALM*
2. Router# **ank***username/instance@REALM*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router# **ank***username@REALM*	**ank**（新しいキーを追加）コマンドを使用して、ユーザーを KDC に追加します。このコマンドを実行するとパスワードの入力が求められ、ユーザはルータに対して認証するために入力する必要があります。
ステップ 2	Router# **ank***username/instance@REALM*	**ank** コマンドを使用して、ユーザの特権インスタンスを追加します。

次のタスク

たとえば、Kerberos レルム CISCO.COM のユーザ *loki* を追加するには、次の Kerberos コマンドを入力します。

```
ank loki@CISCO.COM
```

（注） Kerberos レルム名は、大文字で指定する必要があります。

ネットワーク管理がイネーブル レベルでルータに接続できるように、特権インスタンスを作成できます。たとえば、イネーブル モードを開始するためにクリア テキスト パスワードを入力する（またセキュリティを脅かす）必要がないようにできます。

新しい特権（この場合 enable ですが、任意に指定できます）を使用して *loki* のインスタンスを追加するには、次の Kerberos コマンドを入力します。

```
ank loki/enable@CISCO.COM
```

以下の各例では、パスワードの入力が求められます。このパスワードは、ユーザ *loki* がログイン時に使用できるように、ユーザに付与する必要があります。

「Kerberos インスタンス マッピングの有効化 （13 ページ）」では、Kerberos インスタンスを多様な Cisco IOS XE 特権レベルにマッピングする方法について説明します。

KDC での SRVTAB の作成

Kerberos プロトコルを使用するために認証するすべてのルータは、SRVTAB を持っている必要があります。SRVTAB の抽出の詳細については、「*SRVTAB* の抽出」を参照してください。

KDC に SRVTAB エントリを作成するには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
Router# **ark** *SERVICE/HOSTNAME@REALM*	**ark**（add random key）コマンドを使用して、ホストまたはルータがサポートするネットワークサービスを KDC に追加します。

たとえば、*router1* という Cisco ルータ用の Kerberos 化認証サービスを Kerberos レルム CISCO.COM に追加するには、次の Kerberos コマンドを入力します。

```
ark host/router1.cisco.com@CISCO.COM
```

すべての Kerberos 化ホスト上に、認証にこの KDC を使用するすべてのネットワーク サービスに関するエントリを作成します。

SRVTAB の抽出

SRVTAB には、（他の情報も含まれますが）KDC データベースに入力したサービス プリンシパルのパスワードまたはランダムに生成されたキーが含まれます。サービス プリンシパル キーは、そのサービスを実行するホストと共有する必要があります。そのためには、SRVTAB をファイルに保存し、Kerberos レルムにあるルータおよびすべてのホストにそのファイルをコピーします。SRVTAB エントリをファイルに保存することを、SRVTAB の抽出といいます。SRVTAB を抽出するには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
`Router# xst router-name host`	kdb5_edit コマンド **xst** を使用して、SRVTAB エントリをファイルに書き込みます。

たとえば、host/router1.cisco.com@CISCO.COM SRVTAB をファイルに書き込むには、次の Kerberos コマンドを入力します。

```
xst router1.cisco.com@CISCO.COM host
```

quit コマンドを使用して、kdb5_edit プログラムを終了します。

Kerberos プロトコルを使用するルータの設定

Kerberos レルムの定義

ルータが、Kerberos データベースに定義されているユーザを認証するには、KDC を実行するホストのホスト名または IP アドレスと Kerberos レルムの名前を知っている必要があります。また、オプションで、ホスト名またはドメイン ネーム システム（DNS）ドメインを Kerberos レルムにマッピングする機能がルータに必要です。

特定の Kerberos レルムで、指定した KDC に対して認証するようにルータを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。DNS ドメイン名の先頭にはドット（.）を付ける必要があります。

手順の概要

1. Router(config)# **kerberos local-realm***kerberos-realm*
2. Router(config)# **kerberos server***kerberos-realm* {*hostname* | *ip-address* } [*port-number*]
3. Router(config)# **kerberos realm** {*dns-domain* | *host* } *kerberos-realm*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router(config)# **kerberos local-realm***kerberos-realm*	ルータのデフォルト レルムを定義します。
ステップ 2	Router(config)# **kerberos server***kerberos-realm* {*hostname* | *ip-address* } [*port-number*]	特定の Kerberos レルムで使用する KDC、およびオプションで KDC が監視するポート番号をルータに指定します（デフォルト値は 88 です）。
ステップ 3	Router(config)# **kerberos realm** {*dns-domain* | *host* } *kerberos-realm*	（任意）ホスト名または DNS ドメインを Kerberos レルムにマッピングします。

次のタスク

（注） KDC を実行するマシンおよびすべての Kerberos 化ホストは 5 分の期限内で通信する必要があり、通信できない場合、認証は失敗します。そのため、すべての Kerberos 化マシン（特に KDC）は、ネットワーク タイム プロトコル（NTP）を実行する必要があります。

kerberos local-realm、**kerberos realm**、および **kerberos server** コマンドは、UNIX krb.conf ファイルに相当します。下記の表は、Cisco IOS XE コンフィギュレーション コマンドから Kerberos 5 コンフィギュレーション ファイル（krb5.conf）への対応一覧です。

表 *2 : Kerberos 5* のコンフィギュレーション ファイルおよびコマンド

krb5.conf ファイル	**Cisco IOS XE のコンフィギュレーション コマンド**
[libdefaults] `default_realm = DOMAIN.COM`	（コンフィギュレーション モードで） **kerberos local-realm** *DOMAIN.COM*

[domain_realm]
 	
`.domain.com = DOMAIN.COM`
 	
`domain.com = DOMAIN.COM`
	（コンフィギュレーション モードで）
	
	kerberos realm
	.domain.com
	DOMAIN.COM
	kerberos realm
	domain.com DOMAIN.COM

[realms]
 	
`kdc = DOMAIN.PIL.COM:750`
 	
`admin_server = DOMAIN.PIL.COM`
 	
`default_domain = DOMAIN.COM`
	（コンフィギュレーション モードで）
	
	kerberos server
	DOMAIN.COM 172.65.44.2
	(*172.65.44.2*
	is the example IP address for *DOMAIN.PIL.COM*
	)

Kerberos レルムの定義例については、Kerberos レルムの定義例のモジュールを参照してください。

SRVTAB ファイルのコピー

リモートユーザが Kerberos 認定証を使用してルータに対して認証できるようにするには、ルータが KDC 秘密キーを共有する必要があります。そのためには、KDC で抽出した SRVTAB をルータにコピーする必要があります。

SRVTAB ファイルを Kerberos レルムのホストにコピーする最もセキュアな方式は、ファイルを物理メディアにコピーし、各ホストの場所に行き、そのシステムに手動でファイルをコピーすることです。ルータに物理メディア ドライバがない場合、SRVTAB ファイルをルータにコピーするには、TFTP を使用してネットワークを介して転送する必要があります。

KDC からルータに対して SRVTAB ファイルをリモート コピーするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# kerberos srvtab remote {hostname | ip-address} {filename}`	KDC から SRVTAB ファイルを取得します。

SRVTAB ファイルをルータから KDC にコピーする場合、**kerberos srvtab remote** コマンドでこのファイルの情報を解析し、**kerberos srvtab entry** 形式でルータの実行コンフィギュレーションに保存します。ルータをリブートしたときに SRVTAB が使用できるようにするには（KDC から取得する必要はありません）、**write memory** コンフィギュレーション コマンドを使用し、実行コンフィギュレーション（解析した SRVTAB ファイルを含みます）を NVRAM に書き込みます。

SRVTAB ファイルのコピー例については、「SRVTAB ファイルのコピー例 （14 ページ）」を参照してください。

Kerberos 認証の指定

これまでの操作でルータの Kerberos の設定が完了しました。そのため、ルータは Kerberos を使用して認証できます。次の手順は、認証するようにルータに指示することです。AAA によって Kerberos 認証が容易になるため、**aaa authentication** コマンドを入力し、認証方式として Kerberos を指定する必要があります。詳細については、「認証の設定」の章を参照してください。

認定証転送の有効化

これまでの手順で Kerberos を設定すると、Kerberos 化ルータに対して認証されているユーザは TGT を持ち、その TGT を使用してネットワーク上のホストに対して認証できます。ただし、ユーザがホストの認証後に認定証のリストを表示しようとすると、出力には Kerberos 認定証が表示されません。

Kerberos 化された Telnet、rcp、rsh、および rlogin（適切なフラグ付き）を使用するときに、ルータからネットワーク上の Kerberos 化リモート ホストに対して認証する場合、オプションで、ユーザの TGT を転送するようにルータを設定できます。

Kerberos レルムで他のホストに接続するときにユーザーの認定証を転送するように、すべてのクライアントに強制するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# kerberos credentials forward`	Kerberos 認証に成功したときに、すべてのクライアントがユーザーの認定証を転送するように強制します。

認定証の転送を有効にすると、ユーザーの TGT は、認証を受ける次のホストへ自動的に転送されます。この方法で、ユーザーはKerberos レルム内の複数のホストに接続できます。新しい TGT を取得するたびに KINIT プログラムを実行する必要はありません。

ルータに対する Telnet セッションの開始

ネットワーク内からルータに対して Telnet セッションを開始するユーザを認証するために、Kerberos を使用するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# aaa authentication login {default | list-name } krb5_telnet`	Telnet を使用してルータに接続する場合、ログイン認証を設定して Kerberos 5 Telnet 認証プロトコルを使用します。

ルータに対する Telnetセッションは認証されますが、イネーブル モードを開始するには、ユーザがクリア テキスト パスワードを入力する必要があります。後述する **kerberos instance map** コマンドを使用すると、事前に定義した特権レベルでルータに対して認証できます。

暗号化された Kerberos 対応 Telnet セッションの確立

ユーザーがセキュア Telnetセッションを開始するもう 1 つの方法は、Encrypted Kerberized Telnet を使用することです。Encrypted Kerberized Telnet を使用すると、Telnet セッションを確立する前に、ユーザーは Kerberos 認定証によって認証されます。Telnet セッションは、64-bit Cipher Feedback（CFB）による 56-bit データ暗号規格（DES）暗号を使用して暗号化されます。送受信データは暗号化され、クリア テキストではないため、着信したルータまたはアクセス サーバの整合性は制御しやすくなります。

（注） この機能を使用できるのは、56-bit暗号化イメージを持っている場合だけです。56 ビット DES 暗号化は、米国政府の輸出管理規制の対象となります。

ルータからリモート ホストに対して、Encrypted Kerberized Telnet セッションを確立するには、EXEC コンフィギュレーション モードで次のコマンドのいずれかを使用します。

コマンド	目的

`Router(config)# connect host [port] /encrypt kerberos`
 	
または
 	
`Router(config)# telnet host [port] /encrypt kerberos`
	暗号化された Telnet セッションを確立します。

ユーザが Cisco ルータからリモート ホストに対する Telnet セッションを開始すると、ルータとリモートホストは、Kerberos 認定証を使用してユーザを認証するためにネゴシエートします。この認証に成功すると、ルータとリモートホストは、暗号化を使用するかどうかをネゴシエートします。このネゴシエーションに成功すると、着信および発信トラフィックは、64-bit CFB による 56-bit DES を使用して暗号化されます。

ユーザが、リモート ホストから Kerberos 認証用に設定された Cisco ルータに対してダイヤルインすると、Telnet セッションに暗号化を使用するかどうかについて、ホストとルータでネゴシエーションが試行されます。このネゴシエーションに成功すると、ルータは Telnet セッション中のすべての発信データを暗号化します。

暗号化のネゴシエーションに成功しなかった場合、セッションは終了し、ユーザは、暗号化された Telnet セッションの確立に失敗したというメッセージを受信します。

リモート ホストから双方向暗号化をイネーブル化する方法については、リモート ホスト デバイスのマニュアルを参照してください。

暗号化された Kerberos 対応 Telnet を使用してセキュアな Telnet セッションを開始する例については、この章で後述する「暗号化された Telnet セッションの例 （15 ページ）」を参照してください。

必須の Kerberos 認証の有効化

セキュリティの追加レイヤとして、リモートユーザがルータに対して認証した後に、ユーザは Kerberos 化 Telnet、rlogin、rsh、および rcp だけを使用してネットワーク上の他のサービスに対して認証できます。Kerberos 認証を必須にしていない状態で Kerberos 認証に失敗すると、アプリケーションは、そのネットワーク サービスのデフォルト認証方式を使用して、ユーザーの認証を試行します。たとえば、Telnet および rlogin はパスワードの入力を求め、rsh はローカル rhost ファイルを使用して認証を試行します。

Kerberos 認証を必須にするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# kerberos clients mandatory`	リモート ホストとの間で Kerberos プロトコルをネゴシエートできない場合、Telnet、rlogin、rsh、および rcp を失敗に設定します。

Kerberos インスタンス マッピングの有効化

「KDC での SRVTAB の作成 （7 ページ）」で説明したように、KDC データベースにユーザの管理インスタンスを作成することができます。**kerberos instance map** コマンドを使用すると、その管理インスタンスを Cisco IOS XE 特権レベルにマッピングできます。それによって、事前定義した特権レベルで、ユーザーはルータに対するセキュア Telnet セッションを開くことができます。イネーブルモードを開始するためにクリアテキストのパスワードを入力する必要はありません。

Kerberos インスタンスを Cisco IOS XE 特権レベルにマッピングするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# kerberos instance map` *instance privilege-level*	Kerberos インスタンスを Cisco IOS XE 特権レベルにマッピングします。

KDC データベースにユーザ *loki*（たとえば、*loki/admin*）の Kerberos インスタンスがある場合、ユーザ *loki* は、loki/admin としてルータに対して Telnet セッションを開始し、特権レベル 15 で自動的に認証します。インスタンス「admin」は特権レベル 15 にマッピングされるという前提です。（ルータに対する Telnet セッションの開始 （11 ページ）を参照してください。）

Cisco IOS XE コマンドは、 **privilege level** コマンドを使用して、さまざまな権限レベルに設定できます。

Kerberos インスタンスを Cisco IOS XE 権限レベルにマッピングした後、ユーザーがログインするたびに Kerberos インスタンスをチェックするようにルータを設定する必要があります。マッピングされた Kerberos インスタンスに基づいて、ユーザーに EXEC シェルの実行を許可するかどうかを決定するための承認を実行するには、**krb5-instance** キーワードを指定して **aaa authorization** コマンドを使用します。詳細については、「認可の設定」の章を参照してください。

Kerberos の監視とメンテナンス

現在のユーザの認定証を表示または削除するには、EXEC モードで次のコマンドを使用します。

手順の概要

1. Router# **show kerberos creds**
2. Router# **clear kerberos creds**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router# **show kerberos creds**	現在のユーザの認定証キャッシュに含まれる認定証を一覧表示します。
ステップ 2	Router# **clear kerberos creds**	転送済みの認定証を含め、現在のユーザの認定証キャッシュに含まれるすべての認定証を破棄します。

Kerberos 設定の例

Kerberos レルムの定義例

デフォルトの Kerberos レルムとして CISCO.COM を定義するには、次のコマンドを使用します。

```
kerberos local-realm CISCO.COM
```

CISCO.COM KDC が、ホスト 10.2.3.4 でポート番号 170 を使用して実行されていることをルータに示すには、次の Kerberos コマンドを使用します。

```
kerberos server CISCO.COM 10.2.3.4 170
```

DNS ドメイン cisco.com を Kerberos レルム CISCO.COM にマッピングするには、次のコマンドを使用します。

```
kerberos realm.cisco.com CISCO.COM
```

SRVTAB ファイルのコピー例

host123.cisco.com というホスト上の SRVTAB ファイルを、router1.cisco.com というルータにコピーするには、次のようなコマンドを使用します。

```
kerberos srvtab remote host123.cisco.com router1.cisco.com-new-srvtab
Valid Starting          Expires                 Service Principal
13-May-1996 14:59:44    13-May-1996 23:00:45    krbtgt/CISCO.COM@CISCO.COM
chet-2500# show privilege
Current privilege level is 15
chet-2500# q
Connection closed by foreign host.
chet-ss20% telnet chet-2500
Trying 172.16.0.0 ...
Connected to chet-2500.cisco.com.
Escape character is '^]'.
User Access Verification
Username: chet/restricted
Password:
```

```
chet-2500# show kerberos creds
Default Principal:  chet/restricted@CISCO.COM
Valid Starting          Expires                 Service Principal
13-May-1996 15:00:32    13-May-1996 23:01:33    krbtgt/CISCO.COM@CISCO.COM
chet-2500# show privilege
Current privilege level is 3
chet-2500# q
Connection closed by foreign host.
chet-ss20%
```

暗号化された Telnet セッションの例

ルータから「host1」というリモート ホストに対して、暗号化された Telnet セッションを確立する例を示します。

Router> **telnet host1 /encrypt kerberos**

その他の参考資料

次の項では、No Service Password-Recovery 機能の関連資料を示します。

関連資料

関連項目	マニュアル タイトル
パスワードの設定、変更および忘失パスワードの回復	「Configuring Security with Passwords, Privilege Levels and, Login Usernames for CLI Sessions on Networking Devices」機能モジュール
システム イメージのロードと再起動	「Using the Cisco IOS Integrated File System」機能モジュール
セキュリティ コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上の注意事項、および例	『*Cisco IOS Security Command Reference*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

標準

標準	タイトル
なし	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、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
この機能でサポートが追加または変更された RFC はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Kerberos の設定に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *3 : Kerberos* の設定に関する機能情報

機能名	リリース	機能情報
暗号化された Kerberos 対応 Telnet	Cisco IOS XE Release 2.1	Encrypted Kerberized Telnet を使用すると、Telnet セッションを確立する前に、ユーザーは Kerberos 認定証によって認証されます。Telnet セッションは、64-bit Cipher Feedback（CFB）による 56-bit データ暗号規格（DES）暗号を使用して暗号化されます。送受信データは暗号化され、クリア テキストではないため、着信したルータまたはアクセス サーバの整合性は制御しやすくなります。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 次のコマンドが導入または変更されました。**connect** および **telnet**。
Kerberos V クライアントのサポート	Cisco IOS XE Release 2.1	Kerberos 5 のサポートでは、Kerberos 5 をすでに配置している組織は、ルータ上で、他のネットワーク ホスト（UNIX サーバや PC など）ですでに使用している同じ Kerberos 認証データベースを使用できます。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。