



Kerberos の設定

- [Kerberos によるスイッチ アクセスの制御の前提条件 \(1 ページ\)](#)
- [Kerberos に関する情報 \(1 ページ\)](#)
- [Kerberos を設定する方法 \(6 ページ\)](#)
- [Kerberos 設定の監視 \(6 ページ\)](#)
- [その他の参考資料 \(6 ページ\)](#)

Kerberos によるスイッチ アクセスの制御の前提条件

次に、Kerberos を使用してスイッチ アクセスを制御するための前提条件を示します。

- リモート ユーザがネットワーク サービスに対して認証を得るには、Kerberos レルム内のホストと KDC を設定し、ユーザとネットワーク サービスの両方に通信を行い、相互に認証させる必要があります。これを実現するには、互いの識別が必要です。KDC 上の Kerberos データベースにホストのエントリを追加し、Kerberos レルム内のすべてのホストに KDC が生成した KEYTAB ファイルを追加します。また、KDC データベースにユーザ用のエントリも作成します。
- Kerberos サーバには、ネットワーク セキュリティサーバとして設定されていて、Kerberos プロトコルを用いてユーザを認証できるスイッチを使用できます。

ホストおよびユーザのエントリを追加または作成する場合の注意事項は次のとおりです。

- Kerberos プリンシパル名はすべて小文字でなければなりません。
- Kerberos インスタンス名はすべて小文字でなければなりません。
- Kerberos レルム名はすべて大文字でなければなりません。

Kerberos に関する情報

ここでは、Kerberos の情報を提供します。

Kerberos とスイッチ アクセス

ここでは、Kerberos セキュリティ システムをイネーブルにして設定する方法について説明します。Kerberos セキュリティ システムは、信頼できるサードパーティを使用してネットワーク リソースに対する要求を認証します。



- (注) Kerberos の設定例では、信頼できるサードパーティを、Kerberos をサポートし、ネットワーク セキュリティ サーバとして設定され、Kerberos プロトコルを使用してユーザを認証するスイッチとすることができます。

Kerberos の概要

Kerberos はマサチューセッツ工科大学 (MIT) が開発した秘密キーによるネットワーク 認証 プロトコルです。データ暗号規格 (DES) という暗号化アルゴリズムを暗号化と認証に使用し、ネットワーク リソースに対する要求を認証します。Kerberos は、信頼できるサードパーティという概念を使ってユーザとサービスに対してセキュリティの検証を実行します。この信頼できるサードパーティをキー発行局 (KDC) と呼びます。

Kerberos は、ユーザが誰であるか、そのユーザが使用しているネットワーク サービスは何であるかを検証します。これを実行するために、KDC (つまり信頼できる Kerberos サーバ) がユーザにチケットを発行します。これらのチケットには有効期限があり、ユーザ クレデンシャルのキャッシュに保存されます。Kerberos サーバは、ユーザ名やパスワードの代わりにチケットを使ってユーザとネットワーク サービスを認証します。



- (注) Kerberos サーバには、ネットワーク セキュリティ サーバとして設定されていて、Kerberos プロトコルを用いてユーザを認証できるのであれば、どのスイッチも使用できます。

Kerberos のクレデンシャル発行スキームでは、*single logon* という手順を使用します。この手順では、ユーザを 1 回認証すると、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。

このソフトウェア リリースは Kerberos 5 に対応しています。Kerberos 5 では、すでに Kerberos 5 を使用している組織が、(UNIX サーバや PC などの) 他のネットワーク ホストが使用している KDC 上の Kerberos 認証データベースを使用できます。

Kerberos は次のネットワーク サービスをサポートしています。

- Telnet
- rlogin
- rsh

次の表に、一般的な Kerberos 関連用語とその定義を示します。

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、クライアントはスイッチに対して認証を得て、スイッチは他のスイッチに対して認証を得ます。
許可	ユーザがネットワークやスイッチにおいてどのような権限を有しており、またどのような動作を実行できるかを、スイッチが識別する手段
クレデンシヤル	認証チケット (TSG ¹ 、サービスクレデンシヤルなど) を表す総称。Kerberos クレデンシヤルで、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にした場合、ユーザ名やパスワードを再入力する代わりにこれを使用できます。証明書の有効期限は、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、 <code>user@REALM</code> という形式です (たとえば、 <code>smith@EXAMPLE.COM</code>)。Kerberos インスタンスのある Kerberos プリンシパルは、 <code>user/instance@REALM</code> という形式です (たとえば、 <code>smith/admin@EXAMPLE.COM</code>)。Kerberos インスタンスは、認証が成功した場合のユーザの承認レベルを指定するために使用できます。各ネットワーク サービスのサーバは、Kerberos インスタンスの許可マッピングを適用し実行できますが、必須ではありません。 (注) Kerberos プリンシパル名およびインスタンス名はすべて小文字でなければなりません。 (注) Kerberos レルム名はすべて大文字でなければなりません。
KDC ²	ネットワーク ホストで稼働する Kerberos サーバおよびデータベースプログラムで構成されるキー発行局
Kerberos 対応	Kerberos クレデンシヤルのインフラストラクチャをサポートするために変更されたアプリケーションやサービスのことを指す用語
Kerberos レルム	Kerberos サーバに登録されたユーザ、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 サーバを信頼して、ユーザまたはネットワーク サービスに対する別のユーザまたはネットワーク サービスの ID を検証します。 (注) Kerberos レルム名はすべて大文字でなければなりません。

用語	定義
Kerberos サーバ	ネットワーク ホストで稼働しているデーモン。ユーザおよびネットワーク サービスはそれぞれ Kerberos サーバに ID を登録します。ネットワーク サービスは Kerberos サーバ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。
KEYTAB ³	ネットワーク サービスが KDC と共有するパスワード。Kerberos 5 以降のバージョンでは、ネットワーク サービスは KEYTAB を使って暗号化されたサービス クレデンシヤルを暗号解除して認証します。Kerberos 5 よりも前のバージョンでは、KEYTAB は SRVTAB ⁴ と呼ばれます。
プリンシパル	Kerberos ID と呼ばれ、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。 (注) Kerberos プリンシパル名はすべて小文字でなければなりません。
サービス クレデンシヤル	ネットワーク サービスのクレデンシヤル。KDC からクレデンシヤルが発行されると、ネットワーク サービスと KDC が共有するパスワードで暗号化されます。ユーザ TGT ともパスワードを共有します。
SRVTAB	ネットワーク サービスが KDC と共有するパスワード。SRVTAB は、Kerberos 5 以降のバージョンでは KEYTAB と呼ばれています。
TGT	身分証明書のこと、KDC が認証済みユーザに発行するクレデンシヤル。TGT を受け取ったユーザは、KDC が示した Kerberos レalm 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。

¹ チケット認可チケット

² キー発行局

³ キー テーブル

⁴ サーバテーブル

Kerberos の動作

リモートユーザが **device** を Kerberos サーバとして使用してネットワークサービスで認証されるには、次の手順を実行する必要があります。Kerberos をカスタマイズする方法はいくつかありますが、ネットワークサービスにアクセスしようとするリモートユーザは、3つのセキュリティレイヤを通過しないとネットワークサービスにアクセスできません。

リモートユーザが **device** を Kerberos サーバとして使用してネットワークサービスで認証されるには、次の手順を実行する必要があります。

境界スイッチに対する認証の取得

ここでは、リモート ユーザが通過しなければならない最初のセキュリティ レイヤについて説明します。ユーザは、まず境界スイッチに対して認証を得なければなりません。リモート ユーザが境界スイッチに対して認証を得る場合、次のプロセスが発生します。

1. ユーザが境界スイッチに対して、Kerberos 未対応の Telnet 接続を開始します。
2. ユーザ名とパスワードの入力を求めるプロンプトをスイッチが表示します。
3. スイッチが、このユーザの TGT を KDC に要求します。
4. KDC がユーザ ID を含む暗号化された TGT をスイッチに送信します。
5. スイッチは、ユーザが入力したパスワードを使って TGT の暗号解除を試行します。
 - 暗号解除に成功した場合は、ユーザはスイッチに対して認証を得ます。
 - 暗号解除に成功しない場合は、ユーザ名とパスワードを再入力 (Caps Lock または Num Lock のオン/オフに注意) するか、別のユーザ名とパスワードを入力してステップ 2 の手順を繰り返します。

Kerberos 未対応の Telnet セッションを開始し、境界スイッチの認証を得ているリモート ユーザはファイアウォールの内側にいますが、ネットワーク サービスにアクセスするには、KDC から直接認証を得る必要があります。ユーザが KDC から認証を得なければならないのは、KDC が発行する TGT はスイッチに保存されており、ユーザがこのスイッチにログオンしないかぎり、追加の認証に使用できないからです。

KDC からの TGT の取得

ここでは、リモート ユーザが通過しなければならない 2 番目のセキュリティ レイヤについて説明します。ユーザは、ネットワーク サービスにアクセスするために、このレイヤで KDC の認証を得て、KDC から TGT を取得しなければなりません。

KDC に対して認証を得る方法については、『*Cisco IOS Security Configuration Guide, Release 12.4*』の「Security Server Protocols」の章にある「Obtaining a TGT from a KDC」を参照してください。

ネットワーク サービスに対する認証の取得

ここでは、リモート ユーザが通過しなければならない 3 番目のセキュリティ レイヤについて説明します。TGT を取得したユーザは、このレイヤで Kerberos レルム内のネットワーク サービスに対して認証を得なければなりません。

ネットワーク サービスに対して認証を得る方法については、『*Cisco IOS Security Configuration Guide, Release 12.4*』の「Security Server Protocols」の章の「Authenticating to Network Services」を参照してください。

Kerberos を設定する方法

Kerberos 認証済みサーバ/クライアント システムを設定する手順は、次のとおりです。

- Kerberos コマンドを使用して KDC を設定します。
- Kerberos プロトコルを使用するようにスイッチを設定します。

Kerberos 設定の監視

Kerberos 設定を表示するには、次のコマンドを使用します。

- **show running-config**
- **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。
- **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。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Kerberos コマンド	『Cisco IOS Security Command Reference』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィ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

シスコのテクニカル サポート

説明	リンク
<p>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。</p> <p>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。</p> <p>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。</p>	<p>https://www.cisco.com/c/ja_jp/support/index.html</p>

