Cisco機器 （ルータ/操作・設定・トラブル対応）

学習内容

1. 状態確認の基本 `show` コマンド
2. ルータの初期設定と基本操作
3. アクセス制御とパスワード設定
4. SSHによるセキュアなリモートアクセス
5. パスワードリカバリー手順

01

状態確認の基本`show`コマンド

show version コマンド

ルータのハードウェアやソフトウェアの基本情報を一度に確認するコマンドです

IOSバージョン	稼働時間 (Uptime)	メモリ容量
現在稼働しているCisco IOSのバージョンとフィーチャーセット	ルータが最後に起動してからの経過時間	搭載されているDRAMとフラッシュメモリのサイズ

CPU情報	インターフェース	コンフィグレーションレジスタ
ルータに搭載されているCPUのモデル名や情報	搭載されているインターフェースの種類と数	起動時の動作を決定する重要な値 (例: 0x2102)

show running-config コマンド

現在メモリ上で動作しているアクティブな設定内容をすべて表示します

ホスト名	パスワード設定	インターフェース設定
設定されているルータの識別名	各種パスワードの暗号化状態や設定内容	各ポートのIPアドレス、速度、Duplexなどの設定

ルーティング設定	アクセスリスト	Line設定 (VTY/Console)
スタティックルートやダイナミックルーティングプロトコルの設定	トラフィック制御のためのACL設定	リモートアクセスやコンソール接続のパスワード設定

show interfaces コマンド

インターフェースの物理的・論理的な状態やトラフィック統計を詳細に確認します

L1/L2ステータス

物理層とデータリンク層が正常か (up/down) を確認

IPアドレス/MACアドレス

設定されているIPアドレス、サブネットマスク、MACアドレスを表示

統計情報

送受信パケット数、エラー数、衝突数などの詳細なカウンタ

インターフェースの状態判断

show interfacesコマンドの出力1行目で、物理層とデータリンク層の状態が分かります

状態	物理層 (Interface is)	データリンク層 (Line protocol is)	原因の例
正常	up	up	正常に通信可能な状態
対向か設定の問題	up	down	**キープアライブの不一致**、カプセル化方式の違い、クロック設定ミス
物理的な問題	down	down	ケーブル未接続、対向機器の電源OFF、インターフェースの故障
手動で無効	administratively down	down	**shutdownコマンド**が設定されている (no shutdownで有効化)

02

ルータの初期設定と基本操作

インターフェースの基本設定手順

通信を行うためにインターフェースにIPアドレスを設定する一般的な流れです

1. グローバルコンフィグモードに移行する `configure terminal`
2. 対象のインターフェースを選択する `interface インターフェース名`
3. インターフェースに説明を追加する `description 説明文`
4. IPアドレスとサブネットマスクを設定する `ip address IPアドレス マスク`
5. インターフェースを有効化する `no shutdown`

管理を快適にする便利な設定

必須ではありませんが、設定しておくと管理や運用が格段に楽になるコマンドです

logging synchronous

コンソール入力中にログメッセージが表示されても、入力行が崩れるのを防ぐ

exec-timeout 0 0

コンソールやVTYセッションが、無操作でタイムアウトするのを無効化する

banner motd

ログイン前に警告などのメッセージを表示し、セキュリティ意識を高める

03

アクセス制御とパスワード設定

特権EXECモードへのパスワード設定

設定変更が可能な特権モードを保護するコマンドには2種類あり、secretが推奨されます

enable password	enable secret
パスワードが**平文**で保存される	パスワードが**暗号化**されて保存される
コンフィグを見られるとパスワードが分かってしまう	**セキュリティ性が高い**
暗号化強度が低い (復号可能)	両方設定されている場合、**secretが優先される**

パスワードの暗号化

`service password-encryption` コマンドで可読性のあるパスワードを保護します

このコマンドを実行すると、コンフィグ内の `enable password` や `line` パスワードなど、**平文で保存されている全てのパスワード**が簡易的に暗号化されます。

暗号化強度は高くないため、あくまで「ショルダーハック（覗き見）」対策程度のものと認識することが重要です。

一度暗号化したパスワードは、`no service password-encryption` を実行しても**元には戻りません**。

04

SSHによるセキュアなリモートアクセス

SSH設定の5ステップ

安全なリモートアクセスのために、以下の手順でSSHを有効化します

ホスト名とドメイン名	RSA暗号鍵の生成	ユーザ認証の設定	VTY回線の設定	SSH接続の許可
暗号鍵を生成するための前提条件として設定	`crypto key generate rsa`で暗号化の元となる鍵を作成	`username`コマンドでSSHログイン用のユーザとパスワードを作成	`login local`でローカルユーザ認証を有効化	`transport input ssh`でSSH接続のみを許可

SSH 試験対策ポイント

CCNAなどの試験で問われやすいSSH設定の要点をまとめました

必須コンポーネント

SSH有効化には**ホスト名、ドメイン名、RSA鍵**が最低限必要

認証方式

`login local` は、`username`コマンドで作成したローカルデータベースを参照する設定

プロトコル制限

`transport input ssh` を設定すると、**Telnetでの接続は拒否される**

05

パスワードリカバリー手順

パスワードリカバリーの基本概念

起動時に設定ファイル(startup-config)を意図的に読み込ませないことで、パスワードを回避します

ルータは通常、起動時にNVRAMにある `startup-config` を読み込み、`running-config` に反映させます。

パスワード情報も `startup-config` に含まれています。

そこで、**コンフィグレーションレジスタ**の値を変更し、`startup-config` を**無視して起動**させます。

これにより、パスワードが設定されていない状態で特権モードに入ることが可能になります。

パスワードリカバリーの具体的な手順

以下の手順に従って操作することで、忘れたパスワードを再設定できます

1. コンソール接続し、ルータを再起動。**Break信号**を送信してROMMONモードに入る
2. コンフィグレジスタを `0x2142` に変更 `confreg 0x2142`
3. `reset` コマンドでルータを再起動
4. 初期設定ダイアログを `Ctrl+C` でスキップし、`enable` で特権モードに入る
5. 元の設定をメモリに読み込む `copy startup-config running-config`
6. 新しいパスワードを設定する `enable secret 新パスワード`
7. 必要なインターフェースを有効化する `no shutdown`
8. コンフィグレジスタを通常値 `0x2102` に戻す `config-register 0x2102`
9. 最後に設定を保存する `copy running-config startup-config`