Telnet/SSH

学習内容

TelnetとSSHの仕組みを理解し、安全な遠隔操作の重要性を確認します

1. Telnetの概要と仕組み
2. SSH（Secure Shell）の概要と特徴
3. TelnetとSSHの決定的な違い
4. まとめと推奨事項

01

Chapter 1: Telnetの基本 — 暗号化されていない遠隔操作

Telnetの概要と仕組み

ネットワーク接続機器を遠隔操作するためのアプリケーション層プロトコル

ネットワークに接続された機器（サーバやルータなど）を遠隔操作する

利用には操作対象機器にTelnetサーバ機能が有効である必要がある

クライアント側から命令を入力し、サーバー側で処理した結果が返信される

接続時にはTCPの宛先ポート番号 **23番** が使用される

Telnetの最大の問題点：セキュリティリスク

平文（暗号化なし）での通信は盗聴の危険性を伴います

すべてのデータが平文

入力した**パスワード**を含め、通信内容全体が暗号化されずに送信される

盗聴の危険性

ネットワーク上でデータを傍受されると、機密情報が**容易に漏洩**するリスクがある

02

Chapter 2: SSHの基本 — 安全な遠隔操作

SSH（Secure SHell）の概要

通信内容を**暗号化**することで安全な遠隔操作を実現

暗号化通信

パスワードや操作内容を**暗号化**し、通信の安全性を確保する

推奨プロトコル

Ciscoなどのネットワーク機器管理で**現在最も推奨**されている

使用ポート

接続時にはTCPの宛先ポート番号 **22番** が使用される

認証とバージョン

SSH2のRSA公開鍵暗号認証が主流で、セキュリティが強化されている

TelnetとSSHの決定的な違い

セキュリティと使用ポート番号の違いを明確に理解する

Telnet		SSH
なし	通信の暗号化	あり
危険	セキュリティ	安全
23番	TCPポート番号	22番