# syslog

# 学習内容

1. syslogの概要と役割
2. ログの構成要素：FacilityとSeverity
3. Cisco機器におけるsyslogのデフォルト設定
4. 実務で推奨されるログ表示設定
5. 外部syslogサーバーへの送信設定
6. ログレベルの適切な運用方法

01

# syslogの概要と役割

# syslogとは：ログメッセージ転送の標準規格

障害の原因究明やセキュリティ監視に不可欠

syslogは、ネットワーク機器やサーバーが生成するログメッセージを転送するための**標準規格**

クライアント／サーバー型プロトコルであり、送信側（ルータ/スイッチ）から受信側（ログサーバー）へ**テキスト形式**でログを送信

メッセージは主にUDPまたはTCPの**ポート番号514**を使用して送信される

機器の動作状況を把握し、**トラブルシューティング**や**セキュリティ監視**に役立つ

# syslogメッセージの構成要素

FacilityとSeverityの組み合わせでログを識別

| Facility（ログの出力元） |
| --- |
| auth, authpriv: 認証サービス |
| daemon: 各種デーモン |
| kern: カーネル |
| mail: メールシステム |
| local0〜7: 独自利用可能 |

| Severity（重要度・優先度） |
| --- |
| 0: emerg（システム停止レベル） |
| 3: err（一般的なエラー） |
| 5: notice（重要な通知） |
| 7: debug（デバッグ情報） |

# Severityレベルと意味（Cisco定義を含む）

数値が小さいほど深刻度が高い

| Level | キーワード (Cisco) | 数値 | 説明 |
|---|---|---|---|
| emerg | emergencies | 0 | システム停止レベル、非常に危険な状態 |
| alert | alerts | 1 | 危険な状態、即時対応が必要 |
| crit | critical | 2 | 重大な障害、クリティカル状態 |
| err | errors | 3 | 一般的なエラー |
| warning | warnings | 4 | 警告 |
| notice | notifications | 5 | 重要な通知（注意すべき情報） |
| info | informational | 6 | 情報メッセージ |
| debug | debugging | 7 | デバッグ情報 |

02

# Cisco機器におけるデフォルト設定と推奨設定

# Cisco syslogデフォルト値と実運用での課題

デフォルト設定のままでは運用上不十分

| デフォルト値（課題あり） | 実運用での推奨対応 |
| --- | --- |
| ログバッファサイズ: 4096バイト（非常に小さい） | ログバッファを512000バイト等に拡張 |
| タイムスタンプ: **無効** | タイムスタンプとタイムゾーンを**有効化** |
| 同期ロギング: 無効 | ロギング同期化（`logging synchronous`）を有効化 |
| syslogサーバ利用: 無効 | ログサーバーのIPアドレスを明示的に指定 |
| syslogサーバ送信レベル: informational（ログが多い） | 運用に合わせたトラップレベルを設定（例: `notifications`） |

# 分かりやすいログ表示のための推奨設定

タイムスタンプと通し番号で解析を容易に

**時刻同期とタイムスタンプ**

`service timestamps` コマンドでログに**ミリ秒・タイムゾーン付き**時刻を付与。NTP設定も必須

**ログ通し番号の付与**

`service sequence-numbers` でログに通し番号を付与し、ログ欠損や順序の調査に役立てる

**同期ロギングの有効化**

`logging synchronous` コマンドで**作業中のログ割り込み**を防ぎ、設定変更時の視認性を向上させる

# 外部syslogサーバーへの送信設定ステップ

Cisco推奨の設定値とFacilityの指定

1. 内部ログバッファを拡張: `logging buffered 512000`（デフォルト4096から拡張）
2. syslogサーバーのIPアドレスを指定: `logging host 192.168.10.100`
3. 送信するログの最小レベルを指定: `logging trap informational`（level 6以上が対象）
4. 送信時のFacilityを指定: `logging facility local5`（サーバー管理者と連携し、識別しやすい番号を選択）
5. インターフェースリンクステータスの明示的設定: `logging event link-status`

# 適切なログレベル運用の目安

ログレベルを絞り込み、必要な情報のみを収集する

| 通常運用時 | 広域のシステム監視 | 障害調査時（一時的） | 最低限のセキュリティ |
| --- | --- | --- | --- |
| **notifications** | **informational** | **debugging** | **critical** |
| Level 5 | Level 6 | Level 7 | Level 2 |