株式会社ケイ・シー・シー

Linux Professional Institute Japan LPI-JAPAN

LPICレベル3　301技術解説無料セミナー

2011/12/18

株式会社ケイ・シー・シー
ソリューションセンターユニット　ITラーニングセンター
村田　一雄

講師プロフィール

■会社概要

株式会社ケイ・シー・シー

http://www.kcc.co.jp/

■講師紹介

ソリューションセンターユニット　ITラーニングセンター所属

Linuxをメインにネットワーク・セキュリティ・XML・資格取得講座など
様々な技術研修を担当

Linux Professional Institute

アウトライン

1. LPIC レベル3　試験概要
   - LPIC試験概要
   - Linux学習環境の構築
   - 学習方法

2. 技術解説項目
   - 主題301　概念とアーキテクチャおよび設計
   - 主題304　使用法
   - 主題305　統合と移行
   - 主題306　キャパシティプランニング

LPICレベル3　試験概要

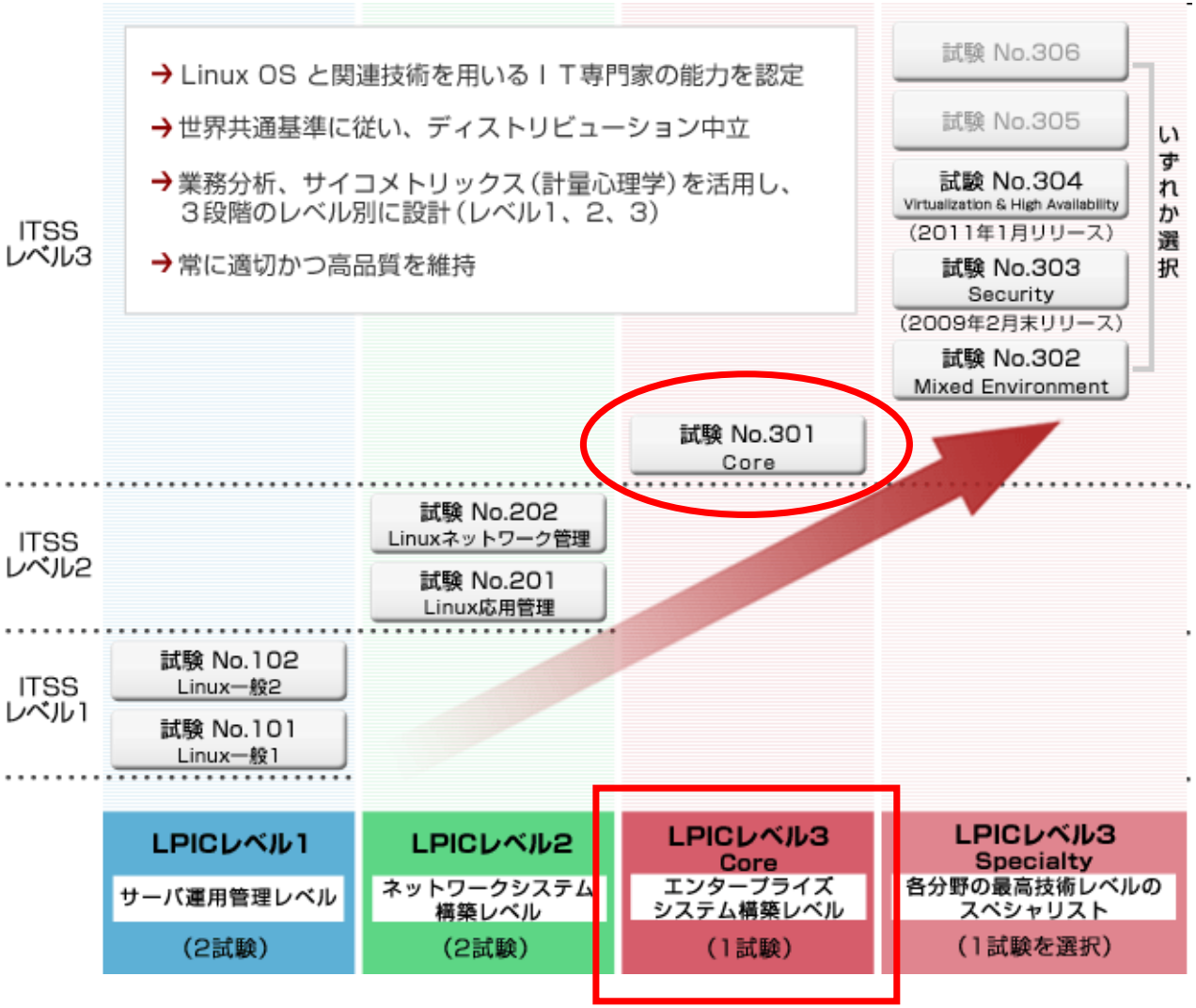
Linux技術者認定試験(LPIC)の特長

株式会社ケイ・シー・シー

- グローバルな認定制度
  - Linuxスキルが全世界で認定される
- ベンダニュートラル
  - どのようなLinux環境でもスキルを活用できる
- 世界最大規模
  - Linux認定資格としては世界最大規模

Linux Professional Institute

LPIC試験の構成



Linux Professional Institute

LPICレベル3 301Core 試験概要

■高負荷に耐えうる大規模システムの構築が行えるプロフェッショナルとして認定

- エンタープライズレベルのシステムを考慮したLinux環境のシステム計画、設計、構築、実装ができる
- Linux環境のキャパシティプランニングを行い、リソース問題のトラブルシューティングができる

■レベル3 Coreの認定基準

- レベル2に認定されており、かつ、301Core試験に合格すると「LPICレベル3 301Core」に認定される

Linux Professional Institute

301Core試験の出題範囲

- 主題301:　概念、アーキテクチャおよび設計
- 主題302:　インストールおよび開発
- 主題303:　設定
- 主題304:　使用法
- 主題305:　統合と移行
- 主題306:　キャパシティプランニング

Linux学習環境の構築

株式会社ケイ・シー・シー

■インターネットをフルに活用
- 関連キーワードで分からないものはとにかく調べる
- 信頼できる「お気に入りサイト」を見つけておく
  - JM Project, Linux JF Project, @ITなど

■実機を使った学習
- コマンドは実機で実行してみる
- manを活用する

■学習環境の構築
- 無償ディストリビューション(CentOS, Fedora, Ubuntu等)を利用
- Linux専用マシンがあればベスト
- VM環境の構築を検討
  - VMWare Server / Playerなど無償仮想化ツールの導入

Linux Professional Institute

LPIC試験　傾向と対策

株式会社ケイ・シー・シー

■幅広い出題範囲

- 出題範囲詳細をもとにして、すべて網羅する
- 得意分野をつくる

■実務に則した問題

- 参考書だけの勉強ではなく、実機で確認する
- コマンドの出力結果やエラーメッセージをしっかり把握する
- 重要な設定ファイルは主な設定項目（パラメータ）も覚える

Linux Professional Institute

LPIC試験　傾向と対策

株式会社ケイ・シー・シー

CBT(Computer Based Testing)試験

- コンピュータを操作して問題に解答
- 試験中、問題は何度も繰り返し参照可能
- 試験終了と同時に結果が判明

試験時間の有効活用

- 90分で60問の問題
- 四者択一または五者択一、複数選択、記入式の3パターン
  - 問題はしっかり読む
  - 択一問題は迅速に解答し、時間を確保する
  - あやふやな問題はチェックをつけて、後から解答する
  - 全体的に見直す時間を確保する

Linux Professional Institute

LPICレベル3　技術解説

主題301　概念とアーキテクチャおよび設計

301.1 LDAPの概念とアーキテクチャ	重要度3
301.2 ディレクトリ設計	重要度2
301.3 スキーマ	重要度3

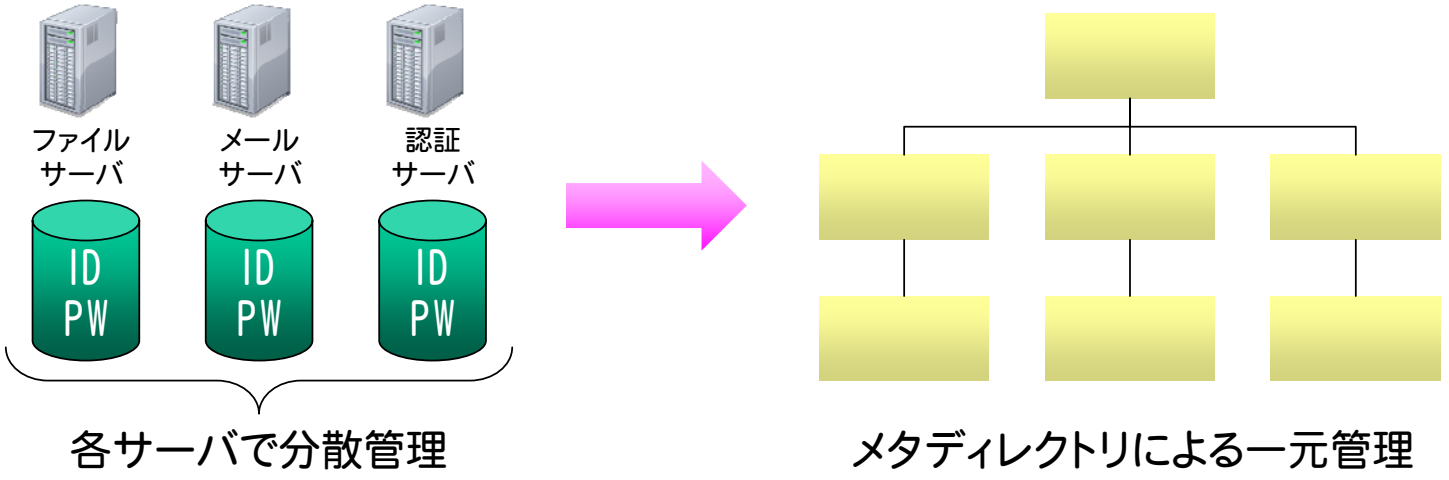
ディレクトリサービスとは

ディレクトリサービス

- さまざまな情報を階層構造に格納して管理・利用するための仕組み
- 「人」や「もの」といった実在する「もの」の情報を格納するのに利用される

メタディレクトリ

- ネットワーク上で物理的に分散している情報を論理的に結合し、検索や管理を容易にするしくみ



ディレクトリサービスの標準プロトコル

X.500

- ITU-T(国際電気通信連合　電気通信標準化部門)で勧告された
  ディレクトリサービスに関する国際規格
- DAP (Directory Access Protocol)プロトコルでアクセスするよう規定
- 高機能だが、実装に多くのリソースを必要とするため普及しなかった

LDAP (Lightweight Directory Access Protocol)

- DAPプロトコルを軽量化し、TCP/IP上で動作するように必要な機能を
  取り出したプロトコル
- 既存のインターネットサービスとの連携が可能
- 標準的にLDAPv3 (RFC2251～2256)が利用される

LDAPの実装

■商用製品

- Microsoft Active Directory (Microsoft社)
- Novell eDirectory (Novell社)

■オープンソース

- OpenLDAP
- Fedora Directory Server
- Apache Directory

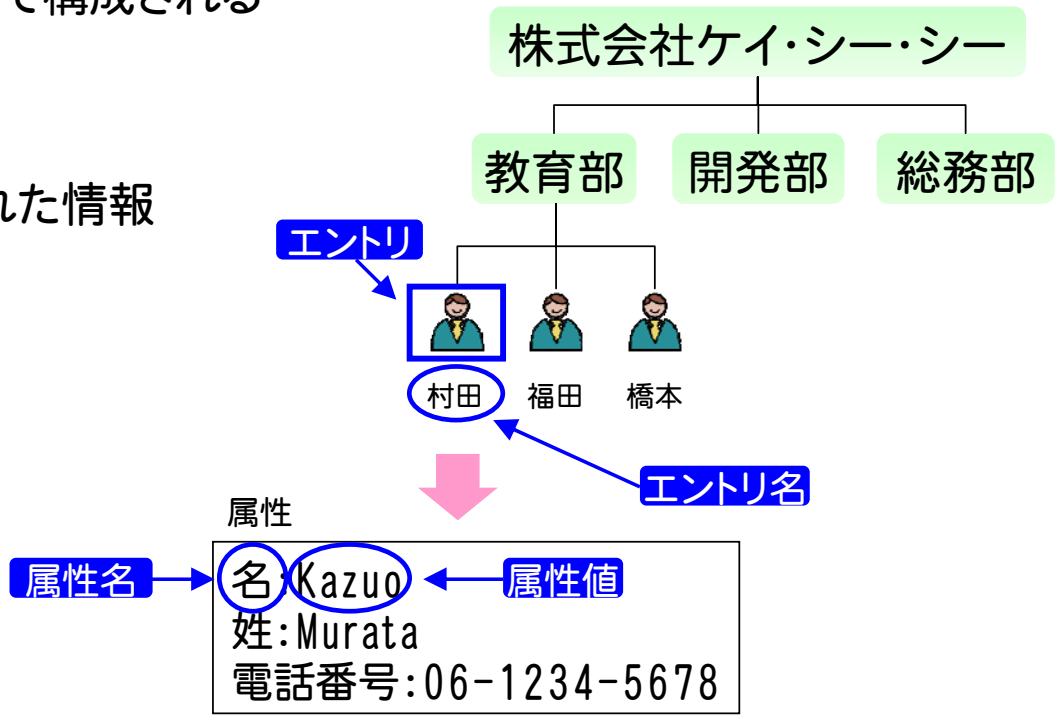
Linux Professional Institute

LDAPのデータモデル

■ディレクトリに格納する情報
- ディレクトリに格納する情報の単位をエントリという
- 各エントリは実在する情報(人やもの)に対応し、エントリ名が付けられる
- 各エントリに格納する情報は1つまたは複数の属性から構成される
- 属性は属性名と属性値で構成される

■属性名
- エントリに関連付けられた情報

■属性値
- 属性に格納される値



主な属性名

o	組織名（Organization）
ou	組織単位（Organizational Unit）
c	国名（Country name）
cn	一般名称（Common Name）
sn	姓（SurName）
dc	ドメイン構成要素(Domain Component)
mail	メールアドレス（mail）
telephoneNumber	電話番号（Telephone Number）

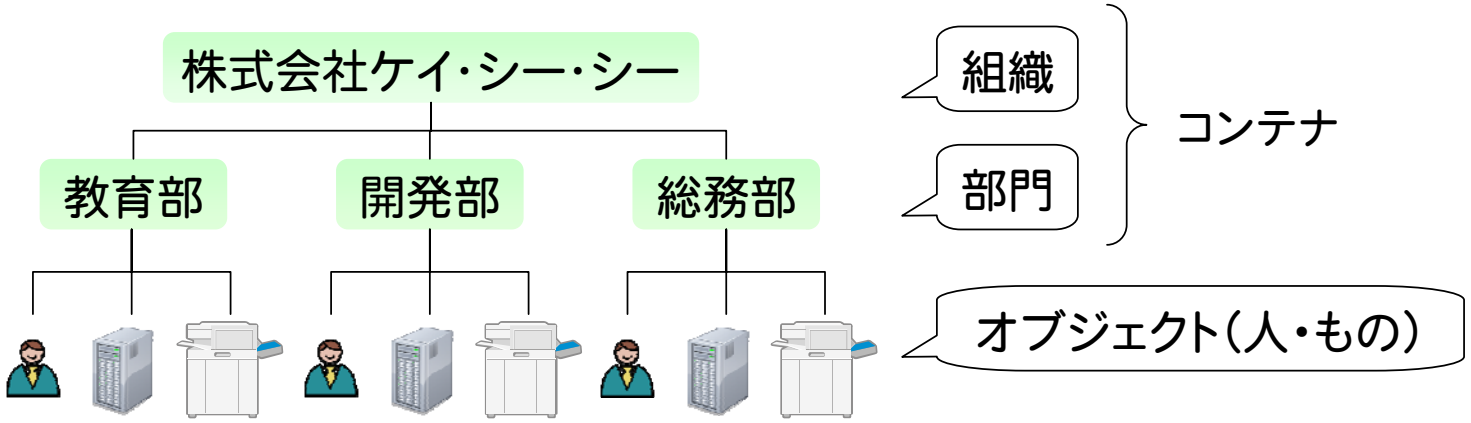
名:Kazuo
姓:Murata
電話番号:06-1234-5678

cn:Kazuo
sn:Murata
telephoneNumber:06-1234-5678

エントリの管理

DIT (Directory Information Tree)

- 各エントリが管理される階層構造
- 階層構造を構成するために存在するエントリをコンテナという



エントリの識別

■エントリの識別
- 各エントリはRDNまたはDNにより区別される

■相対識別名 (Relative DN: RDN)
- 同一階層内で一意に識別する名前
- 「属性名=属性値」と記述

■識別名(Distinguished Name: DN)
- エントリをDIT内で一意に識別する名前
- 下位エントリから上位に向かってRDNをカンマ(,)で区切って記述

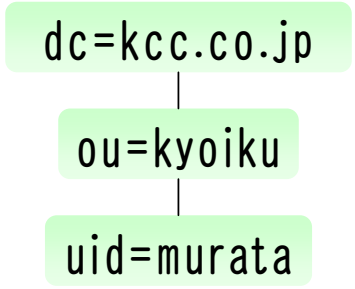
相対識別名(RDN)と識別名(DN)

相対識別名(RDN)

同一階層内で一意

識別名(DN)

DIT内で一意



dc=kcc.co.jp

ou=kyoiku, dc=kcc.co.jp

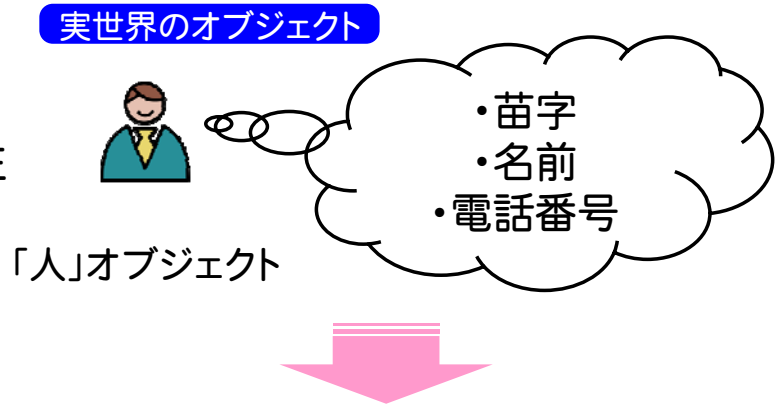
uid=murata, ou=kyoiku, dc=kcc.co.jp

オブジェクトクラス

■オブジェクトクラスとは
- エントリに必要な属性および保有できる属性を定義するための特殊な属性
- 1つのエントリは必ずObjectClass属性を持たなければならない
- エントリに必要な属性によって使用するオブジェクトクラスが決まる

■必須属性 (required attribute)
- エントリに登録しなければならない属性

■許可属性 (allowed attribute)
- エントリに登録できる属性



オブジェクトクラスの構造型

■オブジェクトクラスの構造型

- オブジェクトクラスは他のオブジェクトクラスの機能を継承して作成される
- 継承元となるオブジェクトクラスを基底クラス、基底クラスを継承して作られるクラスを派生クラスという
- オブジェクトクラスには以下の3つの種類がある

構造型（STRUCTUAL）	●実際のものと対応するオブジェクトクラス ●エントリは必ず1つ以上の構造型オブジェクトクラスが必要
抽象型（ABSTRUCT）	●他のオブジェクトの基底クラスとなる ●派生クラスの親クラスとしてのみ利用可 ●「top」はすべてのオブジェクトクラスの基底クラス
補助型（AUXILIARY）	●構造型クラスに特徴を追加する ●単独でエントリを生成することはできない

スキーマ

■スキーマとは
- オブジェクトクラスや属性を定義するもの
- OpenLDAPではスキーマファイルにて定義する
  - ○○○.schemaというファイル名

■スキーマで定義する内容
- オブジェクトクラスの定義
  - オブジェクトクラスの構造型
  - 必須属性
  - 許可属性
- 属性の定義
  - 属性の型
  - 属性値の検索方法（照合規則）

「人」オブジェクト

「person」オブジェクトクラス

・必須属性
　名前、苗字
・許可属性
　電話番号、関連情報、
　パスワード、コメント

「person」オブジェクトクラス

必須属性
・cn, sn
許可属性
・telephoneNumber, seeAlso,
　userPassword, description

「telephoneNumber」属性

属性型： 電話番号型
検索方法:
・文字列の完全一致
・文字列の部分一致

「seeAlso」属性

標準スキーマと拡張スキーマ

標準スキーマ

- スキーマの要素(オブジェクトクラス・属性)はOID (Object IDentifier)という識別子によって管理される
- OIDは全世界で一意でなければならない
- OIDはISOで標準化されており、管理はIANA (Internet Assigned Numbers Authority)で行っている

拡張スキーマ

- 用意されているスキーマでは定義できないオブジェクトクラス・属性がある場合は独自作成できる
- 独自スキーマを作成する際は以下の点に留意する
  - OIDが重複しないこと
  - スキーマファイルは新規に作成する
    (既存のスキーマファイルを編集しない)

基本スキーマファイル

主な基本スキーマファイル

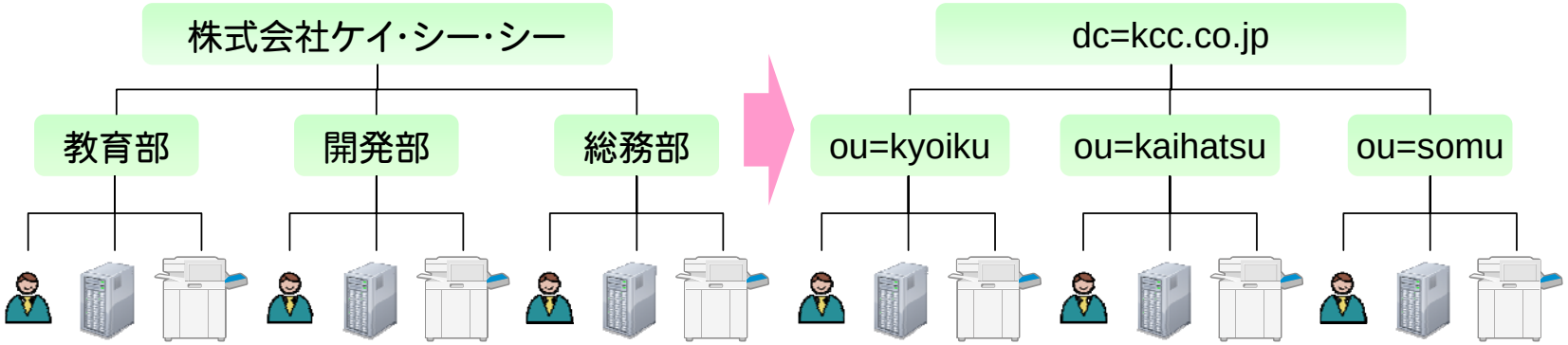
- パッケージインストールした場合、/etc/openldap/schemaディレクトリに格納される

core.schema	OpenLDAP Coreスキーマ【必須】
cosine.schema	COSINEとInternet X.500スキーマ【必須】
inetorgperson.schema	inetOrgPersonクラスを定義するスキーマ
misc.schema	開発中のオブジェクトクラス定義を含むスキーマ
nis.schema	NISで扱う情報を定義するスキーマ
openldap.schema	OpenLDAPプロジェクトの実験用スキーマ
java.schema	Javaオブジェクトを扱うためのスキーマ
corba.schema	CORBAオブジェクトを扱うためのスキーマ

DITの設計

DITの設計ポイント

- 大分類はツリーの上位に、小分類のものは下位に置く
- 同一階層にあるエントリは同一カテゴリのものを配置する
- 識別子(DN)が一意になるように構築する



エントリの設計

エントリの設計ポイント

- エントリが持つ情報を属性値としてすべて表現できるか
- エントリに格納する情報(オブジェクトクラスで定義)
  - 必須属性
  - 許可属性
- 情報のデータ型(文字列、数値、バイナリデータなど)
- 検索の際にどのように利用されるか(照合規則)
  - 完全一致が必要
  - データの有無が必要

属性	属性値	データ型
ユーザ名	murata	文字列型
シャドウパスワード	yyvyWUCDEN･･･	文字列型
UID	500	数値型
GID	500	数値型

オブジェクトクラスの設計

■オブジェクトクラスの設計ポイント

- エントリの内容に従って、適用するオブジェクトクラスを決定する
- 構造型(STRUCTUAL)のオブジェクトクラスを最低1つ含める

属性	属性値	データ型
ユーザ名	murata	文字列型
パスワード	yyvyWUCDEN･･･	文字列型
UID	500	数値型
GID	500	数値型

posixAccountオブジェクトクラス(補助型)
必須属性:
cn, uid, uidNumber, gidNumber,
homeDirectory

inetOrgPersonオブジェクトクラス(構造型)
必須属性:
sn, cn
※personオブジェクトクラスから継承

オブジェクトクラス定義スキーマ(1)

■「posixAccount」オブジェクトクラスの定義

①OID、オブジェクトクラスの名前
②オブジェクトクラスの説明
③基底オブジェクトクラスと構造型
④必須属性($は区切り文字)
⑤許可属性(同上)

```
objectclass ( 1.3.6.1.1.1.2.0 NAME 'posixAccount'
        DESC 'Abstraction of an account with POSIX attributes'
        SUP top AUXILIARY
        MUST ( cn $ uid $ uidNumber $ gidNumber $
             homeDirectory )
        MAY ( userPassword $ loginShell $ gecos $ description))
```

①OIDは1.3.6.1.1.1.2.0で、「posixAccount」という名前のオブジェクトクラス
②「POSIX属性を持つアカウントの抽象化」
③「top」を基底オブジェクトクラスとした補助型オブジェクト
④cn、uid、uidNumber、gidNumber、homeDirectory属性は必須
⑤userPassword、loginShell、gecos、description属性はオプション

オブジェクトクラス定義スキーマ(2)

「inetOrgPerson」オブジェクトクラスの定義

```
objectclass ( 2.5.6.6 NAME 'person'
        DESC 'RFC2256: a person'
        SUP top STRUCTUAL
        MUST ( sn $ cn )
        MAY ( userPassword $ telephoneNumber $ seeAlso $
            description ) )
```

snとcnが必須属性

```
objectclass ( 2.5.6.7 NAME 'organizationalPerson'
        DESC 'RFC2256: an organizational person'
        SUP person STRUCTUAL
        MAY ( title $ x121Address $ registered Address ...(略)
```

personを継承

```
objectclass ( 2.16.840.1.113730.3.2.2 NAME 'inetOrgPerson'
        DESC 'RFC2798: Internet Organizational Person'
        SUP organizationalPerson STRUCTUAL
        MAY ( audio $ businessCategory $ carLicense $ ...(略)
```

organizationalPersonを継承

属性定義スキーマ(1)

「cn」属性の定義

```
attributetype ( 2.5.4.3 NAME 'cn' 'commonName' )
        DESC 'RFC2256: common name(s) for which the entity is
              known by'
        SUP name )
```

← 基底値としてname属性を継承

「uid」属性の定義

```
attributetype ( 0.9.2342.19200300.100.1.1
        NAME ( 'uid' 'userid' )
        DESC 'RFC1274: user identifier'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{256} )
```

属性定義スキーマ(2)

「uidNumber」属性の定義

```
attributetype ( 1.3.6.1.1.1.1.0 NAME 'uidNumber'
        DESC 'An integer uniquely identifying a user in an
              administratvie domain'
        EQUALITY integerMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )
```

属性のデータ型は整数型
1つの属性しか登録できない

「gidNumber」属性の定義

```
attributetype ( 1.3.6.1.1.1.1.1 NAME 'gidNumber'
        DESC 'An integer uniquely identifying a group in an
              administratvie domain'
        EQUALITY integerMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )
```

属性定義スキーマ(3)

■「homeDirectory」属性の定義

```
attributetype ( 1.3.6.1.1.1.1.3 NAME ‘homeDirectory’
        DESC ‘The absolute path to the home directory’
        EQUALITY caseExactIA5Match
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )
```

■「sn」属性の定義

```
attributetype ( 2.5.4.4 NAME ‘sn’ ‘surname’ )
        DESC ‘RFC2256: last (family) name(s) for which the
        entity is known by’
        SUP name )
```

ディレクトリ情報の記述

LDIF (LDAP Data Interchange Format)

- LDAPデータを表現するためのテキスト形式のファイルフォーマット
- ディレクトリ情報の追加・変更などに使用する

★LDIFのフォーマット

```
# コメント
dn:
属性記述子: 属性値
・・・

# コメント
dn:
属性記述子: 属性値
・・・
```

1エントリ分の情報

エントリと次のエントリの間は空白行で区切る

LDIFの記述ルール

```
#ルートノード
dn: dc=kcc.co.jp
objectClass: domain
dc: kcc.co.jp

#教育部
dn: ou=kyoiku,dc=kcc.co.jp
objectClass: organizationalUnit
ou: kyoiku

#Kazuo Murataのエントリ
dn: cn=kazuo murata,ou=kyoiku,dc=kcc.co.jp
objectClass: inetOrgPerson
objectClass: posixAccount
cn: Kazuo Murata
sn: Murata
uid: murata
...(略)
```

1行目は必ず「dn」で始める（コメント行除く）

「objectClass」は各エントリに必須

適用するオブジェクトクラスの記述

LPICレベル3　技術解説

主題304:使用法

304.1 ディレクトリの検索　　重要度2
304.2 LDAPコマンドラインのツール　　重要度4

ディレクトリの検索・LDAP関連コマンド(1)

ldapsearchコマンド

- 登録されたエントリを検索する

【書式】 ldapsearch [オプション] フィルタ [属性]

-D *DN*	ディレクトリへのバインドに使うDNを指定する
-w *パスワード*	簡易認証のパスワードを指定する
-y *ファイル名*	簡易認証のパスワードをファイルから読み込む
-x	簡易認証を使用する
-W	簡易認証のプロンプトを表示する
-b *ベースDN*	検索の開始位置を指定する
-L	検索結果をLDIFv1で表示する
-LL	検索結果のコメントを出力しない
-LLL	検索結果のコメントとLDIFバージョンを出力しない

ディレクトリの検索・LDAP関連コマンド(2)

ldapsearchコマンドの実行例

ログインシェルとして/bin/shを使用するユーザのユーザIDを検索

簡易認証を利用　バインドDNを指定　認証プロンプトを表示　検索開始位置を指定

```
$ ldapsearch -x -LLL -D 'cn=Manager,ou=kyoiku,dc=kcc.co.jp' -W -b
'dc=kcc.co.jp' 'loginShell=/bin/sh' 'uid'
Enter LDAP Password:

dn: cn=kazuo murata,ou=kyoiku,dc=kcc.co.jp
uid: murata

dn: cn=hiroyuki fukuda,ou=kyoiku,dc=kcc.co.jp
uid: fukuda
(略)
```

ディレクトリの検索・LDAP関連コマンド(3)

ldapsearchコマンドの検索フィルタ

&	論理積 (and)
|	論理和 (or)
!	論理否定 (not)
=	等しい
~=	ほぼ等しい (近似値)
>=	～以上
<=	～以下
*	任意の値 (any)

(cn=Taro*)
→cnがTaroで始まるエントリ

(&(sn=Yamada)(o=systems))
→snが「Yamada」かつ、「systems」という組織に所属するエントリ

(|(sn=Yamada)(sn=Sato))
→snが「Yamada」または「Sato」であるエントリ

(&(|(sn=Yamada)(sn=Sato))(cn=Taro~))
→snが「Yamada」か「Sato」で、かつ、cnが「Taro」で始まるエントリ

(&(sn=Yamada)(!(cn=Taro*)))
→姓が「Yamada」で名前が「Taro」で始まるものを除くエントリ

ldapツール

LDAP関連コマンド(slapdの起動中に実行)

- エントリの追加 (ldapadd)
- エントリの変更 (ldapmodify)
- 登録されたエントリのRDNの変更 (ldapmodrdn)
- 登録されたエントリの削除 (ldapdelete)
- 登録されたエントリのパスワード変更 (ldappasswd)

LDAP関連コマンドの実行

- ldapaddの実行
  - 追加エントリ情報を記述したLDIFファイルを指定
- ldapmodifyの実行
  - 「changetype: modify」が記述されたLDIFファイルを指定

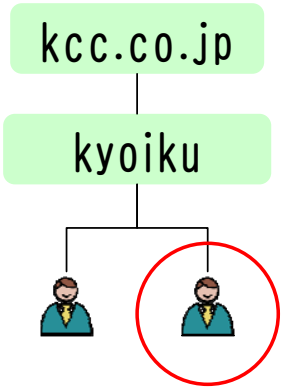
エントリの追加(ldapaddコマンド)

手順

① 追加するエントリ情報をLDIFファイルとして作成する

kcc.ldifファイルの内容

```
dn: cn=taro yamada,ou=kyoiku,dc=kcc.co.jp
cn: taro yamada
givenName: taro
gidNumber: 550
homeDirectory: /home/users/yamada
...(略)
```



② ldapaddコマンドでエントリ追加する

ldapaddコマンド

- エントリを追加する (ldapmodify –aと同じ)

【書式】 ldapadd [オプション]

```
$ ldapadd –x –D ‘cn=Manager,ou=kyoiku,dc=kcc.co.jp’ –W –f kcc.ldif
Enter LDAP Password:
adding new entry “cn=taro yamada,ou=kyoiku,dc=kcc.co.jp”
```

エントリの変更(ldapmodifyコマンド)

ldapmodifyコマンド

- エントリおよび属性を更新・追加する

【書式】 ldapmodify [オプション]

-f *ファイル名*	エントリの情報を読み込むファイル名を指定する
-D *DN*	ディレクトリへのバインドに使うDNを指定する
-w *パスワード*	簡易認証のパスワードを指定する
-y *ファイル名*	簡易認証のパスワードをファイルから読み込む
-x	簡易認証を使用する
-W	簡易認証のプロンプトを表示する
-a	新規にエントリを追加する(ldapaddと同じ)

エントリの変更(ldapmodifyコマンド)

changetypeディレクティブ

- LDIFファイルにchangetypeディレクティブを記述することにより、エントリの追加・削除、属性の追加・削除・変更をすることができる

エントリの追加

```
dn: cn=taro yamada,ou=kyoiku,dc=kcc.co.jp
changetype: add
cn: taro yamada
...(略)
```

エントリの削除

```
dn: cn=taro yamada,ou=kyoiku,dc=kcc.co.jp
changetype: delete
```

属性の追加・削除・変更(ldapmodifyコマンド)

エントリに「telephoneNumber」属性を追加

```
dn: cn=taro yamada,ou=kyoiku,dc=kcc.co.jp
changetype: modify
add: telephoneNumber
telephoneNumber: 06-1234-5678
```

changetype: modify ← エントリ属性変更の宣言
add: telephoneNumber ← 属性の追加宣言

エントリから「telephoneNumber」属性を削除

```
dn: cn=taro yamada,ou=kyoiku,dc=kcc.co.jp
changetype: modify
delete: telephoneNumber
```

changetype: modify ← エントリ属性変更の宣言
delete: telephoneNumber ← 属性の削除宣言

エントリのユーザIDを「777」に変更

```
dn: cn=taro yamada,ou=kyoiku,dc=kcc.co.jp
changetype: modify
replace: uidNumber
uidNumber: 777
```

changetype: modify ← エントリ属性変更の宣言
replace: uidNumber ← 属性の変更宣言

属性の追加・削除・変更(ldapmodifyコマンド)

属性の追加・削除・変更を1つのファイルに記述

```
dn: cn=Taro Yamada,ou=kyoiku,dc=kcc.co.jp
changetype: modify
add: telephoneNumber
telephoneNumber
-
dn: cn=Taro Yamada,ou=kyoiku,dc=kcc.co.jp
changetype: modify
delete: telephoneNumber
-
dn: cn=Taro Yamada,ou=kyoiku,dc=kcc.co.jp
changetype: modify
replace: uid
uid: 777
```

区切り

区切り

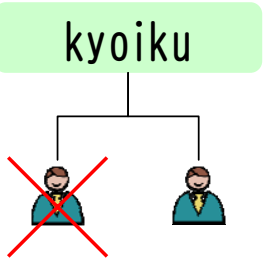
エントリの削除(ldapdeleteコマンド)

- ldapdeleteコマンド
  - エントリを削除する

【書式】 ldapdelete [オプション] [識別名]

```
$ ldapdelete -x -D 'cn=Manager,ou=kyoiku,dc=kcc.co.jp' -W
'cn=taro yamada,ou=kyoiku,dc=kcc.co.jp'
Enter LDAP Password:
$
```

正常に終了した場合は画面には何も表示されない



slapツール

- LDAP関連コマンド(slapdの停止時に実行)
  - エントリの追加 (slapadd)
  - データベースの内容をLDIFファイルとして出力 (slapcat)
  - インデックスの更新 (slapindex)
  - パスワードハッシュの生成 (slappasswd)

エントリの追加(slapaddコマンド)

slapaddコマンド

- エントリの追加を行う
- slapdを起動しない場合にエントリを追加できる
- 管理者権限で実行する必要がある
- 実行時に上位エントリの名前やスキーマの検証を行わない
  →ldapaddを使用するほうが望ましい

【書式】 slapadd [オプション]

```
# slapadd -l kcc.ldif
```

-l *ファイル名*	指定したLDIFファイルからエントリ情報を読み込む
-b *ベースDN*	エントリを追加するベースDNを指定する
-c	エラーが生じた場合でも動作を継続する

エントリのバックアップ(slapcatコマンド)

slapcatコマンド

- データベースの内容をLDIFファイルに出力する
- バックアップファイルはslapaddコマンドでリストアすることができる

【書式】 slapcat [オプション]

```
# slapadd -l buckup.ldif
```

-l	出力するLDIFファイルの名前を指定する
-b *ベースDN*	データベースのベースDNを指定する
-n *数*	指定したDNのサブツリーのエントリのみを出力する

インデックスの再生成、パスワード値の生成

slapindexコマンド

- データベースのインデックスを再生成

-c	エラーが生じた場合でも動作を継続する
-v	エントリを追加するベースDNを指定する
-f *ファイル名*	slapd.confファイルの代わりに利用する設定ファイルを指定する

slappasswdコマンド

- パスワード値の生成

-v	冗長モードで実行する
-s *パスワード*	指定されたパスワードをハッシュ化する
-T *ファイル名*	指定されたファイルをハッシュ化する
-h *スキーム*	パスワードのハッシュ化のスキームを指定する {CRYPT}・{MD5}・{SMD5}・{SSHA}・{SHA}が指定可能 デフォルトは{SSHA}

LPICレベル3　技術解説

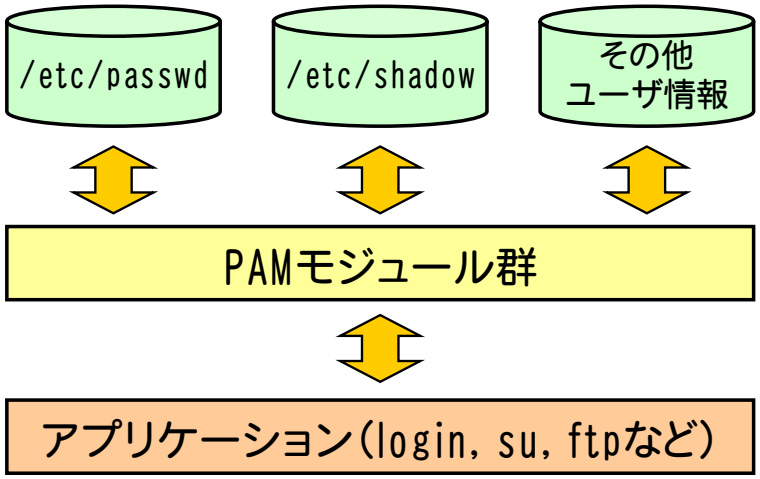
主題305:統合と移行

305.1 PAMとNSSのLDAP統合　　重要度2
305.3 LDAPと各種UNIXサービスの統合　　重要度1

PAMとNSSのLDAP統合

PAMとNSS

- PAM (Pluggable Authentication Module)
  - 様々な認証方式を一元的に管理するしくみ
  - 認証が必要なアプリケーションが参照するモジュール群



- NSS (Name Service Switch)
  - 各種情報取得の検索順を指定するしくみ

PAMの認証にLDAPを利用する(1)

ldap.confの設定

- LDAPクライアントとして動作する際に参照する設定ファイル

host	利用するLDAPサーバのホスト名を指定する
base	LDAP検索を行うベースDNを指定する
binddn	LDAP操作を行う際に利用するバインドDNを指定する
bindpw	LDAP操作を行う際に利用するバインドDNのパスワードを指定する

```
...(略)

host 192.168.1.200
base dc=kcc.co.jp
binddn cn=Manager,ou=kyoiku,dc=kcc.co.jp
bindpw abcdefg

...(略)
```

PAMの認証にLDAPを利用する(2)

PAMの設定例(/etc/pam.d/system-auth)

```
#%PAM-1.0
auth            required        pam_env.so
auth            sufficient      pam_unix.so nullok try_first_pass
auth            requisite       pam_succeed_if.so uid >= 500 quiet
auth            sufficient      pam_ldap.so use_first_pass
auth            required        pam_deny.so

account         required        pam_unix.so broken_shadow
account         sufficient      pam_succeed_if.so uid < 500 quiet
account         [default=bad success=ok user_unknown=ignore] pam_ldap.so
account         required        pam_permit.so

password        requisite       pam_cracklib.so try_first_pass retry=3
password        sufficient      pam_unix.so md5 shadow nullok try_first_pass
use_authtok
password        sufficient      pam_ldap.so use_authtok
password        required        pam_deny.so

session         optional        pam_keyinit.so revoke
session         required        pam_limits.so
```

PAMの認証にLDAPを利用する(3)

nsswitch.confの設定例

```
...(略)

passwd: files ldap
shadow: files ldap
group:  files ldap

...(略)
```

LDAPと各種UNIXサービスの統合

SSHとLDAPの統合

1. OpenSSH LDAP Public Key Patchを適用
   - ソースインストール
2. OpenSSHの設定

★sshd_configの設定例

```
UseLPK yes
LpkServers ldap://192.168.1.200
LpkUserDN ou=users,dc=kcc.co.jp
LpkGroupDN ou=groups,dc=kcc.co.jp
LpkBindDN cn=Manager,ou=kcc.co.jp
LpkBindPw ldappass
```

LDAPの利用を有効化

LDAPサーバのアドレス

3. スキーマファイル（openssh-lpk_openldap.schema）をslapd.confにインクルード

LPICレベル3　技術解説

主題306:キャパシティプランニング

306.1 リソース使用率を測定する　　重要度4

vmstatコマンド(1)

■メモリ・CPUの使用量を監視

【書式】 vmstat [-a] [秒 [回数]]

-a	アクティブ/非アクティブなメモリを表示する
-d	ディスクに関する統計情報を表示する
-p	指定したパーティションの統計情報を表示する
-S	指定した単位で表示する

コマンド実行例

```
$ vmstat 3 5
procs -----------memory---------- ---swap-- ----io--- --system-- -----cpu-----
 r  b   swpd   free   buff  cache   si   so   bi   bo   in   cs us sy id wa st
 0  0      0 512916  26772 375072    0    0  317   35  671  185  2  4 90  4  0
 1  0      0 512940  26772 375072    0    0    0    0  750  295  1  1 98  0  0
 0  0      0 512916  26780 375072    0    0    0   11  648  146  0  1 99  0  0
 0  0      0 512916  26780 375072    0    0    0   23  648  150  1  0 99  0  0
 0  0      0 512916  26788 375072    0    0    0    7  649  147  0  1 99  0  0
```

vmstatコマンド(2)

procs	r	実行待ちプロセス数
	b	割り込み不可のスリープ状態にあるプロセス数
memory	swpd	仮想メモリ量
	free	空きメモリ量
	buff	バッファに割り当てられているメモリ量
	cache	キャッシュに割り当てられているメモリ量
swap	si	ディスクからスワップインされているメモリ量
	so	ディスクへスワップアウトされているメモリ量
io	bi	ブロックデバイスから受け取ったブロック
	bo	ブロックデバイスに送られたブロック
system	in	1秒あたりの割り込み数
	cs	1秒あたりのコンテキストスイッチの回数
cpu	us	CPU総時間に対するユーザ時間の割合
	sy	CPU総時間に対するシステム時間の割合
	id	CPU総時間に対するアイドル時間の割合
	wa	I/O待ち時間
	st	仮想マシンに使用された時間

sarコマンド(1)

■システム活動データのレポート表示

- システム状況を収集し、バイナリ形式で出力(sadcコマンド)
- バイナリで出力されたデータをテキスト形式で表示(sarコマンド)

【書式】 sar オプション [-s 開始時刻] [-e 終了時刻] [-f ログファイル名]
[表示間隔(秒)] [回数]]

-b	ディスクの入出力と転送レート情報を表示
-f	ログファイルを指定
-n DEV	ネットワーク関連の情報を表示
-n EDEV	ネットワーク関連のエラー情報を表示
-r	メモリとスワップ関連の情報を表示

sarコマンド(2)

ディスク関連情報の表示

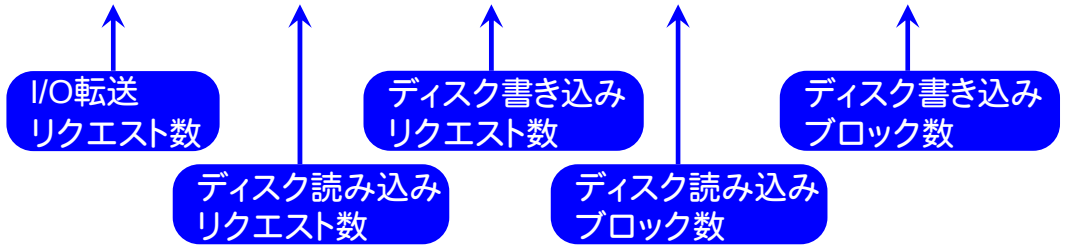
```
$ sar -b –f /var/log/sa/sa01
Linux2.6.18-238.el5 (station200.kcc.co.jp)   2011年12月01日

12時50分43秒       LINUX RESTART

13時00分01秒       tps      rtps      wtps    bread/s     bwrtn/s
13時10分01秒     14.17      6.93      7.24     187.92      113.03
13時20分01秒      7.83      4.60      3.23     237.26       43.50
13時30分01秒      7.94      2.64      5.30      42.88       75.84

...

平均値:           4.48      1.14      3.34      24.60       43.19
```



sarコマンド(3)

ネットワークインターフェイス情報の表示

```
$ sar -n DEV -f /var/log/sa/sa01
Linux2.6.18-238.el5 (station200.kcc.co.jp)   2011年12月01日

12時50分43秒       LINUX RESTART

13時00分01秒  IFACE  rxpck/s  txpck/s  rxbyt/s  txbyt/s  rxcmp/s  txcmp/s  rxmcst/s
13時10分01秒     lo     0.00     0.00     0.00     0.00     0.00     0.00      0.00
13時10分01秒   eth0     0.80     0.13    51.54   116.21     0.00     0.00      0.01
13時10分01秒   sit0     0.00     0.00     0.00     0.00     0.00     0.00      0.00
13時20分01秒     lo     0.00     0.00     0.00     0.00     0.00     0.00      0.00
13時20分01秒   eth0     1.09     0.48    77.03   590.20     0.00     0.00      0.01
13時20分01秒   sit0     0.00     0.00     0.00     0.00     0.00     0.00      0.00

...

平均値:          lo     0.00     0.00     0.00     0.00     0.00     0.00      0.00
平均値:        eth0     0.12     0.12    83.82    83.82     0.00     0.00      0.01
平均値:        sit0     0.00     0.00     0.00     0.00     0.00     0.00      0.00
```

送受信パケット数

送受信バイト数

送受信圧縮パケット数

受信マルチキャストパケット数

iostatコマンド

各種統計情報の表示

- CPU統計
- ディスクI/O統計

```
$ iostat
Linux2.6.18-238.el5 (example)   2011年08月19日

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           1.11    0.03    2.33    2.67    0.00   93.86

Device:            tps   Blk_read/s   Blk_wrtn/s   Blk_read   Blk_wrtn
sda               6.80       501.82        41.06     701325      57380
sda1              0.05         1.54         0.00       2158          4
sda2              6.74       500.04        41.05     698831      57376
dm-0             19.06       499.06        41.05     697466      57376
dm-1              0.11         0.85         0.00       1184          0
hdc               0.01         0.12         0.00        164          0
```

CPU統計

ディスクI/O統計

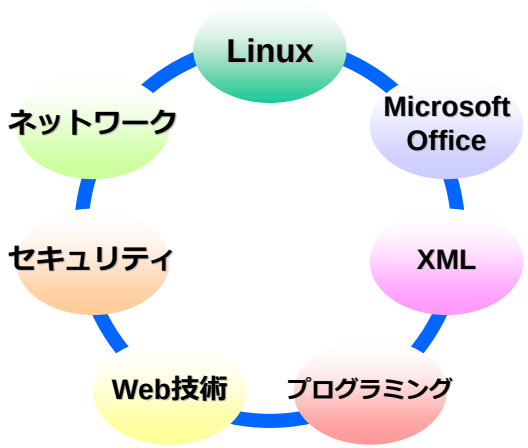
ご参考

■カスタマイズ研修のご案内

- LPIC試験対策研修
- Linux基礎、Linuxサーバ構築
- その他、ネットワーク・セキュリティ・XML・Web技術など
  各種IT研修をカスタマイズして提供

弊社研修サービスホームページ

http://www.kcc.co.jp/lpic/



IT技術研修
- ●Linux（基礎・システム管理・サーバ構築）
- ●ネットワーク（TCP/IP・LAN/WAN・無線技術）
- ●セキュリティ（技術解説・セキュリティマネジメント）
- ●XML（XML/DTD・XSLT・XML Schema）
- ●Web技術（HTML・CSS・JavaScript・Ajax）
- ●プログラミング（C・Java・Android・Perl・PHP・Ruby）
- ●Microsoft Office（基礎/応用・VBA）

資格試験対策
- ◆LPICレベル1～3
- ◆XMLマスター・ベーシック
- ◆CompTIA A+・Network+・Security+
- ◆Ruby技術者認定試験 Silver
- ◆情報処理技術者試験

Linux Professional Institute

株式会社ケイ・シー・シー

ご清聴ありがとうございました

Linux Professional Institute