



LinuC レベル2 技術解説 オンラインセミナー

~受験に向けての準備とポイント解説~

2021/2/14 (Sun) 13:00-14:00

LPI-Japanプラチナスポンサー 株式会社ゼウス・エンタープライズ 鯨井 貴博(LinuCエヴァンジェリスト)









鯨井貴博

LPI-Japan プラチナスポンサー 株式会社ゼウス・エンタープライズ LinuCエバンジェリスト

大学時代 Unixの存在を知り、日経Linuxを読み始める。 2000年にVine Linux 2.0で一度挫折を経験。 その悔しさを忘れきれず、2007年 他業種からIT業界に転職しLinuxに再チャレンジ。

SE・商用製品サポート・インストラクター・プロジェクト管理などを経験し、現在に至る。 自分自身が学習で苦労した経験から、初心者を含む受講者に分りやすい講義を行うように心がけている。

また、興味の向くIT技術・オープンソースソフトウェアなどについて、 Opensourcetehブログ(<u>https://www.opensourcetech.tokyo/</u>)で執筆中。 実際に自分でやってみる/使ってみる・開発者本人から話を聞いてみることを大切にしています。





Linus Torvaldsさん(Linux開発者)

Igor Sysoevさん(nginx開発者)





Alexei Vladishevさん(Zabbix開発者) © LPI-Japan / EDUCO all rights reserved.





提供するITサービス

リナックス・ネットワークグループ



クロスボーダーSE&ITソリューショングループ

ディネータ)による支援サービスを行っています。

思疎通面でのデメリット回避などに力を発揮します。

コンビュータシステムの企画・開発・保守

積算代行 与信代行サービス 特定労働者派遣

翻訳業務 通訳業務

語学力堪能なエンジニア(クロスボーダーSE)とヘルプデスク(バイリンガルコー

技術用語を多く含む会話の通訳、ドキュメントの翻訳という専門性を活かし、オフ

ショア開発のプロジェクト、外国人技術者を多数かかえる現場などにありがちな意

「Zeus Linux Training Center / Zeus Network Training Center」で行います。 資格取得の支援、新しい知識の習得に努め、つねに高水準のサービスの提供をめざ

コンピュータシステムの企画・開発・保守 請負業務

特定労働者派遣



アプリケーショングループ



Zeus Linux Training Center / Zeus Network Training Center

当社で培われた技術者向け研修カリキュラムを、一般のお客様や企業様向けに提供 することを目的としたITキャリアスクール「Zeus Linux Training Center / Zeus Network Training Center」を運営しています。 成まで、「現場ですぐに活躍できる人材」の育成をめざした研修は、技術者を求め る企業からも高い評価をいただいています。

教育事業(BtoB、BtoC)

社員教育 試験会場





https://www.zeus-enterprise.co.jp/solution/service









③	提供するITサービス		
COURSE ~コース紹介~		会場	銀座ほこてん子供プログラミング教室 〒104-0061 東京都中央区銀座5丁目8-20 銀座コア8階
Minecraftコース		対象年齢	小学校3年~6年
大人気ゲーム!Minecraftを使って楽しくプログラミング!	ッチャンロボットをプログニレクトーズ協スストで、プレイ	講習時間	10:30~11:30/12:00~13:00/13:30~14:30/ 15:00~16:00/16:30~17:30
ヤーの代わりに様々な作業をとても短い時間で行わせることができます!プログラジョン	ミング的手法を使い、Minecraftの世界を自由に作り上げ	講習曜日	毎日
→各コマ、集合型レッスン定員12名・オンラインレッスン定員3名		持ち物	筆記用具
	Contractions of the second sec	入学金	ありません
			6,000円~(税込)/月2回~(1コマ60分)
			Minecraftのライセンス代:3300円 (税込) / テキスト代:2530円(税込)
※ 保護者同伴可能		無料体験	好評受付中!必要機材は全てお貸しします!
オンラインレッスン対応!! ***********************************	キャンペーン 兄弟・姉妹一緒の10 全員月謝がずっと お申し込みで %OFF!		

%OFF!



https://www.it-training.tokyo/kids/index.html



4







- 1. LinuC Level2試験とは
 - 試験概要と特徴
- 2. 技術解説
 - 主題2.11 : ファイル共有サービス 2.11.1 Sambaの設定と管理 - 主題2.12 : システムのセキュリティ 2.12.1 iptables や firewalld によるパケットフィルタリング
- 3. Q&A







仮想環境を含むLinuxのシステム設計、ネットワーク構築において、アーキテクチャに基づいた設計、導入、 保守、問題解決ができる技術者を認定する試験

- ✓ Linuxシステムの設計、構築、監視、トラブルシューティングができる。
- ✓ 仮想マシンやコンテナの仕組みを理解し、その管理と運用ができる。
- ✓ セキュリティとシステムアーキテクチャの基本を理解し、サービスの設計、構築、運用・管理ができる。

201試験/202試験の両方に合格することでレベル2に認定 1試験あたり 15,000円(消費税別) ピアソンVUEにおけるCBT or PBT(団体受験用)

詳細は、<u>https://linuc.org/linuc2/</u>









LinuC Level2試験とは



201試験	202試験
2.01 : システムの起動とLinuxカーネル	2.07 : ネットワーククライアントの管理
2.01.1 ブートプロセスとGRUB	2.07.1 DHCPサーバーの設定と管理
2.01.2 システム起動のカスタマイズ	2.07.2 PAM認証
2.01.3 Linux カーネルの構成要素	2.07.3 LDAPクライアントの利用方法
2.01.4 Linuxカーネルのコンパイル	2.07.4 OpenLDAPサーバーの設定
2.01.5 カーネル実行時における管理とトラブルシューティング	2.08:ドメインネームサーバー
2.02 : ファイルシステムとストレージ管理	2.08.1 BINDの設定と管理
2.02.1 ファイルシステムの設定とマウント	2.08.2 ゾーン情報の管理
2.02.2 ファイルシステムの管理	2.08.3 セキュアなDNSサーバーの実現
2.02.3 論理ボリュームマネージャの設定と管理	2.09 : HTTPサーバーとプロキシサーバー
2.03 : ネットワーク構成	2.09.1 Apache HTTPサーバーの設定と管理
2.03.1 基本的なネットワーク構成	2.09.2 OpenSSLとHTTPSの設定
2.03.2 高度なネットワーク構成	2.09.3 nginxの設定と管理
2.03.3 ネットワークの問題解決	2.09.4 Squidの設定と管理
2.04 : システムの保守と運用管理	2.10 : 電子メールサービス
2.04.1 makeによるソースコードからのビルドとインストール	2.10.1 Postfixの設定と管理
2.04.2 バックアップとリストア	2.10.2 Dovecotの設定と管理
2.04.3 ユーザへの通知	2.11:ファイル共有サービス
2.04.4 リソース使用状況の把握	2.11.1 Sambaの設定と管理
2.04.5 死活監視、リソース監視、運用監視ツール	2.11.2 NFSサーバーの設定と管理
2.04.6 システム構成ツール	2.12:システムのセキュリティ
2.05:仮想化サーバー	2.12.1 iptables や firewalld によるパケットフィルタリング
2.05.1 仮想マシンの仕組みとKVM	2.12.2 OpenSSH サーバーの設定と管理
2.05.2 仮想マシンの作成と管理	2.12.3 OpenVPNの設定と管理
2.06 : コンテナ	2.12.4 セキュリティ業務
2.06.1 コンテナの仕組み	2.13 : システムアーキテクチャ
2.06.2 Dockerコンテナとコンテナイメージの管理	2.13.1 高可用システムの実現方式
	2.13.2 キャパシティプランニングとスケーラビリティの確保
	2.13.3 クラウドサービス上のシステム構成
https://linuc.org/linuc2/range/201.html	2.13.4 典型的なシステムアーキテクチャ

https://linuc.org/linuc	2/range/201.html
https://linuc.org/linuc.	2/range/202.html















④過去セミナーの動画

<u>https://www.youtube.com/user/LPIJapan</u>1年でコンテンツが充実しましたね!

	op	en your	NEXT fu	ture OPCEL	
	Linu 頼ら	れるため	の、頼れる)資格 LP	I-JAPAN
LPI-JAPAN LPI-Japan ホーム 動画) 者数 921人 再生リスト チャ:	ンネル フリートーク	概要 Q、		チャンネ
LinuC 技術解説無料セミナー	 すべて再生 			8	
デーマ ハードディスクのレイアウトと パーティション い(-ティションの場景の解説~デモ)	デーマ 重要なシステムサービス (システムのログ)	デース システムの保守と運用管理 (リソースの使用状況の密題、監索ソール)	デーマ ファイルシステムとストレージ管打 (ファイルシステムやVPS、LVMなどの構造とデモ	デーマ 里 GNUとUnixのコマンド (コマンド、バイブ、正規表現などの解説とデモ)	デーズ アカウント管理 セキュリティ管理業
LinuCレベル1 Version10.0 技術解説無料セミナ111033 [2021/01/23]LinuC-1 技術解 説セミナー「八ードウェア	LinuCレベル1 Version104 技術解説無料セミナー [2021/1/17]LinuC-1 技術解説 セミナー「重要なシステム	LinuCレベル2 Version10.0 技術解説無料セミナ10235 [2020/12/19]LinuC-2 技術解 説セミナー「システムの保	LinuCレベル2 Version10.0 技術解説無料セミナ1112225 [2020/12/5]LinuC-2 技術解説 セミナー「ファイルシステ	LinuCレベル1 Version10.0 技術解説無料セミナー59920 [2020/11/29]LinuC-1 技術解 説セミナー「GNUとUnixの	LinuCレベル1 Versid 技術解説無料セミン [2020/11/07]LinuC-1 技 説セミナー「アカウント
LPI-Japan 62 回視聴 + 1 日前	LPI-Japan 136 回視聴・6 日前	LPI-Japan 301 回視聴・1 か月前	LPI-Japan 311 回視聴 + 1 か月前	LPI-Japan 385 回視聴・1 か月前	LPI-Japan 418 回視聴・2 か月前
HTML5 技術解説無料セミナ・	-				
<u>アーマ</u> オフライン・ストレージ系 (Web Storget ^P Indexed Database A 禁急電道とよう) HTML5プロフェッショナル認定 レー 技術解説無料セミナー	[2020/07/12]HTM 系API概要」 LPIJapan・646回視聴 当日寄せられた質問に 富士通ラーニングメデ・ 00:11	AL5-1技術解説セミナー「オ ・6 か月前 ついては、動画の最後に載せていますの ィアの紹介 02-20 HTML5ブ	ノライン・ストレージ いでご覧ください。00:00 スタート 00:	29	
OSS-DB 技術解説無料セミナ	 ・ ・ ・				
************************************	H デーズ VACUUM,ANALYZEの 目的と使い方 (原用新聞)	テーマ デーマ バックアップ方法 (運用管理)	-		

[2020/07/19]OSS-DB Silver 技術解説セミナー「運用管...

[2020/10/17]OSS-DB Silver技 [[2020/09/05]OSS-DB Silver]

技術解説セミナー「運用管...

術解説セミナー「運用管理...





LinuC





```
学習の具体的な進め方(2~3か月程度)
 試験範囲の確認(LinuC HP)
 LinuC認定教材の購入・1週目読込
 LinuC認定教材・Webサイトを参考に、実機操作(サーバ構築やコマンド操作)を試す
  ※操作やトラブルシュートで力が身に付く!
 LinuC認定教材 2週目読込
 問題集やメルマガサンプル問題で理解力確認
  ※理解不足箇所の洗い出し
 LinuC認定教材 3週目
  ※弱点の補強
 受験申込
 問題を8~9割以上、正解となるまで繰り返し解く
 苦手な部分を重点的に復習
                ・受験まで継続して学習すること
                ・繰り返し学習し、理解度/問題正解率を高めた状態で受験すること
 受験
```









主題2.11:ファイル共有サービス

<u>2.11.1 Sambaの設定と管理</u>

重要度 4

概要 さまざまなクライアント用にSambaサーバーを設定できる。これには、クライアントがログインするSambaの設定やサーバー が参加するワークグループの設定、共有ディレクトリの定義、インストールにおけるトラブルシューティングも含まれる。 詳細

Samba の設定ファイルとログファイル /etc/samba/, /var/log/samba/ Samba のユーティリティとデーモン samba, smbd, nmbd, winbindd smbcontrol, smbstatus, testparm, smbpasswd, nmblookup, net, smbclient, samba-tool Windowsのユーザ名をLinuxのユーザ名にマッピングする。 ACL および AD のセキュリティ getfacl, setfac









主題2.12 : システムのセキュリティ

2.12.1 iptables や firewalld によるパケットフィルタリング

重要度

概要 IPパケットを転送したり、ネットワークアドレス変換(NATやIPマスカレード)を実行するようシステムを設定し、ネットワークを保護することができる。これには、ポートリダイレクトの設定、フィルタルールの管理、攻撃の回避も含まれる。 詳細

iptables および ip6tables のツール

iptables, ip6tables

IPパケットの転送

3

/proc/sys/net/ipv4/, /proc/sys/net/ipv6/

ルーティングテーブルを管理するためのツール

ポートリダイレクト

発信元や宛先のプロトコルやポート、アドレスに基づいて、IPパケットの受入と拒否を行うフィルタおよびルールの表示と保存 /etc/services

フィルタ設定の保存および再読込

iptables-save, iptables-restore

firewalld で設定の確認と変更ができる。

firewalld, firewall-cmd

ufw で設定の確認と変更ができる。

ufw









Sambaの歴史





LinuC





1992年 Andrew Tridgell氏により作成



(<u>https://www.samba.org/~tridge/</u>)

- 1994年 日本語サポートパッチ追加
- 1999年 Samba2.0.0リリース 日本Sambaユーザ会設立(<u>http://www.samba.gr.jp/</u>)
- 2001年 Samba2.2.0リリース Windows NTドメインコントローラ機能追加
- 2003年 Samba3.0.0リリース Active Directoryクライアント機能追加
 - NTFSサポートなど各種機能追加
- 2006年 Active Directoryドメインコントローラ機能の追加がはじまる
- 2012年 Samba4.0.0リリース Active Directoryドメインコントローラ機能追加

C 2021年1月 最新バージョンは Samba4.13.4(<u>https://www.samba.org/samba/history/</u>)







Sambaとは



 $^{\odot}$ LPI-Japan / EDUCO all rights reserved. 15



LinuC





Sambaとは

- "LinuxなどのUnix系サーバでWindowsサーバ機能を実装させるソフトウェア"
- ⇒ 周りのWindowsからみると、仲間がいるようにみえる!









Sambaの機能

- ▶ ファイルサーバ機能 共有フォルダ提供、そのフォルダに関するアクセス制御などWindows共有と同等の機能を提供
- ▶ プリントサーバ機能 Windowsネットワークにおけるネットワークプリンタ機能を提供
- ▶ ネットワーク機能 WindowsネットワークにおけるSambaの表示や名前解決を提供
- ▶ ドメインコントローラ機能 Active DirectoryやNTドメインのドメインコントローラ機能(認証統合)を提供
- ▶ ファイル共有クライアント機能 Windowsクライアントのように振舞い共有へアクセスする機能









Sambaを構成するデーモン

➤ smbd

ファイル共有やSambaの多くの部分を担当(139/tcp・445/tcp)

➤ nmbd

Windowsネットワークにおける名前解決、ブラウジング機能などを担当(137/udp・138/udp)

➤ winbindd

NSS(Name Server Switch)機能を担当 ※Windowsドメインとのユーザアカウントの統合

その他(Active Directoryドメイン関連)
 LDAP、Kerberos、DNS、NTPなど









Sambaのインストール









Sambaのインストール

- CentOS7/8などRPM系
 yum install samba samba-client
- > UbuntuなどDebian系 sudo apt(apt-get) update sudo apt(apt-get) install samba

※色々な機能を有しているSambaなので、 依存パッケージが多くあります。 ubuntu@ubuntu:~\$ **sudo apt upgrade samba** パッケージリストを読み込んでいます... 完了 依存関係ツリーを作成しています 状態情報を読み取っています... 完了

以下のパッケージが新たにインストールされます: libllvm11 liblzf1 linux-headers-5.8.0-40-generic linux-hwe-5.8-headers-5.8.0-40 linux-image-5.8.0-40-generic linux-modules-5.8.0-40-generic linux-modules-extra-5.8.0-40-generic 以下のパッケージはアップグレードされます: apt apt-transport-https apt-utils brave-browser dnsmasg-base firefox firefox-locale-en firefox-locale-ja gir1.2-mutter-6 grub-common grub-pc grub-pc-bin grub2-common libapt-pkg6.0 libasound2 libasound2-data libatopology2 libc-bin libc-dev-bin libc6 libc6-dbg libc6-dev libcephfs2 libdrm-amdqpu1 libdrm-common libdrm-intel1 libdrm-nouveau2 libdrm-radeon1 libdrm2 libegl-mesa0 libegl1 libgbm1 libgl1 libgl1-mesa-dri libglapi-mesa libgles2 libglvnd0 libglx-mesa0 libglx0 libmutter-6-0 libnetplan0 libnss-systemd libopenjp2-7 libp11-kit0 libpam-systemd libproxv1-plugin-gsettings libproxv1-plugin-networkmanager libproxv1v5 libpulse-mainloop-glib0 libpulse0 libpulsedsp librados2 libsystemd0 libtracker-control-2.0-0 libtracker-miner-2.0-0 libtracker-sparal-2.0-0 libudev1 libwavpack1 libxatracker2 linux-firmware linux-generic-hwe-20.04 linux-headers-generic-hwe-20.04 linux-image-generic-hwe-20.04 linux-libc-dev locales Ishw Isof mesa-va-drivers mesa-vdpau-drivers mesa-vulkan-drivers mutter mutter-common nautilus-sendto netplan.io p11-kit p11-kit-modules pulseaudio pulseaudio-module-bluetooth pulseaudio-utils python-apt-common python3-apt python3-distupgrade python3-pil python3-update-manager sudo systemd systemd-sysv systemd-timesyncd tar tracker tzdata ubuntu-drivers-common ubuntu-release-upgrader-core ubuntu-release-upgrader-gtk udev update-manager update-manager-core update-notifier update-notifier-common virtualbox virtualbox-dkms virtualbox-qt xdg-utils xserver-common xserver-xephyr xserver-xorg-core xserver-xorg-legacy xwayland アップグレード: 108 個、新規インストール: 7 個、削除: 0 個、保留: 0 個。 448 MB 中 383 MB のアーカイブを取得する必要があります。 この操作後に追加で 536 MB のディスク容量が消費されます。

続行しますか? [Y/n] y









Sambaの設定



© LPI-Japan / EDUCO all rights reserved. 21







Sambaの設定は、 "smb.conf" で行う。

ubuntu@ubuntu:~\$ cat -n /etc/samba/smb.conf 23 24 [global] セクション 25 26 ## Browsing/Identification ### 27 28 # Change this to the workgroup/NT-domain name your Samba server will part of workgroup = WORKGROUP 29 変数 30 31 # server string is the equivalent of the NT Description field server string = %h server (Samba, Ubuntu) 32









セクションについて

- ▶ [global] Sambaのグローバル設定を記述する
- ▶ [homes] ユーザのホームディレクトリに関する設定を記述する
- ▶ [printers] 共有プリンターに関する設定を記述する
- ▶ [文字列] 指定文字列名の共有を作成し、その共有設定を記述する
- ▶ [文字列\$]

共有名の最後に "\$"を付与すると隠し共有(通常非表示で共有名を手入力で指定した者のみアクセス可能)となる









変数について

≻ %h

Samba が動作しているマシンの インターネットホスト名。

≻ %H

```
%u で指定されたユーザーのホームディレクトリ。
```

≽ %u

現在のサービスのユーザー名 (存在する場合)。

≻ %U

セッションのユーザー名 (クライアントが接続時に 送信したものであるが、実際に接続したユーザー名と同じであるとは 限らない)。

≻ %S

現在のサービス名 (存在する場合)。

≻ %m

クライアントマシンの NetBIOS 名。

≻ %I

クライアントマシンの IP アドレス。

≻ %i

クライアントが接続してきたサーバーの IP アドレス。

≻ %G

%U のプライマリグループ。

≻ %g

LinuC

~%u のプライマリグループ。

http://www.samba.gr.jp/project/translation/current/htmldocs/manpages/smb.conf.5.html







パラメータについて

- workgroup = ワークグループ名
 Windowsネットワークで使われるワークグループ名を指定
- netbios name = 名前
 Windowsネットワークで利用される名前の指定
- ➤ valid users = ユーザ名

共有ヘアクセス可能なユーザを指定 複数ユーザ記載する場合、",(カンマ)"で区切る

- browseable = yes/no
 共有を表示させる/表示させない
- path = 共有のパス
 共有の場所を示す
- ▶ read only = yes/no 読み取り専用かどうか
- guest ok = yes/noゲストアクセスの可否
- hide dot files = yes/no
 - ".(ドット)で始まるファイルを表示する/しない





LinuC





smb.confへのパラメータ設定時の注意



このパラメーターは右記のパラメーターの別名である:guest ok.

guest ok (S)

このパラメーターが yes のサービスに付いては、サービスへの接続の際にパスワードが要求されない。この場合、guest account の権限で操作が行われる。

このパラメーターは restrict anonymous = 2 のメリットを無効にする。

このオプションに関する詳細については、<u>security</u>セクションを参照のこと。

既定值: guest ok = no



http://www.samba.gr.jp/project/translation/current/htmldocs/manpages/smb.conf.5.html







Samba(smb.conf)の設定確認

➤ testparmコマンド

ubuntu@ubuntu:~\$ testparm Load smb config files from /etc/samba/smb.conf -v:デフォルト値を含めて表示する Unknown parameter encountered: "readeable" Ignoring unknown parameter "readeable" Loaded services file OK. Server role: ROLE STANDALONE Press enter to see a dump of your service definitions _ Enterを押すと、 # Global parameters [global] log file = /var/log/samba/log.%m $\log g = file$ map to guest = Bad User $max \log size = 1000$ obey pam restrictions = Yes pam password change = Yes panic action = /usr/share/samba/panic-action %d passwd chat = *Enter¥snew¥s*¥spassword:* %n¥n *Retype¥snew¥s*¥spassword:* %n¥n *password¥supdated¥ssuccessfully*. passwd program = /usr/bin/passwd %u server role = standalone server server string = %h server (Samba, Ubuntu) unix password sync = Yes usershare allow quests = Yesidmap config * : backend = tdb

testparmコマンドオプション -s:内容確認のEnter押下を求めない

デフォルト値以外のパラメーター覧が出力される









Samba(smb.conf)の設定確認

▶ testparmコマンド



Global parameters [global] log file = /var/log/samba/log.%m









Sambaのユーザ管理



© LPI-Japan / EDUCO all rights reserved. 29







Sambaのユーザ管理

以下の順で実施する

- ① Linuxユーザ追加 (useradd/passwd)
- ② Sambaユーザ追加 (pdbedit)

pdbeditコマンドオプション			
-a :ユーザ追加			
-x : ユーザ削除			
-L : Sambaユーザー覧表示			

LinuxユーザとSambaユーザの情報は 別々に管理されている!

ubuntu@ubuntu:~\$ sudo useradd ichiro ubuntu@ubuntu:~\$ sudo passwd ichiro
新しいパスワード:
新しいパスワードを再入力してください:
passwd: パスワードは正しく更新されました

```
ubuntu@ubuntu:~$ sudo pdbedit -a ichiro
new password:
retype new password:
Unix username:
                   ichiro
NT username:
Account Flags:
                  ΓU
User SID:
                S-1-5-21-2101493541-2007677032-2764911150-1001
Primary Group SID: S-1-5-21-2101493541-2007677032-2764911150-513
Full Name:
Home Directory:
                   ¥¥ubuntu¥ichiro
HomeDir Drive:
Logon Script:
Profile Path:
                ¥¥ubuntu¥ichiro¥profile
Domain:
                 ubuntu
```









システムのセキュリティ



© LPI-Japan / EDUCO all rights reserved. 31







ファイアウォール(firewalld)

- ➢ 設定状況確認 firewall-cmd --list-all
- ▶ 設定追加(TCP139を開放する場合) firewall-cmd --add-port=139/tcp --permanent systemctl reload firewalld

ubuntu@ubuntu:~\$ sudo firewall-cmdadd-port=139/tcppermanent
success ubuntu@ubuntu:~\$ sudo systemctl reload firewalld ubuntu@ubuntu:~\$ sudo firewall-cmdlist-all
public target: default
icmp-block-inversion: no interfaces:
sources:
services: dhcpv6-client ssh ports: 139/tcp
protocols: masquerade: no forward-ports:
source-ports: icmp-blocks: rich rules:



firewall-cmd⊐マ	' ンドオプション
list-all	: 設定一覧
permanent	:永続的に追加
add-port	:解放ポート追加
remove-port	:解放ポート削除
add-service	:解放サービス追加
remove-service	:解放サービス削除









ファイアウォール(firewalld)

- ▶ /usr/lib/firewalld/servicesディレクトリにあるサービス用の設定ファイルが用意されている Sambaの場合、samba.xml
- ▶ 設定追加(Sambaサービスを開放する場合)

firewall-cmd --add-service=samba -permanent systemctl reload firewalld

```
ubuntu@ubuntu:~$ ls /usr/lib/firewalld/services/ | grep samba
                                                                      ubuntu@ubuntu:~$ sudo firewall-cmd --add-service=samba --
samba-client.xml
                                                                      permanent
samba-dc.xml
                                                                      success
samba.xml
                                                                      ubuntu@ubuntu:~$ sudo systemctl reload firewalld
                                                                      ubuntu@ubuntu:~$ sudo firewall-cmd --list-all
ubuntu@ubuntu:~$ cat /usr/lib/firewalld/services/samba.xml
                                                                      public
<?xml version="1.0" encoding="utf-8"?>
                                                                       target: default
<service>
                                                                       icmp-block-inversion: no
 <short>Samba</short>
                                                                       interfaces:
 <description>This option allows you to access and participate in Windows sources:
  file and printer sharing networks. You need the samba package installed
                                                                       services: dhcpv6-client samba ssh
  for this option to be useful.</description>
                                                                       ports: 139/tcp
 <port protocol="udp" port="137"/>
                                                                       protocols:
 <port protocol="udp" port="138"/>
                                                                       masquerade: no
 <port protocol="tcp" port="139"/>
                                                                       forward-ports:
                                                                                                     追加されたサービス設定
 <port protocol="tcp" port="445"/>
                                                                       source-ports:
 <helper name="netbios-ns"/>
                                                                       icmp-blocks:
</service>
                                                                       rich rules:
```









ファイアウォール(ufw) ※Uncomplicated Firewallの略

➢ 設定状況確認 ufw status / ufw status verbose

▶ 設定追加(TCP139を開放する場合) ※ufwプロセス起動が前提

ufw enable

ufw default deny ufw allow 139/tcp ubuntu@ubuntu:~\$ **sudo ufw enable** Command may disrupt existing ssh connections. Proceed with operation (y|n)? y

ファイアウォールはアクティブかつシステムの起動時に有効化されます。 ubuntu@ubuntu:~\$ sudo ufw allow 139/tcp ルールを追加しました ルールを追加しました (v6) ubuntu@ubuntu:~\$ sudo ufw status verbose 状態: アクティブ ロギング: on (low) Default: deny (incoming), allow (outgoing), disabled (routed) 新しいプロファイル: skip

То	Action	From
22/tcp	ALLOW	IN Anywhere
139/tcp	ALLOW	/ IN Anywhere
22/tcp (v6)	ALLOV	W IN Anywhere (v6)
139/tcp (v6)	ALLO\	W IN Anywhere (v6)

https://help.ubuntu.com/community/UFW

http://manpages.ubuntu.com/manpages/bionic/man8/ufw.8.html









ファイアウォール(ufw) ※Uncomplicated Firewallの略

▶ 設定追加(Sambaサービスを開放する場合) ufw allow samba

ubuntu@ubuntu:~\$ sudo ufw app list

利用可能なアプリケーション:

CUPS

- Nginx Full
- Nginx HTTP
- Nginx HTTPS
- OpenSSH

Samba

ubuntu@ubuntu:~\$ sudo ls /etc/ufw/applications.d/

cups nginx openssh-server samba

ubuntu@ubuntu:~\$ sudo cat /etc/ufw/applications.d/samba [Samba]

title=LanManager-like file and printer server for Unix

description=The Samba software suite is a collection of programs that implements the SMB/CIFS protocol for unix systems, allowing you to serve files and printers to Windows, NT, OS/2 and DOS clients. This protocol is sometimes also referred to as the LanManager or NetBIOS protocol. ports=137,138/udp|139,445/tcp ubuntu@ubuntu:~\$ sudo ufw allow samba

ルールを追加しました

ルールを追加しました (v6)



ubuntu@ubuntu:~\$ **sudo ufw status verbose** 状態: アクティブ ロギング: on (low) Default: deny (incoming), allow (outgoing), disabled (routed) 新しいプロファイル: skip

То	Action	From	
22/tcp	ALLOW	/IN Anyv	where
139/tcp	ALLOV	V IN Any	where
137,138/udp	(Samba)	ALLOW IN	Anywhere
139,445/tcp	(Samba) A	ALLOW IN	Anywhere
22/tcp (v6)	ALLO'	W IN Any	where (v6)
139/tcp (v6)	ALLC	WIN An	ywhere (v6)
137,138/udp	(Samba (v6))	ALLOW I	Anywhere (v6)
139,445/tcp	(Samba (v6))	ALLOW IN	Anywhere (v6)

https://help.ubuntu.com/community/UFW

http://manpages.ubuntu.com/manpages/bionic/man8/ufw.8.html







Linuxセキュリティモジュール

> SELinux

ログ出力モード or 無効化に変更 setenforce 0 vi /etc/sysconfig/selinux にて、SELINUX=permissive(もしくは、disable)とする

> AppArmor

Sambaを動作させるのに影響ないと思いますが、影響あった場合以下(無効化)を実施。 sudo systemctl disable apparmor sudo systemctl reboot









Sambaの起動









smb/nmbの両プロセスを起動します

Main PID: 44508 (nmbd)

```
ubuntu@ubuntu:~$ sudo systemctl start smbd
ubuntu@ubuntu:~$ sudo systemctl start nmbd
ubuntu@ubuntu:~$ sudo systemctl status smbd nmbd

    smbd.service - Samba SMB Daemon

   Loaded: loaded (/lib/systemd/system/smbd.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2021-01-28 19:19:01 JST; 15s ago
    Docs: man:smbd(8)
        man:samba(7)
        man:smb.conf(5)
  Process: 44476 ExecStartPre=/usr/share/samba/update-apparmor-samba-profile (code=exited,
status=0/SUCCESS)
  Main PID: 44498 (smbd)
   Status: "smbd: ready to serve connections..."
   Tasks: 4 (limit: 14233)
   Memory: 8.7M
   CGroup: /system.slice/smbd.service
        ta44498 /usr/sbin/smbd --foreground --no-process-group
        tq44500 /usr/sbin/smbd --foreground --no-process-group
        tq44501 /usr/sbin/smbd --foreground --no-process-group
        mg44503 /usr/sbin/smbd --foreground --no-process-group
1月 28 19:19:01 ubuntu systemd[1]: Starting Samba SMB Daemon...
1月 28 19:19:01 ubuntu systemd[1]: Started Samba SMB Daemon.
• nmbd.service - Samba NMB Daemon
   Loaded: loaded (/lib/systemd/system/nmbd.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2021-01-28 19:19:03 JST; 13s ago
    Docs: man:nmbd(8)
        man:samba(7)
        man:smb.conf(5)
```









動作確認

Windowsのエクスプローラにて、<u>¥¥SambaのIPアドレス</u>を実施



共有(Samba)にアクセスできた!









Samba関連コマンド









smbstatus

▶ 現在のSamba接続情報を表示

ubuntu@ubuntu:~\$	sudo	smbstatus
-------------------	------	-----------

Samba	Samba version 4.11.6-Ubuntu						
PID	Username	Group	Machine	Protocol Version Encryption	Signing		
44559	ubuntu	ubuntu	192.168.1.131 (ipv	/4:192.168.1.131:53748) SMB3_11		partial(AES-128-CMAC)	
Service	e pid	Machine	Connected at	Encryption Signing			
IPC\$	44559	192.168.1	.131 土 1月 30 19時2	1分31秒 2021 JST			

No locked files









smbcontrol

▶ smbd・nmbd・winbinddのプロセスにメッセージを送信する ※クライアント接続を切断する例

Samba PID	version 4. Username	11.6-Ubuntu. Group	Machine	Protocol Version Encryption	Signing	
44559	ubuntu	ubuntu	192.168.1.131	l (ipv4:192.168.1.131:53748) SMB3_11	-	partial(AES-128-CMAC)
Service	e pid	Machine	Connected at	Encryption Signing		
IPC\$	44559	192.168.1	.131 土 1月 30 1	.9時21分31秒 2021 JST		
No loc	ked files					
ubuntu ubuntu	ı@ubuntu: ı@ubuntu:	~\$ sudo sm ~\$ sudo sm	bcontrol 44559 bstatus	close-share IPC\$		
Samba PID	version 4. Username	.11.6-Ubuntu Group	Machine	Protocol Version Encryption	Signing	
44559	ubuntu	ubuntu	192.168.1.131	l (ipv4:192.168.1.131:53748) SMB3_11	-	partial(AES-128-CMAC)
Service	e pid	Machine	Connected at	Encryption Signing		

No locked files

http://www.samba.gr.jp/project/translation/4.0/htmldocs/manpages/smbcontrol.1.html









nmblookup

▶ NetBIOS 名を検索やマスターブラウザの表示など

ubuntu@ubuntu:~\$ **sudo nmblookup ubuntu** 192.168.1.237 ubuntu<00>

ubuntu@ubuntu:~\$ **sudo nmblookup -A 192.168.1.237** Looking up status of 192.168.1.237

ubuntu	<00> -	B <active></active>
ubuntu	<03> -	B <active></active>
ubuntu	<20> -	B <active></active>

ubuntu@ubuntu:~\$ **sudo nmblookup -M workgroup** 192.168.1.237 workgroup<1d>









smbclient

⋟ smbクライアントコマンド

ubuntu@ubuntu:~\$ **sudo smbclient //192.168.1.237/DVDDrive -U ichiro** Enter WORKGROUP¥ichiro's password: Try "help" to get a list of possible commands. smb: ¥>



http://www.samba.gr.jp/project/translation/3.6/htmldocs/manpages-3/smbclient.1.html







smbpasswd

> pdbeditで作成したユーザのパスワード変更やユーザの有効化/無効化など

\$ smbpasswd Old SMB password: New SMB password: Retype new SMB password: Password changed for user taro











Windowsのnetコマンド

⋟ smbクライアントコマンド

C:¥Users¥jiro>**net use** 新しい接続は記憶されません。

ステータス ローカル名 リモート名 ネットワーク名

OK ¥¥192.168.1.237¥IPC\$ Microsoft Windows Network コマンドは正常に終了しました。

C:¥Users¥jiro>**net use ¥¥192.168.1.237¥IPC\$ /delete** ¥¥192.168.1.237¥IPC\$ が削除されました。

C:¥Users¥jiro>**net use** 新しい接続は記憶されません。

一覧にエントリが存在しません。



https://docs.microsoft.com/ja-jp/troubleshoot/windows-server/networking/net-commands-on-operating-systems







samba-tool

▶ ドメインコントローラ管理で使用するツール(ドメイン構築・ドメインユーザ管理)

LinuC300に関するセミナー資料(<u>https://lpi.or.jp/news/event/docs/20170218_lpic300.pdf</u>)の P69・76を参照

※Sambaを使ったActive Directoryドメインコントローラ構築に興味がある方は上記リンクをご確認ください。









Appendix









Sambaパスワードを変更した際に、Linuxユーザパスワードも同期させる

 smb.confに以下を設定する unix password sync = Yes pam password change = Yes

なお、Sambaの仕様のため、root権限のあるユーザではなく、パスワード変更は一般ユーザで実施すること

amba	Root ユーザで unix password sync オプションが動作しない						
◆ユーザ会	対象		J0017				
	この文書は、以下のプロダクトに付いて説明したものです。	最終更新日	2001/03/17				
	Samba 2.0.x	作成者	たかはしもとのぶ				
メインページ Sambaとは	状況	最終更新者					
 メーリングリスト iamba技術情報 マニュアル(4.13.2対 5) 	unix password sync = yes の環境で、root 権限のあるユーザでパスワードを変更すると、UNIX 側のパスワードが同期して変更されません。						
, ニュアル(旧ver) ニュアル(3.6.22対) 式のSamba3- DWTO(6版:4.6.6	これは Samba の仕様です。 root 権限のあるユーザが smbpasswd コマンドを呼び出す場合は、一般ユーザが smbpasswd コマンドを呼び出す場合と異なり、直接 smbpasswd ファイルを更新します。この処理では unix password sync オプションは考慮されていないため、UNIX 側のパスワードは同期されません。						

%AA%E3%83%97%E3%82%B7%E3%83%A7%E3%83%B3%E3%81%8C%E5%8B%95%E4%BD%9C%E3%81%97%E3%81%AA%E3%81



%84







その他、サンプル設定

Samba動作PCに搭載されているDVDドライブを共有する ※タブレットPCなどでDVDドライブがないケースなどを \geq 想定

[DVDDrive] path = /media/ubuntu acl allow execute always = yes ・・・共有上のすべてのファイルを実行できるようにする read only = No browseable = yes locking = no ・・・排他制御の実施/未実施 quest ok = yesroot preexec = /bin/mount /dev/sr0 /media/ubuntu root postexec = /bin/umount /media/ubuntu

- ・・・共有へ接続前にrootとして実行する内容
- ・・・共有から接続した後にrootとして実行する内容

利用ユーザを制限した共有作成 \geq [share]

path = /shareread only = yes browseable = yes valid users = ubuntu,ichiro









本日のまとめ









- Samba
 - ▶ 役割/機能
 - ≻ 設定(smb.conf)
 - ▶ ユーザ管理
 - ▶ 関連コマンド
 - ▶ サンプルコンフィグ
- ・ システムセキュリティ
 - ➤ firewalld
 - ≻ ufw









Q & A







Thank you for join today's seminar!





https://www.opensourcetech.tokyo/ https://twitter.com/matt_zeus

https://www.facebook.com/takahiro.kujirai.1