評価ガイド
ntopng and nProbe

Rev2.0

2024年1月4日

ジュピターテクノロジー

変更履歴

版	発行日	変更内容
第 1.0 版	2020/02/07	初版作成
第 1.1 版	2020/02/13	ntopng and nProbeのモデルを追加
第 1.3 版	2020/04/28	OVAを提供する方式に変更。評価は、Oracle VB + ovaに統一した
第 1.4 版	2020/6/15	™の削除, p6にisoファイルリリースのリンクを追加
第 1.5 版	2022/10/03	GPGキー変更にともなうアップグレード方法を追記
第 2.0 版	2024/1/4	v6.0リリース及び新規ISOリリースに伴う変更

ntop社 ntopng及びnProbeの評価をご検討頂き、誠にありがとうございます。

本ガイドではntop社の両製品を評価していただく為に、インストール・基本的な設定手順及び留意事項を説明いたします。

目　次

1. はじめに

ntop社のntopng及びnProbeは、高速でトラフィック情報を分析し対象ネットワークの監視を実現する製品です。製品ごとに役割が異なります。以下に製品概要を説明します。

- ntopng・・・リアルタイム性が高いL7高速トラフィック分析を実現し、フローコレクターとして長期のトラフィック分析ができます。ルーターやスイッチのミラーポート、もしくはRITEポート、TAPと直接接続することで、高速のトラフィック分析ツールとして動作します。また、nProbeと連携することで監視対象ルーターが分散した環境でもNetFlow v5,v9/IPFIXによるトラフィック分析が可能となる高速トラフィック分析ツールです。

- nProbe ・・・xFlowに対応していないルーターを補助するNetFlowプローブ製品です。モードが3種類あり、NetFlowプローブのProbeモード、MySQL/DiskにNetFlowデータを収集するコレクタモード、受信したxFlowをNetFlow v5,v9/IPFIXに変換してコレクタに送信するProxyモードの3モードをサポートします。

本評価ガイドでは、Vmware Workstation Player/物理環境で各製品の評価ができるよう、ご紹介しております。

2. ntopng and nProbe 評価版について

評価版について

◆本評価マニュアルでは、弊社が提供するISOファイルを使って、VMware Workstation/物理環境上に評価環境をセットアップする方法をご紹介します。

注意）インストールは、インターネット環境が必須となります。

◆評価版利用上の注意

ntopngは起動から10分間経過するとコミュニティ版にダウングレード、nProbeは25,000フローを受信した時点でフローの受信を停止します。有償版での検証を進めるには、適宜それぞれのプロセスを定期的に再起動して、ご評価願います。

◆評価用ISOファイルの入手について

評価版ISOファイルのご利用は、弊社までお申し込み下さい。

[評価版リクエストサイト]

https://www.jtc-i.co.jp/support/download/

評価版システム要件

◆ ntopng及びnProbeのISOをインストールするシステム要件は、以下の通りです。

CPU	メモリ	HDD
2コア以上の割り当て	4GB以上の割り当て	20GB以上の割り当て

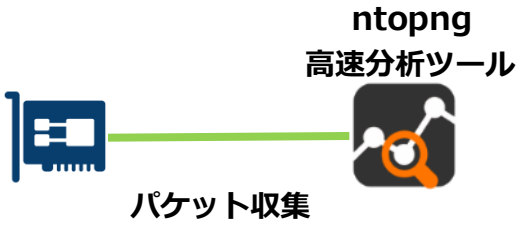
上記記載の要件はISO評価版を動作させるのに必要な最低要件となります。高負荷環境を想定しているシステム要件ではございませんので、ご注意ください。

ntopngにアクセスする場合は、WEBブラウザが必要となります。
弊社では、Google Chromeの最新版を推奨いたします。

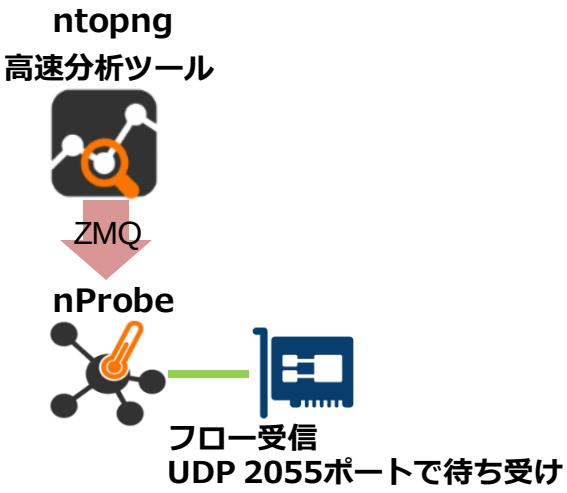
評価版ISOファイルの構成

弊社が提供するISOファイルを使ってインストールすれば、以下の2パターンの評価が出来ます。1つ目は自PCのNICを流れるトラフィックを監視をする「NIC直接監視」の評価。2つ目は、NetFlowやsflowを受信する「xFlow受信」の評価となります。

評価パターン①
ntopngのNIC直接監視の評価
※本評価ドキュメントの5章～7章までの評価環境



評価パターン②
ntopng+nProbe xFlow受信の評価
※本評価ドキュメント8章の評価環境



3. ISOインストール

本章では以下のバージョンを使用しています。

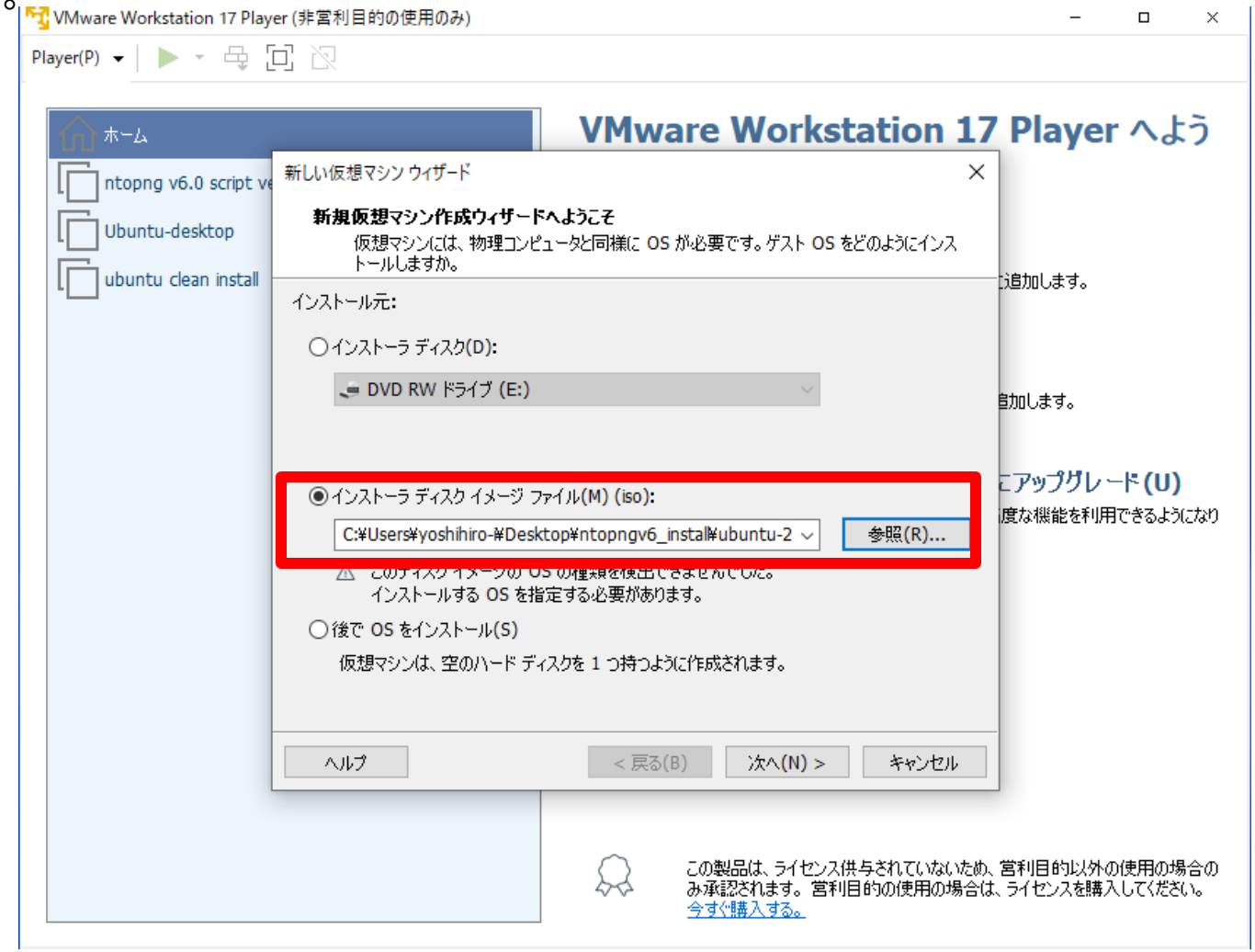
◆Windows 11 x64
◆nProbe 10.X and ntopng v6.X Stable版
◆VMware Workstation 17

ISOインストール(1)

「新規マシンの作成(N)」をクリックしてください。

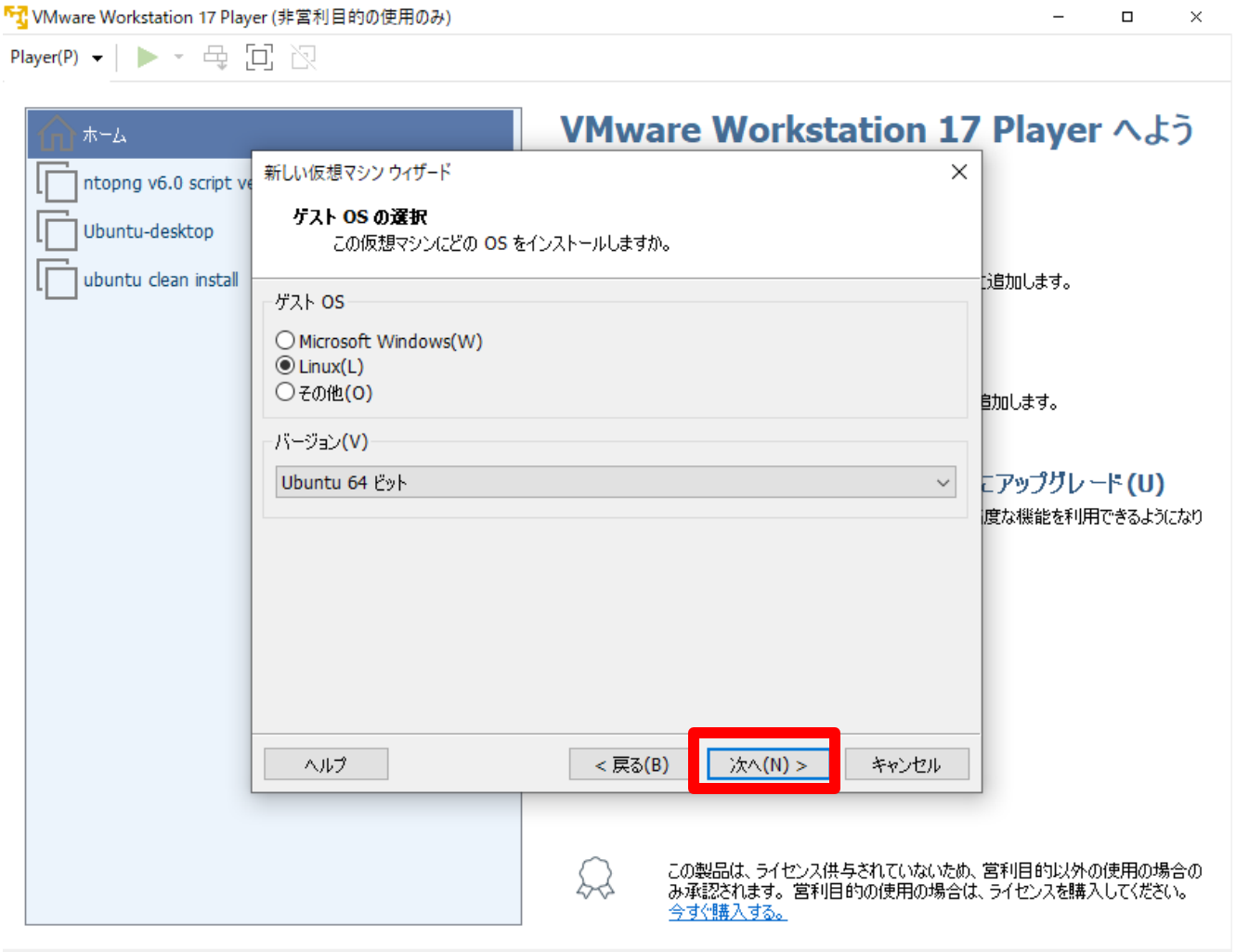
ISOインストール(2)

「**参照(R)**」をクリックし、弊社サイトからダウンロードしたisoファイルを選択して、「次(N)>」をクリックします。



ISOインストール(3)

「Linux(L)」、「Ubuntu 64ビット」が選択されていることを確認し、「次(N)>」をクリックします。

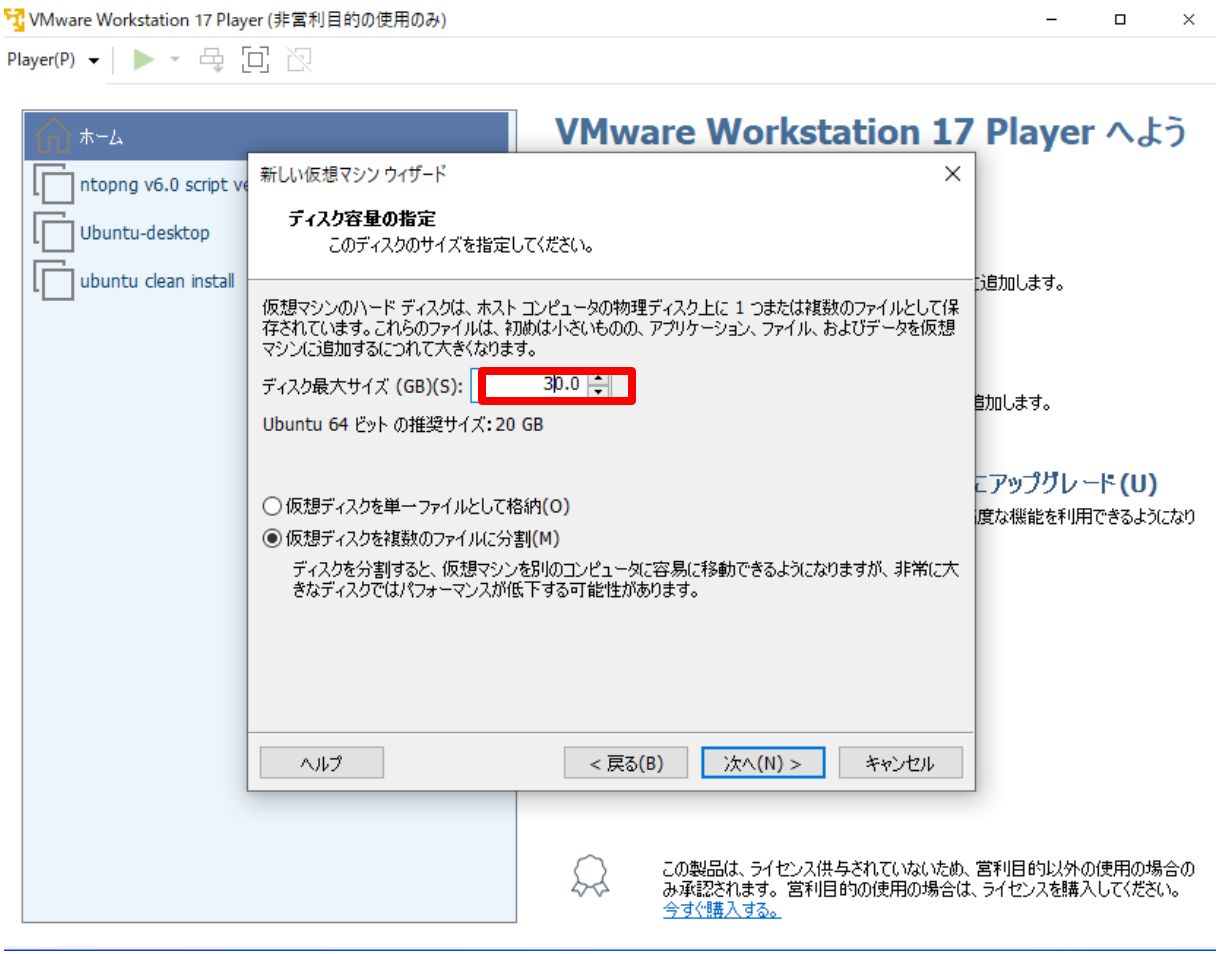


ISOインストール(4)

仮想マシン名に任意の名称、場所には仮想マシンを保存するディレクトリを指定してください。
「次(N)>」をクリックします。

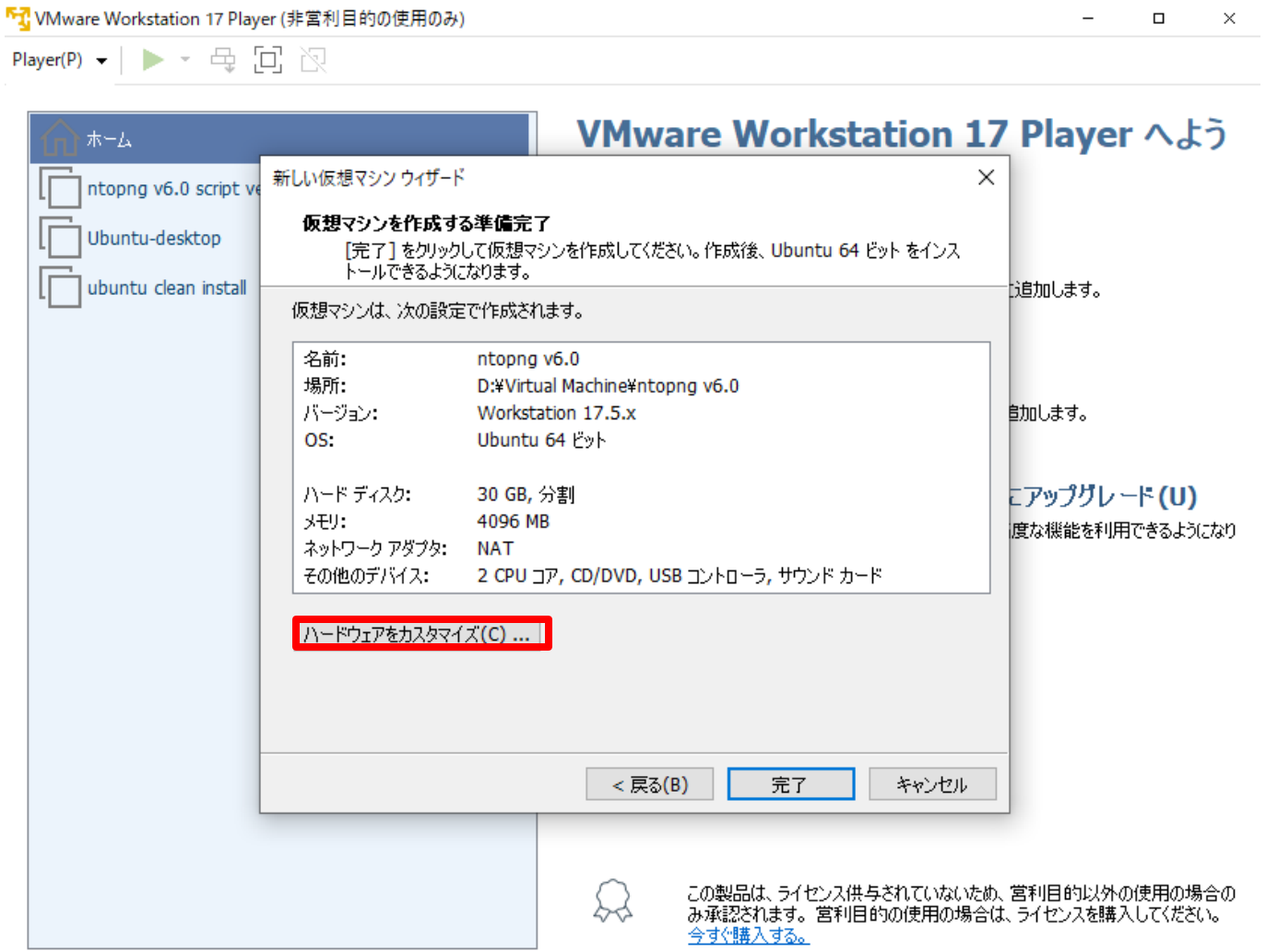
ISOインストール(5)

ディスク最大サイズ(GB)(S)を30.0に設定し、「次(N)>」をクリックします。



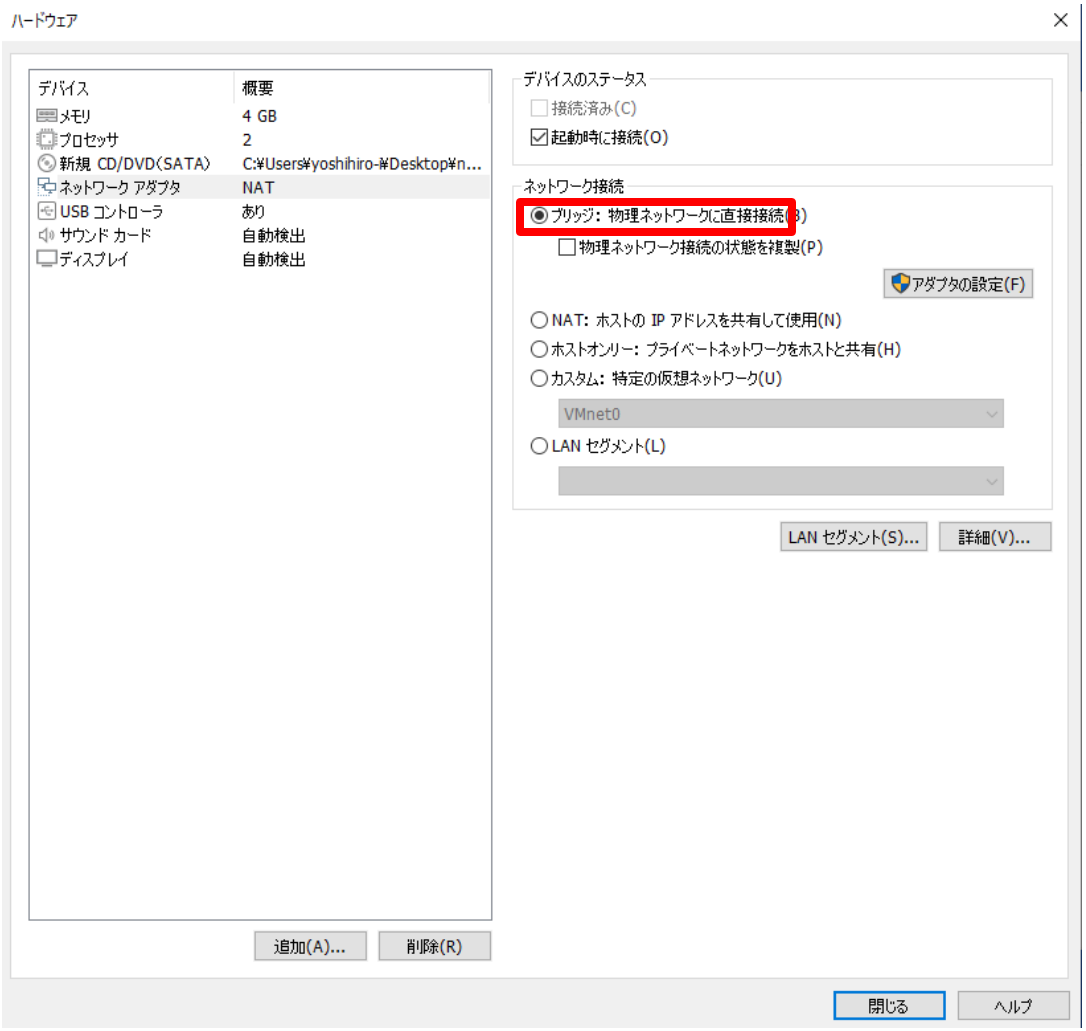
ISOインストール(6)

ハードウェアをカスタマイズ(C)... をクリックします。



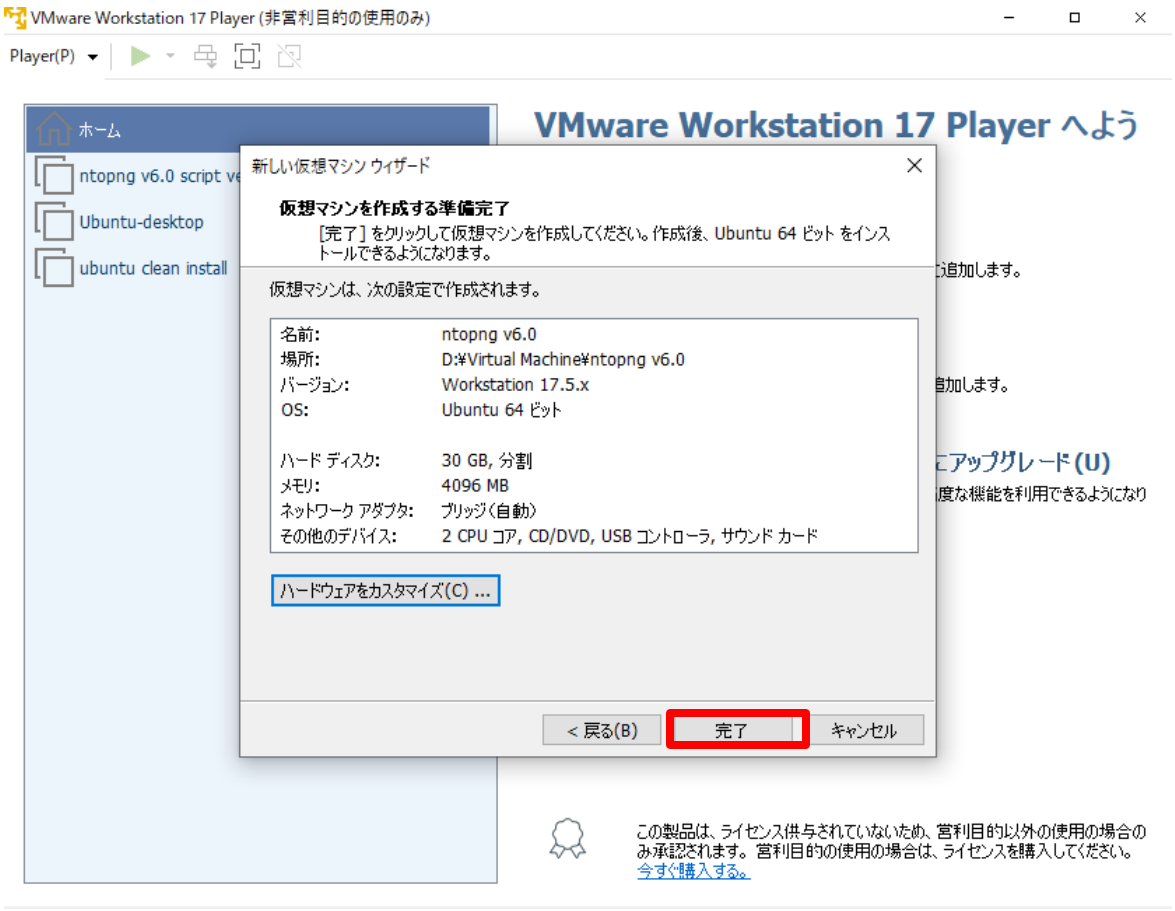
ISOインストール(7)

ブリッジをクリックし、「閉じる」ボタンをクリックします。



ISOインストール(8)

ネットワークアダプタが、”ブリッジ(自動)”なっていることを確認し、「完了」ボタンをクリックします。

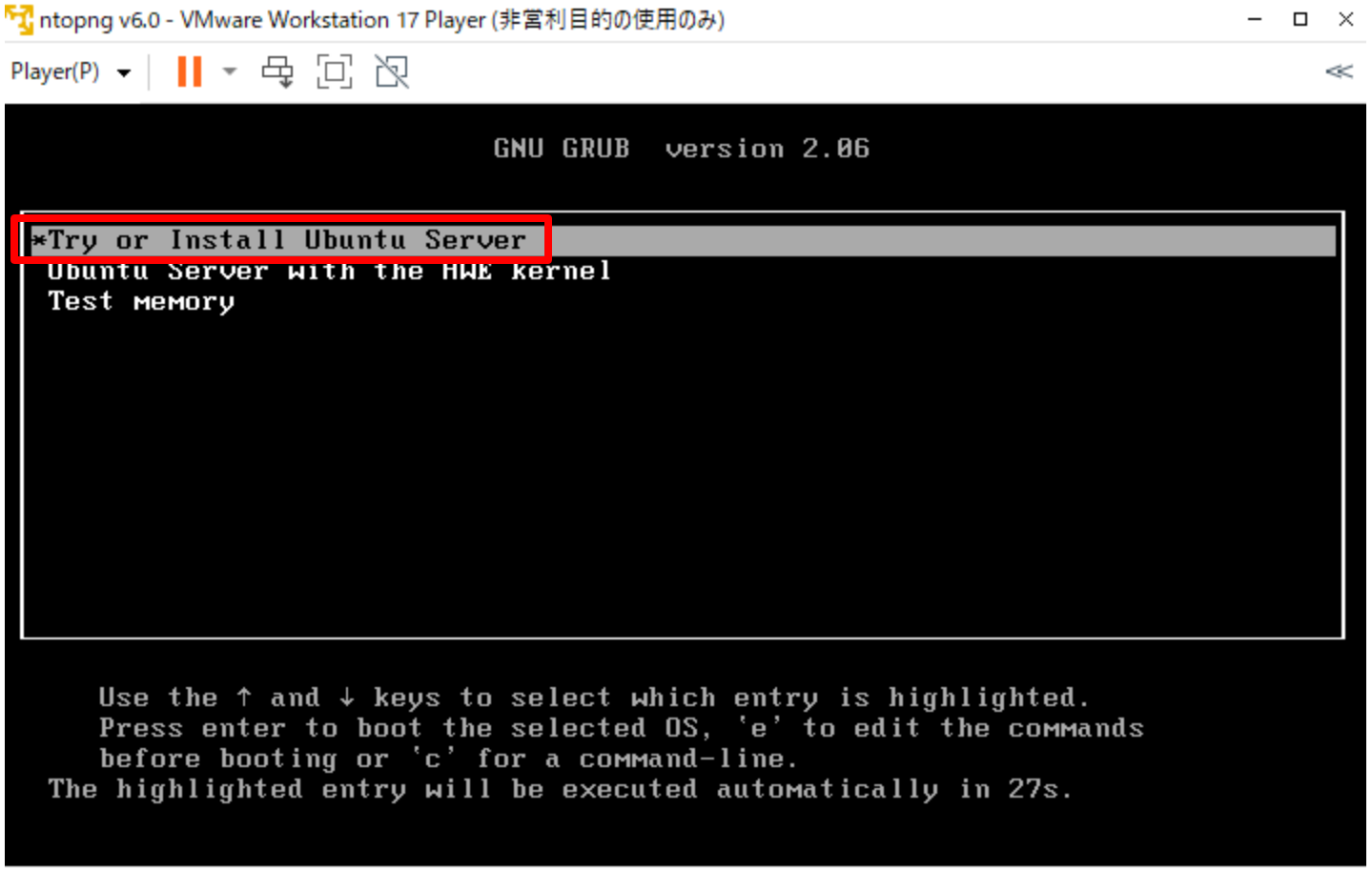


ISOインストール(9)

「仮想マシンの再生(L)」ボタンをクリックします。

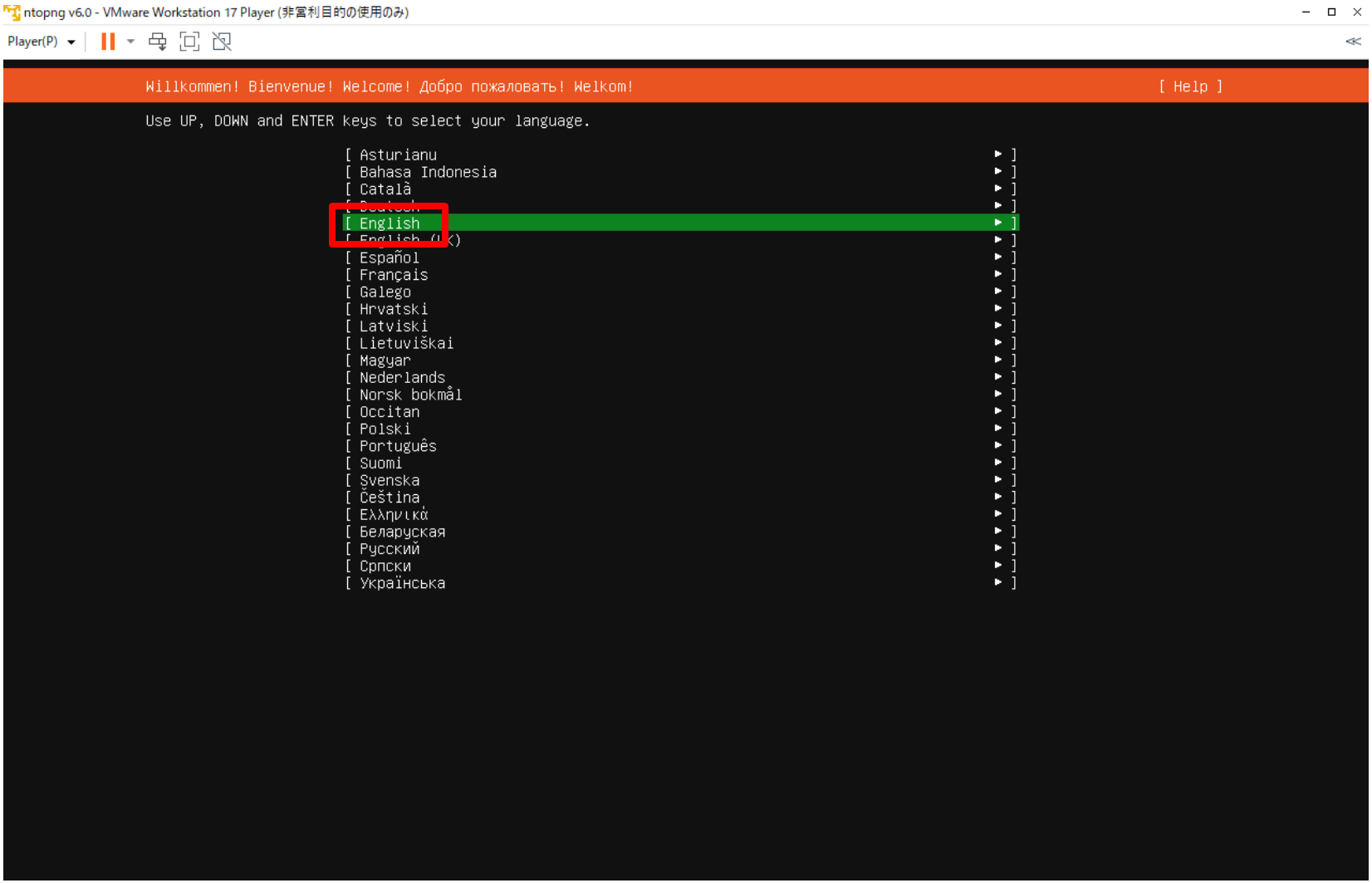
ISOインストール(10)

「*Try or Install Ubuntu Server」が選択されていることを確認し、Enterを押します。



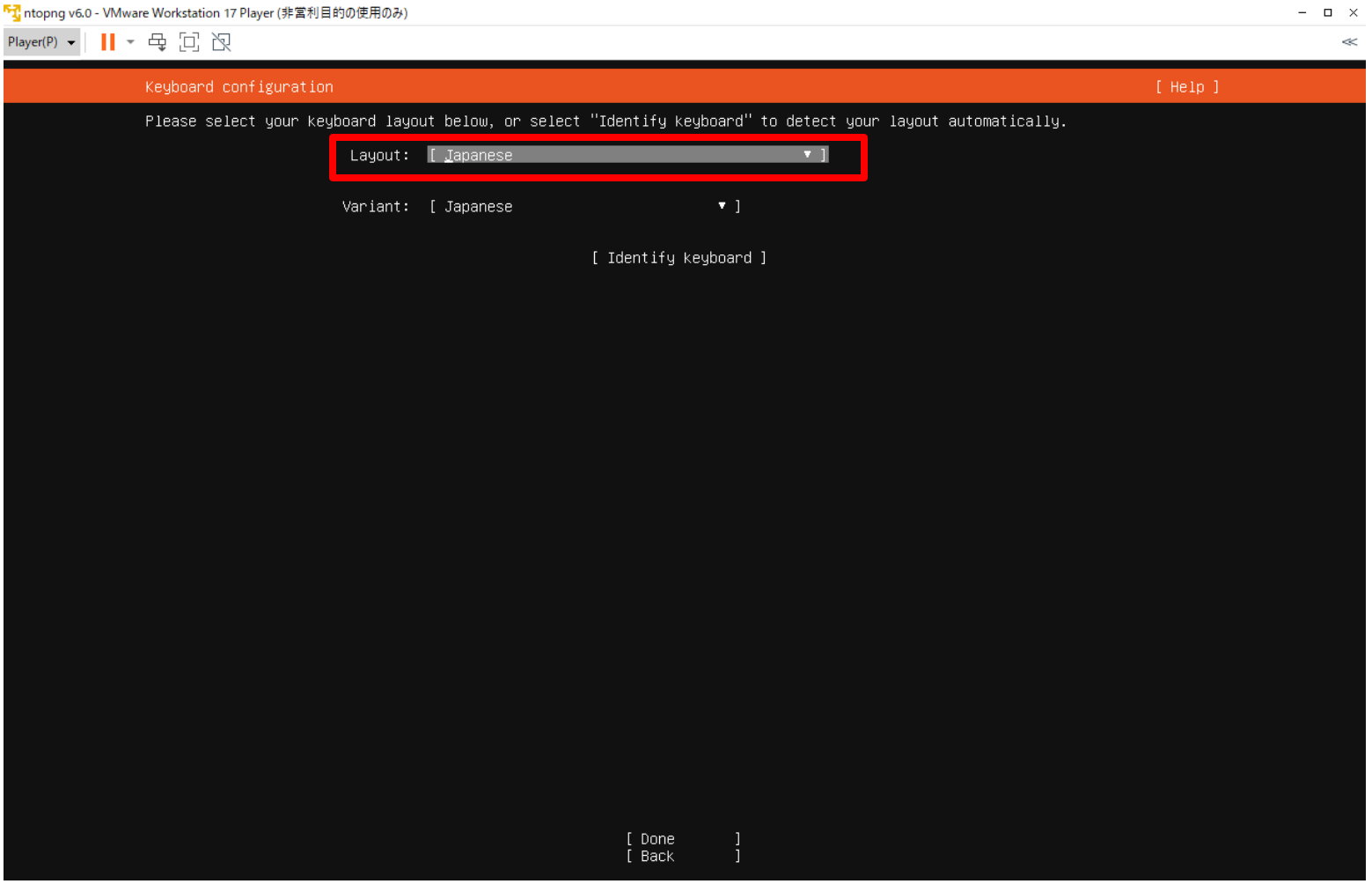
ISOインストール(11)

言語選択で「English」が選択されていることを確認し、Enterを押します。



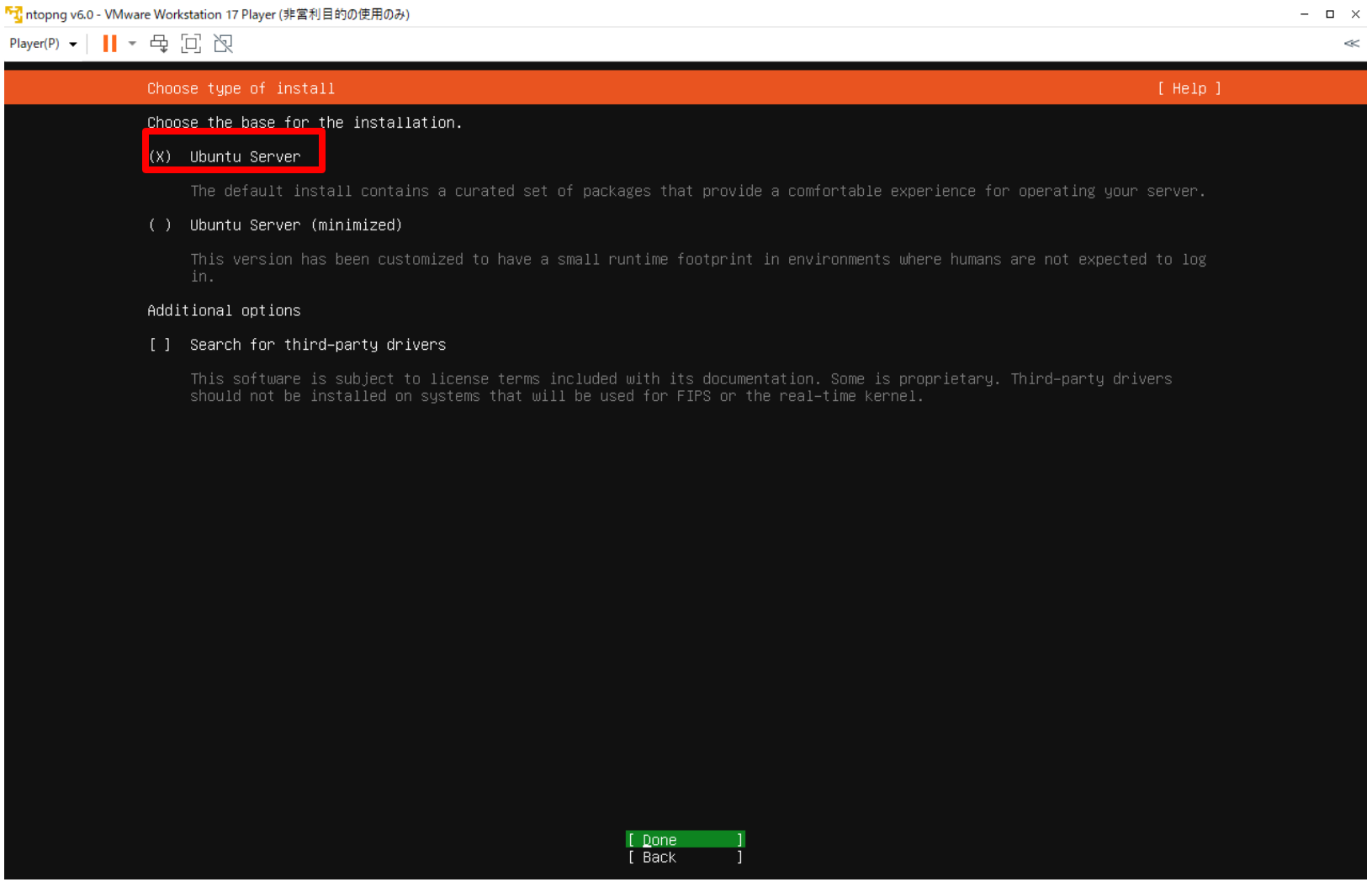
ISOインストール(12)

キーボード選択で「Japanese」を選択し、Enterを押します。



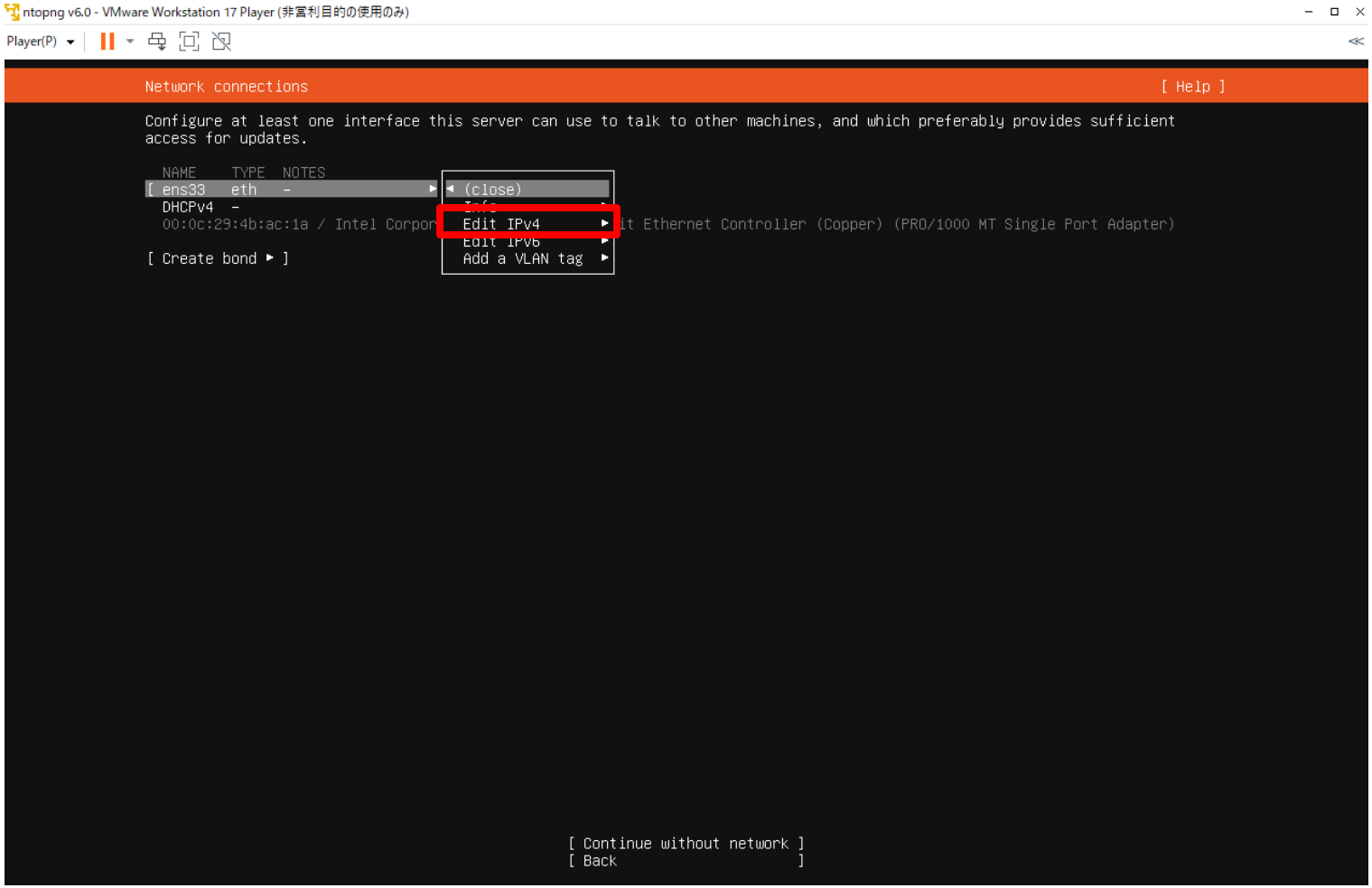
ISOインストール(13)

「Ubuntu Server」が選択されていることを確認し、「Done」を選択Enterを押します。



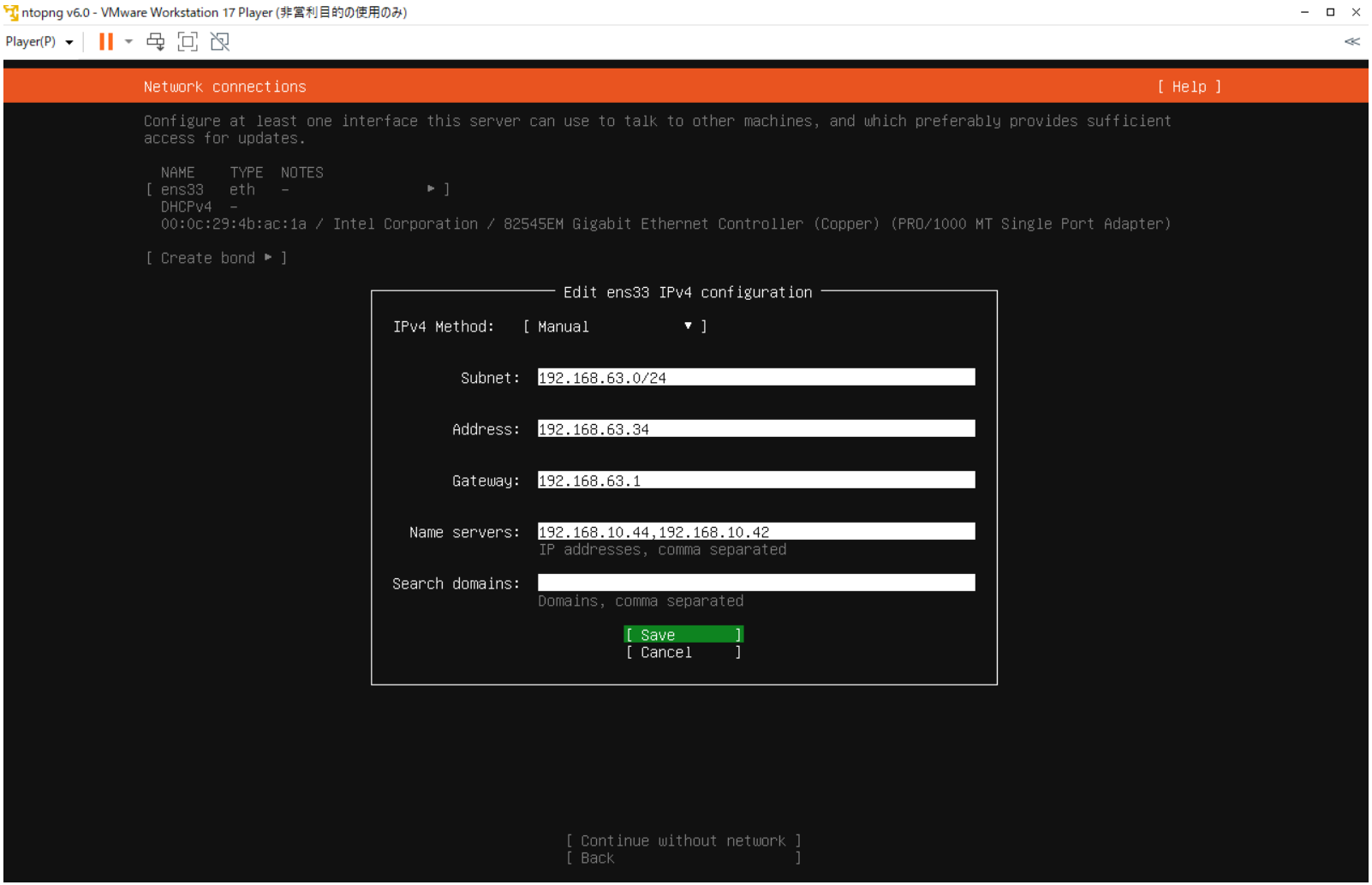
ISOインストール(14)

環境によいIPアドレスを設定してください。以下は手動でIPアドレスを設定する例です。該当のNICを選択し、「Edit IPv4」を選択し、Enterをクリックします。



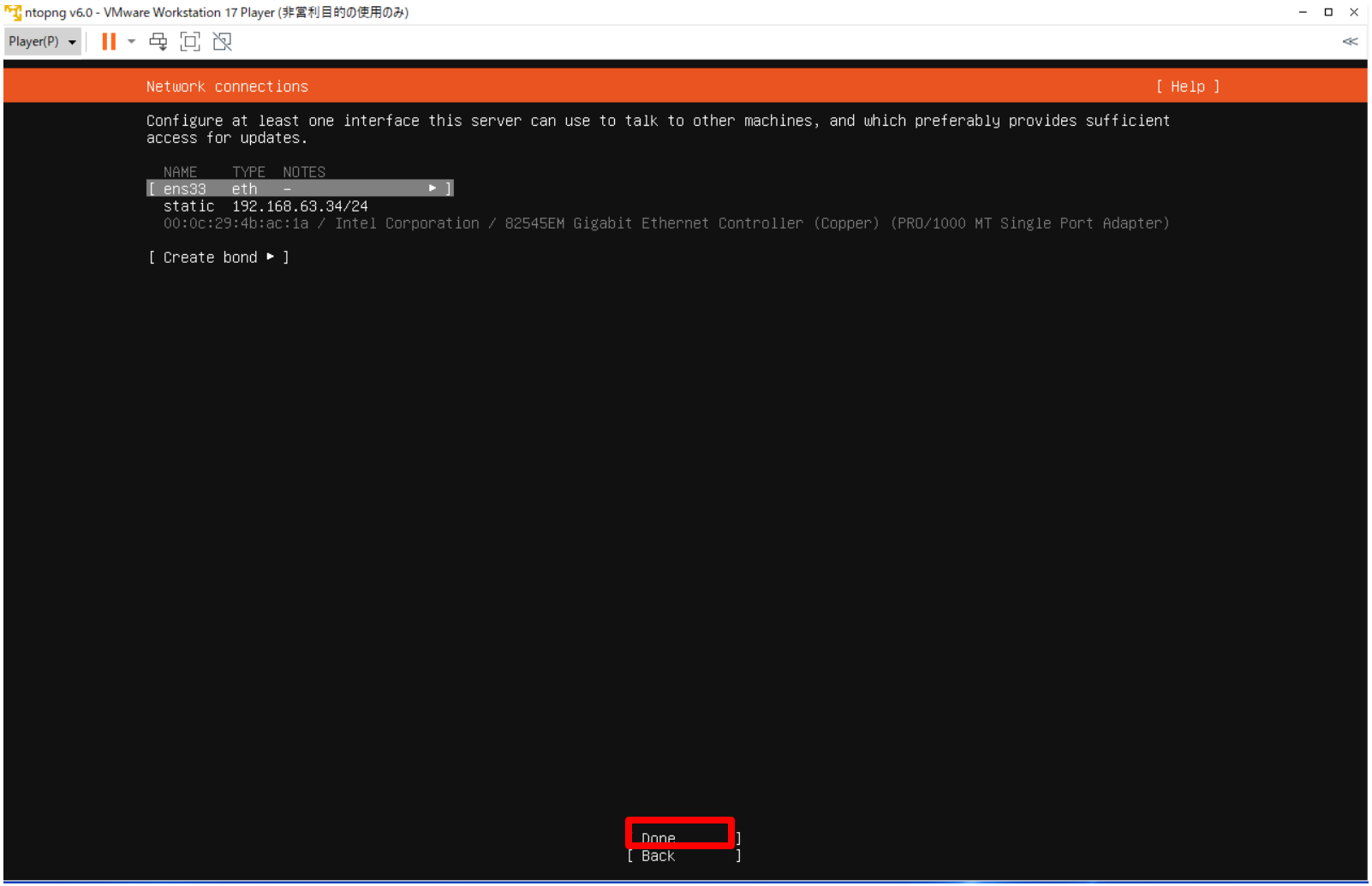
ISOインストール(15)

IPアドレスを設定してください。以下は手動でIPアドレスを設定する例です。



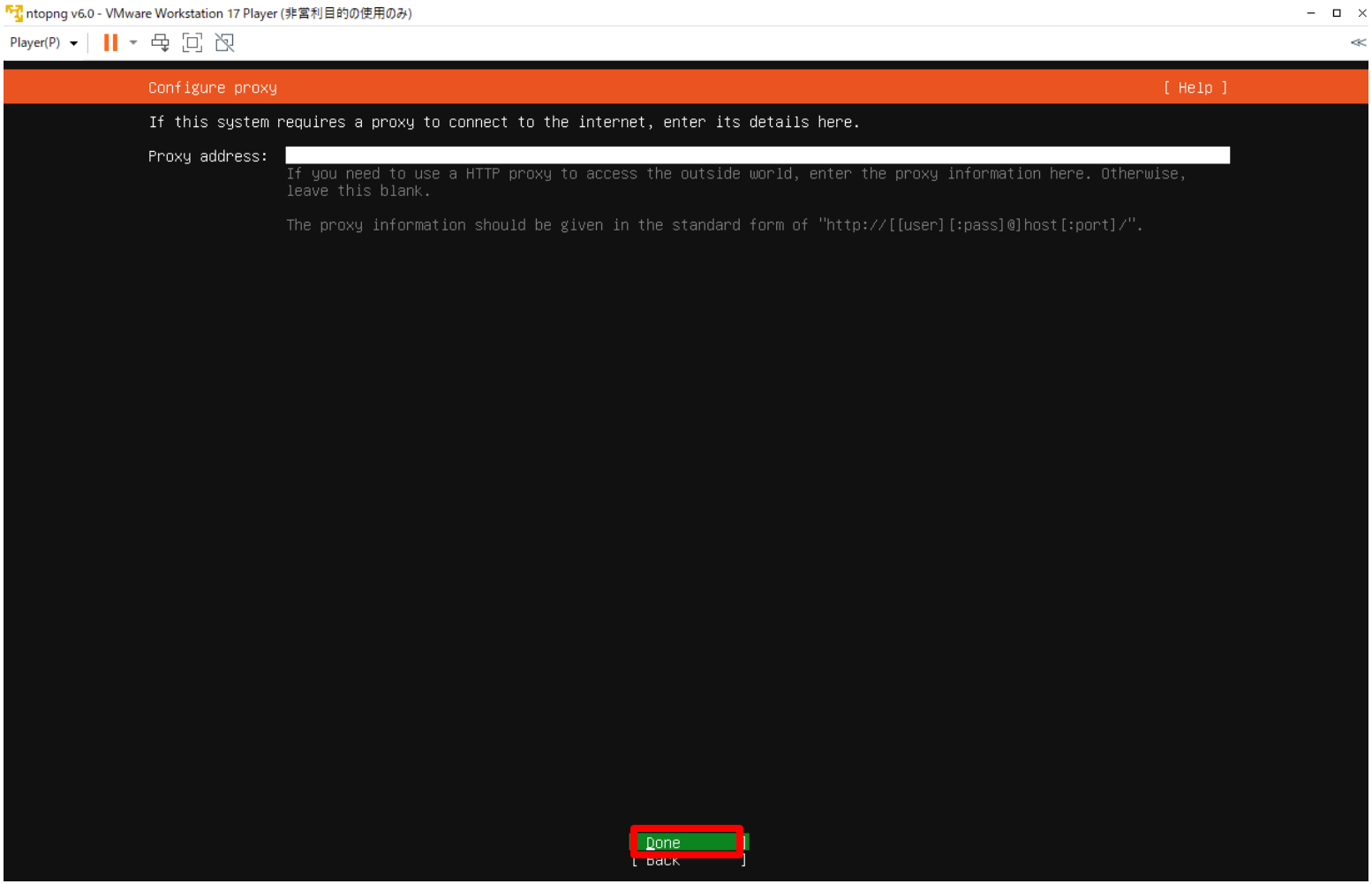
ISOインストール(16)

設定が完了したら、「Done」を選択しEnterを押します。



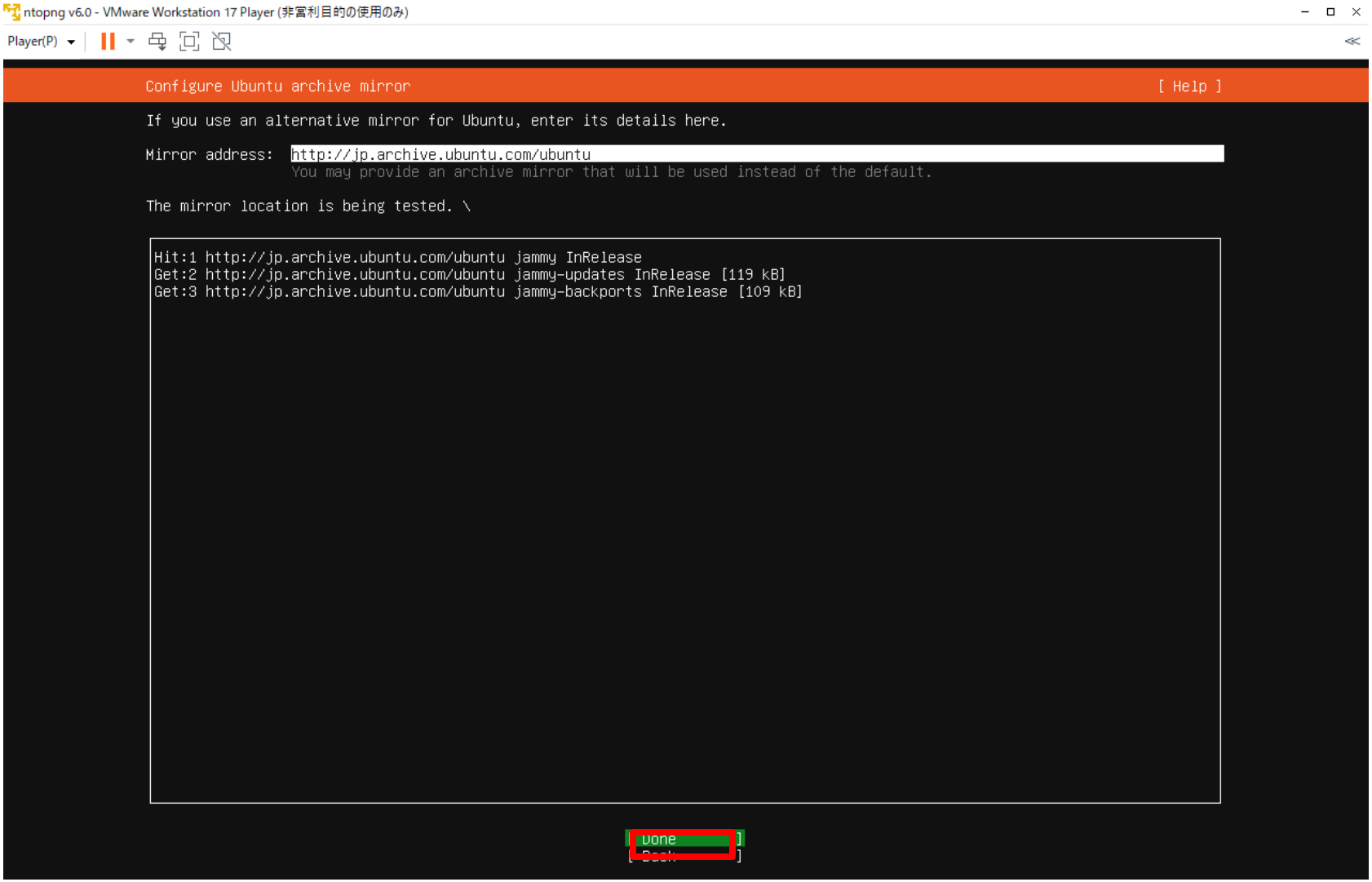
ISOインストール(17)

プロキシ環境でなければ、「Done」を選択しEnterを押します。



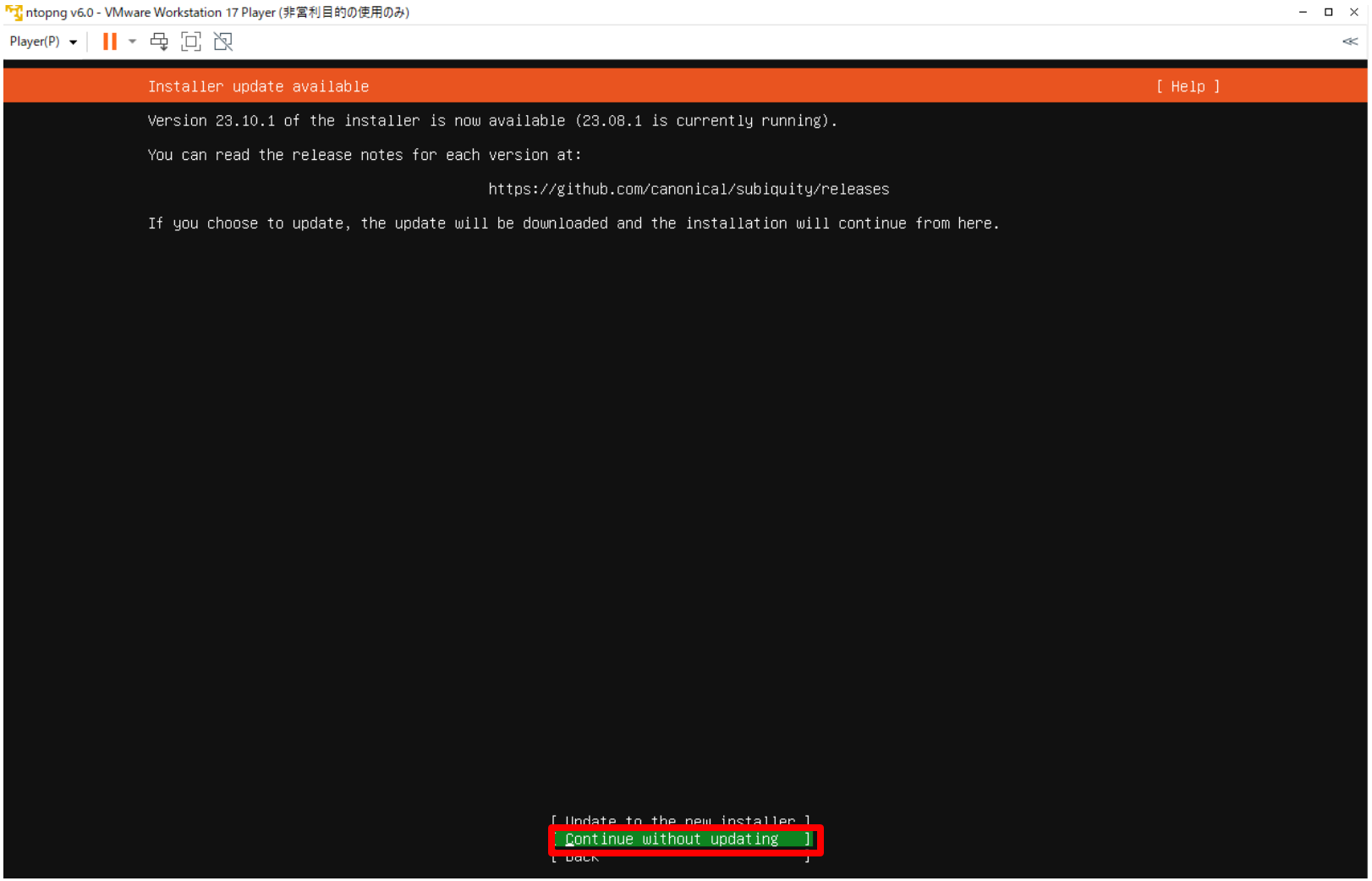
ISOインストール(18)

「Done」を選択しEnterを押します。



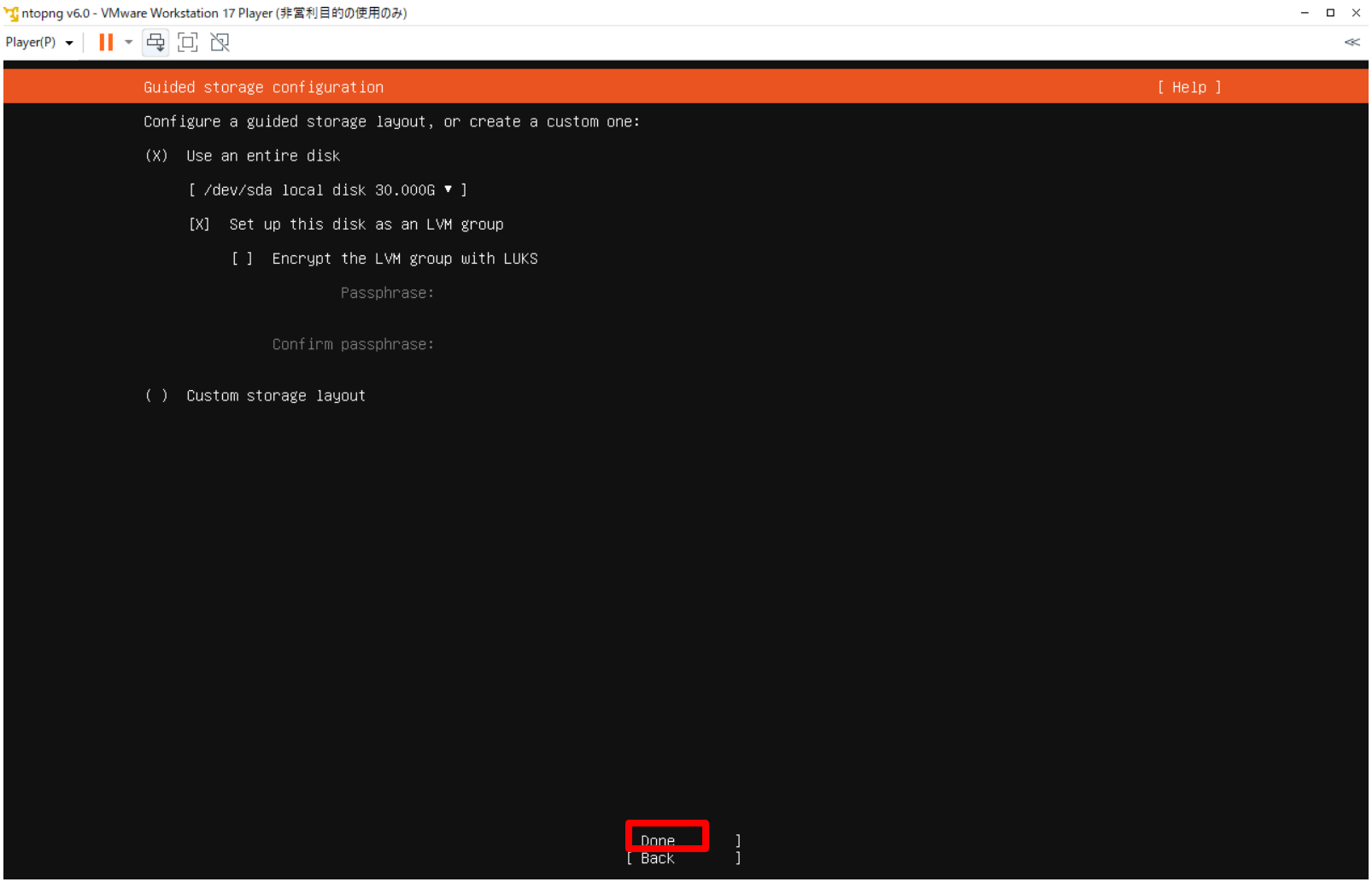
ISOインストール(19)

「Continue without updating」を選択しEnterを押します。



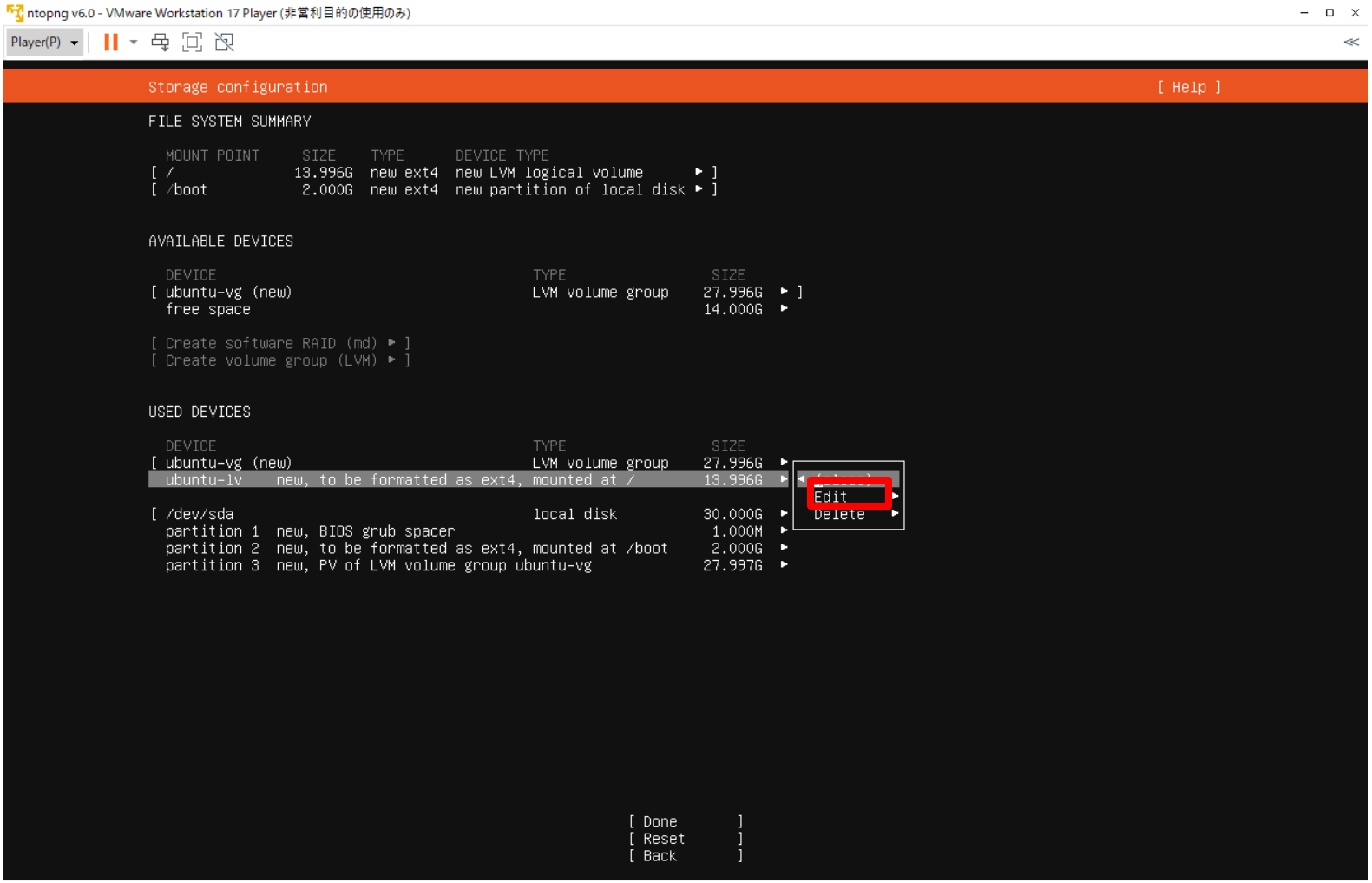
ISOインストール(20)

「Done」を選択しEnterを押します。



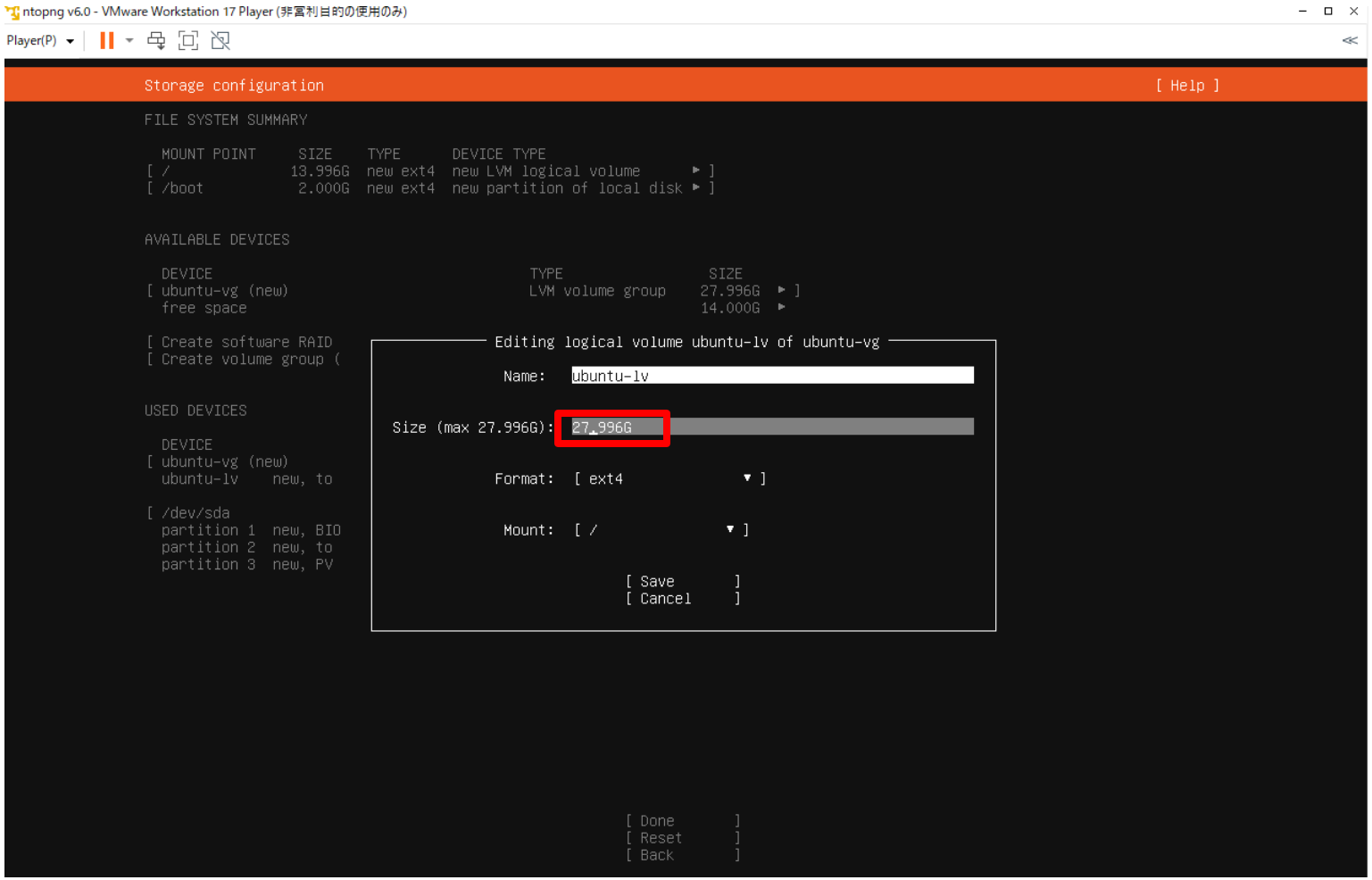
ISOインストール(21)

「ubuntu-lv」を選択しEnterを押します。「Edit」を選択し、Enterを押します。



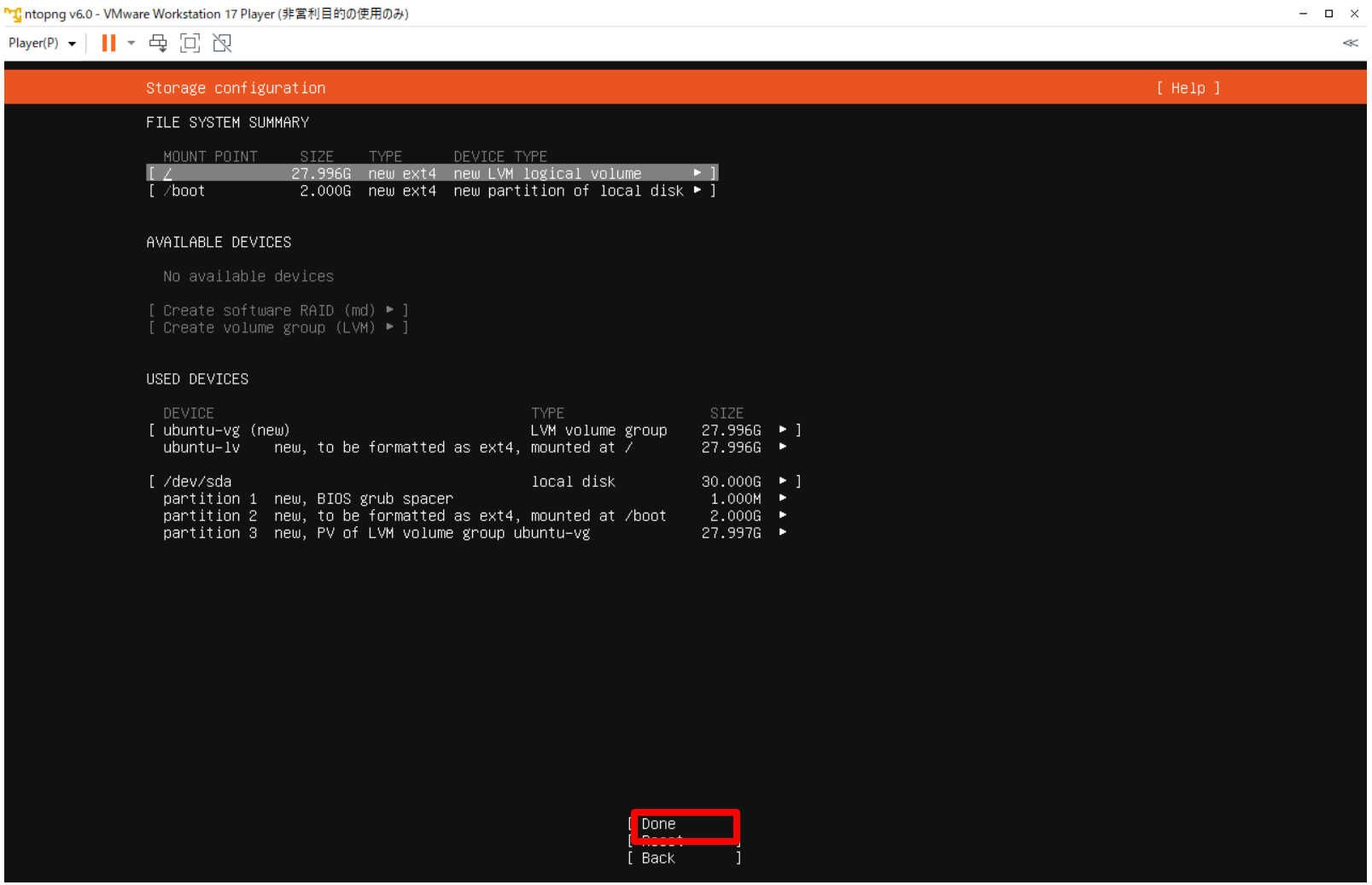
ISOインストール(22)

「Size」に最大サイズを設定。「Save」を選択し、Enterを押します。



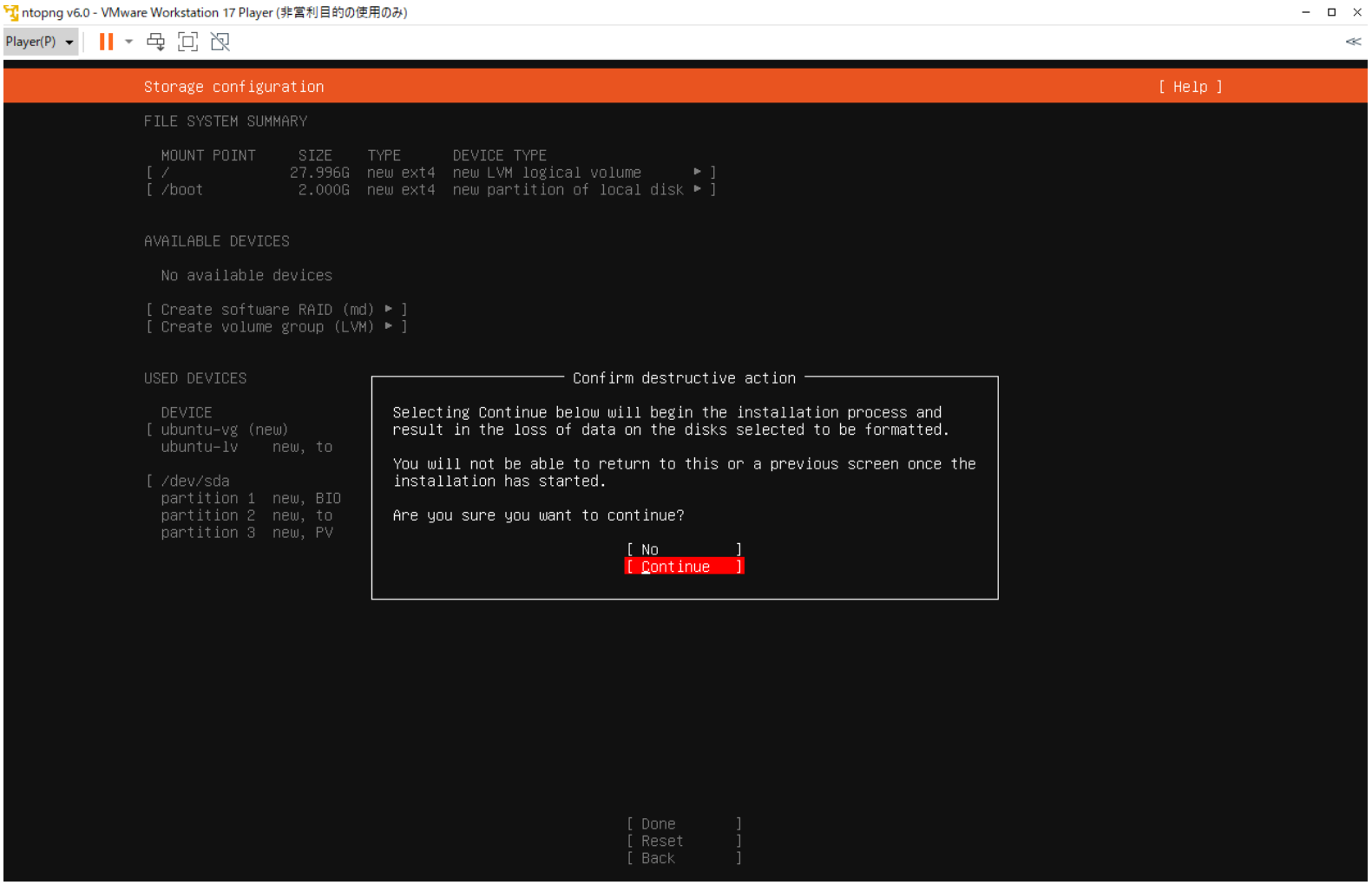
ISOインストール(23)

「Done」を選択し、Enterを押します。



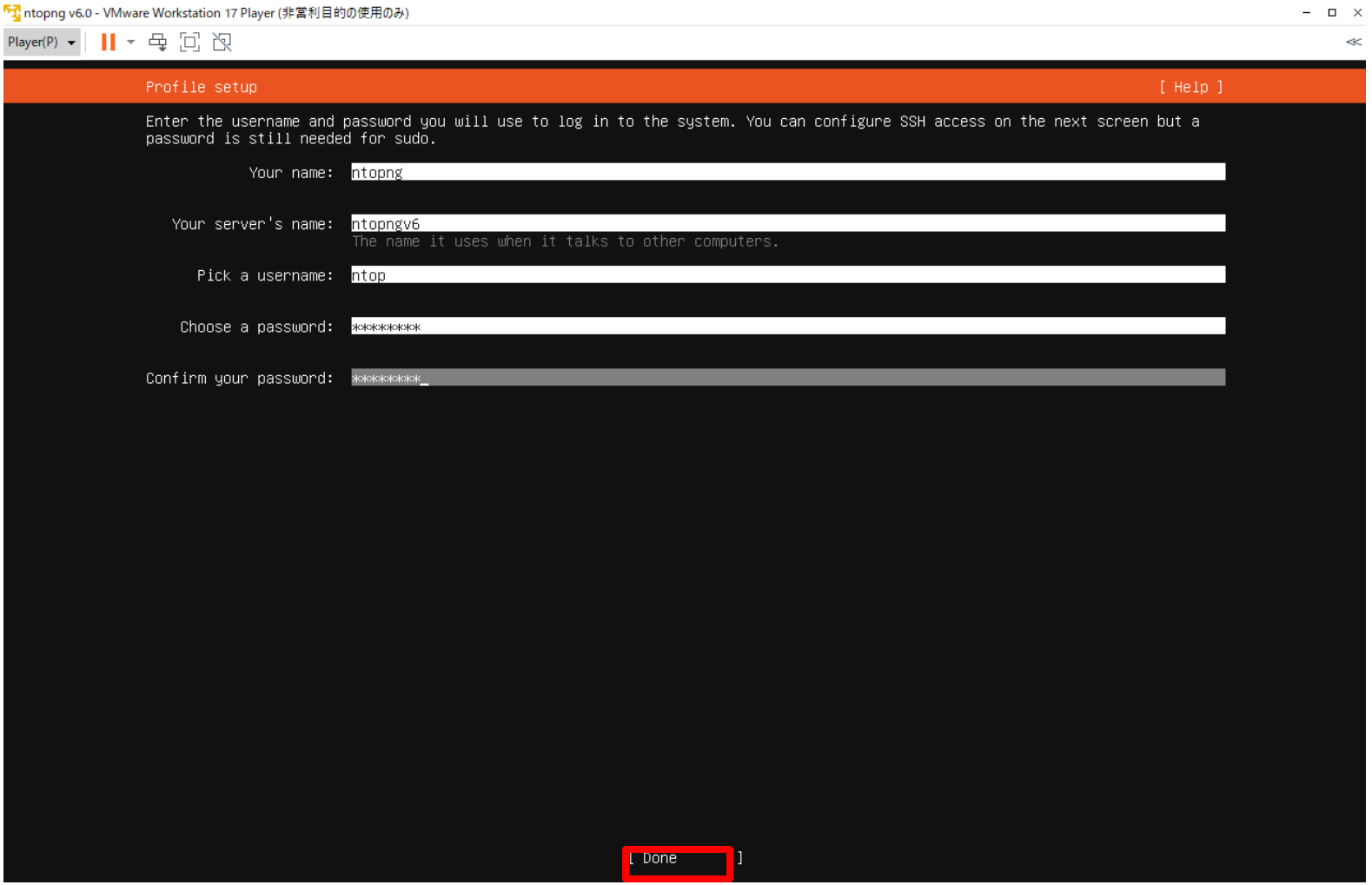
ISOインストール(24)

「Continue」を選択し、Enterを押します。



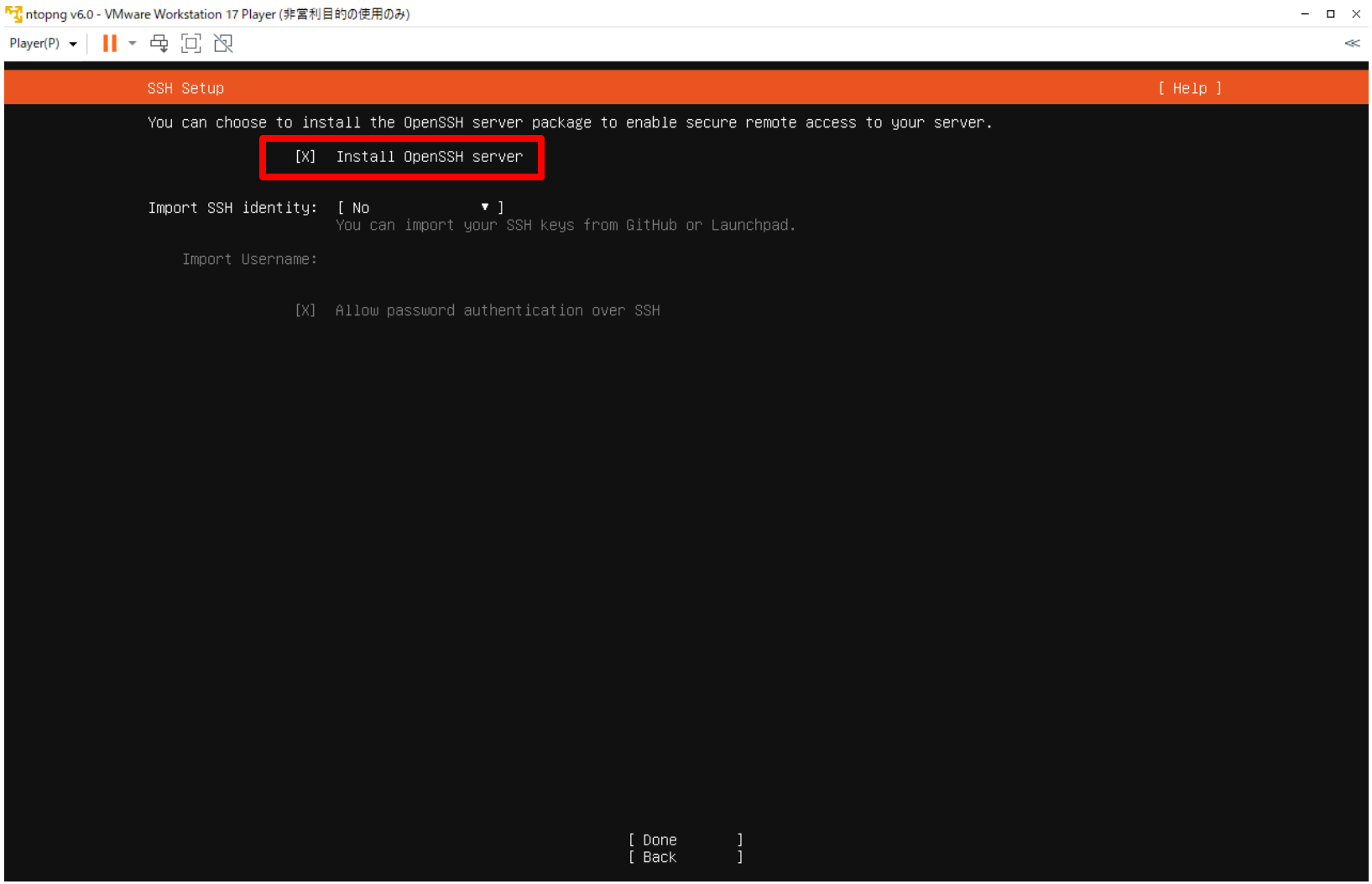
ISOインストール(25)

サーバー名、ユーザー名を設定し、「Done」を選択しEnterを押します。



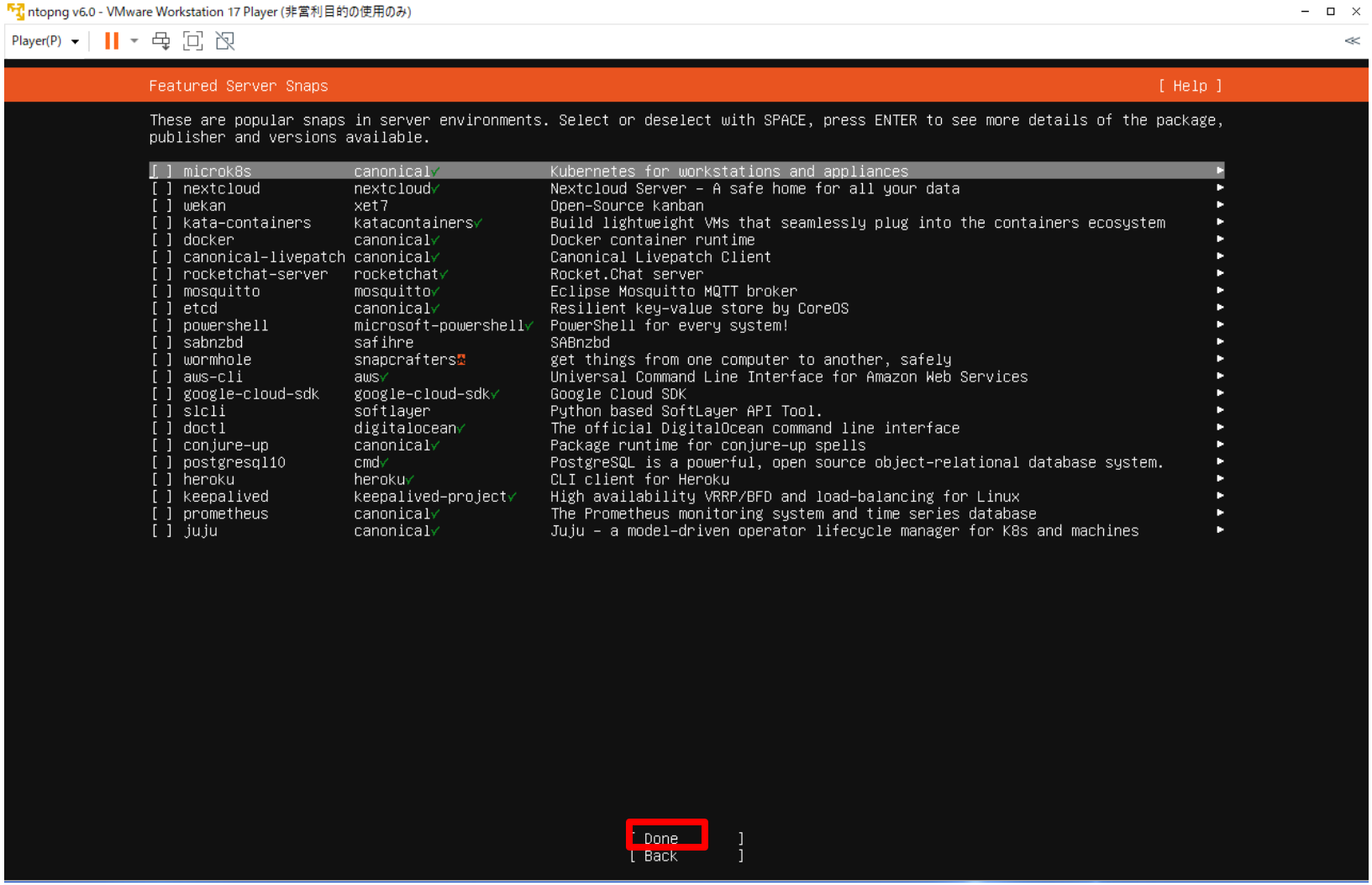
ISOインストール(26)

「Install OpenSSH server」に✓を入れ、「Done」を選択しEnterを押します。



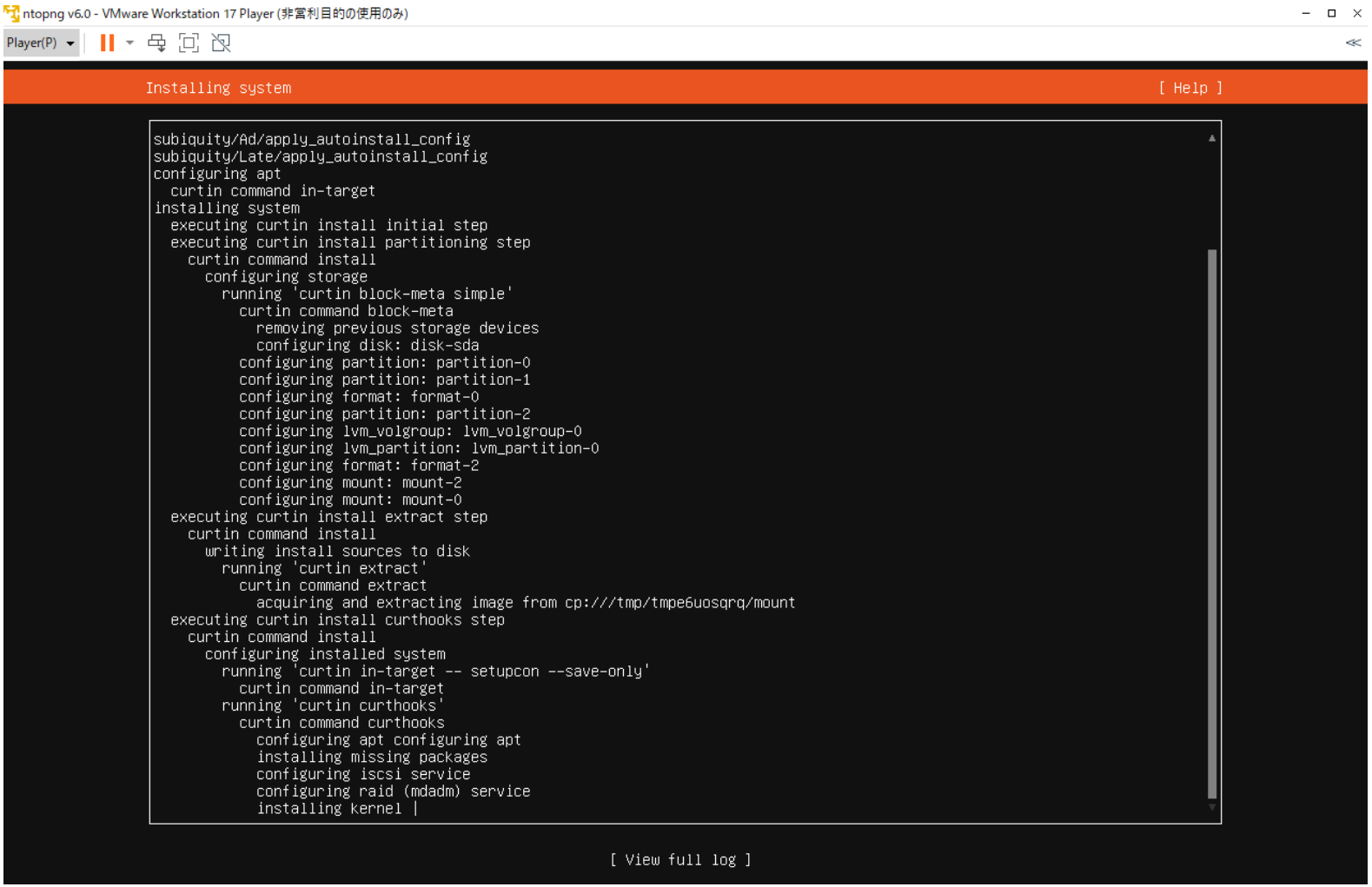
ISOインストール(27)

「Done」を選択しEnterを押します。



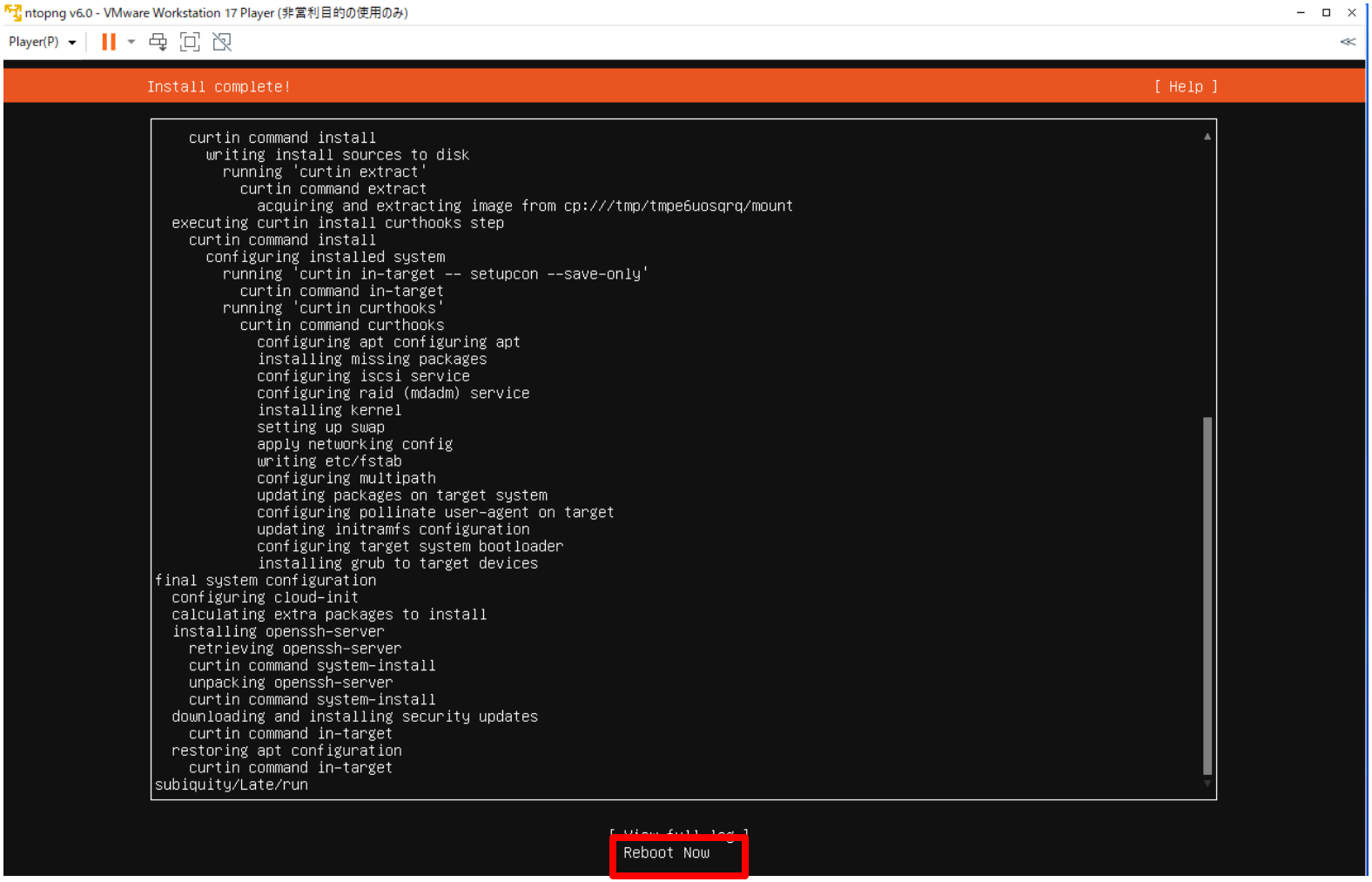
ISOインストール(28)

インストールが開始します。しばらくお待ちください。



ISOインストール(29)

「Install complete!」と表示されたのちに、「Rebbot Now」を選択しEnterを押します。これでインストールは完了です。



4. ntopngのインストール

本章では以下のバージョンを使用しています。

◆Windows 11 x64
◆nProbe 10.X and ntopng v6.X Stable版
◆VMware Workstation 17

ntopngのインストール(1)

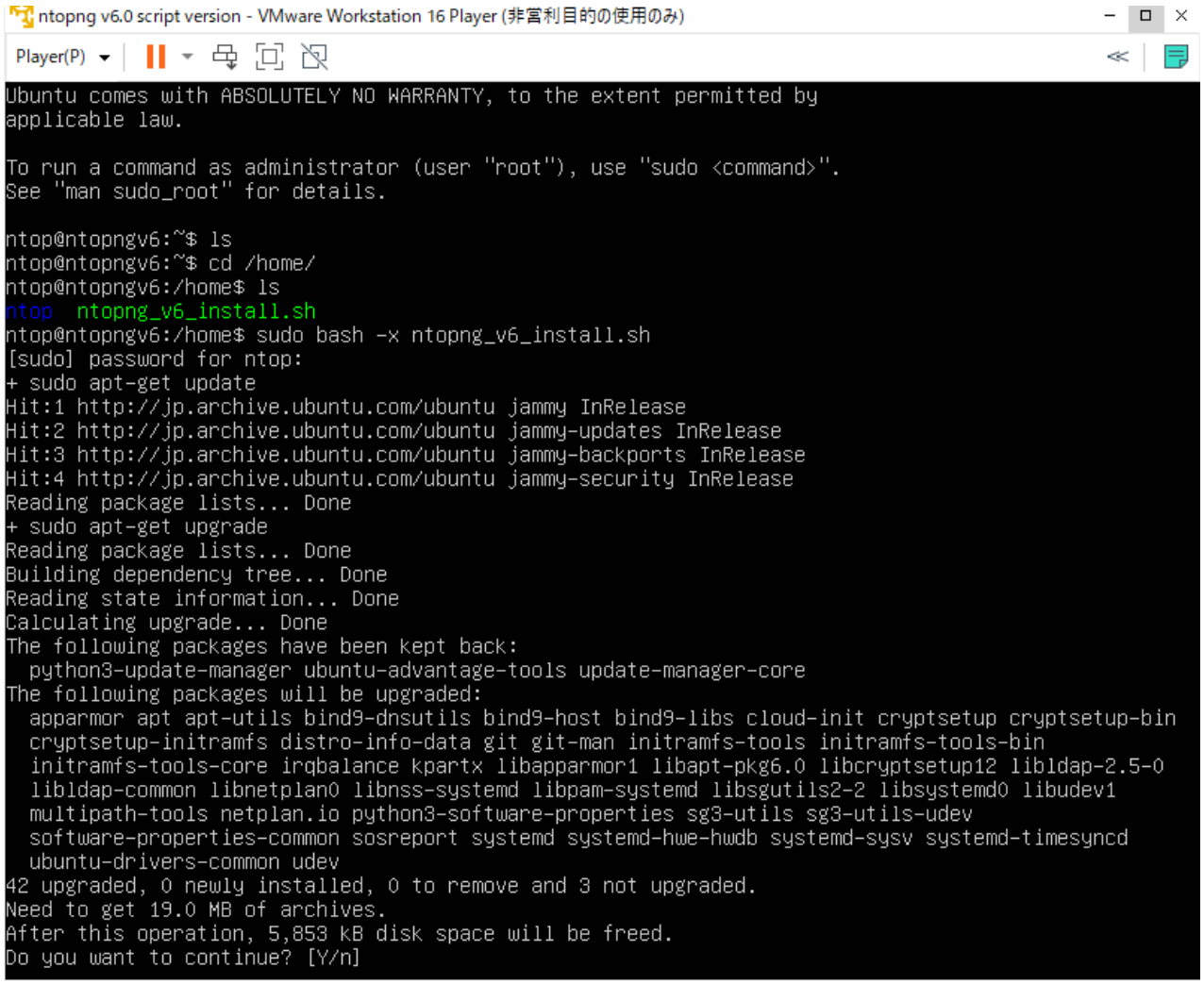
前章でISOからインストールしたubuntuサーバーには、ntopngのインストールスクリプトが包含されております。本章では、インストールスクリプトを実行しntopngをインストールします。

前章でインストールしたubuntuにログインしてください。そして、/homeに移動しインストールスクリプトを実行します。実行ユーザーはインストール時に作成したユーザーで、sudoを使います。

```
$cd /home
$sudo bash  –x ntopng_v6_install.sh
```

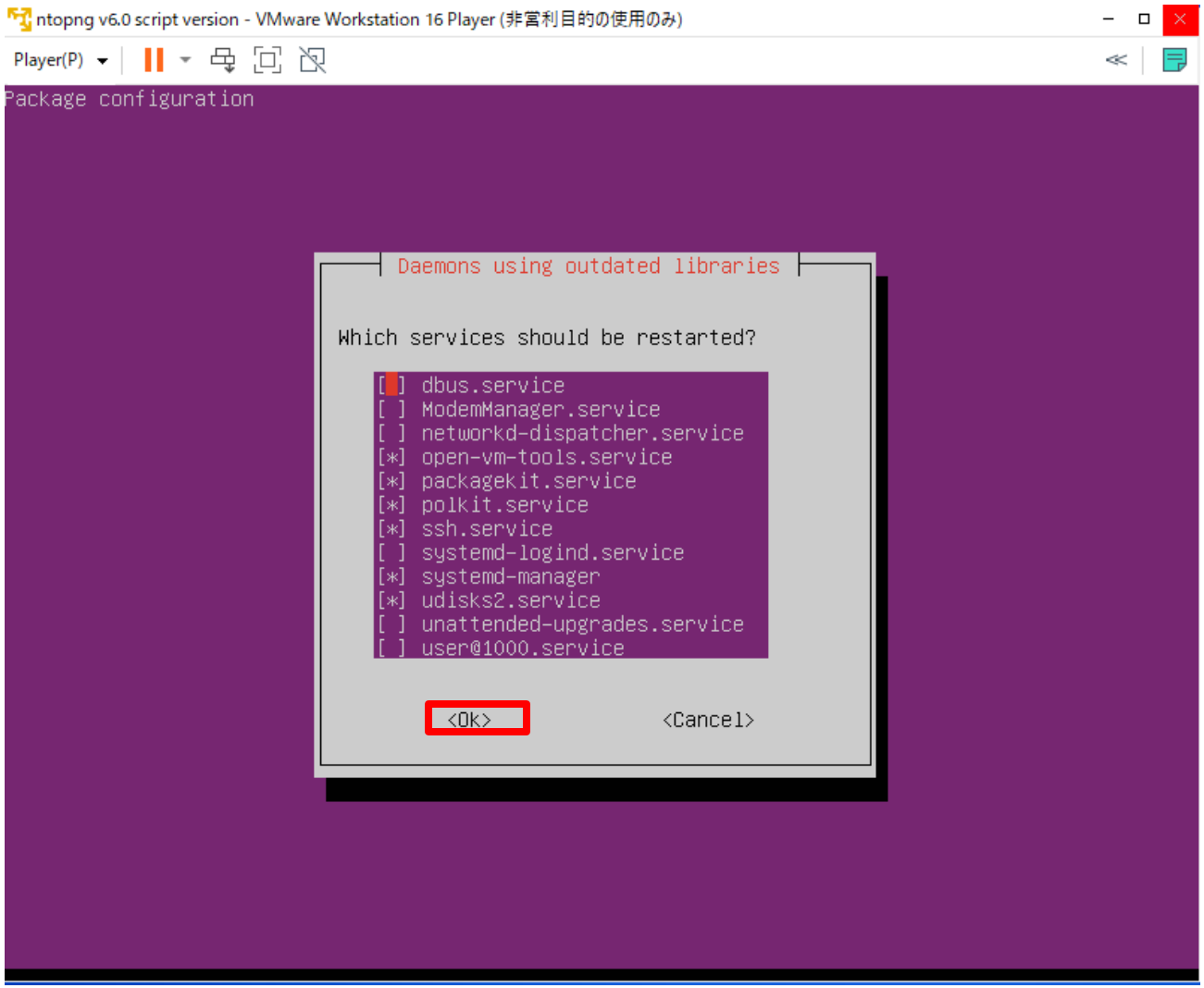
ntopngのインストール(2)

「Do you want to continue? [Y/n]」と表示されるので、「Y」を入力しEnterを押します。



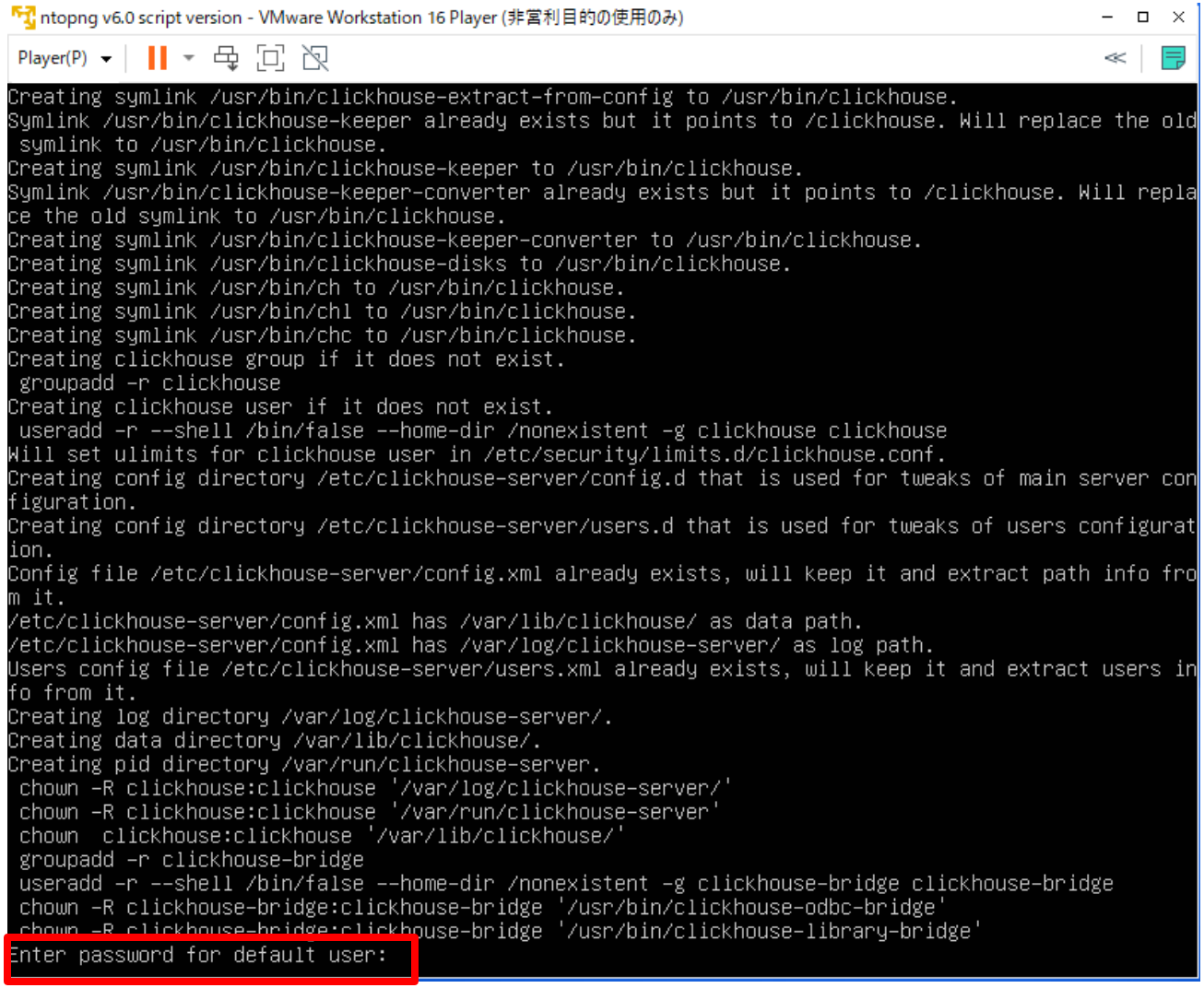
ntopngのインストール(3)

下記の画面が表示されるので、「<OK>」を選択しEnterを押します。



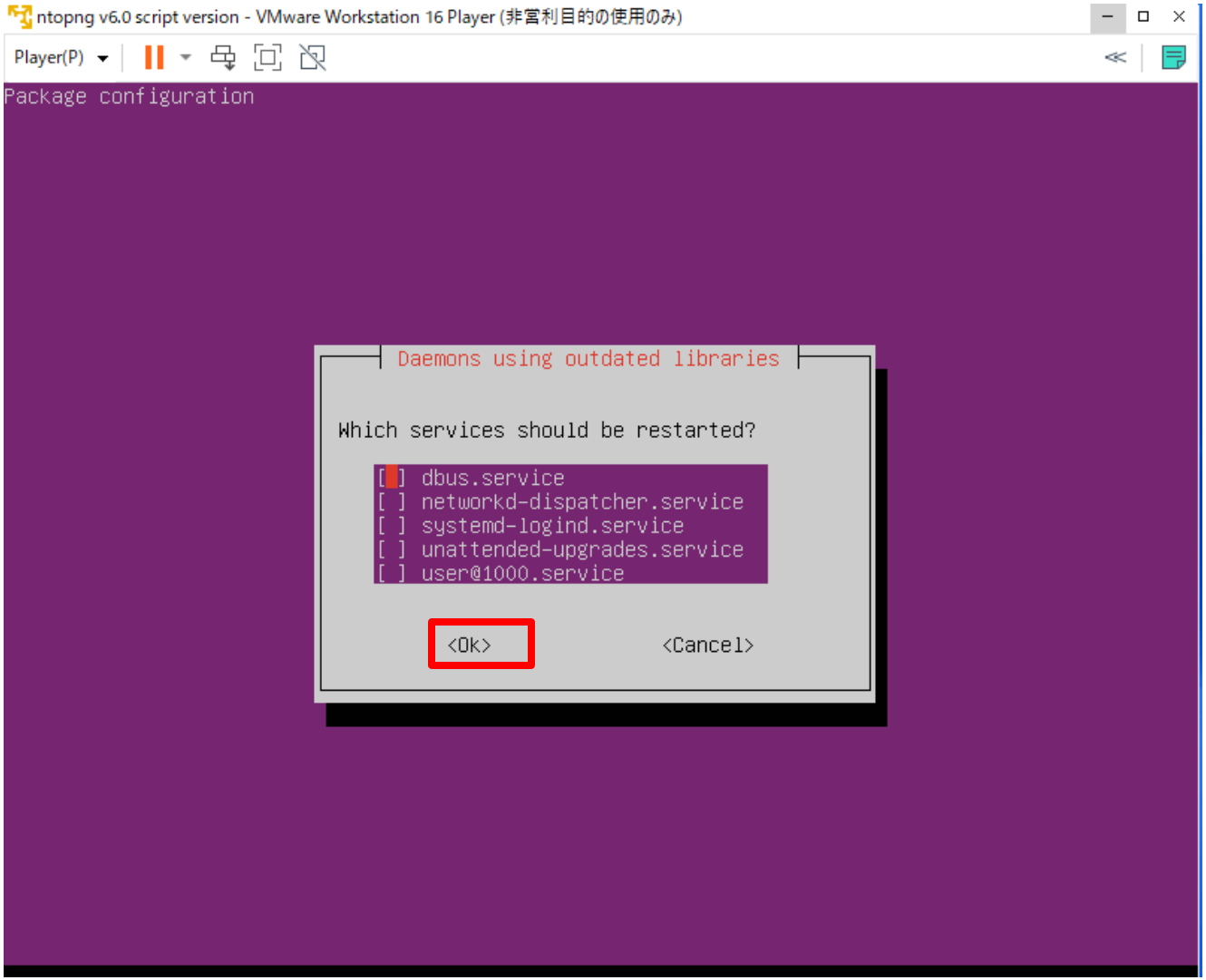
ntopngのインストール(4)

「Enter Password for default user:」と表示されるので、**必ず”default”と入力し**Enterを押します

- 

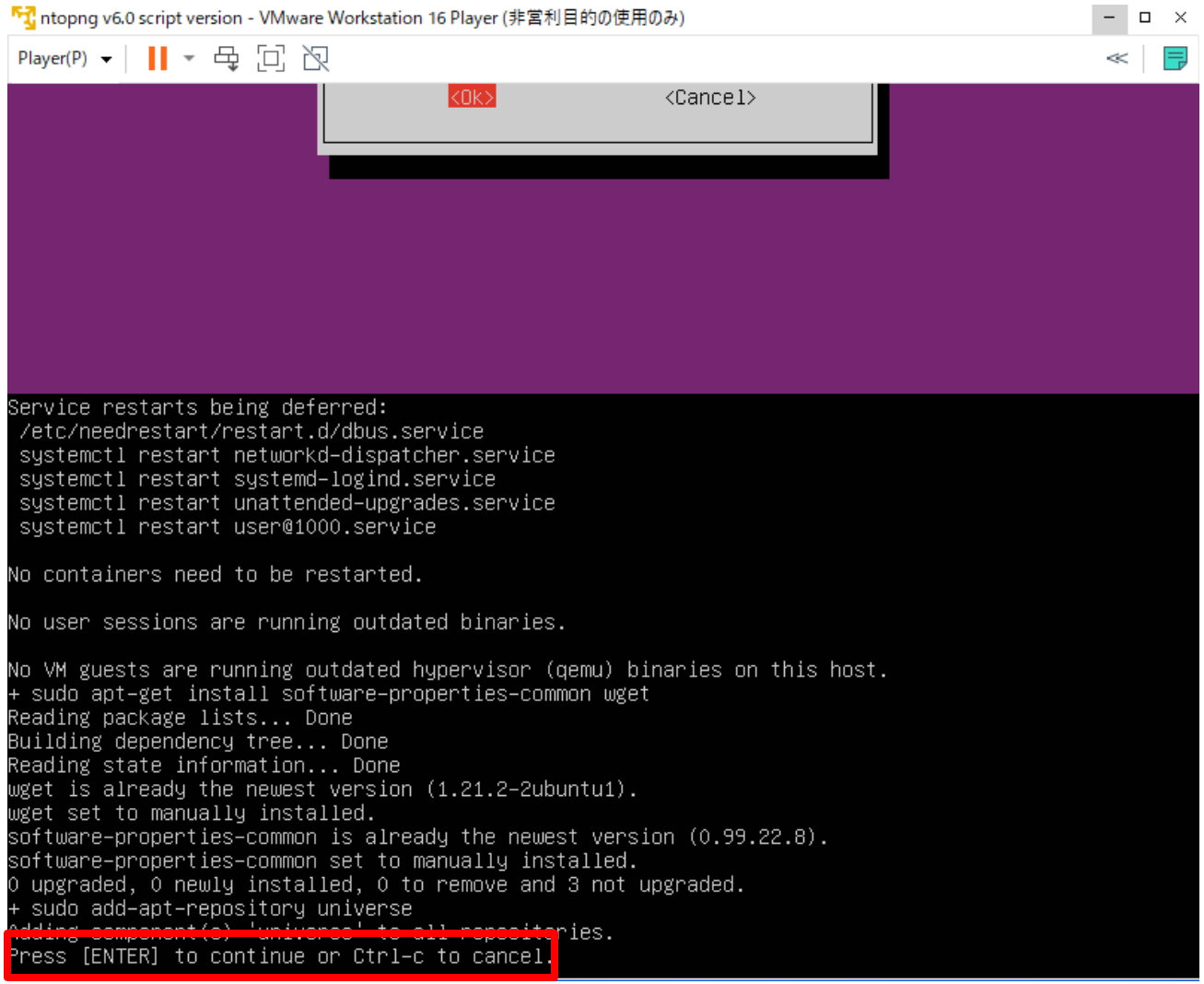
ntopngのインストール(5)

下記の画面が表示されるので、「<OK>」を選択しEnterを押します。



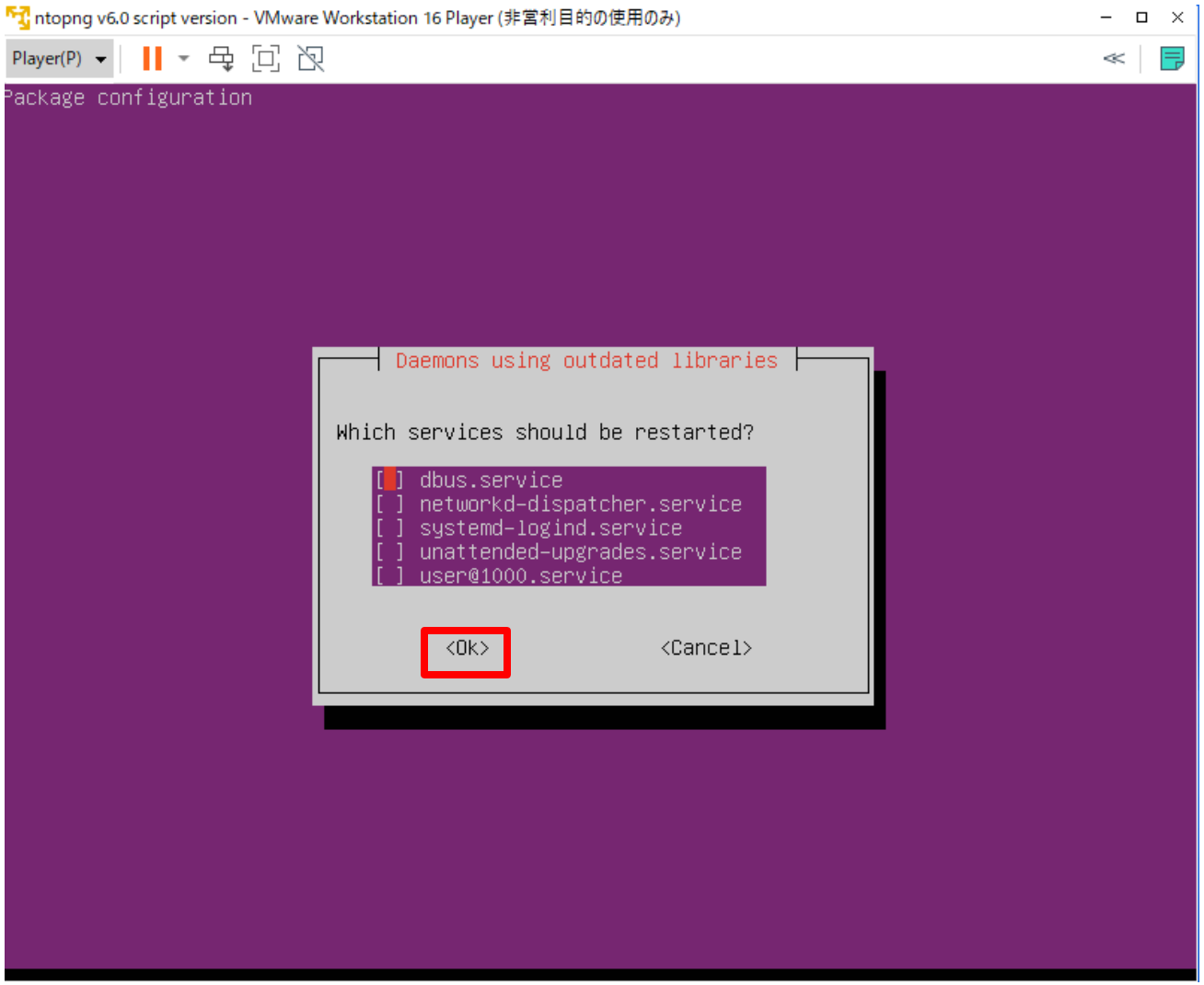
ntopngのインストール(6)

「Press [ENTER] to continue …」と表示されるので、Enterを押します。



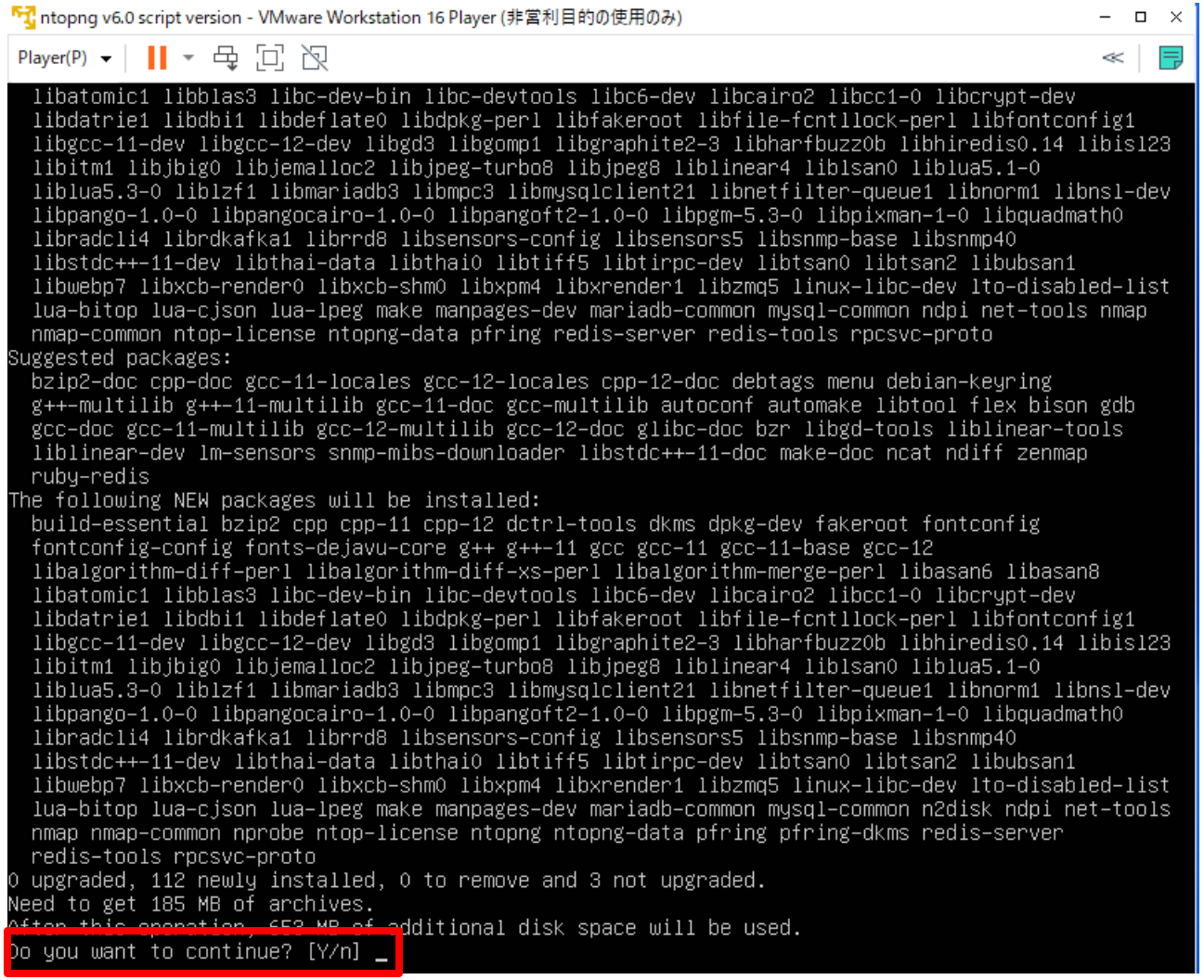
ntopngのインストール(7)

下記の画面が表示されるので、「<OK>」を選択しEnterを押します。



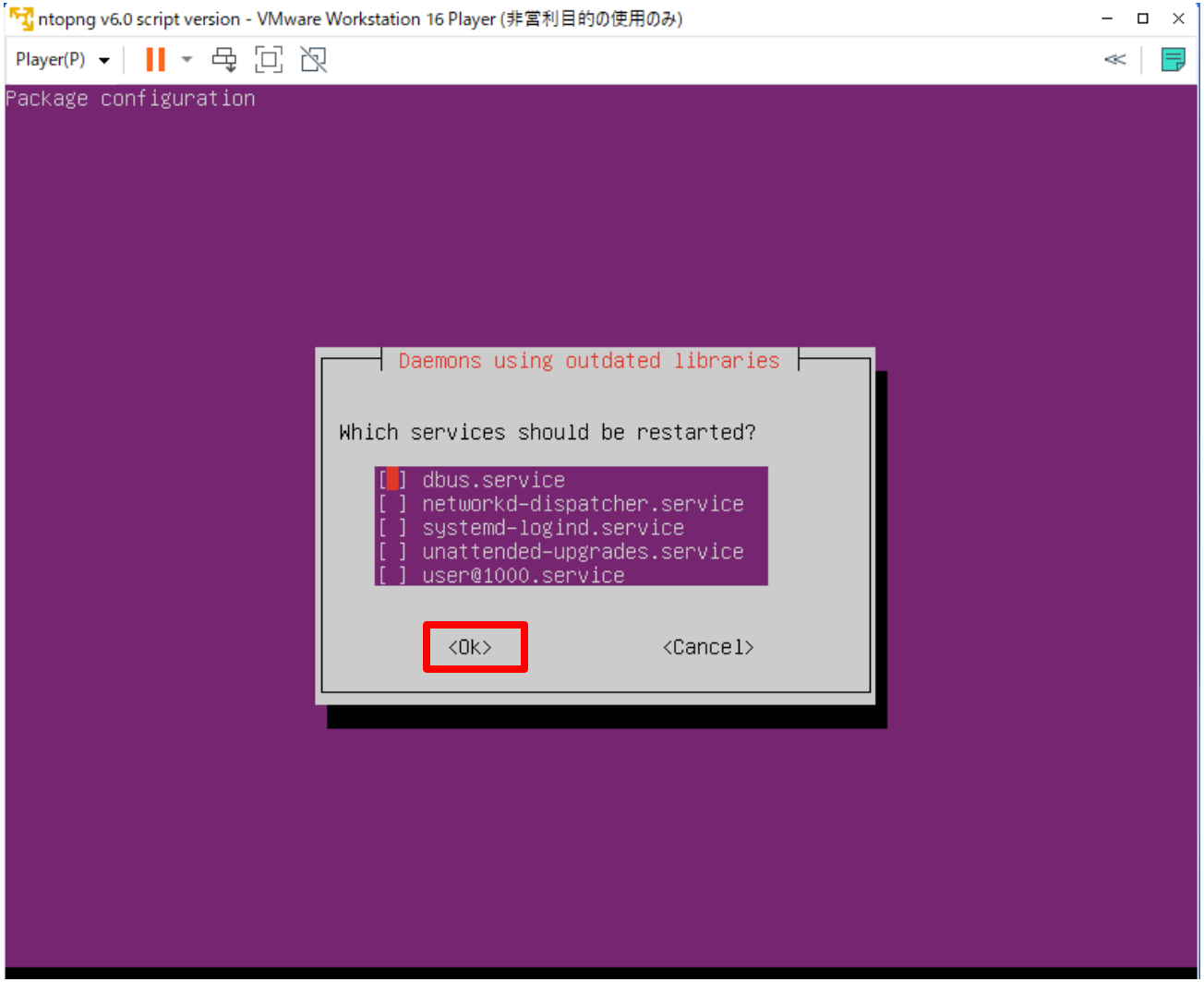
ntopngのインストール(8)

「Do you want to continue?[Y/n]」と表示されるので、「Y」を入力しEnterを押します。



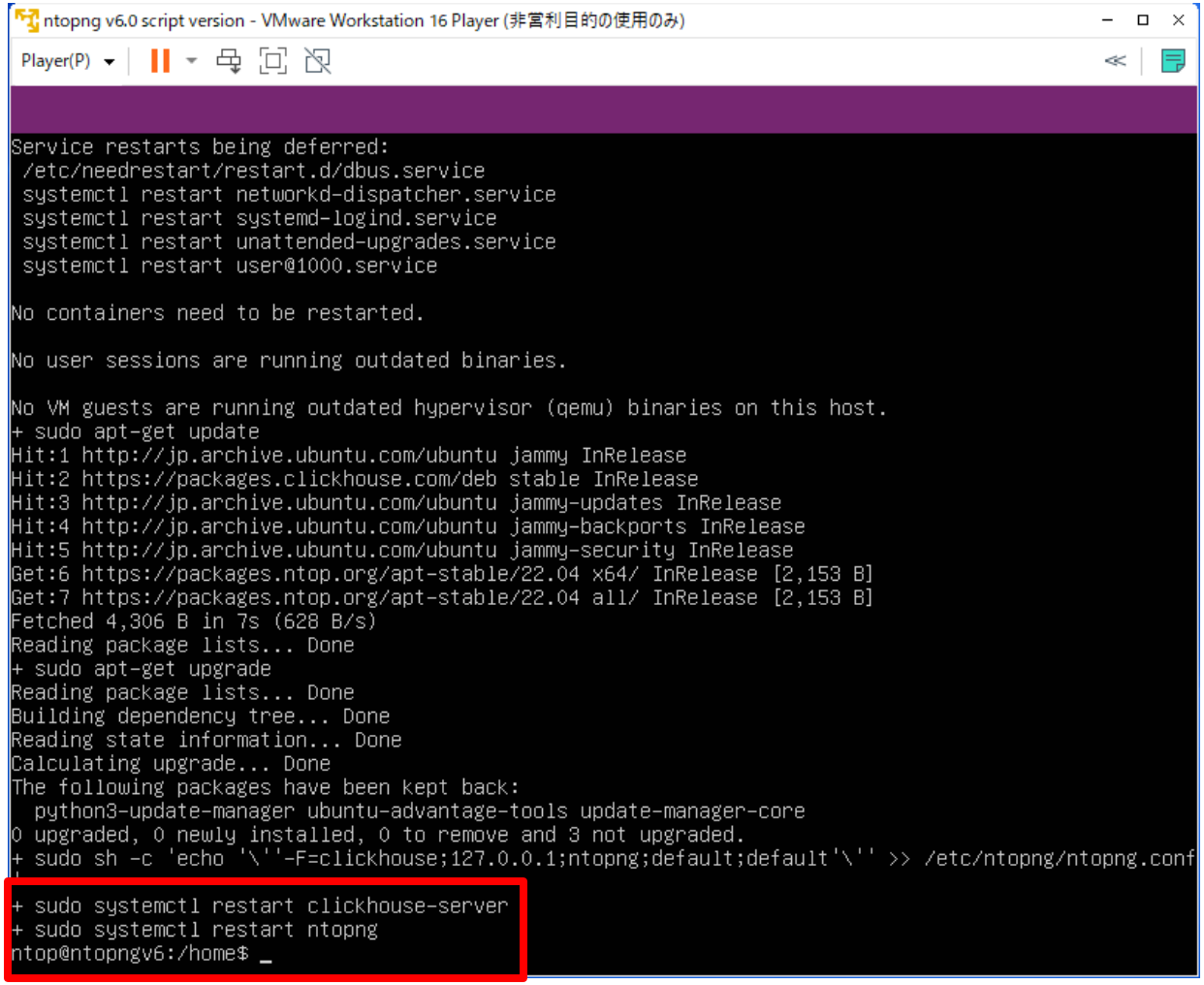
ntopngのインストール(9)

下記の画面が表示されるので、「<OK>」を選択しEnterを押します。



ntopngのインストール(10)

以下の画面のように、clickhouse-serverとntopngが再起動され、プロンプトが戻れば完了です。



ntopngのインストール(11)

コマンドでntopngの起動確認を行います。

```
$sudo systemctl status ntopng
● ntopng.service - ntopng high-speed web-based traffic monitoring and analysis>
     Loaded: loaded (/etc/systemd/system/ntopng.service; enabled; vendor preset>
     Active: active (running) since Thu 2024-01-04 10:22:57 JST; 1min 44s ago
   Main PID: 2045 (ntopng-main)
      Tasks: 30 (limit: 4515)
     Memory: 219.0M
        CPU: 9.108s
     CGroup: /system.slice/ntopng.service
             mq2045 /usr/bin/ntopng /run/ntopng.conf
```

上記の標準出力のように、Active: activeとなっていればntopngは正常に起動しております。

ntopngのインストール(12)

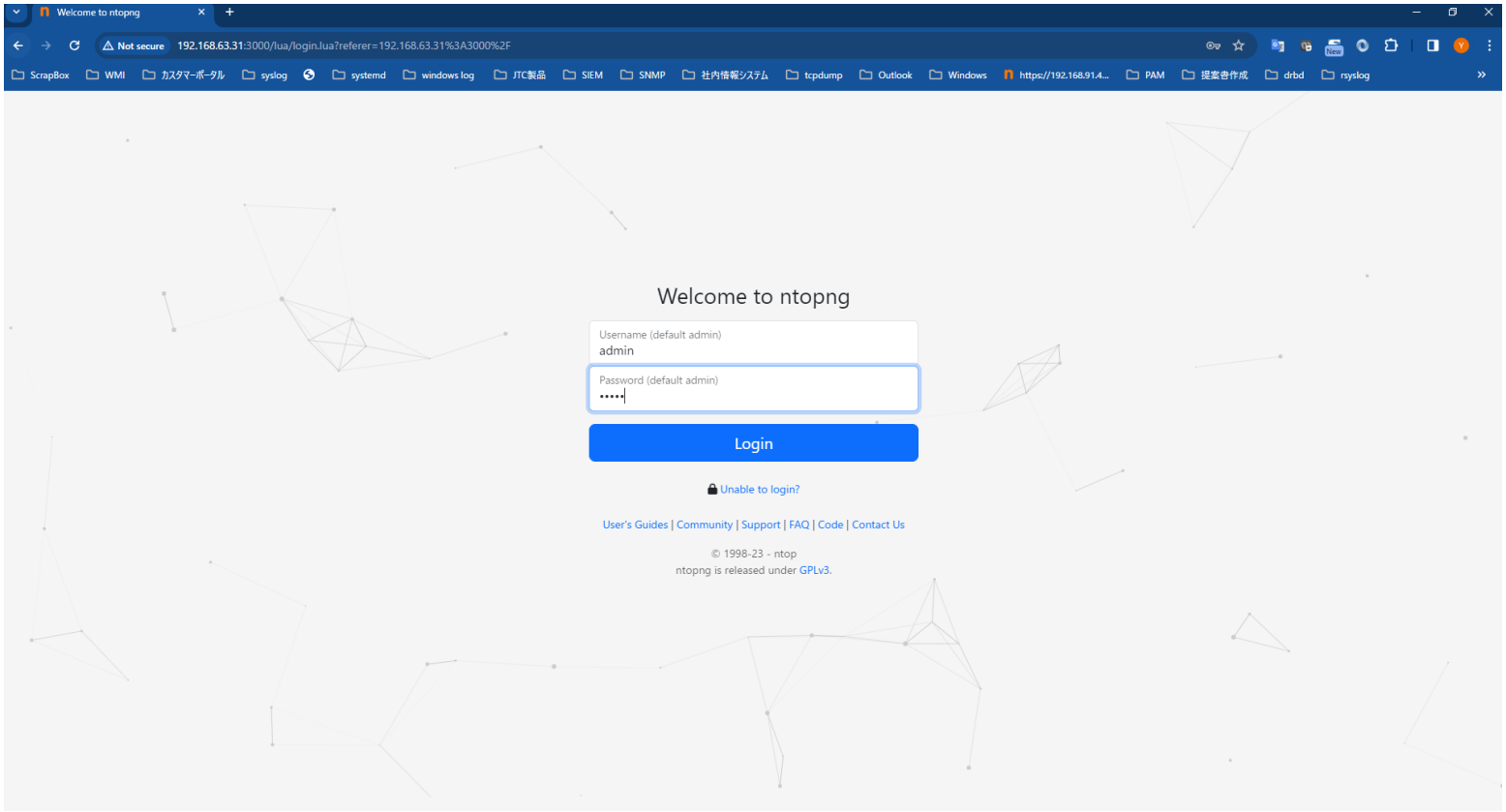
コマンドで nProbeの起動確認を行います。

```
$sudo systemctl status nprobe
● nprobe.service - nprobe extensible NetFlow v5/v9/IPFIX probe/collector
     Loaded: loaded (/etc/systemd/system/nprobe.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2024-01-04 10:22:46 JST; 4min 44s ago
   Main PID: 1090 (nprobe@lo)
      Tasks: 4 (limit: 4515)
     Memory: 31.8M
        CPU: 6.156s
     CGroup: /system.slice/nprobe.service
             mq1090 /usr/bin/nprobe /run/nprobe.conf
```

上記の標準出力のように、Active: activeとなっていればnprobeは正常に起動しております。

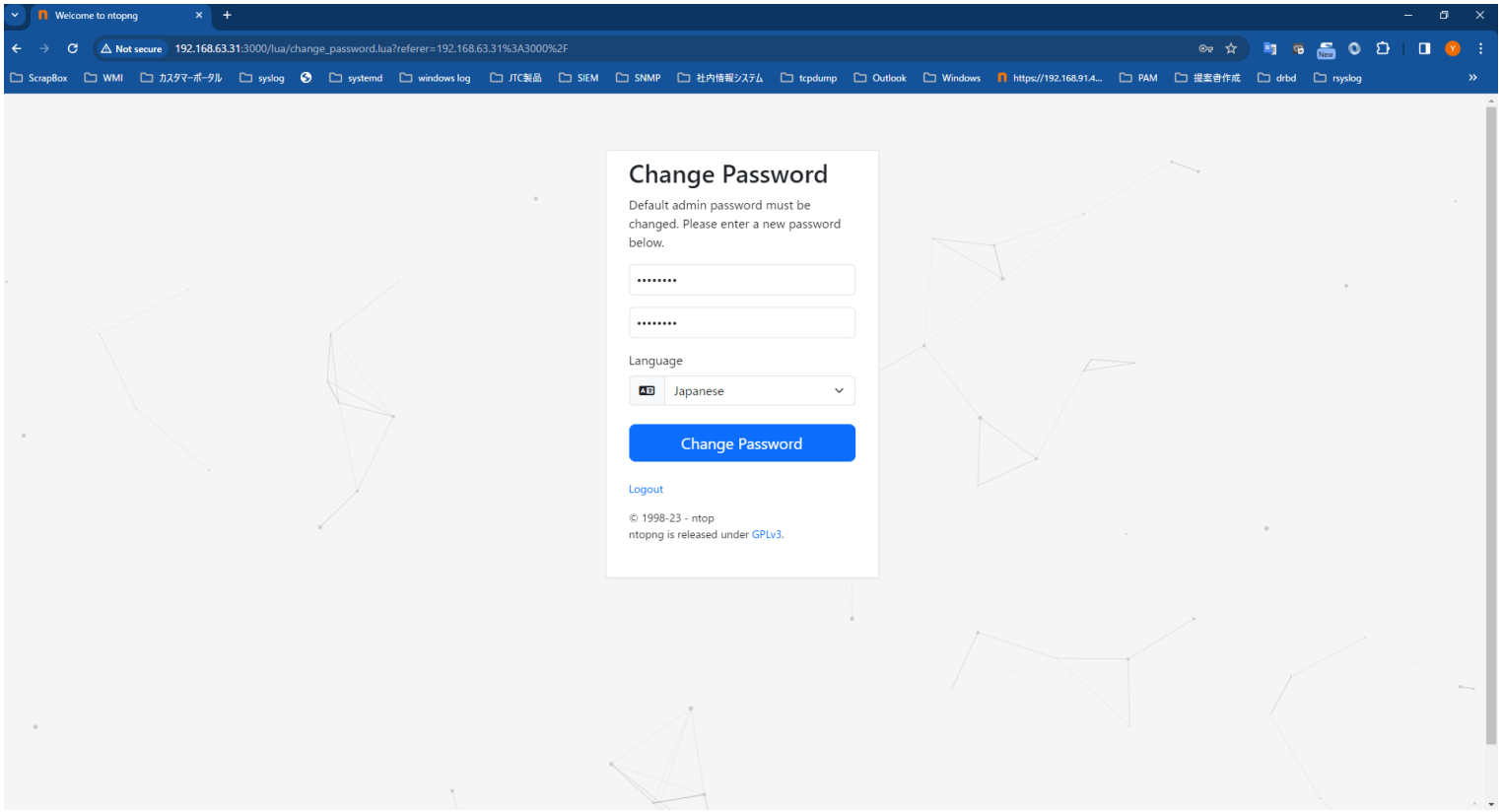
ntopngのインストール(13)

最後にWebブラウザでntopngの起動確認を行います。本ドキュメント”ISOインストール(14)”で設定したIPアドレス情報を使って、Webブラウザでアクセスします。http://設定したIPアドレス:3000 を入力すると以下のWelcome画面が表示されます。admin/adminと入力し、「Login」ボタンをクリックします。



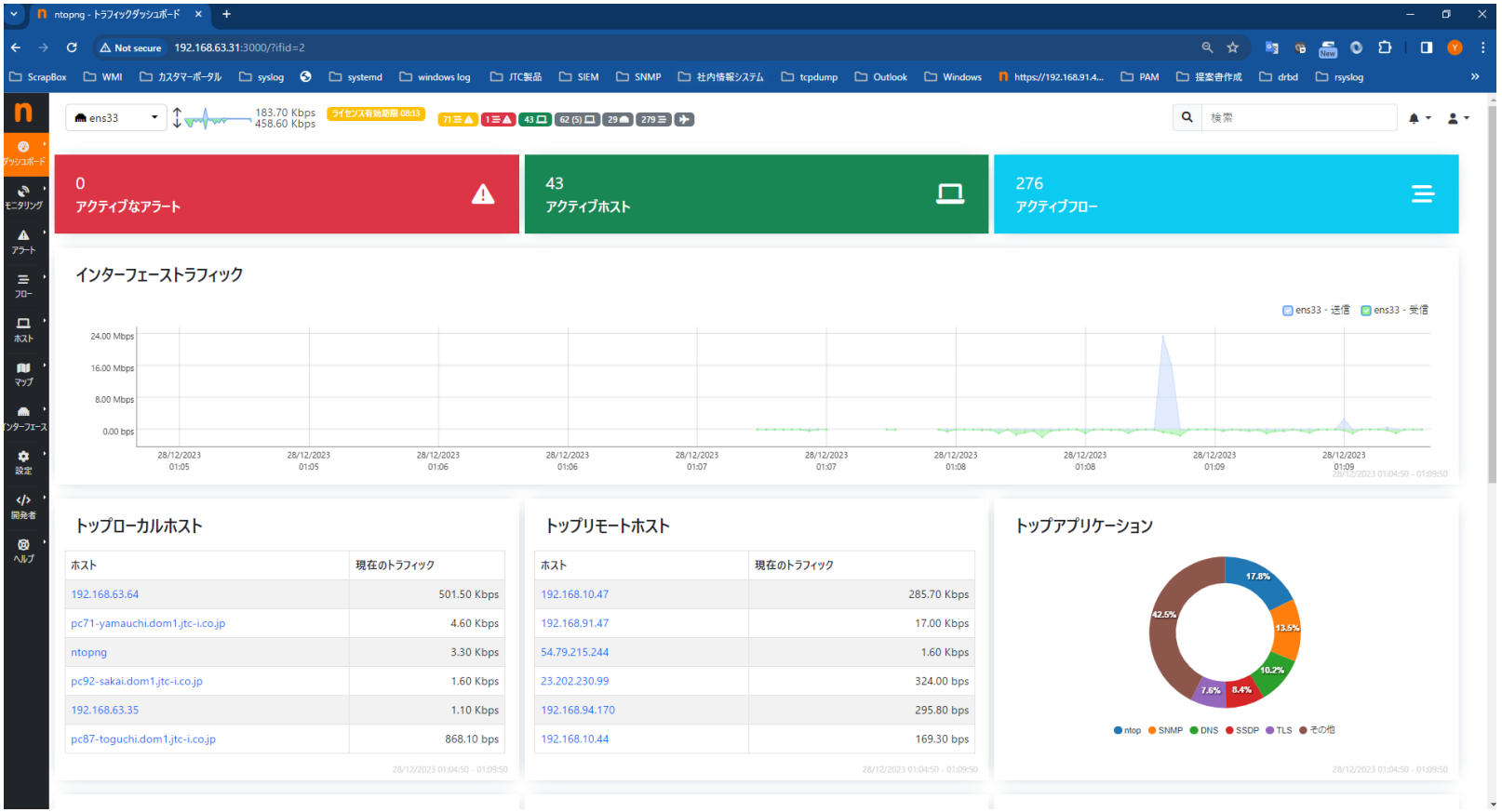
ntopngのインストール(14)

“Change Passowrd”画面が表示され、パスワード変更が求められますので任意のパスワードを設定してください。「Change Password」ボタンをクリックし、次に進んでください。



ntopngのインストール(15)

以下の画面の様にntopngのダッシュボードが表示されれば、起動確認は完了です。本画面のようなリッチな画面は商用版で起動している証拠です。10分経過するとフリー版の画面に遷移ますので適宜再起動をして商用版の機能をお楽しみください。



5. NIC直接監視評価パターン

本章では以下のバージョンを使用しています。

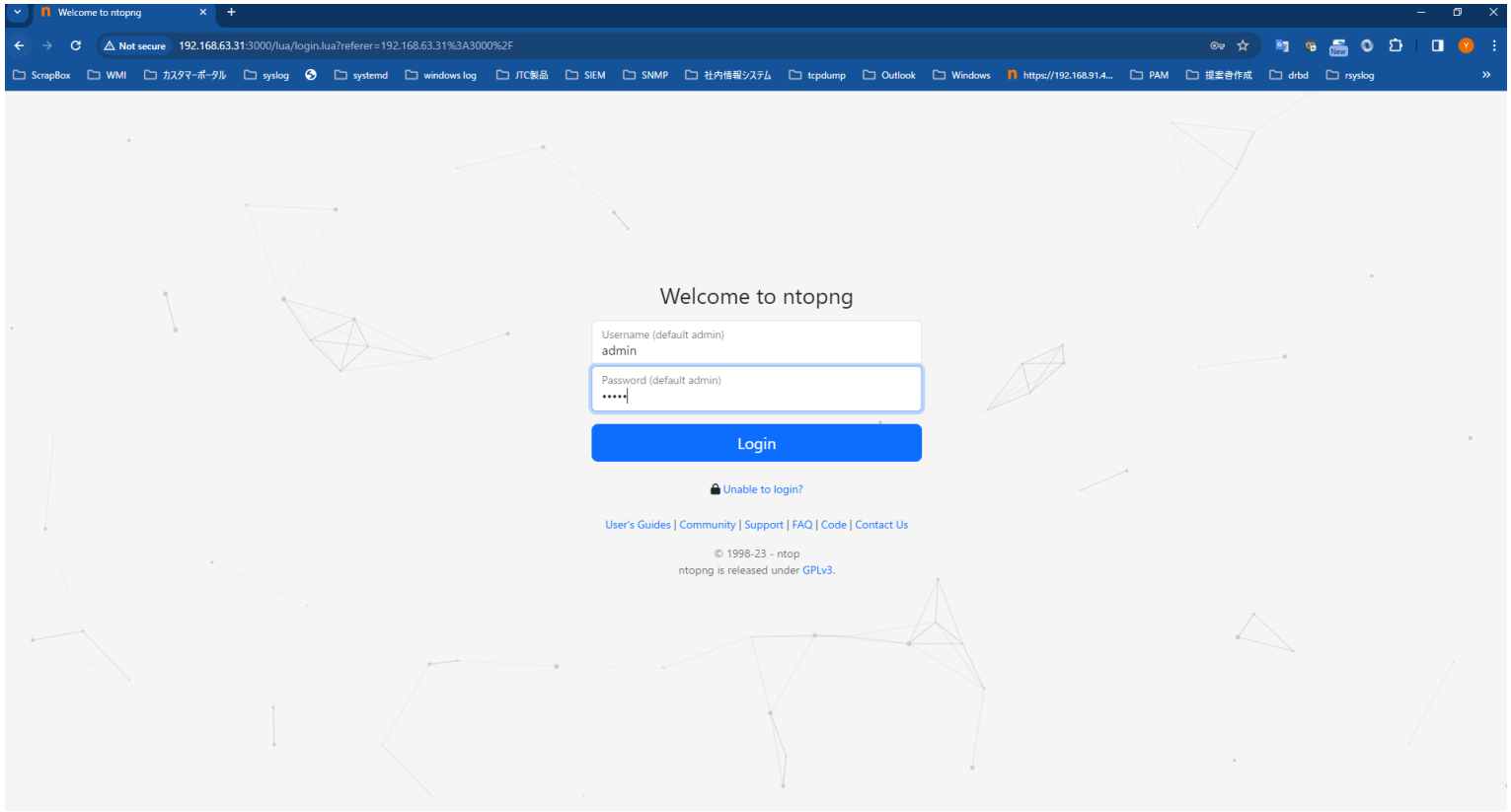
◆Windows 11 x64
◆nProbe 10.X and ntopng v6.X Stable版
◆VMware Workstation 17

ntopng NIC直接監視評価環境

弊社サイトからダウンロードしたISOイメージは、ntopngが直接自NICを監視する設定が施してあります。本章では、下図の直接自PCのNICを監視する設定環境をご紹介します。

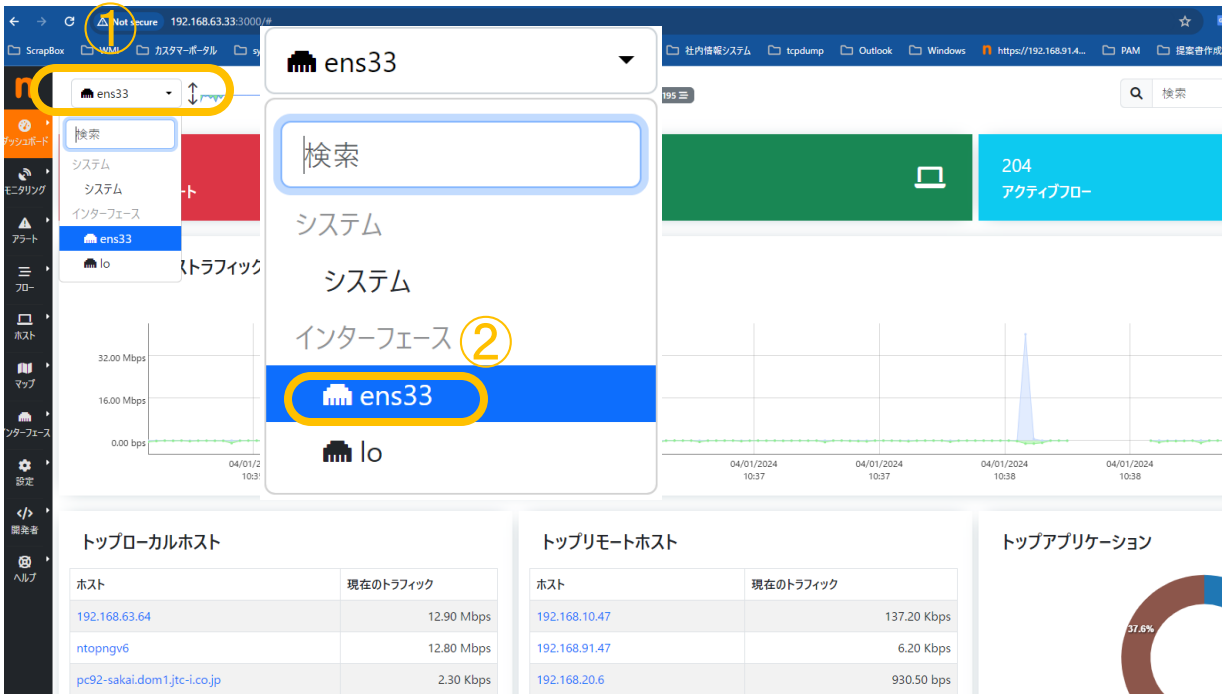
ntopngへのアクセス(1)

ntopngのWEBインターフェイスに進みます。http://<UbuntuのIPアドレス>:3000にアクセスしてください。ユーザ名:admin　パスワード: ntopdemoでログインすると次スライドの画面が表示されます。



ntopngへのアクセス(2)

ntopngのWEBインターフェースに進みます。ログイン後画面左上のプルダウンメニューを押し、本マニュアル「初期設定(1)」で確認したデバイス名を選択してください。



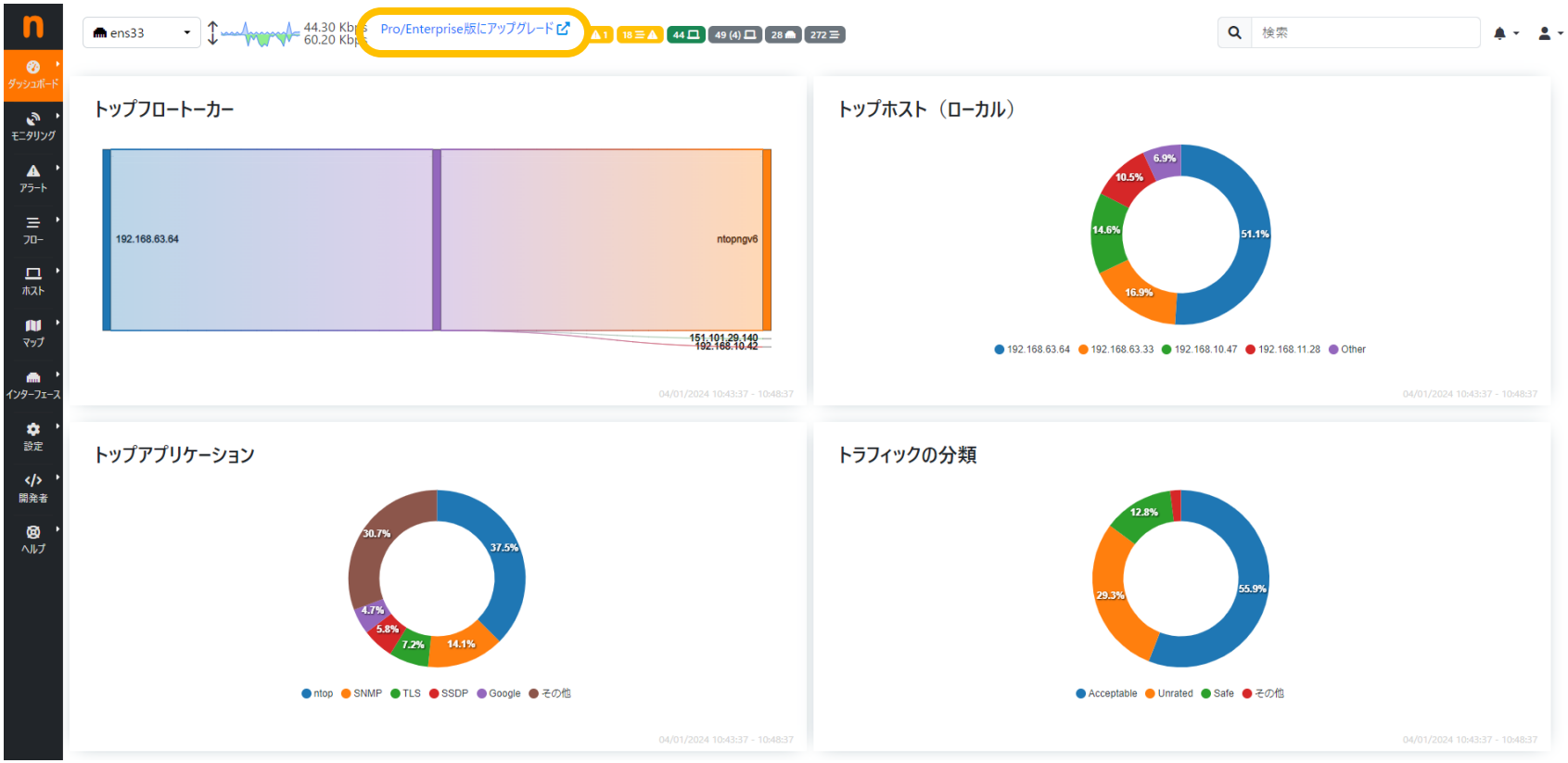
※本来であれば、ここで選択するデバイスは、ルータ、スイッチ等のミラーポートに接続されたデバイスとなります。本環境は、あくまでntopngの単体評価が目的なので自端末のネットワークに接続されたNICを監視対象としています。

ntopngへのアクセス(3)

選択したインターフェイスに流れるトラフィックが表示されます。最初に表示される画面は、トラフィックダッシュボードとなり、ローカルホスト及びリモートホストのトラフィックが表示されます。また、画面上部に「ライセンスはXX:XXに期限切れします」と表示されます。こちらの時間が0となると、ntopngはコミュニティ版にダウングレードします。

ntopngへのアクセス(4)

参考にコミュニティ版にダウングレードした場合のダッシュボード画面をご紹介します。有用な様々な画面が表示されなくなります。



6. ntopng Enterprise版評価方法

Enterprise版評価方法

ntopngは起動から10分でコミュニティ版にダウングレードします。※10分間しかEnterprise版を評価できませんのでご注意ください。コミュニティ版とEnterprise版では大きく機能差があります。

Enterprise版評価を実行する為に、Webブラウザの右画面人型マークをクリックし、ntopngを再起動してください。

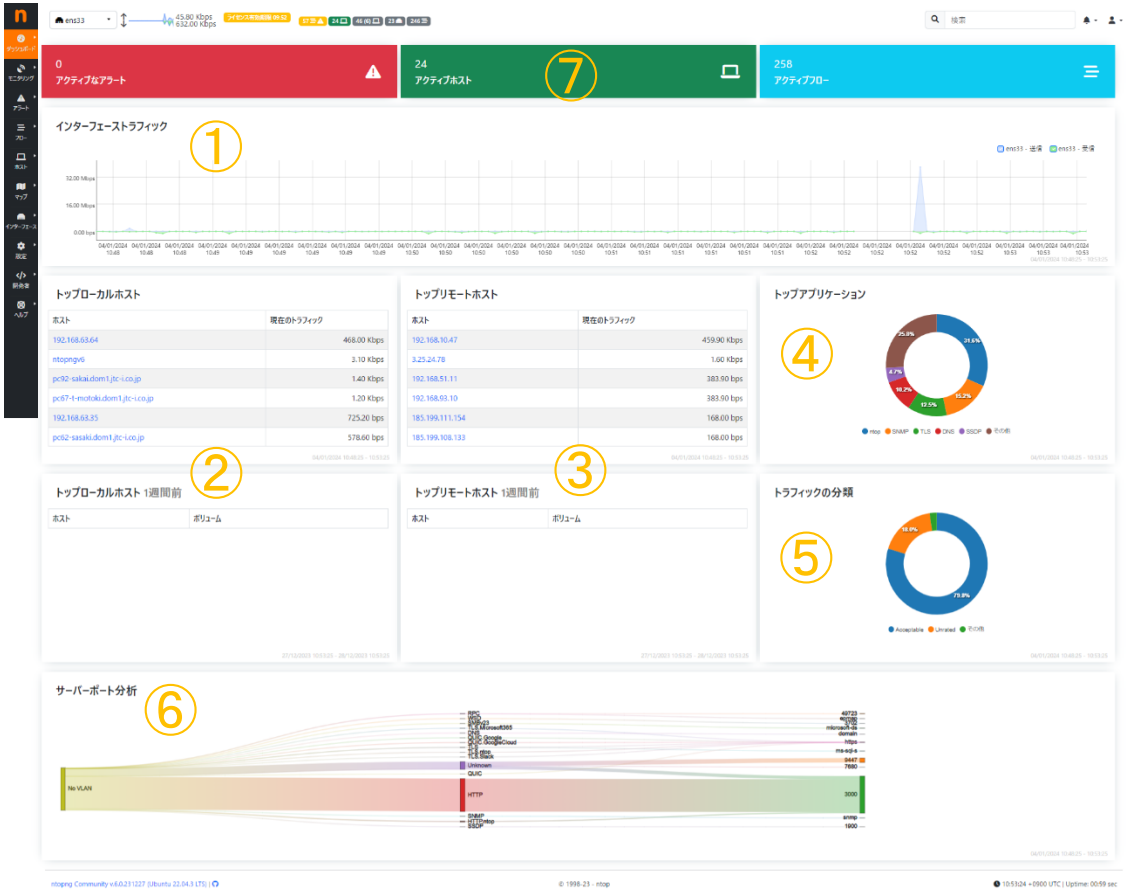
7. ntopng NIC直接監視評価 基本画面説明

ntopngは非常に多くの画面・グラフが存在します。本評価ガイドでは、その一部をご紹介いたします。

※より詳細に関しては、弊社デモをご用命ください。

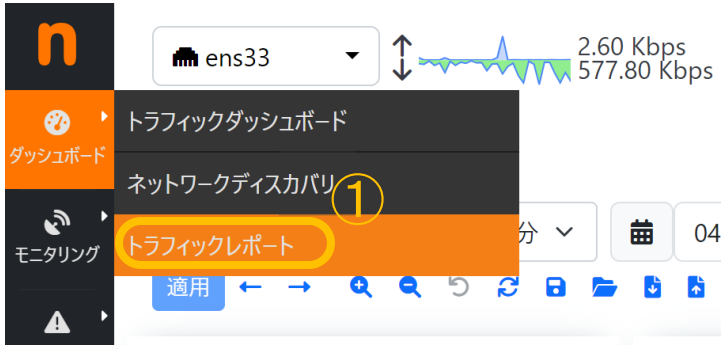
トラフィックダッシュボード画面

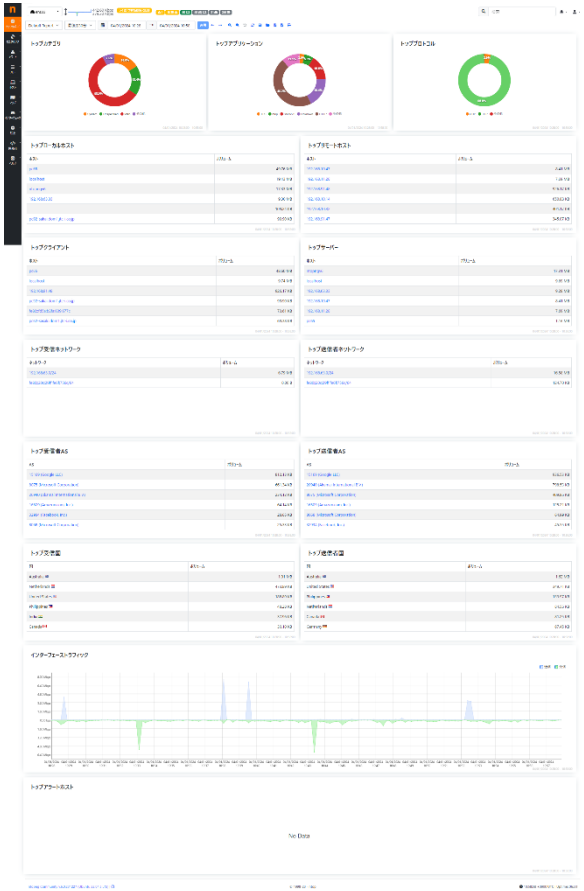
ntopngのトップ画面「トラフィックダッシュボード」は、全てリアルタイム表示となり、次の7種類のトラフィック情報を確認できます。①「インターフェイストラフィック」②「トップローカルホスト」③「トップリモートホスト」④「トップアプリケーション」⑤「トラフィックの分類」⑥「サーバーポート分析」⑦「アクティブアラート/ホスト/フローへのリンク」があり、インターフェイストラフィックでは監視対象全てのインターフェイスのトラフィック量をリアルタイムで監視することができます。



トラフィックレポート画面

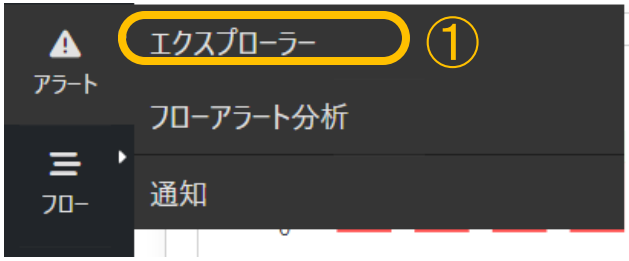
画面左メニューの「ダッシュボード」から①「トラフィックレポート」をクリックすると、ネットワークインターフェイスのトラフィック量、ローカル/リモートの通信割合、アプリケーション、アプリケーショントラフィック割合、トップローカルホスト、トップリモートホストといった情報を日時を指定してレポートを作成することができます。本機能によって、日・週・月ごとのレポートを作成することができます。

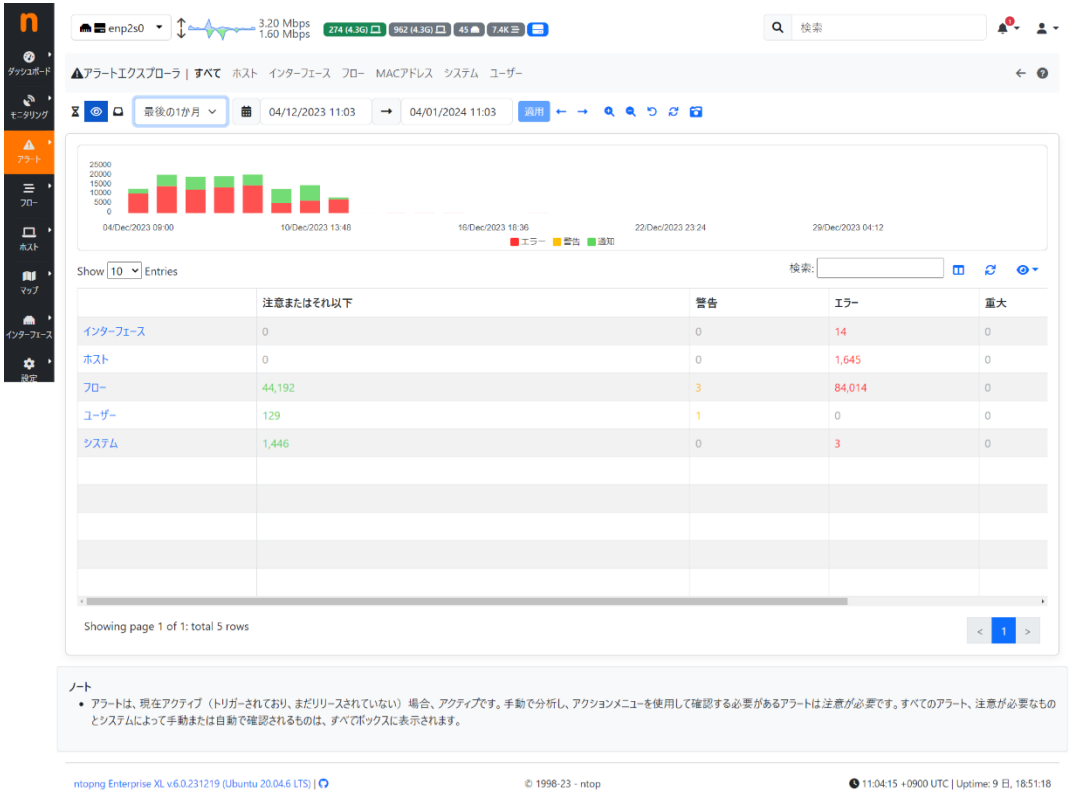




アラートエクスプローラ画面

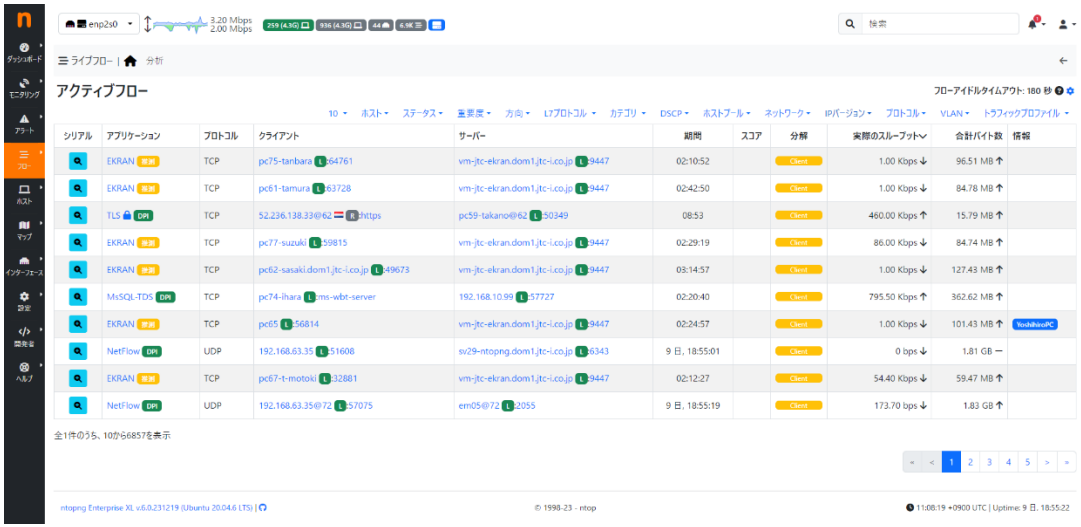
画面左メニューの①「エクスプローラ」をクリックし、現在・過去に発生したアラートの一覧を確認することができます。本機能によって、監視ネットワークの異常をいちはやく検知し、素早いアクションを起こすことが可能です。





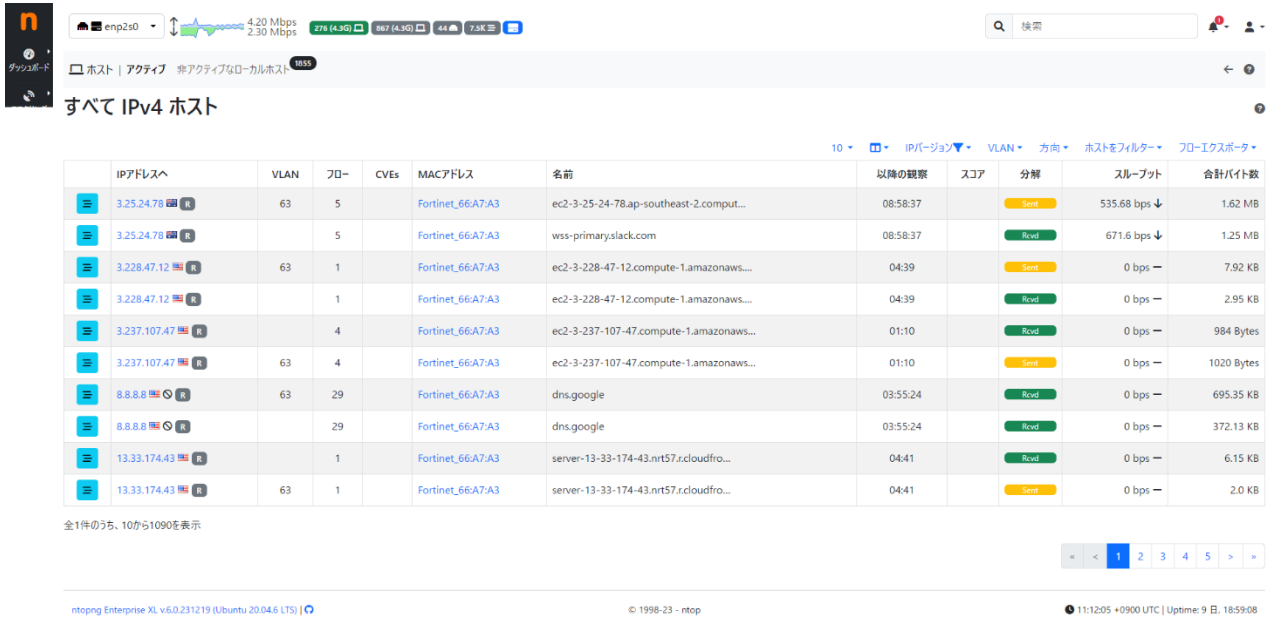
ライブフロー画面

画面左メニューの「フロー」をクリックし「ライブ」を選択すると、リアルタイムで流れているフローの一覧が表示されます。アプリケーション、クライアント、サーバーといった項目はリンクとなっておりそれぞれのメニューにジャンプすることができます。また、フィルタに「ホスト」「状態」「方向」「アプリケーション」「カテゴリ」「IPバージョン」があり、それぞれソートすることができます。本機能によって、現在発生している通信をリアルタイムで確認することができます。



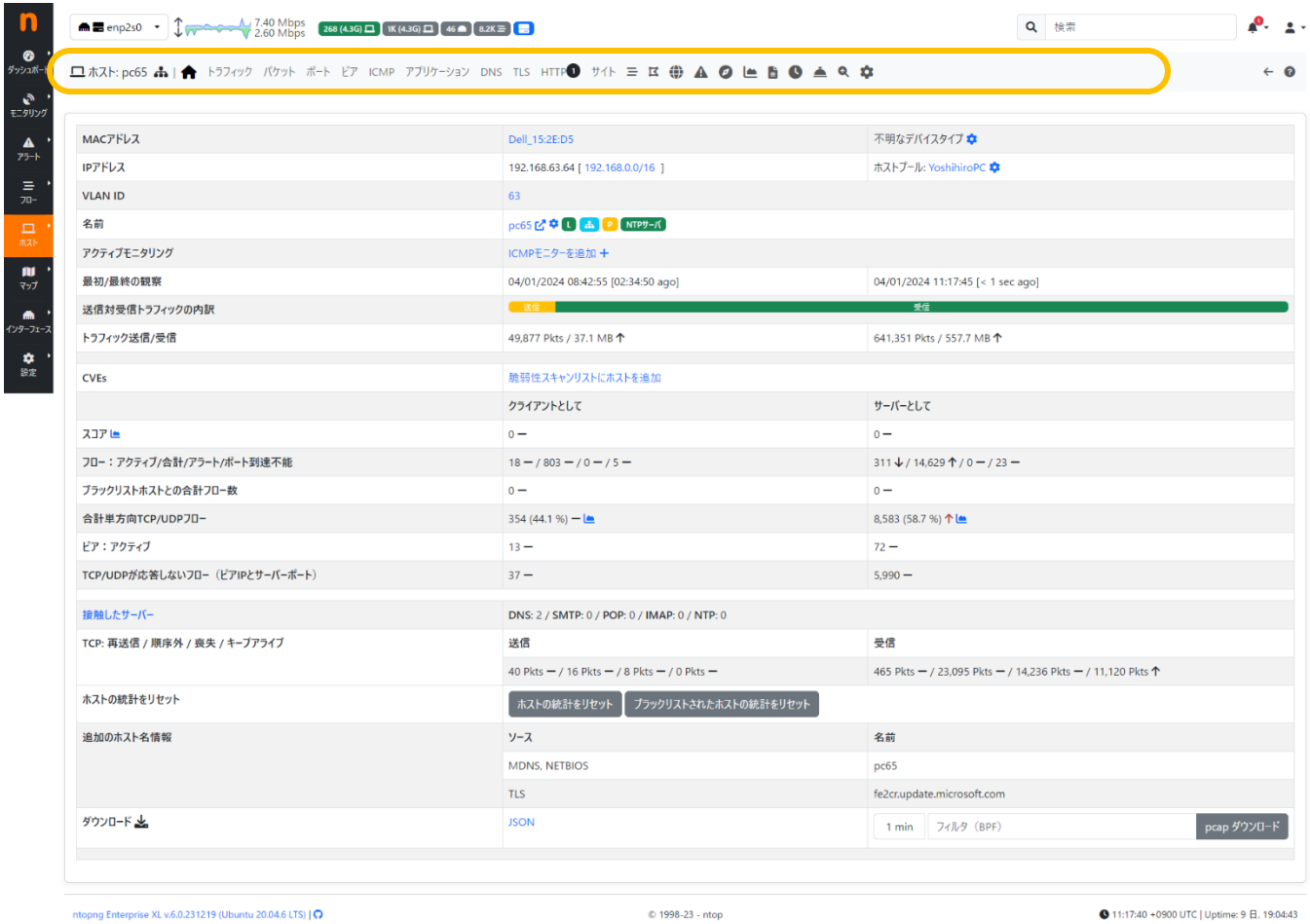
ホスト画面(1)

画面左メニューの「ホスト」から「ホスト」をクリックすると、アクティブなホスト一覧が表示されます。IPアドレスはリンクになっています。「分解」はトラフィック送受の割合。ホストごとの「スループット」、「合計バイト」を確認できます。さらに詳細はIPアドレスのリンクをクリックするとそれぞれのホストごとのトラフィックを解析することができます。



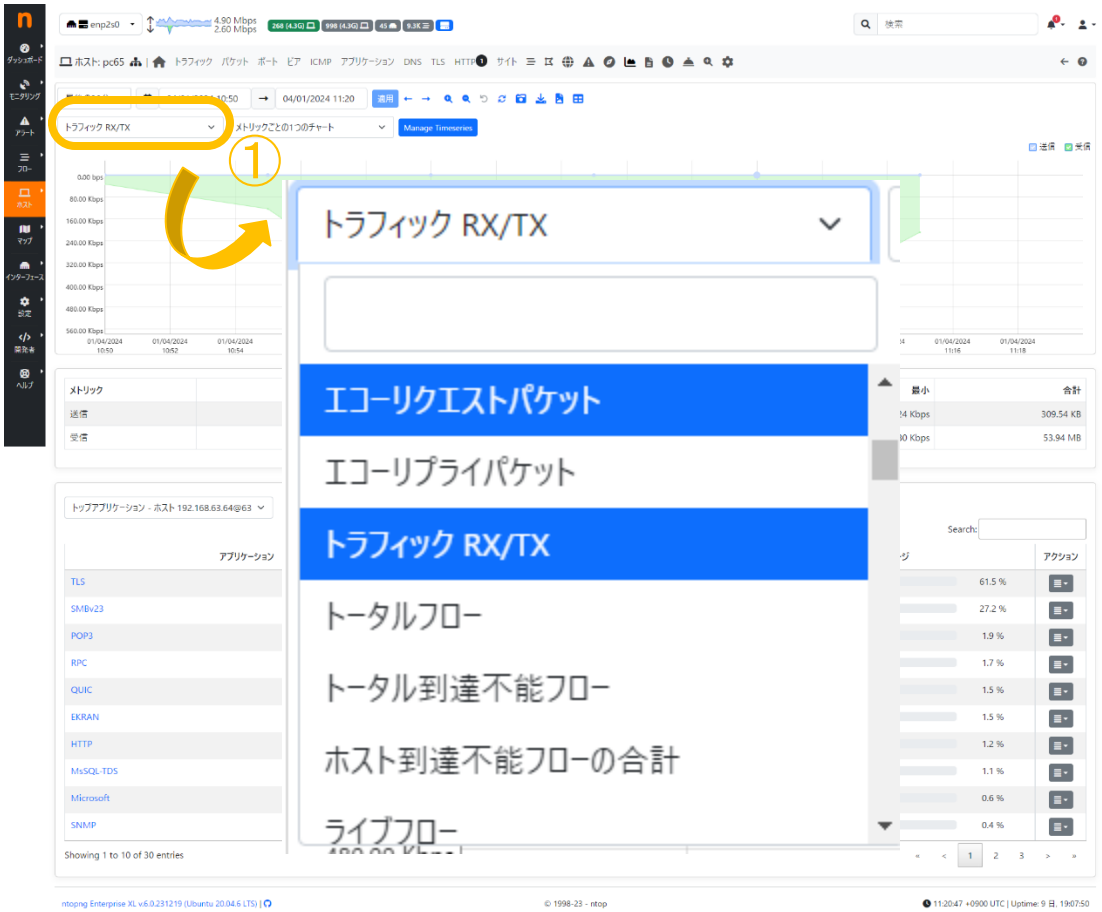
ホスト詳細画面(2)

画面は「pc65」をクリックしたものです。メニューに「ホーム」「トラフィック」「パケット」「ポート」「ピア」「ICMP」「アプリケーション」..「グラフ」「設定」等のメニューがあり、ホスト単位に分析をすることができます。



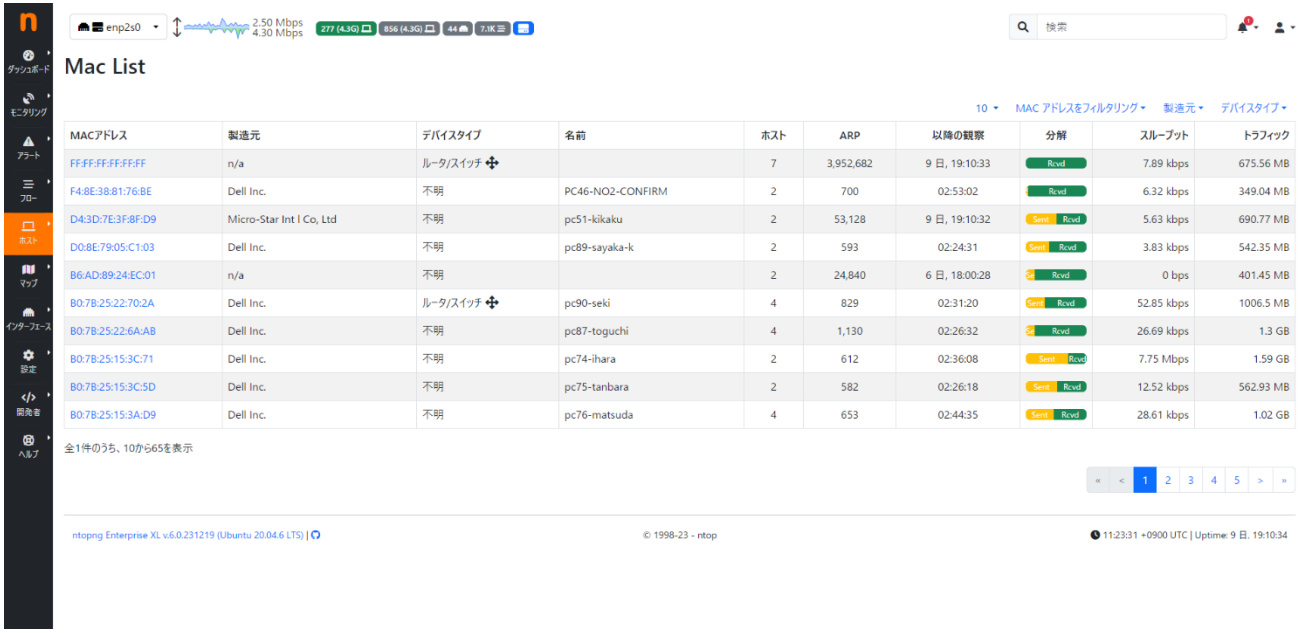
ホスト画面(3) グラフ

画面は「pc65」の「グラフアイコン」クリックした画面です。該当ホストのみのトラフィック情報が表示され、過去～現在のトラフィックを分析することができます。画面①のプルダウンをクリックするとL4/L7/カテゴリといったより詳細な項目で該当ホストのトラフィック分析ができます。



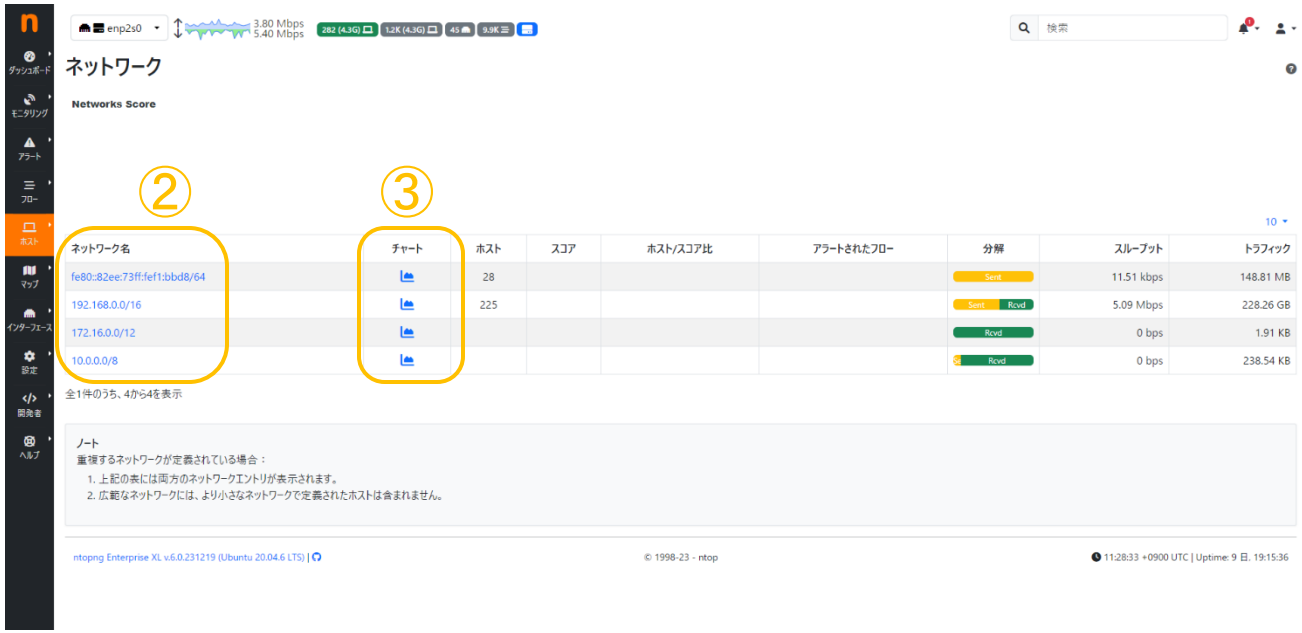
MACアドレス画面

画面左メニューの「ホスト」から「MACアドレス」をクリックすると、所属ネットワーク内で確認できるMACアドレス一覧を表示し、ホストのトラフィック情報を表示します。さらに詳細はMACアドレスのリンクをクリックすれば、ホストごとのトラフィックを解析することができます。



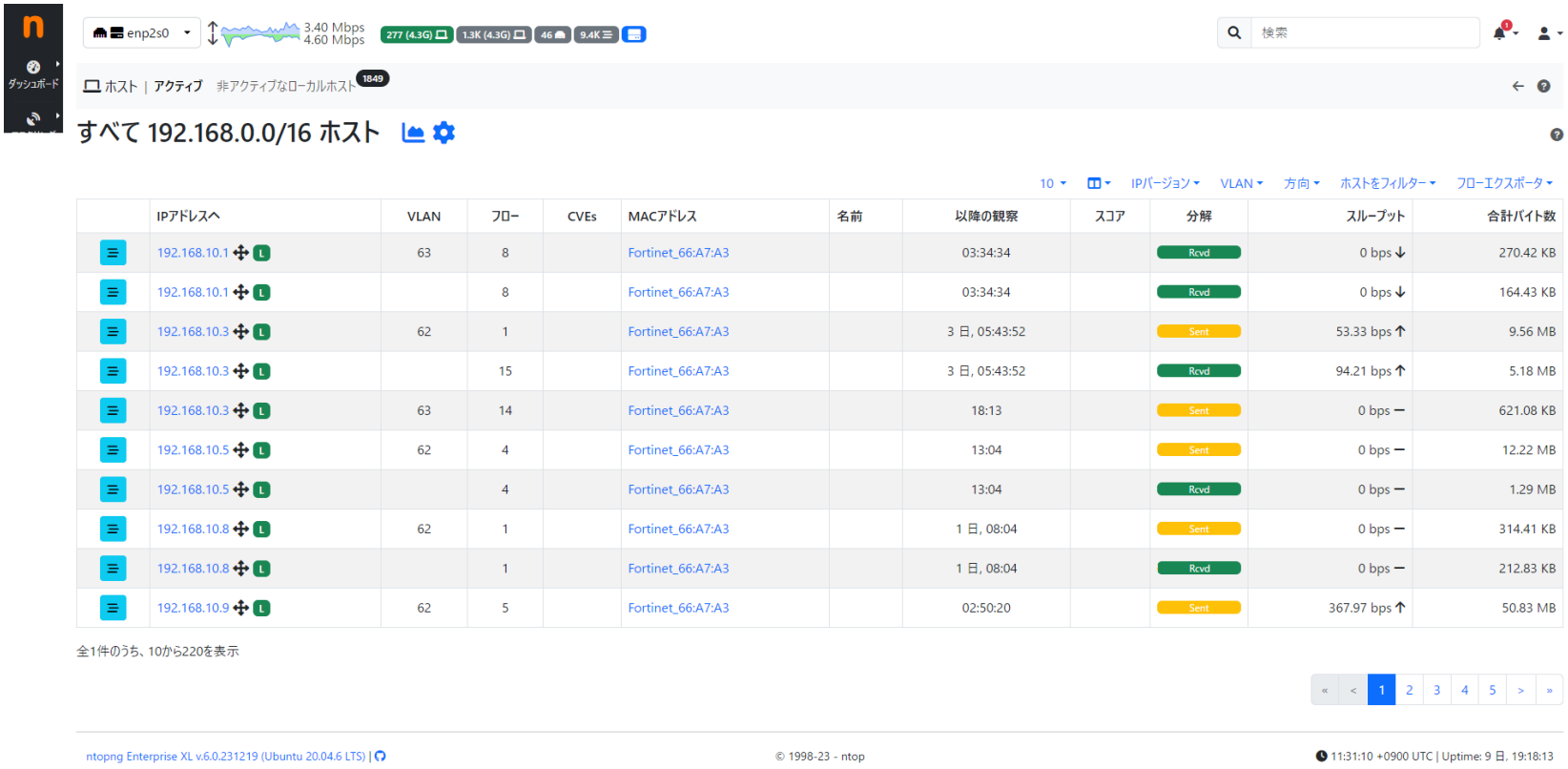
ネットワーク画面(1)

画面左メニューの「ホスト」から「ネットワーク」をクリックすると、所属ネットワークで確認できるサブネットごとのトラフィック状況を確認することができます。②のサブネットリンクと③グラフリンクをクリックすると、トラフィック詳細を解析することができます。



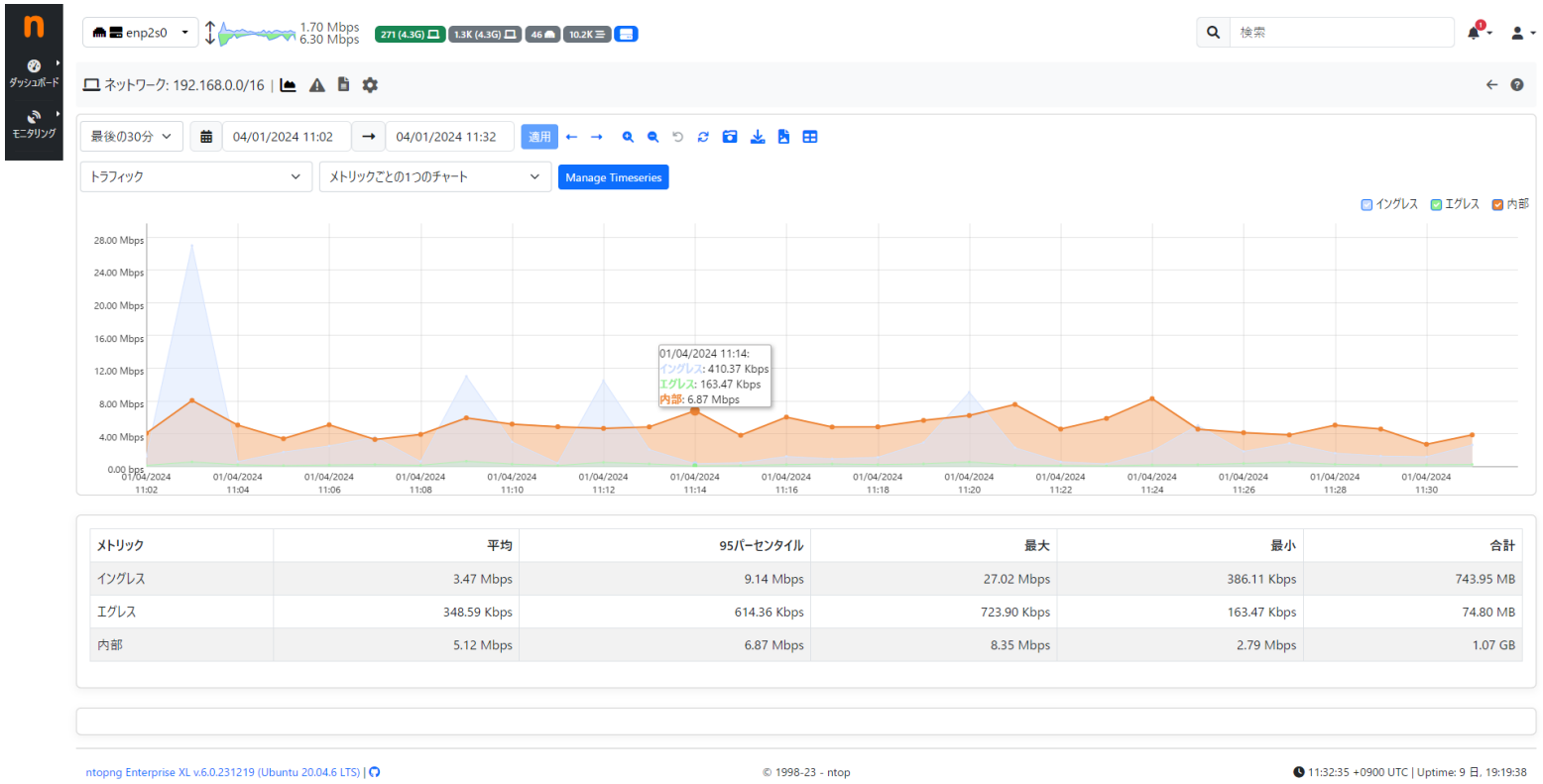
ネットワーク画面(2)

画面は、前スライドページ(ネットワーク画面(1))の「192.168.0.0/16」サブネットリンクをクリックしたものです。サブネットに所属しているホストの一覧が表示されます。



ネットワーク画面(3)

画面は、前スライドページ(ネットワーク画面(1))の「192.168.0.0/24」グラフリンクをクリックしたものです。中長期視点で対象とする時間帯を絞った分析をすることができます。

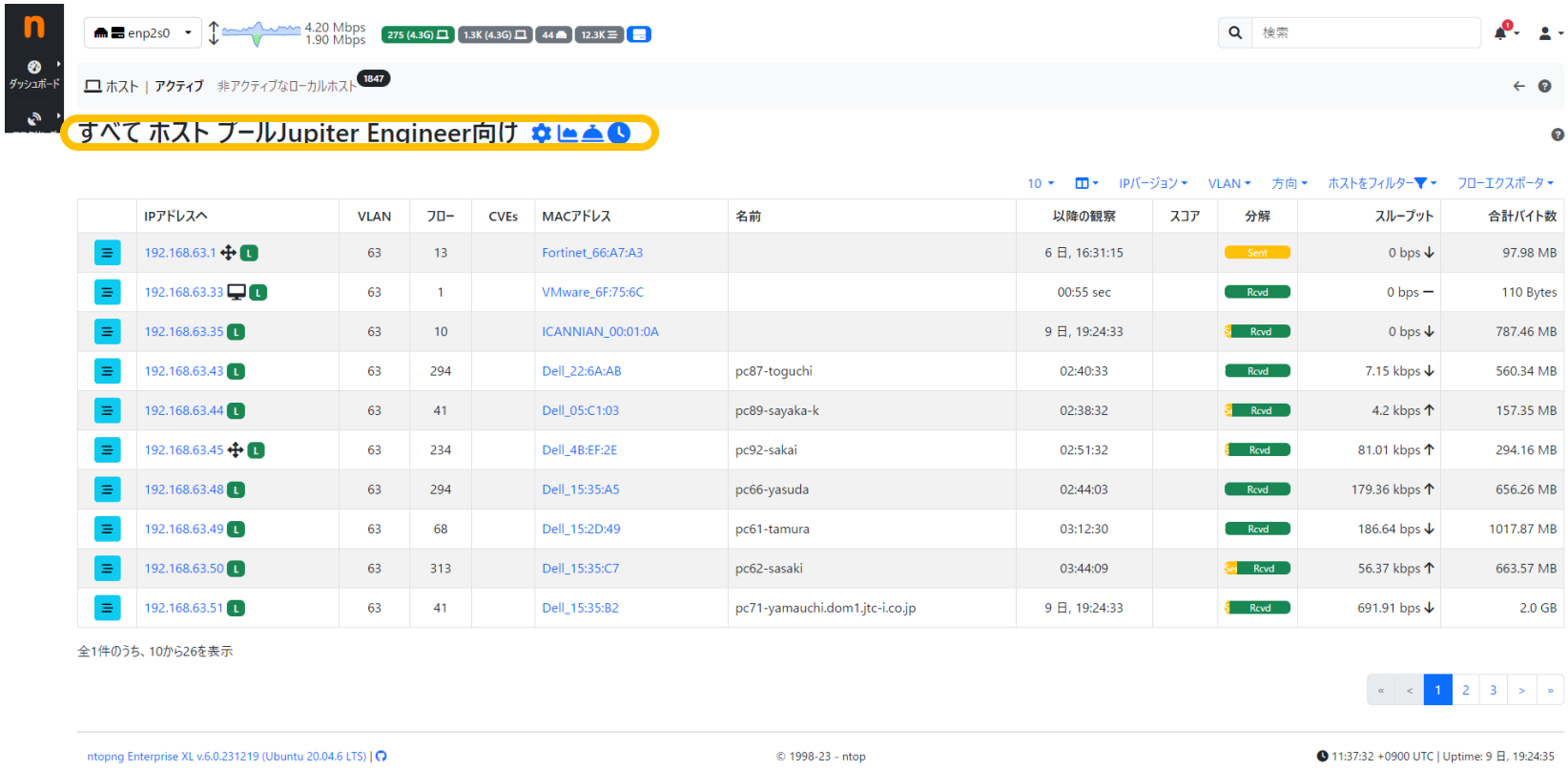


ホストプール画面(1)

画面左メニュー「ホスト」から「ホストプール」をクリックすると、ホストプールリスト画面が表示されます。②の「歯車」ボタンを押すとホストプールの編集をすることができます。設定した「プール名」リンクをクリックすると、ホストプールの詳細トラフィック情報を確認することができます。

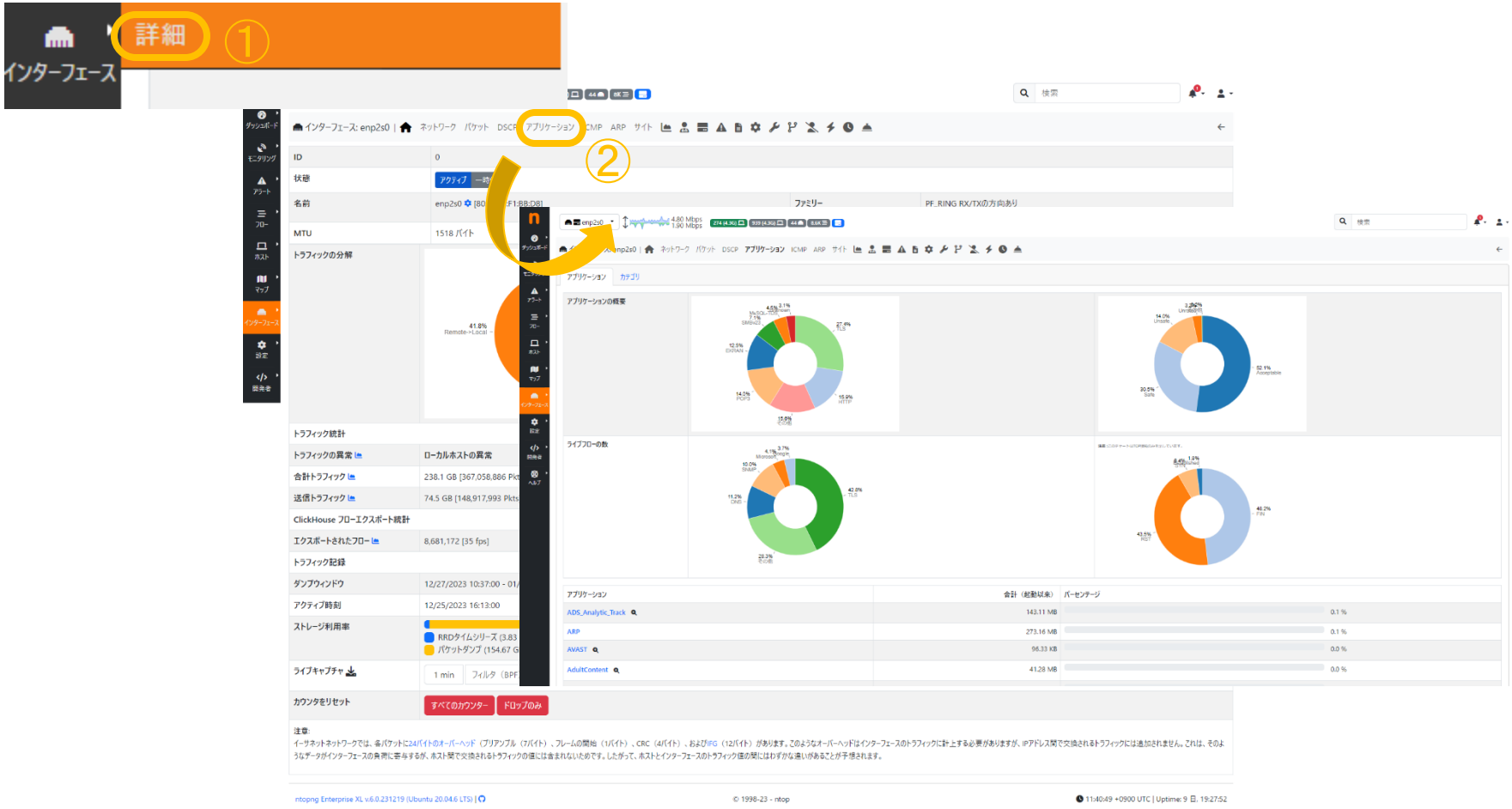
ホストプール画面(2)

画面は別途作成した「Jupiter Engineer」ホストプール画面となります。設定したサブネット通りの表示になっていることが確認できます。本機能を利用して組織・部署といったサブネット区分けができる環境であればサブネットごとのトラフィック量や分析が容易となります。



インターフェィス画面

画面左メニューの「インターフェイス」から「詳細」、そして「アプリケーション」を選択した画面です。この画面でL7トラフィックまで確認することができ、対象インターフェィスの利用状況・どのアプリケーションが帯域を占有しているかを確認することができます。



8. ntopng+nProbe xFlow受信評価パターン

本章では以下の設定方法をご案内します。

1. ntopng and nProbe評価環境
2. ntopng設定変更
3. nProbe設定変更
4. ntopng正常動作確認

ntopng + nProbe評価準備(1)

ntopng+nprobe環境を評価するには以下の準備が必要です。先ずはnprobeの設定変更を実施します。

```
$cd /etc/nprobe
$sudo cp –p nprobe.conf.ntopng.sample nprobe.conf
$sudo vim nprobe.conf
～snip～
#--collector-port=6363
--collector-port=2055
～snip～
:wq!
$sudo systemctl restart nprobe
$ sudo systemctl status nprobe
● nprobe.service - nprobe extensible NetFlow v5/v9/IPFIX probe/collector
   Loaded: loaded (/etc/systemd/system/nprobe.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2024-01-04 11:49:06 JST; 4s ago
```

上記の標準出力のように、Active: activeとなっていればnprobeは正常に起動しております。上記では、nprobeの受信ポートを6363/udpから2055/udpに変更しております。

ntopng + nProbe評価準備(2)

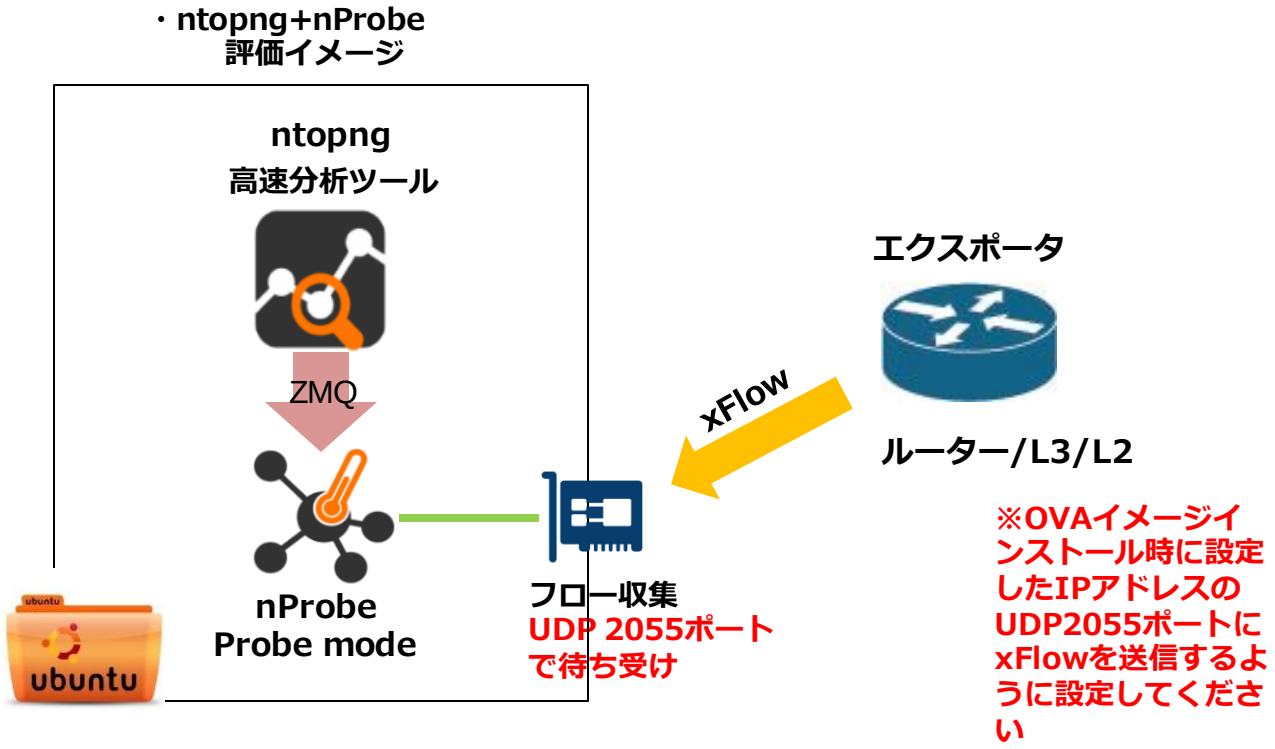
次にntopngの設定変更を実施します。以下では、ntopng.confに-i=で始まる2行を追加しております。-i=ens33の設定は、環境によって異なりますので適宜ご自身のNICデバイス名を確認し変更してください。

```
$cd /etc/ntopng
$sudo vim ntopng.conf
～snip～
-F=clickhouse;127.0.0.1;ntopng;default;default
-i=tcp://127.0.0.1:5556
-i=ens33
～snip～
:wq!
$ sudo systemctl status ntopng
● ntopng.service - ntopng high-speed web-based traffic monitoring and analysis tool
   Loaded: loaded (/etc/systemd/system/ntopng.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2024-01-04 11:57:25 JST; 4s ago
```

上記の標準出力のように、Active: activeとなっていればntopngは正常に起動しております。

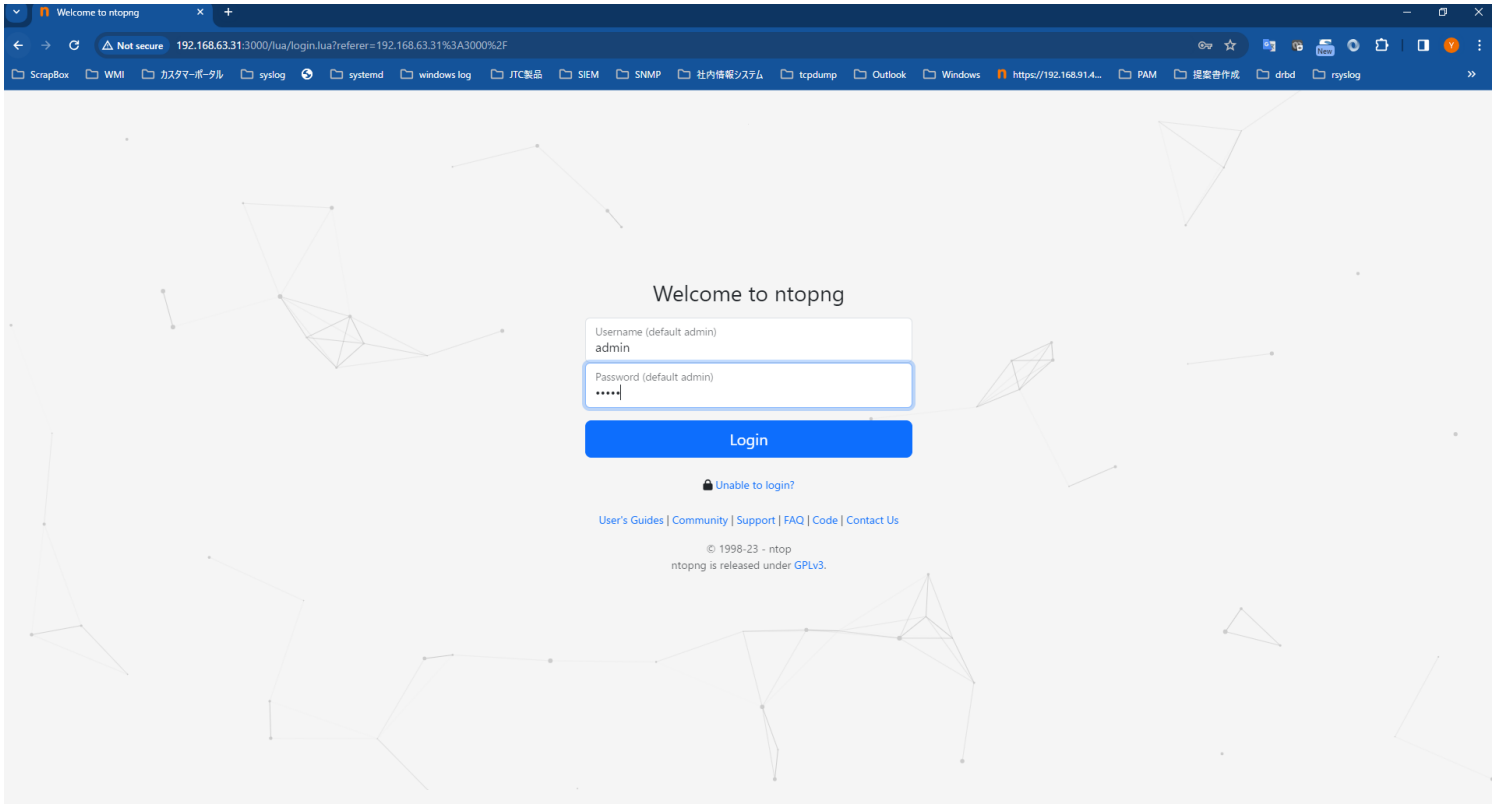
ntopng + nProbe評価環境

貴社設置のルーター等がxFlow(NetFlow v9/v5, sflow v5等)をエクスポートできる場合、本モードを利用してフローを収集することができます。



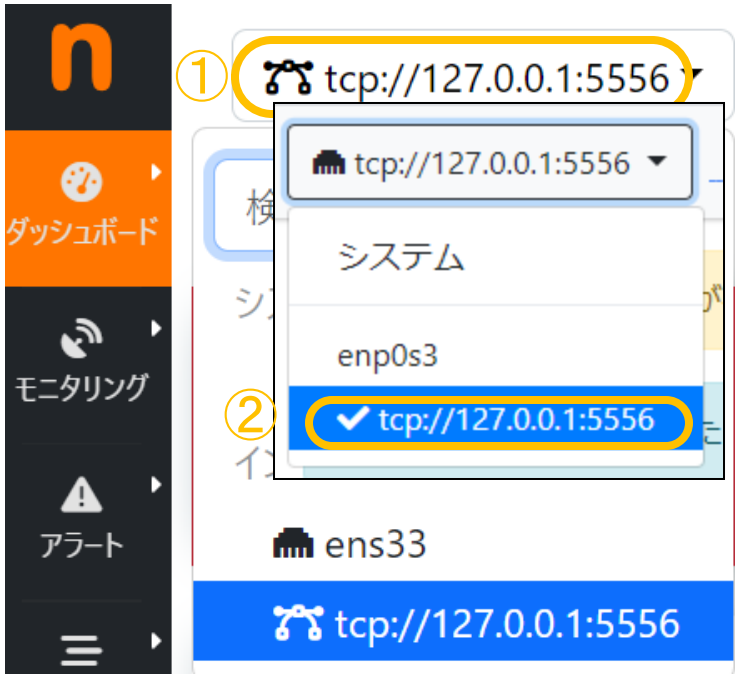
ntopngへのアクセス(1)

ntopngのWEBインターフェイスに進みます。http://<UbuntuのIPアドレス>:3000にアクセスしてください。ログインすると次スライドの画面が表示されます。



ntopngへのアクセス(2)

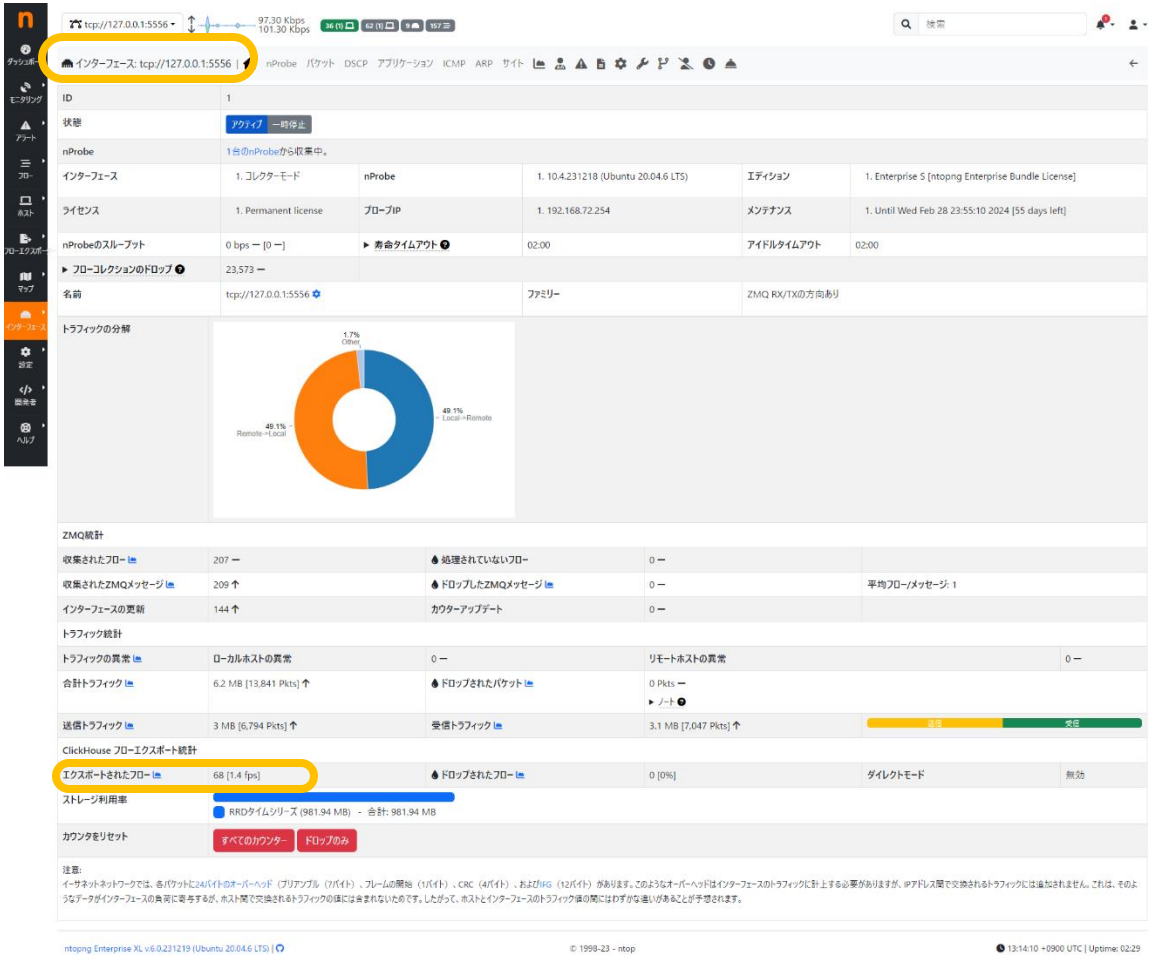
ntopngのWEBインターフェースに進みます。ログイン後画面左上のプルダウンメニューを押し、本マニュアル「tcp://127.0.0.1:5556」を選択してください。



※「enp0s3」がUbuntuのNICを監視するインターフェイス。「tcp://127.0.0.1:5556」がxFlowを受信するインターフェイスとなります。

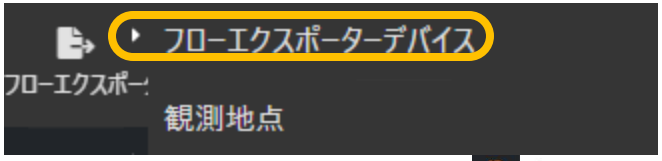
ntopng+nProbeの動作確認(1)

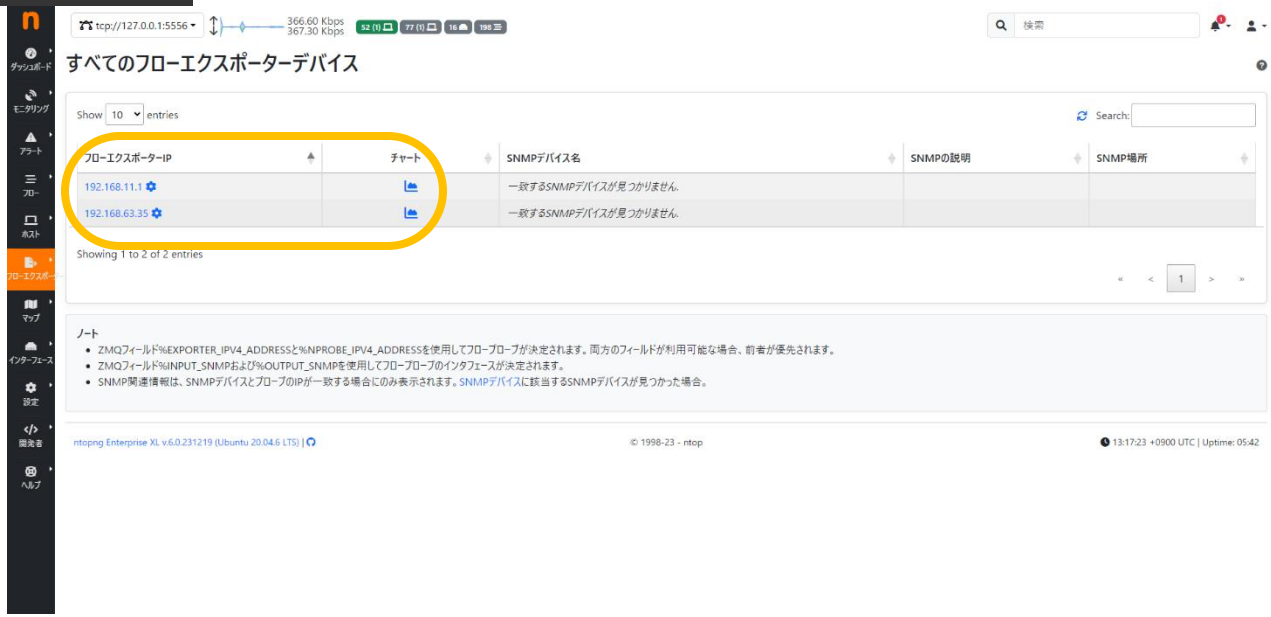
①「tcp://127.0.0.1:5556」が選択されていることを確認し、画面左メニューの「インターフェイス」を押してください。xFlowを正しく受信している場合は画面中段に「エクスポートされたフロー」がカウントアップされます。



ntopng+nProbeの動作確認(2)

画面左メニューの「フローエクスポータ」、「フローエクスポーターデバイス」を押してください。Ubuntuに設定したIPアドレスのUDP2055ポートにxFlowを送信しているエクスポータが存在する場合は、「フローエクスポータIP」にエクスポータのIPアドレスが表示されます。





※画面操作は、NICの直接監視と同様となります。また、エクスポータごとに仮想インターフェイスを作成することも可能です。詳細は弊社までお問い合わせください。

9. お問い合わせ先

ジュピターテクノロジー株式会社

〒183-0023
東京都府中市宮町一丁目40番地
KDX府中ビル6F

Tel　042-358-1250
Fax　042-360-6221
URL　http://www.jtc-i.co.jp/

技術サポートに関するお問合せ
https://www.jtc-i.co.jp/support/customerportal/index.php