

Startup Guide

スタートアップガイド はじめにお読みください

856-127905-001-00 2008年 10月 初版



© NEC Corporation 2008
弊社の許可なく複製・改変などを行うことはできません。
このマニュアルは再生紙を使用しています。

箱を開けてから本装置の初期設定を完了するまでの手順を説明します。
このスタートアップガイドに従って作業してください。

1 添付品を確認する

梱包箱を開け、添付品がそろっていることを確認してください。添付品の確認は、装置に添付の「構成品表」を参照してください。

重要 添付のCD-ROMは、再セットアップの時に必要となりますので大切に保管しておいてください。

- *1 ご注文の構成により、本体に実装されている場合があります。ハードディスクドライブ取り付けネジは特殊ネジです。大切に保管してください。
- *2 バックアップCD-ROMの中には「ユーザーズガイド」や各種オンラインドキュメントも格納されています。ユーザーズガイドやオンラインドキュメントはAdobe Readerで閲覧できるPDFファイルです。

2 ユーザーズガイドを読む

ユーザーズガイドはバックアップCD-ROMの中に格納されています。ユーザーズガイドはAdobe Readerで閲覧できるPDFファイルで、次のHTMLファイルから表示させることができます。

<バックアップCD-ROM>:/NEC/manual.html

ユーザーズガイドでは、本装置を安全に取り扱うための注意事項やStartup Guideでは記載されていないセットアップに関する詳細な説明、運用やアップグレードに関する説明が記載されています。また、「故障かな?」と思ったときのトラブル回避の手段やサービスに関する情報も記載されています。本装置を取り扱う前にぜひお読みください。

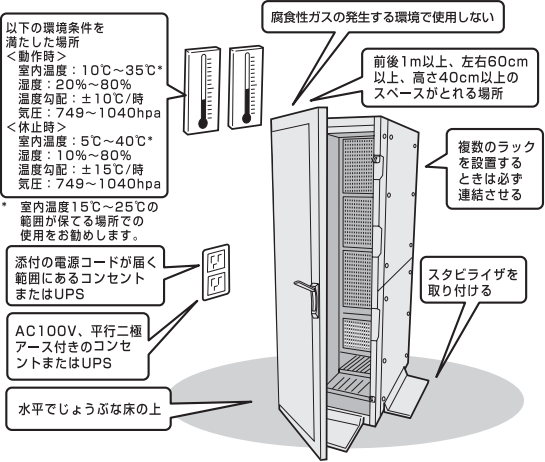


ヒント PDFファイルを閲覧するためには、Adobe Reader 日本語版が必要です。Adobe Readerはアドビ社のWebサイトから無償でダウンロードすることができます (http://www.adobe.co.jp)。

3 ラックを設置する

本体はEIA規格に適合した19型(インチ)ラックか、卓上に設置して使用します。ラックに設置する場合は、次の条件を守ってラックを設置してください。

重要 ラックの設置は必ず複数名で行ってください。



安全に関するご注意

装置をセットアップする前に「ユーザーズガイド」の「使用上のご注意 -必ずお読みください-」をお読みの上、注意事項を守って正しくセットアップしてください。

警告

- めれた手で電源プラグの抜き差しをしないでください。感電するおそれがあります。
- 雷が降り出したらケーブル類を含め装置に触らないでください。落雷による感電のおそれがあります。
- 「ユーザーズガイド」に記載されている内容を除き、分解・修理・改造を行わないでください。

注意

- 持ち運びの際は2人以上で装置の底面をしっかりと持って運んでください。
- 水、湿気、ほこり、油、煙の多い場所、また直射日光の当たる場所に設置しないでください。
- 装置に添付されている電源コード以外を使用しないでください。
- 電源コードは指定の電圧で、アース付きのコンセントに接続してください。
- 電源コードはタコ足配線にしないでください。

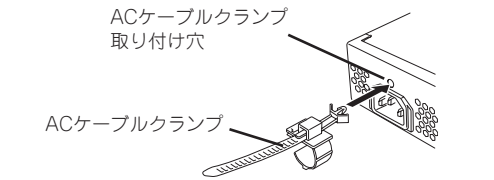
4 本体を設置する

本体を卓上またはEIA規格に適合した19型(インチ)ラックに設置します。

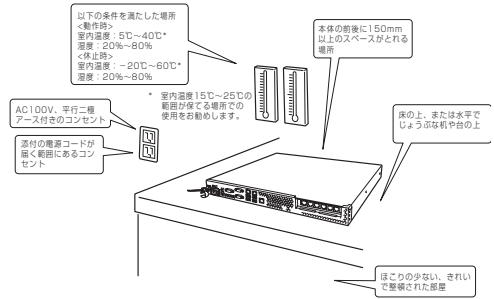
重要 本体を卓上またはラックに設置する前に必ず、本体の前面にACケーブルクランプを取り付けてください。

ACケーブルクランプの取り付け

本装置に添付のACケーブルクランプを本装置の前面の電源コネクタの上にあるACケーブルクランプ取り付け穴に「カチッ」とはまるまで差し込んで取り付けてください。

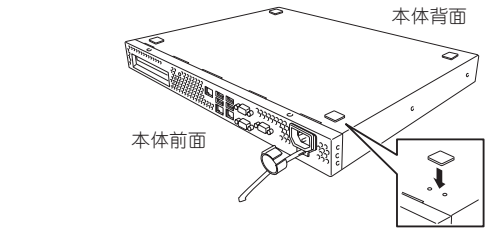


～卓上に設置する場合～



ゴム足の取り付け

本装置に添付のゴム足(滑り止め用)を本装置の底面に貼り付けてください(4か所)。



～ラックに設置する場合(ブラストライバが必要)～

以降に記載している本書のラックの設置方法は、下記の型番のラックに対応しております。

- ・NW19N176IP(SP) 35Uラック
- ・NW19N196IP(SP) 39Uラック

上記とは別の下記対応ラックへの本体の設置方法については、オプション設定しております下記ラック搭載キット添付の手順書に従ってください。

対応ラック

- ・N8140-74 13Uラック
- ・N8140-92 36Uラック
- ・N8140-93 36Uラック(増設用)
- ・N8140-94 24Uラック
- ・N8140-98 44Uラック
- ・N8140-99 44Uラック(増設用)

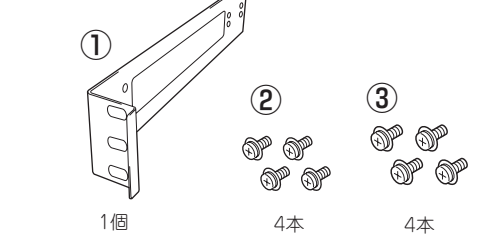
オプション

- ・BT0125-A0005 Express5800シリーズ 19インチラック用搭載キット

上記の対応ラック以外への本体の搭載は、お客様責任となることをご了承ください。

取り付け部品の確認

- ① マウントブラケット
- ② ネジA (M4)
- ③ ネジA (M5)



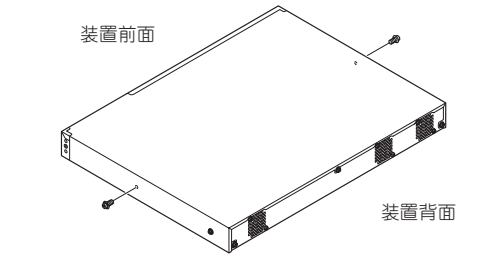
重要 ラックの設置や本体の取り付けは必ず複数名で行ってください。

5 ケーブルを接続する

本体前面にLANケーブルを接続した後、添付の電源コードを接続します。ユーザーズガイドの2章を参照してください。

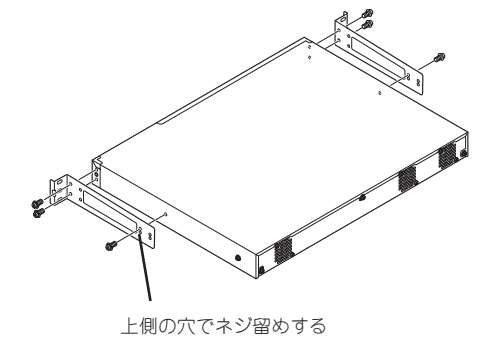
重要 シリアルポートコネクタには専用回線を直接接続することはできません。

1 本体装置の側面からM4ネジ(2本)を取り外す。

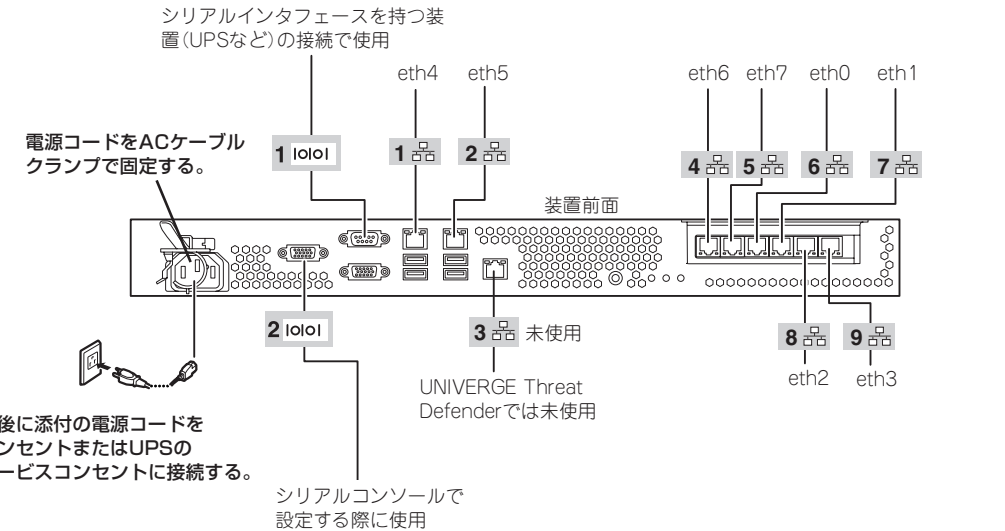
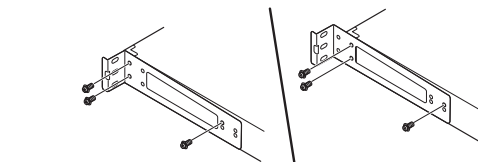


2 本体装置に添付されているマウントブラケットを取り付ける。

手順1で取り外したM4ネジ2本と本体装置に添付されているM4ネジ4本を使用します。



ヒント マウントブラケットの取り付け位置を変えることにより、ラック搭載位置を20mm奥にすることができます。



引き続きシステムのセットアップをします。裏面をご覧ください。➡➡➡➡➡


6 設定用PCのセットアップ

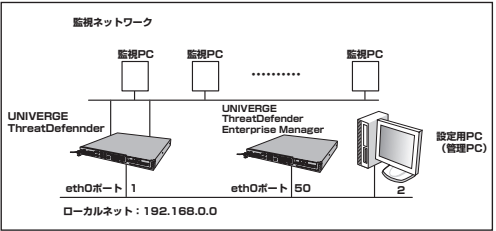
セットアップで使用する設定用PCの設定を行います。

- 1 設定用PCのIPアドレスを変更します。

工場出荷時には、以下のネットワーク構成を想定して設定しています。

設定用PCのIPアドレスを、192.168.0.2に設定します。

 ヒント 管理用ポート(eth0)と同じサブネットのIPアドレスを設定します。




- 2 設定用PCにSSH対応のクライアントソフトをインストールします。

7 SSH接続による設定変更

SSHのクライアントソフトでCounterACTにログインし、コマンド管理ツールを使ってドメイン名、管理用インタフェースIPアドレス、サブネットマスク、デフォルトゲートウェイの変更を行います。

1. SSH接続によるCounterACTのログイン

-  重要 設定用PCをUNIVERGE ThreatDefenderシリーズの管理用ポートeth0にクロスケーブルにて接続します。
- UNIVERGE ThreatDefenderシリーズの残りのポートにはケーブルを接続しないでください。

以下の内容をSSH v2対応のクライアントソフトに設定してCounterACTと接続します。

工場出荷時の設定	
IPアドレス	UNIVERGE ThreatDefender : 192.168.0.1 UNIVERGE ThreatDefender Enterprise manager : 192.168.0.50
TCPポート	22
サービス	SSHv2
ユーザ名	root
パスワード	nec123

2. ドメイン名、DNSサーバIPアドレスの変更


- 1 ドメイン名、DNSサーバの設定を変更するため、以下のコマンドを実行します。

fstool dns

- 2 メニューに従ってドメイン名とDNSサーバのIPアドレスを設定します。

[a]を入力しDNSサーバのアドレスを入力します。
[d]を入力しDNSサーバのアドレスを削除します。
セーブするために[s]を入力します。

3. メールサーバのホスト名の変更

 ヒント メールサーバを使用しない場合は、次のSSH接続許可IPアドレスの変更へ進んでください。

- 1 メールサーバのホスト名を変更するため、以下のコマンドを実行します。

fstool mail_conf

すると、以下のような画面が表示されるので1)Define mail-relay. を実行するため[1]と入力します。
ここで新しいホスト名を入力します。

- 2 表示されるメニューからDefine mail-relay.を選択し、新しいホスト名を入力します。

- 3 表示されるメニューからQuit.を選択し、メールサーバの設定を終了します。

4. SSH接続許可IPアドレスの追加

- 1 SSH接続を許可するIPアドレスを設定するため、以下のコマンドを実行します。

fstool ssh

SSH access listが表示されますので[a]を入力し、UNIVERGE ThreatDefenderシリーズ運用時に管理用ポートeth0が接続されるネットワーク内の他のネットワーク機器に割り当てられていないIPアドレスを追加します。

- 2 SSH接続を許可するIPアドレスを設定します。

- 3 リストに追加されたことを確認したら[s]を入力して内容を更新します。

5. UNIVERGE ThreatDefenderシリーズのホスト名の変更

- 1 ホスト名を変更するため、以下のコマンドを実行します。

fstool netconfig -h *hostname*

*hostname*の部分に変更するホスト名を入力します。

- 2 変更の確認を行うため、以下のコマンドを実行します。

cat /etc/sysconfig/network

6. 管理用(root)パスワードの変更

- 1 管理用(root)パスワードを変更するため、以下のコマンドを実行します。

passwd

新しいパスワードを入力して(6ー15文字)、もう一度確認のために同じパスワードを入力します。
パスワードの変更完了メッセージが表示されたら完了です。

7. ネットワーク設定の変更

- 1 ネットワーク設定を変更するため、以下のコマンドを実行します。

fstool netconfig


- 2 表示されるメニューからConfigure default gatewayを選択し、デフォルトゲートウェイのipアドレスを入力します。

- 3 設定を反映するためApply Change now?に[yes]を入力します。

- 4 管理用ポート(eth0)のIPアドレスを変更するため、表示されるメニューからConfigure network interfacesを選択します。

- 5 画面にしたがって管理用ポート(eth0)のIPアドレスを変更します。

設定変更が完了するとネットワーク・サービスの再起動を行うかどうかの確認メッセージ“Restart network service?(yes/no)”が表示されます。ここでは[no]を入力します。

-  重要 もし[yes]を選択するとSSH接続を維持できなくなりますので、必ず[no]を選択してください。

- 6 [b]を入力してメニュー画面に戻り、Quitを選択してネットワーク設定を終了します。

8. UNIVERGE ThreatDefenderシリーズの再起動(終了)

- 1 システムに設定を反映させるため、以下のコマンドを実行しOSを再起動します。

shutdown -r now

8 CounterACT Consoleのインストール

CounterACT Consoleのインストールを行います。


1. 設定用PCのIPアドレス変更


前述の「4.SSH接続許可IPアドレスの設定」にて設定したIPアドレスを設定用PCに割り当てます。
ただし、使用していないIPアドレスに限りです。

2. CounterACT Consoleのインストール

- 1 バックアップ CD-ROMを設定用PCのドライブに挿入します。

オートラン機能により自動的に下図の画面が表示されますので、「Install CounterACT _ 6.2.3」をクリックします。

 ヒント Internet Explorerなどのブラウザから「http://xxx.xxx.xxx.xxx/install」へアクセスすることでインストールすることも可能です(xxx.xxx.xxx.xxxは管理用ポートeth0のIPアドレス)。

-  重要 自動的に表示されない場合は、<CD-ROMドライブ>\autorun.exeを実行してください。

- 2 Choose Install Folder画面が表示されますので、インストール先のフォルダを指定して「Next」をクリックします。

- 3 Choose Shortcut Folder画面が表示されますので、ショートカットフォルダの作成場所を選択して「Next」をクリックします。

- 4 Pre-Installation Summary画面が表示されますので、インストール情報を確認して「Install」をクリックします。


- 5 Install Complete画面が表示されますので、「Done」をクリックします。

9 CounterACT Setup Wizardの実行

CounterACTのSetup Wizardを実行します。

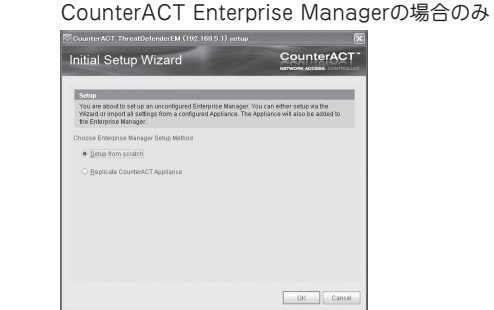
1. CounterACT Consoleアイコンをダブルクリックし、CounterACT Consoleを起動します。

CounterACT Console Login画面が表示されたら、初期パスワード(NEC123)でログインしてください。

 ヒント CounterACT Console初回起動時はInitial Setup Wizardが起動します。

2. UNIVERGE ThreatDefender Enterprise managerの場合、Choose Enterprise Manager Setup Method画面が表示されますので[Setup from scratch]にチェックを入れ「OK」をクリックします。

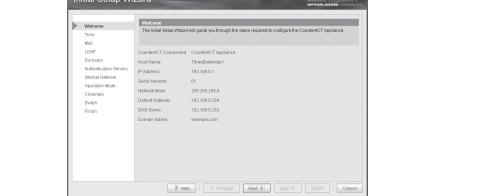
CounterACT Enterprise Managerの場合のみ



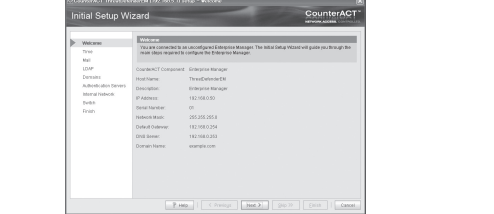
Choose Enterprise Manager Setup Method画面

3. Welcome画面が表示されますので「Next」をクリックします。

CounterACT Applianceの場合




CounterACT Enterprise Managerの場合



4. Time画面が表示されますので「Set time manually」をクリックします。

Set time & date画面が表示されますので現在の年/月/日/時刻を入力し「OK」をクリックします。


Time画面で「Next」をクリックすると時刻設定の更新が始まります。「Finished」と表示された後、「Next」をクリックします。

-  重要 インストール作業環境によっては「Finished」ではなく「Failed」と表示される場合もあります。

- 「Stop」ボタンで中断すると手動で設定した時刻が反映されない事がありますので、「Finished」または「Failed」が表示されたら「Next」をクリックします。

5. レポート通知先メールアドレス及びメールサーバのホスト名を設定します。

Mail画面が表示されますので“レポート通知先メールアドレス”、“メールサーバのホスト名”を入力し「Next」をクリックします。
Mail設定が更新され「Finished」と表示されたら「Next」をクリックします。

-  重要 インストール作業環境によっては「Finished」ではなく「Failed」と表示される場合もあります。

6. LDAP画面が表示されますので「Skip」をクリックします。

7. Domains画面が表示されますので「Skip」をクリックします。

8. Authentication Servers画面が表示されますので「Skip」をクリックします。

9. 監視対象ネットワーク範囲の設定をします。

Internal Network画面が表示されますので「Add」をクリックします。

IP Address Range画面が表示されますので監視対象ネットワーク範囲を入力し「OK」をクリックします。
Internal Network画面で「Next」をクリックします。
Internal Network設定が更新され「Finished」と表示された後「Next」をクリックします。

10. Operation Mode画面が表示されますので「Next」をクリックします。

Operation Mode設定が更新され「Finished」と表示されたら「Next」をクリックします。

11. Channels画面が表示されますので「Next」をクリックします。

Channels設定が更新され「Finished」と表示されたら「Next」をクリックします。

12. Switch画面が表示されますので「Skip」をクリックします。

13. Finish画面が表示されますので「Finish」をクリックします。

10 工場出荷時の不要設定の削除

1. 必要に応じてCounterACT Consoleから以下を変更します。

- ログインパスワードの変更

CounterACT Consoleにてログイン後、メニューバー → Tools → OptionsよりUsersの順に選択し、“admin”のパスワードを変更してください。

- CounterACT Console接続許可IPアドレスの変更
CounterACT Consoleにてログイン後、メニューバー → Tools → OptionsよりAccess → Consoleの順に選択し、[0.0.0.0] - [255.255.255.255]と設定されている範囲を適当な値に変更してください。

- ポータル接続許可IPアドレスの変更

CounterACT Consoleにてログイン後、メニューバー → Tools → OptionsよりAccess → Webの順に選択し、[192.168. 0 . 0] - [192.168. 1 . 255]と設定されている範囲を適当な値に変更してください。

設定方法の詳細はユーザーズガイド3章の「CounterACT Consoleによる設定変更作業1」を参照してください。

SSH接続による設定変更作業

1. SSH接続許可IPアドレスの削除

遠隔操作できないようにするため、不要なSSH接続許可IPアドレス登録を削除する必要があります(すべてのSSH接続許可IPアドレスを削除することはありません)。

- 1 SSH接続許可IPアドレスを削除するため、以下のコマンドを実行します。

fstool ssh

- 2 SSH access listが表示されるので[d]を入力し、デフォルト設定を削除します。

SSHaccesslist : 192.168.0.0 -192.168.1.255 ←デフォルト設定削除


- 3 不要なリストをすべて削除するまで[d]を入力し削除します。

不要なリストがすべて削除されたら[s]を入力して内容を更新します。


11 監視用ポートの接続ネットワークの変更

CounterACT Consoleにてログイン後、メニューバー → Tools → OptionsよりChannelsの順に選択し、監視用ポート設定の変更を行います。

DHCPを利用する場合と利用しない場合とで手順が異なりますので、ご注意ください。
設定方法の詳細はユーザーズガイドの3章「CounterACT Consoleによる設定変更作業2」を参照してください。

-  重要 Channel ConfigurationごとにDHCPの設定を行いますので、混在している場合はそれぞれ対応する手順で変更を行ってください。

- 1つのChannel ConfigurationにDHCPを利用するセグメントと利用しないセグメントを含む場合はDHCPを利用する手順で行います。
DHCPを利用しないセグメントは手動でIPアドレスを設定します。

-  ヒント 自動検出などの機能を使用する場合は、監視用ネットワークポートをネットワークに接続してください。

12 ライセンスの登録

CounterACT Consoleにてログイン後、メニューバー → Tools → OptionsよりAppliance →ライセンス登録する装置を選択 → Licenseの順に選択し、ライセンスの登録を行います。
設定方法の詳細はユーザーズガイドの3章の「ライセンスの登録」を参照してください。

13 ポリシーのセットアップ

CounterACT Consoleにてログイン後、メニューバー → Tools → OptionsよりPolicy → IPS Policy Managerの順に選択し、ポリシーの設定を行います。
設定方法の詳細はユーザーズガイドの4章の「IPSポリシーの設定」を参照してください。

14 バックアップを取得する

ここまで設定したシステムの基本設定のバックアップを取得します。
[Tools]-[Appliance Management]を選び、オプション画面にて、バックアップするHost nameを選択して、バックアップを実施します。詳しくは、ユーザーズガイドの4章の「バックアップ」を参照してください。

以上で完了です。