2 セットアップ

本体の設置からお使いなれる状態にするまでの手順について説明します。また、装置を再セットアップする場合もここに記載している説明を参照してください。

設置と接続

本体の設置と接続について説明します。

設　置

本装置は卓上またはEIA規格に適合したラックに設置して使用します。

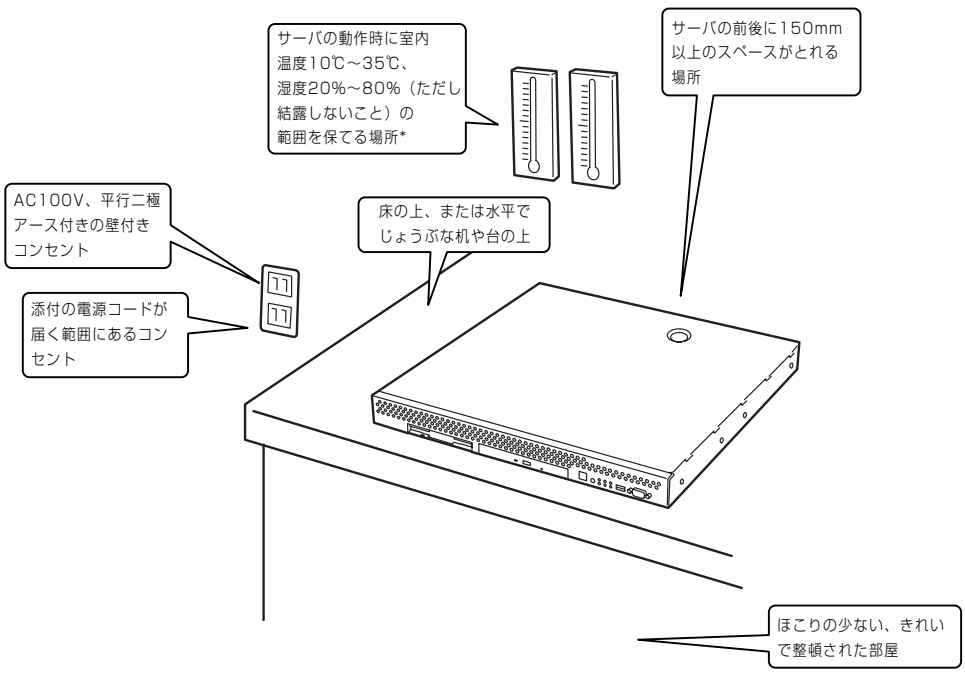
卓上への設置

⚠ 注意

装置を安全にお使いいただくために次の注意事項を必ずお守りください。指示を守らないと、火傷やけがなどを負うおそれや物的損害を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

- **指定以外の場所に設置しない**

本体の設置にふさわしい場所は次のとおりです。

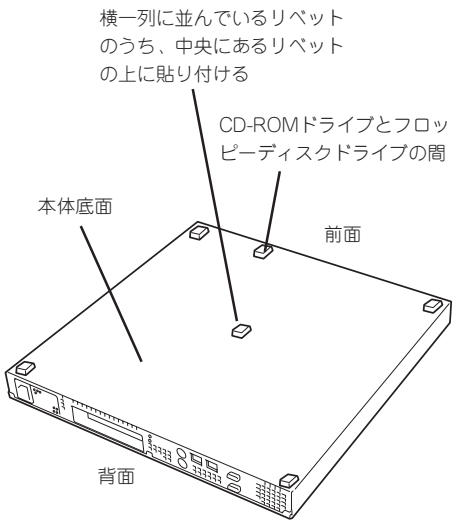


* 室内温度15℃～25℃の範囲を保てる場所での使用をお勧めします。

次に示す条件に当てはまるような場所には、設置しないでください。これらの場所に本装置を設置すると、誤動作の原因となります。

- 温度変化の激しい場所(暖房器、エアコン、冷蔵庫などの近く)。
- 強い振動の発生する場所。
- 腐食性ガスの発生する場所、薬品類の近くや薬品類がかかるおそれのある場所。
- 帯電防止加工が施されていないじゅうたんを敷いた場所。
- 物の落下が考えられる場所。
- 電源コードまたはインタフェースケーブルを足で踏んだり、引っ掛けたりするおそれのある場所。
- 強い磁界を発生させるもの(テレビ、ラジオ、放送／通信用アンテナ、送電線、電磁クレーンなど)の近く(やむを得ない場合は、保守サービス会社に連絡してシールド工事などを行ってください)。
- 本装置の電源コードを他の接地線(特に大電力を消費する装置など)と共用しているコンセントに接続しなければならない場所。
- 電源ノイズ(商用電源をリレーなどでON/OFFする場合の接点スパークなど)を発生する装置の近くには設置しないでください。(電源ノイズを発生する装置の近くに設置するときは電源配線の分離やノイズフィルタの取り付けなどを保守サービス会社に連絡して行ってください。)

卓上に置く場合は、本体底面に添付のゴム足を貼り付けてください。
設置場所が決まったら、本体の底面をしっかりと持って、設置場所にゆっくりと静かに置いてください。本装置は3台まで積み重ねて置くことができます。



ラックへの設置

ラックの設置については、ラックに添付の説明書を参照するか、保守サービス会社にお問い合わせください。
ラックの設置作業は保守サービス会社に依頼することもできます。

⚠警告

装置を安全にお使いいただくために次の注意事項を必ずお守りください。指示を守らないと、人が死亡する、または重傷を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

- **指定以外の場所で使用しない**
- **アース線をガス管につながない**

⚠注意

装置を安全にお使いいただくために次の注意事項を必ずお守りください。指示を守らないと、火傷やけがなどを負うおそれや物的損害を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

- **一人で搬送・設置をしない**
- **一人で部品の取り付けをしない**
- **荷重が集中してしまうような設置はしない**
- **ラックが不安定な状態でデバイスをラックから引き出さない**
- **複数台のデバイスをラックから引き出した状態にしない**
- **定格電源を超える配線をしない**

次に示す条件に当てはまるような場所には、ラックを設置しないでください。これらの場所にラックを設置したり、ラックに本装置を搭載したりすると、誤動作の原因となります。

- 装置をラックから完全に引き出せないような狭い場所。
- ラックや搭載する装置の総質量に耐えられない場所。
- スタビライザが設置できない場所や耐震工事を施さないと設置できない場所。
- 床におうとつや傾斜がある場所。
- 温度変化の激しい場所(暖房器、エアコン、冷蔵庫などの近く)。
- 強い振動の発生する場所。
- 腐食性ガスの発生する場所、薬品類の近くや薬品類がかかるおそれのある場所。
- 帯電防止加工が施されていないじゅうたんを敷いた場所。
- 物の落下が考えられる場所。

- 強い磁界を発生させるもの(テレビ、ラジオ、放送/通信用アンテナ、送電線、電磁クレーンなど)の近く(やむを得ない場合は、保守サービス会社に連絡してシールド工事などを行ってください)。
- 本装置の電源コードを他の接地線(特に大電力を消費する装置など)と共用しているコンセントに接続しなければならない場所。
- 電源ノイズ(商用電源をリレーなどでON/OFFする場合の接点スパークなど)を発生する装置の近く(電源ノイズを発生する装置の近くに設置するときは電源配線の分離やノイズフィルタの取り付けなどを保守サービス会社に連絡して行ってください)。

本体をラックに取り付ける手順を以下に示します。取り外し手順については、取り付け手順の後で説明しています。
ここでは、NEC製のラックまたは他社製ラックへの取り付け手順について説明します。
NEC製のラックのうち、N8540-28/29/38に取り付ける場合は、オプションの「N8143-35 ラック取り付け用ブラケット」が必要です。取り付け手順については、N8143-35 ラック取り付け用ブラケットに添付の説明書を参照するか、保守サービス会社にお問い合わせください。

⚠警告

装置を安全にお使いいただくために次の注意事項を必ずお守りください。指示を守らないと、人が死亡する、または重傷を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

- **規格外のラックで使用しない**
- **指定以外の場所で使用しない**

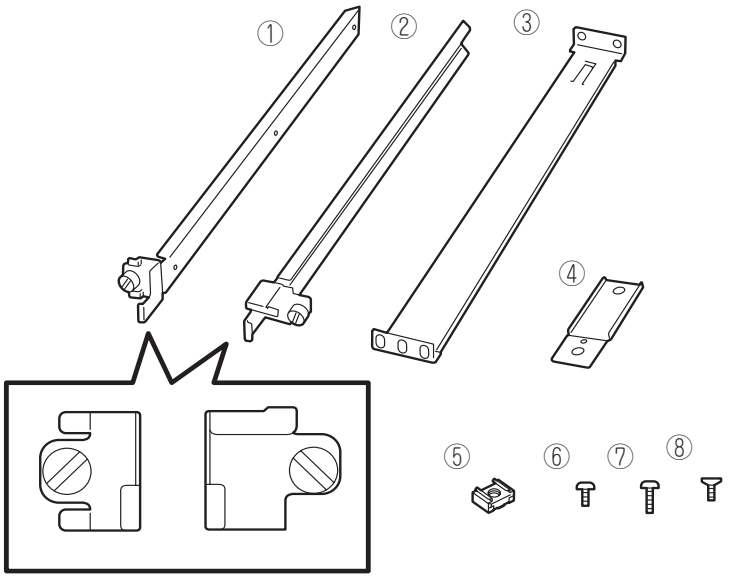
⚠注意

装置を安全にお使いいただくために次の注意事項を必ずお守りください。指示を守らないと、火傷やけがなどを負うおそれや物的損害を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

- **落下注意**
- **装置を引き出した状態にしない**
- **カバーを外したまま取り付けない**
- **指を挟まない**

取り付け部品の確認

ラックへ取り付けるために次の部品があることを確認してください。



項番	名称	数量	備考
①	マウントブラケット(L)	1	「L」と刻印されている。
②	マウントブラケット(R)	1	「R」と刻印されている。
③	サポートブラケット	2	
④	エクステンションブラケット	2	
⑤	コアナット	8	
⑥	ネジA	4	M3ネジ、ネジ部の長さ: 5mm、マウントブラケット(L)/(R)を装置に固定する際に使用する。
⑦	ネジB	6	M5ネジ、ネジ部の長さ: 10mm、サポートブラケットを固定する際に使用する。
⑧	ネジC	2	皿ネジ、エクステンションブラケットを固定する際に使用する。

必要な工具

ラックへ取り付けるために必要な工具はプラスドライバとマイナスドライバです。

取り付け手順

次の手順で本体をラックへ取り付けます。

重要

NEC製のラックのうち、N8540-28/29/38への取り付けにはN8143-35 ラック取り付け用ブラケットが必要となります。また、取り付け方法についてはN8143-35 ラック取り付け用ブラケットに添付の説明書をご覧ください。

● マウントブラケットの取り付け

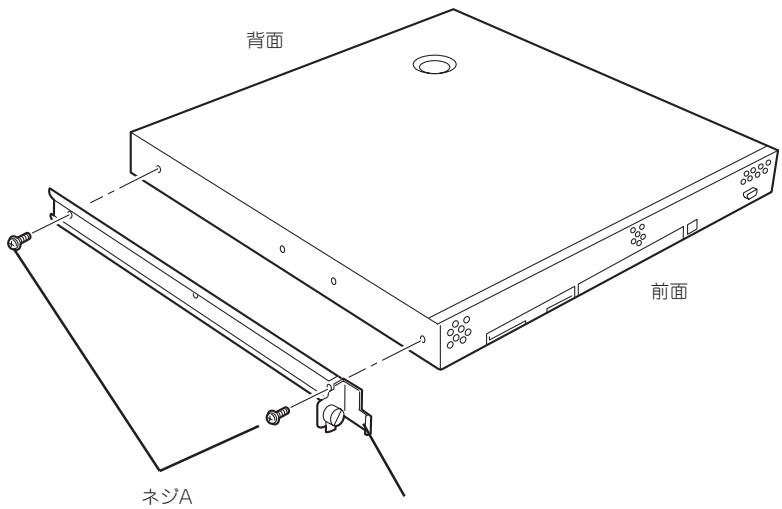
1. マウントブラケットのネジ穴と本体側面のネジ穴を合わせる。

   チェック

   ブラケットの向きを確認して取り付けてください。本体左側面にマウントブラケット(L)、右側面にマウントブラケット(R)を取り付けます。それぞれのブラケットに「L」、「R」と刻印があります。

2. マウントブラケットをネジA(2本)で本体に固定する。

3. もう一方の側面にマウントブラケットを手順1～2と同じ手順で取り付ける。

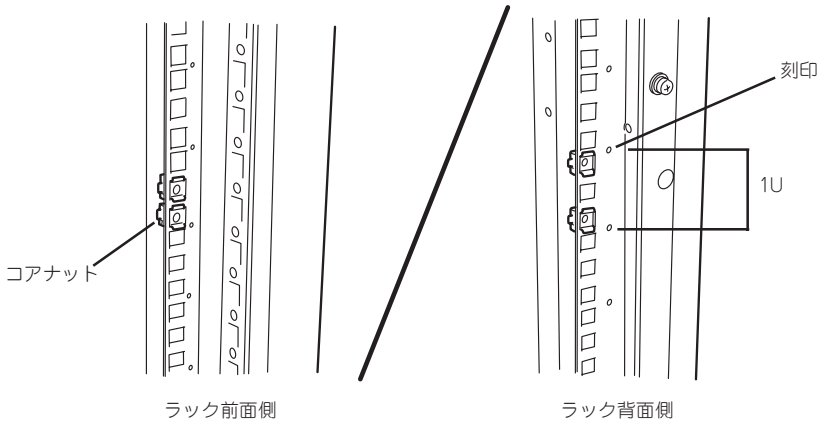


● **コアナットの取り付け**

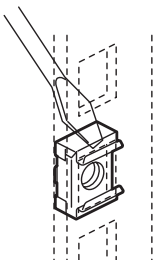
サポートブラケットを固定する位置に本装置に添付のコアナットを取り付けます。コアナットはラックの前面（左右とも）に各2個、背面（左右とも）に各2個の合計8個取り付けます。

コアナットは「1U（ラックでの高さを表す単位）」の中に2個取り付けてください（NEC製のラックでは、1U単位に丸い刻印があります）。1Uあたり、スロット（角穴）が3つあります。3つのスロットのうち、ラック前面側では下の2つのスロットに、ラック背面側では上下のスロットにコアナットを取り付けます。

コアナットはラックの内側から取り付けます。ラックの前面に取り付けたコアナットは、上側が本体のセットスクリューの受けとなります。下側はサポートブラケット前面の固定に使用します。背面のコアナットはサポートブラケット背面の固定用として使われます。



コアナットは下側のクリップをラックの四角穴に引っかけてからマイナスドライバなどで上側のクリップを穴に差し込みます。

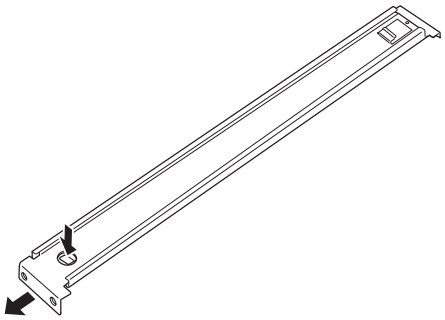


チェック

ラックの前後、左右に取り付けたコアナットの高さが同じであることを確認してください。

● サポートブラケットの取り付け

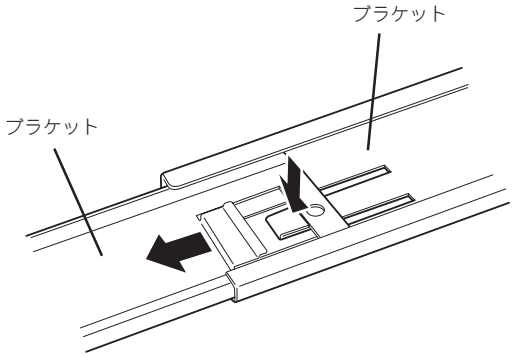
1. サポートブラケットのロックを解除して引き延ばす。



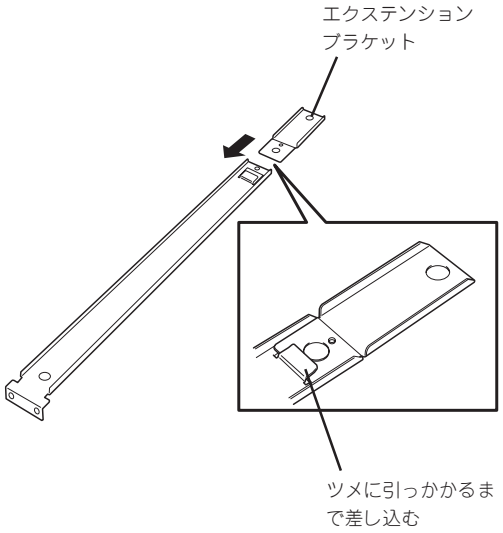
2. <ラックの前後の奥行きが700mm以上の場合のみ>

ラックの前後の奥行きが700mm以上の場合のみ以下の手順を行います。

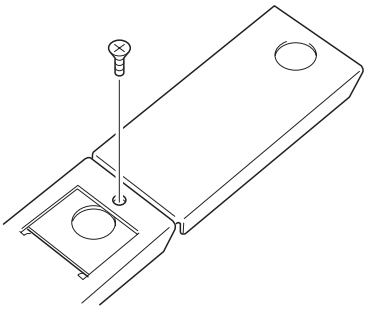
① サポートブラケットのロックを解除してブラケットを分解する。



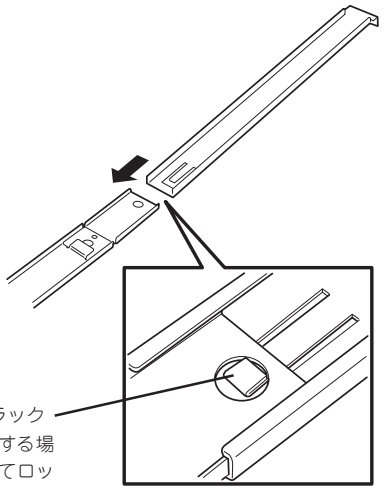
② エクステンションブラケットを一方のブラケットに差し込む。



③ エクステンションブラケットをネジC(1本)で固定する。

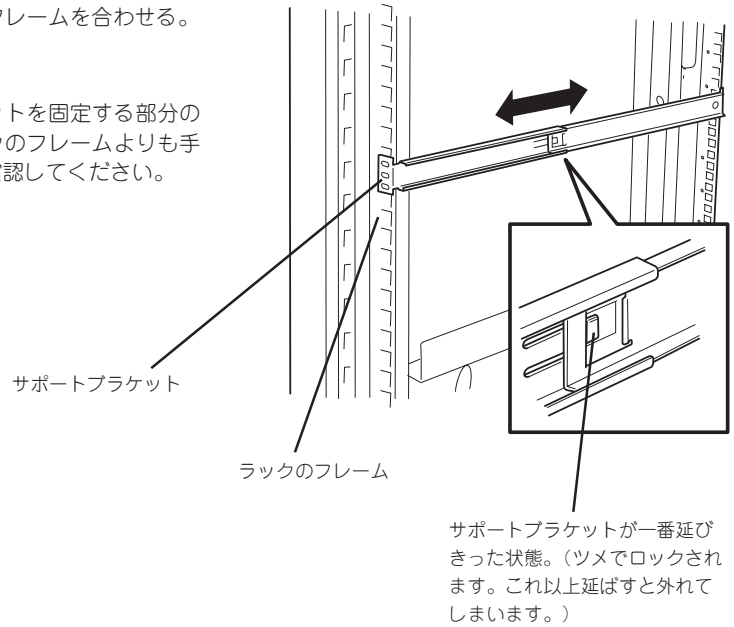


④ もう一方のブラケットをエクステンションブラケットに差し込む。



3. コアナットを取り付けた位置にサポートブラケット前後のフレームを合わせる。

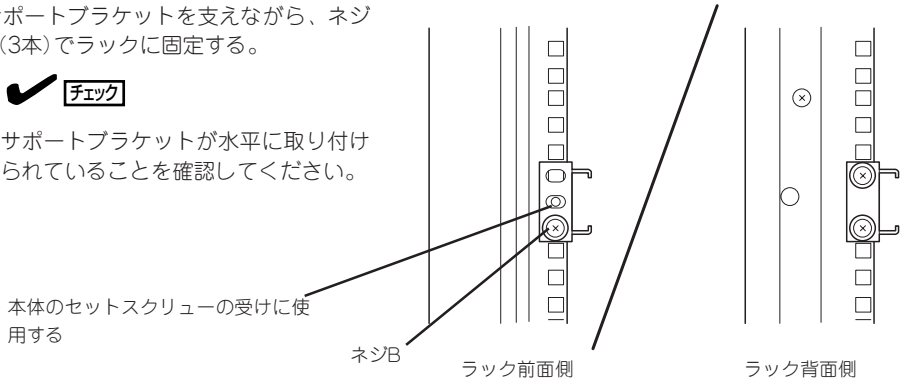
> ✔ チェック
>
> サポートブラケットを固定する部分のフレームがラックのフレームよりも手前にあることを確認してください。



4. サポートブラケットを支えながら、ネジB(3本)でラックに固定する。

チェック

サポートブラケットが水平に取り付けられていることを確認してください。



重要

サポートブラケットのネジ穴は多少上下にずらすことができる程度のクリアランスを持っています。初めて取り付ける場合は、コアナットのネジ穴がサポートブラケットのネジ穴の中央に位置するようにしてから固定してください。もし、装置を取り付けたときに装置の上下に搭載している装置にぶつかる場合は、いったん本装置を取り出してサポートブラケットの固定位置を調整してください(ぶつかる装置の取り付け位置も調整する必要がある場合もあります)。

5. もう一方のサポートブラケットを手順1～4と同じ手順で取り付ける。

チェック

すでに取り付けているサポートブラケットと同じ高さに取り付けていることを確認してください。

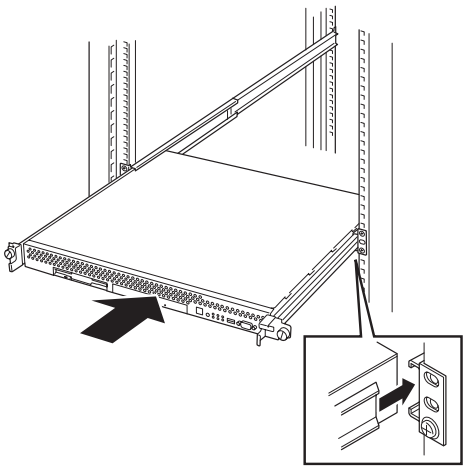
- **本体の取り付け**

取り付けは1人でもできますが、なるべく複数名で行うことをお勧めします。

1. 本体前面が手前になるようにして持つ。
2. 本体側面に取り付けたマウントブラケットをサポートブラケットに差し込みながらラックへ押し込む。

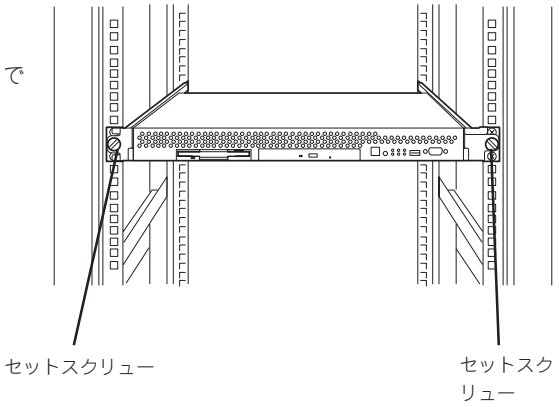
重要

装置の上下に搭載している装置にぶつかる場合は、いったん本装置を取り出してサポートブラケットの固定位置を調整してください。(ぶつかる装置の取り付け位置も調整する必要がある場合もあります)。



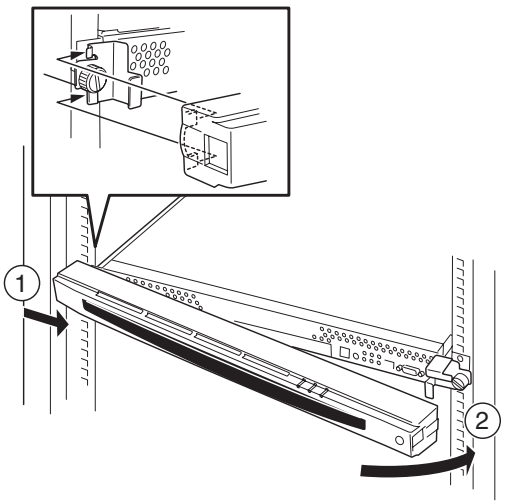
● **本体の固定**

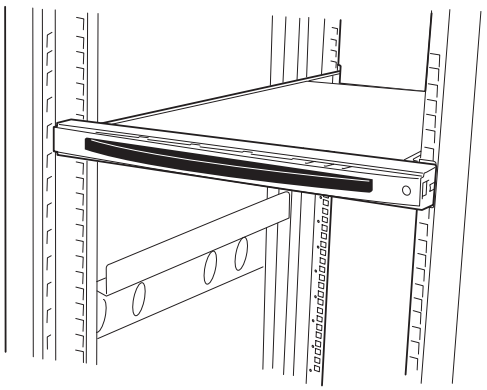
1. 本体をラックへ完全に押し込む。
2. 前面の左右にあるセットスクリューでラックに固定する。



3. フロントベゼルを取り付ける。

   以上で完了です。





取り外し手順

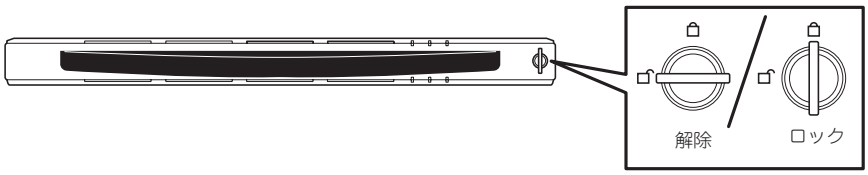
次の手順で本体をラックから取り外します。取り外しは1人でもできますが、なるべく複数名で行うことをお勧めします。

⚠ 注意

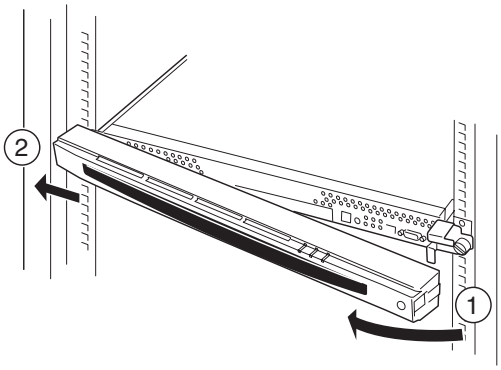
装置を安全にお使いいただくために次の注意事項を必ずお守りください。指示を守らないと、火傷やけがなどを負うおそれや物的損害を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

- **指を挟まない**
- **ラックが不安定な状態でデバイスをラックから引き出さない**
- **落下注意**
- **装置を引き出した状態にしない**
- **複数台のデバイスをラックから引き出した状態にしない**
- **動作中に装置をラックから引き出さない**

1. フロントベゼルのロックを解除する。

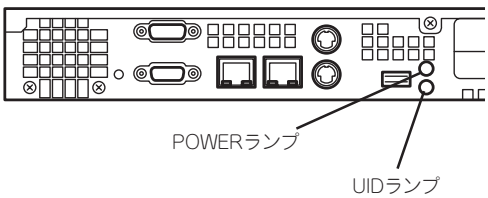


2. フロントベゼルを取り外す。
3. 本体の電源をOFF（POWERランプ消灯）にする。
4. 本体前面にあるUIDスイッチを押して、UIDランプを点灯させる。



5. 本体に接続しているすべてのケーブル、および電源コードを取り外し、UIDランプが消灯していることを確認する。

> **チェック**
>
> 本体背面のケーブルや電源コードを取り外す前にUIDランプで取り外そうとしている装置であることを確認してください。

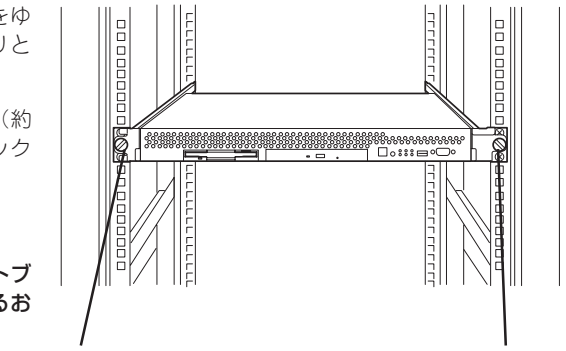


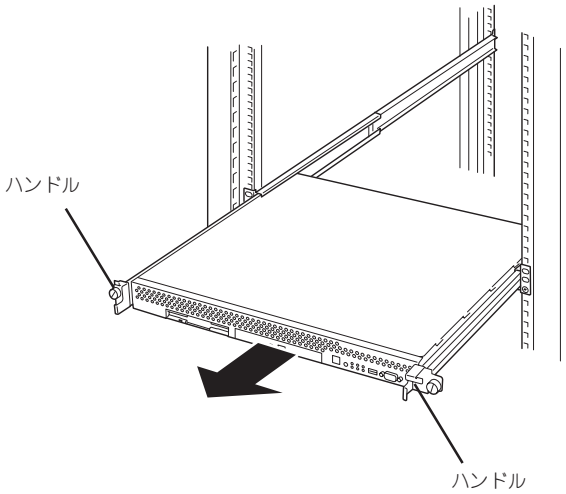
6. 前面の左右にあるセットスクリューをゆるめて、ハンドルを持ってゆっくりとラックから引き出す。

   本体の両端をしっかりと持てる位置（約15cmほど）までゆっくりと静かにラックから引き出してください。

重要

装置を引き出しすぎると、サポートブラケットから装置が外れて落下するおそれがあります。





7. 本体の左右底面をしっかりと持って取り外し、じょうぶで平らな机の上に置く。

重要

装置を引き出したまま放置しないでください。必ずラックから取り外してください。

ラックの機構部品も取り外す場合は、「取り付け手順」を参照して取り外してください。

接　続

本体をネットワークに接続します。
ネットワークケーブルを本体に接続してから添付の電源コードを本体に接続し、電源プラグをコンセントにつなげます。

⚠警告

装置を安全にお使いいただくために次の注意事項を必ずお守りください。指示を守らないと、人が死亡する、または重傷を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

- ぬれた手で電源プラグを持たない
- アース線をガス管につながない

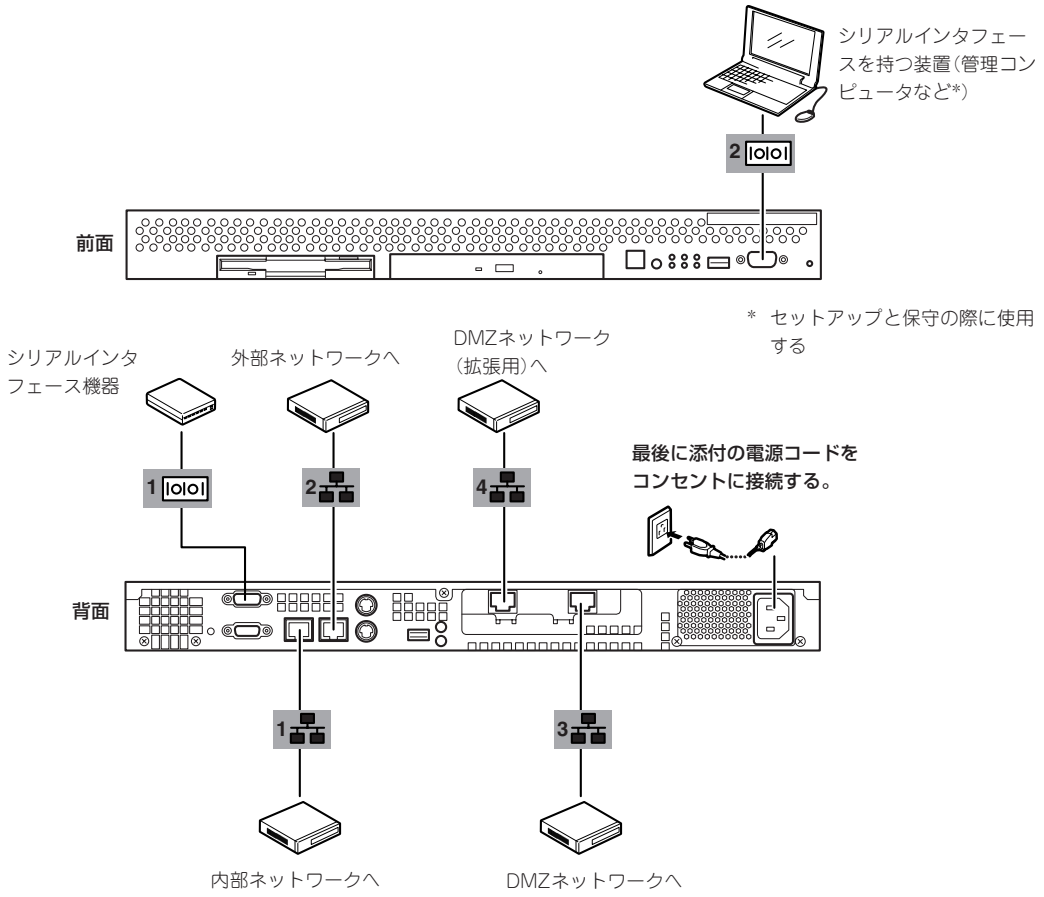
⚠注意

装置を安全にお使いいただくために次の注意事項を必ずお守りください。指示を守らないと、火傷やけがなどを負うおそれや物的損害を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

- 指定以外のコンセントに差し込まない
- たこ足配線にしない
- 中途半端に差し込まない
- 指定以外の電源コードを使わない
- プラグを差し込んだままインタフェースケーブルの取り付けや取り外しをしない
- 指定以外のインタフェースケーブルを使用しない

重要

- 本体および接続する周辺機器の電源をOFFにしてから接続してください。ONの状態のまま接続すると誤動作や故障の原因となります。
- NEC以外(サードパーティ)の周辺機器およびインタフェースケーブルを接続する場合は、お買い求めの販売店でそれらの装置が本装置で使用できることをあらかじめ確認してください。サードパーティの装置の中には本装置で使用できないものがあります。



チェック

ネットワークに接続する前に次の点について確認してください。

- ネットワーク機器

  必要なルータ、ハブ、ケーブルが準備されていることを確認してください。

- クライアントPC

  本装置とは別に、Windows XP、Windows 2000、Windows NT、または Windows 98のWindows OSが利用可能なクライアントマシン(PC)を用意してください。クライアントからのポリシーの設定・インストールに利用します。

以上で本体の電源をONにできる状態になりました。
購入後、初めて本体の電源をONにする場合は、この後の「初めてのセットアップ」をご覧ください。再セットアップの場合は、77ページの「再セットアップ」を参照してください。

初めてのセットアップ

購入後、初めて本製品をセットアップする時の手順について順を追って説明します。二重化構成を構築する場合は、まず4章の「二重化構成について」を参照してください。

セットアップの概要

本製品のセットアップには、本体以外のマシンや接続のためのケーブルなどが必要です。また、それぞれのマシンについてもソフトウェアのインストールなど準備が必要です。

- **本体**

  FireWall-1(Linux版)のモジュール、および基本設定ツールがrpm形式でハードディスク上の「/opt/necfws/RPMS」にインストール済みです。

  これらをこの後に示す手順に従って展開・コンフィグレーションしてください。

- **管理コンピュータ**

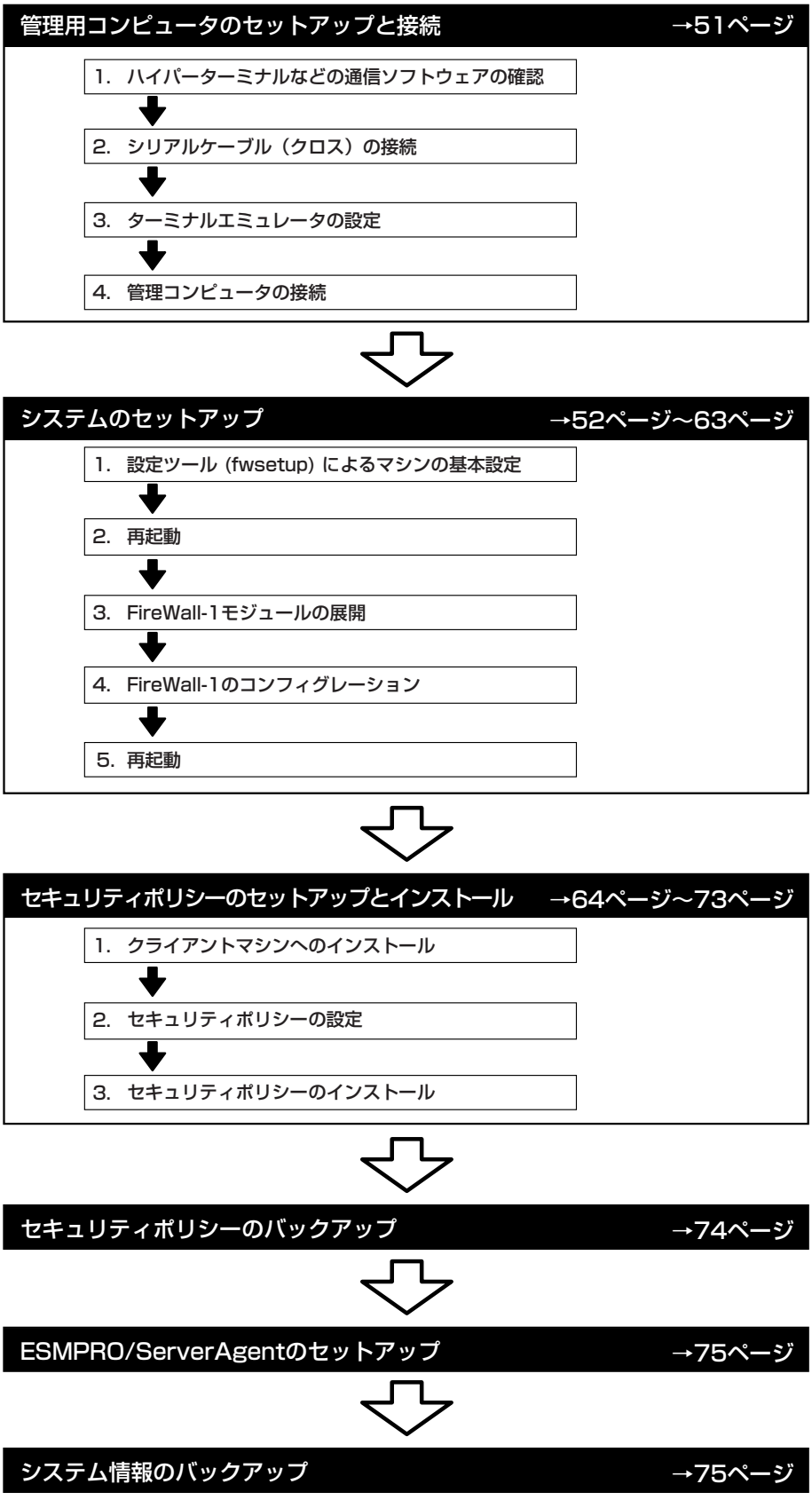
  システムの基本設定をするために使用する管理コンピュータに、あらかじめWindows 98ハイパーターミナルなどの通信ソフトが入っていることを確認してください。

  また、ターミナルエミュレータの設定を別途記述しています。確認してください。

- **クライアントPC**

  ポリシー編集用のクライアントPC(Windows 98/NT/2000/XPで動作するネットワーク上のコンピュータ)には、本装置に同梱されているCheck Point Next GenerationのCD-ROMからモジュールやGUIクライアントをインストールしてください。詳しくはこの後の説明を参照してください。

次ページにセットアップの流れを示します。


管理用コンピュータのセットアップと接続 →51ページ
1. ハイパーターミナルなどの通信ソフトウェアの確認
2. シリアルケーブル（クロス）の接続
3. ターミナルエミュレータの設定
4. 管理コンピュータの接続
システムのセットアップ →52ページ～63ページ
1. 設定ツール（fwsetup）によるマシンの基本設定
2. 再起動
3. FireWall-1モジュールの展開
4. FireWall-1のコンフィグレーション
5. 再起動
セキュリティポリシーのセットアップとインストール →64ページ～73ページ
1. クライアントマシンへのインストール
2. セキュリティポリシーの設定
3. セキュリティポリシーのインストール
セキュリティポリシーのバックアップ →74ページ
ESMPRO/ServerAgentのセットアップ →75ページ
システム情報のバックアップ →75ページ

管理コンピュータのセットアップと接続

本体の電源がOFFの状態で、管理コンピュータを本体前面にあるシリアルポート2(COM2)に接続し、システムを起動してください。

① 本体に接続するために必要なもの

- シリアルインタフェース(RS232C)を持ったコンピュータ
- 通信用ソフトウェア(例：Windows 98ハイパーターミナル)
- シリアルケーブル(クロス)

  K210-84(05)(9pin-9pin) または K208-12(03) (9pin-25pin)のうち、お手持ちのコンピュータに適合するケーブルをご利用ください。

② ケーブルの接続

本体前面にあるシリアルポート2(COM2)にシリアルケーブル(クロス)を接続してください。

③ ターミナルエミュレータの設定

ターミナルエミュレータのパラメータは以下のように設定してください。

ボーレート:　19,200bps
パリティ:　なし
キャラクタ長:　8bit
ストップビット:　1bit

④ 管理コンピュータの接続

本体の電源を投入後、しばらく(3分程度)してから管理コンピュータの<Enter>キーを押すと、管理コンピュータのディスプレイにloginプロンプトが表示されます。

管理コンピュータから「root」と入力し、「Password」に同梱の「rootパスワード」に書かれているパスワードを入力します。 ログインに成功すると「#」のプロンプトが表示されます。

重要　**rootのパスワードは、基本設定ツールで出荷時のパスワードから変更してください。詳しくはこの後の説明を参照してください。**

これで管理コンピュータの接続ができました。
以降の説明では、管理コンピュータからの操作でシステムをセットアップしていきます。

システムのセットアップ

Server自身のホスト名，IPアドレス，ルーティング情報など必要な基本設定は、設定ツール(/opt/necfws/bin/fwsetup)を使って簡単に設定することができます。
この設定ツールは管理コンピュータからfwsetupコマンドを入力して起動させます。
入力は対話形式になっていますので、設定が必要な項目について短時間で設定が可能です。

基本設定ツールでの設定項目

本設定ツールでの設定項目およびそれぞれの制限事項は以下のとおりです。

- **ホスト名(設定必須)**

  ホスト名はFQDN形式で入力してください。

- **インタフェースのIPアドレスとネットマスク(設定必須)**

  最低2つの設定が必要です。最大4つのインタフェースの設定が可能です。3つ目以降は任意です。途中のインタフェース(LANポート番号)を飛ばしての設定はできません。

- **ネームサーバのIPアドレス(設定任意)**

  最大3つのネームサーバを指定できます。本項目を省略した場合はネームサーバによるアドレス解決を行いません。

- **管理者のメールアドレス(設定必須)**

  1つのメールアドレスのみ設定できます。

- **メールゲートウェイのホスト名またはIPアドレス(設定任意)**

  システムがメールを送信する時にSMTP接続するメールサーバのIPアドレスを指定します。ホスト名で指定する場合はFQDN形式で入力してください。ただし、ネームサーバでその名前からIPアドレスが引ける必要があります。ネームサーバのIPアドレスを省略した場合、本項目は必ずIPアドレスを指定してください。本項目は省略可能ですが、その場合はFireWall-1や二重化機能などシステムが発信するメールはローカルのrootユーザー宛てに配送されます。本項目を省略した場合は定期的にメールをチェック、削除し、メールによってディスクを圧迫することがないように注意してください。また、FireWall-1や二重化機能では緊急時にメールで警告を通知することがあるため、本項目は必ず設定することをお勧めします。

- **デフォルトゲートウェイのIPアドレス(設定必須)**

  1つのIPアドレスのみ設定できます。

- **(静的)ルーティングテーブル(設定任意)**

  宛先アドレスとネットマスクおよびゲートウェイの組み合わせを指定します。本項目は省略することもできます。最大設定数は1000です。

  動的ルーティングはサポートしません。

- **ARPテーブル(設定任意ですがNAT使用時は必須)**

  NAT(アドレス変換)後の公開用IPアドレスを指定します。NAT機能を使用しない場合は、設定を省略することができます。最大設定数は1000です。

- **Trap送信先IPアドレス(設定任意)**

  Trap送信先(ESMPRO/ServerManager)のIPアドレスを指定します。ESMPRO/ServerManagerとの連携を行わない場合は設定を省略することができます。最大設定数は1000です。

- **NTP (時刻同期)サーバのIPアドレス(設定任意)**

  NTP(時刻同期)サーバのIPアドレスを指定します。本項目は設定を省略することができます。最大設定数は1000です。

- **FireWall-1で取得されるログの保管日数(設定必須)**

  1～90日の範囲で設定ができます。

- **二重化機能の設定(設定任意)**

  二重化構成を使用する場合に設定します。詳しくは「二重化構成について」を参照してください。

- **rootユーザーのパスワード変更(設定任意)**

  省略できますが、セキュリティ上、変更することをお勧めします。

- **現在の時刻設定(設定任意)**

  省略できます。

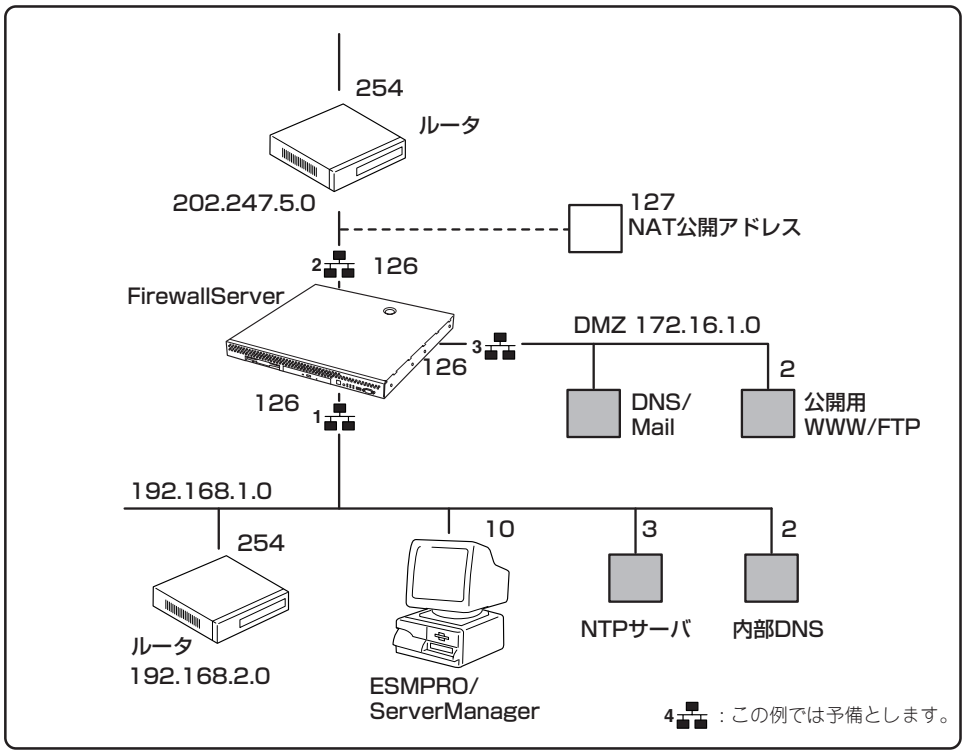
- **サービスの起動と停止(設定必須)**

  起動時に 必要なサービスを起動、および不要なサービスを停止させるための設定ができます。必ず1度は実行してください。

重要 **上記の設定後は、本体を再起動させてください。**

設定ツールによる基本設定

以下のネットワーク構成を例にして基本設定ツールの使い方を説明します。設定はrootユーザーで行います。



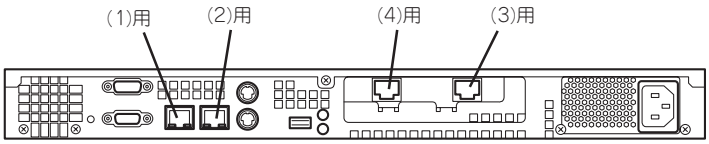
```
# /opt/necfws/bin/fwsetup ····· ①

Firewall Server configuration tool Ver.1.4

hostname: fws.nec.co.jp ····· ②

interface address(1): 192.168.1.126
netmask(1): 255.255.255.0
interface address(2): 202.247.5.126
netmask(2): 255.255.255.0
interface address(3): 172.16.1.126
netmask(3): 255.255.255.0
interface address(4):                    ····· ③
No.  IF address       netmask
  1  202.247.5.126    255.255.255.0
  2  192.168.1.126    255.255.255.0
  3  172.16.1.126     255.255.255.0       ····· ④
("a"=add | "m num"=modify | "d num"=delete | "l"=list | Enter=next):

nameserver(1): 192.168.1.2 ····· ⑤
nameserver(2):
No.  nameserver address
  1  192.168.1.2
("a"=add | "m num"=modify | "d num"=delete | "l"=list | Enter=next):

administrator e-mail address: xyz@nec.co.jp ····· ⑥

use mail gateway? (y/n)[n]: y ····· ⑦
mail gateway: 192.168.1.2
```

① 設定ツールを起動する。

② ホスト名を設定する。

ホスト名はFDQNで入力してください。

③ LANポート別にIPアドレスとネットマスクを設定する。



ここに示すネットワーク構成例では4ポート目(4)は「予備」なので何も入力せずに<Enter>キーを押してスキップしています。

④ 設定した内容をリストで表示。

複数項目を設定した場合は、設定後に一覧表を表示します。一覧から設定内容の追加、および修正、削除、一覧表の再表示をキー入力から操作できます。

<A>キー + <Enter>キー: ポートの設定を追加する。
<M>キー +「変更するポート番号」+ <Enter>キー: 指定したポートの設定を変更する。
<D>キー +「削除するポート番号」+ <Enter>キー: 指定したポートの設定を削除する。
<L>キー + <Enter>キー: リストを再表示する。
<Enter>キー: 次の項目へスキップする。

⑤ ネームサーバのIPアドレスを設定する。

⑥ 管理者のメールアドレスを設定する。

⑦ メールゲートウェイのIPアドレスを設定する。

<Y>キーを押して値を入力します。省略する場合は<N>キーを押してください。

```
default gateway IP address: 202.247.5.254 ..... ①

static routing ..... ②
destination(1): 192.168.2.0
netmask(1): 255.255.255.0 ..... ③
gateway(1): 192.168.1.254
destination(2): 202.247.5.127
netmask(2): 255.255.255.255 ..... ④
gateway(2): 172.16.1.2
destination(3):
No.  destination      netmask          gateway
  1  192.168.2.0      255.255.255.0    192.168.1.254
  2  202.247.5.127    255.255.255.255  172.16.1.2
("a"=add | "m num"=modify | "d num"=delete | "l"=list | Enter=next):

proxyarp(1): 202.247.5.127 ..... ⑤
proxyarp(2):
No.  proxyarp IP address
  1  202.247.5.127
("a"=add | "m num"=modify | "d num"=delete | "l"=list | Enter=next):

trap sink host(1): 192.168.1.10 ..... ⑥
trap sink host(2):
No.  trap sink host
  1  192.168.1.10
("a"=add | "m num"=modify | "d num"=delete | "l"=list | Enter=next):

NTP server address(1): 192.168.1.3 ..... ⑦
NTP server address(2):
No.  NTP server address
  1  192.168.1.3
("a"=add | "m num"=modify | "d num"=delete | "l"=list | Enter=next):
```

① デフォルトゲートウェイのIPアドレスを設定する。

② ルーティングテーブルを設定する(任意)。

後述の「アドレス変換のためのルーティングテーブル、ARPテーブルの設定」も参照してください。

③ 宛先のIPアドレス、ネットマスク、およびそのネットワークへのゲートウェイアドレスを設定する。

④ destinationにNAT後のIPアドレス(公開アドレス)を、gatewayにNAT前のIPアドレス(実アドレス)を設定する。

NATのためのルーティングの設定ではnetmaskには 255.255.255.255 を指定します。

NATの対象ホストが別ネットワークに存在する場合、gatewayにはそのネットワークへのゲートウェイアドレスを設定します。

⑤ ARPテーブルを設定する(NAT使用時は必須)。

NAT後のIPアドレス(公開アドレス)を設定してください。

⑥ trap送信先IPアドレスを設定する(任意)。

ESMPRO/ServerManagerがインストールされているマシンのIPアドレスを設定してください。

⑦ NTP(時刻同期)サーバのIPアドレスを設定する(任意)。

```
log file rotation(days): 90 ····· ①

Use cluster system? (y/n)[n]: ····· ②

once again input? (y/n)[n]:····· ③

change root password? (y/n)[n]: y ····· ④
Changing password for user root
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully

Mon May 21 16:48:44 JST 2001
set date and time? (y/n)[n]: y ····· ⑤
date and time (MMDDhhmm[[CC]YY]): 05191653
Mon May 21 16:53:01 JST 2001
set date and time? (y/n)[n]:

replace startup-scripts? (y/n)[n]: y ····· ⑥

Please reboot the system.

#shutdown -r now ····· ⑦
```

① FireWall-1で取得されるログの保存日数を設定する。

② ここでは二重化機能の設定は行いません。二重化構成を構築する場合でも、ここでは必ず、<N>キーを押してください。

③ ここまでの設定項目について設定を変更したいときは、<Y>キーを押す。次に進む場合は、<N>キーを押す。

④ 出荷時に設定されているパスワードを変更する（任意）。

重要

- **セキュリティのためにも、出荷時のパスワードから変更することをお勧めします。**
- **パスワードは推測されにくく覚えやすいものを用意してください。**

⑤ 時刻の設定を変更する（任意）。

⑥ 必要なサービスの起動および不要なサービスの停止を行う（必須）。

ここでは必ず<Y>キーを押してください。

⑦ 設定を有効にするため、システムを再起動する。

FireWall-1モジュールの展開

管理コンピュータから次の手順でFireWall-1のモジュールを展開します。

```
# cd /opt/necfws/RPMS ..... ①
# rpm -i CPshrd-50-00.i386.rpm ..... ②
# rpm -i CPfw1-50-00.i386.rpm ..... ③

**********************************************************************

       Important - DON'T FORGET TO:
Log in again and run cpconfig in order to register the
license and configure Check Point VPN-1/FireWall-1 NGFeature Pack 1.
               :
               :

# shutdown -r now ..... ④
```

① ディレクトリを変更する。

② SVN Foundation(CPshared)パッケージを展開する。必ずFireWall-1のパッケージよりも前に展開してください。

③ FireWall-1パッケージを展開する。

④ 終了後、再起動する。

FireWall-1のコンフィグレーション

次に管理コンピュータからFireWall-1付属のcpconfigコマンドを実行します。
以下の手順でコンフィグレーションを行ってください。

```
# cpconfig

Welcome to Check Point Configuration Program
================================================
Please read the follwing license agreement.
Hit 'ENTER' to continue...  ..... ①
                :
                :
                :
Do you accept all the terms of this license agreement? (y/n) [y] ? y ..... ②

which Module would  you like to install?
----------------------------------------
(1) VPN-1 & FireWall-1 Enterprise Primary Management and Enforcement Module
(2) VPN-1 & FireWall-1 Enforcement Module
(3) VPN-1 & FireWall-1 Enterprise Primary Management
(4) VPN-1 & FireWall-1 Enterprise Secondary Management
(1) VPN-1 & FireWall-1 Enterprise Log Server

Enter your selection (1-5/a) [1]: 1 ..... ③
IP forwarding disabled
Hardening OS security: IP forwarding will be disabled during boot.
Generating default filter
Default Filter installed
Hardening OS Security: default filter will be applied during boot.
This program will guide you through several steps where you
will define your VPN-1 & FireWall-1 configuration.
At any later time, you can reconfigure these parameters by
running cpconfig
```

① <Enter>キーを押す。

使用許諾書が表示されますのでお読みください。

② 使用許諾に承認した場合は<Y>キーを押す。

③ インストールするモジュールを選択する。

通常は1を選択し、一体型構成でインストールします。

FireWall-1管理モジュールを別マシンにインストールして管理する、分散型構成でインストールする場合は2を選択してください。二重化のために分散型構成でインストールする場合、以降の設定内容については「二重化構成について」を参照してください。

```
Configuring Licenses...
============================
Host           Expiration Features

Do you want to add licenses (y/n) [n] ? y

Do you want to add licenses [M]anually or [F]etch from file: m
IP Address:202.247.5.126
Expiration Date:
Signature Key:
SKU/Features:

License was added successfully

 License will be put into kernel after cpstart


Configuring Administrators...
============================
No VPN-1 & FireWall-1 Administrators are currently
defined for this Management Station.
Administrator name: fws-admin
Password:
Verify Password:
Permissions for all Management Clients (Read/[W]rite All, [R]ead Only
All, [C]ustomized) W

Administrator fws-admin was added successfully and has
Read/Write permissions to all management clients

Add another one (y/n) [n] ? n

Configuring GUI clients...
=========================
GUI clients are trusted hosts from which
Administrators are allowed to log on to this Management Station
using Windows/X-Motif GUI.

Do you want to [C]reate a new list, [A]dd or [D]elete one?: c
Please enter the list hosts that will be GUI clients.
Enter hostname or IP address, one per line, terminating with CTRL-D
or your EOF character.
192.168.1.99
Is this correct (y/n) [y] ? y
```

① <Y>キーを入力して、ライセンスを追加する。

② <M>キーを入力して、ライセンスをを画面から(マニュアルで)登録する。

③ 事前に取得したライセンス情報を入力する。

ライセンスは、FirewallServerのライセンス製品に添付されている「ライセンス申請書」をNS-SolへFAXして取得してください。本製品(N8100-845)には「ライセンス申請書」は含まれていません(「FirewallServerの製品体系」を参照してください)。

④ FirewallServer(FireWall-1)の管理者名、およびパスワード、属性を設定する。

⑤ 管理者を追加する場合は、<Y>キーを、登録を終了する場合は<N>キーを押す。

⑥ <C>キーを入力して、クライアントマシンのリストを新規作成する。

⑦ セキュリティポリシーの設定を行うクライアントマシンのIPアドレスを設定する。

複数のIPアドレスを設定する場合は改行して複数行入力します。入力を終了する場合は<Ctrl>-<D>キーを押します。

⑧ 入力したアドレスが正しければ<Y>キーを押す。

```
Configuring Groups...
=====================
VPN-1 & FireWall-1 access and execution permissions
-------------------------------------------
Usually, a VPN-1 & FireWall-1 module is given group permission
for access and execution.
You may now name such a group or instruct the installation
procedure to give no group permissions to the VPN-1 & FireWall-1 module.
In the latter case, only the Super-User will
be able to access and execute the VPN-1 & FireWall-1 module.

Please specify group name [<RET> for no group permissions]:  ..... ①

No group permissions will be granted. Is this ok (y/n) [y] ? y  ..... ②

Setting Group Permissions... Done.


Configuring Random Pool...
==========================
You are now asked to perform a short random keystroke session.
The random data collected in this session will be used in
various cryptographic operations.

Please enter random text containing at least six different
characters. You will see the '*' symbol after keystrokes that
are too fast or too similar to preceding keystrokes. These
keystrokes will be ignored.

Please keep typing until you hear the beep and the bar is full.

    [.....................] ..... ③

Thank you.


Configuring Certificate Authority...
====================================
The system uses an internal Certificate Authority
to provide Secured Internal Communication (SIC) Certificateies
for the components in your System.

Note that your components won't be able to communicate
with each other until the certificate Authority is initialized
and they have their SIC Certificate.

Press 'Enter' to initialize the certificate Authority... ..... ④
 Internal Certificate Authority created successfully
 Certificate was created successfully
Certificate Authority initialization ended successfully
```

① FirewallServerでは通常グループを作成しないので<Enter>キーを押して続ける。

② <Y>キーを押して続ける。

③ バーがフルになるまでランダムキーを入力する。

④ インターナルCA(Certificate Authority)の設定を行う。

<Enter>キーを押してください。

```
Configuring Certificate's Fingerprint...
=========================
The following text is the fingerprint of this Management machine:
XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX ..... ①


Do you want to save it to a file? (y/n) [n] ?  n
generating GUI-clients INSPECT code
initial_management:
compiled OK.

Hardening OS Security: Initial policy will be applied
until the first policy is installed

In order to complete the installation of module
you must reboot the machine.
Do you want to reboot? (y/n) [n] ?  y ..... ②
```

① GUIクライアントを接続したとき、接続したFireWall-1が正しいものであるかを確認するための文字列が表示される。

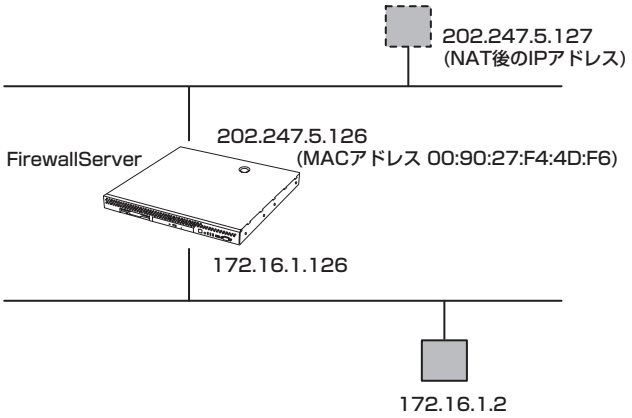
この文字列をディスク上に保存する場合は、<Y>キーを、保存しない場合は、<N>キーを入力します。

② 終了後、再起動する。

以上でFirewallServerの基本設定が終了しました。この後、GUIクライアントからポリシーの設定を行います。

NATのためのルーティングテーブル・ARPテーブルの設定[参考]

DMZ上やローカルネット内のサーバのアドレスを静的にNAT(アドレス変換)し、インターネット上に公開する場合、ルーティングテーブルとARPテーブルの設定を別途おこなう必要があります。
構成例の場合、DNS/Mailサーバと、公開用WWW/FTPサーバが該当するホストになります。
以下のように設定します。



ルーティングテーブル

前述の図のように、172.16.1.2のアドレスを 202.247.5.127に変換し、バリアセグメント上のホストに見立てる場合、以下のようなルーティングテーブルを追加する必要があります。

destination　202.247.5.127
(netmask　255.255.255.255)
gateway　172.16.1.2

変換後のアドレスをdestination、実際のアドレスをgatewayに指定してください。
fwsetupのstatic routingの項目で設定することができます。

NATの対象ホストが別ネットワークに存在する場合、gatewayにはそのネットワークへのゲートウェイアドレスを設定します。

ARPテーブルの設定

インターネット上のホストとアドレス変換されたホストとが通信をする場合、さらに変換後アドレスに対するMACアドレスがFirewallServerの外側インタフェースに付けられているMACアドレスであるという対応づけが必要です。
fwsetupのproxyarpに変換後のアドレスを指定することで自動的に設定することができます。

重要　**Linux版FireWall-1 Next Generationでは、Ver.4.1と同様にルーティングとARPテーブルの設定を行う必要があります。**

セキュリティポリシーのセットアップとインストール

セキュリティ機能をセットアップする「Policy Editor」をクライアントマシンにインストールし、編集したポリシーをインストールします。
次の条件を満たすコンピュータにPolicy Editorやその他のツールをインストールして、クライアントマシンとして使用します。

- オペレーティングシステム: Windows XP Home/professional、
  Windows 98/Me、
  Windows NT 4.0 Workstation(SP6a)、
  Windows NT 4.0 Server(SP6a)、
  Windows 2000 Professional(SP1、SP2)、
  Windows 2000 Server(SP1、SP2)、
  Windows 2000 Advanced Server(SP1、SP2)
- ディスク空き容量: 40MB以上
- メモリ: 128MB以上

* 上記は2002年3月現在の情報です。今後のパッチリリースにより変更になる可能性があります。

クライアントマシンへのインストール

クライアントマシンにPolicy Editorをインストールします。ここでは、Policy Editorといっしょにログを解析するためのツール「Log Viewer」とシステムの状態をチェックする「System Status」もインストールします。

1. コンピュータのCD-ROMドライブにCheck Point Next Generation CD-ROMをセットする。

   自動的にインストールプログラムが起動し、画面が表示されます。
   インストールプログラムが起動しない場合は¥wrappers¥windowsフォルダにある「demo32.exe」を実行してください。

2. [Next]をクリックする。

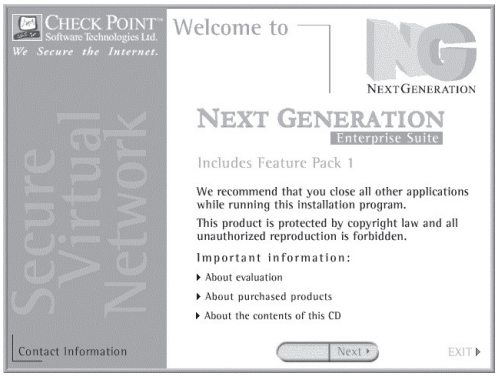
   使用許諾契約書が表示されます。

3. 内容をよく読み、同意する場合は[Yes]をクリックする。

   同意しない場合は[No]をクリックして終了します。
   プロダクトメニューの画面が表示されます。

4. [SERVER/GATEWAY COMPONENTS]を選択し、[Next]をクリックする。

   プロダクト選択の画面が表示されます。



5. [Management Clients]のみをチェックして [Next]をクリックする。

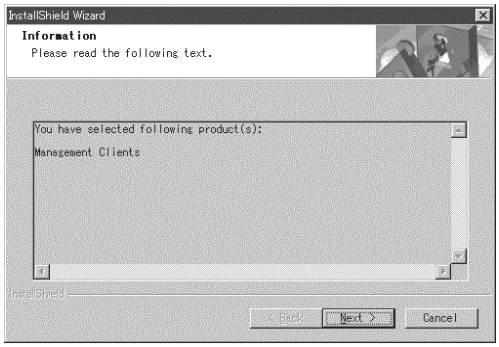
> **チェック**
>
> その他のコンポーネントのチェックは外します。

6. 右図の内容が表示されていることを確認し、[Next]をクリックする。

   インストール先のフォルダを指定する画面が表示されます。

7. 必要に応じてフォルダを変更し、[Next]をクリックする。

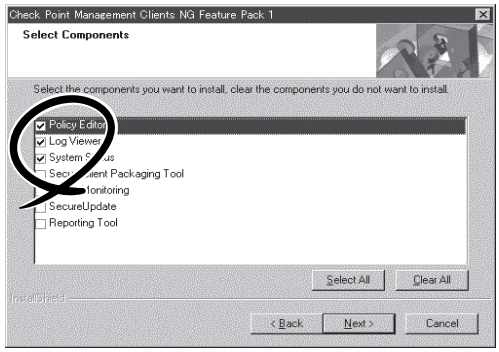
   インストールするコンポーネントを選択する画面が表示されます。



8. [Policy Editor]と[Log Viewer]、[System Status]をチェックし、[Next]をクリックする。

   インストールが開始されます。

9. インストール完了メッセージが表示されたら[OK]をクリックして終了する。



セキュリティポリシーの設定

Policy Editorを使用し、FirewallServerと接続してポリシーを作成します。ネットワーク構成に応じたポリシールールを作成してください。
Policy Editorの使い方についてはFireWall-1に付属のマニュアルを参照してください。
以下にポリシールールの例を説明しますが、ここで説明するルールは一例であり全ての環境に適用できるものではありません。また、ここで説明するルールは動作を保証するものではありません。予めご了承ください。

Policy Editorでのログイン

Policy Editorを起動し、cpconfigで登録したユーザー名とパスワード、およびFirewallServerの内側(管理クライアント側)のアドレスを入力します。

ネットワークオブジェクトの作成

ポリシールール作成に必要なネットワークオブジェクトを作成します。
54ページのネットワーク構成例では以下のネットワークオブジェクトを作成します。

- **ネットワーク**

localnet1	ネットワークアドレス:	192.168.1.0
	ネットマスク:	255.255.255.0
	NAT	
	Translation method:	Hide
	Hiding IP Address:	202.247.5.126
localnet2	ネットワークアドレス:	192.168.2.0
	ネットマスク:	255.255.255.0
	NAT	
	Translation method:	Hide
	Hiding IP Address:	202.247.5.126

DMZnet	ネットワークアドレス:	172.16.1.0
	ネットマスク:	255.255.255.0

内部ネットワークからNAT変換を行って外部にアクセスする場合は、「NAT」タブで「Add Automatic Address Translation rules:」にチェックをし、「Translation method:」をHide、「Hiding IP Address」にファイアウォールの外側のインタフェースのアドレスを入力します。

その他に内部ネットワークがあればさらにオブジェクトを作成します。

- **ワークステーション**

WebFtpServer	IPアドレス:	172.16.1.2
	NAT	
	Translation method:	Static
	Network valid address:	202.247.5.127
DnsMailServer	IPアドレス:	172.16.1.3
	NAT	
	Translation method:	Static
	Network valid address:	202.247.5.128
LocalDnsServer	IPアドレス:	192.168.1.2
ESMPROMgr	IPアドレス:	192.168.1.10

ホストを外部に公開する場合は、「NAT」タブで「Add Automatic Address Translation rules」にチェックをし、「Translation method:」をStatic、「Network valid address:」に公開用の外部アドレスを入力します。

その他にポリシールール作成に必要なワークステーションが存在する場合はさらにオブジェクトを作成します。

- **グループ**

LocalNet-G	In Group:	localnet1、localnet2

内部のネットワークを1つのグループにまとめて登録します。

その他にポリシールール作成に必要なグループがある場合はさらにオブジェクトを作成します。

- **サービスグループ**

InternetServices	In Group:	ftp、http、https
SilentServices	In Group:	NBT(nbdatagram、nbname、nbsession)、bootp

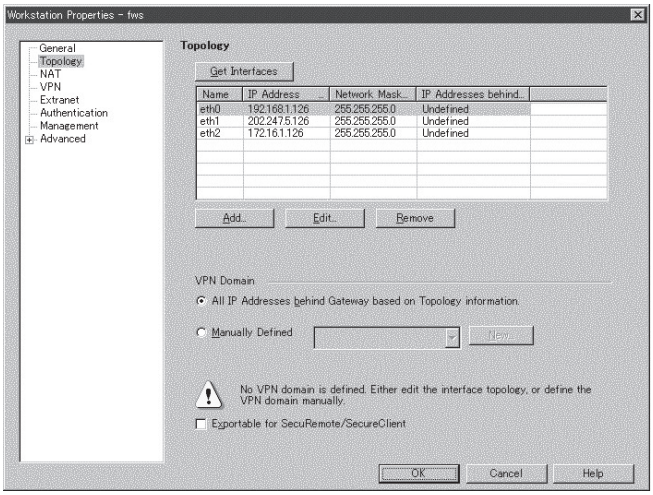
ポリシールール作成で1行のルールに複数のサービスを記述する場合などは、サービスのグループを定義することでルールを簡潔に記述することができます。

上記は、内部からインターネットにアクセスを許可するサービスのグループと、内部ネットワークにブロードキャストで流れているサービスでログに記録する必要のないサービスのグループを作成します。

ファイアウォールオブジェクトの設定

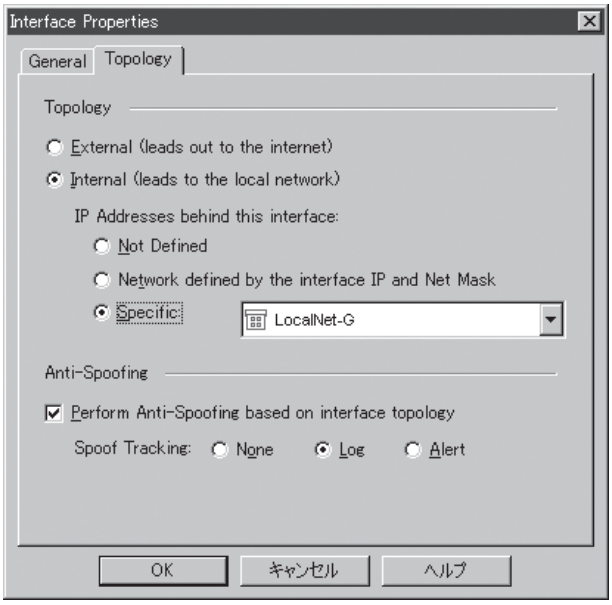
ファイアウォールのオブジェクトは、最初にPolicy Editorで接続したときに自動生成されます。自動作成されたファイアウォールオブジェクトはそのままではIP Spoofing(アドレス詐称)の対応がされていないため、Anti-Spoofingの設定を行います。そのためには、各インタフェースの先にどのネットワークが存在するかを登録(Topologyを設定)する必要があります。

ファイアウォールオブジェクトのプロパティの「Topology」ページを開き、各インタフェースを選択して[Edit...]をクリックします。

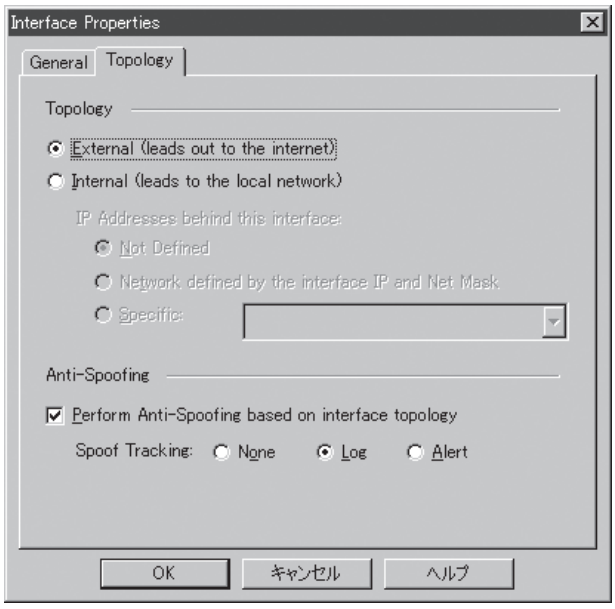


「Interface Properties」ウィンドウが表示されるので、「Topology」タブで適切な設定を行います。

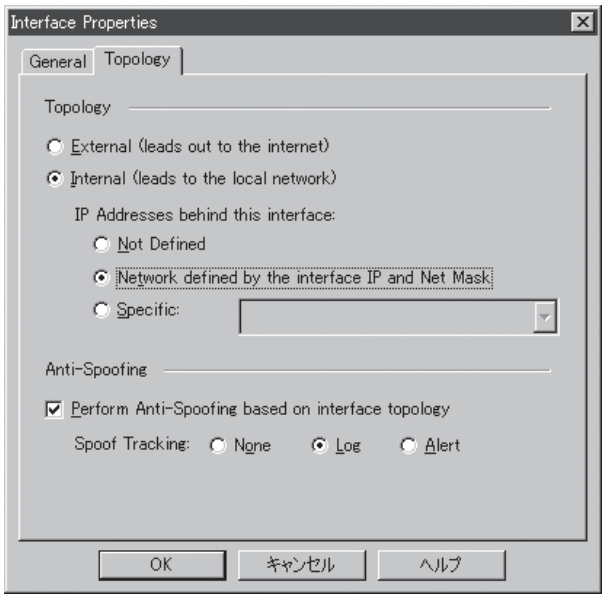
内側のインタフェースの場合は「Internal」を選択し、内部が単一ネットワークの場合は「Network defined by the interface IP and Net Mask」を、複数ネットワークの場合は「Specific」を選択します。「Specific」を選択した場合は、内部ネットワークのグループ(上記で作成したLocalNet-G)を指定します。
また、「Perform Anti-Spoofing based on interface topology」にチェックをします。



外側のインタフェースの場合は「External」を選択します。
また、「Perform Anti-Spoofing based on interface topology」にチェックをします。



DMZのインタフェースの場合は「Internal」および「Network defined by the interface IP and Net Mask」を選択します。
また、「Perform Anti-Spoofing based on interface topology」にチェックをします。
もしDMZが複数のネットワークで構成されている場合は、前述の内側のインタフェースの設定と同様にDMZネットワークのグループを用意し、「Specific」を選択してDMZのネットワークグループを指定します。



ポリシールールの作成

オブジェクトの作成が終わったらポリシールールを作成します。
以下はポリシールールの例です。

NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME
1	ESMPROMgr	fws	snmp	accept	Log	Policy Targets	Any
2	Any	fws	Any	drop	Alert	Policy Targets	Any
3	LocalNet-G	DnsMailServer	pop-3 smtp	accept	Log	Policy Targets	Any
4	Any	DnsMailServer	dns smtp	accept	Log	Policy Targets	Any
5	DnsMailServer	LocalNet-G	dns smtp	accept	Log	Policy Targets	Any
6	LocalDnsServer	Any	dns	accept	Log	Policy Targets	Any
7	Any	WebFtpServer	http ftp	accept	Log	Policy Targets	Any
8	DMZnet	LocalNet-G	Any	reject	Alert	Policy Targets	Any
9	LocalNet-G	DMZnet	Any	reject	Alert	Policy Targets	Any
10	LocalNet-G	Any	InternetServices	accept	Log	Policy Targets	Any
11	Any	Any	SilentServices	drop	None	Policy Targets	Any
12	Any	Any	Any	drop	Alert	Policy Targets	Any

各ルールの意味は以下のとおりです。

1. ESMPRO/ServerManagerがインストールされているマシンから、SNMPでFirewallServerの監視ができるように許可する。
2. その他のFirewallServer自身へのアクセスは全て拒否する。
3. 内部ネットワークのクライアントからDMZ上のメールサーバに対してメールの送受信ができるように許可する。
4. インターネット上のホストからDNS要求を受けられるように、また、メールを受信できるように許可する。
5. 4とは逆に、DNS要求を出せるように、また、メールの配信ができるように許可する。このとき、DnsMailServerから内部ネットワークへはアクセスができないよう、LocalNet-G以外へのアクセスを許可します。
6. 内部DNSサーバからインターネット上のDNSサーバに対してDNS要求が出せるように許可する。
7. インターネットおよび内部のネットワークからWeb/FTPサーバに対してHTTP、FTPのアクセスができるように許可する。
8. DMZから内部ネットワークへはアクセスを拒否する。
9. (上記で設定したルール以外で)内部ネットワークからDMZへはアクセスを拒否する。
10. 内部ネットワークからインターネットに対してInternetServicesに登録されたサービスのアクセスを許可する。
11. SilentServicesに登録されたサービスはアクセスを拒否し、ログは表示しない。
12. 上記以外のアクセスは全て拒否する。

セキュリティポリシーのインストール

ポリシー作成後、「Policy」→「Install...」を実行してセキュリティポリシーをインストールしてください。

公開サーバを二重化する場合の設定

内部ネットワークまたはDMZネットワークに設置されている公開サーバを二重化する場合、FireWall-1のポリシー設定に注意が必要となります。

ここでは前述のポリシー設定において、ＤＭＺネットワーク上のメールサーバ(DnsMailServer)がCLUSTERPRO Lite! for Linuxにより二重化されているMailWebServerと仮定して、ポリシーの追加設定の内容を説明します。

- **注意点**

  － インターネットから公開サーバに通信させる場合の注意

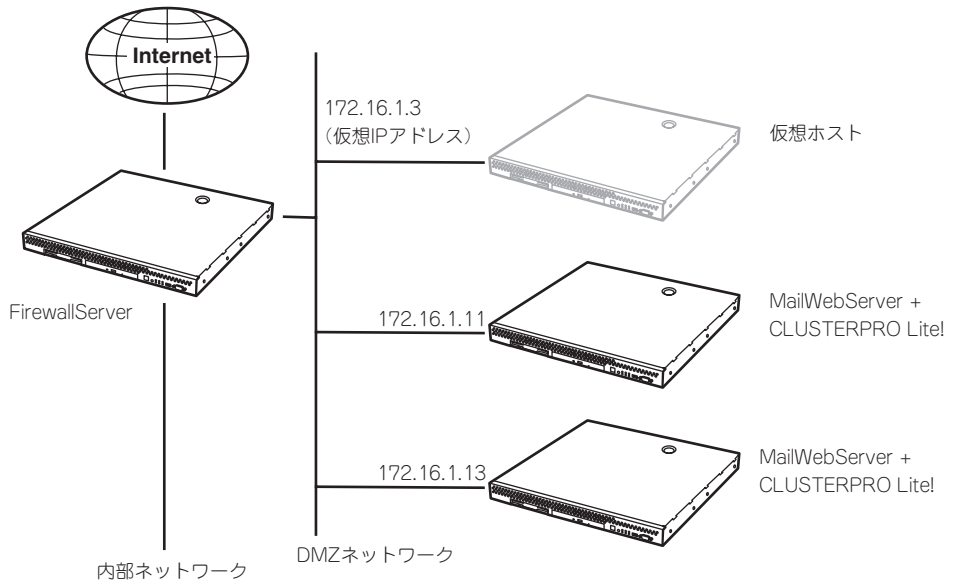
  CLUSTERPRO Lite!では2台の公開サーバの実IPアドレスとは別に仮想IPアドレスを設定します。FireWall-1で静的NATの設定を行う際、NATの実IPアドレスとしてはCLUSTERPRO Lite!で設定した仮想IPアドレスを指定する必要があります。(公開サーバのオブジェクトは、CLUSTERPRO Lite!で指定した仮想IPアドレスで作成します。)

  － 公開サーバから内部ネットワークあるいはインターネット上のホストに通信させる場合の注意

  CLUSTERPRO Lite!で二重化されたサーバから他のホストに対して通信を行う場合、接続元のIPアドレスは各サーバの実IPアドレスになります。そのため、FireWall-1のポリシーでは各サーバの実IPアドレスからの通信を許可するためのルールが必要になります。(各サーバの実IPアドレスのオブジェクトを作成し、このオブジェクトからのアクセスを許可します。)

重要 **サーバの二重化については製品によってその方法が異なります。ご使用の二重化製品の説明書をよく読み、通信の動作を理解した上でFireWall-1のポリシー設定を行ってください。**

- **構成例**



● **設定内容**

上記構成例でMailWebServerを二重化する場合の設定は以下になります。

前述の「セキュリティポリシーの設定」のポリシー設定例では以下の1は設定済みなので、2と3の設定を行います。

1. 公開用のメールサーバのオブジェクト(DnsMailServer)を仮想IPアドレス(172.16.1.3)で定義し、NATの設定を行う。
2. MailWebServerのオブジェクトをそれぞれ各サーバの実IPアドレスで定義する。

   DnsMailServer-master　172.16.1.11
   DnsMailServer-slave　172.16.1.12

3. 接続元がメールサーバとなる通信を制御する場合は、SourceをDnsMailServer-master、DnsMailServer-slaveとしてポリシールールを設定する。

   前述までのポリシーに対して変更を加える場合は、ルールNo.5のSourceを以下のように変更します。

セキュリティポリシーのバックアップ

万一の故障による再インストールに備えて、設定したセキュリティポリシーのバックアップを作成します。

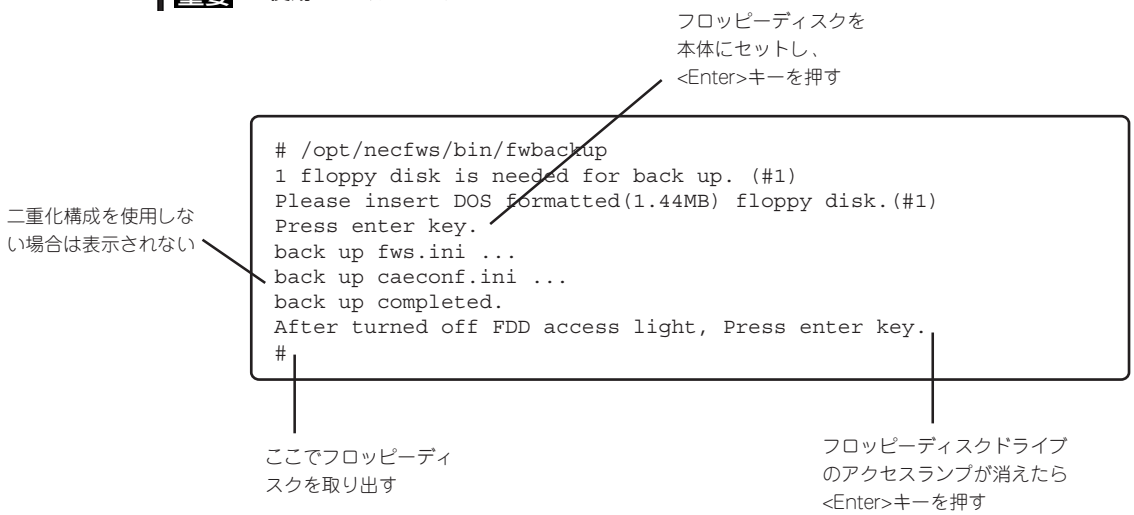
fwsetupコマンドにより設定したシステムの基本設定やクライアントマシンで編集したポリシーをバックアップするためには以下のファイルをバックアップする必要があります。

- /opt/necfws/etc/fws.ini
- /usr/clusterpro/ae/etc/caeconf.ini(二重化構成使用時)
- /etc/fw/conf/ 配下
- /etc/fw/database/ 配下
- /etc/fw/lib/ 配下（*.soを除く）

これらのファイルを自動的にDOSフォーマットしたフロッピーにバックアップするため、/opt/necfws/bin/にfwbackupコマンドを用意しています。

このコマンドをコンソールから実行するとフロッピーディスクのセットを促すメッセージが表示されます。
メッセージに従いフロッピーディスクをセットして<Enter>キーを押すと、後は自動的にフロッピーディスクへバックアップします。
バックアップコマンド実行時、バックアップに必要なフロッピーの枚数が表示されるので、必要数のフロッピーディスクをあらかじめ用意してください。
通常はフロッピーディスク1枚でバックアップ可能ですが、ポリシーのルール数やユーザー登録数が極端に多い場合などは1枚に保存できないことがあります。ファイルがフロッピーディスク1枚に保存できない場合には、複数枚のフロッピーディスクに分割してバックアップコピーを行います。メッセージに従ってフロッピーディスクを入れ換えてください。

重要 **バックアップディスクには、必ずDOSフォーマット(1.44MB)済みのブランクディスクを使用してください。**



リストアに関しては、「システムの再インストール」を参照してください。

ESMPRO/ServerAgentのセットアップ

ESMPRO/ServerAgentは出荷時にインストール済みですが、固有の設定がされていません。6章を参照してセットアップしてください。

システム情報のバックアップ

システムのセットアップが終了した後、添付の「保守・管理ツールCD-ROM」にあるオフライン保守ユーティリティを使って、システム情報をバックアップすることをお勧めします。システム情報のバックアップがないと、修理後にお客様の装置固有の情報や設定を復旧（リストア）できなくなります。次の手順に従ってバックアップをしてください。

重要

保守・管理ツールCD-ROMからシステムを起動して操作します。保守・管理ツールCD-ROMから起動させるためには、事前にセットアップが必要です。5章を参照して準備してください。

1. 3.5インチフロッピーディスクを用意する。
2. 装置に添付の「保守・管理ツールCD-ROM」から「オフライン保守ユーティリティ」を起動する。

   「保守・管理ツールCD-ROM」の使い方については5章を参照してください。
3. ［システム情報の管理］から［退避］を選択する。

   以降は画面に表示されるメッセージに従って処理を進めてください。

続いて管理コンピュータに本装置を監視・管理するアプリケーションをインストールします。次ページを参照してください。

管理コンピュータのセットアップ

本装置をネットワーク上のコンピュータから管理・監視するためのアプリケーションとして、「ESMPRO/ServerManager」と「Management Workstation Application（MWA）」が用意されています。
これらのアプリケーションを管理コンピュータにインストールすることによりシステムの管理が容易になるだけでなく、システム全体の信頼性を向上することができます。

ESMPRO/ServerManagerのインストールについては6章を参照してセットアップしてください。

MWAのインストールについては5章、または保守・管理ツールCD-ROM内のオンラインドキュメントを参照してください。

再セットアップ

再セットアップとは、システムの破損などが原因でシステムが起動できなくなった場合などに、添付の「バックアップCD-ROM」を使ってハードディスクを出荷時の状態に戻してシステムを起動できるようにするものです。以下の手順で再セットアップをしてください。

保守用パーティションの作成

「保守用パーティション」とは、装置の維持・管理を行うためのユーティリティを格納するためのパーティションで、16MB程度の領域を内蔵ハードディスク上へ確保します。
FirewallServerの信頼性を向上するためにも保守用パーティションを作成することをお勧めします。
保守用パーティションは、添付の「保守・管理ツールCD-ROM」を使って作成します。詳しくは5章を参照してください。

保守用パーティションを作成するプロセスで保守用パーティションへ自動的にインストールされるユーティリティは、「システム診断ユーティリティ」と「オフライン保守ユーティリティ」です。

再セットアップモードへの変更

本装置は、システムの起動が正常に行われたかどうか常に監視をし、起動に失敗した場合はシステムの再起動を試みる機能が備わっています。再インストール中は、システム起動監視機能を無効にする必要があります。
本機能の有効／無効は、添付の「保守・管理ツールCD-ROM」を使って変更します。詳しくは、6章を参照してください。

重要 **再セットアップが完了したら、システム起動監視機能を有効に戻してください。**

システムの再インストール

ここでは、システムの再インストールの手順について説明します。
二重化構成を構築している場合は、再インストールの手順が異なります。再インストールの手順10までを行った後は「二重化構成について」の二重化構成の再セットアップを参照してください。

重要 **再インストールを行うと、サーバ内の全データが消去され、出荷時の状態に戻ります。必要なデータがサーバ内に残っている場合、データをバックアップしてから再インストールを実行してください。**

再インストールの準備(コンソール接続)

作業を行うためにはコンソールが必要です。本体の電源がOFFの状態で、お手持ちのパソコン(管理コンピュータ)を本体前面のシリアルポート2(COM2)に接続してください。

FirewallServerとの接続に必要なもの

- シリアルインタフェース(RS232C)を持ったコンピュータ
- 通信用ソフトウェア(例:Windows98 ハイパーターミナル)
- シリアルケーブル(クロス)

  K210-84(05)(9pin-9pin)、またはK208-12(03)(9pin-25pin)のうち、お手持ちのコンピュータに合ったケーブルを使用してください。

ケーブルの接続

本体前面にあるコネクタにシリアルケーブル(クロス)を接続してください。

ターミナルエミュレータの設定

ターミナルエミュレータのパラメータは以下のように設定してください。

ボーレート: 19,200bps
パリティ: なし
キャラクタ長: 8bit
ストップビット: 1bit

再インストールに必要なディスク

あらかじめ以下のディスクを用意してください。

- OS CD-ROM
- バックアップ CD-ROM
- Check Point Next Generation
- 再インストール用ディスク
- セキュリティポリシーのバックアップディスク(任意)

再インストールの手順

次の手順に従って再インストールします。

1. 本体前面にあるフロッピーディスクドライブに再インストール用ディスクをセットしFirewallServerを再起動する。

   管理コンピュータのディスプレイに[boot:]の表示が出るまで待ってください。

2. [boot:]の表示がでたらすぐにCD-ROMドライブにOS CD-ROMをセットする。

   自動的にプログラムCD-ROMからのインストールが始まります。インストールは約10分で完了します。
   インストールを完了すると、ディスプレイにインストールの完了を通知するメッセージが表示されます。

3. <Ctrl> - <D>キーを押す。

   自動的に再起動が開始されます。再起動を開始したら、セットしたフロッピーディスクとCD-ROMを本体から取り出してください。

```
>> install finish. press Ctrl+D
bash#
```

ここで<Ctrl> - <D>キーを押す

4. 再起動開始から約3分程度経過したら、管理コンピュータの<Enter>キーを押す。

5. loginプロンプトが表示されたら、「root」と入力し、Passwordに添付品の「rootパスワード」に書かれているパスワードを入力する。

   ログインに成功すると[#]のプロンプトが表示されます。

6. CD-ROMドライブにバックアップCD-ROMをセットし、以下の手順でESMPRO/ServerAgentなどの追加パッケージを展開する。

```
# mount /dev/cdrom
# /mnt/cdrom/nec/Linux/necsetup
# cd /
# umount /dev/cdrom
```

7. CD-ROMドライブからバックアップCD-ROMを取り出す。

8. <あらかじめバックアップしておいた設定をリストアする場合>

   以下のコマンドを実行して基本設定をする。
   設定をバックアップしたフロッピーディスクを本体にセットしてください。

```
# /opt/necfws/bin/fwrestore -i
Please insert backup floppy disk. (#1)
Press enter key.
restore fws.ini ...
restore caeconf.ini ...
restore completed.
After turned off FDD access light, Press enter key.
# /opt/necfws/bin/fwsetup -i /opt/necfws/etc/fws.ini

# shutdown -r now
```

バックアップディスクをセットして<Enter>キーを押す

二重化構成を使用していない場合は表示されない

終了後、再起動する

フロッピーディスクドライブのアクセスランプが消えたら<Enter>キーを押し、その後フロッピーディスクを取り出す

<バックアップのリストアをしない場合>

「設定ツールによる基本設定(54ページ)」を参照して基本設定をする。

9. CD-ROMドライブにCheck Point Next GenerationのCD-ROMをセットし、FireWall-1のモジュールを以下の手順で展開する。

```
# mount /dev/cdrom
# cd /mnt/cdrom/linux/CPshared-50
# rpm -i CPshared-50-00.i386.rpm
# cd /mnt/cdrom/linux/CPFirewall-50
# rpm -i CPfw1-50-00.i386.rpm
# cd /
# umount /dev/cdrom
```

10. CD-ROMドライブからCD-ROMを取り出し、再起動する。

```
# shoutdown -r now
```

二重化構成を構築している場合、この後の作業は「二重化構成について」の二重化構成の再セットアップ（4章）に従ってください。

11. cpconfigを実行してFireWall-1の設定をする。

cpconfigについては「FireWall-1のコンフィグレーション」（59ページ）を参照してください。cpconfigの最後で再起動を実行します。

```
# cpconfig
     :
     :
Do you want to reboot? (y/n) [n] ?y
```

12. <あらかじめバックアップしておいた設定をリストアする場合>

以下のコマンドを実行してFireWall-1の設定をする。

```
# cpstop ―――――――――――――――――――― FireWall-1を停止する
# /opt/necfws/bin/fwrestore -f

Please insert backup floppy disk. (#1)
Press enter key.
There is 1 floppy disk for restore.
restore fw config files ... (1/1)
restore completed.
After turned off FDD access light, Press enter key.

# cpstart
```

FireWall-1を起動する

フロッピーディスクドライブのアクセスランプが消えたら<Enter>キーを押し、その後フロッピーディスクを取り出す

<バックアップのリストアをしない場合>

Policy Editorを使用してポリシーを作成する。

13. Policy Editorでポリシーをインストールする。

ESMPRO/ServerAgentのセットアップ

「システムの再インストール」でESMPRO/ServerAgentは自動的にインストールされますが、固有の設定がされていません。6章を参照してセットアップしてください。

システム情報のバックアップ

システムの再セットアップが終了した後、添付の「保守・管理ツールCD-ROM」にあるオフライン保守ユーティリティを使って、システム情報をバックアップすることをお勧めします。前述の「システム情報のバックアップ」、および5章を参照してください。

～Memo～