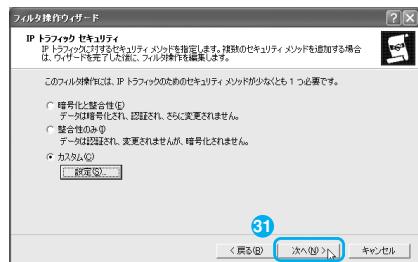
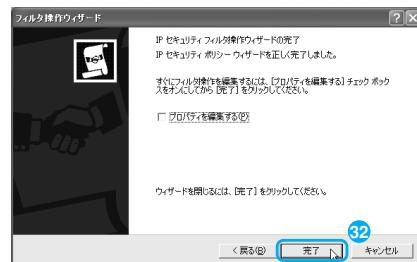


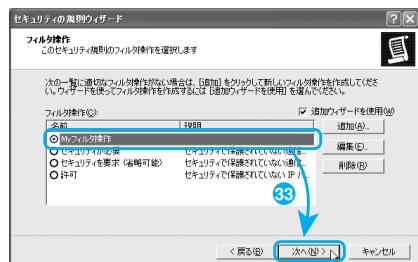
## 31 次へボタンをクリックします。



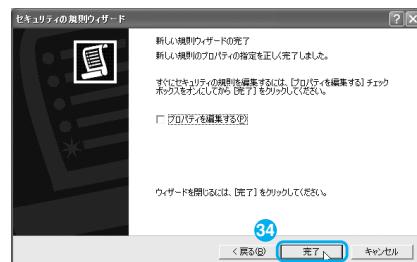
## 32 完了ボタンをクリックします。



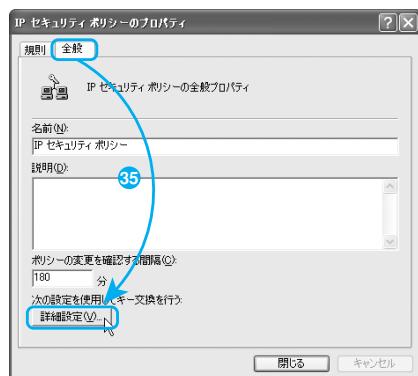
## 33 作成した3フィルタ操作をオンにして、次へボタンをクリックします。



## 34 完了ボタンをクリックします。



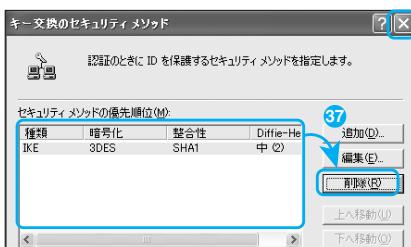
## 35 全般タブをクリックして、詳細設定ボタンをクリックします。



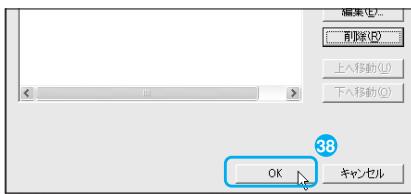
## 36 マスターのPFS (Perfect Forward Security)にチェックを入れ、新しいキーを認証して生成する間隔に値を入力して、メソッドボタンをクリックします。



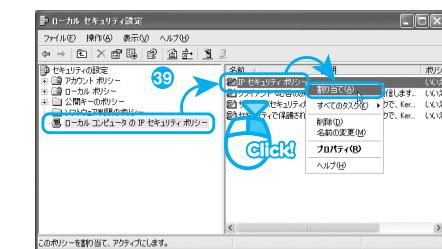
- 37 セキュリティメソッドの優先順位でIKE、3DES、SHA1、中(2)以外の項目を、削除ボタンをクリックして削除します。



- 38 OK→OK→閉じるボタンをクリックします。



- 39 ローカルセキュリティ設定ツールで、左側の画面のローカルコンピュータのIPセキュリティポリシーをクリックし、右側の画面で作成したセキュリティポリシーを右クリックして、割り当てを選択します。



494

## Q. IPsecによる通信確立の確認を行うには

初中上

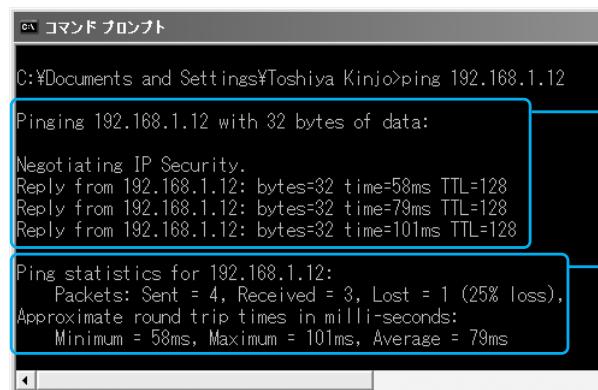
### A. pingコマンドを実行してみます。

ここでは、IPsecの設定を行ったコンピュータ間で通信が行えるかどうかを確認してみましょう。

- 1 コマンドプロンプトを起動して、「ping <相手のIPアドレス>」と入力します。



- 2 数秒後にpingが返ってきます。



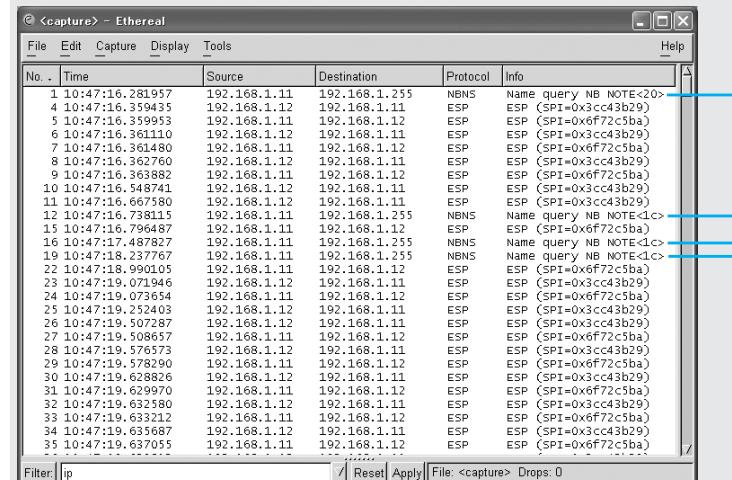
#### 注意 相手側ホストも同様に注意する

以上で設定は完了です。相手側のホストにも同様の設定を行うことで、2台のコンピュータ間で、トランスポートモードESPを使用して、通信を行うことができます。

#### POINT IPsec確立後の通信方法

IPsecによるコネクションが確立したあとは、通常の方法で、コンピュータの一覧を使って相手側のコンピュータの共有フォルダにアクセス

することができます。この場合、やり取りするすべてのパケットは、IPsecによって暗号化が行われます。



#### ブロードキャストによるNetBIOS名前解決要求

ここでは、特定のコンピュータ宛のパケットに対してIPsecが適用されるようにしていくため、ブロードキャストを使ったNetBIOS名前解決要求パケットは、暗号化されていない。ただし、名前解決応答パケットはユニキャストなので暗号化が行われている。

なお、ブロードキャストを除く、2台のコンピュータ間の通信（ユニキャスト）は、すべて暗号化されている（「ESP」と表示されているパケット）。