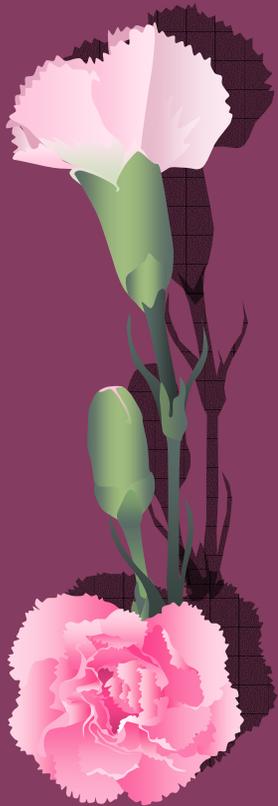


「信頼できるコンピューティング」は 信頼できるか？

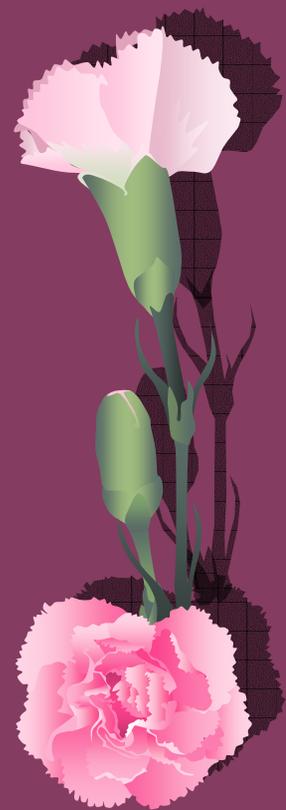
龍谷大学理工学部 小島肇

kjm@rins.ryukoku.ac.jp



今日のお話

- ❁ある一人の
- ❁あまり Windows に詳しくない人が見た
- ❁Windows .NET Server 2003 RC1 の
- ❁デフォルト状態でのセキュリティ状況に関するおぼえがき



「信頼できるコンピューティング」

🌸 (狭い意味での)セキュリティに限った話ではない

➡ セキュリティは、信頼性を高めるための要素のひとつ

🌸 3つのD

➡ Secure by design

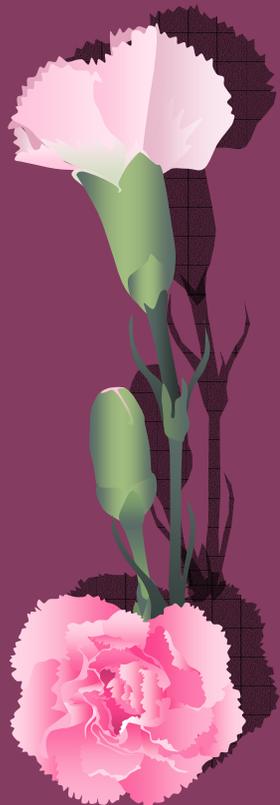
➡ Secure by default

➡ Secure in deployment

🌸 と Communication

“Security and Trustworthy Computing“

<http://www.microsoft.com/enterprise/articles/security.asp>

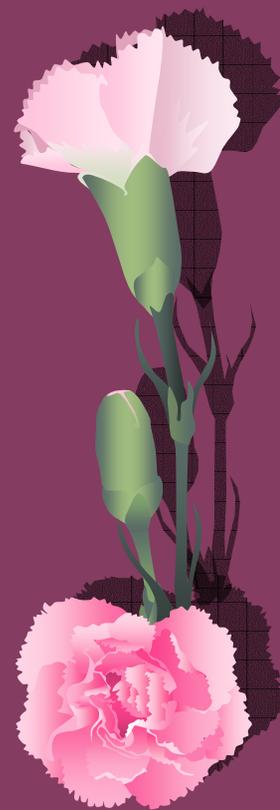


Secure by default

- 🌸 止められる機能はデフォルトで停止させておく。
- 🌸 あらゆる状況において機能を厳重に封鎖 (lock down) する。

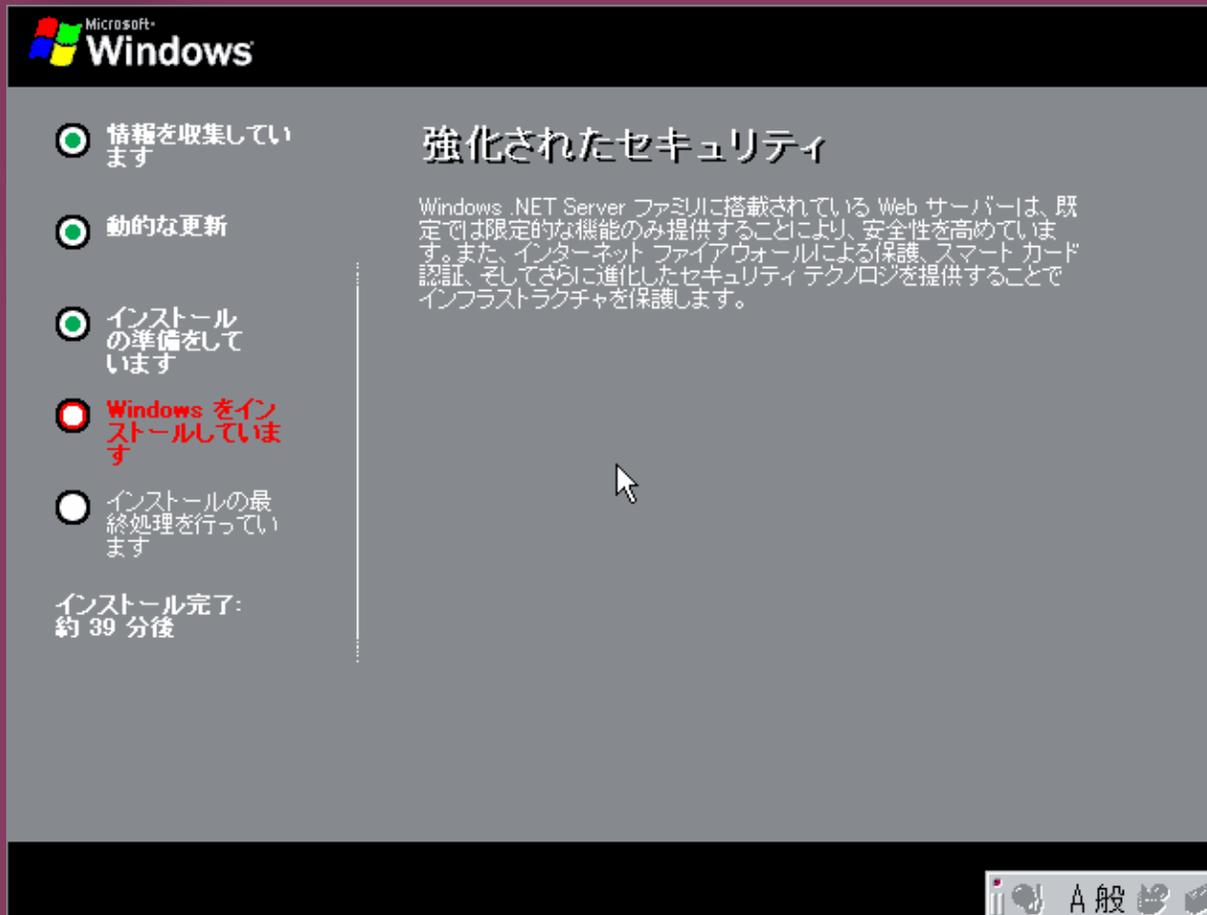
Microsoft is making its products more secure by default, so that components begin their installed life in a secure default state—turned off where possible, and locked down in all cases.

-- “Security and Trustworthy Computing“



Windows .NET Server 2003 RC1 Enterprise Edition

🌸 とりあえずインストールしてみる



The screenshot shows the Windows installation progress screen. At the top left is the Microsoft Windows logo. On the left side, there is a vertical list of five progress indicators, each with a circular icon and text. The third indicator, 'インストールの準備をしています', is highlighted with a red border and a red dot. Below the list, it says 'インストール完了: 約 39 分後'. On the right side, there is a section titled '強化されたセキュリティ' (Enhanced Security) with a paragraph of text. At the bottom right, there is a taskbar with several icons, including a volume icon, a speaker icon, and a network icon.

Microsoft
Windows

- 情報を収集しています
- 動的な更新
- インストールの準備をしています
- Windows をインストールしています**
- インストールの最終処理を行っています

インストール完了:
約 39 分後

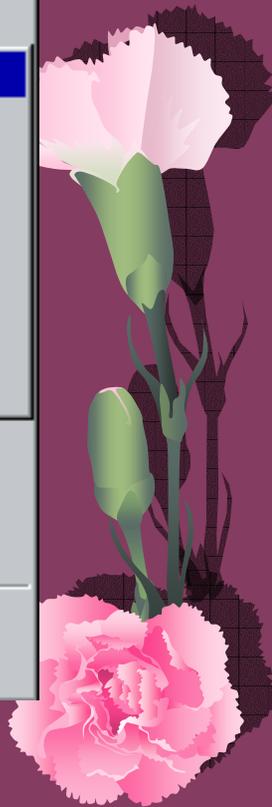
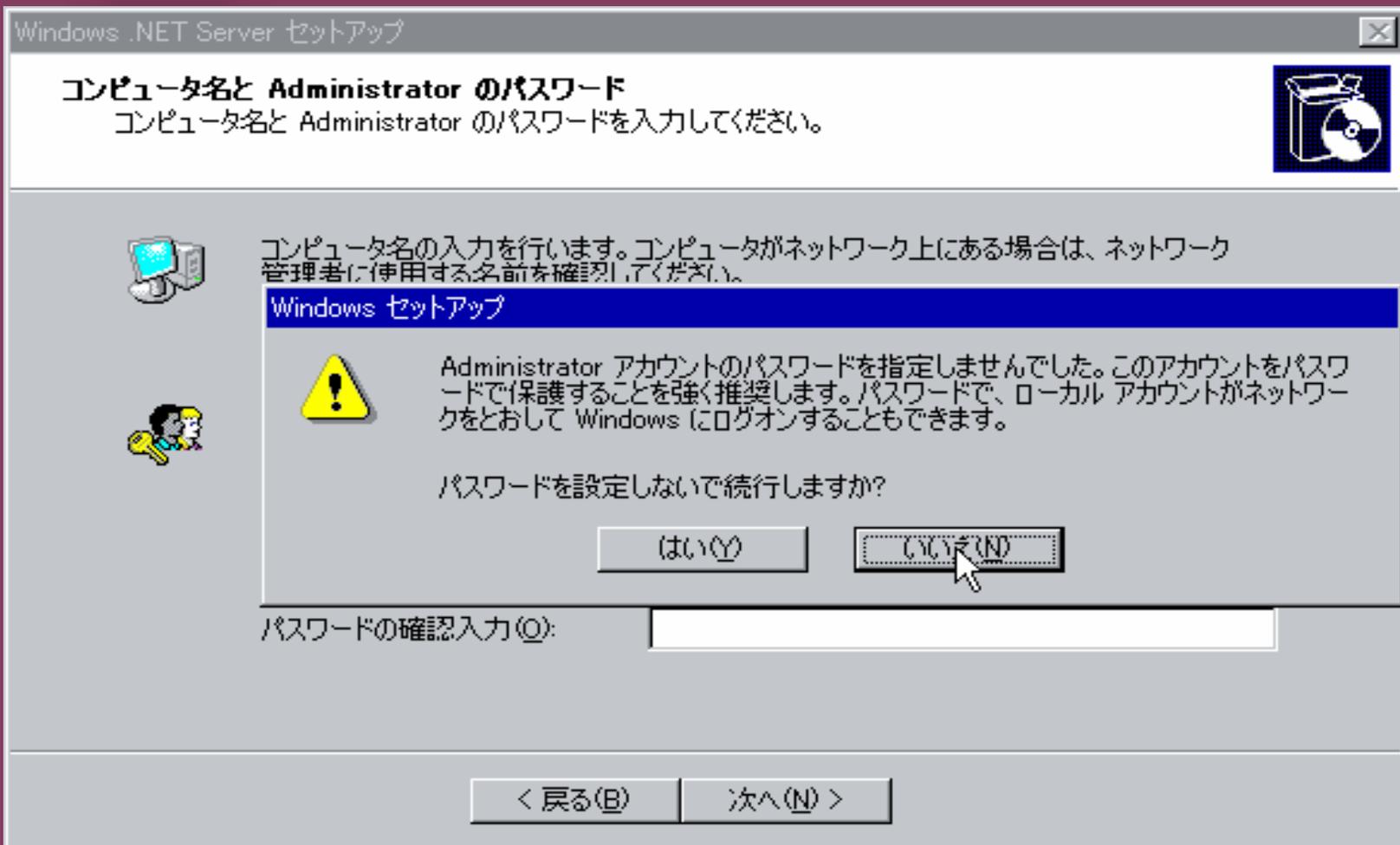
強化されたセキュリティ

Windows .NET Server ファミリに搭載されている Web サーバーは、既定では限定的な機能のみ提供することにより、安全性を高めています。また、インターネット ファイアウォールによる保護、スマート カード認証、そしてさらに進化したセキュリティ テクノロジを提供することでインフラストラクチャを保護します。

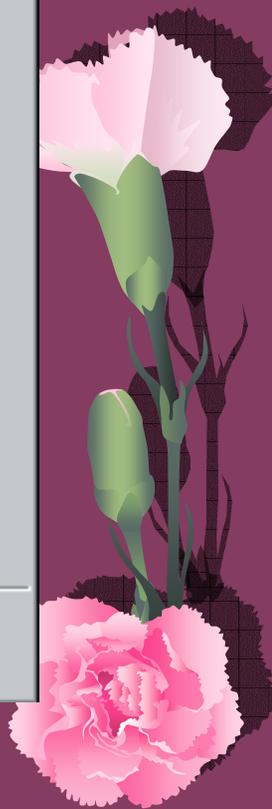
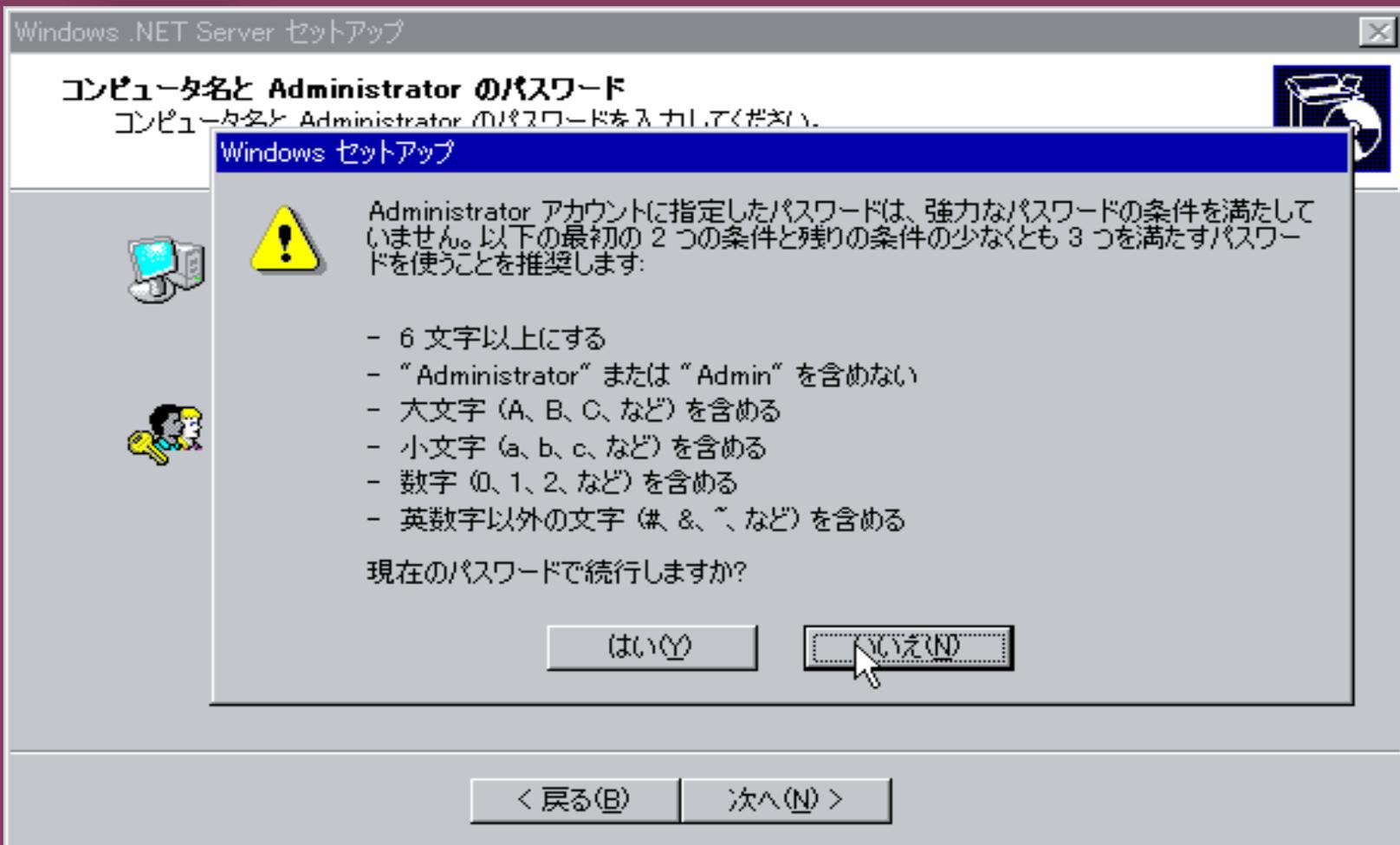
Taskbar: A 般



インストーラ: null パスワードには文句を言う



インストーラ: 不十分なパスワードにも文句を言う



インストール後 nmap してみると

 nmap -sS -O

```
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
```

```
Interesting ports on (133.83.XXX.XXX):
```

```
(The 1597 ports scanned but not shown below are in state: closed)
```

```
Port State Service
```

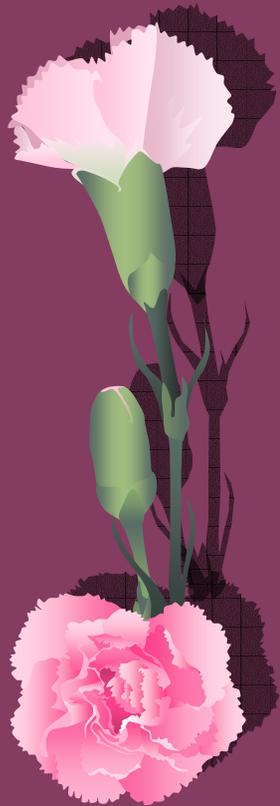
```
135/tcp open loc-srv
```

```
139/tcp open netbios-ssn
```

```
445/tcp open microsoft-ds
```

```
1025/tcp open NFS-or-IIS
```

```
Remote operating system guess: Microsoft Windows.NET Enterprise  
Server (build 36 04-3615 beta)
```



インストール後 nmap してみると

 nmap -sU -O

```
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
```

```
Warning: OS detection will be MUCH less reliable because we did not  
find at least 1 open and 1 closed TCP port
```

```
Interesting ports on (133.83.XXX.XXX):
```

```
(The 1462 ports scanned but not shown below are in state: closed)
```

```
Port State Service
```

```
123/udp open ntp
```

```
137/udp open netbios-ns
```

```
138/udp open netbios-dgm
```

```
445/udp open microsoft-ds
```

```
500/udp open isakmp
```

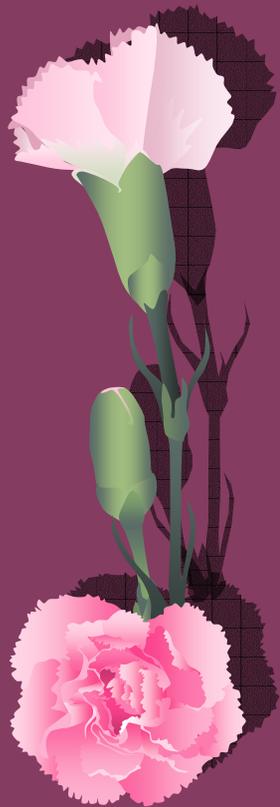
```
4500/udp open sae-urn
```

```
Remote OS guesses: Axis 200+ Web Camera running OS v1.42, Cisco
```

```
Catalyst 2820 Management Console, IBM MVS TCP/IP stack V. 3.2 or
```

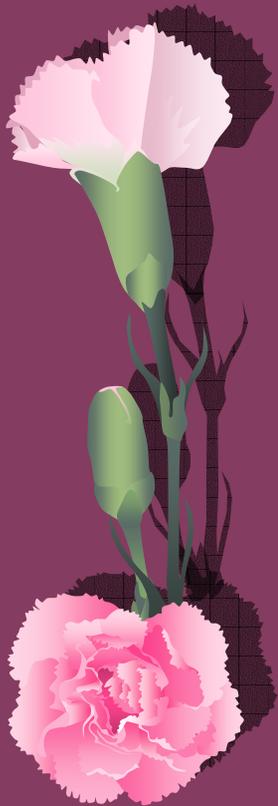
```
AIX 4.3.2, Windows 98SE + IE5.5 sp1, Microsoft Windows.NET
```

```
Enterprise Server (build 3604-3615 beta)
```



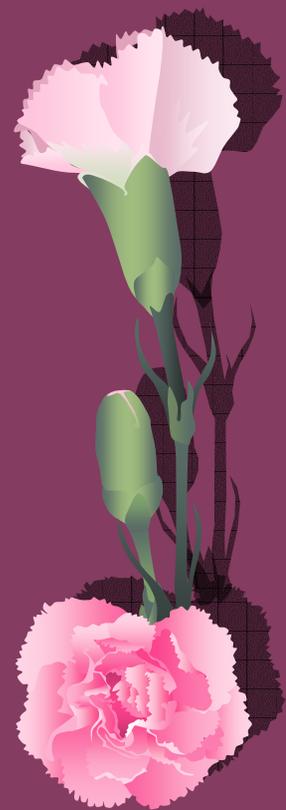
これは何?

- ❁ IIS が上がっていないだけで、port 135, 137-139, 445 は全開
- ❁ .NET Server 2002 にはせっかく ICF (インターネット接続ファイアウォール) があるのだから、せめてインストール中に有効・無効の選択をさせられないのか?
 - ➡ ICF 自体は Windows XP のものと同じです。
 - ➡ 現状では、インストール中に有効にすることはできません。
- ❁ いまどきの Linux なら、デフォルトで packet filter が有効になるのがふつうなのに...



インストール後に有効にすれば いいじゃん

- ❁ それは Secure by Default ではない...
- ❁ アプリ屋さんはデフォルトインストールの状態
で開発・テストをする(ような)ので、イン
ストール時の状態はたいへん重要
 - ➡ わざわざセキュリティのことを考えてくれるア
プリ屋さんは、とっても少ない...
 - ➡ というか、業界だけな気が...

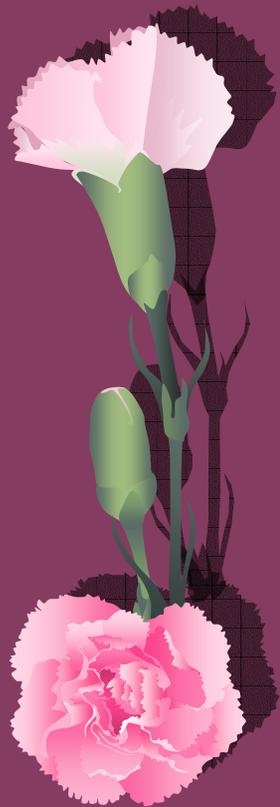


ICF を有効にすると...

 nmap -sS -O

「Web サーバー」「リモートデスクトップ」にチェックを入れた場合(ここでは IIS やリモートデスクトップは起動させていない)

```
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )  
Warning: OS detection will be MUCH less reliable because we did not  
find at least 1 open and 1 closed TCP port  
Interesting ports on (133.83.XXX.XXX):  
(The 1599 ports scanned but not shown below are in state: filtered)  
Port State Service  
80/tcp closed http  
3389/tcp closed ms-term-serv  
Too many fingerprints match this host for me to give an accurate OS  
guess
```

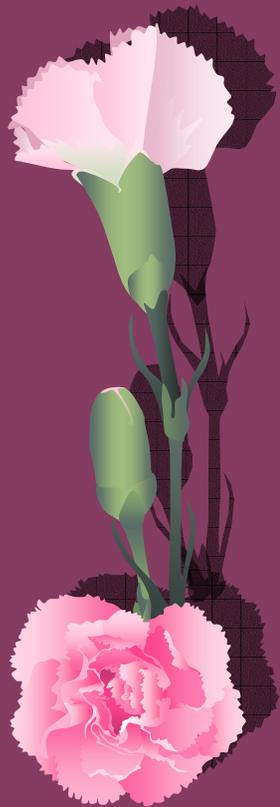


ICF を有効にすると...

 nmap -sU -O

「Web サーバー」「リモートデスクトップ」にチェックを入れた場合(ここでは IIS やリモートデスクトップは起動させていない)

```
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )  
Warning: OS detection will be MUCH less reliable because we did not  
find at least 1 open and 1 closed TCP port  
All 1468 scanned ports on (133.83.XXX.XXX) are: filtered  
Too many fingerprints match this host for me to give an accurate OS  
guess
```



ICF はいいことばかりですか？

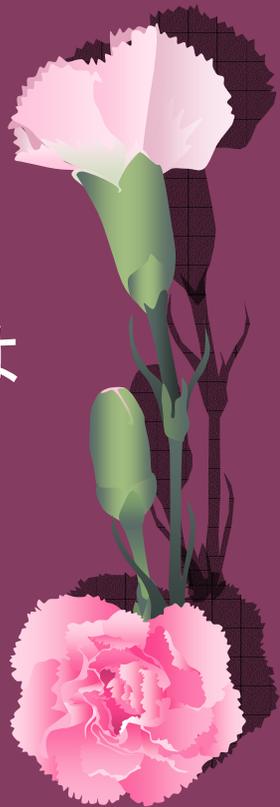
❁ イン트라ネットでは混乱が発生するかもしれませんが、なので「選択させる」がよいと思うのです。

🍃 事例: [samba-jp:13876] Master Browser をまた、奪われてしまいました。から続くスレッド

<http://www.samba.gr.jp/ml/samba-jp/htdocs/200211.month/13876.html>

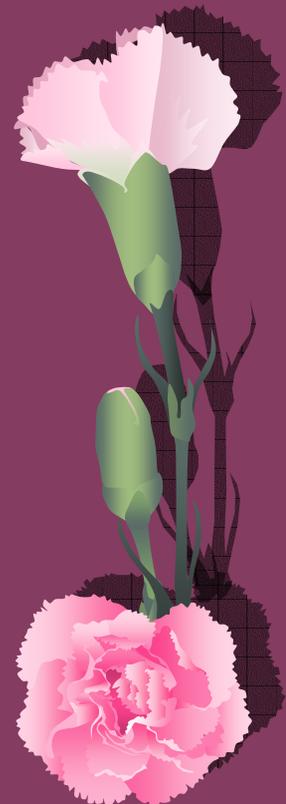
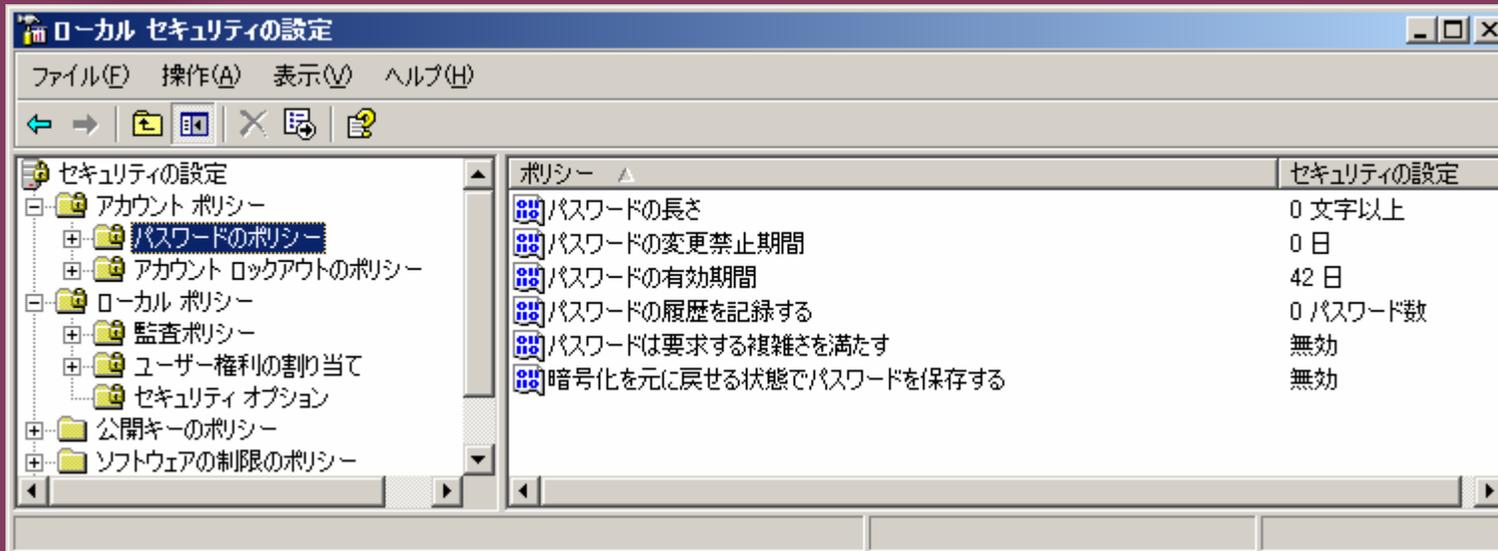
❁ Active Directory をはじめとする、まともなディレクトリサービスが整った環境では、こういう苦労はしなくてすむはずなのですが。

🍃 「だから AD にしよう！」みたいな話は意外なほど聞かない気がするのはなぜ？



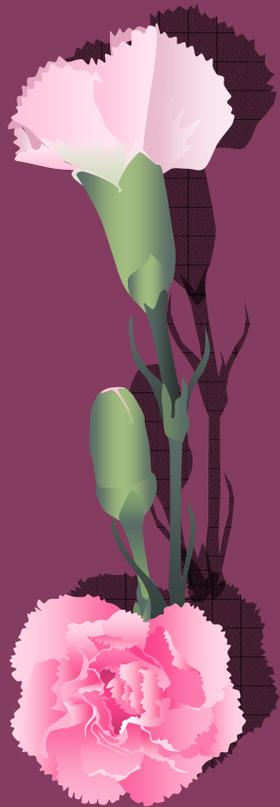
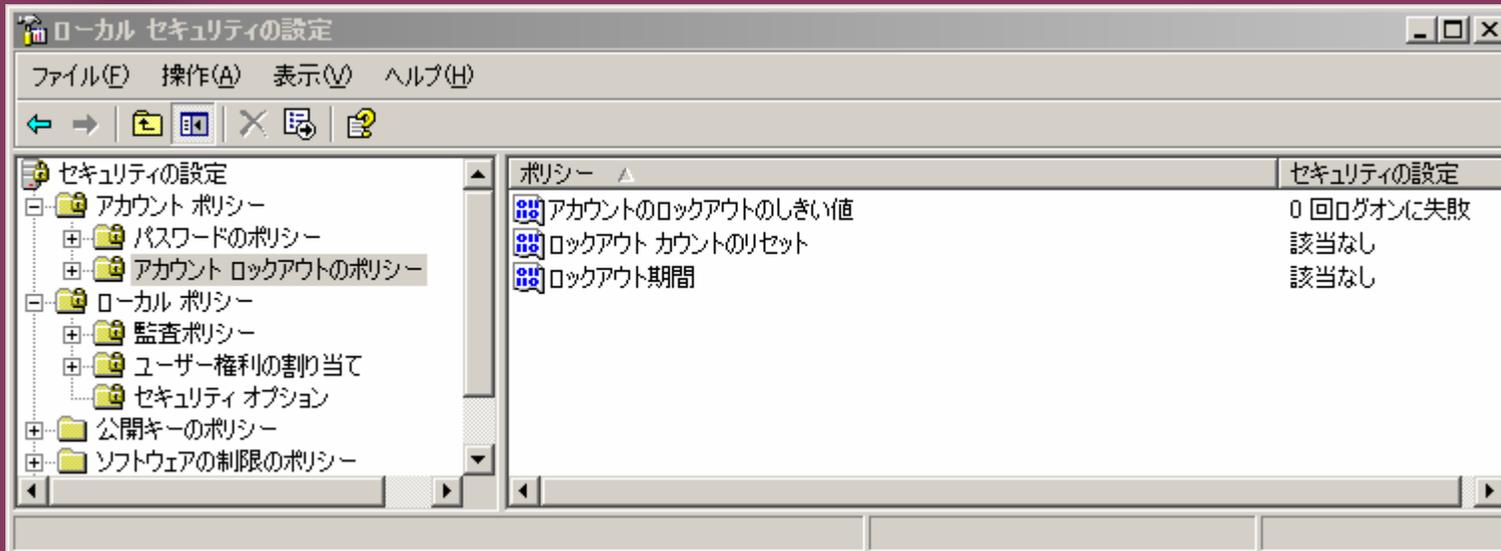
ローカルセキュリティポリシー (1)

- 🌸 パスワードポリシー: Windows 2000 と同じ...。
- 🍌 せめて「パスワードの長さ」はなんとかならないのか...



ローカルセキュリティポリシー (2)

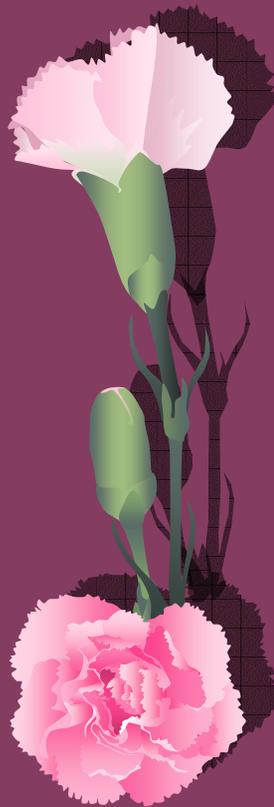
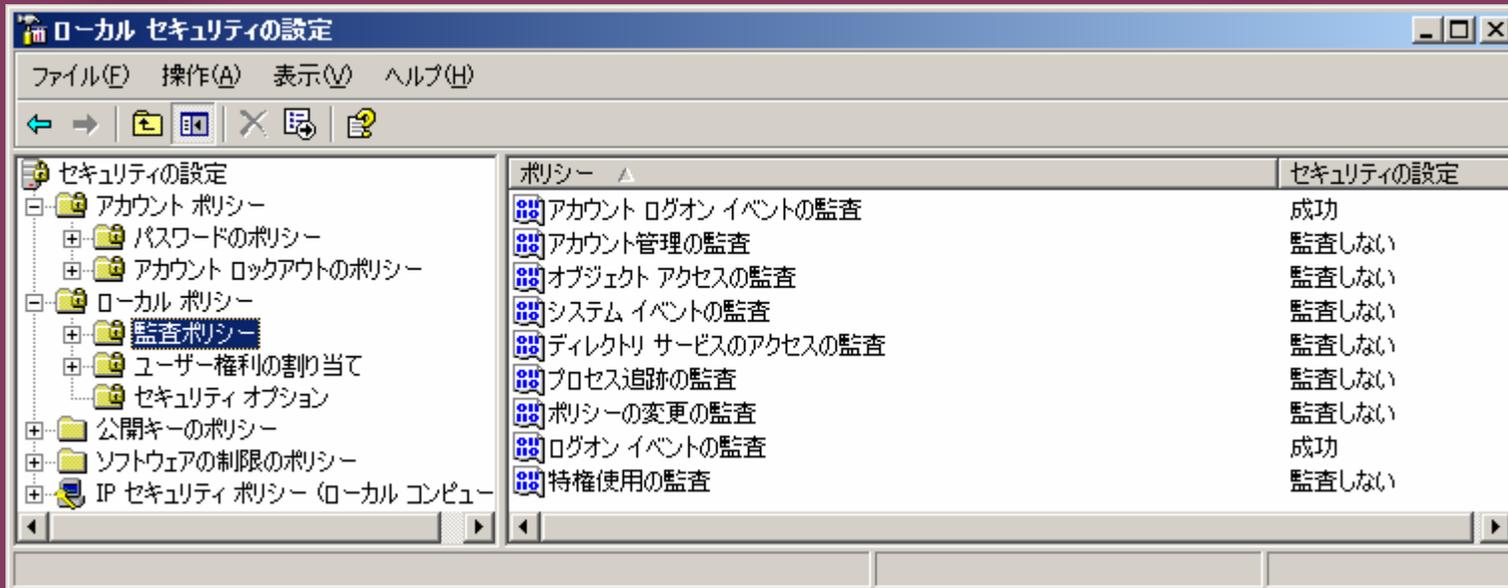
🌸 パスワードロックアウトポリシー: Windows 2000
と同じ....。



ローカルセキュリティポリシー (3)

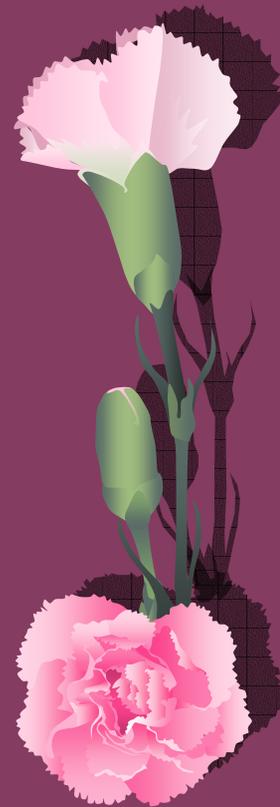
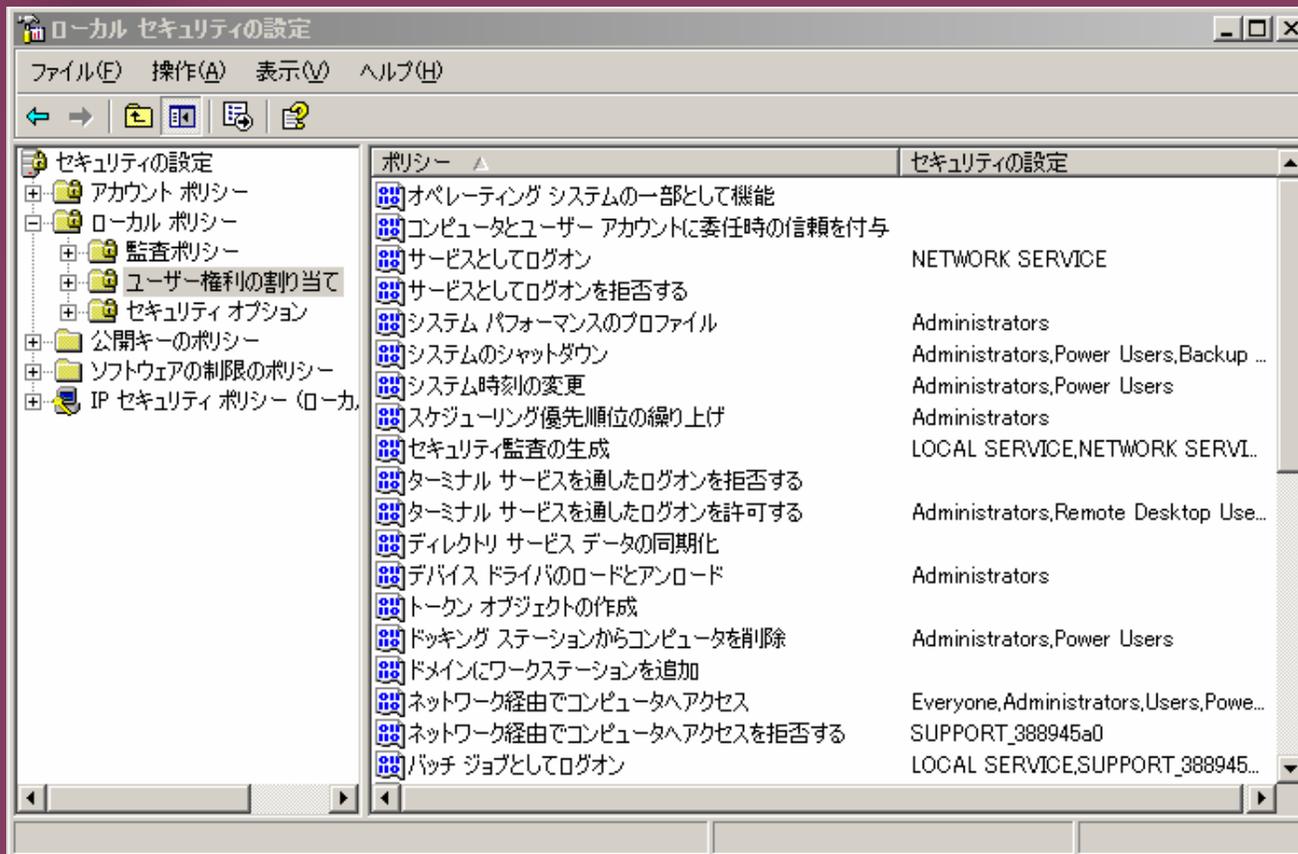
🌸 監査ポリシー:ちょっと変わったとはいえ、これはあまりに不十分ではないか?

🍴 成功だけ見てどうする...



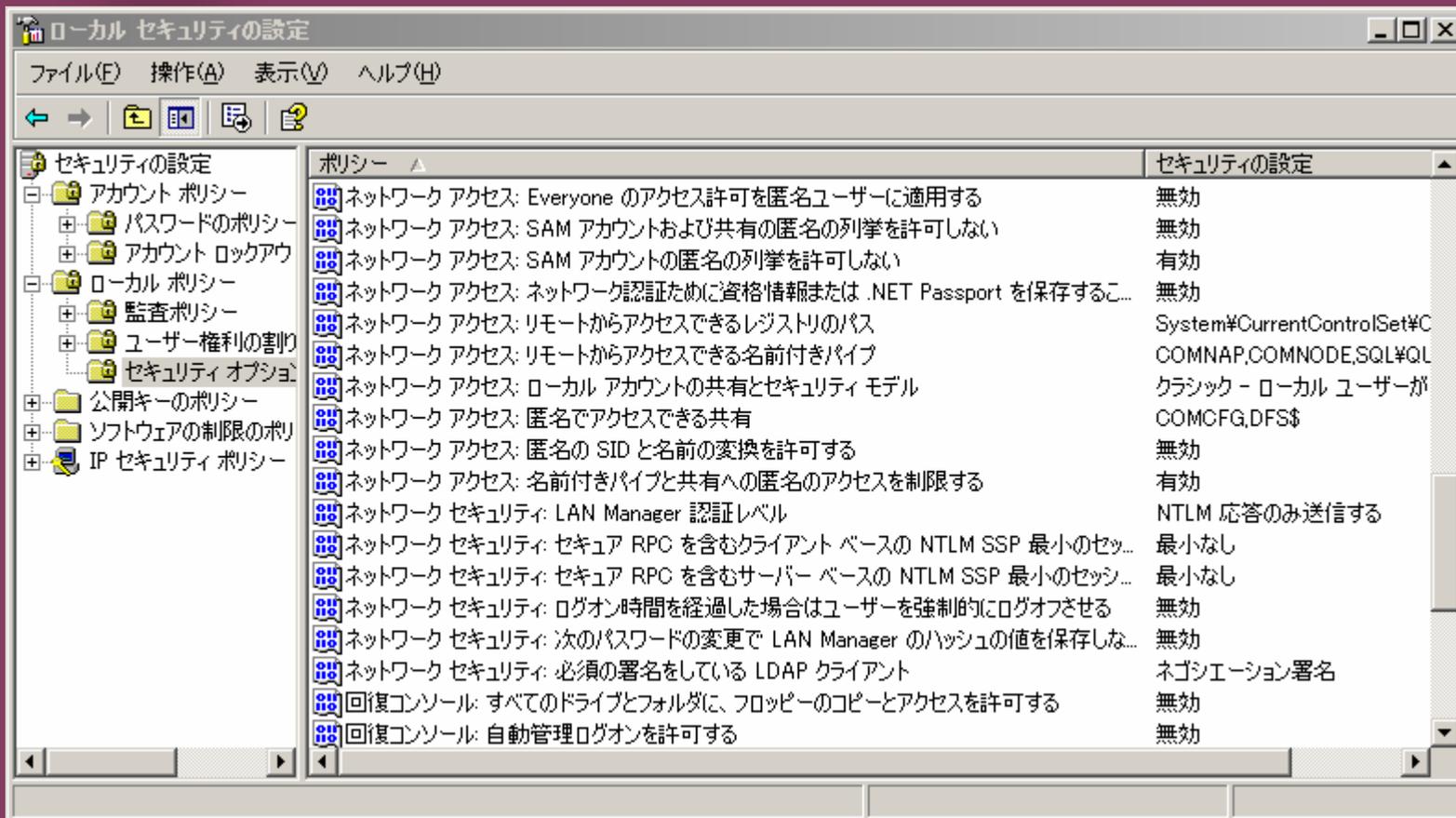
ローカルセキュリティポリシー (4)

ユーザー権利の割り当て



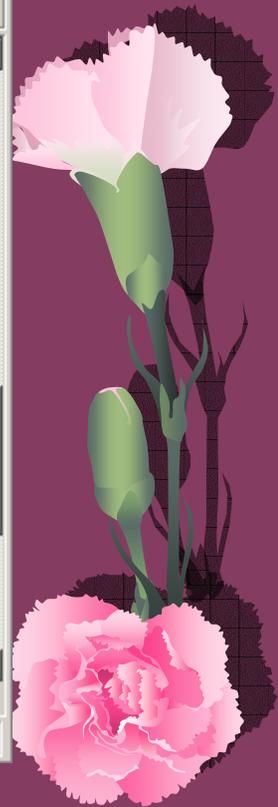
ローカルセキュリティポリシー (5)

🌸 セキュリティオプション – ちょっと前進



The screenshot shows the Windows Local Security Policy console. The left pane shows the tree view with 'Security Options' selected. The main pane displays a list of 16 security options with their current settings.

ポリシー	セキュリティの設定
ネットワーク アクセス: Everyone のアクセス許可を匿名ユーザーに適用する	無効
ネットワーク アクセス: SAM アカウントおよび共有の匿名の列挙を許可しない	無効
ネットワーク アクセス: SAM アカウントの匿名の列挙を許可しない	有効
ネットワーク アクセス: ネットワーク認証のために資格情報または .NET Passport を保存するこ...	無効
ネットワーク アクセス: リモートからアクセスできるレジストリのパス	System#CurrentControlSet#C...
ネットワーク アクセス: リモートからアクセスできる名前付きパイプ	COMNAP,COMNODE,SQL#SQL
ネットワーク アクセス: ローカル アカウントの共有とセキュリティ モデル	クラシック - ローカル ユーザーが
ネットワーク アクセス: 匿名でアクセスできる共有	COMCFG,DFS\$
ネットワーク アクセス: 匿名の SID と名前の変換を許可する	無効
ネットワーク アクセス: 名前付きパイプと共有への匿名のアクセスを制限する	有効
ネットワーク セキュリティ: LAN Manager 認証レベル	NTLM 応答のみ送信する
ネットワーク セキュリティ: セキュア RPC を含むクライアント ベースの NTLM SSP 最小のセッ...	最小なし
ネットワーク セキュリティ: セキュア RPC を含むサーバー ベースの NTLM SSP 最小のセッシ...	最小なし
ネットワーク セキュリティ: ログオン時間を経過した場合はユーザーを強制的にログオフさせる	無効
ネットワーク セキュリティ: 次のパスワードの変更で LAN Manager のハッシュの値を保存しな...	無効
ネットワーク セキュリティ: 必須の署名をしている LDAP クライアント	ネゴシエーション署名
回復コンソール: すべてのドライブとフォルダに、フロッピーのコピーとアクセスを許可する	無効
回復コンソール: 自動管理ログオンを許可する	無効



null 接続に対する反応の違い

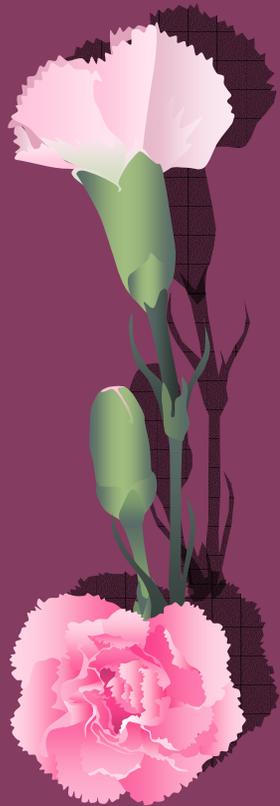
🌸 enum – Win32 information enumeration utility

<http://razor.bindview.com/tools/index.shtml>

🌸 enum -U: get userlist

```
C:\>enum -U 133.83.XXX.XXX ← Windows 2000 Server
server: 133.83.XXX.XXX
setting up session... success.
getting user list (pass 1, index 0)... success, got 5.
Administrator Guest IUSR_BRAI-WIN2000S IWAM_BRAI-WIN2000S
TsInternetUser
cleaning up... success.
```

```
C:\>enum -U 133.83.XXX.YYY ← Windows .NET Server 2003 RC1
server: 133.83.XXX.YYY
setting up session... success.
getting user list (pass 1, index 0)... fail
return 5, アクセスが拒否されました。
cleaning up... success.
```

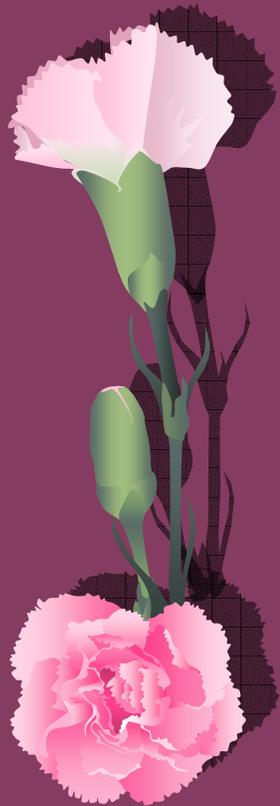


null 接続に対する反応の違い

🌸 enum -P: get password policy information

```
C:\>enum -P 133.83.XXX.XXX
server: 133.83.XXX.XXX
setting up session... success.
password policy:
  min length: none
  min age: none
  max age: 42 days
  lockout threshold: none
  lockout duration: 30 mins
  lockout reset: 30 mins
cleaning up... success.
```

```
C:\>enum -P 133.83.XXX.YYY
server: 133.83.XXX.YYY
setting up session... success.
couldn't get password policy
return 5, アクセスが拒否されました。
couldn't get lockout policy
return 5, アクセスが拒否されました。
cleaning up... success.
```



null 接続に対する反応の違い

🌸 enum -L: get LSA policy information

```
C:\>enum -L 133.83.XXX.XXX
server: 133.83.XXX.XXX
setting up session... success.
opening lsa policy... success.
server role: 3 [primary (unknown)]
names:
  netbios: BRAI-WIN2000S
  domain: TAKO
quota:
  paged pool limit: 33554432
  non paged pool limit: 1048576
  min work set size: 65536
  max work set size: 251658240
  pagefile limit: 0
  time limit: 0
trusted domains:
  indeterminate
netlogon done by a PDC server
cleaning up... success.
```

```
C:\>enum -L 133.83.XXX.YYY
server: 133.83.XXX.YYY
setting up session... success.
opening lsa policy... success.
names: ←ここで enum が異常終了
```



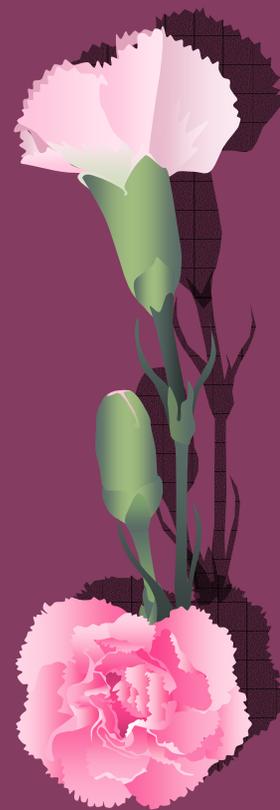
null 接続に対する反応の違い

enum -S: get sharelist

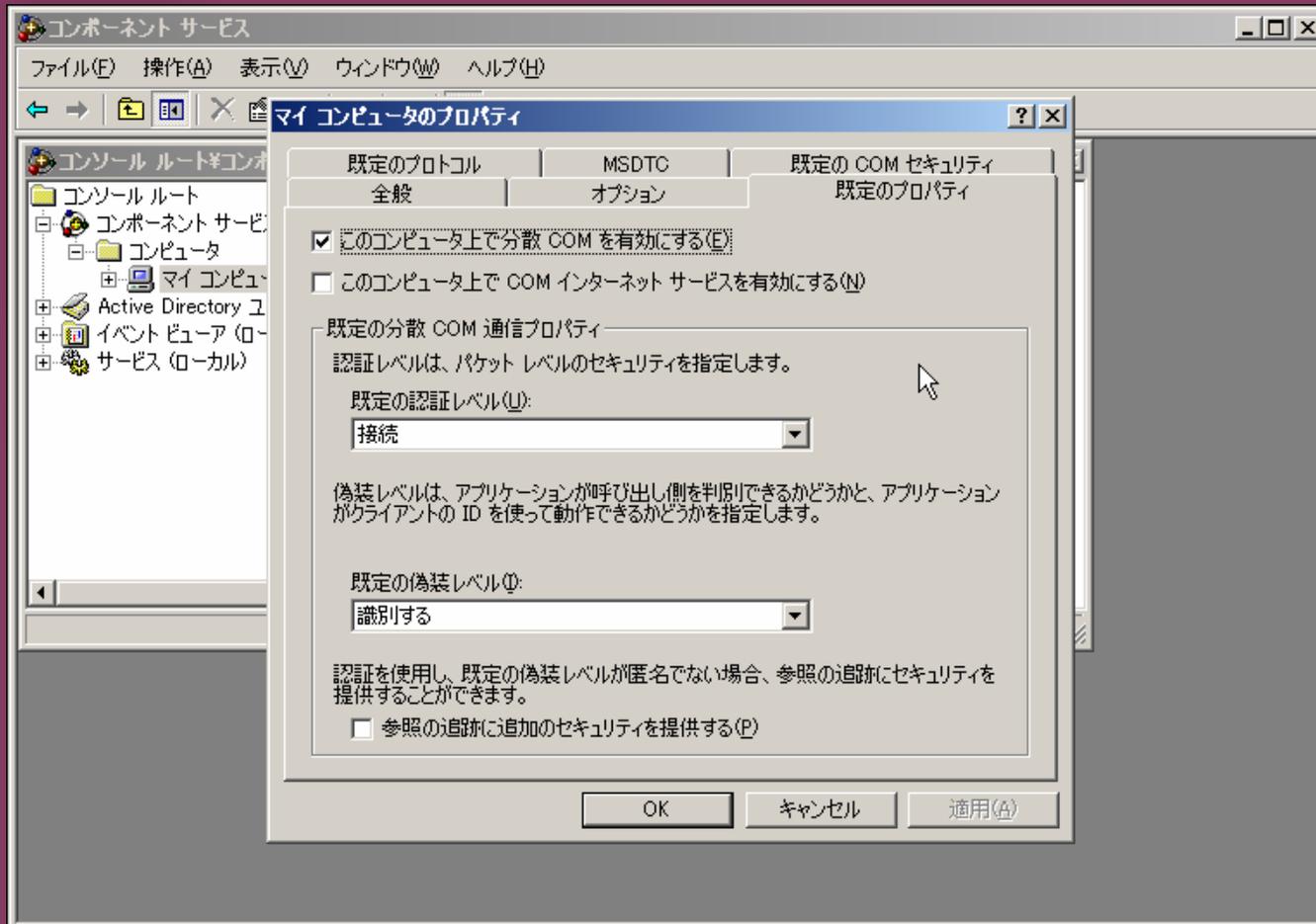
```
C:\>enum -S 133.83.XXX.XXX
server: 133.83.XXX.XXX
setting up session... success.
enumerating shares (pass 1)... got 3 shares, 0 left:
  IPC$  ADMIN$  C$
cleaning up... success.
```

```
C:\>enum -S 133.83.XXX.YYY
server: 133.83.XXX.YYY
setting up session... success.
enumerating shares (pass 1)... got 3 shares, 0 left:
  IPC$  ADMIN$  C$
cleaning up... success.
```

-  ポリシー「SAM アカウントおよび匿名の共有の列挙を許可しない」を有効にすることで拒否できる



DCOM – もちろん有効



IE'en (remotely controls Internet Explorer using DCOM) で遊ぼう!?
http://www.securityfriday.com/ToolDownload/IEen/ieen_doc.html



IIS 6.0 をインストールしてみる

サーバーの構成ウィザード

サーバーの役割

このサーバーをセットアップして、複数の特定の役割を実行させることができます。このサーバーに複数の役割を追加する場合は、このウィザードを再度実行してください。

役割を選択してください。役割を追加していない場合は、追加することができます。既に追加している場合は、その役割を削除できます。追加または削除する役割が一覧に表示されていない場合は、[プログラムの追加と削除](#)を開いてください。

サーバーの役割	構成済み
ファイル サーバー	はい
プリント サーバー	はい
Web アプリケーションサーバー (IIS、ASP.NET)	はい
メール サーバー (POP3、SMTP)	はい
ターミナル サーバー	はい
リモート アクセス / VPN サーバー	はい
ドメイン コントローラ (Active Directory)	はい
DNS サーバー	はい
DHCP サーバー	はい
ストリーミング メディア サーバー	はい
WINS サーバー	はい

Web アプリケーションサーバー (IIS、ASP.NET)

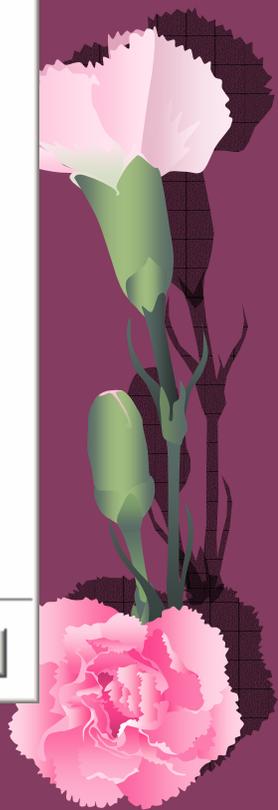
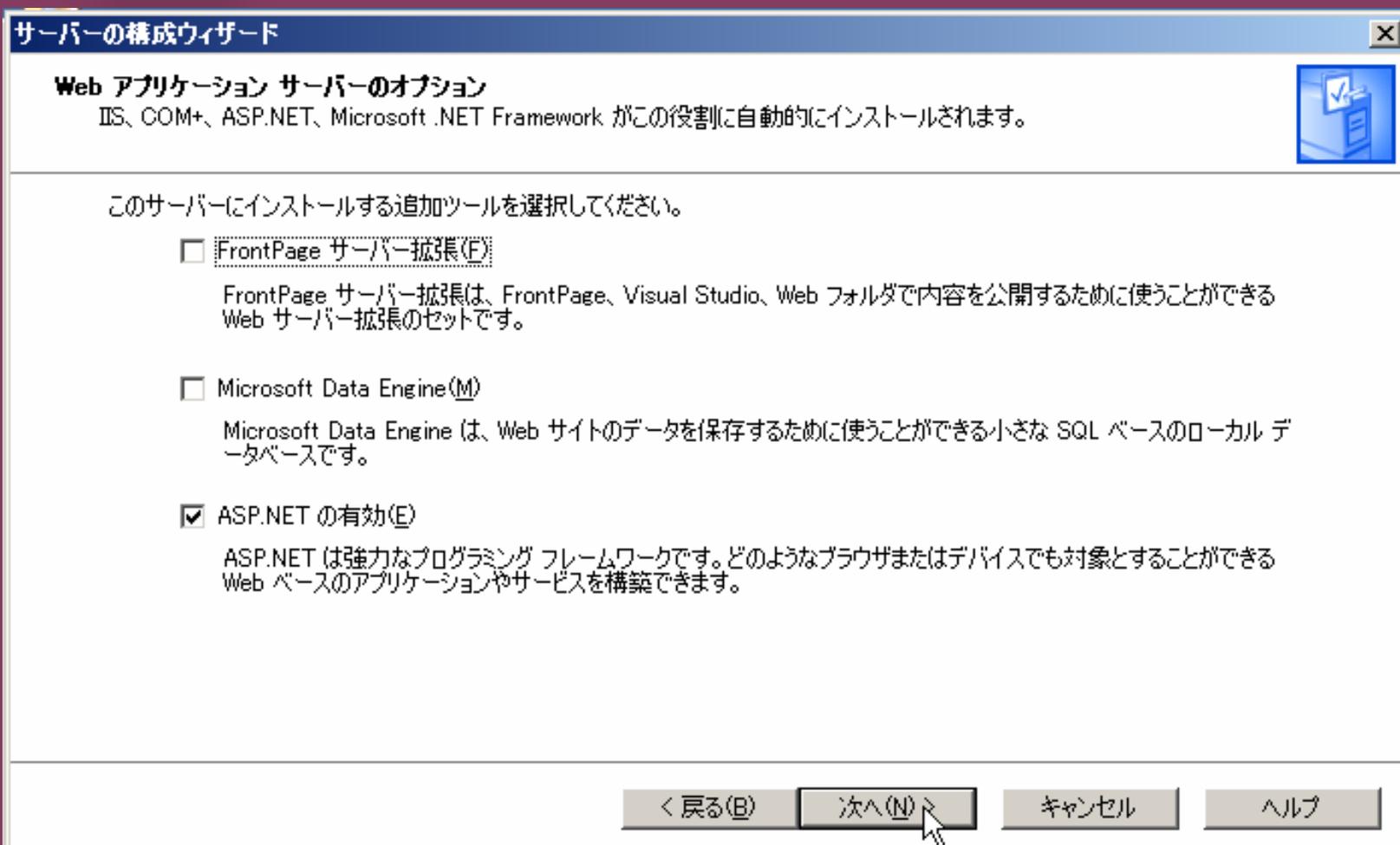
Web アプリケーション サーバーは、インターネット インフォメーション サービス (IIS)、ASP.NET、COM+ を含む Web アプリケーションや Web サービスを構築、展開、操作するのに必要なコア テクノロジーを提供します。

[Web アプリケーション サーバーについての詳細情報を表示する](#)

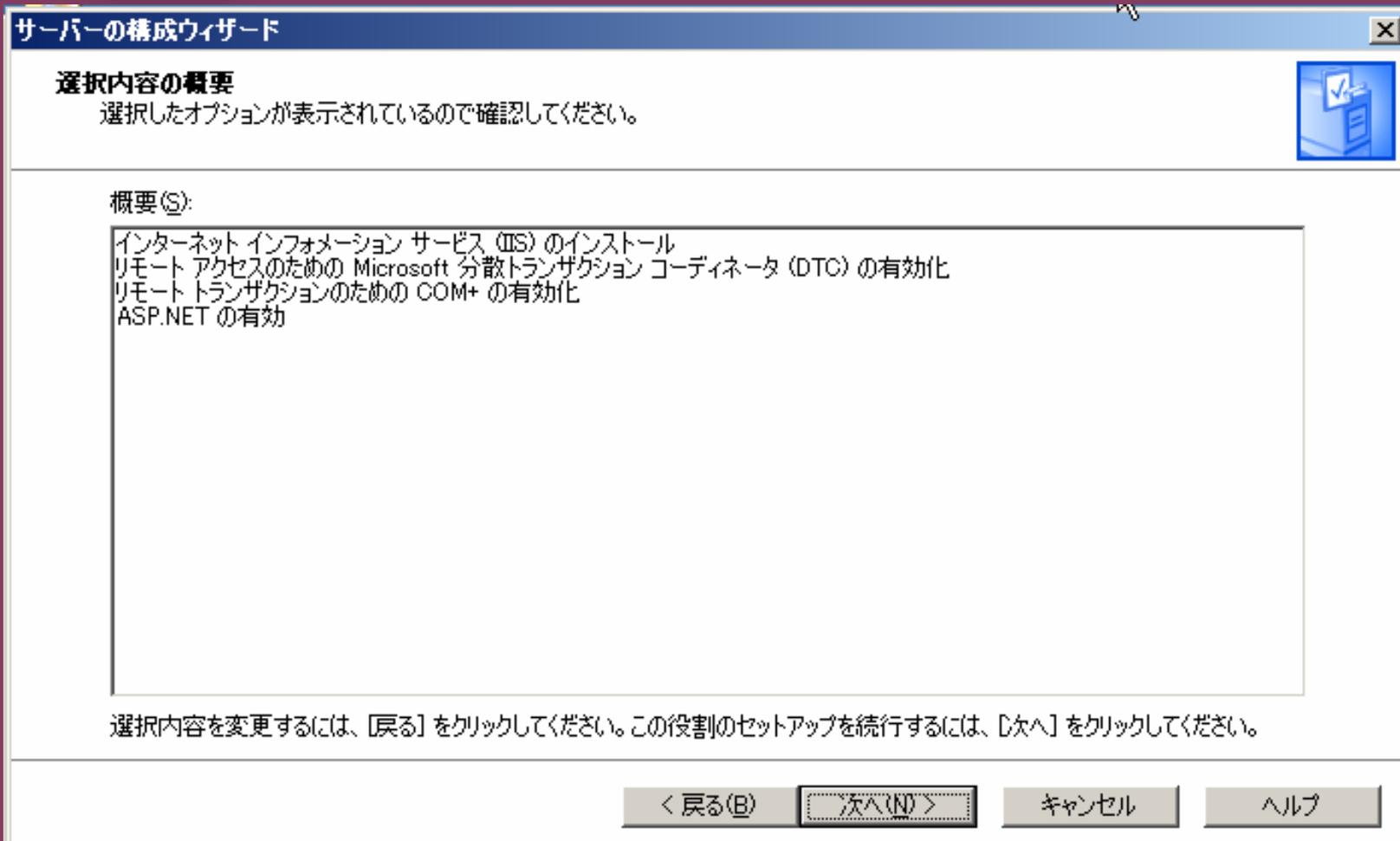
< 戻る(B) 次へ(N) > キャンセル ヘルプ



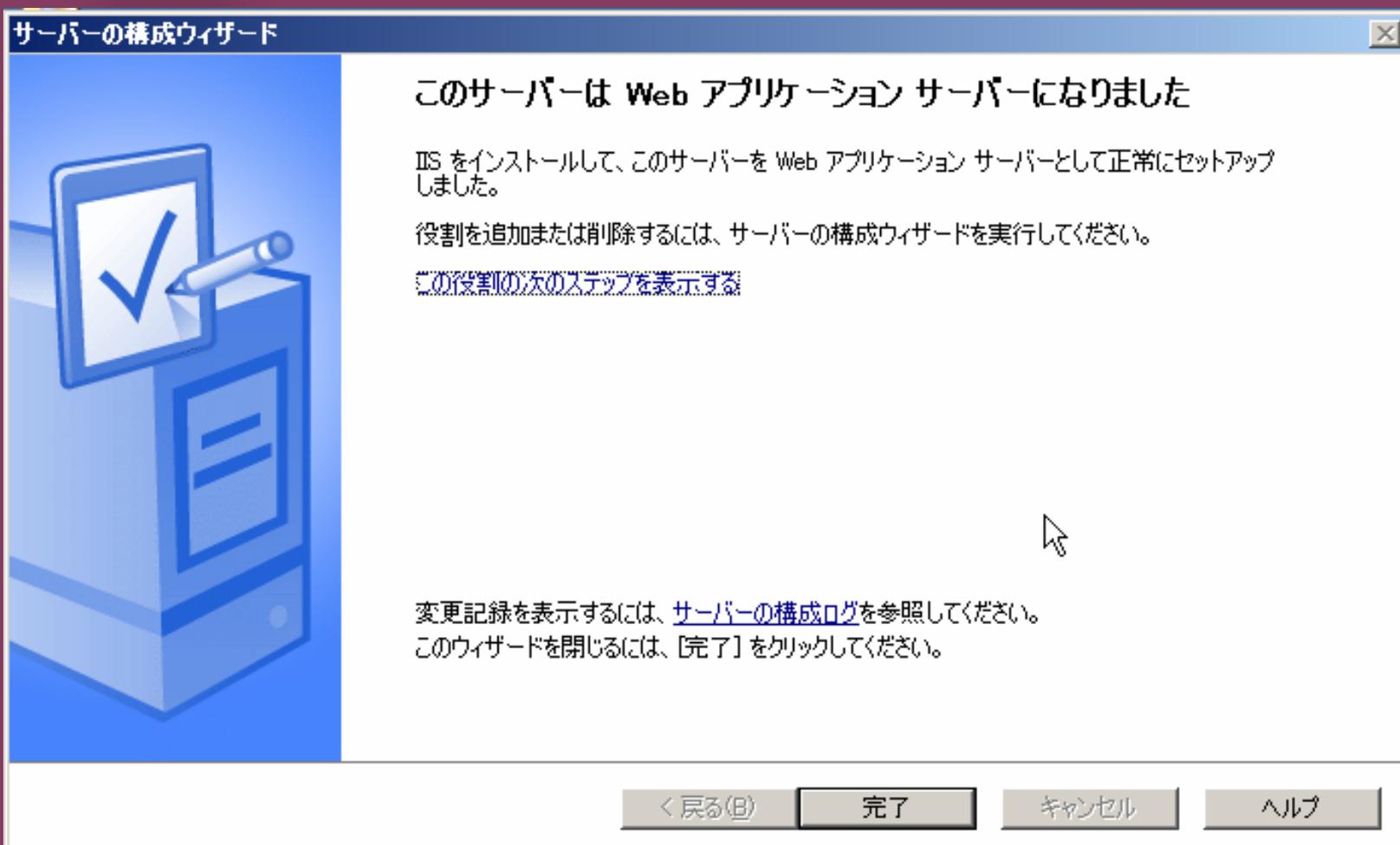
IIS 6.0 をインストールしてみる



IIS 6.0 をインストールしてみる



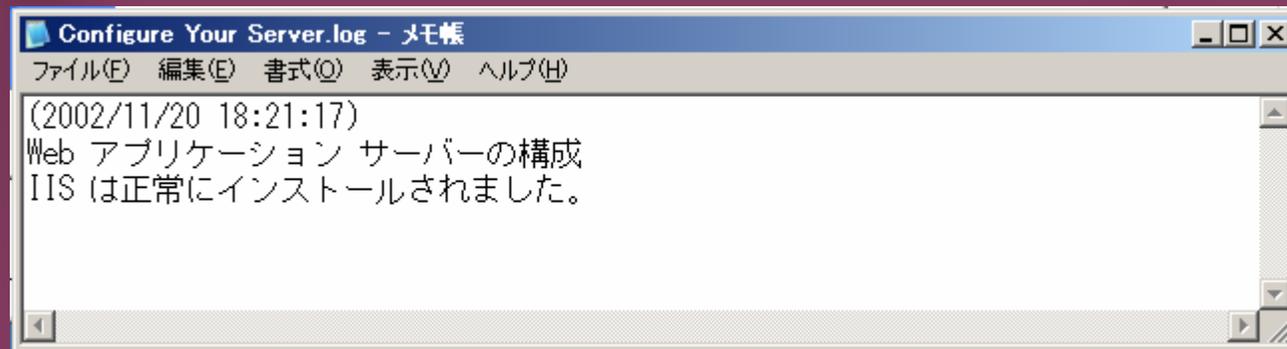
IIS 6.0 をインストールしてみる



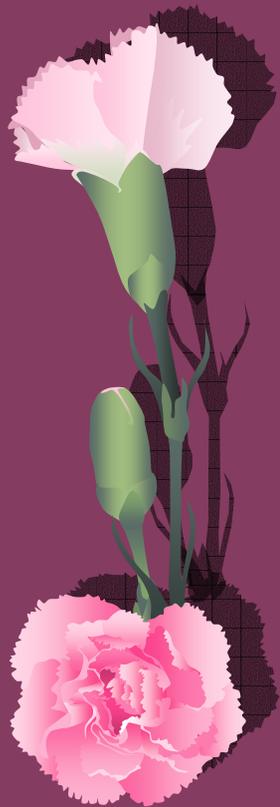
IIS 6.0 をインストールしてみる

🌸 サーバーの構成ログ

🍌 もうちょっとなんとかならんのか (^^;;;)

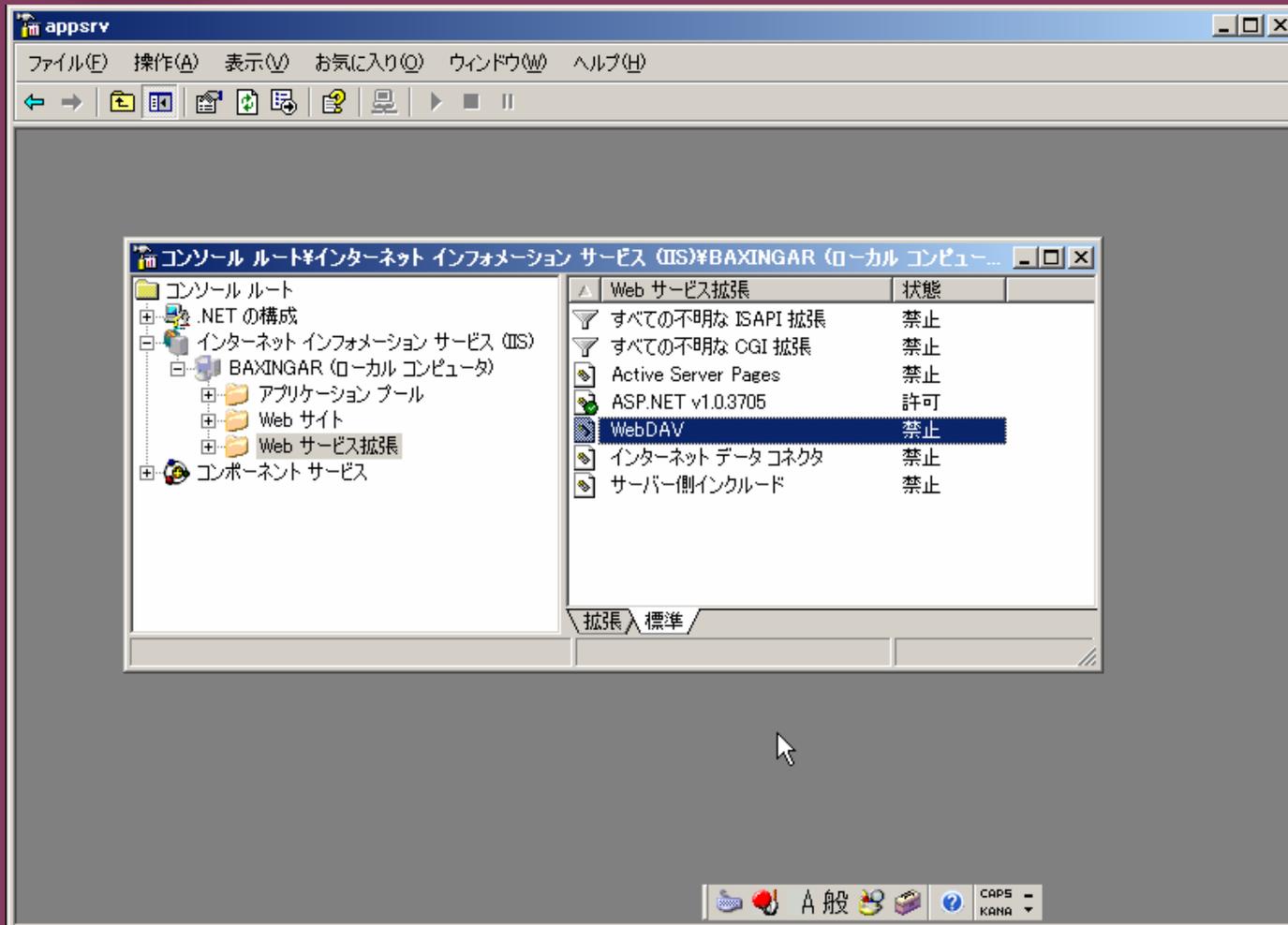


```
Configure Your Server.log - メモ帳
ファイル(F) 編集(E) 書式(O) 表示(V) ヘルプ(H)
(2002/11/20 18:21:17)
Web アプリケーション サーバーの構成
IIS は正常にインストールされました。
```



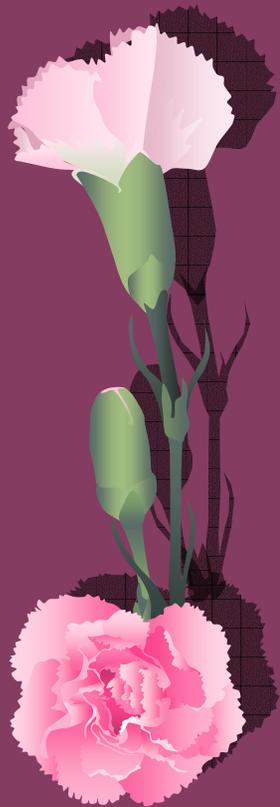
IIS 6.0 を設定してみる

🌸 上記のようにインストールした場合の状態



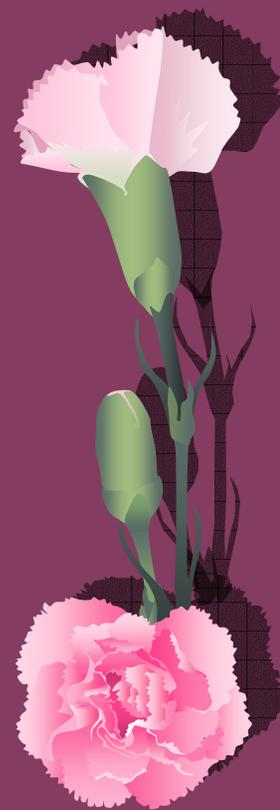
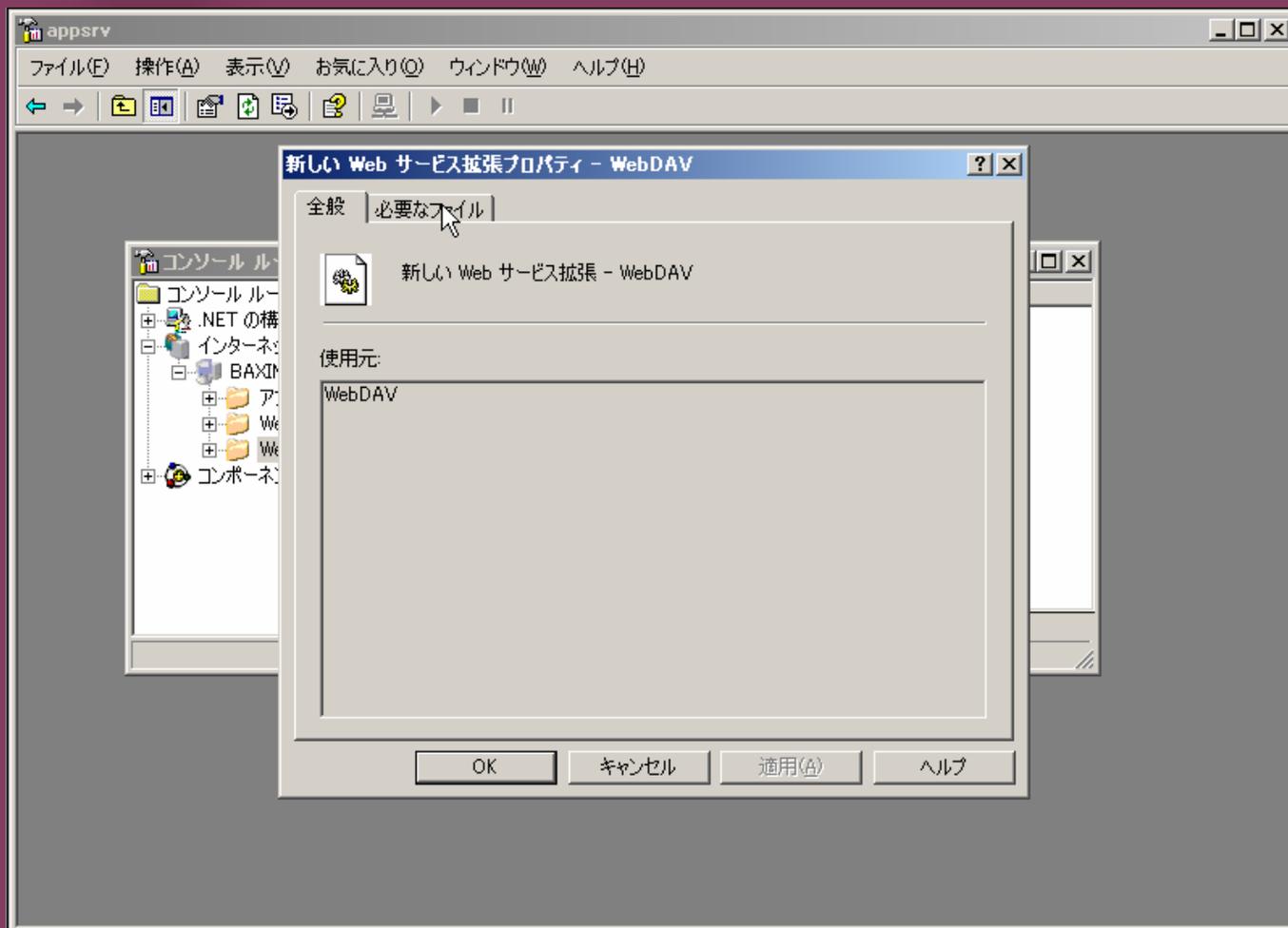
The screenshot shows the IIS 6.0 console window for the local computer. The left pane shows the tree view with 'Web サービス拡張' (Web Service Extensions) selected. The right pane displays a table of installed extensions and their status.

Web サービス拡張	状態
すべての不明な ISAPI 拡張	禁止
すべての不明な CGI 拡張	禁止
Active Server Pages	禁止
ASP.NET v1.0.3705	許可
WebDAV	禁止
インターネット データ コネクタ	禁止
サーバー側インクルード	禁止



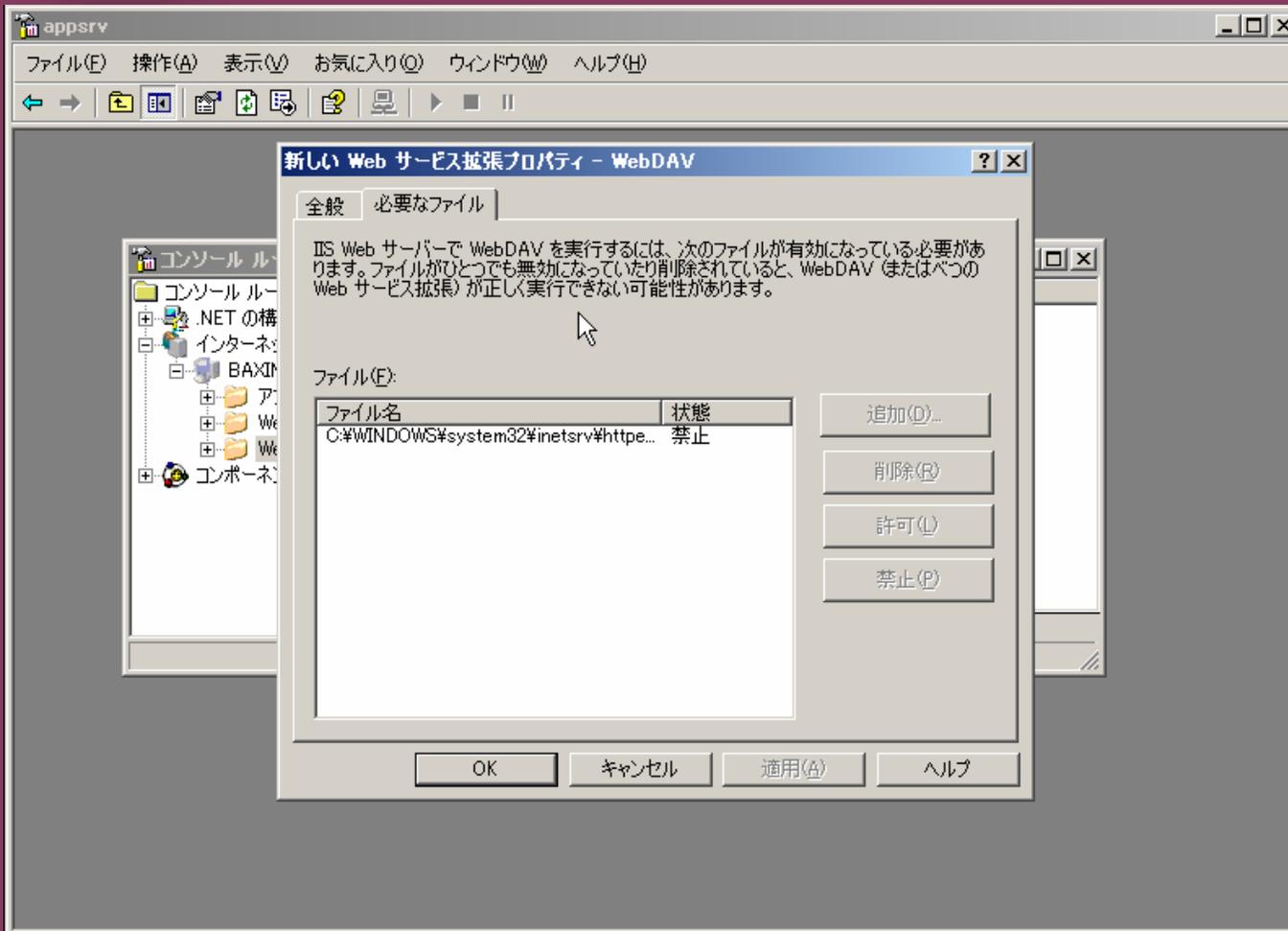
IIS 6.0 を設定してみる

🌸 ダブルクリックしてみる



IIS 6.0 を設定してみる

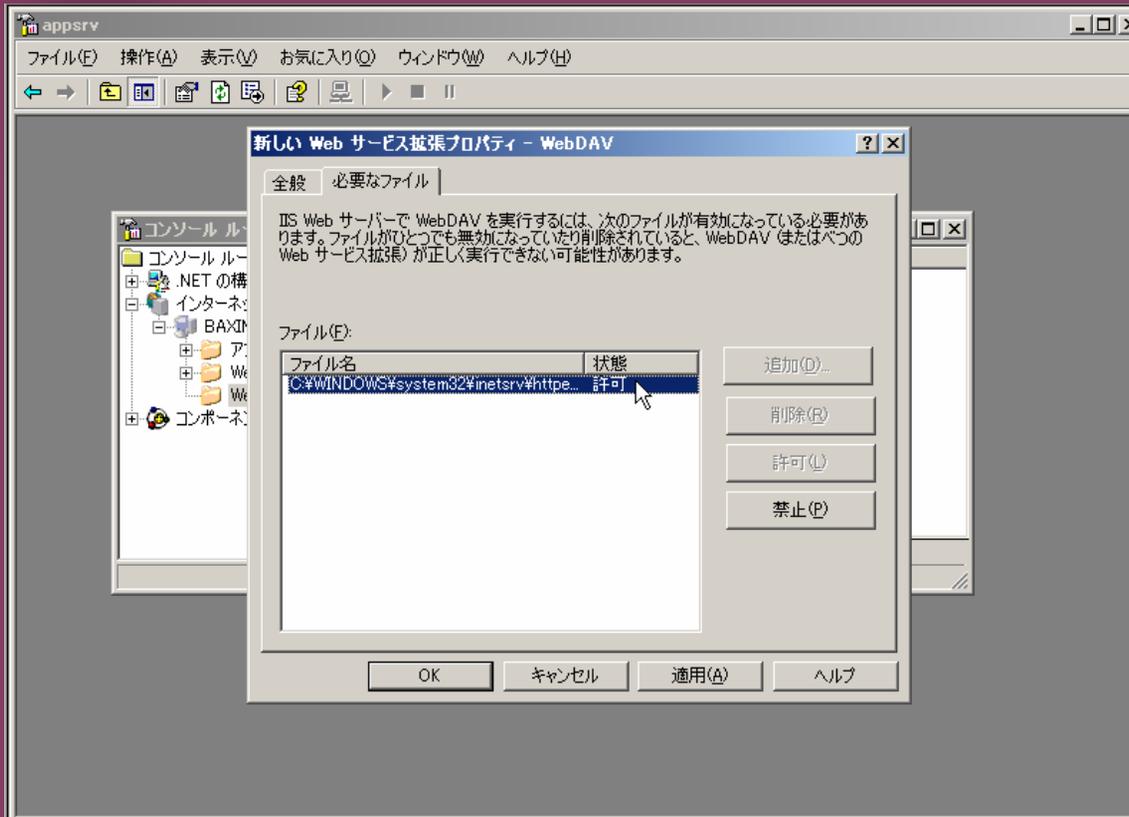
🌸 「必要なファイル」タブ



IIS 6.0 を設定してみる

🌸 ファイル名をダブルクリックすると、いきなり「有効」に

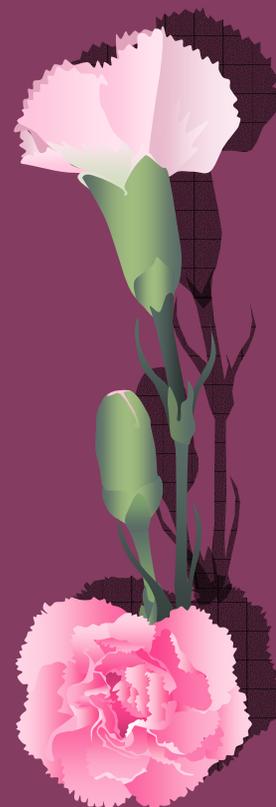
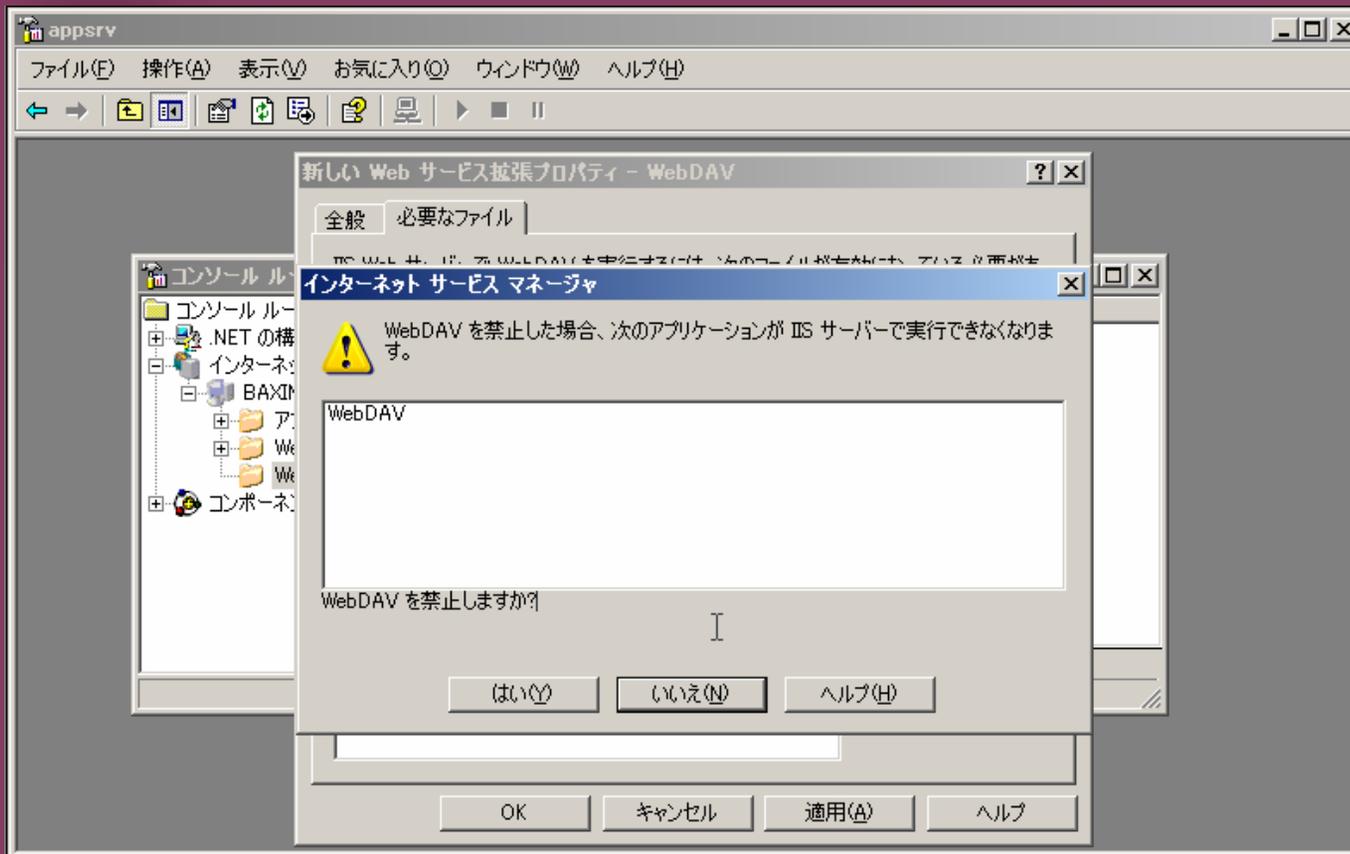
- 👉 ダイアログ一切なし
- 👉 しかもデフォルトは「OK」



IIS 6.0 を設定してみる

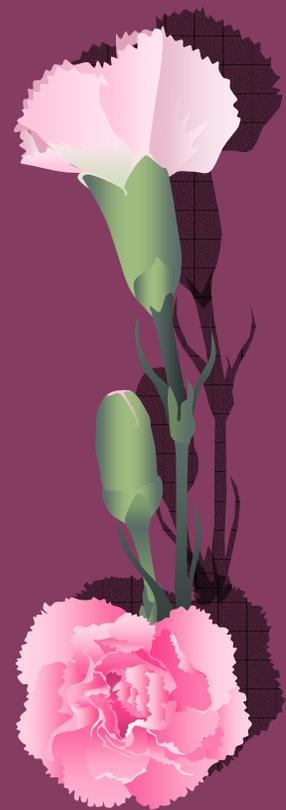
🌸 ここで「禁止」をクリックすると...

👉 こちらはダイアログが出る。おまけにデフォルトは「いいえ」



IIS 6.0 を設定してみた感想

- 🌸 どうやら、「デフォルト:機能満載」時代の操作感がまだまだ幅を利かせているようだ。
 - 👉 RC2 では直っているのかなあ



強引なまとめ

- ❁ Windows .NET Server 2003 RC1 は、Windows 2000 Server よりもデフォルトセキュリティは向上しているが、期待されたほど徹底されているわけではない。特に port 135, 137~139, 443 全開はシャレになってない。
- ❁ 利便性との兼ね合いはもちろん考慮すべきだが、「信頼できるコンピューティング」と言っている割には、あいかわらず利便性が優先されすぎている点が少なくないと思う。下手に lockdown するとサポートが大変になるという話もあるが、それは「信頼できるコンピューティング」に対する明確な否定であると思う。
利便性との兼ね合いという観点から見れば、インストール時に管理者に明確に選択させるようにすればよいだけだと私は思う。
- ❁ ICF の活用など、できることはきちんとやって頂きたい。今からでも遅くはないはずだ。「Linux ではとっくに xx なのに...」というパターンにはもう飽きた。
- ❁ もうすぐ登場する RC2 で、「なんだ直ってるじゃん」と言うことになるのを期待しつつ...



おしまい

🌸 質問ありますか？

