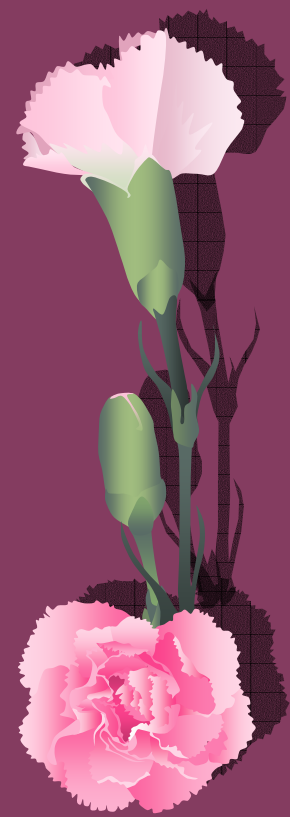
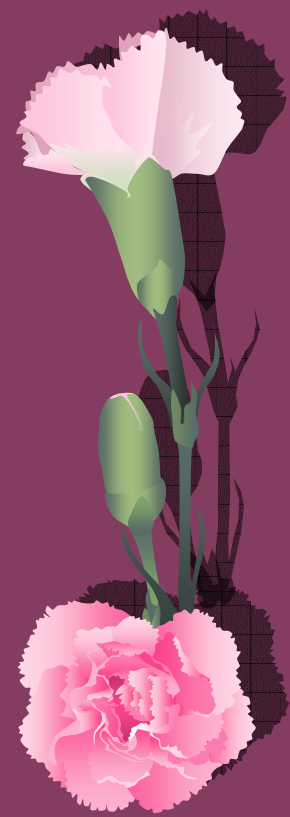
「信頼できるコンピューティング」は信頼できるか？

龍谷大学理工学部　小島肇
kjm@rins.ryukoku.ac.jp



今日のお話

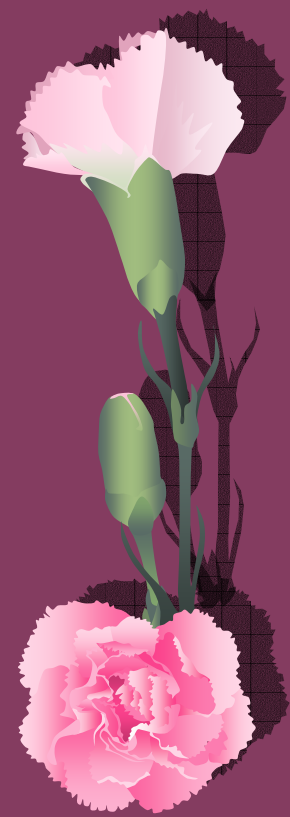
- ある一人の
- あまり Windows に詳しくない人が見た
- Windows .NET Server 2003 RC1 の
- デフォルト状態でのセキュリティ状況に関するおぼえがき



「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

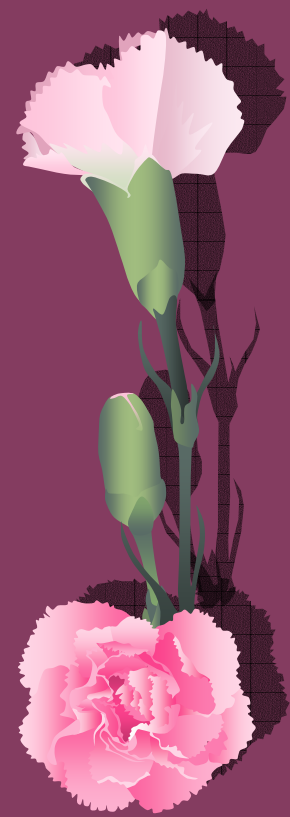
“Security and Trustworthy Computing“
http://www.microsoft.com/enterprise/articles/security.asp



Secure by default

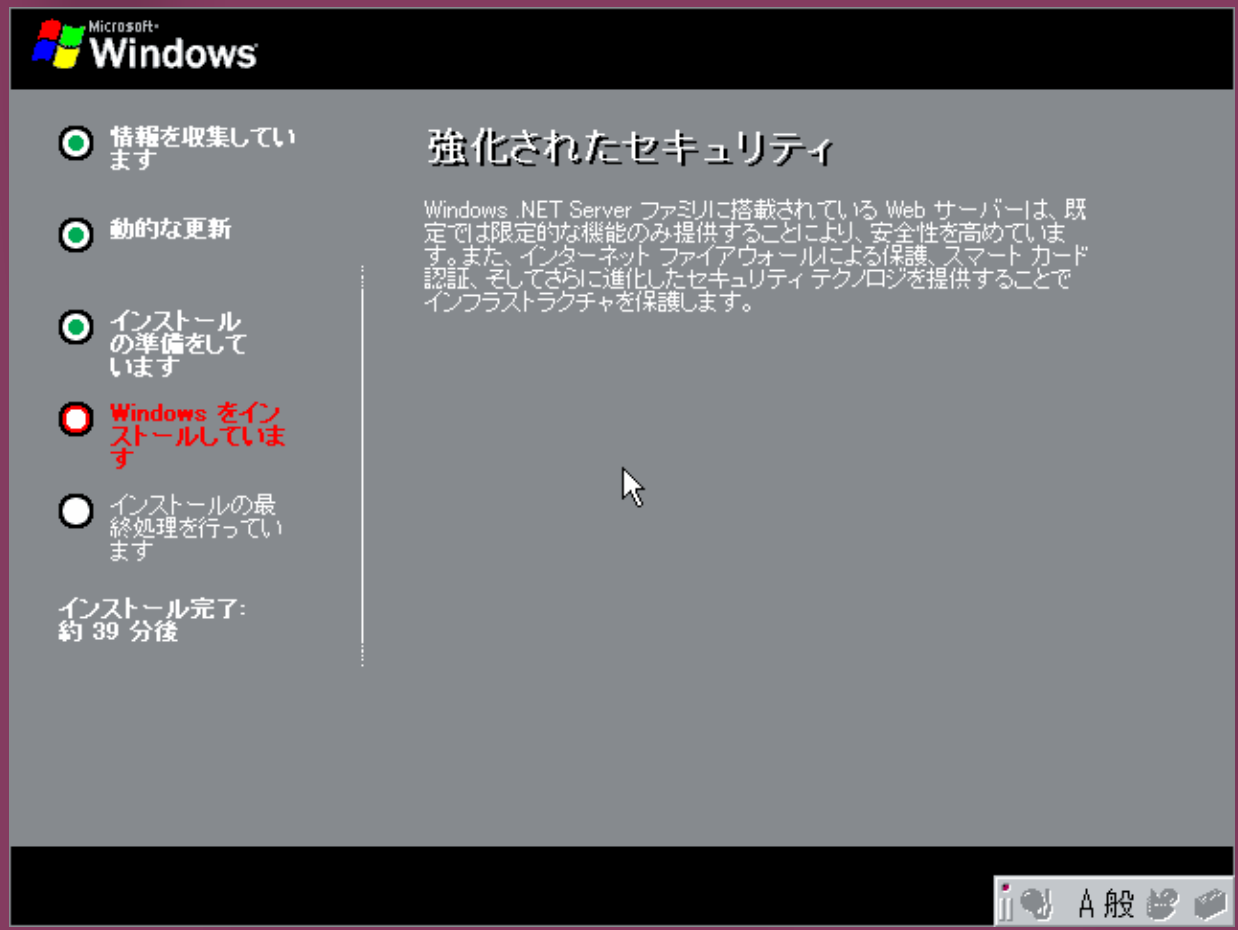
- 止められる機能はデフォルトで停止させておく。
- あらゆる状況において機能を厳重に封鎖 (lock down) する。

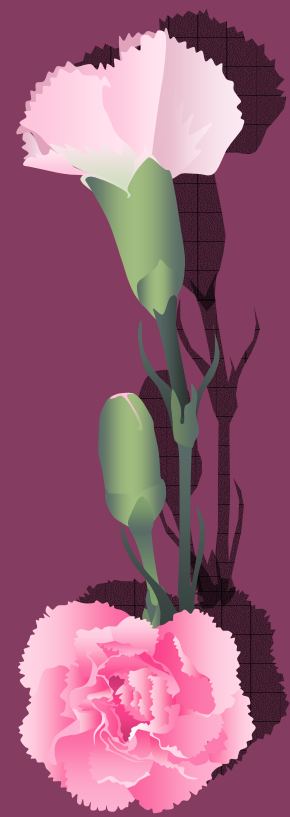
> Microsoft is making its products more secure by default, so that components begin their installed life in a secure default state—turned off where possible, and locked down in all cases.
>
> -- “Security and Trustworthy Computing“



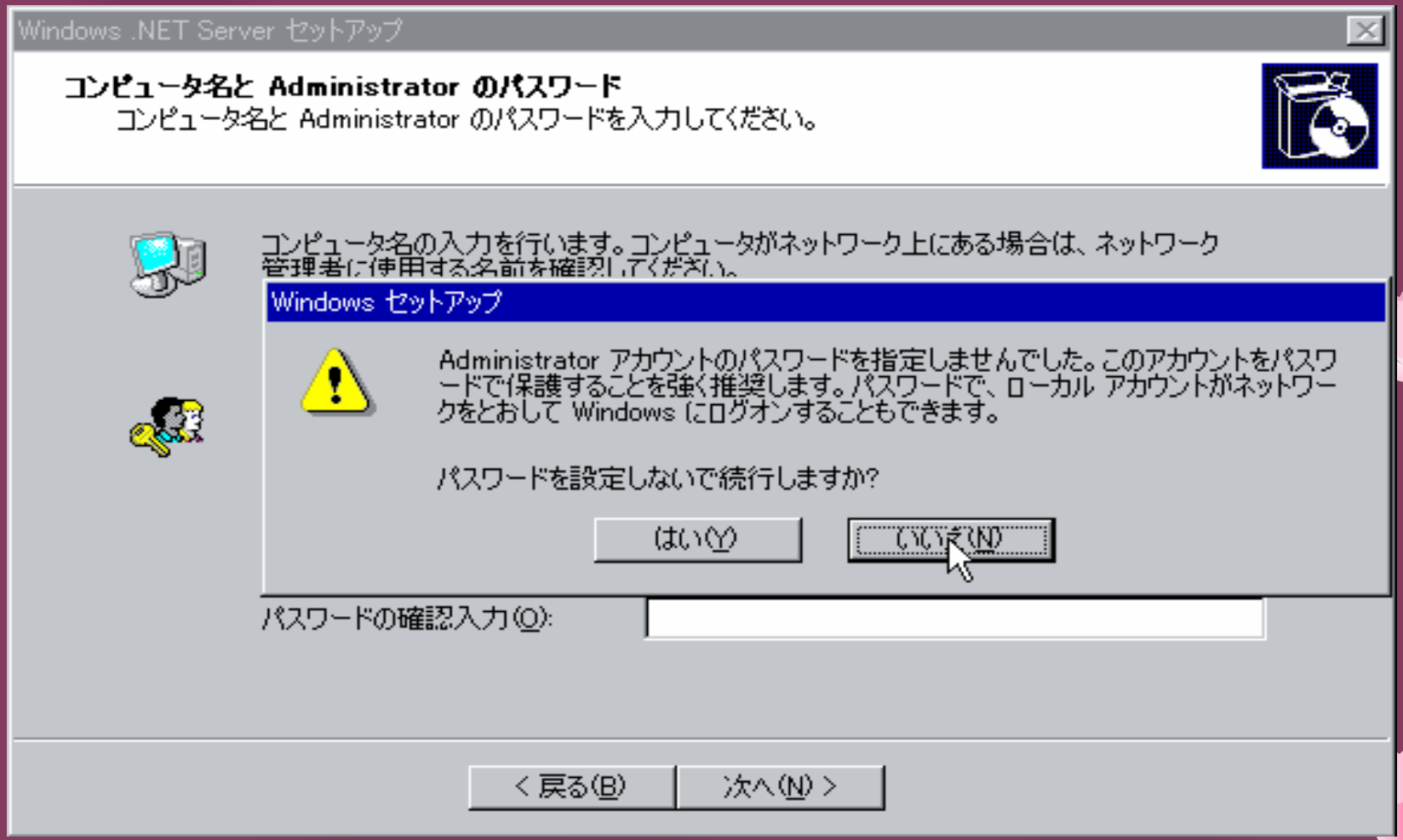
Windows .NET Server 2003 RC1 Enterprise Edition

- とりあえずインストールしてみる





インストーラ: null パスワードには文句を言う

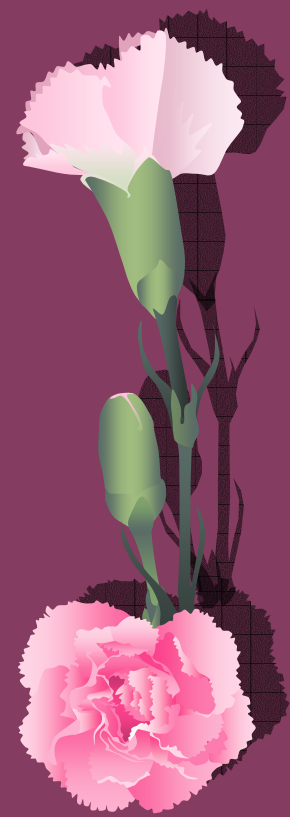


インストーラ: 不十分なパスワードにも文句を言う

インストール後 nmap してみると

- nmap -sS -O

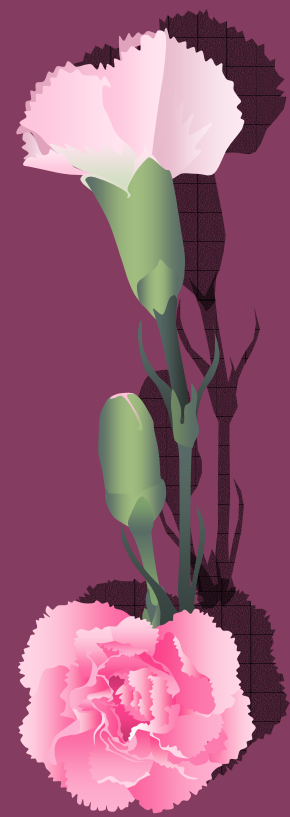
```
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on (133.83.XXX.XXX):
(The 1597 ports scanned but not shown below are in state: closed)
Port State Service
135/tcp open loc-srv
139/tcp open netbios-ssn
445/tcp open microsoft-ds
1025/tcp open NFS-or-IIS
Remote operating system guess: Microsoft Windows.NET Enterprise
Server (build 36 04-3615 beta)
```



インストール後 nmap してみると

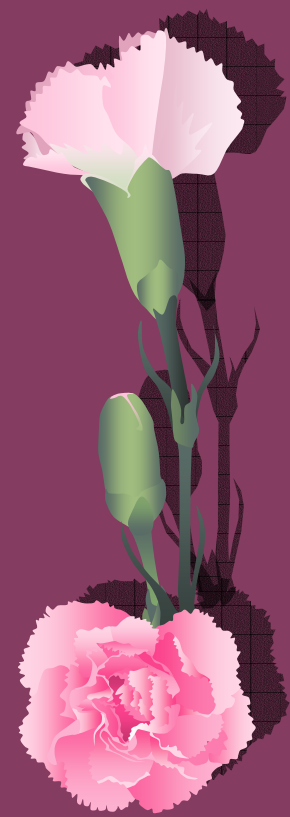
- nmap -sU -O

```
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Warning: OS detection will be MUCH less reliable because we did not
find at lea st 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 Ma nagement 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)
```



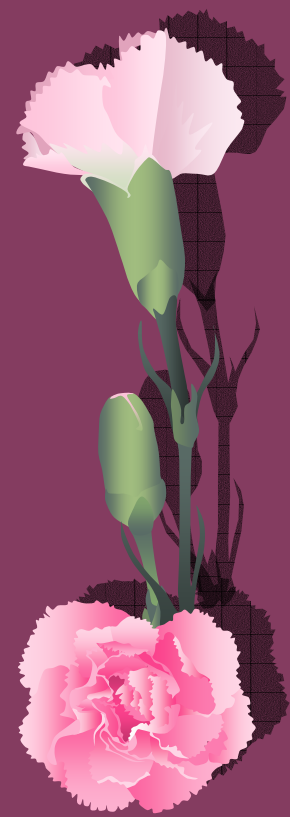
これは何?

- 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ーじゃん

- 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…

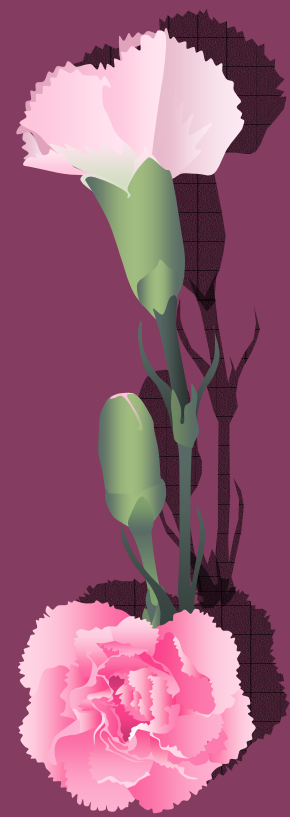


ICF を有効にすると…

- 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 lea st 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
```

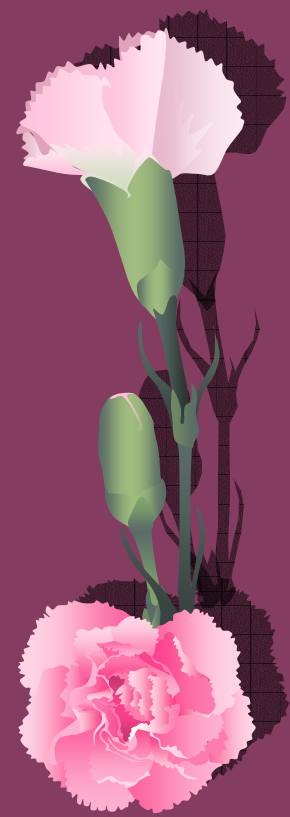


ICF を有効にすると…

- nmap -sU –O

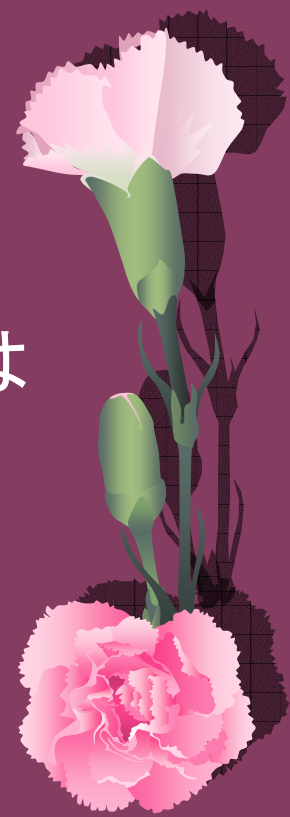
「Web サーバー」「リモートデスクトップ」にチェックを入れた場合（ここでは IIS やリモートデスクトップは起動させていない）

```
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Warning: OS detection will be MUCH less reliable because we did not
find at lea st 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
```



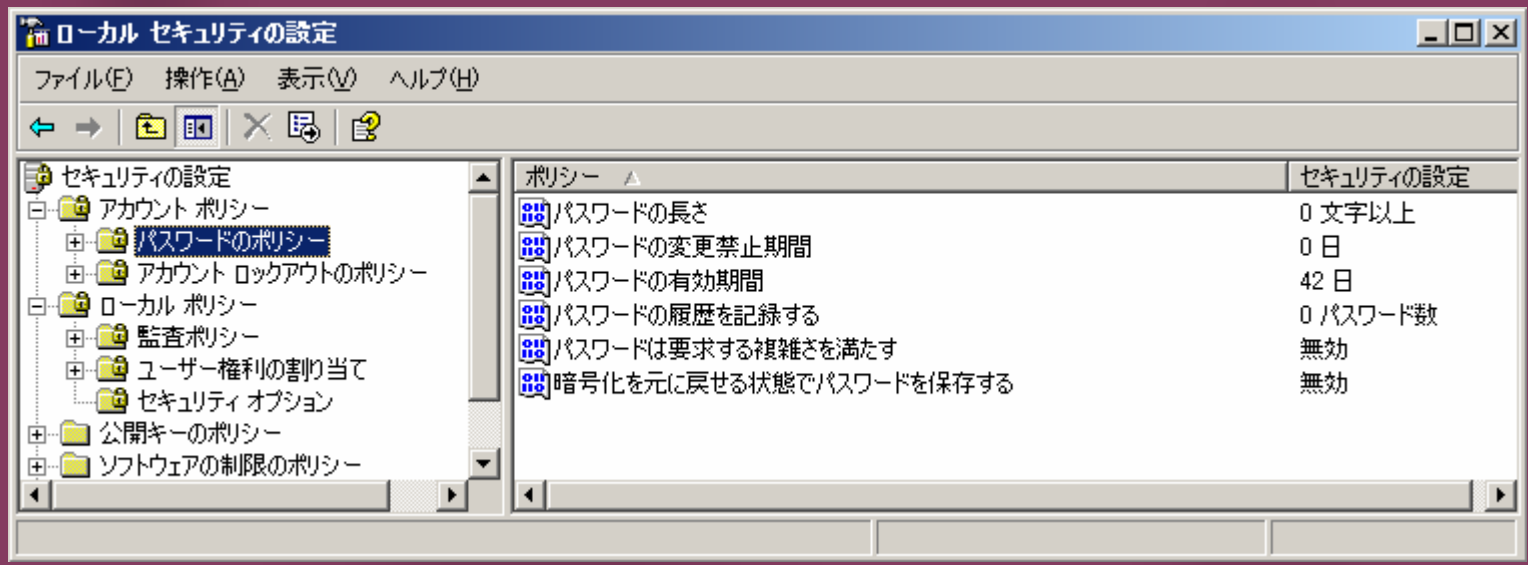
ICF はいいことばっかりですか?

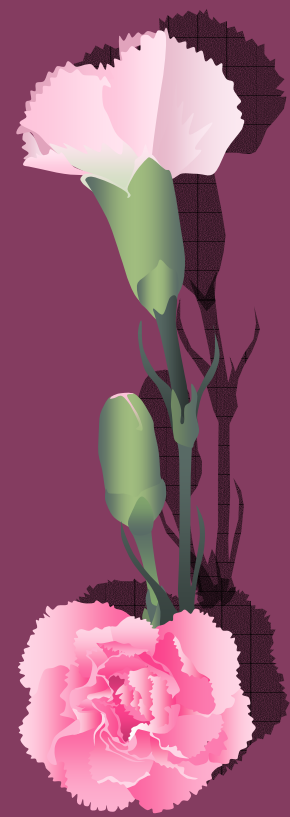
- イントラネットでは混乱が発生するかもしれません。なので「選択させる」がよいと思うのです。
  - 事例: [samba-jp:13876] Master Browser をまた、奪われてしまいました。から続くスレッド
    http://www.samba.gr.jp/ml/samba-jp/htdocs/200211.month/13876.html
- Active Directory をはじめとする、まともなディレクトリサービスが整った環境では、こういう苦労はしなくてすむはずなのですが。
  - 「だから AD にしよう!」みたいな話は意外なほど聞かない気がするのはなぜ?



ローカルセキュリティポリシー (1)

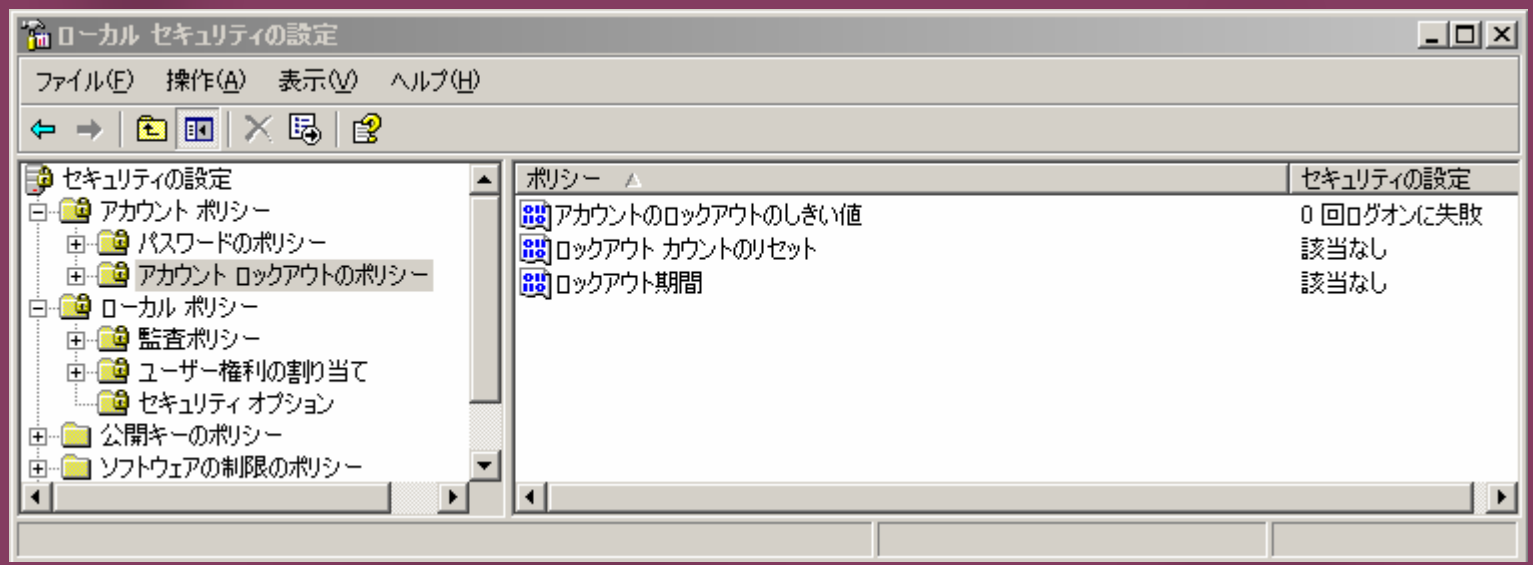
- パスワードポリシー: Windows 2000 と同じ…。
  - せめて「パスワードの長さ」はなんとかならないのか…





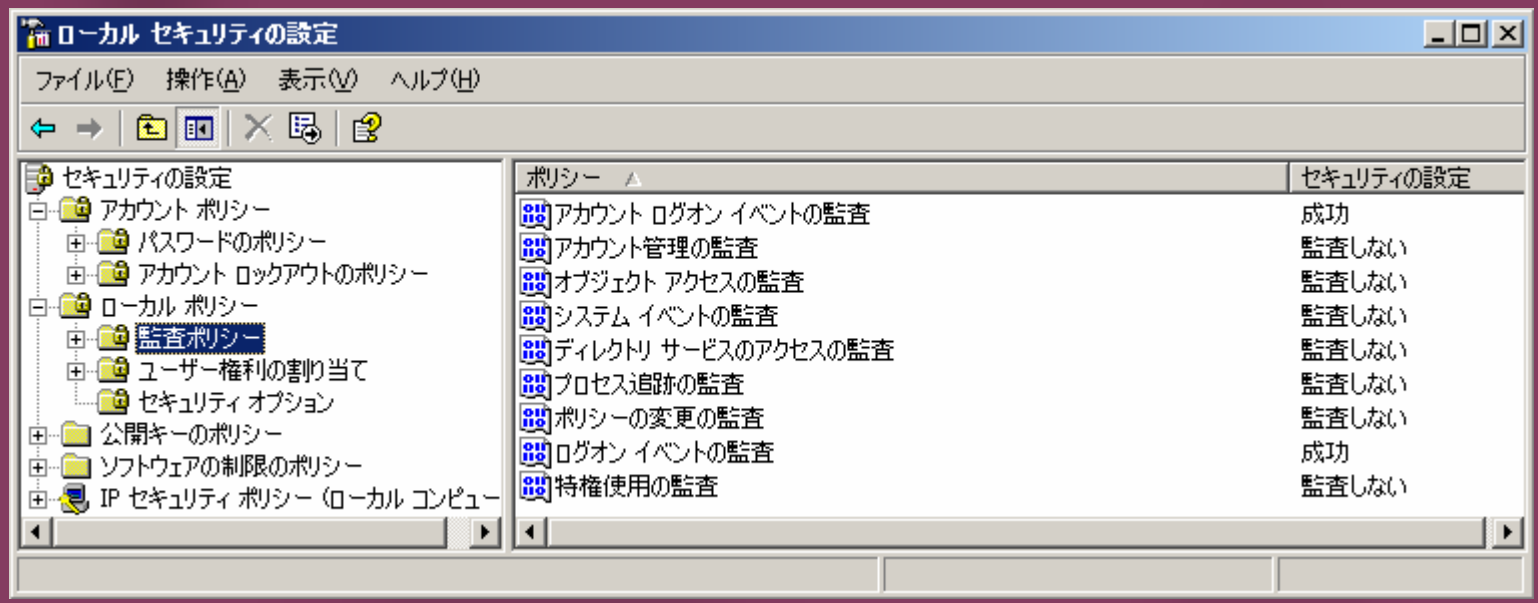
ローカルセキュリティポリシー (2)

- パスワードロックアウトポリシー: Windows 2000 と同じ…。



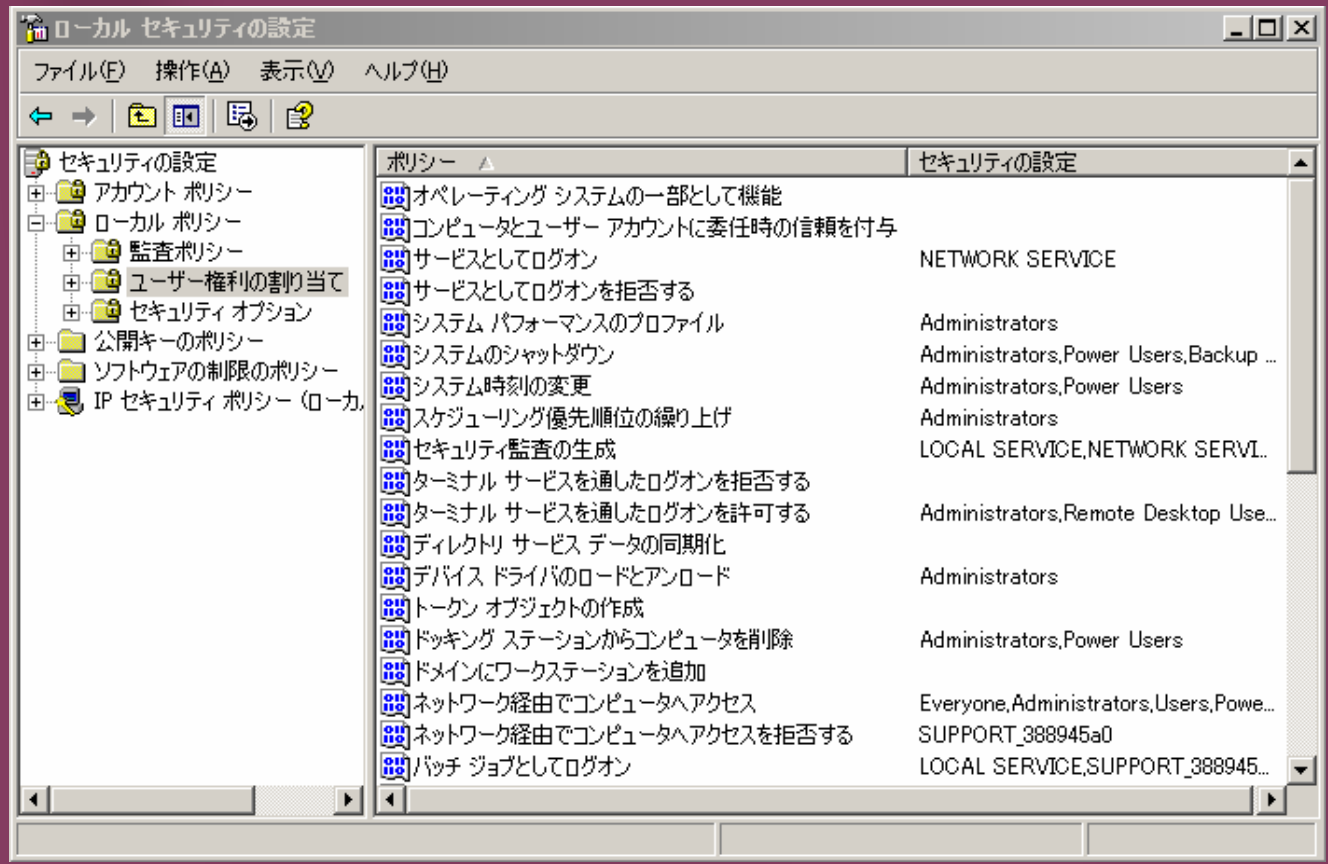
ローカルセキュリティポリシー (3)

- 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…



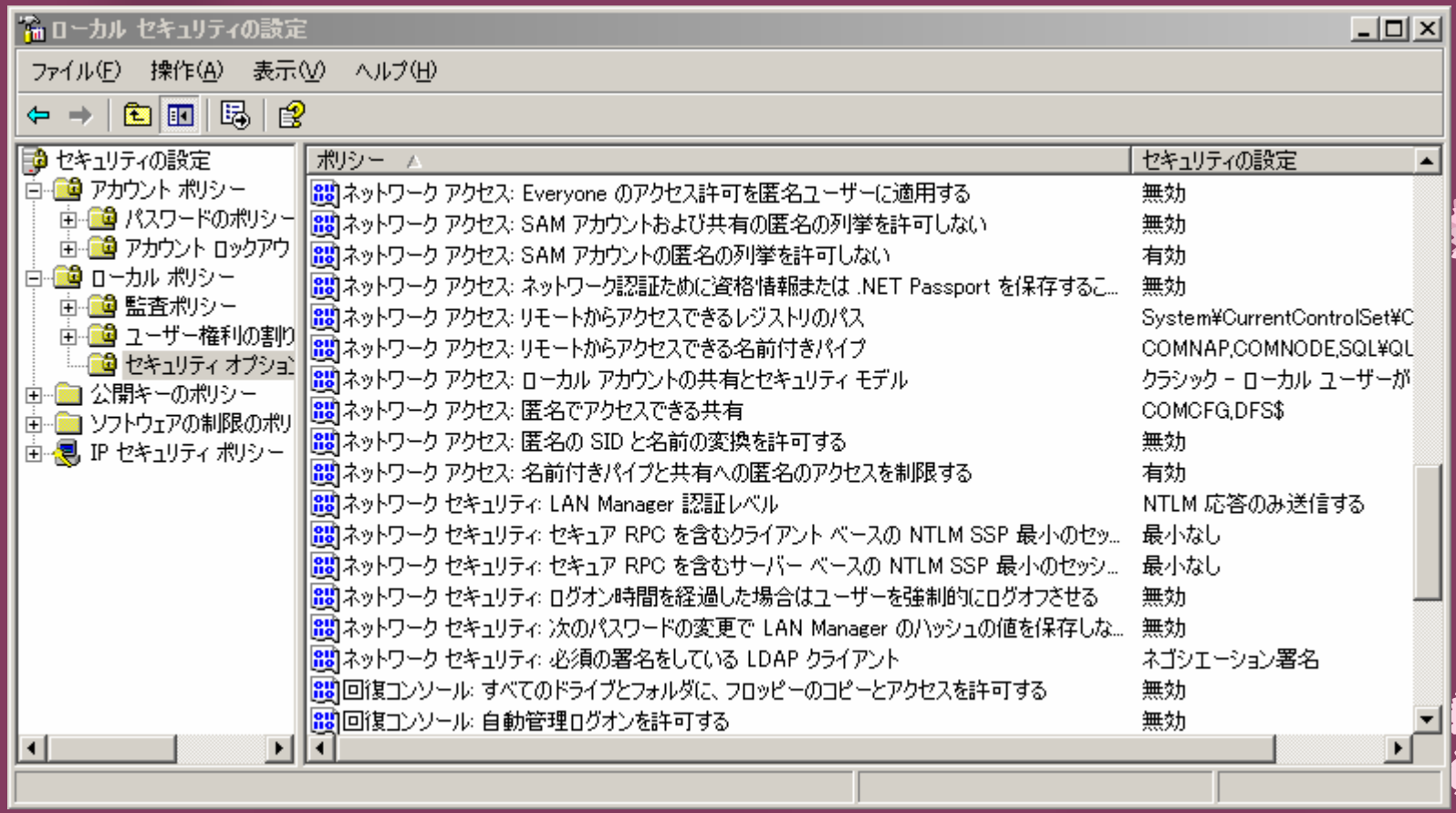
ローカルセキュリティポリシー (4)

- 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

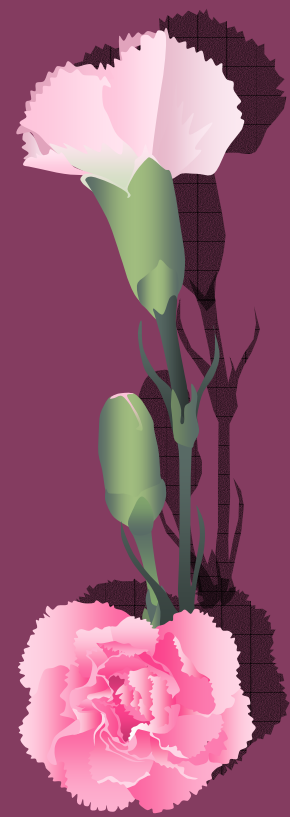


null 接続に対する反応の違い

- 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.
```

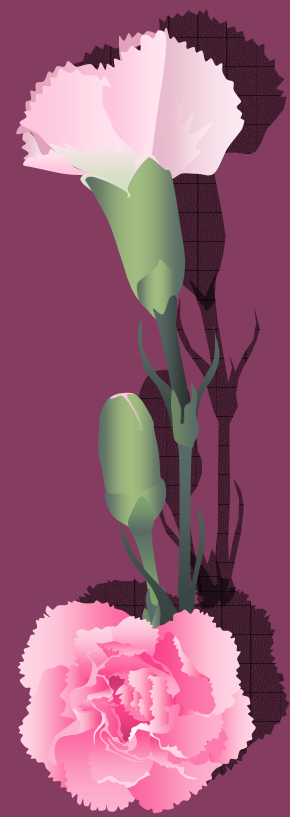


null 接続に対する反応の違い

- 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.
```

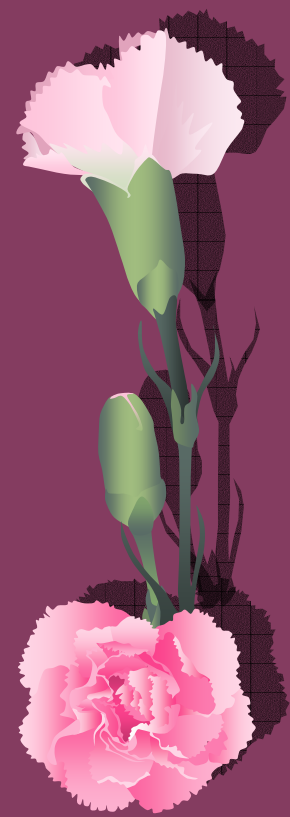


null 接続に対する反応の違い

- 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
```



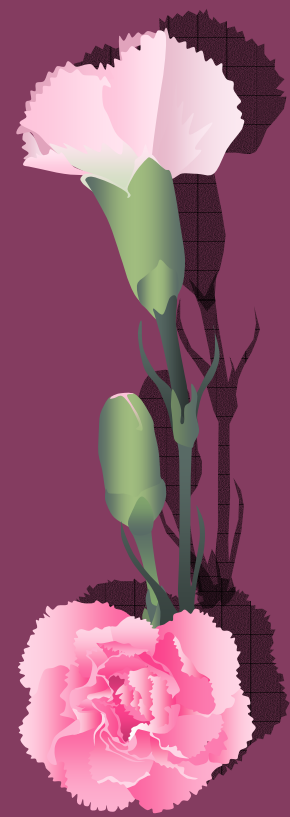
null 接続に対する反応の違い

- enum –S: get sharelist

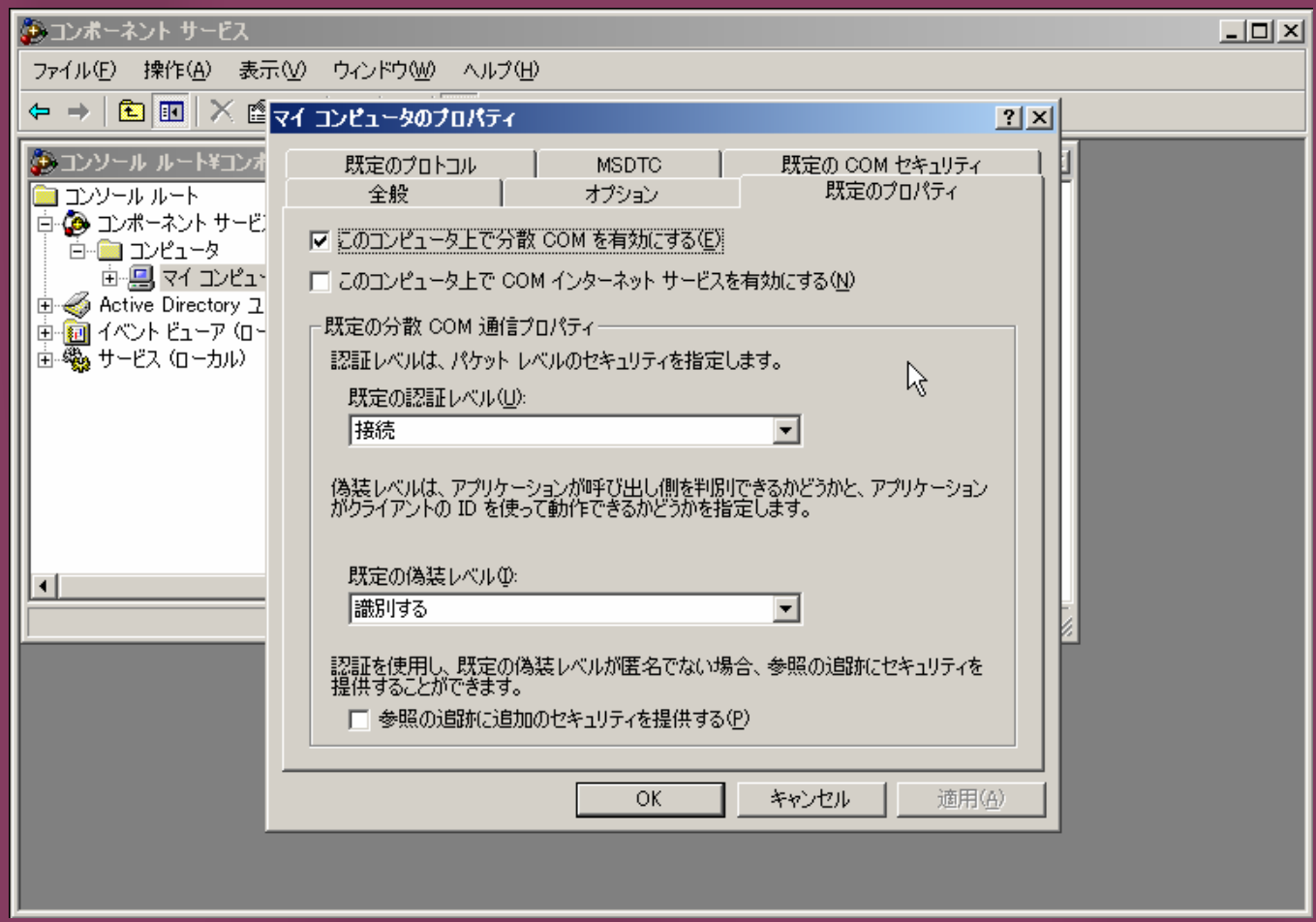
```
C:¥>enum -S 133.83.XXX.XXX
server: 133.83.XXX.XXX
setting up session... success.
enumerating shares (pass 1)... got 3 shares, 0 left:
  IPC$  ADMIN$  C$
cleaning up... success.

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

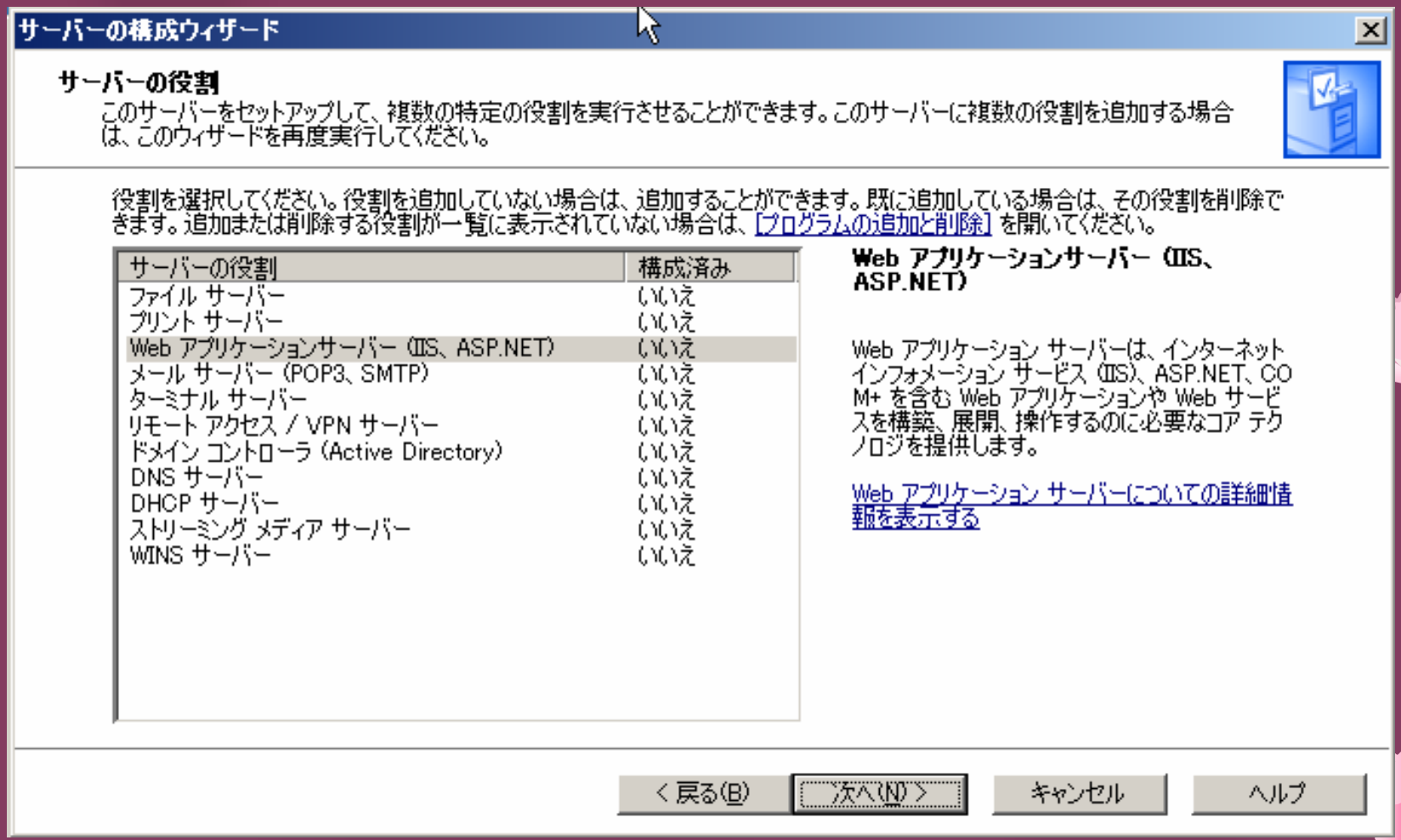


DCOM – もちろん有効

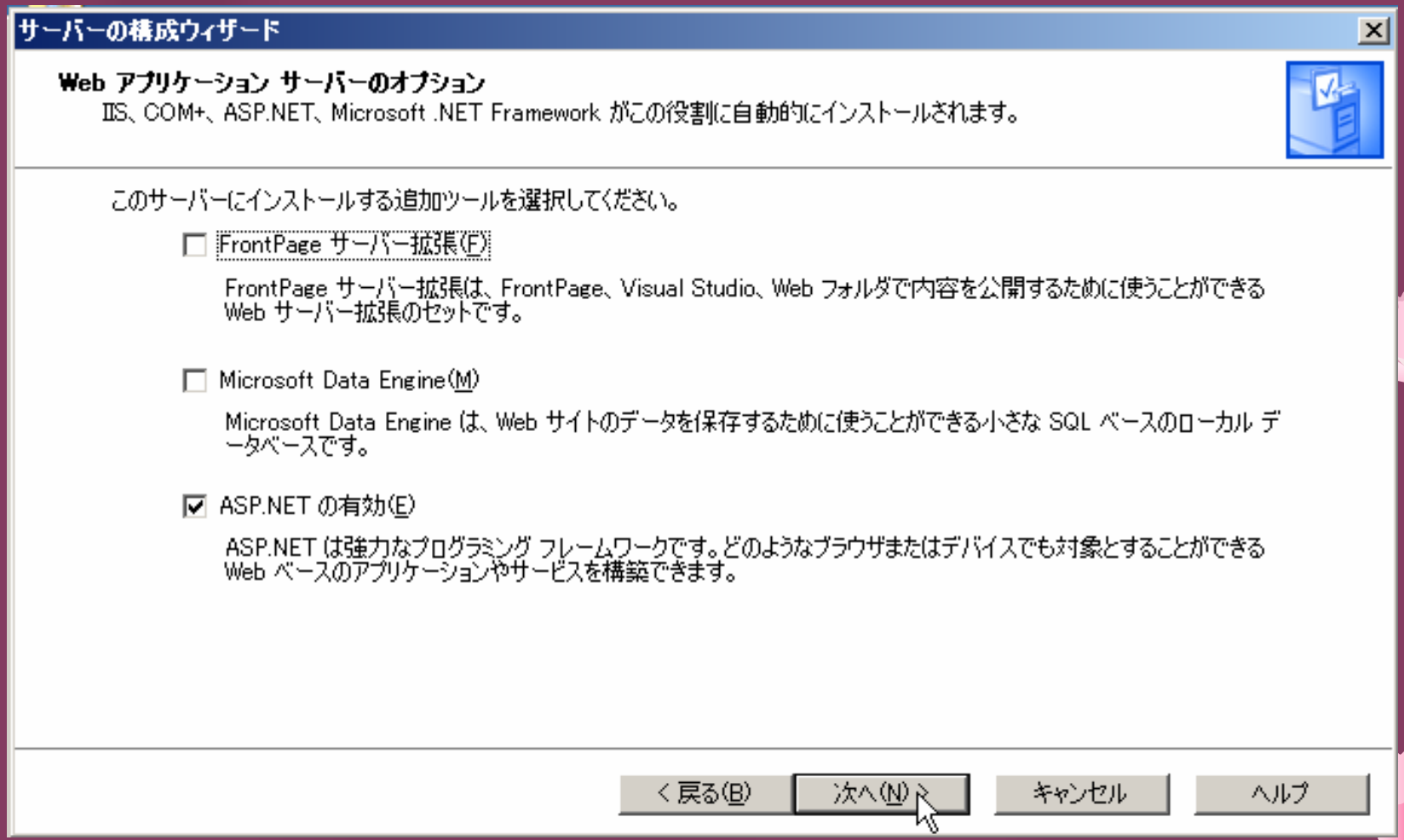


IE’en (remotely controls Internet Explorer using DCOM) で遊ぼう!?
http://www.securityfriday.com/ToolDownload/IEen/ieen_doc.html

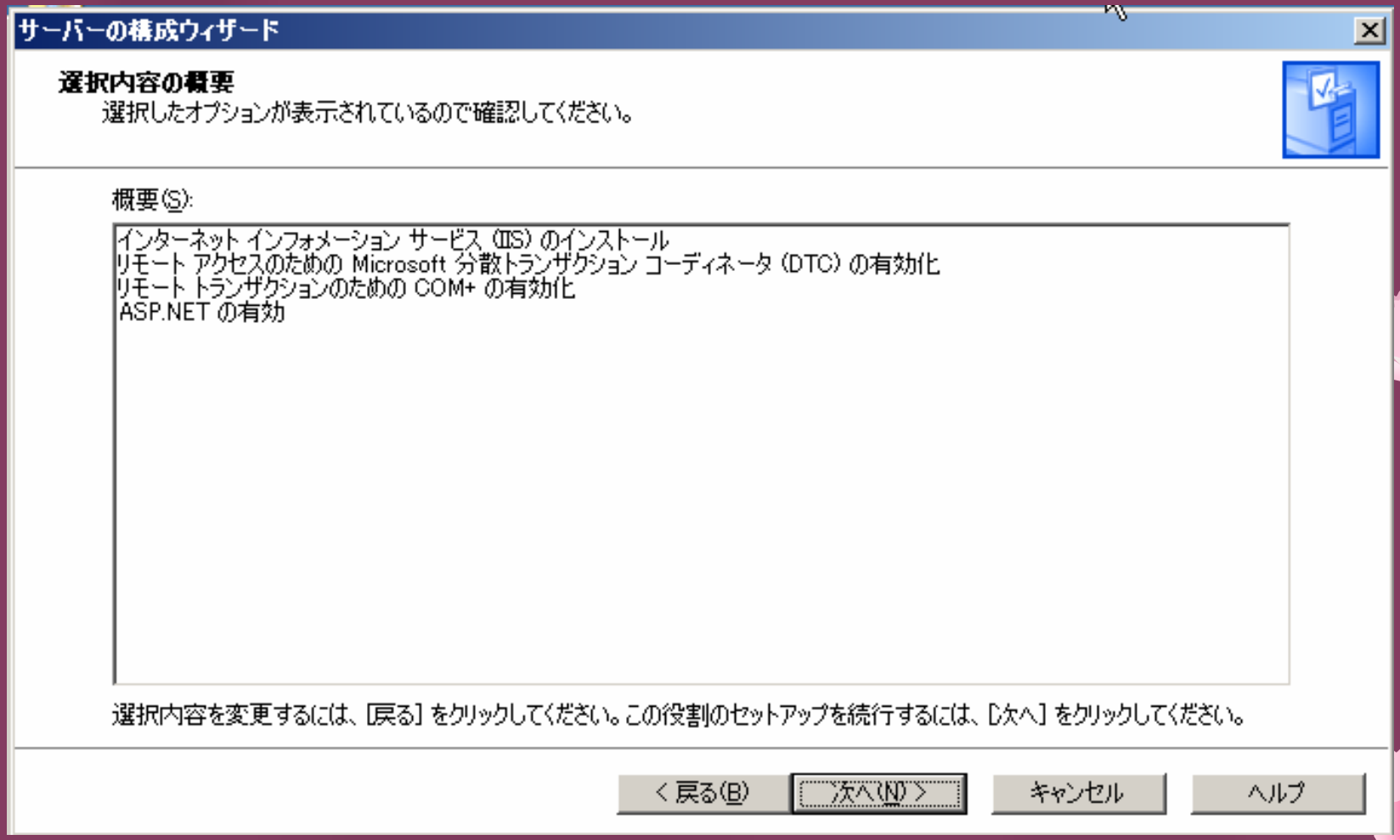
IIS 6.0 をインストールしてみる



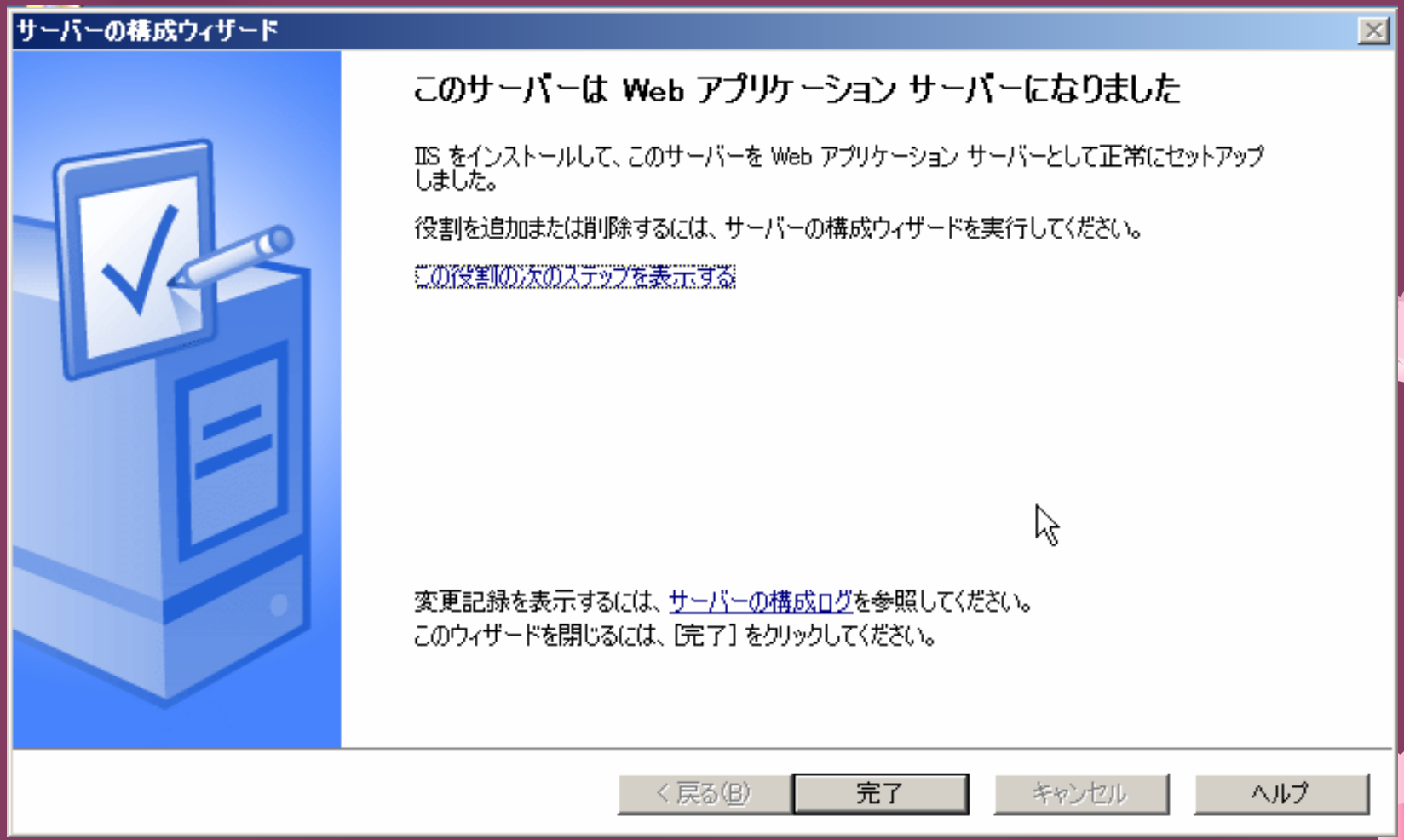
IIS 6.0 をインストールしてみる



IIS 6.0 をインストールしてみる

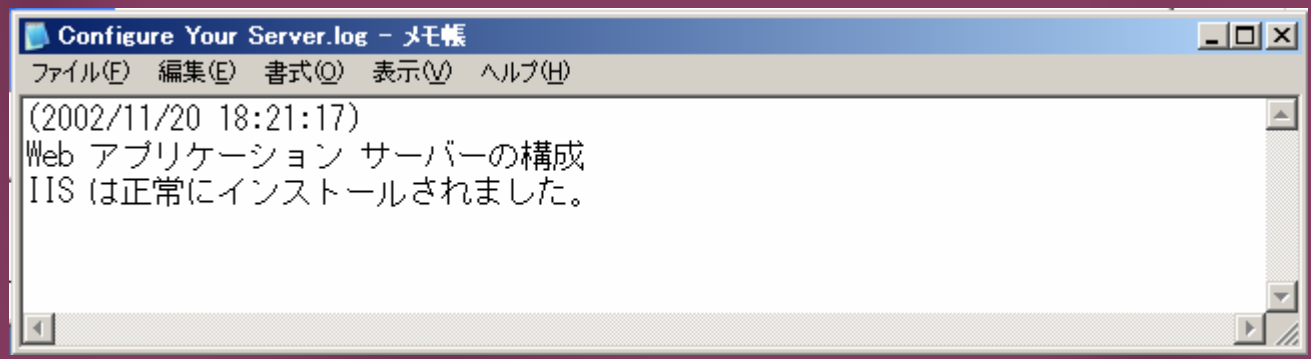


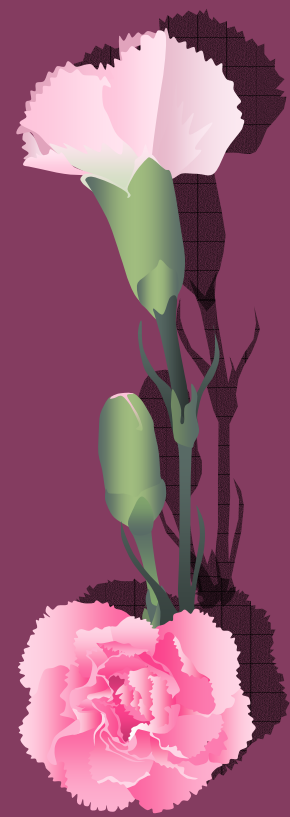
IIS 6.0 をインストールしてみる



IIS 6.0 をインストールしてみる

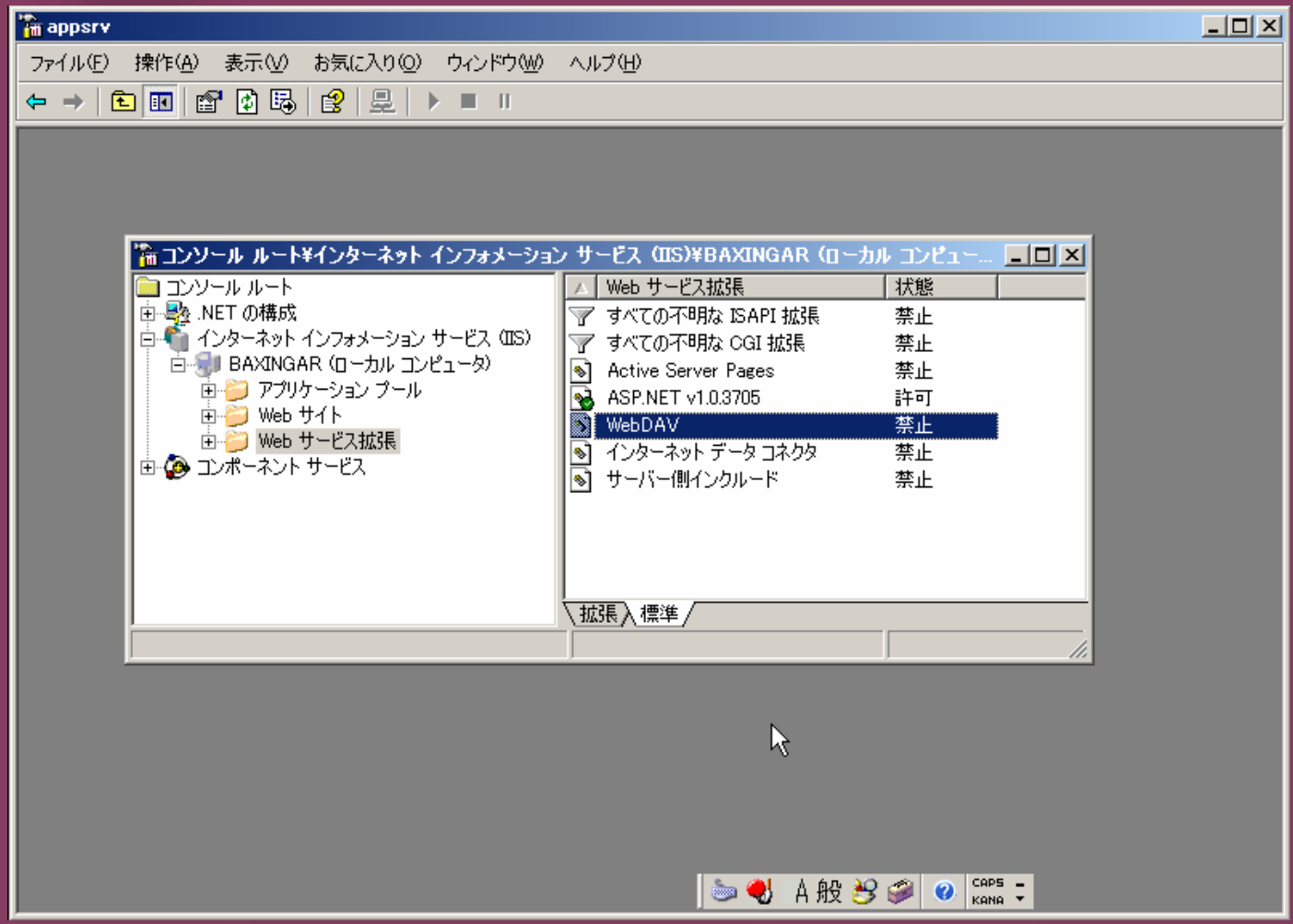
- サーバーの構成ログ
  - もうちょっとなんとかならんのか (^^;;;)





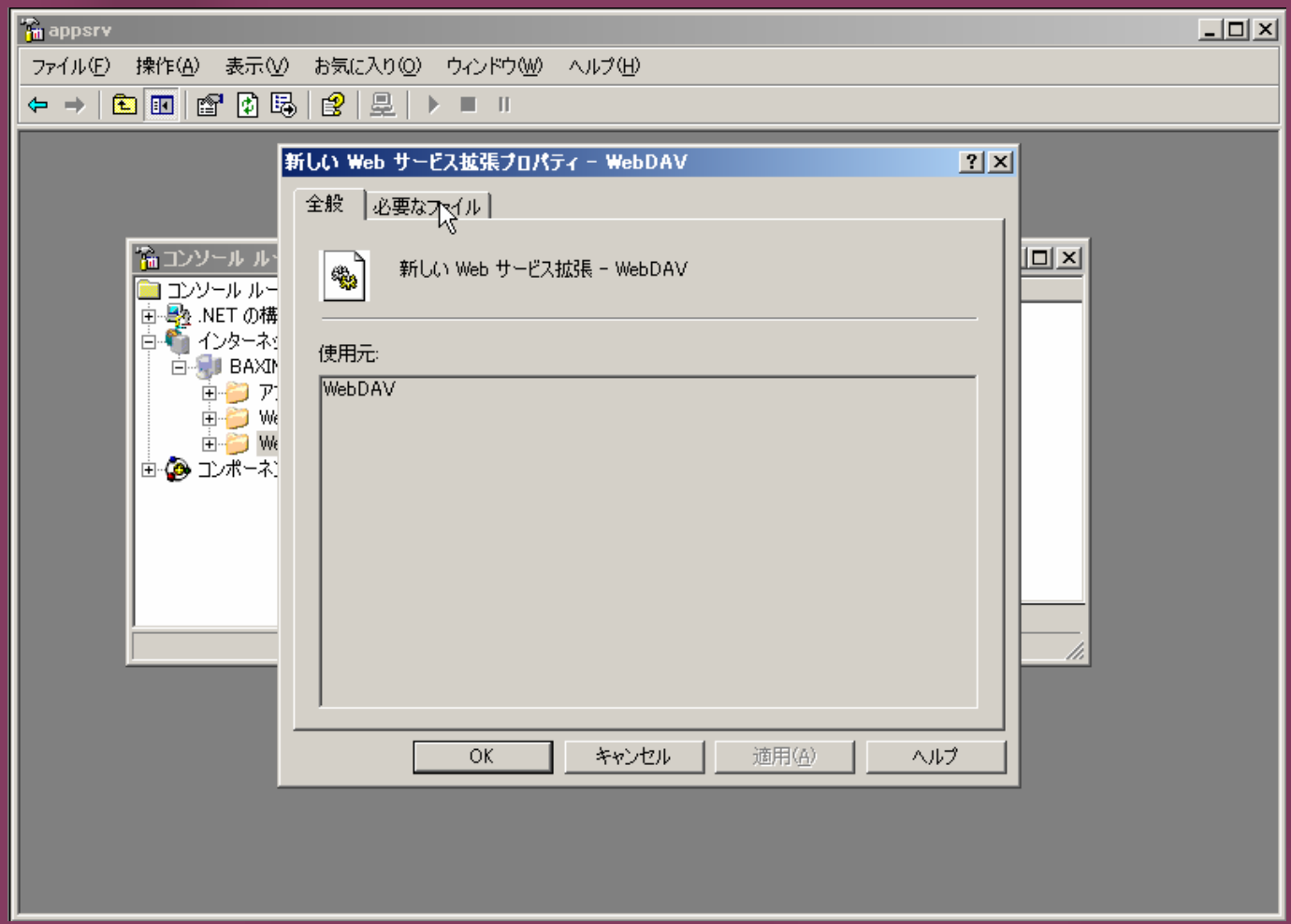
IIS 6.0 を設定してみる

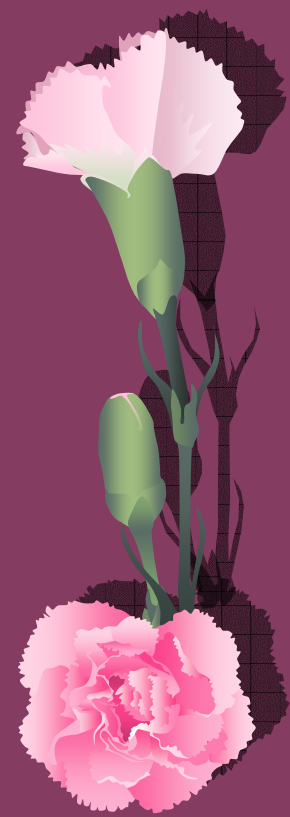
- 上記のようにインストールした場合の状態



IIS 6.0 を設定してみる

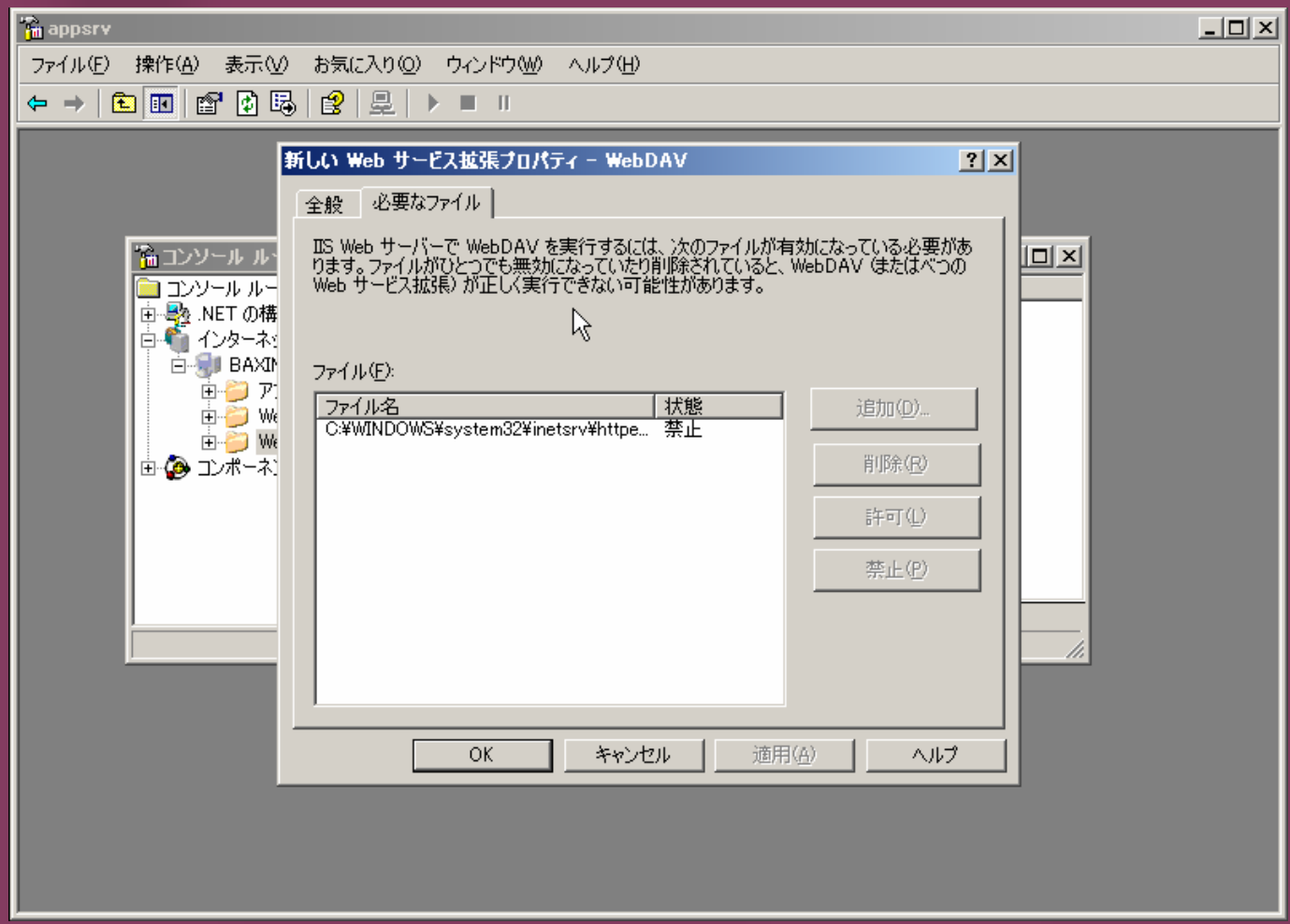
- ダブルクリックしてみる

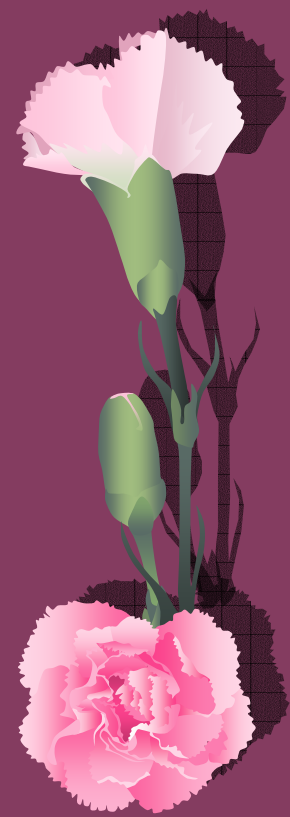




IIS 6.0 を設定してみる

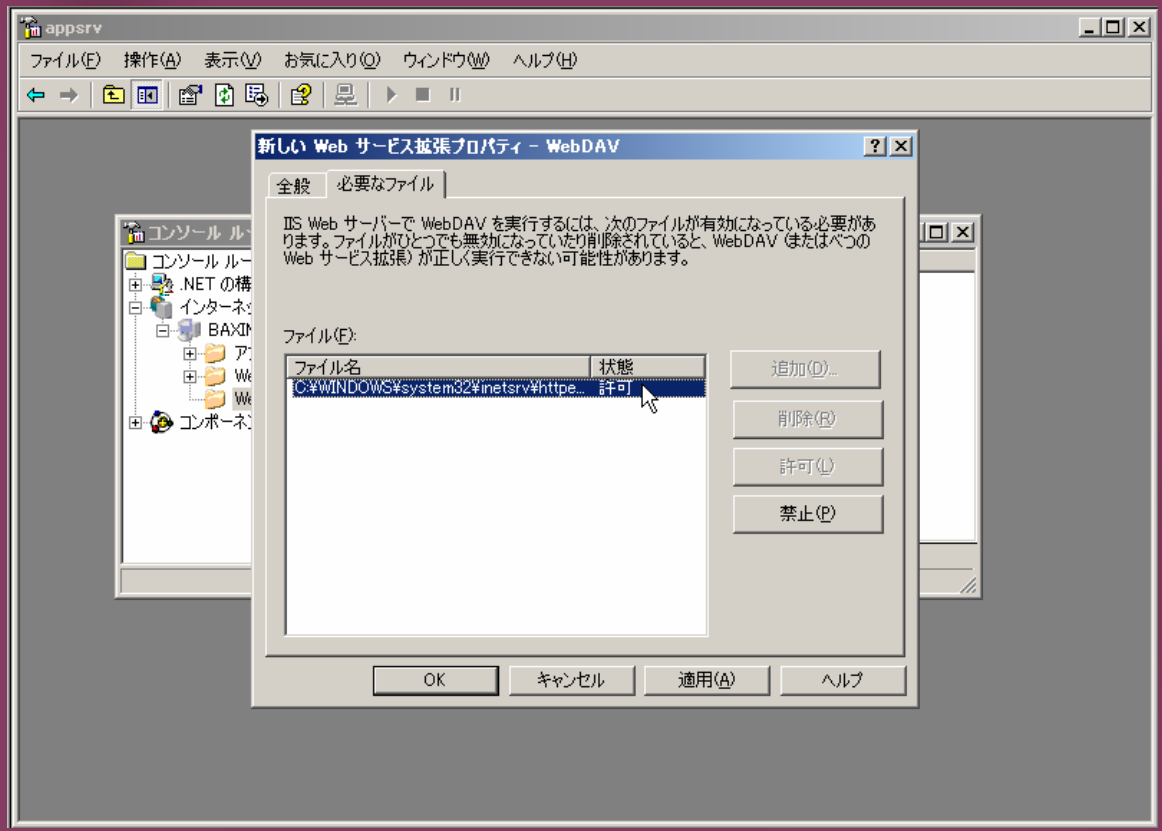
- 「必要なファイル」タブ





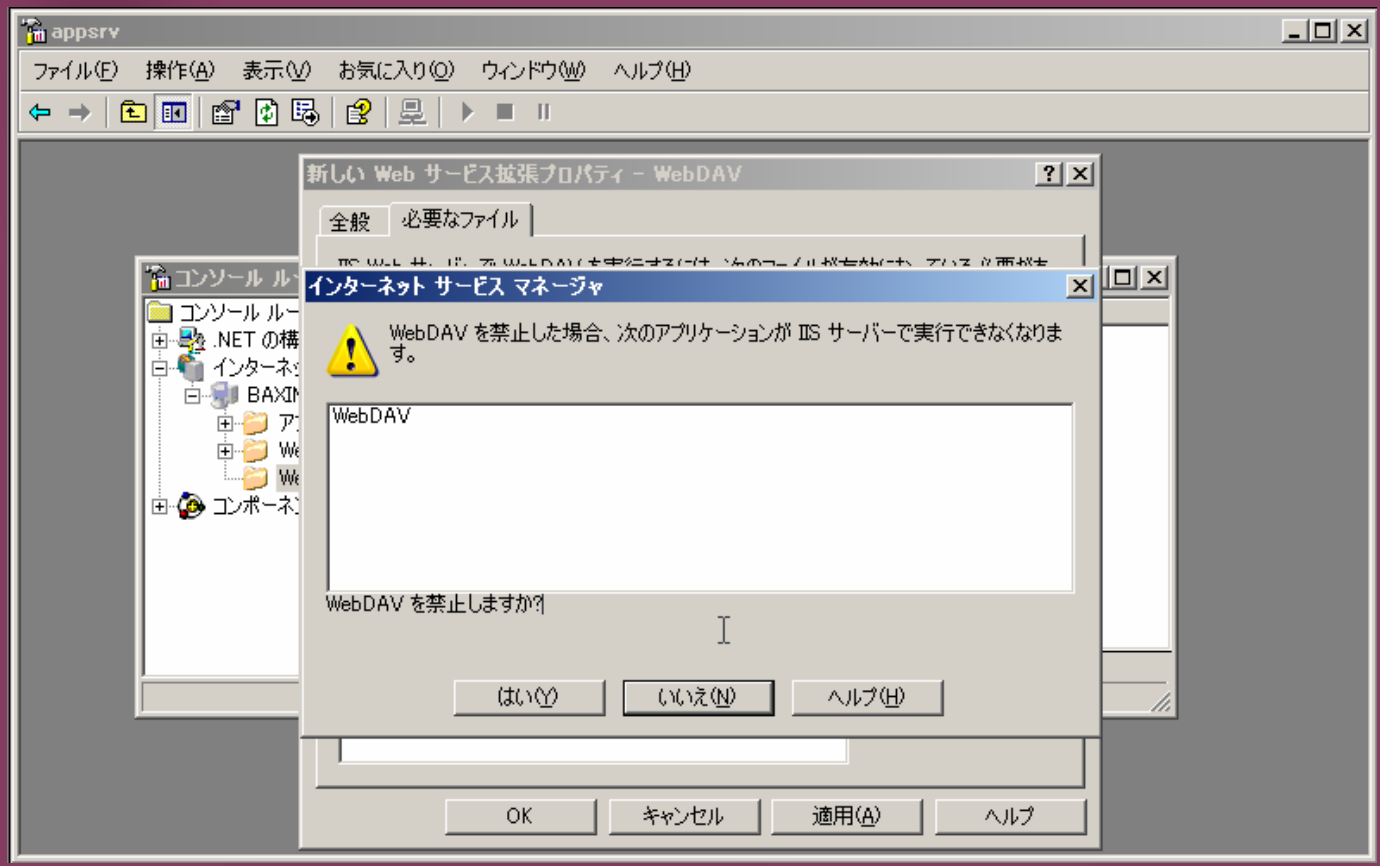
IIS 6.0 を設定してみる

- ファイル名をダブルクリックすると、いきなり「有効」に
  - ダイアログー切なし
  - しかもデフォルトは「OK」



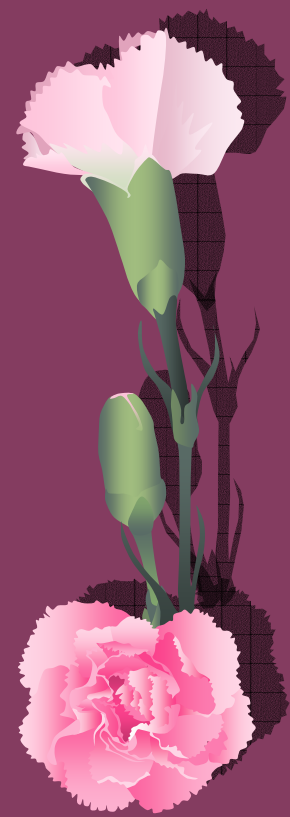
IIS 6.0 を設定してみる

- 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」



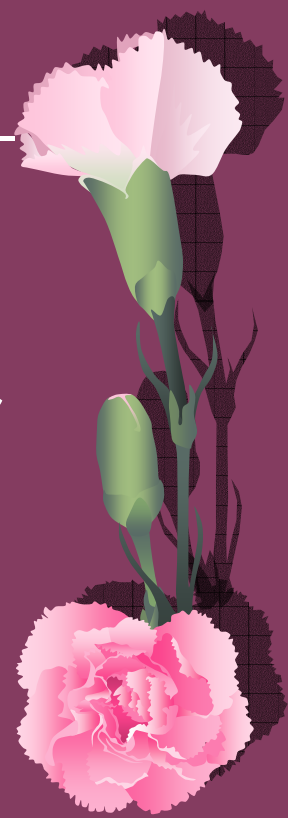
IIS 6.0 を設定してみた感想

- 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ように思う。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?