[Windows20000]パソコンのセキュリティを高めよう

(2002年1月～5月掲載)

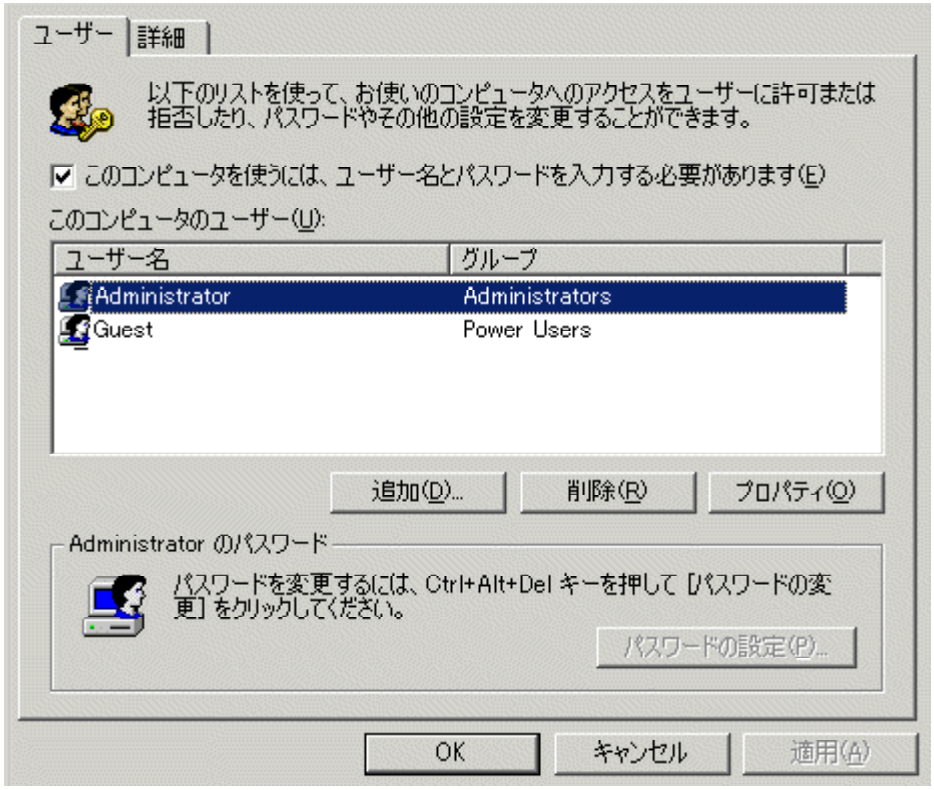
このコンテンツは、個人が自宅で利用しているパソコンを対象にしています。
システム管理者やネットワーク管理者がいる場合はその指示にしたがってください。
WindowsXP も発売されて、販売されているパソコンの大部分が、WindowsXP か Me になっていますが、Windows20000 の話題です。
わたしが、WindowsXP を利用してないだけなんですけどね。(^_^;)
今回の内容は、Windows20000 が対象ですが、WindowsXP でも参考になる部分があれば幸いです。
え～っと、今回の話題は、b-mobile に加入したのもあり、インターネット常時接続環境が簡単に利用できるようになったので、自分の使っている PC の確認もかねて書いています。
内容ですが、１．お金をかけない　２．なるべく簡単な操作でできることを目標にしています。
といっても、管理ツールなどを使うので超初心者には難しいかもしれません。
自分のパソコンを守るだけでなく、パソコンを踏み台にされて人に迷惑をかける原因をつくらないためにもセキュリティをしっかりしたいものです。

内容一覧

１．Administratorの名称変更とパスワードを長文化しよう

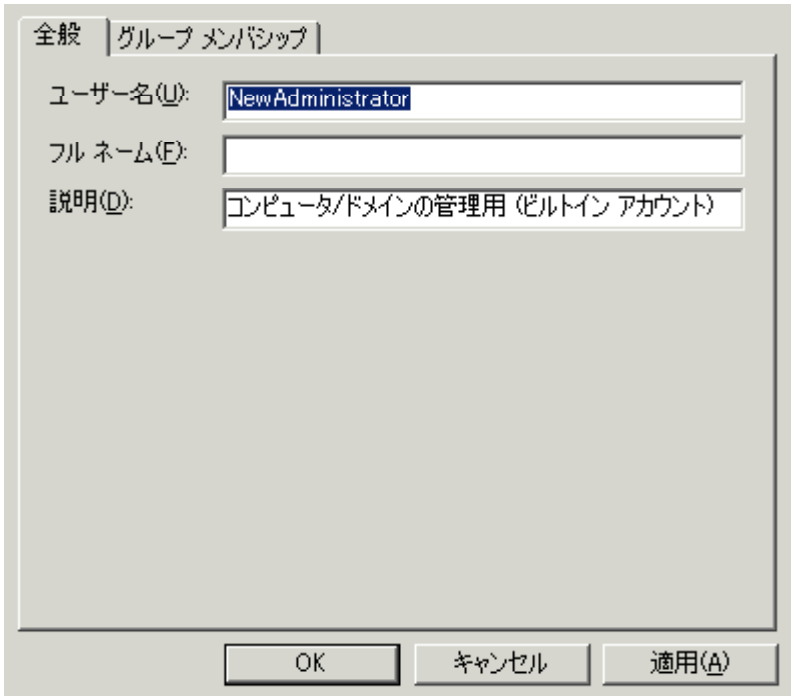
Windows20000 を初めて使うときに、Administrator のパスワードを設定したと思います。
Administrator ってなんだろう？と思った人も多いはずです。
面倒だから、パスワードなんて覚えられないといって、Enter（return）キーだけ押して、パスワードは空白ということもあるかもしれません。
また初期状態でユーザー名が Administrator となっているのでそのままの場合ということもあるとおもいます。
Administrator というのは、Windows を操作する最大の権限をもっています。
Windows20000 では、一台のパソコンに複数のユーザーを作ると、それぞれ他人のファイルを読み書きすることができないようになっています。
Administrator として操作すると、すべてのファイルを読み書きできますし、ユーザーのパスワードも変更することが可能になります。
外部からの侵入では、Administrator に対してパスワードを破ろうとしてくることがあります。（Administrator としてアクセスできれば、操作は思いのまま）
まず、ユーザー名を変更することで、ユーザー名を Administrator と前提としたパスワード破りを防ぐことができます。これは、Administrator というユーザー名を変更しない場合が多分にあるためです。
ユーザー名は、かな漢字を利用したものにすると、英数字を利用したものに比べ、ユーザー名が特定しにくくなります。
そして、**パスワードは英数字ですが、大・小文字を区別するので、大・小文字組み合わせたもの**にしましょう。そして、パスワードは、長文にしましょう。
またできることなら**ロックアウト機能を有効**にするためにも、新規ユーザーを作成しそのユーザーを利用して通常利用するようにすると良いでしょう。（ちょっと補足で説明）
操作方法（ユーザー名の変更）

スタート　→　設定「コントロールパネル」　→　ユーザーとパスワード



Administrator を選んで、プロパティを選びます。

ここで、「このコンピュータを使うには、ユーザー名とパスワードを入力する必要があります」のチェックを必ずつけてください。チェックをしていないとパスワード入力が自動化して、自動ログオンしてしまいます。



ユーザー名に新しいユーザー名を入力します。画面では NewAdministrator となっています。（入力した、ユーザー名を忘れないようにしてください）

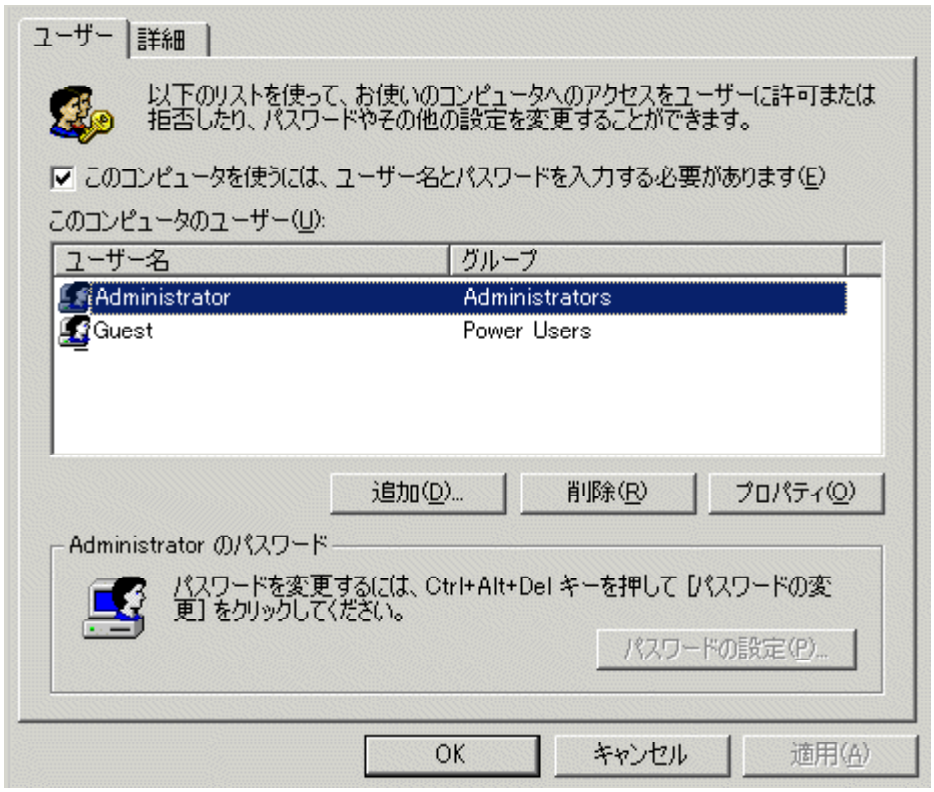
操作方法（パスワードの変更方法）

ユーザーとパスワードの画面にもあるように、「Ctrl+Alt ＋ Del」キーを押すことで Windows のセキュリティという画面が現れます。

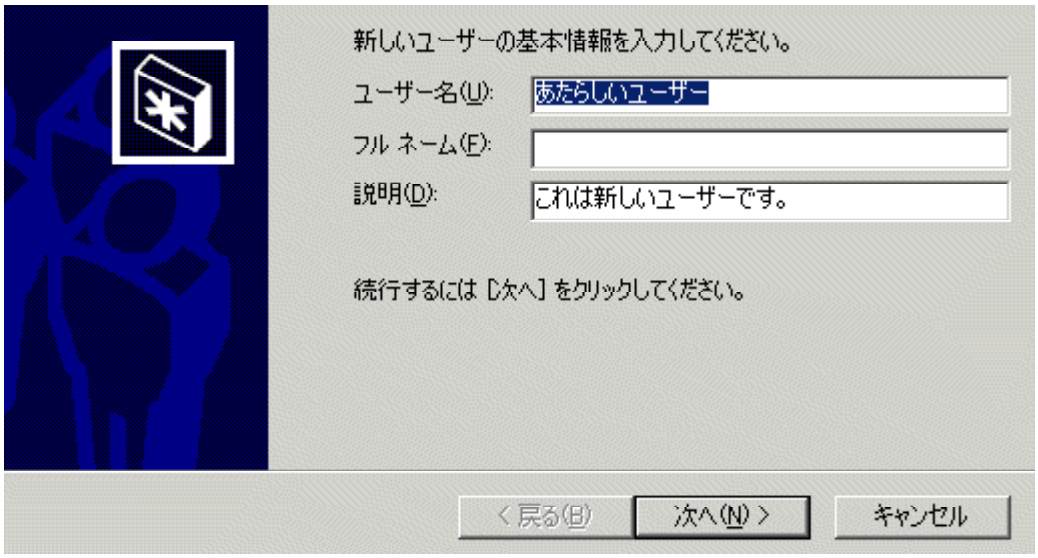
このなかの、パスワードの変更を選んで、今使っているパスワード、新しいパスワードを２回入力してください。

ちょっと補足

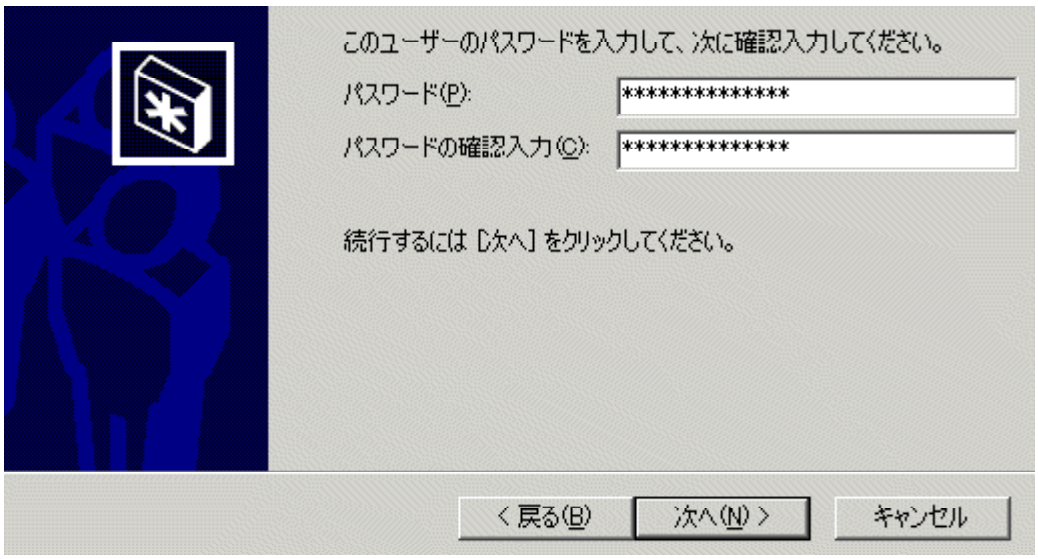
Administrator ですが、ビルドインアカウント（初期設定の Administrator のこと）は削除することができません。また、ユーザーを追加した場合に、「ユーザーに許可するアクセス権を設定してください」という項目があります。
ここで「その他から Administrator」を選んだ場合は、Administrators グループに所属することになります。この Administrator と Administrators グループの違いですが、１．回復コンソール（修復ツール）操作、２．EFS（EncryptingFileSystem）回復エージェントの操作、３．ディレクトリサービス復元モードへのログオンが Administrator グループではできないということです。
まあ、Windows 起動時に F8 を押すことで現れるメニューだったりで普通使うことはないはずです。（３．ディレクトリサービスなんて、ActiveDirectory 環境が対象だし）
また、**ロックアウト機能**といって連続でパスワード間違えると、パスワードに使用したユーザー名での使用を不可能にする機能があります。この機能が**使用できないアカウントが、ビルドインアカウントである、Administrator** になります。Administrators グループに所属している場合にはロックアウト機能は有効に出来ます。
このあたりの話もあって、通常 Administrator として使用する場合は、Administrator グループに所属するユーザーを新規に作成しロックアウト機能を有効にして利用するのが良いと思います。
操作方法（ユーザーの追加）
スタート　→　設定「コントロールパネル」　→　ユーザーとパスワード



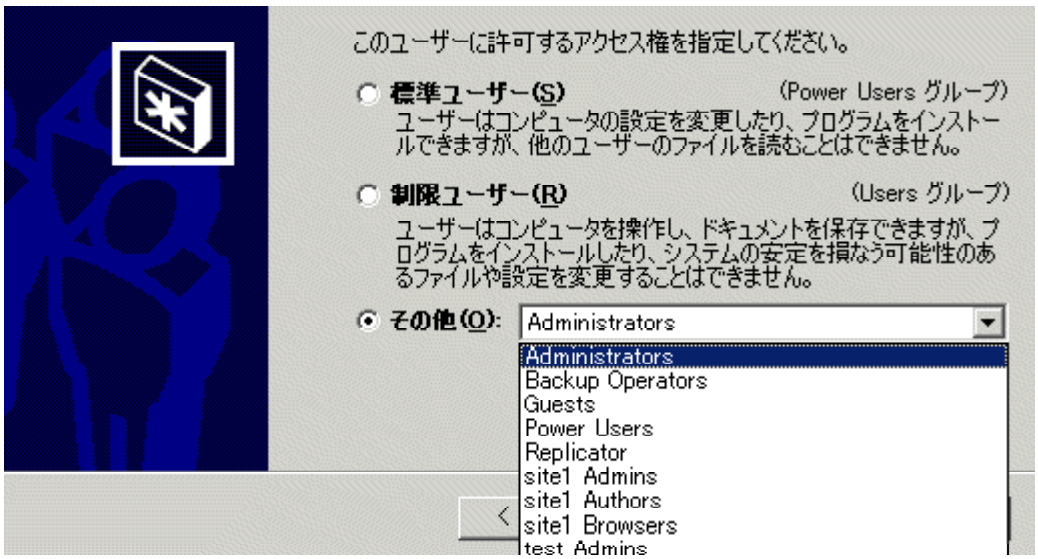
追加を選びます



ユーザー名を入力します。フルネームと説明は省略化しても問題ありません。



パスワードを２回入力します。（何も入力せずに次へを選べば、パスワードは空白になります）

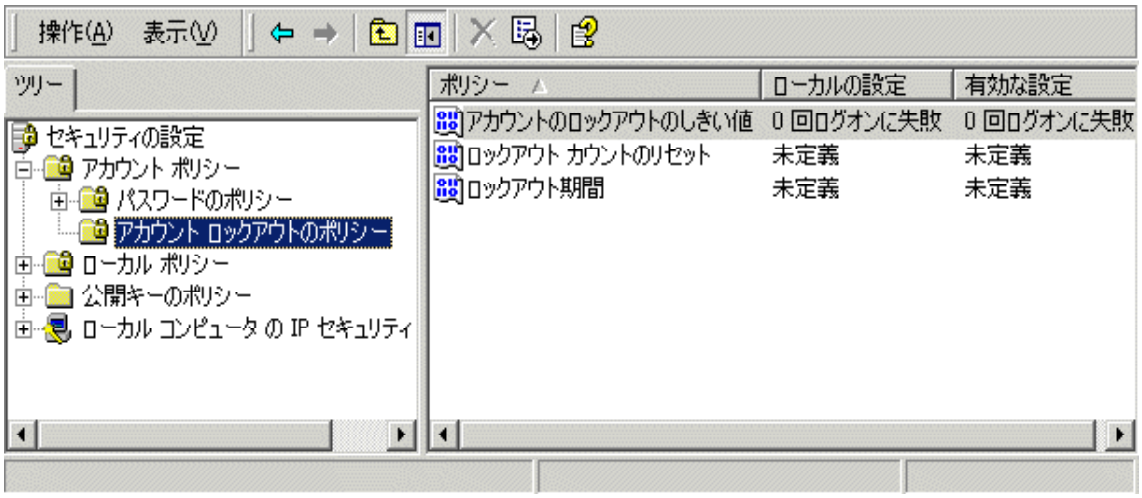


ユーザーのアクセス権を設定します。
ソフトウェアのインストールなど操作ができない場合があるため、標準ユーザーではなく、その他から Administrators を選びます。

2. ロックアウト機能を有効にしよう

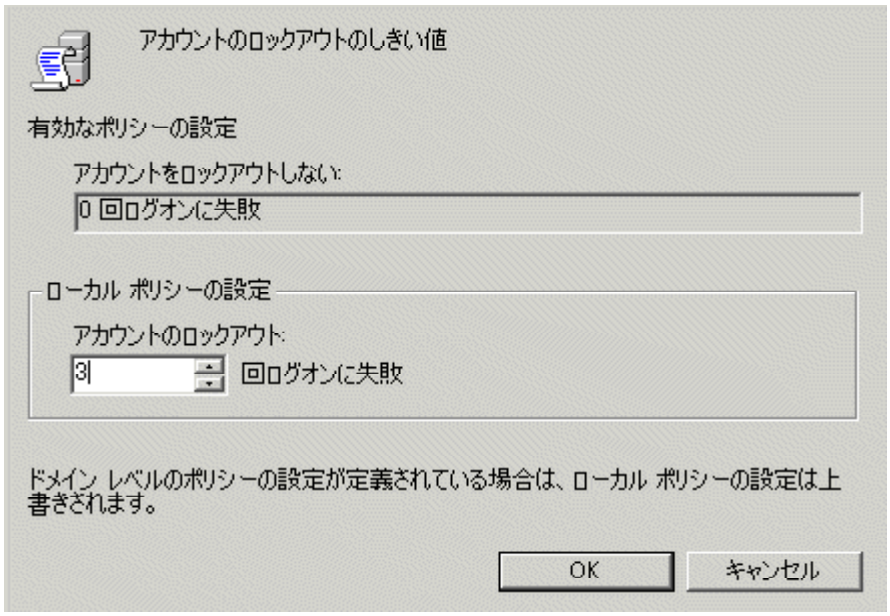
ロックアウトとは

ロックアウト機能は、ログインするときにパスワードを**連続して間違える**と、その時に使用したユーザー名でのログインを**使用不可**にする機能のことです。
銀行のキャッシュカードで暗証番号を連続して間違えるとカードが使用できなくなる仕組みと同じで、他人による不正使用を防止する働きがあります。
ロックアウト機能を利用することで、外部からの不正侵入（もちろんあなたの PC を誰かが操作する）で、パスワードを多数生成して、手当たり次第にパスワードを入力する方法（時間を無視すればパスワードを解くことが出来る）を防ぐことができます。この場合の防ぐというのは、時間がやたらとかかるためあきらめさせるというのもあります。
注意事項
ロックアウト機能を使用するには、ビルドインアカウントの Administrator 以外のユーザーで利用する必要があります。ビルドインアカウントの Administrator は、ロックアウトされないので設定はできません。
設定方法
スタート → 設定「コントロールパネル」 → 管理ルーツ → ローカルセキュリティポリシー



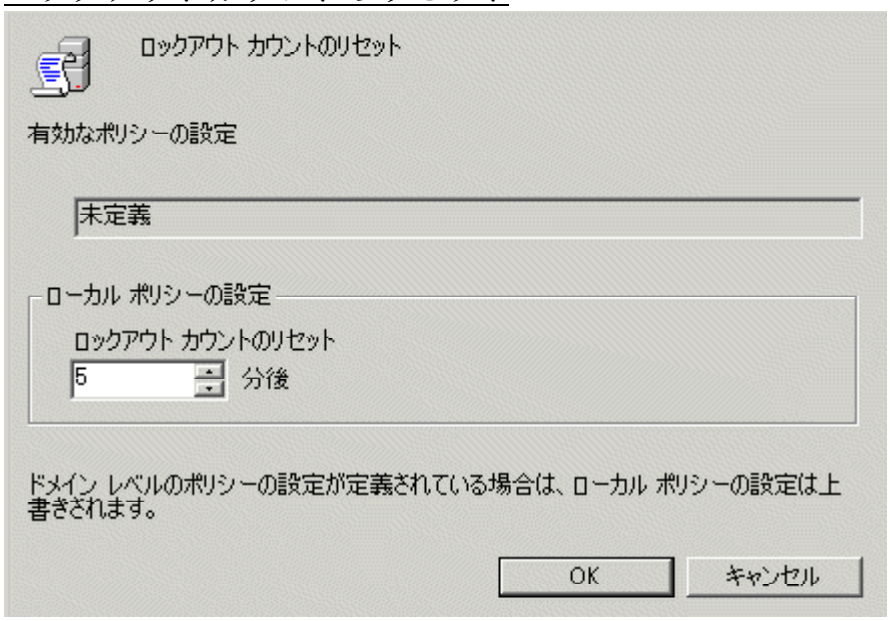
セキュリティの設定にある、アカウントロックアウトのポリシーを選びます。（画面左側を左ペインといいます）
選ぶと、画面右側（右ペイン）に項目が現れます。しきい値、カウントのリセット、期間の３項目があるはずです。
項目の選択は、項目上で右クリックのセキュリティを選ぶか、左のダブルクリックで設定可能になります。

アカウントのロックアウトしきい値



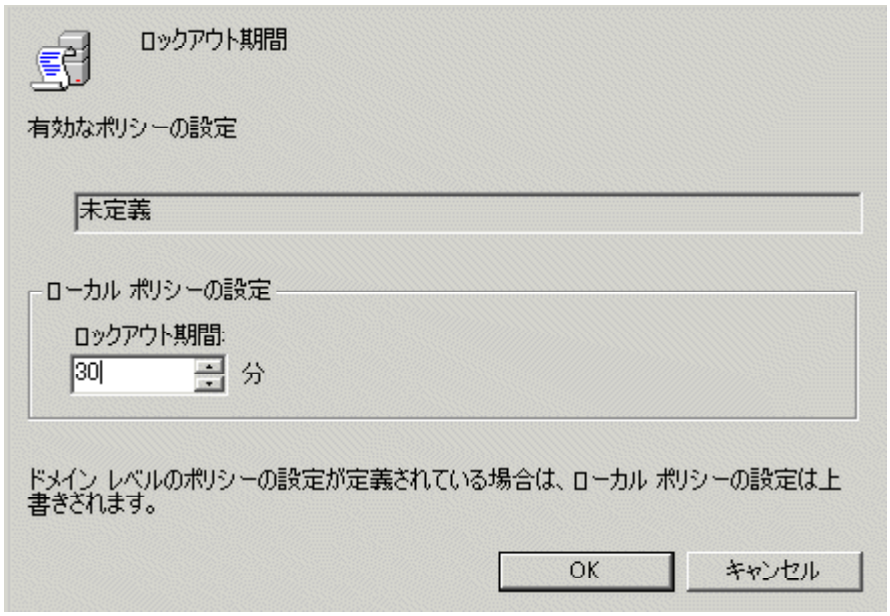
ロックアウトするまでの回数を設定します。画面では「３回」に設定しています。
３回を越えて（４回以上）パスワードを間違えるとロックアウトすることになります。
３～５回の範囲で設定するのが、一般的ではないでしょうか。
ロックアウト機能は、利用者でパスワードを入力するときにも機能しますのであまり回数を少なくすると、**利用者自身がロックアウト**されてしまうので注意してください。
ここで回数を決め、「OK」を選ぶと、以下のカウントのリセット、ロックアウト期間はそれぞれ**３０分に自動設定**されます。変更することは可能ですが、このままでも問題ないと思います。

ロックアウトカウントのリセット



パスワードが間違っていた回数を記憶している時間です。（そのはず(^^ゞ）
設定した時間が経過したものからパスワード間違いの回数から削除します。
ロックアウト期間と同じ時間設定で問題ないと思うのですが・・・。
画面では５分後に設定となっています。

ロックアウト期間



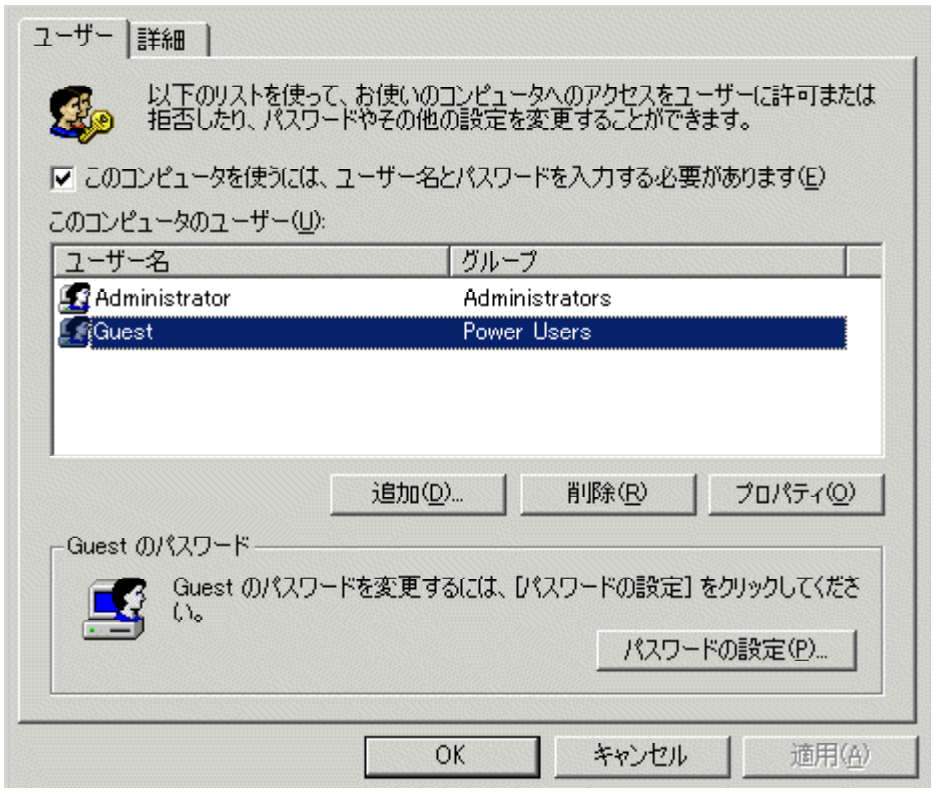
ロックアウトする時間を設定します。
画面だと「３０分」となっていますので、パスワードを連続して間違えてロックアウトされた場合、３０分間はそのユーザー名でログインすることができません。

---

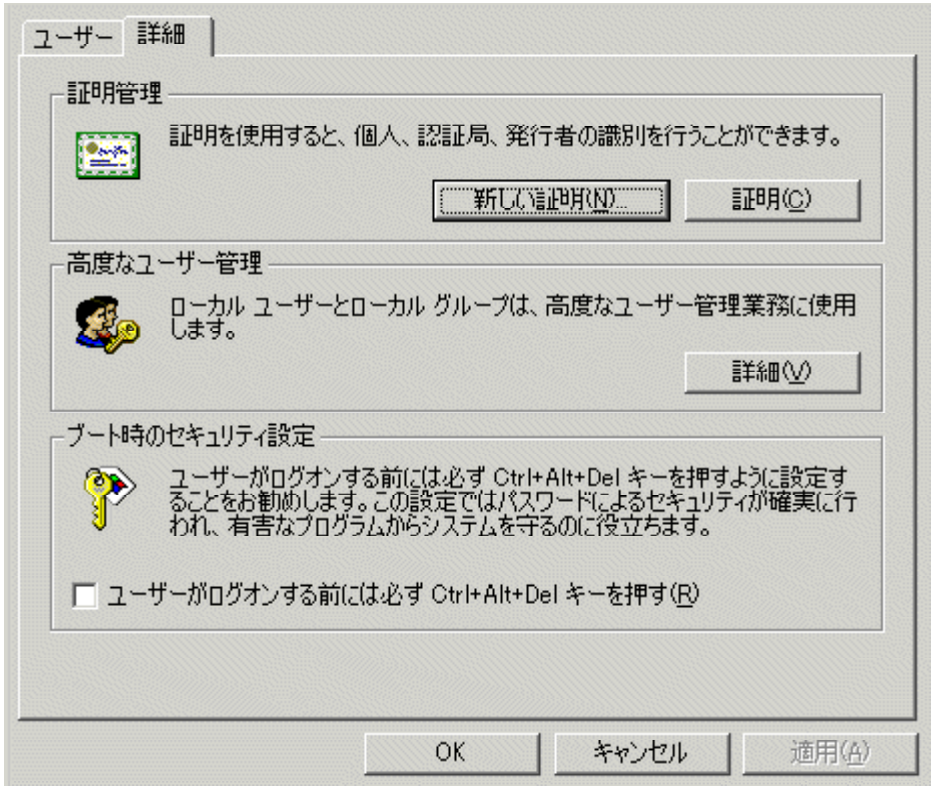
3. Guestアカウントを無効にしよう

Guest アカウントは、Windows2000 をネットワークに接続している場合に、匿名ユーザーからのアクセスを許可するのに使用します。
匿名ユーザーは、Windows2000 をファイルサーバーやプリンタサーバーなどに利用しているとき、利用者のユーザー登録を行わなくても利用できるユーザーにあたります。
Windows9x 系と併用している環境では、利便性からこの Guest アカウントを利用して匿名ユーザーとして接続する場合があります。
そのため、インターネットに接続している場合、Guest アカウントが有効になっていると、匿名ユーザーによる接続を許可してしまうため、ファイルの共有などが行われていると、外部からデータが読み書きされるおそれがありますし、ワームやウイルスなどといった悪質なファイルを送り込まれる恐れがあります。

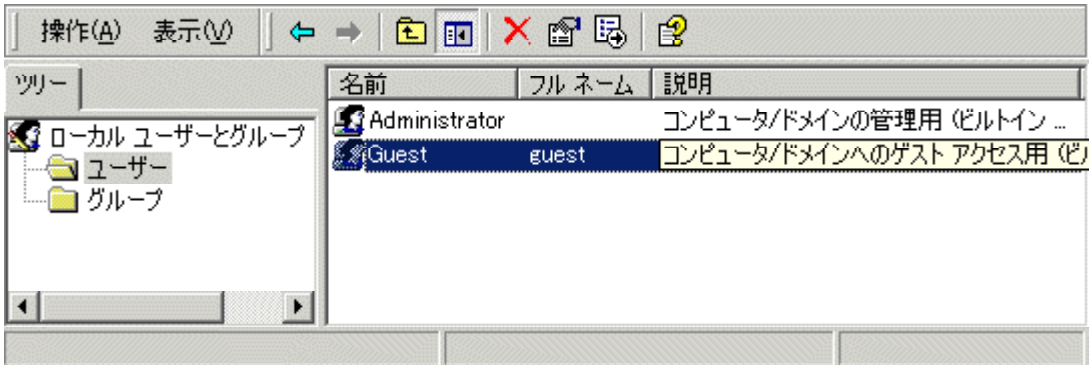
<u>設定方法</u>
スタート → 設定「コントロールパネル」 → ユーザーとパスワード



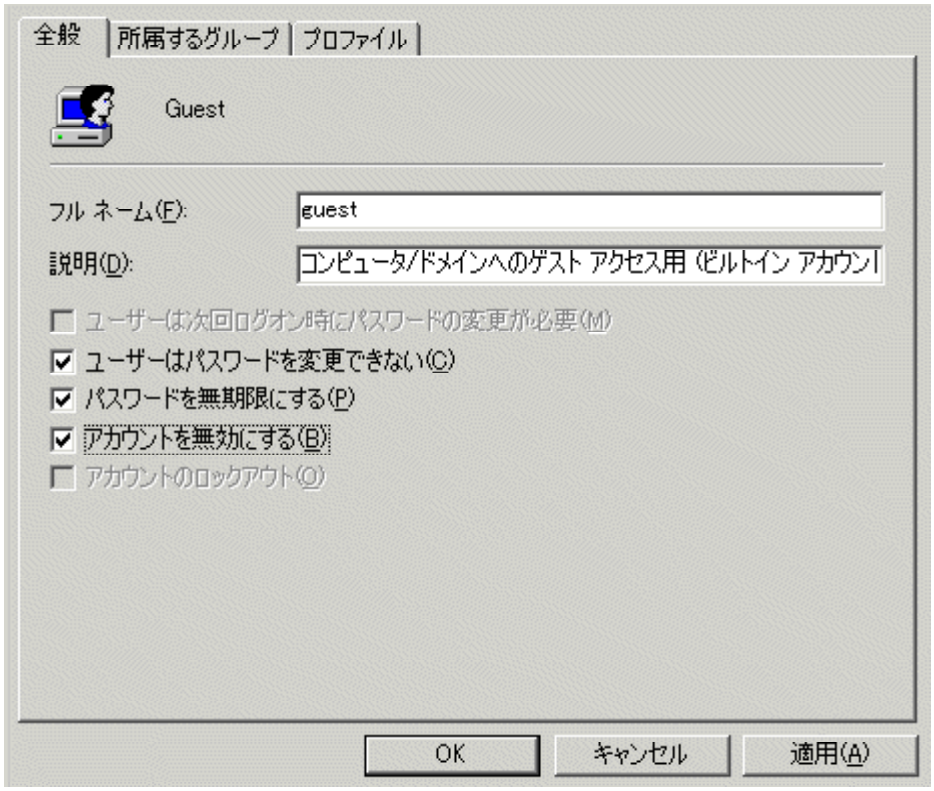
タグから「詳細」選びます



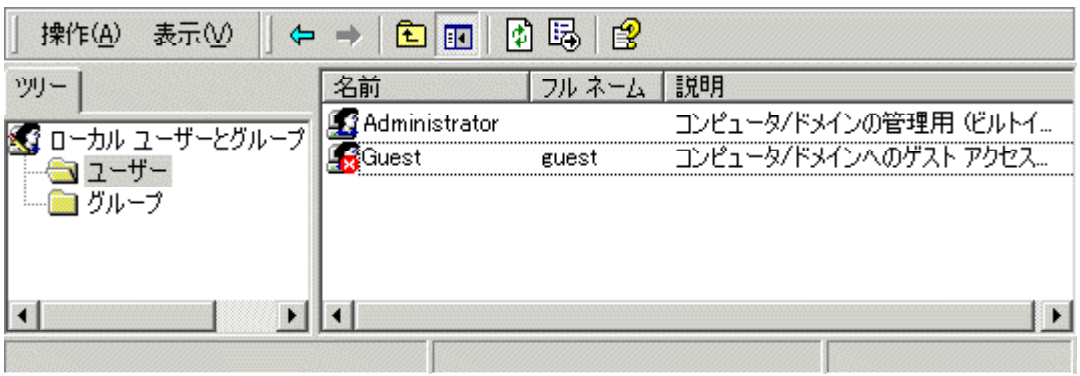
高度なユーザー管理「詳細」をクリック



左ペインで「ユーザー」を選択、右ペイン「Guest」を右クリックしプロパティを選びます



「アカウントを無効にする」のチェックを入れ「OK」(または適用)

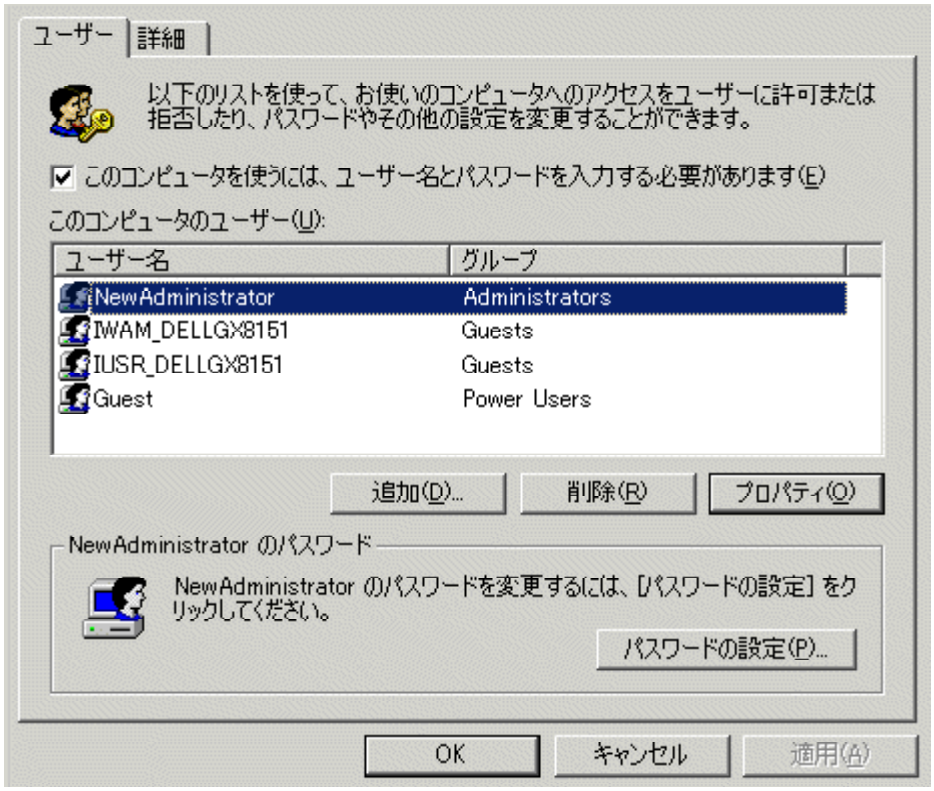


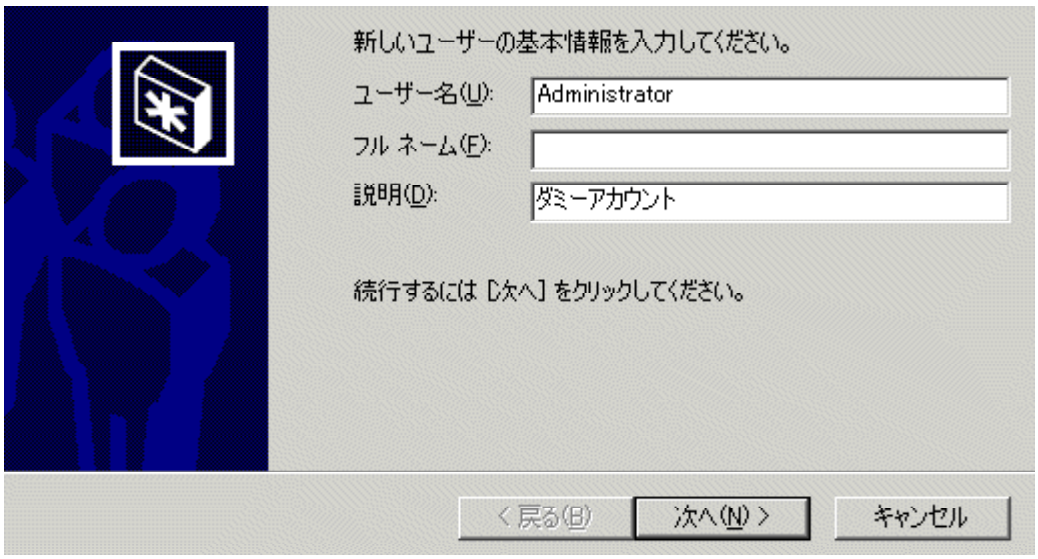
Guest のプロパティを開いた画面で、Guest アイコンに"X"が付いていれば無効になっている

4. Administratorのダミーアカウントを設定しよう

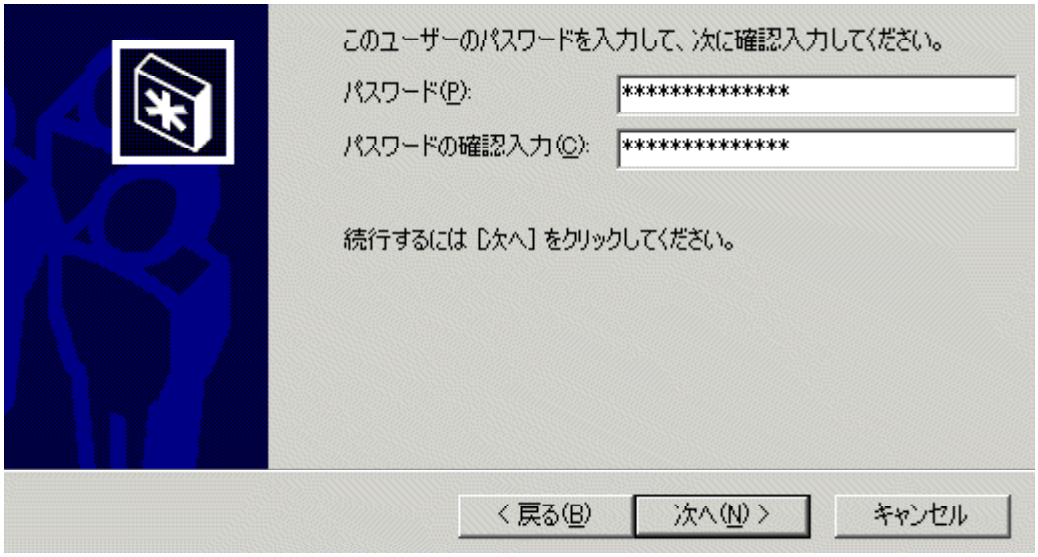
最初に、Administrator というユーザー名を変更しました。
ここでは、不正侵入のターゲットとして狙われやすい Administrator を制限ユーザーとして設定します。この Administrator はダミーユーザーとして使用しますので通常使用することはありません。ダミーユーザーは、監査機能を使用して一般的に多い Administrator になりすまして不正侵入を試みようとするのをチェックするのに利用します。
制限ユーザーとして、Guests グループアカウントを利用します。

<u>設定方法</u>
スタート → 設定「コントロールパネル」 → ユーザーとパスワード → 追加

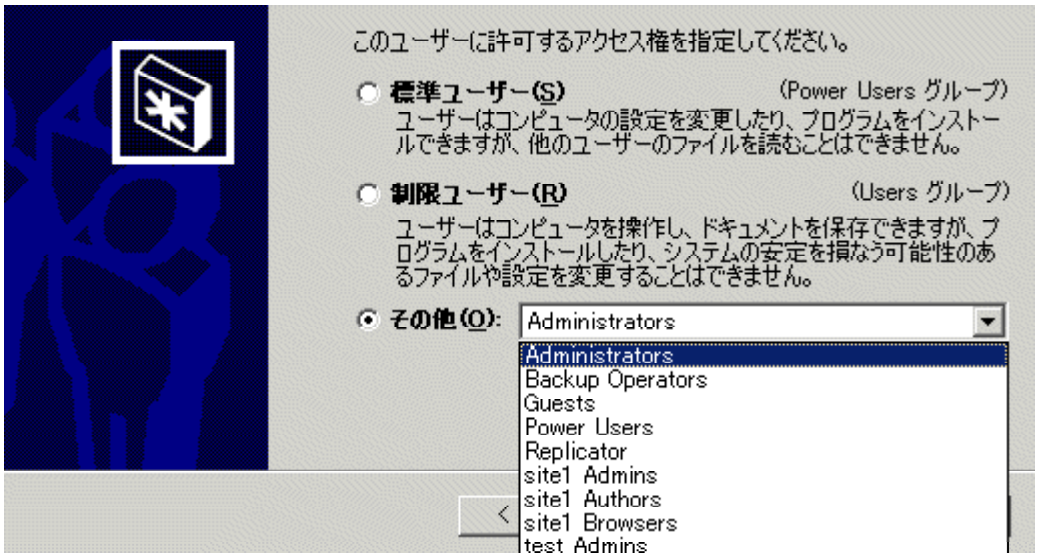




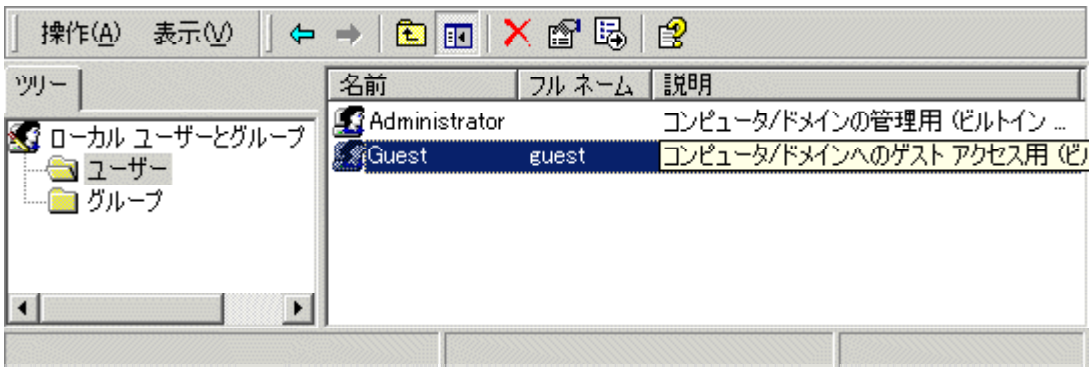
ユーザー名を「Administrator」とします。管理上判別が付くように、説明にダミーアカウントであることを明示しておきます。（説明は省いても問題ありません）



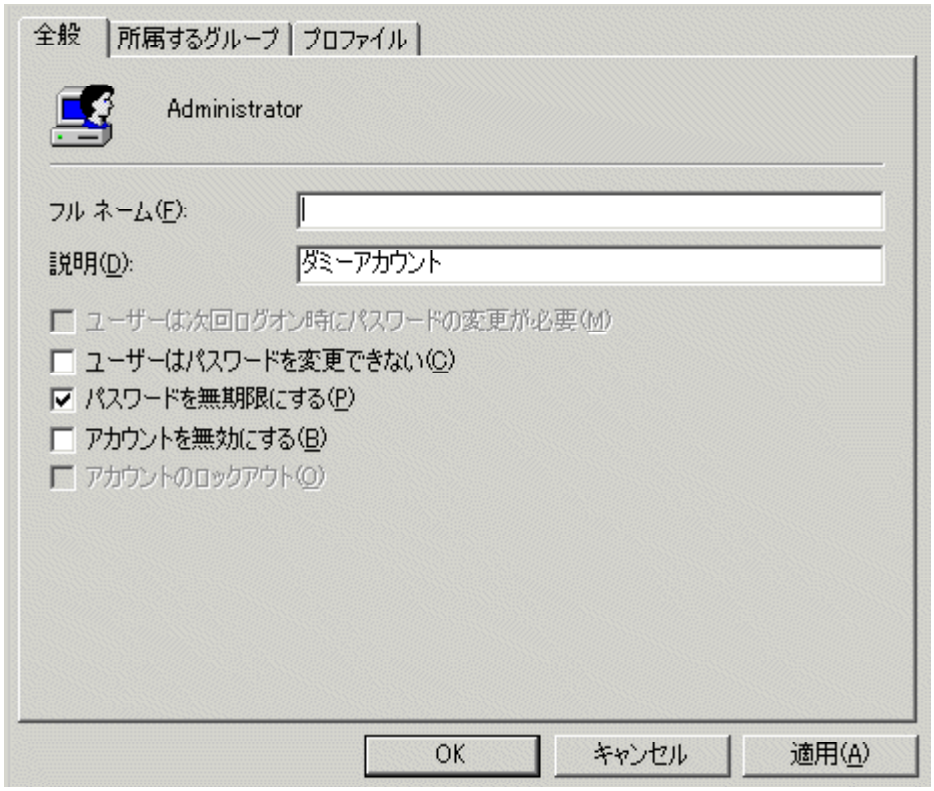
パスワードを登録します。これは大小文字を組み合わせ出来る限り長くします。
ダミーアカウントの Administrator ではログオンすることはないのでパスワードを覚えれなくても問題ありません。



アクセス権の設定をします。
その他から、Guest ｓグループを選びます。
ユーザーとパスワードの画面に戻りますので、Administrator が Guest ｓグループとなっていれば、適用を選択して Administrator のダミーアカウント設定は完了です。
続いて、詳細タグ → 高度なユーザー管理「詳細」を選びます。



左ペインでユーザーを選択し、右ペインでダミーアカウントの Administrator を選びプロパティを開きます。（注！画面は流用しているためダミーアカウントがありません！）
プロパティ画面は、Administrator をダブルクリックするか、右クリック→プロパティで開きます。



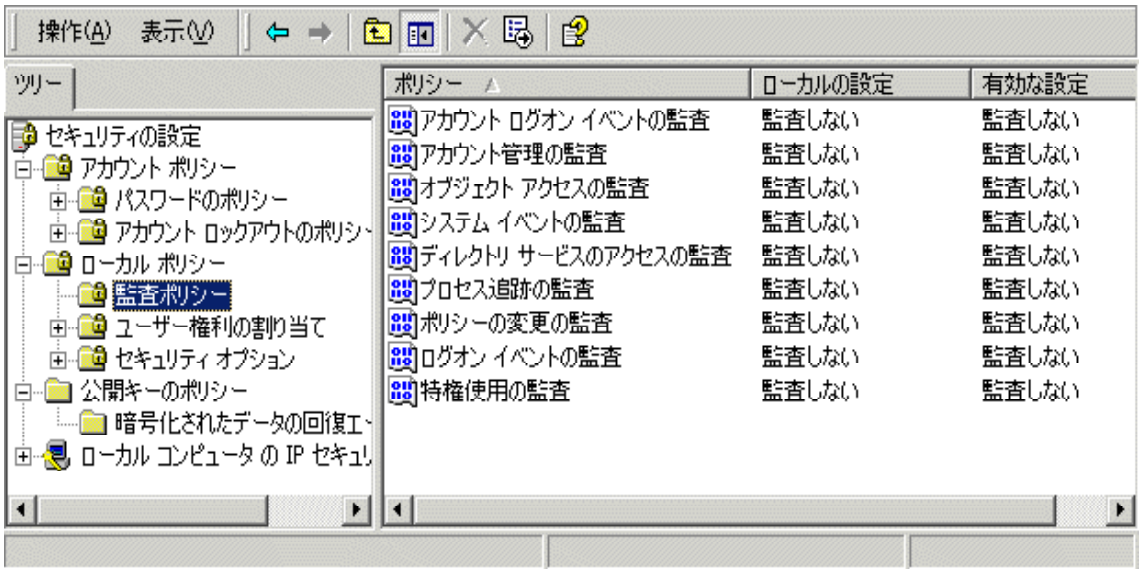
「全般」タグにある、チェック項目から、「ユーザーはパスワードを変更できない」と「パスワードを無期限にする」のチェックを入れます。
「OK」または「適用」を選べばすべての設定は終了です。

---

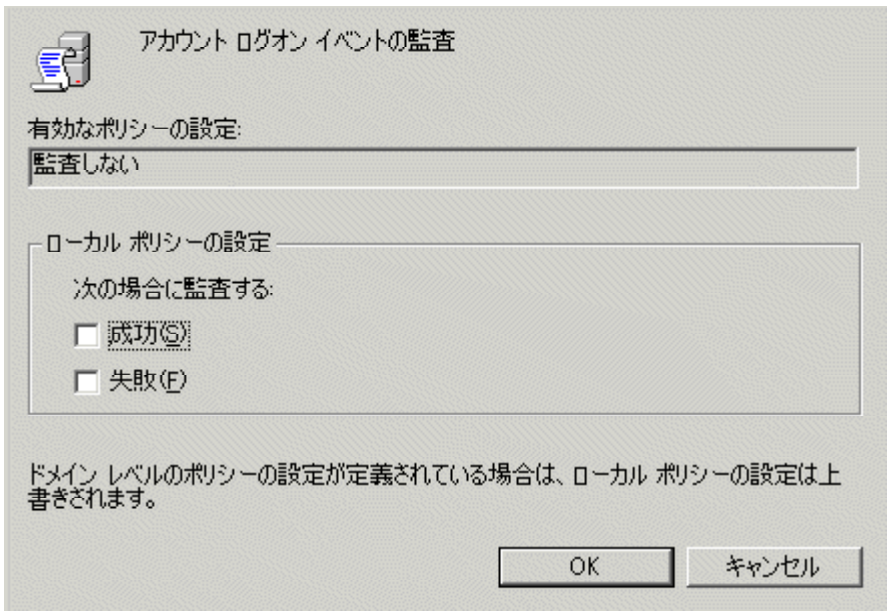
5. 監査を設定して不正侵入をチェックできるようにしよう

４．で設定した、ダミーアカウントの Administrator に不正アクセスがないかをチェックするために監査機能を有効にします。
監査機能は設定よって、アカウントへのログオンやファイルの読み書きなど多岐にわたってチェックをすることができます。
監査機能では、チェックを実施するために若干の時間と、頻繁にチェックをする場合には CPU 負荷がかかりますし、膨大なログ（記録）が発生しますので必要なものを確実にチェックできるようにするのがいいと思います。見るのもうんざりするような、ログの山では必要な情報が読みとることができません。
また、ログを定期的に見るようにしてください。不審に気づいてから、ログを見ても、何処に問題があるのか読み取ることができません。

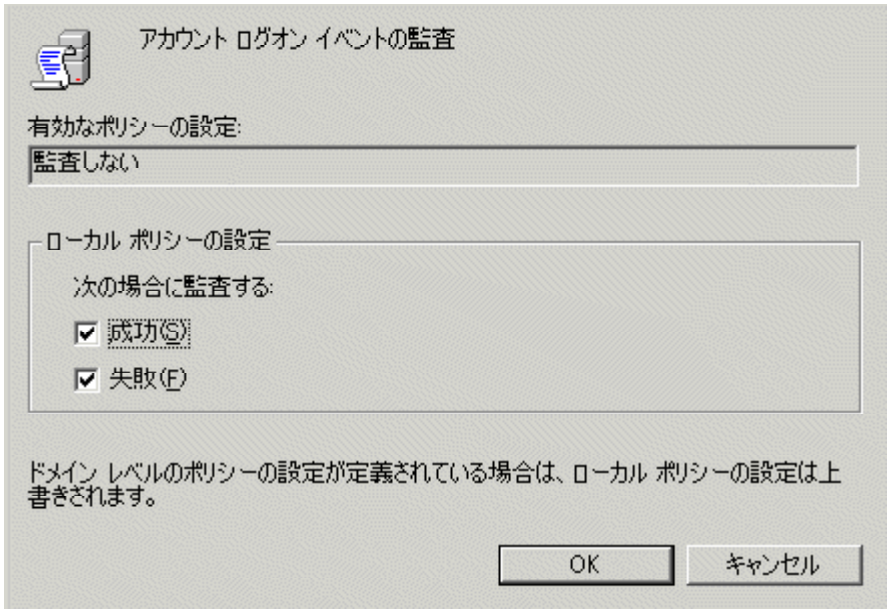
<u>設定方法</u>
スタート → 設定「コントロールパネル」 → 管理ツール → ローカルセキュリティポリシー
左ペインから、ローカルポリシー「監査ポリシー」を選択します。



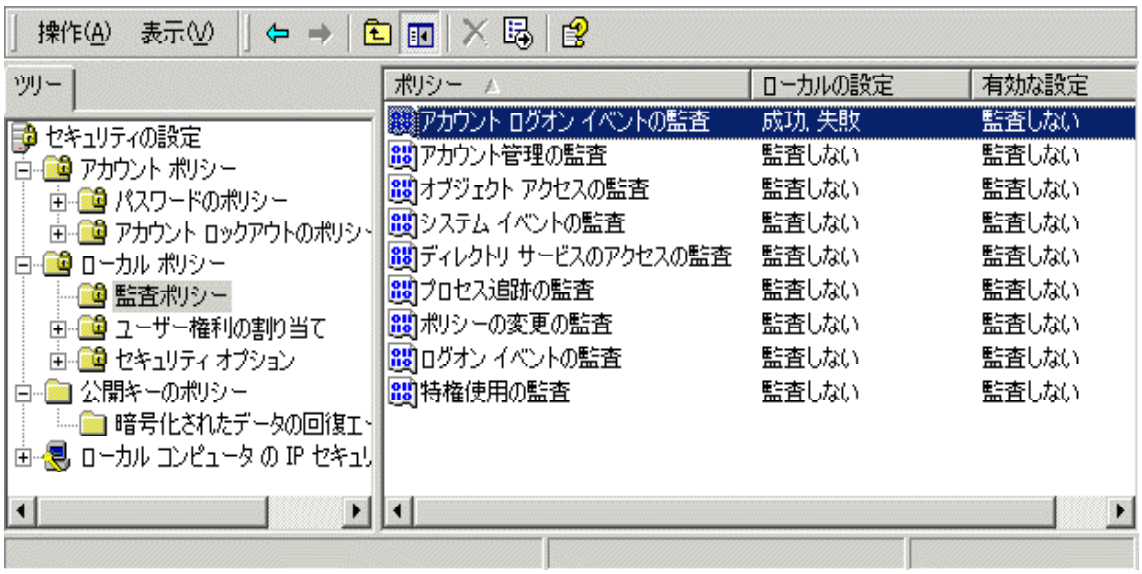
右ペインの「アカウントログオンイベントの監査」を選択し、ダブルクリックか右クリックでセキュリティを選びます。



ローカルポリシーの設定にある、次の場合に監査するのチェックボタンを「成功・失敗」どちらもチェックします。



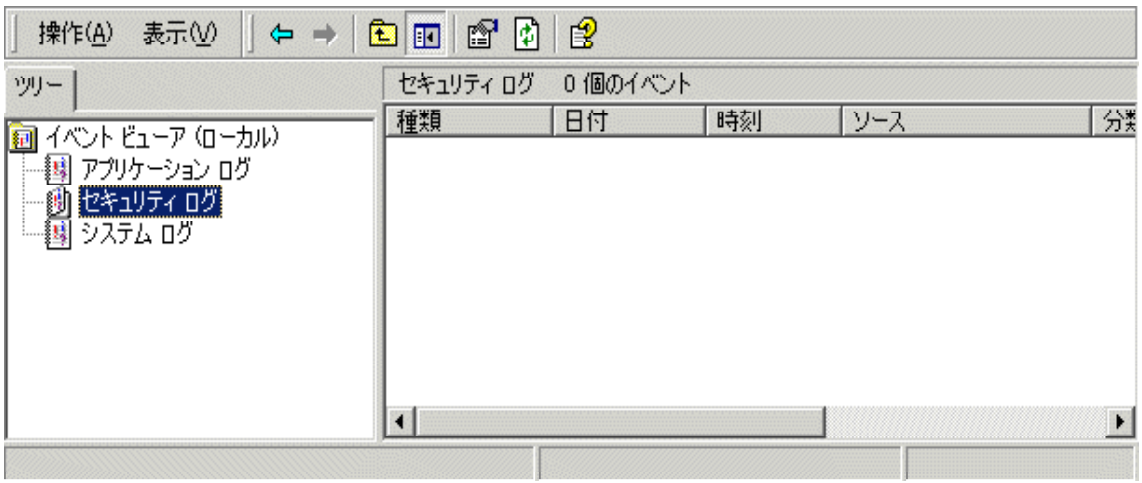
チェックをしたら、「OK」をクリックします。



設定が出来ると、項目右側のローカルの設定に監査項目が表示されます。

監査のチェック方法

監査のチェックは、管理ツールにあるイベントビューアを使用します。



左ペインの、セキュリティログを選ぶと、右ペインにログオンの成功・失敗が表示されます。

項目をダブルクリックすれば、詳細が表示されます。

ログオンの成功・失敗は、自分がログオンした場合も記録されるので、通常の記録状態を把握しておくとよいでしょう。

より詳細な監査をするには～補足～

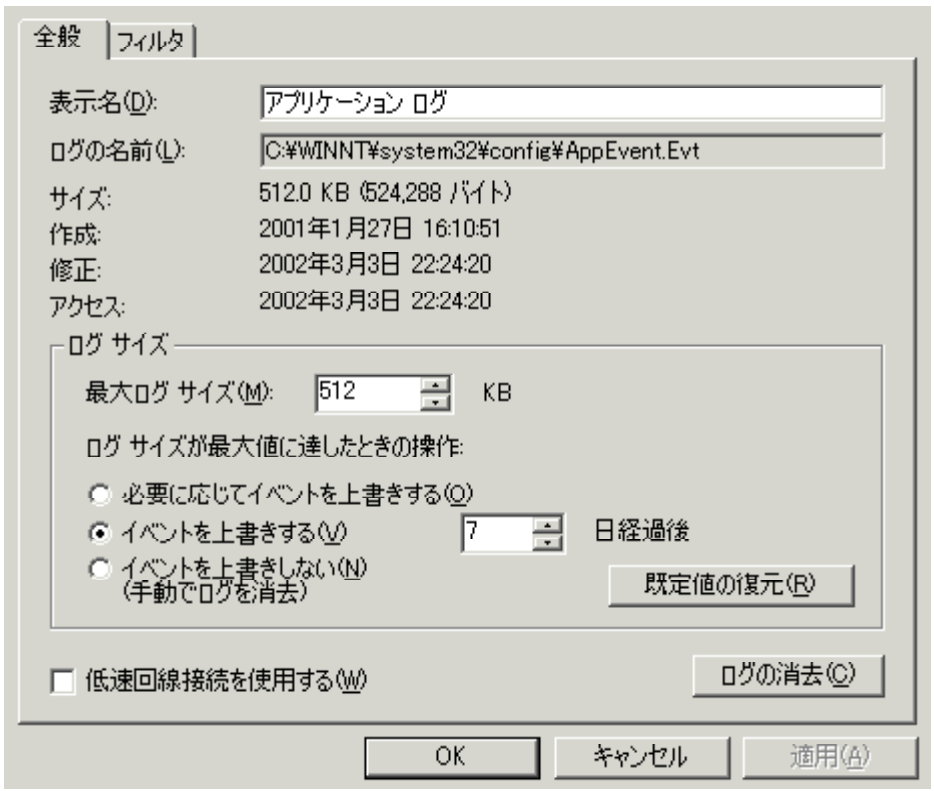
より詳細な記録を必要とする場合には、次の内容で監査機能を設定するとよいそうです。

ポリシー	ローカルの設定
アカウントログオンイベントの監査	成功、失敗
アカウント管理の監査	成功、失敗
オブジェクトアクセスの監査	監査しない
システムイベントの監査	監査しない
ディレクトリサービスの監査	監査しない
プロセス追跡の監査	成功、失敗
ポリシー変更の監査	成功、失敗
ログオンイベントの監査	成功、失敗
特権使用の監査	監査しない

イベントログは、イベントビューアでみることができますが、初期設定では「アプリケーションログ、セキュリティログ、システムログ」それぞれで、ファイルサイズの**上限５１２ KB、７日以上経過すると記録を上書き**するとなっています。ハードディスクの容量に余裕があるようなら、ファイルサイズの上限を増やして、保存日数を延ばした方がよいと思います。そのかわりに、記録量が非常に多くなりますのでそのつもりで。

設定方法

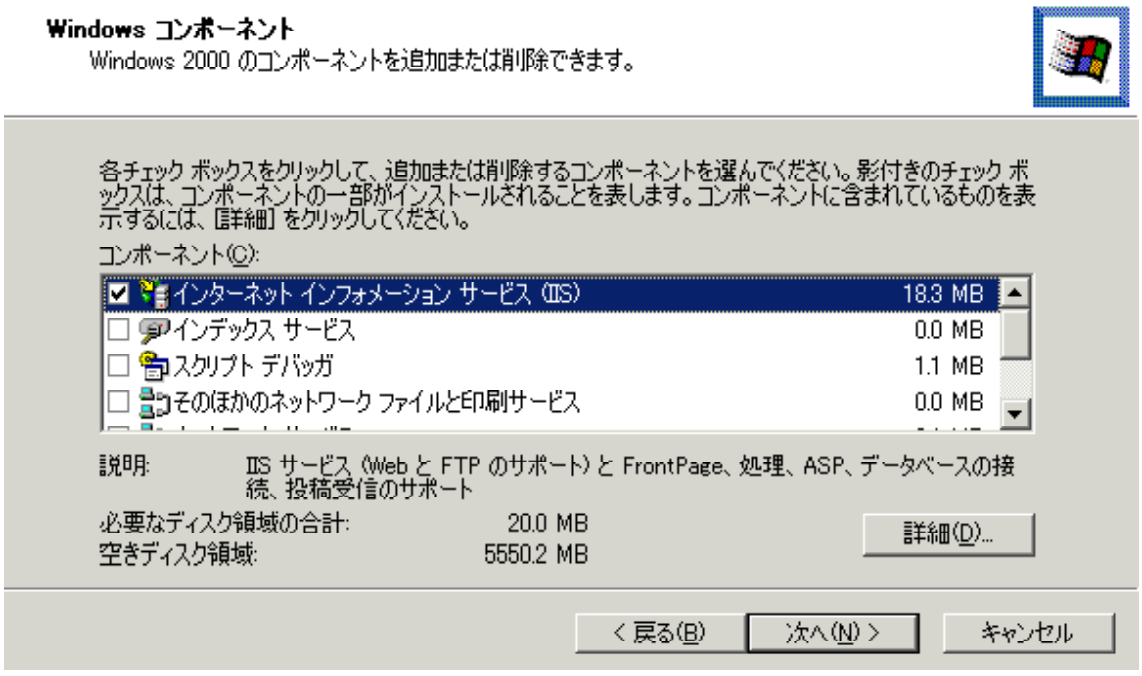
管理ツールにあるイベントビューアを開き、左ペインのそれぞれの項目で右クリック「プロパティ」を選びます。



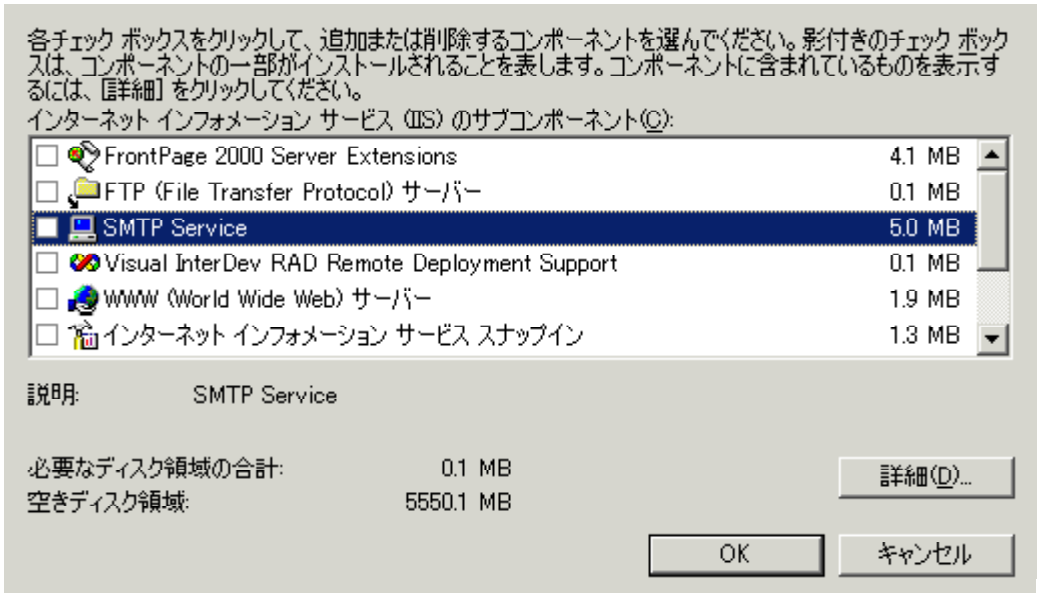
6. IISとSNMPサービスの停止を確認しよう

IIS（Internet Information Service）やSNMPサービスが利用できる状態で、適切な設定を行なっていない場合には、外部からの不正な侵入がしやすくなります。
IISは２０００年に猛威をふるった、CodeRedやNimdaといったワームなどのターゲットとなります。
感染した場合、感染源としてワームを発信するようになりますので注意が必要です。
また、往々にして重大なセキュリティーホールが発見されるサービスでもありますので、利用しない限りはコンポーネントを追加しないようにしましょう。
IISは、WWWサーバーやメールサーバーを構築・公開するのに使用し、SNMPはSNMP対応のネットワーク機器と情報交換や制御をするために使用します。
通常インストールしている場合には、IISやSNMPは利用できないようになっていますが、プリインストールのパソコンを購入している場合に、最初から利用可能となっている場合がありますので注意してください。
一度でも、コンポーネントとしてIISなどを追加した場合に、HFNetChkなどを利用してHotfixの適用を確認した場合に、IIS関連のHotfixが未適用として表示される場合があります。
その場合は、表示されたHotfixを必ず適用してください。

確認方法
コントロールパネル → アプリケーションの追加と削除 → Windowsコンポーネントの追加と削除 を選びます。



インターネットインフォメーションサービス（IIS）のチェックが入っていれば、チェックをはずします。（同時にSNMPサービスもチェックがはずれます）
SNMPの確認
IISを選択し「詳細」を選びます。



SMTP のチェックが入っていればはずします。IIS のチェックをはずせば詳細に含まれている内容は全てはずれるはずです。

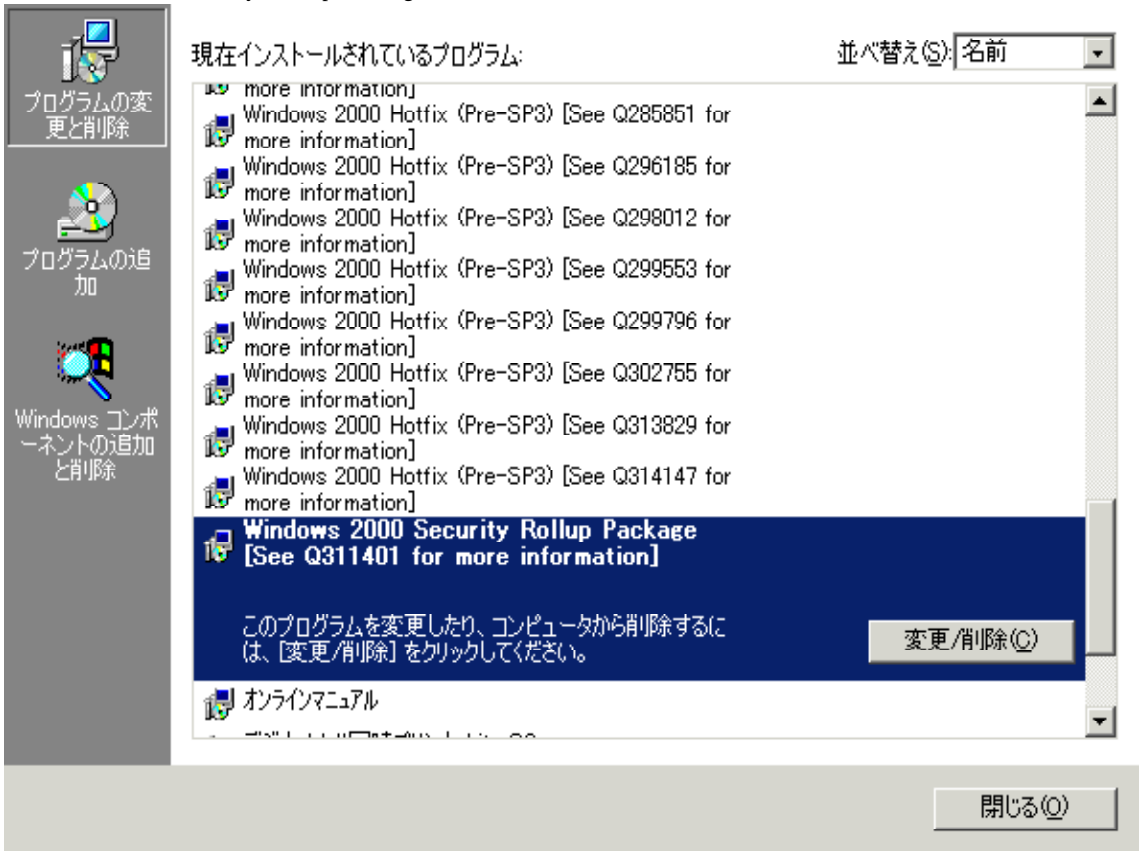
---

7. Hotfixは必ず適用しよう

Hotfix は、マクロソフトが提供する修正モジュール（プログラム）のことです。
WindowsUpdate 機能によって提供されている場合もありますが、Hotfix 配信までのタイムラグやアップデート機能が動作しない場合などがありますので、マクロソフトのホームページからダウンロードすることをおすすめします。
Hotfix 適用の前提として、Windows2000 ＋ SP2（ServicePack）＋ SRP1（SecurityRollupPackage）の構成になっている必要があります。(2002 年 8 月に SP3 が発表されているため、Windows2000 ＋ SP3 の構成を標準とするのがよい。SP3 は、SP1・SP2・SRP1 とその後に発表されている Hotfix が含まれるが、SP3 発表後新たな Hotfix が発表されているので確認を行う必要がある)
SP2 が適用されているかの確認は、コントロールパネルにある、システム「全般」で行います。

システムに ServicePack2 の表示があれば、SP2 が適用されている状態。
また、SRP1 の適用状態の確認は、システムでは確認できないため、次の方法で確認します。

コントロールパネル　→　アプリケーションの追加と削除「プログラムの変更と削除」に Windows2000SecurityRollupPackage の表示があるか確認します。



この２つのプログラムが適用されていれば、現在（2002.4）公開されている Hotfix を適用することが可能となります。

Hotfixを手に入れるには

Hotfix（SP2・SRP1 を含む）は、マイクロソフトのホームページから入手することが可能です。
おすすめは、必要な Hotfix を製品別に表示することのできる、Technet です。
（セキュリティ　→　製品別修正プログラム一覧を選ぶことで必要な Hotfix を入手可能です）
ただし、SP2 はファイルの容量が大きいため、雑誌の付録かマイクロソフトの配布サービスを利用して手に入れた方がいいと思います。

Hotfix の注意点

Hotfix の適用には適用順序があり、原則は公開された順に適用します。
Windows2000/XP では自動的に最新のモジュールを適用する機能が備わっていますので、普段利用するときには、意識しなくても問題ないと思います。
Hotfix や SRP は、特定の問題を解消するために作成されているために、新たな問題を発生する場合があります。しかし、発生している問題点を解消した方が、セキュリティー上好ましいため、Hotfix の適用は速やかに行ってください。
Hotfix の適用方法や未適用の Hotfix を探す方法は、HFNetChk & QChain を利用しようを参考にしてください。

ブラウザやメールソフトも忘れないで

ホームページを閲覧するためのブラウザ（InternetExplorer や Netscape）、メールソフト（OutlookExpress）などにも、Hotfix や Patch（パッチ）といった修正プログラムが公開されています。必ず利用しているソフトの提供元をチェックして、最新の修正プログラムを適用してください。

InternetExplorer（IE5.5）に Hotfix を適用している状態
更新バージョン以降に表示されている SP2、Qxxxxxx は全て Hotfix

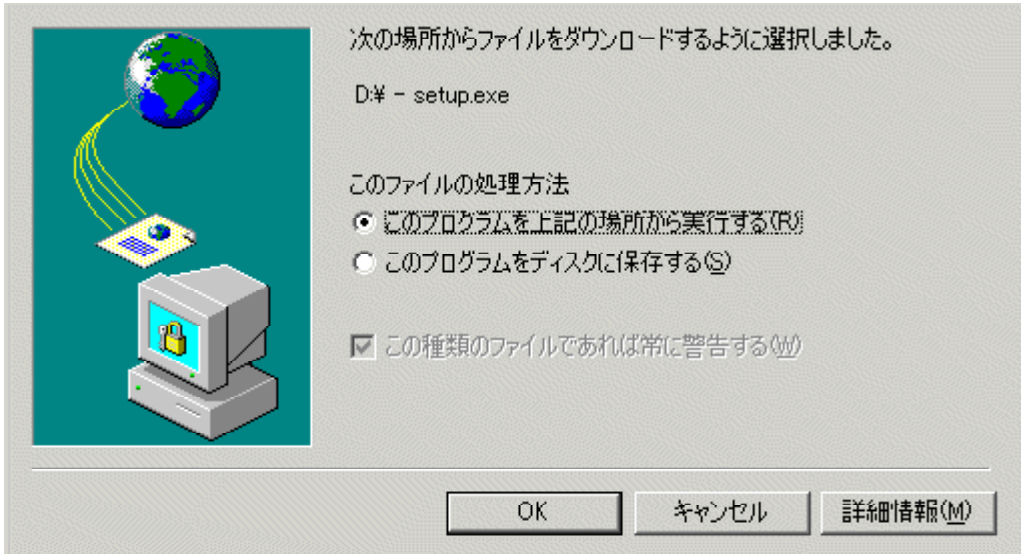
8. Microsoft Security Tool Kit CDを入手しよう

マクロソフトのＨＰでは、**セキュリティツールキット（以下 MSTK）というＣＤを無償で配布**しています。
今回紹介している内容は、２００１年１１月上旬に提供された MSTK を利用しています。
MSTK は、WindowsNT3.5/4.0SP3 以上/2000 を使用し、インターネットに接続しているパソコンを対象に、セキュリティ強化（標準化）を簡単に行うためのツールが入っています。
Windows95/98/Me や WindowsXP を利用している場合には、マイクロソフトアップデートなどを利用して必要なファイルをダウンロードしてください。
また、MSTK はセキュリティ強化を補助するのが目的のツールなので、ウイルス対策や新たに発生した問題などの対応は必ず実施してください。

MSTKの利用方法
MSTK のツール構成は次のようになっています。
１． ServicePack（SP）
２． Hotfix
３． IIS（Internet Information Service/Server）用のセキュリティ強化ツール
４． HFNetChk や Qchain などの Hotfix の適用支援ツール
５． セキュリティに関するドキュメント
とても難しそうな内容ですが、基本的な利用法は非常に簡単になっています。
MSTK インストール
MSTK の CD を挿入すると、MSTK の概要が表示されます。(readme.html)

この中にある、現在のシステムをほ保護するという項目にある「今すぐインストール」をクリックするか、CD-ROM のルートフォルダにある「setup.exe」を実行すると、「Microsoft Security Tool Kit Setup」が実行されます。
「今すぐインストール」を選ぶとダウンロード画面になります。

「このプログラムを上記の場所から実行する」を選んで OK をクリックします。



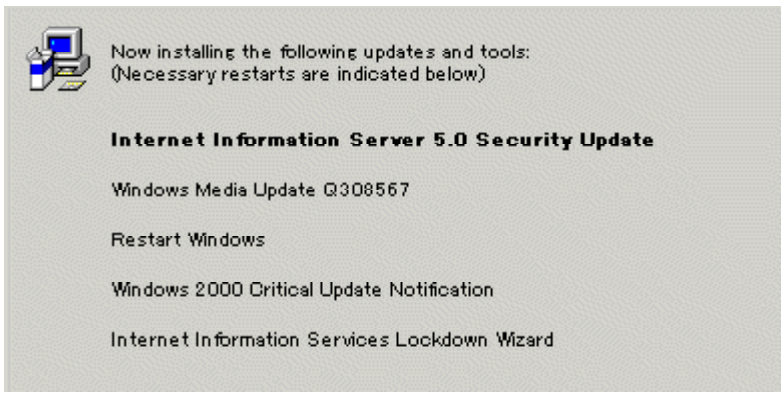
署名の確認が出る場合には、「はい」を選んでください。

OS の種類、InternetExplorer のバージョンや SP の適用状態を自動的に判別するので OS の選択といった特別な操作は不要です。

MSTK セットアップの概要が表示されます。「NEXT」を選んでください。

インストール確認画面（表記は英語）が表示されますので、「Install」をクリックしてください。
下の画面では上から、IIS のセキュリティアップ、Hotfix、再起動、重要な更新のお知らせ、IIS ツールがインストールされるとなっています。

インストール中の画面



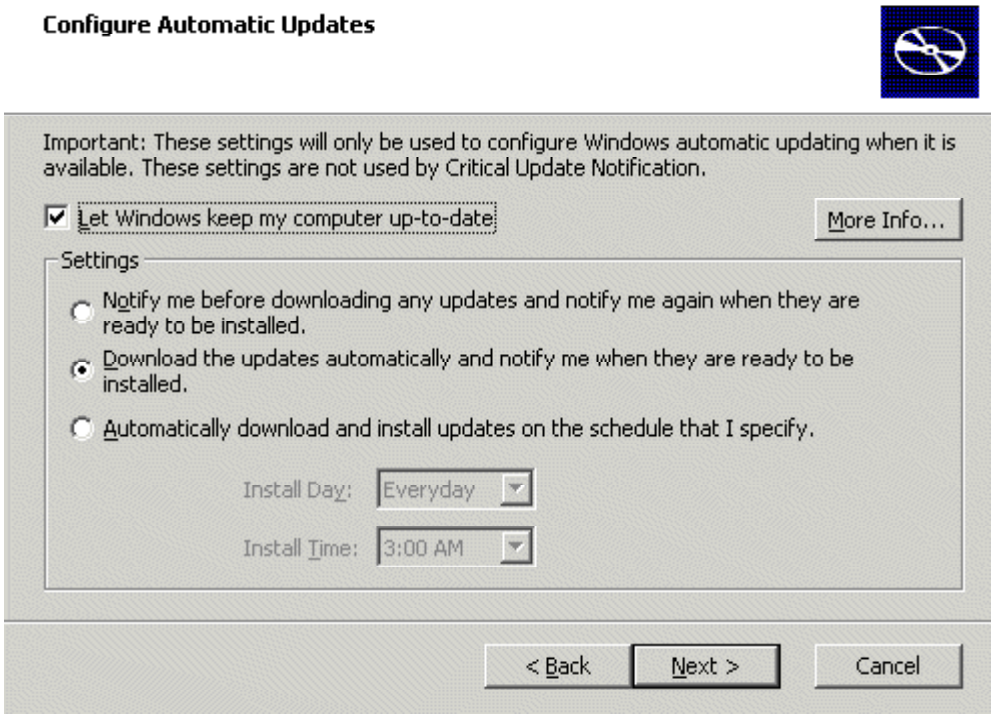
自動的に必要な SP や Hotfix がインストールされます。
インストールが完了すると「再起動」の確認をしてきますので、「OK」をクリックして再起動します。

再起動後、「Windows Critical Update Notification」（重要な更新の通知）のセットアップが実行されます。
重要な更新のお知らせのセットアップ確認がでます。「NEXT」を選んでください。
重要な更新の通知を削除するには、レジストリ操作が必要になります。
削除については、マイクロソフト「Security Tool Kit 重要な更新の通知をアンインストールする方法 」を参照ください。

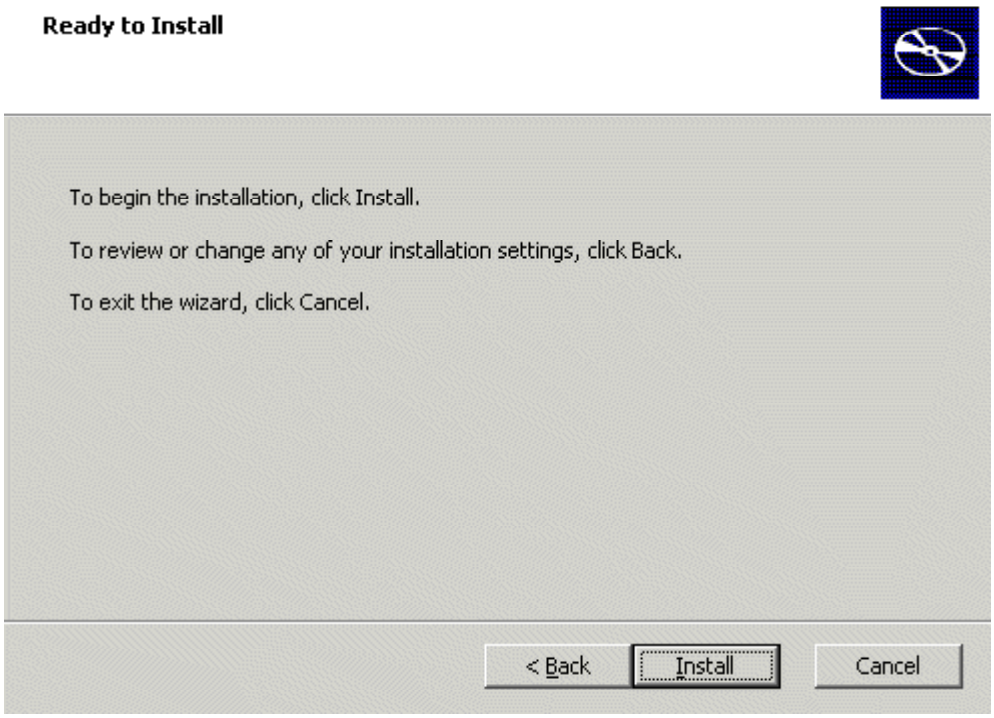
ライセンス承諾確認です。

「I accept the terms of the License Agreement 」のチェックを入れて、「NEXT」を選択します。

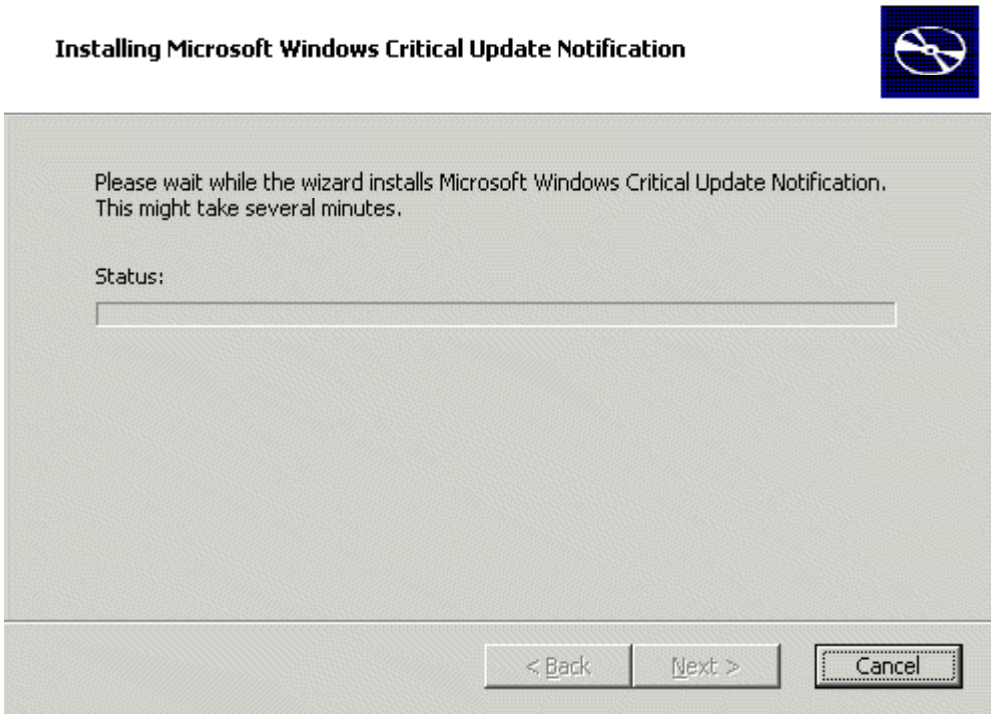
更新周期の設定です。そのままの設定で問題はないと思います。



インストール確認です。「Install」を選んでください。



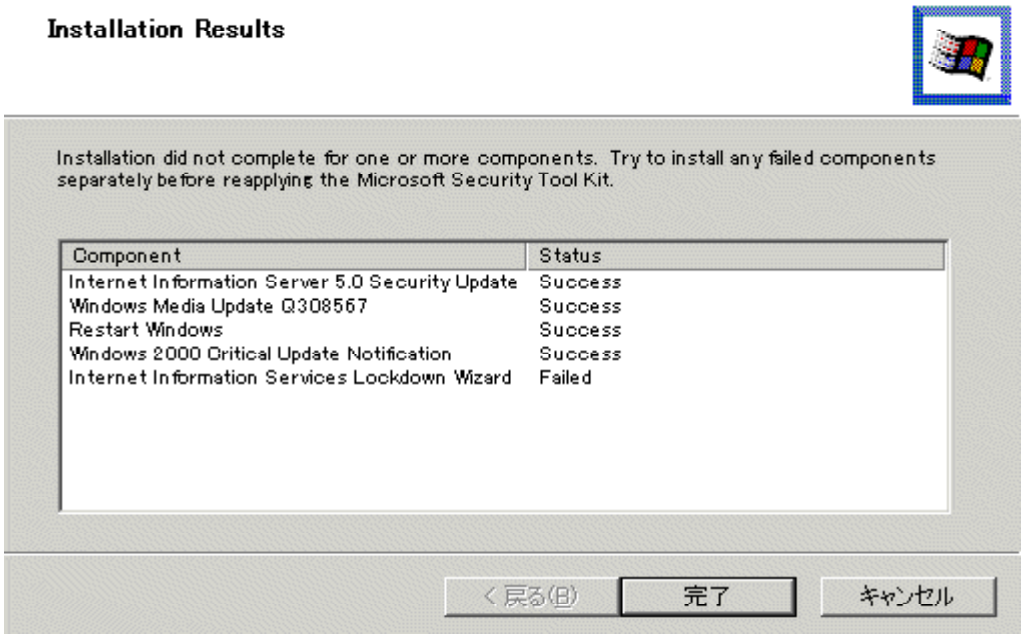
インストール中の画面。



終了表示です。「Finish」を選んでください。

IIS のツールインストール画面です。
これは、IIS を利用してる場合に表示されます。今回は紹介を省略します。
WEB サーバーやメールサーバーとして使用していないときに、この表示が出る場合には IIS がインストールされていますので、サービスを停止することをおすすめします。

最後にインストール結果が表示されます。
画面では、IIS ツールのインストールをキャンセルしたために、一番下の部分でインストール失敗の表示が出ています。
「完了」を選んで作業は終了です。



以上で、MSTK のセットアップは終了です。
この状態でもある程度のセキュリティは確保できていますが、その後に発表されている、Windows2000SecurityRollupPackage（SRP1）や InternetExplorer の累積修正プログラムなどには対応していないので必要 Hotfix は、HFNetChk やマイクロソフトのホームページで調べてください。
入手先
マクロソフトセキュリティツールキット
http://www.microsoft.com/japan/security/kitinfo.asp

9. ウィルス対策は忘れずに

コンピュータウィルスやワームから身を守る方法は、ウィルス対策ソフトを導入するのが、堅実な方法です。
私の周りをみてみると意外に、ウィルス対策ソフトを導入しているユーザーは少ないのに驚くものです。
当然メールを利用して、インターネットも利用しています。
ウィルス対策をしない理由を聞いてみると、”お金がかかる”や”よくわからない（必要という認識がない）”といった話を聞きます。
そこで、ウィルス対策ソフトをわかる範囲で紹介しようと思います。
（紹介には個人的な主観が入っていますのでご了承ください。）

ソフト名	簡単な紹介
ウィルスバスター トレンドマイクロ	国内最大のシェアを誇る（らしい）ソフト。 最新版は、ファイアウォール機能を搭載し PC への外部からの不正アクセスも防ぐ。 ウィルスバスター２０００の頃（現在リリースは２００２）には、パターンファイルが２～３ MB と大きくダウンロードに苦労した覚えがあるが、現在はどうなっているんだろうか。
Norton AntiVirus シマンテック	ウィルスバスターとほぼ同じ機能を持っている製品。 ウィルスパターンをファイルとしてダウンロードできるため、インターネットに接続しない PC や、複数の PC を利用してる場合には便利。 パターンアップデート機能を利用すると、パターンファイルが小さいため、低速回線を利用している場合にダウンロード時間が短くてすむ。 パターンファイルの提供は、インストール時点から１年間無償提供される。 それ以降は、年間２０００円程度のレジスト料金を支払う必要がある。
Mcafee 日本ネットワークアソシエイツ	基本機能は押さえているソフトで、ウィルスバスターや NortonAntVirus と比べても遜色はない。 が、なぜかこれを利用している人を見たことがない。 少し前までは、シェアもそれなりにもっていたが、宣伝で負けてしまったようなものか。
ウィルス警備隊 NEC ホームエレクトロニクス	コンビニで買える（という話の）ソフト。 低価格（¥2980）ながら、基本機能を押さえているのがウリらしい。 韓国では、シェア No.1 だが、日本で売れているかは不明。 ５ユーザーライセンスというお徳用も販売しているので、多数の PC を所持している方は参考にしてみてはいかが。
H+BEDV Antivir Personal Edition	個人利用に限って無償版が提供されている。 ユーザー登録をすると これを書いている時点では、ダウンロードサイトに接続ができない。 マニュアルの日本語訳はここで入手可能。
アンチドート簡易版	簡易版は無償提供。 インストール不要のソフトでダウンロードしたファイルを実行すれば OK。 製品版では、パターンファイルによるアップデートが可能だが、簡易版はパターンファイルとプログラムが一体になったものをダウンロードして使用する必要がある。 いまでは、数少ない NEC PC-98 シリーズ対応のプログラムを提供しているところ。 検索速度は遅め。ウィルスパターン更新は週に１回程度で、その都度プログラムをダウンロードする必要がある。
AVG AntiVirus	ユーザー登録をすると個人利用に限り無償で利用できる。 英語版のみだが、フリーで利用できるものでは一番ポピュラーなものと思う。

とまあいろいろあるのですが、ウィルス対策ソフトを入れたら、必ず定期的にパターンファイルのアップデートをしましょう。

パターンファイルは、ウィルス情報のライブラリです。
これが最新のものでないと、当然最新のウィルスに対応することができません。
パターンファイルは、１週間に１回程度の割合で更新されるので、週に１回パターンファイルの更新を行うようにしましょう。ソフトによっては、自動更新機能もありますので活用してください。
あと自己防衛として、怪しいメールは開かない、メールプレビュー機能を使用しない、Java や ActiveX を実行しないようにすることでも、メールからのウィルス感染を予防することになります。
