Webサーバー構築時の問題点と解決策

Windows 2000におけるセキュアな環境の指針

Supecial Feature

吉田かおる *text by Yoshida, Kaoru*
日本電気株式会社
Eラーニング事業部

「Windowsは脆弱点が多く、サーバーには向かない」という意見があるが、設定さえ誤らなければ、喧伝されるほどの問題は起こらない。むしろ、デスクトップで見慣れた環境だからこそ、馴れや慢心から既知の穴まで放置してしまうのではないだろうか。
当たり前だがサーバーとデスクトップは異なる。デスクトップのつもりで付き合うと痛い目にあうのは必至だ。サーバーのWindowdsとどう付き合えばよいのか、詳細に解説する。

はじめに

ADSLや光ファイバー、CATVなどの高速で常時接続が可能なネットワークの普及により、インターネット接続環境は大幅に向上しました。これにともない、今まではインターネットサービスプロバイダ（ISP）のレンタルWebサービスを利用していたスモールオフィスや一般のユーザーが、自力でWebサーバーを立て、情報発信を行なおうとしています。自分でサーバーを構築すれば、ISPに支払っていたWebサーバーのレンタルコストは削減でき、また、制約によって、利用できなかった機能、たとえばASPスクリプトやCGI、データベースとの連携なども自由に行なえます。しかしその反面、Webサーバーの管理、特にセキュリティ管理が必要となります。匿名性の高いインターネットには、悪意を持つ者もたくさんいることを忘れてはなりません。そして、そうした人々は、あなたのサーバーへの攻撃や不正侵入を企んでいるかもしれないのです。特にWindows 2000の場合、初期状態の設定が、Webサーバーとしての運用を前提としたセキュアなものではなく、どちらかと言えば、初級ユーザー（または初級管理者）にも扱いやすいようにセキュリティ機能が緩和されています。よって、初期状態のままで、Windows 2000をWebサーバーとして公開しようとすると、悪意を持つ者の格好の餌食となる可能性があります。

しかし、セキュリティに関して正しい設定さえすれば、Windows 2000をWebサーバーとして運用することは、UNIXをWebサーバーとして運用するよりも安全であるという意見もあるほどです。そこで、本稿ではWebサーバーを構築する予定のある方や興味のある方を対象に、Windows 2000と標準のインターネットサービスであるInternet Information Service 5.0（IIS）をベースとした、Webサーバーの構築におけるセキュリティの問題点とその解決方法を紹介していきます。

Windows 2000とネットワークのセキュリティを強化する

安全なWebサーバーの構築には、まずその土台となるネットワークやWindows 2000のセキュリティ設定が必要です。土台がしっかりしていなければ、その上で安全なWebサーバーを構築することはできません。特にWindows 2000には複数のセキュリティチェックポイントがあるため、ポイントごとに正しく設定し、悪意のある者からの攻撃を防ぐ「サーバーの要塞化」を行ないます。

Webサーバーを安全なネットワークに配置する

まず、はじめにWebサーバーを配置する場所について考えます。

いくらWindows 2000を要塞化するからといって、インターネットに直接公開することは、セキュリティ上、あまりお勧めできません。通常は、インターネットには、パケットフィルタの機能をもったルーター（スクリーニングルーター）またはファイアウォールを配置し、不要なパケットをブロックした上で、その内部にWebサーバーを配置します（図1）。個人ユーザーであれば、パケットフィルタ機能をもったブロードバンドルーターを活用するとよいでしょう。予算に余裕のあるスモールオフィスでは、ファイアウォールを導入するべきです。ファイアウォールは当然、ブロードバンドルーターよりも高度なセキュリティ機能を提供します。また、その他のクライアントコンピュータがあり、それらがインターネット接続を必要とするのであれば、それらをWebサーバーと同じネットワークに配置するか、またはさらに別のネットワークを作成し、そこに配置するかを検討します（図2）。別のネットワークを作成するためには、ファイアウォールをもう1台追加するか、またはファイアウォールのネットワークインターフェイスをもうひとつ追加します。こうすることで、公開するWebサーバーと他のクライアントコンピュータを明確に分離し、それぞれのネットワークに個別のセキュリティを設定できます。このとき、Webサーバーが配置されるインターネットでも内部ネットワークでもない中間のネットワークのことをDMZ（非武装地帯）と言います。

図1：一般的なWebサーバーの公開

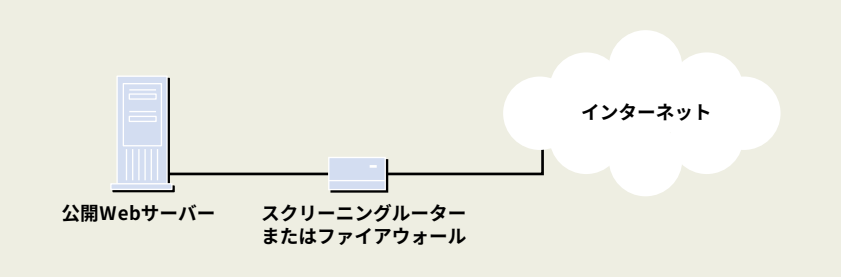
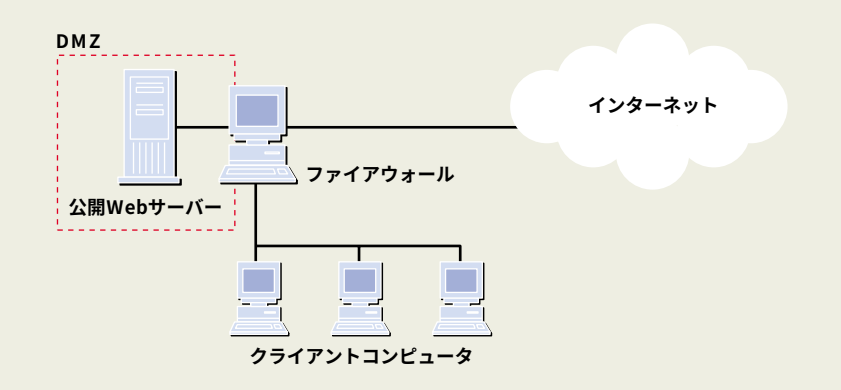


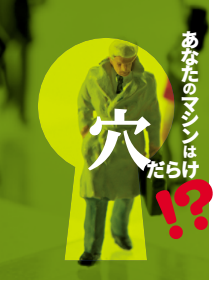
図2：ファイアウォール一台でDMZを構築した例



パーティションの作成とフォーマット形式を決定する

次にWindows 2000をインストールするときの注意です。Windows 2000をインストールする際には、OS用とコンテンツ用に最低2つのパーティションを作成しておいてください。これは悪意を持つ者が、あるパーティションの特定のフォルダへの侵入に成功した場合、同じパーティション内はディレクトリパスを移動するだけでアクセスが可能になるケースがあるからです。パーティションをわけることで、ディレクトリパスの移動による侵入を食い止めることができます。また、すべてのパーティションは、監査、アクセス許可の設定が可能なNTFSでフォーマットすることも重要です。もし、すでにFATでフォーマット済みのパーティションがある場合は、

```
convert ドライブ: /fs:ntfs
```



でNTFSに変換しておきます。

サービスパックや セキュリティアップデートを適用する

Windows 2000は洗練されたOSではありますが、人間が作った以上、完璧なOSではありません。特にセキュリティに関しては、毎日のように新しい問題が浮上しているのが現状です。そこでサービスパックやセキュリティアップデートを適用することが必要となります。サービスパックは定期的（予定では半年に1回）に提供されるシステムの不具合とセキュリティ問題を修正するプログラム集です。サービスパックは累積されているため、最新のサービスパックをWindows 2000に適用することで、Windows 2000登場直後からサービスパックが提供されるまでのすべての問題点を解消することができます。

しかし、サービスパックは定期的に発行されるため、サービスパックの提供後から次のサービスパックの提供までに発生したセキュリティの問題に対応することができません。そこでセキュリティアップデートが必要となります。セキュリティアップデートは、次のサービスパックの提供まで待てない重大なセキュリティの問題に対応するためのパッチです。ただし、なによりも即時性を重要視しているため、サービスパックのように適用後の動作検証は行なわれていません。よって、セキュリティアップデートを適用すると逆にシステムが不安定になる恐れもあります。そのため、セキュリティアップデートは自システムに該当する深刻な問題に対応するものだけを適用し、さほど重要ではない問題は次回のサービスパックで適用するといった手順をとることが推奨されています。

なお、最新のサービスパックとセキュリティアップデートは、マイクロソフトのWindows Updateのページ（http://www.microsoft.com/japan/windows2000/downloads/）から入手できます（図3）。

ローカルポリシーを構成する

Windows 2000には、さまざまなセキュリティパラメータがありますが、ユーザーに自由度を与えるため、そのほとんどは低いセキュリティレベルまたは無効となっています。当然、Webサーバーとして利用するのであれば、セキュリティレベルを引き上げる必要があります。

Windows 2000ではセキュリティパラメータを書き換えるために、ポリシーエディタを使い、ローカルポリシーを編集します（図4）。ポリシーエディタは、［スタート］メニューの［プログラム］-［管理ツール］-［ローカルセキュリティポリシー］で起動できます。ポリシーエディタでは、さまざまなポリシーが階層化されて管理されますが、セキュリティパラメータの設定はおもに［コンピュータの構成］-［Windowsの設定］-［セキュリティの設定］の［アカウントポリシー］と［ローカルポリシー］にまとめられています。

［アカウントポリシー］では、パスワ

図3：Windows Updateではサービスパックやセキュリティアップデートの最新情報を提供している

図4：ローカルセキュリティは集中化されたWindows 2000のセキュリティリポジトリである

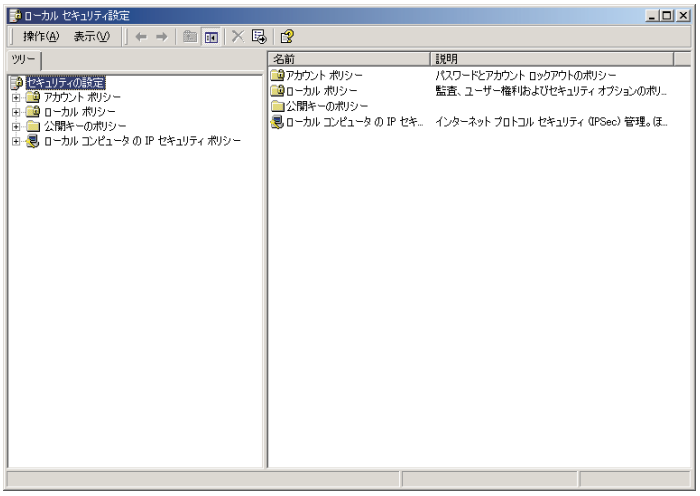


図5：パスワードのポリシーではパスワードの変更に体するポリシーを設定できる

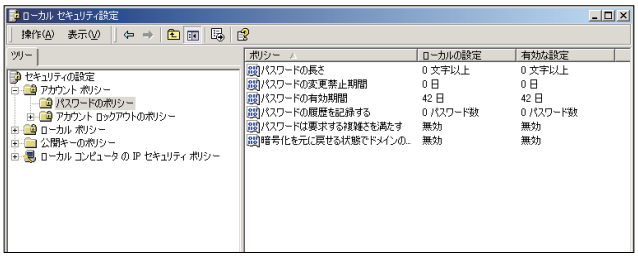
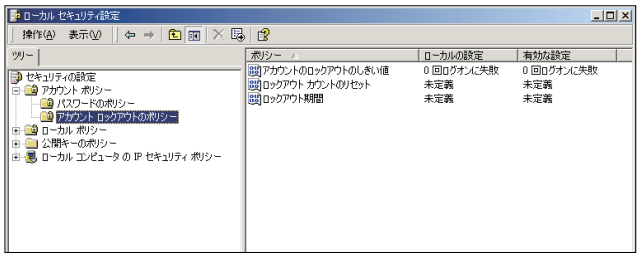


図6：アカウントロックアウトのポリシーはパスワード推測攻撃に有効なポリシー



ードのポリシーとアカウントのロックアウトのポリシーが設定できます。パスワードのポリシーには、パスワードの長さ制限、有効期間、過去に利用したパスワードを禁止する設定などが含まれています（図5）。これらも重要なセキュリティパラメータではありますが、Webサーバーのアカウントは管理者がすべて管理しているはずなので（一般ユーザーのためのアカウントを登録することはありませんよね）、それほど気にする必要はありません。これに対して、アカウントのロックアウトポリシーの設定は重要です（図6）。アカウントのロックアウトは、ログオン時、ユーザー名に対して誤ったパスワードを複数回、入力するとアカウントの利用を禁止（ロックアウト）する設定です。後述するパスワード推測攻撃からシステムを守る際に必要となります。ただし、アカウントのロックアウトポリシーを厳しく設定しすぎると、攻撃者はそれを逆手に取り、わざとさまざまなアカウントをロックアウトさせ、システム運用に支障を来す攻撃を仕掛けられることがありますので、バランスをとった設定が重要です。

［ローカルポリシー］では、「監査ポリシー」と「ユーザー権利の割り当て」、「セキュリティオプション」があります（図7）。監査ポリシーについては後述します。ユーザー権利は、各ユーザーまたはグループがこのコンピュータに対してもつ特権が設定できます。セキュリティオプションは、その他のセキュリティに関わる機能の設定です。

このようにたくさんのセキュリティパラメータがあると、各セキュリティパラメータの意味を理解し、最適な値を設定するのは、熟練の管理者でもなかなか大変な作業となるでしょう。そのため、マイクロソフトのWebサイトでは、セキュリティテンプレート（Hisecweb.inf）を公開しています（http://www.microsoft.com/technet/security/iis5chk.asp）。セキュリティテンプレートは、Webサーバーとして利用するWindows 2000のために推奨される設定集です。このセキュリティテンプレートを、ポリシーエディタでインポートし、必要な修正を加えた後、システムに適用すれば、ローカルポリシーの設定作業を大幅に減らすことができます。

管理者アカウントを変更する

Windows 2000の管理者アカウントは、administratorです。administratorは、システムに対する完全な権限をもつ唯一のユーザーで、administratorでログオンを行なえば、ファイルのアクセス許可の変更からユーザーアカウントの作成に至るまで、自由にシステムに変更を加えることができます。当然、侵入者はこのアカウントに興味を持ち、可能であれば、パスワードを入手したいと考えます。

では、侵入者はどのようにしてパスワードを入手するのでしょうか？　その例としてパスワード推測攻撃があります。パスワード推測攻撃は、推測したユーザー名とパスワードでログオンを試行し、ログオンが成功した場合には、そのユーザー名とパスワードが正しかったと判断する方法です。なお、パスワードの推測には、一般に「総当り（ブルートフ

図7：きめ細かい設定ができるローカルポリシー