特集 2

知っとかなくちゃ！

IIS 6.0 セキュア設定完全ガイド

マイクロソフト株式会社
望月 淳／内藤 仁
MOCHIZUKI, Atsushi／NAITO, Hitoshi

わかりにくいWebの設定もこれで完全掌握！

Webアプリケーションに関する重要な課題

Webアプリケーションの保護は、IT Pro、そしてWebデベロッパーにとって非常に重要で複雑な課題です。Webアプリケーションの設計と実装を行なう際に、そのアプリケーションをいかに保護するかは、必ず最初に検討すべき項目のひとつです。

最近ではASP.NETに対応したWebアプリケーションをさまざまなシーンで目にするようになりました。これほど多様なWebアプリケーションが稼動するようになるまで、セキュリティに関連したお問い合わせを多数いただきました。

たとえば……。

- 新しいWebアプリケーションを開発環境から本番環境に移行したら動作しなくなってしまった。
  - どうすれば問題発生を回避できるのか。
  - 最適な設定方法は何なのか。
- 既存のWebアプリケーションをイントラネット環境からインターネット環境に移行したい。
  - 認証方式のオプションはいくつかあるけれども、どれから検討すればいいのか。
- ブラウザからリクエストを受けてレスポンスを返すまでのプロセス、影響の範囲、セキュリティの設定方法はどうなっているのか。

いずれのケースを考えても、ASP.NETを基盤としたシステムやWebアプリケーションのセキュリティを適切に実装するためには、IIS 6.0そしてASP.NETを含めた一連の認証および承認の手段やメカニズムを明確に理解しておかなければなりません。もし、これらの理解があいまい、あるいは部分的であれば、そのWebアプリケーションのセキュリティは十分な対策がとられているとは言えません。

本稿は、WebデベロッパーがASP.NETベースのWebアプリケーションの設計と実装を行なう際に必要となるIIS 6.0およびASP.NETの認証／承認などのセキュリティ概念やメカニズムの概要について説明します。

これらの機能を利用した経験がないWebデベロッパーにとっては理解しにくいでしょう。セキュリティを実装するためのオプションが多岐にわたることに驚くかもしれません。しかし、本稿を読み、典型的なパターンや考慮すべきポイントを把握することで、最初の一歩としての基礎的な知識が身に付くはずです。

Level
1 2 3 4 (5)

Technology Tools
- ◯ Visual Basic
- ◯ Visual C#
- ◯ Visual C++
- ◯ SQL Server
- ◯ Oracle
- ◯ Access
- ◯ ASP.NET
- ✓ Other: IIS 6.0

ASP.NET Webアプリケーションにおけるセキュリティの要素

ASP.NETはWebアプリケーションに

適切なセキュリティを実装するために、IIS 6.0やASP.NET(.NET Framework)、およびオペレーティングシステムに用意されている基本的なセキュリティサービスと連携して動作しています。

そこで、まずはIIS 6.0とASP.NETの関係から整理していくことにしましょう。

IIS 6.0とASP.NETの関係

IIS 6.0とASP.NETはそれぞれが認証／承認制御の仕組みを持っています(図1)。アプリケーションを設定する際には、それらのセキュリティアーキテクチャの関係を理解しておく必要があります。

「私はデベロッパーだからIISについての理解は必要ない」というわけにはいきません。ASP.NETアプリケーションのセキュリティ構成とIISのセキュリティ構成は完全に独立しています。これらは互いに独立して、あるいは組み合わせて使用することになります。実際にクライアントがWeb要求を発行するとASP.NET Webアプリケーションにおける認証と承認は、

IISユーザー認証
↓
IISユーザー承認
↓
ASP.NETユーザー認証
↓
ASP.NETユーザー承認

の順番で行なわれます。

Webアプリケーションとデータベースの接続

昨今のWebアプリケーションでは、SQL Serverなどのデータベースをバックエンドリソースとして利用するケースが大半を占めていることでしょう。このような、SQL Serverと連携したWebアプリケーションにおいては、認証／承認の仕組みはさらに複雑になります。

ユーザーからみるとSQL Serverデータベースへのアクセスは、Webアプリケーションへの要求の送信とWebアプリケーションからSQL Serverデータベースに接続という2段階のプロセスとなります(図2)。

このシナリオについては最後に簡単に説明します。

図1：IIS 6.0とASP.NETのセキュリティ上の関係

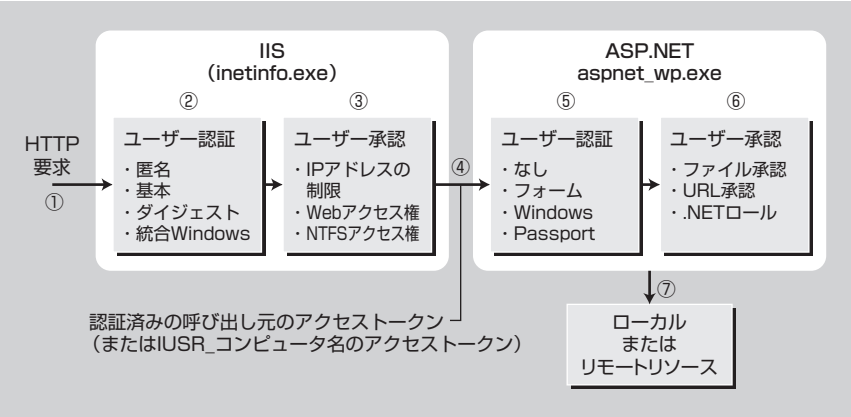
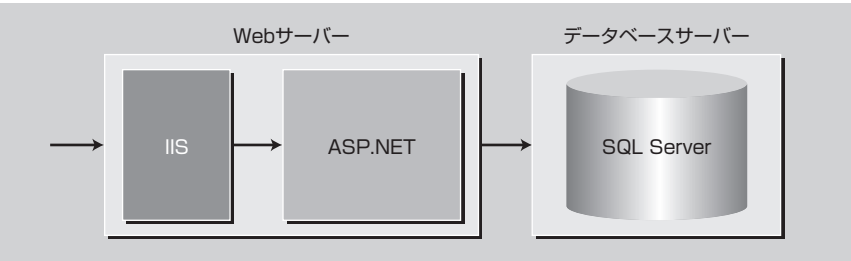


図2：SQL Serverを利用した2階層型ASP.NET Webアプリケーションの構成



まず最初に、セキュリティに関する作業を行なうには、Webアプリケーションのセキュリティ保護に関する2つの基本的な概念を理解する必要があります。「認証」と「承認」です。

「認証」とは、ユーザー名／パスワードなどのユーザーを識別するための資格情報をユーザーから取得し、それらの情報を証明機関に照会して検証するプロセスです。

「承認」とは、証明済みのアイデンティティに対して、特定のリソースへのアクセスを許可するかどうかを決定するプロセスです。Webアプリケーションも承認の機能を利用しています。

認証プロセスではユーザーの身元が確認され、その後の承認プロセスではユーザーが行なえる操作についての確認が行なわれます。

このように認証と承認には密接な関係があり、Webアプリケーションでは、IIS 6.0およびASP.NETの2種類のレベルで実行されます。