実践! 次世代C/Sシステム

クライアント/サーバー

スマートクライアント&Webサービスの実際

中垣 健志
NAKAGAKI, Kenji
株式会社CSKシステムズ
IT生産技術部

第5回

Webサービスでの認証

認証、承認の必要性

インターネットの普及に伴い、実に多くのものがインターネット上で購入できるようになりました。書籍やCD、電化製品、新幹線のチケットなどを、実際に売り場に行くことなく自宅（のPC）で注文し、そして受け取ることができます。

直接売り場で買い物をする場合は、売買という行為の中に“売り手”と“買い手”しか存在しません。そして売り手からみれば、買い手が目の前にいる人だということは明らかです。しかしインターネットを介した売買行為には、売り手と買い手の間に“アプリケーション”が存在します。売り手と買い手はアプリケーションを介してのみ情報をやり取りすることができます。そのためアプリケーションが「今アプリケーションを操作しているのが誰なのか」を把握していなければ、売り手は買い手を特定することができないのです。そのためにアプリケーションに、認証と承認という機能を実装する必要があります。

そこで今回の連載では、この認証／承認の説明と、スマートクライアントでこれらの機能を実装するにはどうすればよいのかについて解説していきます。

レベル >>> Level

1 2 3 4 (5)

言語 >>> Language

- Visual Basic
- C#

ツール >>> Tool

- Visual Studio 2005 Professional
- SQL Server 2005

サンプル >>> Sample

この記事で取り上げたソースコードおよびサンプルプログラムは、
http://www.shoeisha.com/mag/windev/
からダウンロード可能です。

認証と承認の基礎

※認証ってなに？

認証とは、今利用しているユーザーが誰なのかをアプリケーションが認識するための仕組みです。認証の概念を理解してもらうために、ここでは「家で留守番をしている子供」を例にとって説明してみましょう。

さて、家に誰かが訪ねてきました。子供は玄関の覗き穴（いまどきならTV付きインターホンですね）から、来た人が誰かを認識します（図1）。

家は「アプリケーション」、子供は「アプリケーションの認証機能」、家を訪ねてくる人が「アプリケーションを利用するユーザー」に相当します。

図1：認証を行なう

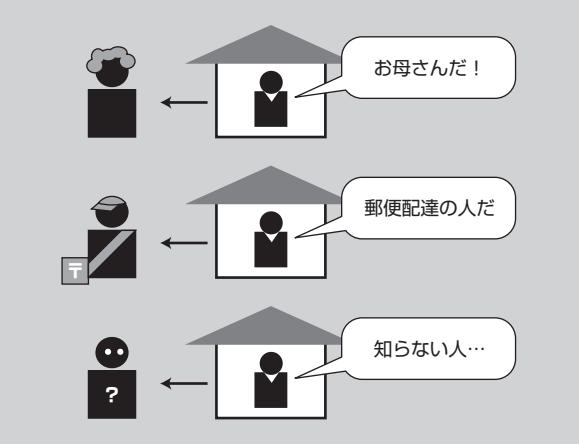
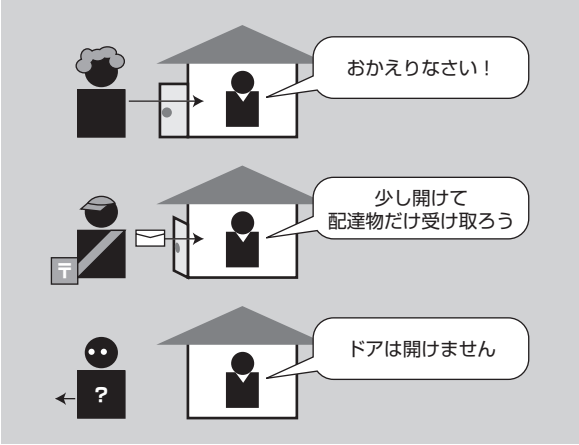


図2：承認方法に合わせて対応する



※承認ってなに？

承認とは、認証したユーザーに対して何ができて何ができないのかを判断することです。再び「家で留守番をする子供」を例にとって考えてみましょう。

訪問者がお母さんの場合は、子供にとって信頼できる相手ということがすでにわかっているため、鍵をはずしドアを開けて家の中に迎え入れます。郵便配達の人は危ない人ではありませんが、念のためにチェーン鍵をかけてから鍵をはずしドアを半開きにして手紙を受け取ります。そして知らない人の場合には、鍵をはずさずドアも開けずに帰ってもらいます（図2）。

このように認証したユーザーにより異なるレベルで対応することが、承認処理に当たります。

※ロールについて

先ほどの例では、留守番をしている子供はお母さんという“個人”に対して「ドアを開けて迎え入れる」という承認処理を行ないました。しかし郵便配達の人に対してはどうでしょうか？　今回この家に郵便配達に来た人を、仮に山田さんとします。次の日は山田さんではなく伊藤さんが郵便を届けにくるかもしれません。この場合、留守番をしている子供に対して「山田さんだったら○○、伊藤さんだったら××」と個人個人についてどう対応するのかを説明するよりは、まとめて「郵便配達の人ならば△△」と説明するほうが簡潔です。つまり子供は家に来た人の個人情報を見るのではなく、「その人がどのような“役割”を持っているのか」ということを元に承認処理をすることになります。役割とは英語で「ロール」を意味します。このように、個人（ユーザー）単位ではなく役割（ロール）単位で承認を行なうこと[注1]がAAfNでは推奨されています。

.NET Frameworkにおける認証と承認

.NET Frameworkでは、認証、承認、ロールに対してそれぞれ対応するクラスやメソッドが用意されています。

※IIdentityインターフェイス

認証を行なうためには少なくとも、今利用しているユーザーをアプリケーションが一意に識別できる必要があります。またアプリケーションによっては、性別や生年月日といったそのユーザーの個人情報を必要とすることもあります。

IIdentityインターフェイスは、そのような情報を保持するクラスのために用意されたインターフェイスです。アプリケーション内に用意された認証処理では、IIdentityインターフェイスの派生クラスを生成する必要があります。IIdentityインターフェイスの派生クラスでは、最低でも次の情報を持つ必要があります。

注1）「ロールベースのセキュリティ」と呼ばれています。