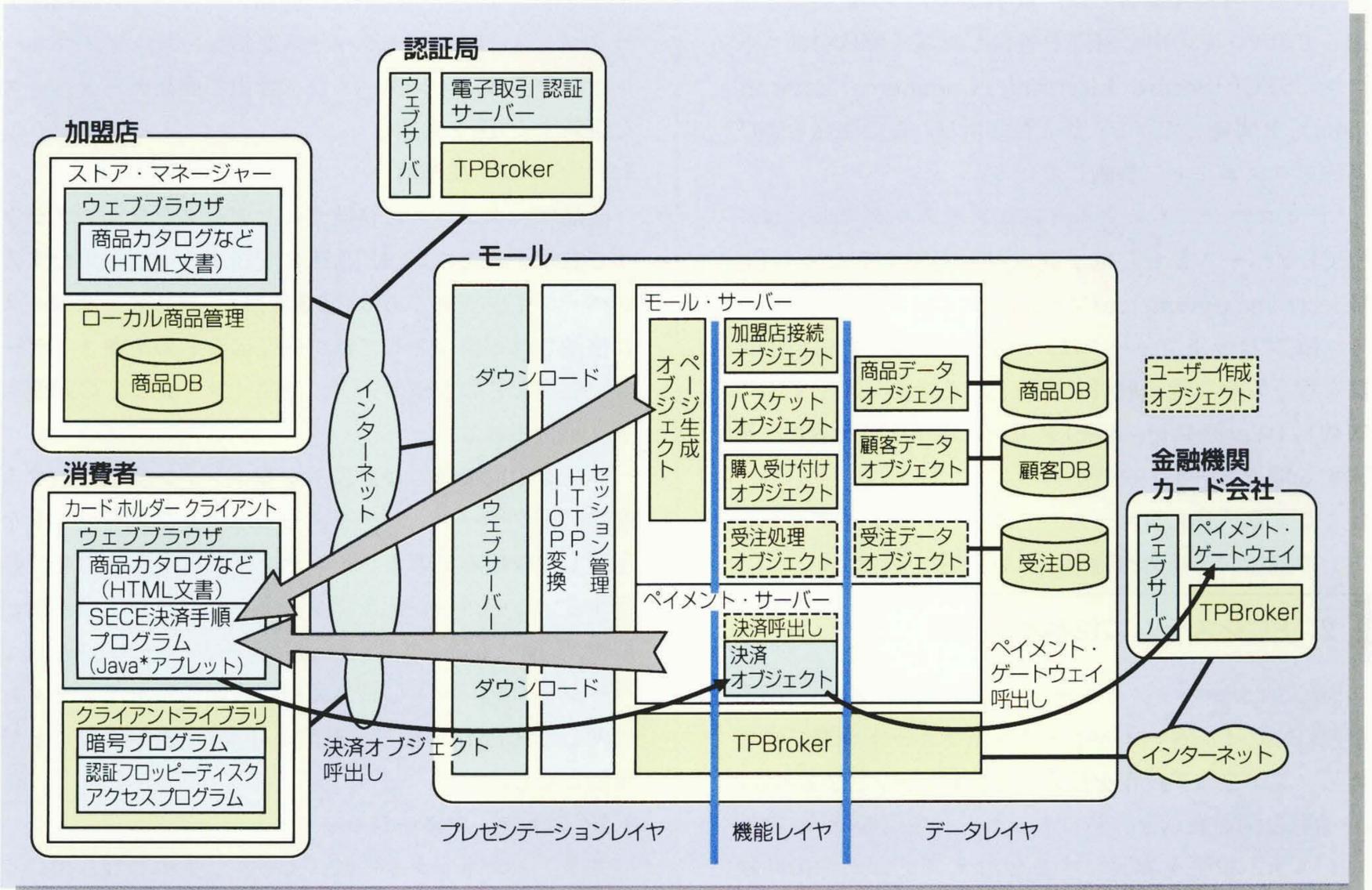


ECシステムのソフトウェアプラットフォーム

Software Platform for Electronic Commerce System

増石 哲也 Tetsuya Masuishi 福岡 寛 Hiroshi Fukuoka
 新田 淳 Jun Nitta 吉村紀久雄 Kikuo Yoshimura



注：略語説明ほか HTML (Hypertext Markup Language), DB (Database), SECE (Secure Electronic Commerce Environment)
 HTTP (Hypertext Transfer Protocol), IIOP (Internet Inter-ORB (Object Request Broker) Protocol)
 * Javalは、米国およびその他の国における米国Sun Microsystems, Inc.の商標である。

「日立コマース・ソリューション・プロダクト」の構造

モール・サーバー、ペイメント・サーバー、ペイメント・ゲートウェイ、ストア・マネージャー、およびカードホルダークライアントがインターネット経由で動作する。この結果、インターネット上で安全性の高い決済を実現する。

インターネットとWWW(World Wide Web)の普及は、大きな社会的インパクトを与えている。インターネットをベースとしたEC(Electronic Commerce:電子商取引)の市場が立ち上がりつつあり、また、インターネットの技術を用いて企業情報システムも構築しようとする動きが盛んになっている。

日立製作所は、インターネット上で安全な商取引を実現するためのソフトウェア製品を、「日立コマース・ソリューション・プロダクト」として提供している。この製品は、電子店舗を実現するためのモール・サーバー、電

子認証を実現する電子取引認証サーバー、認証に基づいた安全性の高い決済を実現するためのペイメント・サーバーとペイメント・ゲートウェイなどで構成している。

「日立コマース・ソリューション・プロダクト」は、安全性の高い商取引を実現するためのSECE(Secure Electronic Commerce Environment)プロトコル、クライアントアプリケーションをサーバから動的にロードして実現するJava、ネットワーク上にソフトウェア部品を分散させてシステムを実現するための分散オブジェクトなどの最新技術を組み合わせて開発したものである。

1. はじめに

インターネットで電子商取引を行う場合に問題視されているのが、安全性の問題である。このための解決策として、暗号技術を用いて安全性を確保した決済プロトコル“SET(Secure Electronic Transaction)”が米国で開発された。通商産業省では、電子商取引の実証実験を推進しており、その中でSETを包含した電子商取引プロトコル“SECE(Secure Electronic Commerce Environment)”を開発している。日立製作所は、この開発および実験プロジェクトに参画している。

「日立コマース・ソリューション・プロダクト」は、SECEをベースとした電子商取引を実現するためのEC(Electronic Commerce)プラットフォームを提供している。ECプラットフォームは、SECEに準拠した決済・認証を行う安全な電子取引の機能と、インターネット上にWWW(World Wide Web)を用いた電子店舗を管理、運営する電子モールの機能を持つ。

ここでは、「日立コマース・ソリューション・プロダクト」の機能的・構造的特徴について述べる。

2. ECシステムに使われる技術

「日立コマース・ソリューション・プロダクト」(図1参照)には、インターネット・イントラネット分野での最新のソフトウェア技術を投入している。その主なものは、(1)柔軟な画面表示を容易にするページ生成機構、(2)柔軟なシステム拡張を容易にする分散オブジェクト指向技術、(3)安全性を高める暗号技術、(4)軽いクライアントを実現するJava技術である。

3. 電子モールの構造

「日立コマース・ソリューション・プロダクト」は、電子モールを構築、運用するためのソフトウェアとしてモール・サーバーを、また、電子店舗を運営するためのソフトウェアとしてストア・マネージャーを提供している。

モール・サーバー内では、店舗データベース、商品データベース、顧客データベースを持つ。ストア・マネージャーからは、インターネット経由で商品データベースを更新する(図2参照)。

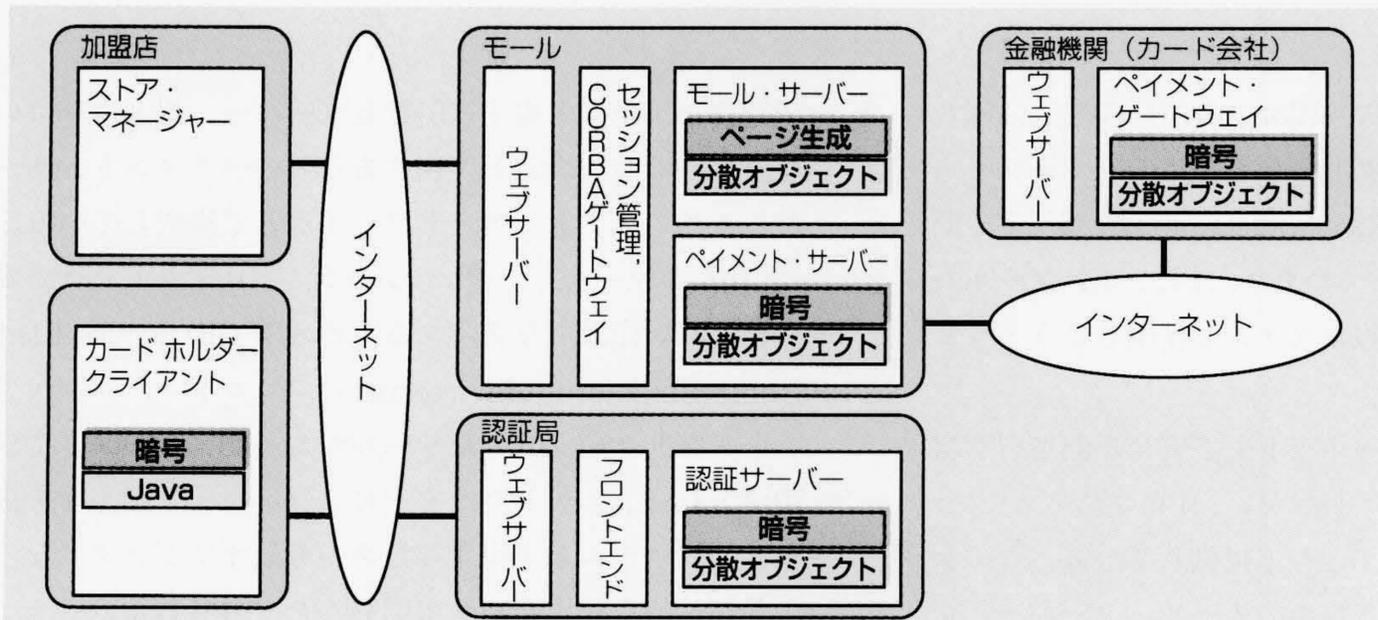
3.1 ページ生成機構

商品データベースに格納されたデータをウェブブラウザで表示するために、HTMLに変換する役割を果たすのがページ生成機構である(図3参照)。商品データベースに格納される情報としては、商品名などのテキストデータ、価格などの数値データ、商品イメージなどの画像データが含まれる。

ページ生成機構では、表示するコンテンツを格納する商品データベースと、データを表示するフォーマットを記述した枠組みであるページテンプレートを入力して動作する。このページテンプレートを、ページ生成機構が解釈、実行することによって商品データベースを検索し、ページテンプレートの該当個所に検索情報をインライン展開してHTMLの内容を動的に作成し、表示することが可能になる。

3.2 ストア・マネージャー

ストア・マネージャーは、モールで集中管理している商品データベースをインターネット経由で店舗から更新する機能と、モールで取り扱った購入申し込みの情報を



注：略語説明
CORBA(Common Object Request Broker Architecture)

図1 「日立コマース・ソリューション・プロダクト」に使われる技術

ページ生成機構、分散オブジェクト指向技術、暗号技術、およびJava技術を使って安全性の高い柔軟な電子商取引システムを実現する。

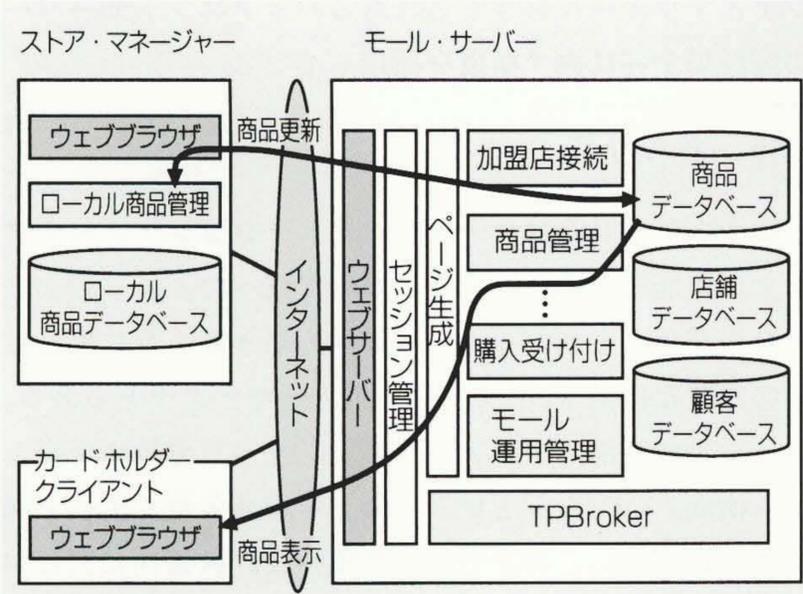


図2 モール・サーバーとストア・マネージャー

モール・サーバーの商品データベースのデータを、ページ生成機構がHTMLに変換して、カードホルダークライアントのウェブブラウザに表示する。ストア・マネージャーは、加盟店接続機構経由で商品データベースを更新する。

店舗システムにダウンロードする機能を持つソフトウェアである。図4に示すような画面から入力されたデータを、http(Hypertext Transfer Protocol)でモール・サーバーの中の加盟店接続モジュールに通信する。

また、店舗側のデータベースを核として、ECのための店舗システムを拡充していくことができるようになっていく。

3.3 カスタマイズ

電子モールは、モール運営者の方針によって機能が大きく変わる可能性を持つ。モール・サーバーでは、プログラムインタフェースを公開することにより、このようなカスタマイズのニーズに対応できるようにしている。

モールには大きく分けて、会員制のものとそうでない

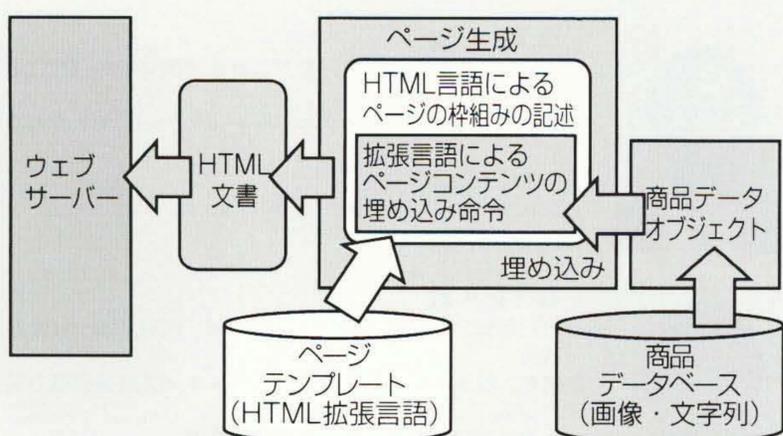


図3 ページ生成の方式

ページ生成機構では、ページテンプレートと言うページのフォーマットを記述した枠組みの中に、商品データベースの中の文字列や画像を埋め込んでHTMLを生成する。



図4 ストア・マネージャーの商品登録画面

この画面から入力したデータが、インターネットを経由して、モール・サーバーの商品データベースを更新する。

ものがある。会員制のモールでは、モールに入ると同時にユーザー名を聞くことが必要となる。ページテンプレート中に、HTML拡張言語を用いてアクションの切り分けを指定することにより、このような制御が行える。

商品の送料は、計算法が地域や商品に大きく依存する。モール・サーバーでは、このような部分についてインタフェースを公開し、カスタマイズを行えるようにしている。

3.4 拡張性

モール・サーバーは、CORBA(Common Object Request Broker Architecture)準拠の分散オブジェクト基盤ソフトウェア“TPBroker”をベースに開発されているため、ソフトウェア部品を追加してつなぎ換えるだけで、比較的容易に機能拡張が可能である。

4. SECEプロトコルの実現

「日立コマース・ソリューション・プロダクト」では、SECEクレジットカード決済機能を提供している(SECEのクレジットカード決済機能は、ビザとマスターカードが主導で制定した国際標準“SET”に準拠している。)。ショッピング時の実際の決済はペイメント・サーバーが担当する。ここでは、公開鍵暗号〔鍵長が1,024ビットのRSA(Rivest, Shamir, Adelman)〕と秘密鍵暗号〔鍵長が56ビットのDES(Data Encryption Standard)〕を使って高い安全性を実現している。

4.1 ペイメント・サーバーでの電子決済

クレジットカード決済は、カードホルダークライアントと、ペイメント・サーバー、およびペイメント・ゲートウェイの3者間の通信で実行される(図5参照)。こ

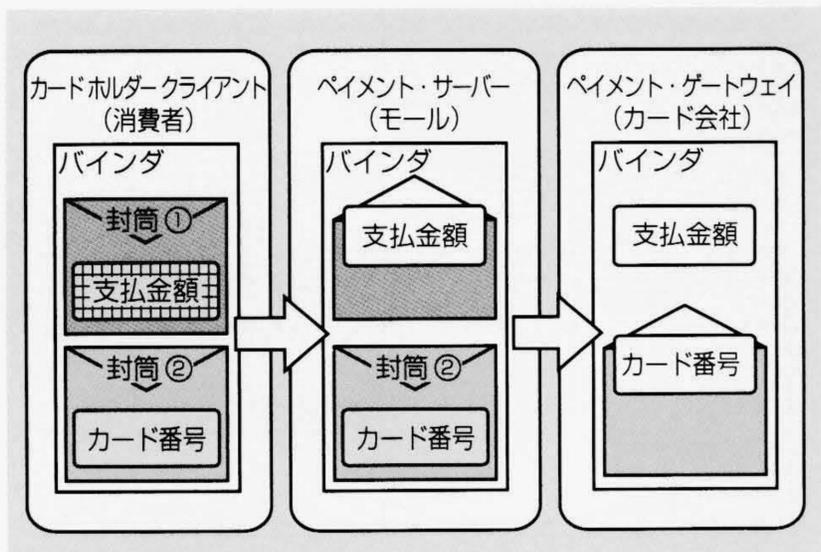


図5 SECEカード決済の仕組み

支払金額とカード番号は、それぞれ別の封筒に入れて(別の鍵で暗号化して)送られる。支払金額の入った封筒①はペイメント・サーバーで開封(復号化)できるが、カード番号の入った封筒②はペイメント・ゲートウェイでしか開封できない。また、封筒①よりも封筒②のほうが頑丈(より強い暗号)である。

こでの、安全性から見た特徴は以下の点にある。

- (1) データの暗号化とデジタル署名の併用により、盗聴防止と改ざん防止が保証される。
- (2) 安全性が特に要求されるクレジットカード番号では、通常データよりも強い暗号で保護している。
- (3) クレジットカード番号は、ペイメント・ゲートウェイだけが解読可能である(モールに置かれるペイメント・サーバーではカード番号を見ることはできない)。

もう一つの特徴は、カードホルダークライアントで行う処理を、ローカルにインストールしたプログラムと、サーバから動的にダウンロードしてくるJavaアプレットに2分割したことである。前者は、今後現れるさまざまな決済手段(銀行決済や電子マネーなど)に共通に使える汎用決済部品であり、後者がクレジットカード固有の処理を担っている。

4.2 電子取引認証サーバーの構造

公開鍵の証書(印鑑証明に相当)を発行するのが、電子取引認証サーバーである。

電子取引認証サーバーの主な機能は、ユーザーからの要求に応じて証書を発行する機能、発行した証書を維持、管理する機能、および証書の発行を承認する機能であり、これらもオブジェクトとして実装されている(もちろん、暗号機能も使っている)。電子取引認証サーバーには、インターネット側からのメッセージをフロントエンドサーバーでいったん受けて十分なチェックを行ってから、

ファイアウォールのうしろにあるバックエンドサーバーの認証局業務に渡す構成を採用している。

5. おわりに

ここでは、「日立コマース・ソリューション・プロダクト」の機能的・構造的特徴について述べた。

今後発生する新たなニーズに対応できるようにするための重要な技術は、ソフトウェアアーキテクチャである。ページ生成機構、ストア・マネージャー、分散オブジェクト指向、Javaなどといった考えを取り入れて実装を図ることにより、これまでよりも柔軟な、拡張性に富むシステム構築の基盤が実現できると思われる。今後も、この製品をより良いシステムとするために展開を図っていく考えである。

参考文献

- 1) 山本, 外: 新しい社会インフラストラクチャーとしての電子商取引を支える「日立コマース・ソリューション」, 日立評論, 79, 4, 381~384(平9-4)

執筆者紹介



増石 哲也

1983年日立製作所入社, 情報・通信開発本部 所属
現在, 電子商取引システム, ソフトウェア開発環境の開発に従事
情報処理学会会員
E-mail: masuishi@isrd.hitachi.co.jp



新田 淳

1982年日立製作所入社, 情報・通信開発本部 所属
現在, 電子商取引システム, トランザクションモニタの開発に従事
情報処理学会会員
E-mail: nitta@isrd.hitachi.co.jp



福岡 寛

1975年日立製作所入社, ソフトウェア開発本部 第2 DC設計部 所属
現在, 電子商取引システム, セキュリティシステムの開発に従事
情報処理学会会員
E-mail: fukuoka@soft.hitachi.co.jp



吉村紀久雄

1972年日立製作所入社, ソフトウェア開発本部 AI設計部 所属
現在, 電子商取引システム, ソフトウェア開発環境の開発に従事
情報処理学会会員, 人工知能学会会員
E-mail: yoshimur@soft.hitachi.co.jp