電子マネーシステム「モンデックス」の新展開

New Trends of the Digital Money System “Mondex”

山下廣太郎 *Kôtarô Yamashita* 田代 勁 *Tsutomu Tashiro*
村松 晃 *Akira Muramatsu*

モンデックスマネーの流れ

モンデックス利用の仕組み
低価格で，洗練された機器類とネットワークが，銀行，小売店，消費者を結び付ける。

“Mondex[※1](モンデックス)”は，現行通貨の電子化を究極のねらいとした電子マネーシステムである。銀行群が運営するオリジネータと呼ぶ機関が現金と引き換えに発行したモンデックスマネーは，現金とまったく同様に商品の購入に使えるほか，個人間で受け渡しすることもできる。オフライン環境でこのような価値の移転を安全に実行することができるように，マネーとその移転のための手続き一切がICカードに封入されている。ICカード内の情報にアクセスするためには上図に示すような各種装置が必要であり，これらの電子マネーインフラストラクチャーを高信頼かつ低価格で提供することは，日立製作所のようなメーカーに課せられた使命である。今，全世界規模でモンデックスの新しい展開が始まっている。

まず，モンデックスインターナショナルが設立され，全世界の銀行が英知を集めて運営する体制が出来上がるとともに，英国に引き続きカナダや香港など世界各地で実験が始まっている。また，マスターカードによってモンデックスが買収され，クレジットカードのICカード化に合わせて，全世界の加盟店でモンデックスが利用できる体制が出来つつある。

一方，技術面でも暗号処理を高速化した新チップが登場し，１枚のカードでモンデックスだけでなくクレジットやGSM(欧州の携帯電話)など複数のアプリケーションが実行できる環境が開発されつつある。さらに，インターネット上でモンデックスによる支払いを行う実験が計画されており，日立製作所はこれらすべての技術的進展に深く関与している。

1. はじめに

1995年に英国スウィンドン市で実験が開始された電子マネー「モンデックス」は，1996年後半に至って全世界的規模での普及の兆しが見え始めてきた。米国，香港，カナダでも実験が始まり，さらにオーストラリア，ニュージーランド，フィリピンでも計画が進んでいる。この背景には，1996年7月のモンデックスインターナショナル社(以下，MXIと言う。)設立による経営基盤のグローバル化がある。

また，クレジットカード会社であるマスターカードがモンデックスの経営権を掌握することが合意された。これにより，世界中のマスターカード加盟店が，将来モンデックスを利用できるショップとして期待されるようになった。

このような利用面での展開とともに，技術面でも新しい動きが活発化し，チップが新しい暗号処理用コプロセッサ付きの新タイプに変わろうとしている。これにより，従来品に比較してバリュー転送時間の短縮と暗号鍵長の増加によるセキュリティの大幅な向上が期待される。

また，1枚のカードで複数の能動的アプリケーションが動作するマルチアプリケーション環境の開発が進んでいる。これにより，例えばモンデックスとクレジットが1枚のICカードで利用できるだけでなく，さらにGSM(欧州の携帯電話標準規格)や各種ロイヤルティプログラムなどが利用できるようになり，新種のコンピュータプラットフォームとして注目を集め始めている。

一方，インターネットを中心とするサイバスペースでもモンデックスの利用が進められている。インターネット上で実用に耐える支払い手段として定着するまでには多くの解決すべき課題があるが，日立製作所はインターネット関連の各種モンデックス機器の計画のほかに，電子決済の標準プラットフォームを目指すSECE(Secure Electronic Commerce Environment)上でモンデックスが利用できる新技術“SET/e-money”の開発に着手している。

ここでは，電子マネーシステム「モンデックス」の展開について，ビジネスと技術の両面から述べる。

2. モンデックスのグローバルな展開

2.1 地理的な展開

1995年7月から英国スウィンドン市で始まったモンデックスの実用化実験では，大きなトラブルもなく技術的に深刻な問題がないことが確認されている。現時点で，このような真に実用的な技術水準に達しているのは，ベルギーの電子マネー“PROTON”とモンデックスの2種類だけであると言われている。

スウィンドン市に続いて米国サンフランシスコ市のWells Fargo銀行本店周辺で小規模な実験が行われ，また1996年10月から香港で香港上海銀行グループによって本格的な試用が開始された。これは実験ではなく，“Soft Launch(軟発進)”と呼ばれている。市内の三つの大きなショッピングセンターで約400店舗が参加して行われており，すでに4万枚近いカードが発行されている。

カナダではトロントの近くのグゥエルフ市で実験が始まり，Royal Bank of Canada と Canadian Imperial Bank of Commerceの2銀行が推進している。英国のエクセター大学，ヨーク大学では学生証と兼用のモンデッ

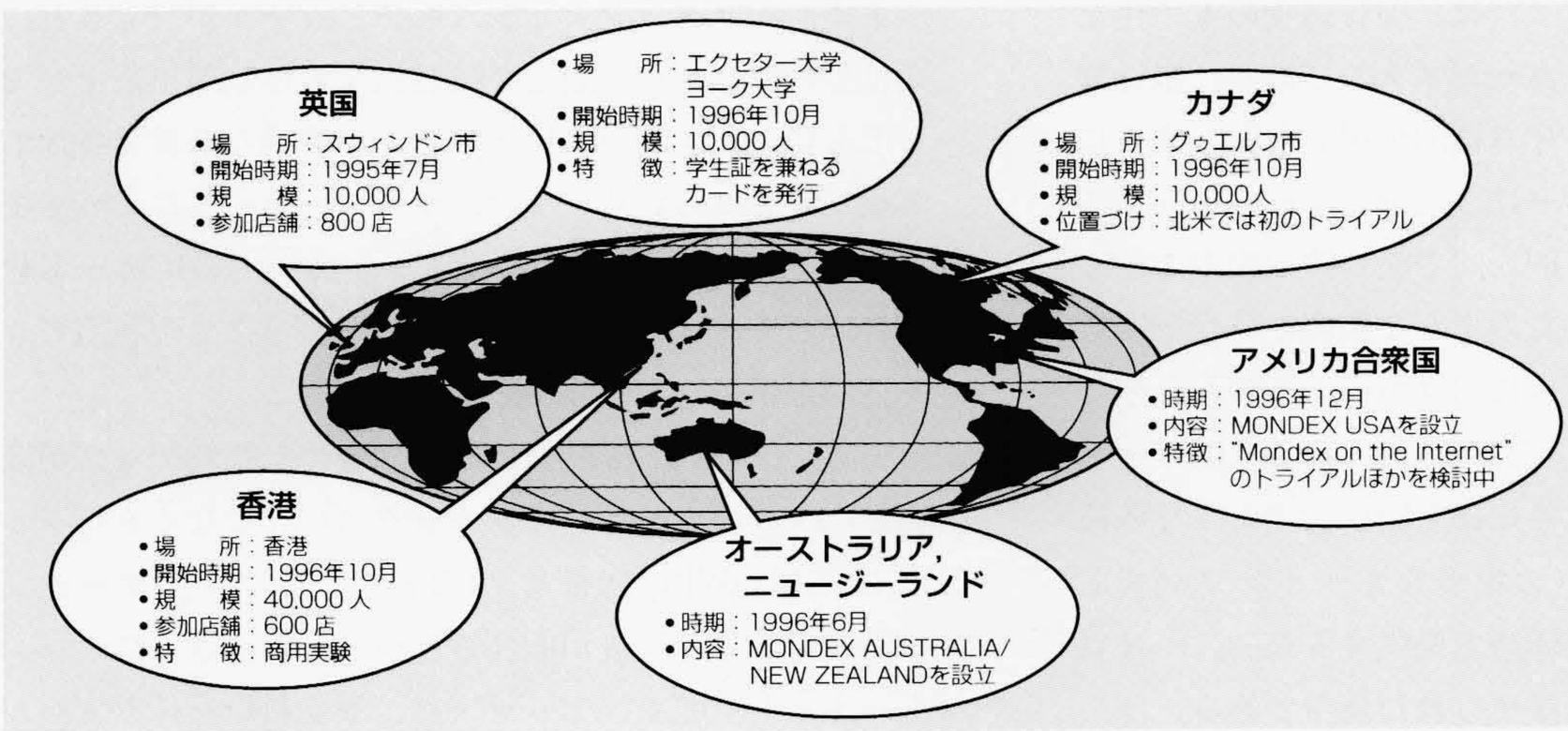


図1　世界各国におけるMondexの実施状況(1997年1月現在)
英国や米国等のほかに，コスタリカや，フィリピン，中国，韓国など，全世界的規模で検討が進んでいる。

※1)　Mondexは，Mondex International Limitedの登録商標である。

クスが登場した。さらに，オーストラリアとニュージーランドでは，上位銀行集団によってモンデックスの導入が決定されており，ニュージーランド最大のウェストパックトラスト銀行では，日立製作所のモンデックス製品・システムを用いた行内トライアルが行われている。そのほか，コスタリカやフィリピンでも計画が進んでいる(**図1**参照)。

2.2　経営面での新展開

1996年11月18日，マスターカードインターナショナル社はMXIの株式の51%を取得することで合意した。マスターカードによるMXIの買収である。これに伴って世界中の約1,270万店のマスターカード加盟店で，将来，モンデックスが利用できるようになるものと期待されている。

元来モンデックスのビジネススキームは銀行が中心となって運営し，銀行がその収益を得る仕掛けとなっている。そこに銀行ではないクレジット業界が参入し，しかも経営権を握るということは，わが国のようなクレジット会社と銀行が画然と区別され，しかも監督官庁も異なる社会からは，一種の混乱と見えるかもしれない。しかし，欧米では銀行もクレジットカードを発行し運用しているので，わが国のような違和感は存在しない。むしろ，実際の商店で利用されるためには，クレジット加盟店ネットワークの利用が有効であることは当初から指摘されており，クレジットカード側にとっても，少額決済はクレジットよりも電子マネーで行うことが望ましいという共通の認識が存在していた。その意味で，マスターカードによる買収は自然な動きであると思われる。

2.3　グローバルな電子マネーへ

マスターカードがMXIを買収したことにより，真の電子マネーと言われるモンデックスを，ビザやアメリカンエクスプレス(AMEX)その他のクレジットカード会社が採用する可能性はさらに大きくなったと考える根拠がある。それは，“EMV”や“SET”の開発という前例があるからである。“EMV”は，その頭文字をとったEuropay，Mastercard，VISAというクレジットカード大手3社が共同で定めたICカードの規格である。これは，各クレジットカード会社がそれぞれ独自規格のICカード版クレジットカード用端末を定めるのでは加盟店の支持が得られないと認識した結果，共同開発されたものである。

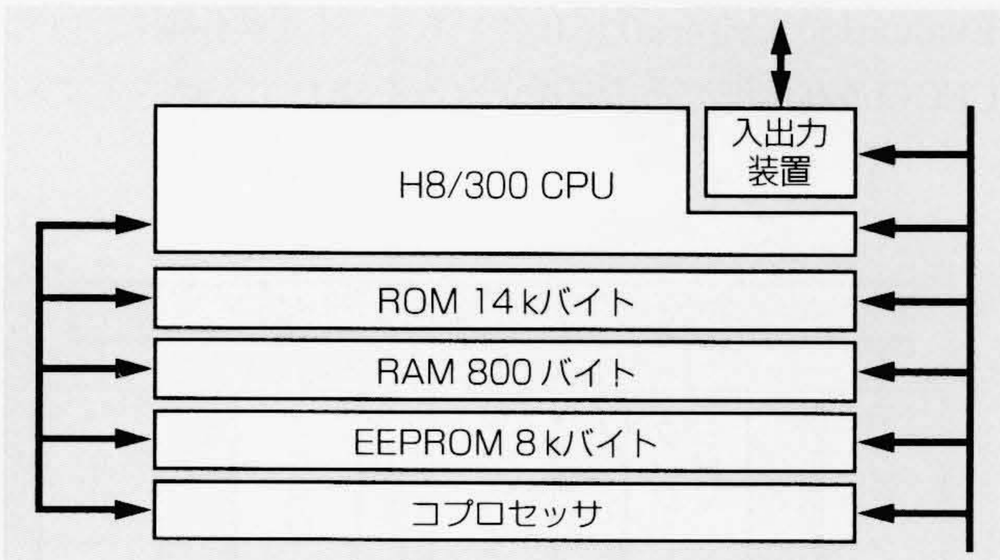
EC(Electronic Commerce)分野でのSET(Secure Electronic Transaction)も同様である。インターネット上でのクレジットカード利用のための取引手順であるSETは，米国IBM社のiKP(internet Keyed Payment Protocol)を基に，マスターカードとネットスケープ社がSEPP(Secure Electronic Payment Protocol)を，ビザとマイクロソフト社がSTT(Secure Transaction Technology)をそれぞれ競って開発していたが，前述と同じ理由で，協調して開発することにした結果の産物である。これは，いわゆるデファクトスタンダード一本やりのコンピュータ業界のアプローチとは一線を画すものであり，モンデックスの展開を占ううえで忘れてはならない点である。

3．技術面での新しい動き

3.1　新チップ

従来のモンデックス用チップ(日立製作所のH8/3102チップ)は，1997年には新しい仕様のチップに切り替わる。より高速にバリュー転送ができ，しかも長い暗号鍵を使うことができるため，セキュリティが飛躍的に高まると期待されている。

新チップは，H8/3111と呼ばれる0.8ミクロンチップと基本的に同一である。3111チップは暗号処理用のコプロセッサを内蔵しており，RSA(Rivest，Shamir，Adelman)の長ビット暗号キー演算(Modular Multiplication)をリアルタイムに実行できる(**図2**参照)。すなわち，このチップはEMVのDDA(Dynamic Data Authentication)に対応しており，もちろんモンデックスにも対応できる。耐タンパ性と呼ばれる不法な攻撃に対する耐性も向上したこの新チップに対して，OS(Operating System)も一新され(MXI MM4)，MXIではこの新しい仕様をロールアウトバージョンと呼んでいる。



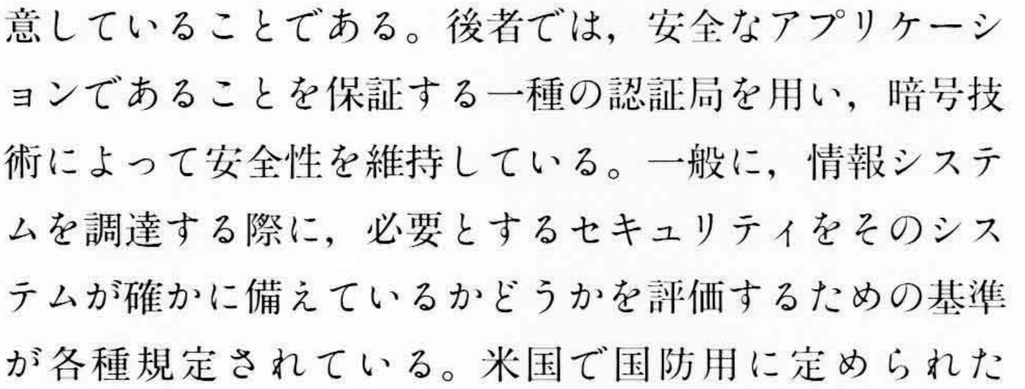
注：略語説明
CPU(Central Processing Unit)
ROM(Read-Only Memory)
RAM(Random Access Memory)
EEPROM(Electrically Erasable Programmable ROM)

図2　H8/3111チップ
暗号処理用のコプロセッサを搭載し，処理の高速化と鍵長増大によるセキュリティ向上を実現する。

3.2　マルチアプリケーション用カードOS

マルチアプリケーション用カードOSは，高性能化したICカード内で複数の能動的アプリケーションを動作させるための環境であり，MXIが仕様を開発した(**図3**参照)。ここで，能動的アプリケーションとは，実行できるデータ処理プログラムを指す。従来のICカードは単なるファイルであった。それはディレクトリ構造を持ち，端末側が要求するファイルを提供する媒体であった。これに対し，モンデックスなどの電子マネー用ICカードでは，小規模ながらプログラムが動作する。受け付けたコマンドに従って暗号処理を行い，残高を計算してこれを新しい値に変更し，履歴を更新してアクセス制御情報を管理する。このようなプログラムを複数独立に動作させるための環境が，マルチアプリケーション用カードOSである。

このOSは，単に複数の能動的アプリケーションを動作させるだけでなく，そのセキュリティを高い水準で確保できる点に特徴がある。すなわち，(1)インタープリタ言語でアプリケーションを記述すること，(2)不正なアクセスをチェックする機構が内蔵されていること，(3)アプリケーションを安全にロード・デリートできるローダを用意していることである。後者では，安全なアプリケーションであることを保証する一種の認証局を用い，暗号技術によって安全性を維持している。一般に，情報システムを調達する際に，必要とするセキュリティをそのシステムが確かに備えているかどうかを評価するための基準が各種規定されている。米国で国防用に定められたTCSC(Trusted Computer Security Evaluation Criteria)や，EC(英国，ドイツ，フランス，オランダ)が定めたITSCEC(Information Technology Security Evaluation Criteria)が有名である。日立製作所は，ITSCECの最高水準であるE6レベルを満たすものとしてマルチアプリケーション用カードOSを開発する計画である。



注：略語説明　OS(Operating System)
EMV(Europay, Mastercard, VISA)
GSM(欧州の携帯電話標準規格)

図3　マルチアプリケーション用カードOS
1枚のカードが多目的に使え，ICカードを新種のコンピュータプラットフォームにする。

マルチアプリケーション用カードOSの導入により，1枚のモンデックス用ICカードでモンデックスだけでなく，クレジットや各種ロイヤルティプログラム，交通料金支払い機能，GSMなどのアプリケーションが実装できる。ただし，現状のメモリ容量から考えると，当初は2～3のアプリケーションに限定されると思われる。またこのOSの開発を契機に，日立製作所だけでなく，ほかの半導体メーカー(モトローラ社，シーメンス社など)とも協調する動きがある。

複数の能動的アプリケーションをICカード上に実装するアプローチは，われわれのマルチアプリケーション用カードOSだけのものではない。サンマイクロシステムズ社のJavaCard[※2)]も同様のねらいを持ったソフトウェア環境である。この技術により，Javaで書かれたアプリケーションはICカードからPC(Personal Computer)，メインフレームまでの幅広いプラットフォームで実行できるようになる。すでに8kバイトのEEPROMを内蔵するモトローラ社製SC49チップを用いたシュランバーガー社の「サイバーフレックス」と呼ぶJavaコンパチブルなICカードが発表されている。JavaCardとMXI－日立製作所のマルチアプリケーション用カードOSとの違いは，スケーラビリティだけではなく，プログラムのマイグレーションやセキュリティに及ぶ。広範な支持を集めているJava言語の存在を考えると，将来の可能性として，スケーラブルなJavaCardとMXI－日立製作所のマルチアプリケーション用カードOSとのセキュリティの融合も考えられる。

3.3　Mondex on the Internet
(インターネット上で利用するモンデックス)

モンデックスをインターネット上での支払いに利用する実験が，MXIと米国AT&T社などで計画されている。しかし，実用水準でモンデックスを利用するためには，以下のような多くの課題を解決しなくてはならない。

(1)　ファイアウォールの通過

モンデックスのバリュー転送プロトコル(Mondex Payment Protocol)は，交信するチップどうしの直接会話形式である。すなわち，両チップ間で暗号化された数回のメッセージをやり取りして，会話が成功裏に終了した時点でバリュー転送が完了する仕掛けとなっている。

※2)　Javaは，米国およびその他の国におけるSun Microsystems, Inc.の商標である。

このため，プロキシサーバが片方のチップの代わりを務めてバリュー転送を仲介することはできず，何らかの手段でファイアウォールをモンデックスメッセージが通過できなくてはならない。

(2)　タイムアウト

従来のモンデックスでは，遠隔送金は主として電話で行われてきた。この場合，送金(バリュー転送)にはごく短時間を要するだけである。したがって，バリュー転送を制御するソフトウェア(IFD)は，例えば1分間を超えた場合にタイムアウトとなるよう設定しておけば問題はなかった。しかし，TCP/IP(Transmission Control Protocol/Internet Protocol)のパケット通信によるインターネット上でのバリュー転送は，1回のメッセージ送信に何秒かかるかわからず，すべての会話が終了するまでには1分ないし数分の時間がかかると予想されている。

したがって，インターネットでモンデックスを利用する場合には，タイムアウトは従来よりも相当長く設定しておく必要がある。それでも，パケットロスが多発するなどネットワークの状態が悪い場合には，しばしばタイムアウトによって交信が中断すると思われる。モンデックスでは，これは通信不良として記録され，事故情報を記録しておくためのログに書き込まれる。一方は送金したのに他方は受け取っていないという場合には，このログは重要な証拠となる。そして現行仕様では，このログが一定回数たまると不良カードとしてロックされてしまう。したがって，タイムアウトの設定が悪いと頻繁にカードロックが発生するおそれがある。

(3)　ロックされたカードのリセット

ロックされたカードは，銀行に持っていってログをリセットしてもらわないかぎり再使用できない。この仕掛けは，通信不良で中断した送金を確実に遂行するため以外に，ログを精査してハッキングやマネーロンダリングなどの犯罪の痕(こん)跡を発見するという目的を持っている。したがって，銀行がチェックする必要性は否定できないが，上記のように頻繁にロックする可能性がある場合，そのたびごとに銀行に出向くのは現実的でない。さらに，国際間などの遠隔地間の通信による送金トラブルを解消するためには，どこの銀行に出向くべきかという問題も指摘されている。

(4)　金庫の稼動率

モンデックス金庫は，銀行や大規模店舗で多額のモンデックスマネーを安全に管理，保管するとともに，同時並行的に発生する支払いや入金などの取引要求に迅速にこたえるための装置である。

この装置をインターネット上での取り引きに使う場合，上に述べたロックの問題が稼動率に大きな影響を与える。すなわち，一定回数の通信不良でカードがロックしてしまうと，多数の相手と24時間取り引きする金庫中のカードは瞬く間にすべてがロックされてしまうと思われるからである。さらに，1回の送金に要する時間が長いため，金庫中の1枚のカードが長時間一つの取り引きに占有されることになり，現行金庫の処理能力を大幅に下回ることが予想される。

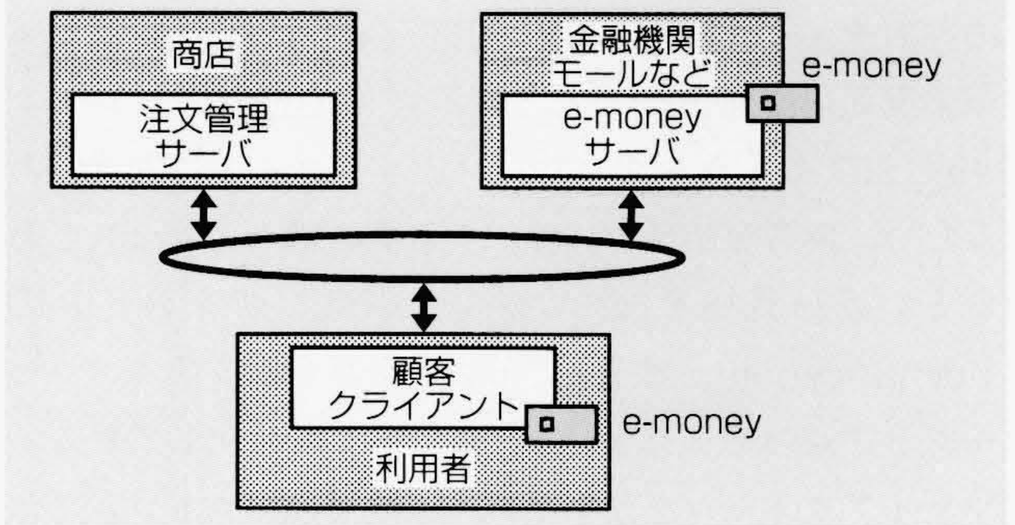
(5)　ほかの支払い方法との共存

インターネット上での支払い手段としては，クレジットや銀行振り込み，各種電子マネーがありうる。この場合，商品選択までは同一モールプログラムを利用し，支払い段階で各手段の支払い処理プログラムを個別に実行させればよいと単純に言い切ることはできない。なぜなら，商品選択から支払いまでの一貫性を維持，保証するために，同一の認証キーとその管理機構を必要とするからである。

この目的のためには，認証機構の完備しているSET(やSECE)と共通の環境で電子マネーの支払いを行うアプローチが，開発工数のうえからもシステムの維持管理のうえからも有効である。これはまた，銀行やクレジット会社によるキャッシングサービスにも対応でき，双方にメリットのある方式である。

4. SET/e-money

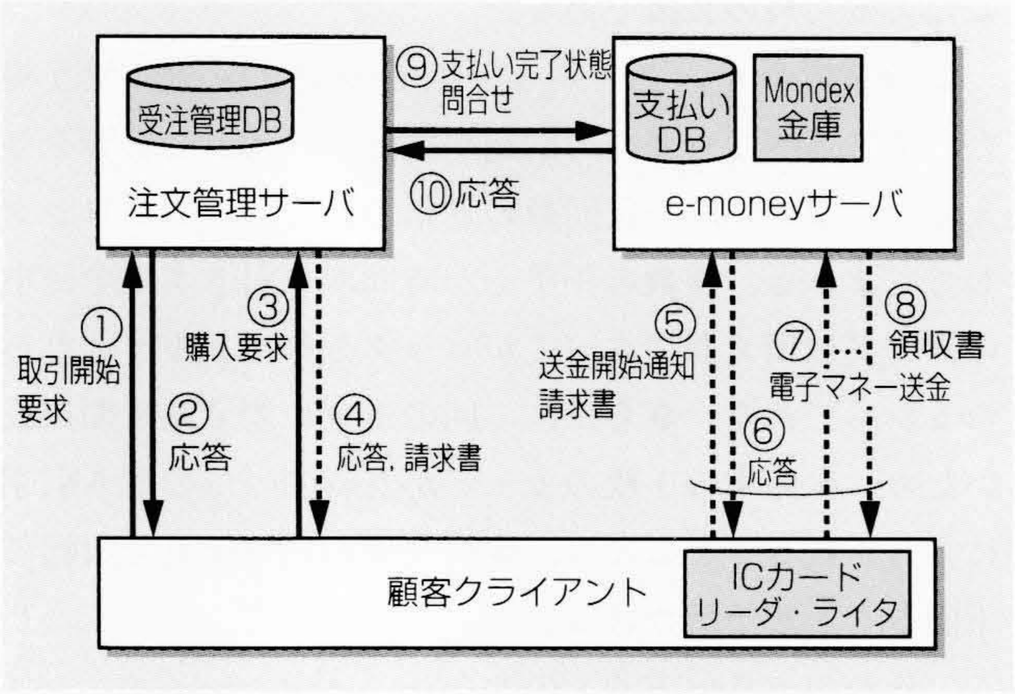
この章では，日立製作所(新金融システム推進本部，システム開発研究所，ビジネスシステム開発センタ)で検討してきた“SET/e-money”について述べる。



注：▒(関与者)，□(ソフトウェアコンポーネント)

図4　SET/e-moneyのモデル構成

電子マネーの支払いは商店とは別の機関に対して行う構成であるが，両者を一体化することもできる。



注：略語説明　DB(Database)

図5　SET/e-moneyのメッセージフロー

顧客クライアントは，商品購入を注文管理サーバに通知した後，請求書を添えてe-moneyサーバに支払いを行う。

“SET/e-money”は，SETの枠組みの中でモンデックスをはじめとする電子マネーによる支払いを実現するためのプロトコルセットである。SETに準拠して，SET/e-moneyは3コンポーネントモデル構成である(**図4**参照)。すなわち，このシステムは，顧客クライアント，注文管理サーバ，およびe-moneyサーバで構成している。e-moneyサーバは電子マネーによる支払いを受け付ける機構であり，モンデックスだけでなく，ビザキャッシュでもPROTONでも使用することができる。そのセキュリティはSETで用意されているもの(暗号，ディジタル署名，認証局など)すべてが利用できる。また，請求書や領収書，払い戻しクーポンなどの概念を導入し，オープンなネットワーク環境でも十分な証拠能力がある。ただし，電子マネーだけしか支払いに使用しない場合でも認証機能を利用するために，SETと同様の初期登録作業が必要である。

SET/e-moneyでの処理の概要を**図5**に示す。SETでの与信チェックの代わりに，SET/e-moneyでは電子マネーの支払いを行う。このプロトコル(e-moneyプロトコル)はSETのトランザクションプロトコルとは別物であるため，両者を結び付けて一つの商品購入プロセスであるという一貫性を保つために，トランザクションID(Identification)を共有し，また，会話を構成するメッセージを共通のセッションキーによって暗号化している。ファイアウォールを通すため，下位層のプロトコルにはHTTP(Hypertext Transfer Protocol)を用いている。この場合のセキュリティはSETに準拠する。

このシステムは，通商産業省の「電子商取引実証実験」ですでに開発されているSECEプラットフォーム上で動作することを技術的な目標と定めている。ただし，グローバルな技術としてSET上に実装するためには，MXI社の合意が必要であり，現在協議中である。

5. おわりに

ここでは，電子マネーシステム「モンデックス」の新しい動きについて，ビジネスと技術の両面から述べた。世界各地でのモンデックス導入の動き，新チップやマルチアプリケーション用カードOSによる技術的優位性の強化，インターネット上での商取引での適用の試みなど，グローバルな経営基盤の上で着実に成長する様子がうかがえる。“Mondex on the Internet”については，日立製作所のアプローチについても簡単に触れた。

マスターカードによるモンデックスの買収により，原則的には電子マネー分野でのモンデックスのデファクトスタンダード化に向けて大きく前進したと評価できる。本稿によって全体像がいくらかでも理解されることを願うものである。

参考文献

1) 日立製作所新金融システム推進本部 編：図解よくわかる電子マネー——モンデックスマネーを中心として，日刊工業新聞社(1996)
2) 須藤，外：図説電子マネー，経済法令研究会(1996)
3) 磯部監修，日立総合計画研究所 編：電子マネーとオープン・ネットワーク社会，東洋経済新報社(1996)

執筆者紹介

山下廣太郎
1974年日立製作所入社，新金融システム推進本部 所属
現在，電子マネーの社会に向けたデバイスやシステムの開発・事業化に従事
E-mail：kotaro @ cm. 03head. hitachi. co. jp

村松　晃
1971年日立製作所入社，新金融システム推進本部 所属
現在，電子マネー関連の技術開発に従事
情報処理学会会員
E-mail：murama @ cm. 03head. hitachi. co. jp

田代　勤
1978年日立製作所入社，システム開発研究所 所属
現在，ECの研究開発に従事
情報処理学会会員
E-mail：tashiro @ sdl. hitachi. co. jp