■11 群（社会情報システム）－ 6 編（流通情報システム）

4 章 入出力装置及び関連システム

（執筆者：道坂　修）［2010 年 9 月 受領］

■概要■

近年の流通情報システムでは，3 章で解説したデータキャリアとしての商品タグの RF-ID，会員カード・電子マネーカードの IC カードを活用することができる．これらを店舗で利用するために必要となる入出力装置として，非接触通信方式によるデータ通信を可能とする RF 装置をベースに，商品タグへの商品コードの読み書きやゲートにおけるタグの検知，電子マネーによる決済や入金など，その業務目的に応じた IC カード端末が提供されている．また，これら IC カード端末では電子マネーカードへの不正な IC 処理を防止するため，高度なセキュリティメカニズムが実装され，端末管理システムや鍵管理システムなどそのセキュリティを支援する周辺システムが構築され，運用されている．

以下に，流通情報システムにおけるデータキャリアと入出力装置，周辺システムとの関連を示す．

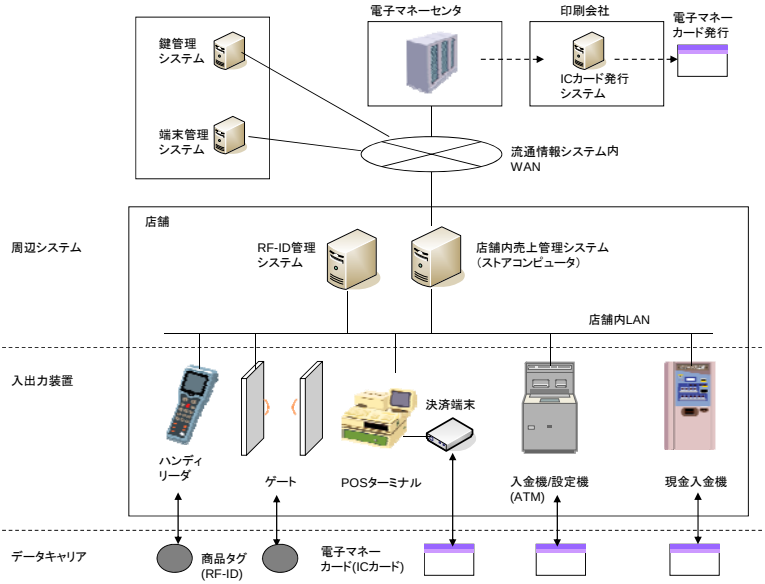


図 4・1　流通情報システムにおけるデータキャリア，入出力装置及び周辺システム

本章では，上記における入出力装置や周辺システムの概要を解説する．

【本書の構成】

本章では，3 章で解説したデータキャリアを取り扱う入出力装置とこれら装置周辺のサブシステムの概要として，4-1 節にて RF-ID 及び IC カードを取り扱う端末や端末管理システム

などの周辺システムを解説する．また，4-2 節にて RF-ID や IC カードなどのデータキャリアを用いた店舗端末（POS ターミナルなど）や店舗業務システムを解説する．

■11 群 － 6 編 － 4 章

4-1 IC カードシステム

（執筆者：道坂　修）［2010 年 9 月 受領］

4-1-1 概　要

3 章に示すとおり，流通情報システムのデータキャリアとして商品タグに添付する RF-ID や小額決済及び購買データに関して POS システムとの連動を行う会員カード（IC カード）を取り扱う IC カードシステムを解説する．

4-1-2 IC カード端末

流通情報システムにおいて，商品タグに用いられる RF-ID 及び会員カードなどに用いられる IC カードの管理やデータの入出力を行う端末はその用途に応じて**表 4･1** に分類される．

表 4・1　IC カード端末の種類

端末の種類	用　途
タグリーダライタ	商品タグ（RF-ID）への商品コードの書き込みまたは読み込みを行う装置
セキュリティゲート	盗難防止を目的として，商品タグ（RF-ID）を付けたままゲートを通過した際に警報をならすための装置
決済端末	電子マネーカードに対し，商品購入時に当該分のバリューの引き去りを行う装置
発券機	電子マネーカードの有効化や記名式カードの場合は券面印刷への氏名などの印字，会員情報と電子マネーカードとの紐付けを行う端末
入金機	プリペイド型電子マネーカードに対し，電子マネー内のバリューのチャージを行う端末
設定端末	電子マネーカードのバリュー残高の確認や各種セキュリティパラメータ（オートチャージ額，1 日の最大チャージ回数，1 日の最大利用額など）の設定，ポイントの確認やポイント管理を行うための端末
モバイル端末	電子マネーカードの決済，入金，設定などを行える携帯型端末

(1)　タグリーダライタ

商品タグへの商品コードの読み書きを行う端末であり，ハンディ型と据置き型がある．また RF-ID の種類がパッシブ型の場合，RF-ID に対し電磁誘導や電波で給電を行う役割も担う．

(a) ハンディ型

店舗にて陳列棚に並ぶ個々の商品に対して，商品タグの添付作業または既に添付された商品タグへの商品コード書き込みを行うため，持ち運びができるタグリーダライタである．主に店員が操作を行うことや，商品タグとタグリーダライタ間の距離を近接させることができるため，送信出力は数 10 mW/MHz 程度であり，周波数帯の利用にあたり許可を必要とする

UHF 帯（900 MHz 帯）の RF-ID において無線局への登録申請を行う必要はない．

(b) 据え置き型

店頭にて商品に添付される商品タグの読み込みを行うために，POS ターミナルと接続して据え置きされるタグリーダライタである．POS ターミナルなどの購買時に商品タグの読み込みを高速に行う必要があることから，一般に商品タグとタグリーダライタ間の距離が比較的長く，送信出力は数 100 mW/MHz となることから，その利用にあたり無線局への登録申請を行う場合がある．

また RF-ID の ID 利用形態によって，RF-ID 管理システムと連携する(c)オンライン型と(d)端末内に閉じて処理を行うオフライン型がある．

(c) オンライン型

出荷時に個々の RF-ID にユーニクに付番，記録される製造コードを利用し，RF-ID と商品コードとの対応を RF-ID 管理システム内の商品コードデータベースに登録するタイプである．このタイプのタグリーダライタはハンディ型の場合は無線 LAN，据置き型の場合は LAN のインタフェースをもつ．**図 4･2** に示すとおり，ステップ 1（商品コードとの対応付け）の過程で，製造コードを商品タグから読み出し，ハンディ型タグリーダライタを用いて製造コードと商品コードとの対応付けを行い，ネットワークを通じ RF-ID 管理システム内の商品コードデータベースに当該対応付けデータを登録する．利用時には，据置き型タグリーダライタなどから製造コードを読み出し，ネットワークを通じ RF-ID 管理システム内の商品コードデータベースに対して製造コードによる商品情報の問合せを行う．

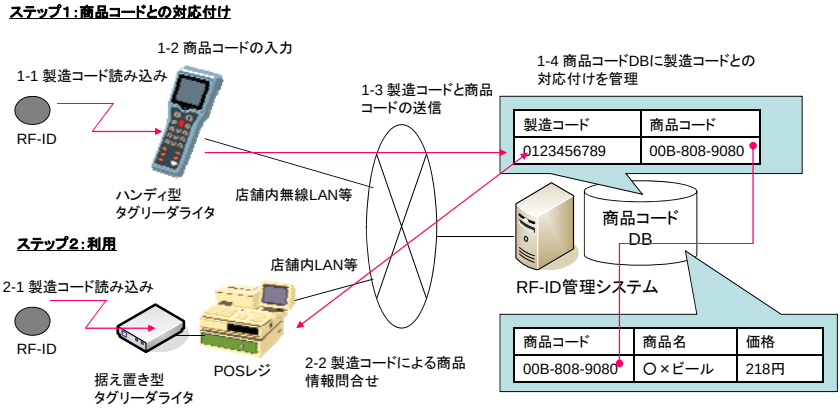


図 4･2　タグリーダライタと RF-ID 管理システムとの連携

(d) オフライン型

タグリーダライタ自身にはネットワーク通信機能をもたず，オフラインで商品コードの書き込み，読み出しを行うタイプである．タグリーダライタに商品コード一覧や書き込み用認証鍵などの情報をもたせ，ハンディ型タグリーダライタを用いて RF-ID に商品コードを書き込む．利用時には RF-ID より商品コードを直に読み込み，店舗内の商品データベースなどに対し商品コードをキーに商品情報を取得する．

(2) セキュリティゲート

CD や衣料品などの高額商品に対し，盗難防止の目的で導入するゲート型タグリーダである．セキュリティゲートは前述の目的により店舗における販売エリア出口または店舗出口に対し配置され，ゲートの両側または片側に高出力のタグリーダを設置し，ゲート通過時の RF-ID を検出する．

現在流通しているセキュリティゲートの種類としては，高出力でパッシブ型 RF-ID を給電，検知するタイプと低出力でアクティブ型 RF-ID を検知するタイプの 2 種がある．また，検出する RF-ID の ID によって警報出力の有無を切り分ける高機能型セキュリティゲートもあるが，店頭にて購入する際に商品タグをはずし，未購入のままゲートを通過した際に，その ID の内容に関わらず警報を鳴らす運用を行っているケースが多い．

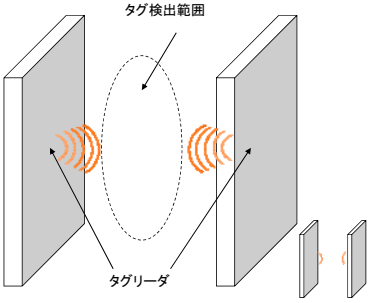


図 4・3　セキュリティゲートのイメージ

(3) 決済端末

店頭の POS ターミナルと連動し，電子マネーカードやポイントカードに対し，商品購入時に当該分のバリューの引き去りやポイントの加算を行う端末である．また，コンビニなどの電子マネー加盟店においては，バリューの引き去りなどの決済機能だけでなく，電子マネーへの現金チャージを行う機能も付加されている場合もある．

以下に決済端末の機能を解説する．

(a) セキュリティメカニズム

電子マネーカードの精算は，電子マネーカードの持つセキュリティ機能（耐タンパメモリやアクセス制御機構による非改ざん性）を信頼し，加盟店における決済やチャージなど，電子マネーカード内のバリューの演算結果を取引データとして電子マネー事業者に提出することで実現されるが，バリューの演算を行う決済端末は特に現金チャージなど，バリューの加算処理を行う場合，決済端末の盗難による不正なバリュー演算を防止しなければならない．これより決済端末は高度なセキュリティメカニズムを実装する必要がある．セキュリティメカニズムの詳細については後述 4-1-4 項(2)にて解説する．

(b) 決済方式

決済端末の決済方式としては，**表 4･2** に示すとおり，電子マネー決済，クレジットカード決済，デビットカード決済の 3 種類がある．

表 4・2　決済端末における決済方式

決済方式	精算のタイミング	暗証番号入力有無	概　要
電子マネー決済	先払い	なし	電子マネーカード内に現金に相当するバリューを予めチャージし，バリューの範囲内で決済を行う
	後払い	なし	電子マネーカードによる決済後，一定期間中の利用額を一括して請求する
クレジットカード決済	後払い	あり	クレジットカードによる決済後，一定期間中の利用額を一括して請求する
デビットカード決済	即時払い	あり	キャッシュカードを用いて銀行口座から当該料金の引き落としを行う

電子マネー決済における料金精算のタイミングは先払い式（プリペイド方式）と後払い方式（ポストペイ方式）の 2 通りがあり，各電子マネーカード事業者によって採用する方式が異なる．一般に，後払い方式の場合，後の料金請求及び料金回収を行うためにクレジットカード決済のインフラを利用するケースがほとんどであり，電子マネーカード利用者には併せてクレジットカードも発行，配布されている．

一般に，電子マネー決済は小額決済，クレジットカード決済やデビットカード決済は高額決済という住み分けがなされており，後者はそのセキュリティ上から暗証番号入力を必要とするため，クレジットカード決済機能をもつ決済端末（CCT : Credit Card Terminal）には暗証番号入力装置（PIN パッド）が実装される．

多くの場合，電子マネーカード決済事業は利用の少ない小額クレジットカード決済の事業領域をカバーすることが目的となっており，クレジットカードと電子マネーカードの事業は密接な関係がある．後払い方式の電子マネー決済では前述のとおりクレジットカード決済のインフラを利用していることや，前述の先払い式の電子マネー決済の場合においても，バリューが規定額以下になった場合や残高不足になった際に予め電子マネーカードと紐付けられたクレジットカードによるチャージを自動的に行うオートチャージサービスも提供されており，電子マネー決済とクレジット決済が複合しているケースも珍しくない．

店頭において各決済方式を実装した個々の決済端末を POS ターミナルに接続する場合もあるが，主に店頭のスペースの都合から各決済方式を 1 台の端末に融合した決済端末も提供されている．特に電子マネー決済とクレジットカード決済の双方を実装する電子マネー・クレジット一体型決済端末やデビットカード決済とクレジットカード決済の双方を実装するデビットカード・クレジットカード一体型決済端末が主流になりつつある．

(c) 対応するカード

表 4･3 に国内の決済端末における対応カードを示す．表における接触 IC カードとは ISO/IEC 7816 に基づくカードとし，非接触 IC カードにおける TypeA, TypeB は ISO/IEC 14443 における伝送方式を示す．また，ISO 18092 は ISO/IEC 18092 において FeliCa® の伝送方式を示す．また，○は対応，△は機種によって対応，－は未対応を示す．

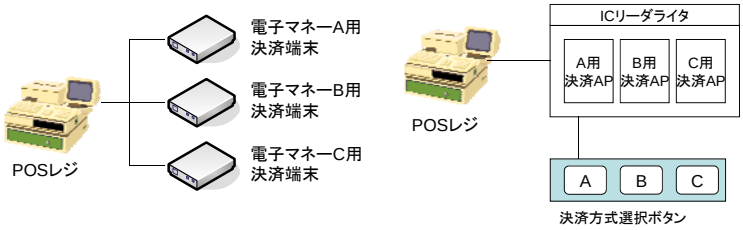
表 4・3　国内の決済端末における対応カード

決済方式	磁気カード	接触 IC カード	非接触 IC カード		
			TypeA	TypeB	ISO 18092
電子マネー決済	－	－	△	△	○
クレジットカード決済	○	○	－	－	－
デビットカード決済	○	○	－	－	－

表 4･3 に示すとおり，決済端末がサポートするカードは端末に実装する決済方式に依存し，主に電子マネー決済では非接触 IC カード，クレジットカード決済及びデビット決済は磁気カード及び接触 IC カードに対応している．国内の電子マネー決済端末では FeliCa® に対応したものが中心であるが，近年では電子マネーカード以外の IC カードの読み書きが行える NFC リーダを搭載した決済端末も普及しつつある．

(d) 対応する決済アプリケーション

クレジット決済やデビットカード決済はクレジットブランドや全国銀行協会，日本デビットカード推進協議会などで標準化されており，決済端末に搭載する決済アプリケーションはそれぞれ一つに集約できる一方で，電子マネー決済は各電子マネー事業者によって方式が異なるため，加盟店で利用する電子マネーカードごとにこれら決済アプリケーションを搭載した決済端末を準備しなければならない．これまでの流通情報システムでは，対応する電子マネーカード単位で決済端末を調達，配備してきたが，前述の店頭における決済端末の配置スペースの関係より，近年では複数の電子マネー決済アプリケーションを 1 台の決済端末に集約できるマルチ決済端末の導入を進めている．



(a) 従来の単一決済端末　　(b) マルチ決済端末

図 4・4　マルチ決済端末の概要

(4)　発券機

電子マネーカードには無記名形式と記名形式の 2 種類があり，記名形式の場合は紛失時の残高保証を行うために会員情報の登録を行う必要がある．また，登録された会員情報は紛失時の本人確認に使われるほか，売上管理システム（ストアコンピュータ）と連携させ，詳細なマーケティング情報を取得することも可能である．

一般に，電子マネーカードの初回発行は会員への電子マネーカードの交付方法に応じて

様々なオペレーションを行う必要があるが，電子マネーカード番号やデフォルト値などの初期データを書き込んでおいた初期カードを店頭もしくは発券機にて準備し，発券時に初期カードに対してカードの有効化を行ったり，記名式カードの場合は券面の印刷を行う場合が多い．

以下に発券機の機能の概要を解説する．

(a) カードの活性化

上記に示す初期カードの盗難による不正利用を防ぐため，発券機は電子マネーカード内の活性化フラグを「有効」に書き換える機能を提供する．

(b) カードの券面印刷（記名式カードの場合）

電子マネーカードによっては，カード所有者の名前をカードの券面に記載するために，発券時に書き換え可能な券面印刷用インクを用いてカード所有者の名前を券面に印刷を行う場合がある．

(c) 会員情報の登録（記名式カードの場合）

発券時に会員情報として氏名，住所，生年月日，性別などの個人情報を電子マネーセンターに登録し，紛失時の残高返金の際の本人確認に利用する．電子マネーセンターでは，紛失時に確認した本人情報を元に，当該本人情報の所有する電子マネーカード番号をネガティブリストに登録し，決済端末などに配布する．

(d) その他，設定値の変更など

発券時に初期カード内のデフォルト設定値または電子マネーセンター内のカードごとに設定値の変更を行う．一般的には以下の設定値の変更が考えられる．

- バリュー上限値
- オートチャージ設定（オートチャージ有無，オートチャージ額，チャージ判定額など）
- オートチャージ時のクレジット番号（電子マネーセンター内）
- その他セキュリティパラメータ（1 日のチャージ回数，オートチャージ回数，決済回数，合計決済額の上限など）

(e) 発券機の種類

発券機は，電子マネーカードのデポジット料または購入料を徴収し上記(a)～(d)の処理を会員のセルフ操作で発券できる自販機型と，店員が発券システムと連動してこれらの操作を行う端末型の 2 種類がある．

(5) 入金機

プリペイド型電子マネーカードに対し，電子マネー内のバリューの加算（チャージ）を行う端末である．特に入金機が盗難された場合，バリューの捏造が可能となるほか，スタッカーに蓄積された紙幣損失による経済的被害が大きいため，極めて高いセキュリティ対策が必要となる．

以下に入金機の機能の概要を解説する．

(a) チャージ手段

電子マネーのバリューチャージ方法としては**表 4･4** が用意されている．

表 4・4　電子マネーのバリューチャージ方法

チャージ方法	入金機における処理
現金チャージ	紙幣を機内に取り込み，現金スタッカー内に蓄積する．投入された紙幣額に応じてバリューを加算する．
クレジットチャージ	クレジットカードを読み込み，チャージ指定額分のクレジット決済を行い，暗証番号の照合や与信による決済可否を照合後，当該額分のバリューを加算する．
銀行口座チャージ	キャッシュカードの読み込み，または銀行口座を指定してチャージ指定額分の資金移動を行い，当該額分のバリューを加算する．
ポイントチャージ	ポイント交換、ポイントダウンロードともいう．電子マネーカードまたは電子マネーセンター内のポイントをバリューに変換し，当該額分のバリューを加算する．

最も多いチャージ手段が現金チャージである．表 4･4 すべてのチャージを可能とする ATM などに類似する多機能入金機もあるが，プリペイド型の場合，残高不足時に決済を利用できないことから，より単価の安い現金入金機を多く設置する必要がある．

銀行口座チャージは，会員が資金移動の際に手数料を負担しなければために利用されにくい傾向があるが，銀行提携型電子マネーカードはこれらのデメリットがなく，ATM 利用とセットで使われる場合が多い．

(b) 入金機のセキュリティメカニズム

入金機のセキュリティ対策は，他の IC カード端末におけるセキュリティメカニズム（詳細については後述 4-1-4 項(2)にて解説）に加え，以下の対策を行っている．

・入金機のこじあけや現金スタッカーの引き去りに対し，耐震センサを有し，これらの脅威が発生した場合，警報を鳴らす仕様となっている．
・入金機の立て付けとして，店舗の外壁から距離を離して設置する，監視カメラの監視の届く範囲に設置する，入金機の撤去が困難となるよう頑丈な器具で固定する，などの対策が打たれている．

(6) 設定端末

電子マネーカードのバリュー残高の確認や前述(4)項(d)に示す各種設定値（オートチャージ額，1 日の最大チャージ回数，1 日の最大利用額など）の設定，ポイントの確認やポイント管理を行うための端末である．一般に，設定端末は電子マネー会員がタッチパネルのガイダンスに従ってセルフ操作を行うことのできる Kiosk 端末型となっており，現金以外の入金機機能や ATM などに複合されて実装されることもある．

設定端末の機能は以下のとおりである．

・バリュー残高の確認
・各種設定値の確認及び設定変更
・ポイント残高の確認
・ポイント管理（ポイントチャージ，他会員へのポイント譲渡，他電子マネー事業者の提

供するポイントとの相互交換など）

(7) モバイル端末

電子マネーカードの決済，入金，設定などを行える携帯型端末である．ハンディ型タグリーダライタと同様に携帯可能な筐体であり，前述の(3)決済端末機能を中心に(5)入金機及び(6)設定端末の機能の一部を有する．これら据置き型の端末と比較し，端末の盗難対策がより重要となるため，IC カード端末におけるセキュリティメカニズム（詳細については後述 4-1-4 項(2)にて解説）に加え，以下のセキュリティ対策を行っている．

- モバイル端末を操作できる店員を事前に設定し，端末操作時に店員の認証を行う．
- アイドル時のタイムアウトを行い，タイムアウト後は再度店員の認証を行わない限り利用できないように端末機能のロックを行う．
- モバイル端末内の相互認証鍵の有効期間を短くし，盗難時の相互認証鍵無効化の効果を高める．

4-1-3 鍵管理システム

(1) 鍵管理の重要性

前述の 4-1-2 項に示すとおり，決済端末などの IC カード端末は電子マネーカードなどの IC カードに対し，不正な端末によるバリューなどの不正な書き込みや偽造カードによる不正な決済などを防止するために，電子マネーカードに対して書き込みを行うことのできる IC カード端末の正当性を認証（外部認証）するとともに，カードの偽造や複製を検知するために IC カード端末が IC カードの正当性を認証（内部認証）することが不可欠である．これらの認証は端末及び IC カード内の暗号演算処理によって実現されるが，用いる暗号アルゴリズムの安全性だけでなく，暗号及び復号を行う暗号鍵が漏洩しないことが大前提となる．

流通情報システムにて利用される電子マネーカードや IC カード端末は，非接触型でかつ高速な決済処理が求められることから，暗号処理が複雑であり消費電力が大きく処理時間を要する公開鍵暗号方式ではなく，共通鍵暗号方式が採用されるケースが多い．また，処理の効率性や鍵管理コストの削減の観点より，外部認証用の鍵と内部認証用の鍵は相互認証用の鍵（以降，相互認証鍵と呼ぶ）として共用化され，一つの鍵として管理されるケースが多い．

これより，流通情報システムでは，電子マネーカードや IC カード端末にて使用する相互認証鍵を安全に管理するための鍵管理システムを構築，運用している．

(2) 鍵管理システムとは

情報流通システムにおける鍵管理システムとは，前述に示す電子マネー用相互認証鍵や取引電文などの暗号化鍵の生成，受け渡し，保管，配信を行うシステムである．本節では電子マネー用相互認証鍵の管理について解説する．

(a) 鍵生成

電子マネーの相互認証に用いる暗号アルゴリズムの種類や鍵長に応じて，外部からの推測が困難である品質の高い鍵データを生成する．一般に，共通鍵暗号方式の場合は乱数を生成し鍵データのビット反転などの異常を検出するパリティビットを付与して鍵データを生成する．パソコンなどに搭載されるソフトウェアが生成する乱数は予め決められた乱数生成規則

と乱数算出に用いるシード値との演算によって生成される擬似乱数であり一定の規則性を持つことから鍵データに用いることは困難である．これより，熱雑音などを用いたランダム性の高い乱数生成器（RNG：Random Number Generator）をもつハードウェアで生成された乱数を用いることが望ましい．

生成した鍵は通常はハードウェア暗号処理装置（HSM：Hardware Security Module）内に保管されるが，装置の故障などを考慮し，そのバックアップをとる．HSM の盗難やバックアップの盗難に備え，HSM 設置場所及び鍵のバックアップ媒体の物理的セキュリティ対策（入退室管理，ビデオカメラによる監視，媒体の金庫保管，金庫の施錠管理）を厳重に行う必要がある．

(b) 鍵受け渡し

生成した鍵は，後に解説する IC カード発行システムに引き渡され，電子マネーカード発行時に相互認証鍵として IC カード内の耐タンパメモリに設定される．通常は IC カード発行システム内においても HSM が設置され，その発行モデルに応じて委託発行先業者に対して安全な方法で鍵データを引き渡す方法がとられる．その具体的方法は電子マネー事業者によって様々であるが，これら鍵の引渡しをシステム化するケースはほとんどなく，暗号化した媒体の手渡しやセキュリティ便などを用いた輸送などにより安全にかつ極秘に行われる．

(c) 鍵配信

IC カード端末への相互認証鍵の設定は，鍵管理システムと後に解説する端末管理システムが連動し，初回の端末設置時及び電子マネー事業者のセキュリティポリシによって定められる鍵の有効期間ごとに鍵管理システムが当該鍵データを IC カード端末へ配信することによって実現される．

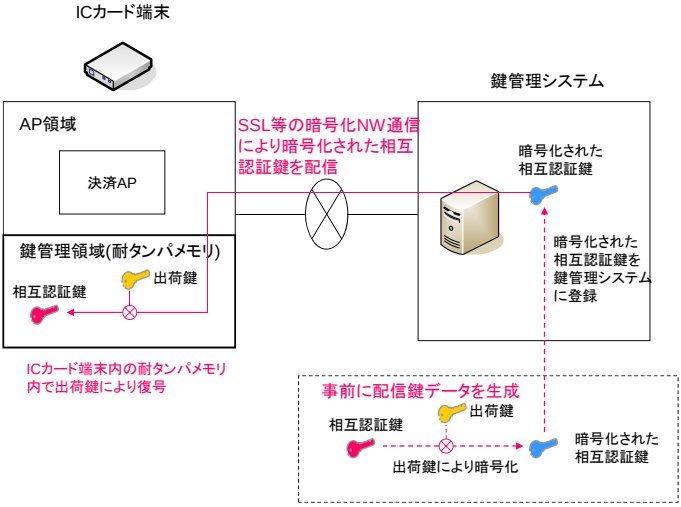


図 4・5　鍵配信の仕組み

IC カード端末と鍵管理システム間は VPN や SSL などの暗号化ネットワークによって接続され，これら通信路の盗聴による鍵データの漏洩を防ぐだけでなく，**図 4･5** に示すとおり，

IC カード端末内の耐タンパメモリ内に予め設定してある出荷鍵によって暗号化された鍵データを配信し，IC カード端末内の耐タンパメモリ内で復号され，同メモリ内に設定される．

4-1-4 端末管理システム

(1) 端末管理の重要性

前述の通り，流通情報システムにおける電子マネーカード及び IC カード端末における相互認証鍵の管理は極めて重要である一方で，相互認証鍵を入手せずとも正当な IC カード端末を不正に利用することにより IC カードへの不正な書き込みが可能となるため，その脅威に対し IC カード端末の不正利用を防止することが不可欠である．特に入金機や入金機能をもつ端末が盗難された場合，無制限にバリューを捏造することが可能となるため，その端末管理には万全な対策が必要となる．

(2) IC カード端末におけるセキュリティメカニズム

流通情報システムにおける IC カード端末では，前述の端末の不正利用に対し，以下のセキュリティ対策を施している．

(a) 開局による IC カード端末内の決済アプリケーションの活性化

IC カード端末の起動時に端末管理システムと通信し，端末認証や端末のステータス確認が成功した場合に，端末内の決済アプリケーションの活性化を行う．端末盗難時に端末ステータスを無効にしておくことで開局を失敗させ，端末内の決済アプリケーションを事実上無効化させる．

(b) POS ターミナルなどの上位端末との接続認証

決済端末の場合は，POS ターミナルと接続して使用されるため，決済端末設置時に POS ターミナルと決済端末間の接続設定を行ったうえで，通常の利用時に機器間の認証を行うことで，盗難時に別の POS ターミナルと接続を行えないようにする．

(c) 端末の死活監視

端末盗難を早期に検知し，(a)などの開局時のステータス確認の際に盗難端末の開局を許可しないようにするため，端末がネットワークにつながっているかその死活を定期的に監視する．

(d) 電源断時の相互認証鍵の消失（鍵の無効化）

端末盗難時に端末の電源供給が絶たれることを想定し，端末内の相互認証鍵を揮発性の耐タンパメモリに保管することで電源断時に相互認証鍵を消失させ，当該鍵の無効化を行う．

(e) 端末の立て付けなどの対策

前述の入金機におけるセキュリティ対策に示すとおり，端末の設置位置や端末の固定により物理的に盗難を困難にする．

(f) 端末のこじ開けなどの対策

外部からの物理的なこじあけ，回路パターンの解析，プローブによる内部データの解析などのタンピング（tamping）行為に対し，IC カード端末はこれらによる攻撃や解析が困難となるように設計された耐タンパメモリを有し，耐タンパメモリ内に相互認証鍵を保管することで当該鍵を保護する．また，耐タンパメモリ内に保持された相互認証鍵はメモリ外に出ることなく耐タンパメモリ内に閉じて暗号演算などを行うことで，認証鍵の漏洩を防ぐ．

(3) 端末管理システムとは

前項(2)における IC カード端末のもつセキュリティメカニズムに対して上記(a)，(c)，(d)の支援を行うとともに，マルチ決済端末などにて決済アプリケーションモジュールや決済音，ネガティブリストなどのアプリケーションデータなどの資源配布を行う機能を提供する．

以下に端末管理システムの機能の概要を解説する．

(a) 端末認証

端末管理システムに登録された IC カード端末の認証を行う．IC カード端末は POS ターミナルとのシリアル通信インタフェースのほか，ネットワークインタフェースも有し，店舗内 LAN を経由して端末管理システムと IC カード端末間で直接認証を行う．これらの認証は端末内の耐タンパメモリまたは SAM モジュール内の端末認証鍵を用いて IP-Sec/VPN または SSL によって行われる．

(b) 端末の死活確認

端末管理システムから IC カード端末に対して定期的に死活を確認するための管理コマンドを送信し，その応答有無から端末の死活を確認する．一般に，店舗における決済端末などは売り場の増設や移設に伴い，一時的に POS レジなどとともに撤去されたり移設されたりするため，応答がない端末が盗難されていると見なすかどうか判断が難しい．これより死活確認の結果，応答のない端末に対して，店舗の管理者に定期的に連絡するなどの手段がとられるほか，これら端末の撤去や増設などのスケジュールと連動させ，正確な端末リストを再登録するなどの運用が行われている．

(c) 端末のセキュリティポリシ更新

前述に示す端末内の鍵の有効期限や電源断時の無効化有無，鍵の再配信の時間間隔などは端末のセキュリティポリシとして設定されており，端末認証が成功している端末に対し，端末管理システムから一括してこれらのポリシの設定を更新することが可能である．

(d) 資源配布

前述 4-1-3 項に示す鍵管理システムと連動し，端末内の鍵の有効期限が切れた場合や電源断後の電源 ON 時において，端末に鍵データを配信する機能を提供する．また，鍵データだけでなく，決済アプリケーションのソフトウェアモジュールや決済時に鳴らす決済音やエラー音，個々の決済アプリケーションが利用する各種データ（ネガティブリストなど）を配信する機能も提供する．これらの資源は端末管理システム内でバージョン管理されており，例えば決済アプリケーションのバージョンアップを行った場合，古いバージョンのアプリケーションが搭載された端末を特定し，当該端末に対しアプリケーションのアップデートを行うこともできる．

4-1-5 IC カード発行システム

IC カード発行システムとは，電子マネーカードに対して電子マネーデータや相互認証鍵を書き込み，その券面印刷やカード所有者への郵送，その他電子マネーカードの発行履歴管理，有効化を行うシステムである．以下にその概要を以下に示す．

(1) IC カードの発行方法

IC カードの発行ではカード所有者ごとにプラスチックカードの表面の印刷や表面の加工

（エンボスなど），更にはクレジット会員の場合はカードの郵送及び郵送を行うための台紙の印刷，封筒の宛名の印刷などが必要となるため，IC カードを発行する事業者（以下 IC カード発行者）は印刷会社へ発行を委託するのが一般的である．以下に一般的な IC カードの発行プロセスを解説する．

(a) 0 次発行

IC チップメーカーから提供される IC チップや端子などの部品をプラスチックカードに埋め込む作業である．特に流通情報システムの場合，商品コードの識別や商品購入時の支払は非接触方式による通信を用いることが多いため，IC チップと非接触通信用アンテナを接続したり，IC チップ及びアンテナをプラスチックカードに埋め込む工程（パッケージング）が必要となる．この時点の IC カードはホワイトカードもしくは白 ROM などと呼ばれ，商品や個人ごとのカスタマイズは行われていない状態である．

(b) 1 次発行

0 次発行を経て提供されたホワイトカードに対し，データ領域やアクセス制御を設定する工程である．この時点では IC カード内の記憶領域にデータ構造が反映されているのみであり，商品や個人ごとのカスタマイズは行われていない状態である．

(c) 2 次発行

1 次発行を経て提供されたカードに対し，商品ごとや個人ごとに異なるデータを IC チップに反映したり，券面に個人情報を印刷したりする工程である．

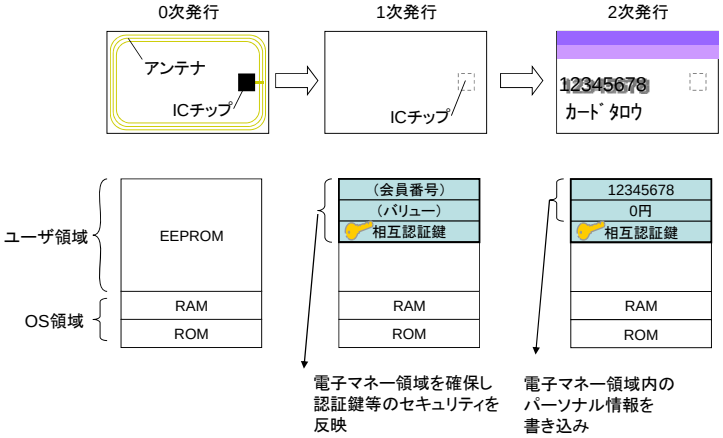


図 4・6　IC カードの発行工程

(2)　IC カードの発行パターン

前述(1)項にて解説した各工程において，どの工程を委託するかによって IC カード発行システムの構成やその機能が異なる．**表 4・5** に発行工程の委託パターンを示す．表にて○が委託対象の工程であることを示す．

表 4・5　IC カード発行工程の委託パターン

パターン	0 次発行	1 次発行	2 次発行				
			共通データ書込	個人データ書込	券面背景印刷	個人情報印刷	郵　送
完全委託	○	○	○	○	○	○	○
一部委託	○	○	○		○		
	○						

表 4･5 において一部を委託するパターンとしては，店頭で即時発行を行うケースが考えられ，①予め券面背景の印刷まで印刷会社に委託して発行した初期カードに対して発券機によって個人データを書き込む（券面への個人情報印刷が不要）パターン，② ①と同様の形態で発行された初期カードに対して券面印刷機能をもつ発券機により個人データを書き込み及び個人情報の券面印刷を行うパターン，③印刷会社からホワイトカードのみを受け取り発券機によって 1 次発行や 2 次発行を行うパターンの 3 種類がある．

(3)　IC カード発行システム

前述の発行パターンにおける IC カード発行システムの機能及び構成を以下に解説する．

(a) 完全委託パターン

完全委託パターンにおける IC カード発行システムの構成を**図 4･7** に示す．

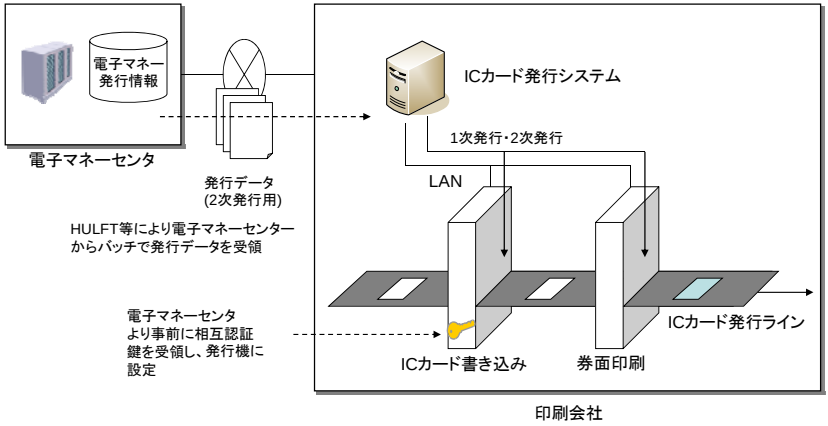


図 4・7　完全委託パターンにおける IC カード発行システムの構成

このパターンの場合，IC カード発行システムは委託先である印刷会社内に構築され，IC カードの発行枚数に応じて IC カード発行ラインが増設される．電子マネーのカード番号などの個人によって異なるデータは電子マネーセンターにて生成される 2 次発行データをバッチ処理で受領し，個々の IC カードに対し発行機によって書き込みを行う．また郵送まで委託する場合，2 次発行済みの IC カードに対し，別のラインで台紙の印刷と台紙へのはめ込み，封

筒への住所ラベル印刷と貼付，封筒への台紙の封入を行っている．

(b) 一部委託パターン

一部委託パターンにおける IC カード発行システムの構成を**図 4･8** に示す．

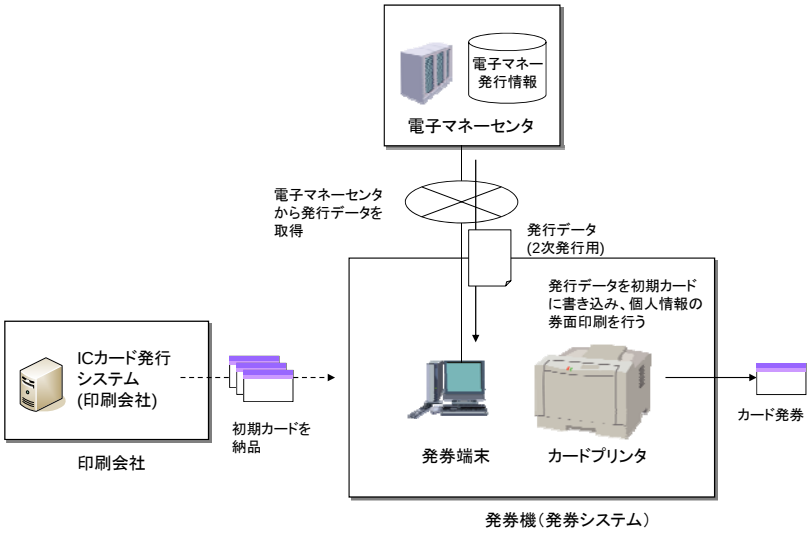


図 4・8　一部委託パターンにおける IC カード発行システムの構成

このパターンの場合，印刷会社内の IC カード発行システムは 0 次発行及び 1 次発行，2 次発行の一部（カード共通のデータ書き込みやカード背景の券面印刷）を行い，初期カードを電子マネー事業者に納品する．次に，電子マネー事業者は印刷会社の納品した初期カードに対し前述の発券機（発券システム）を用いて，個人データの書き込みや個人情報の券面印刷を行い，カードを発券する．

4-1-6 電子マネーセンター

電子マネーセンターは以下の機能をもつ．

(a) 電子マネーによる取引データの集計と加盟店への取引額精算

加盟店内の IC カード端末や決済代行事業者の決済システムにおけるチャージや決済などの取引データをバッチ処理によって集計し，加盟店及び決済代行事業者への取引額精算や取引手数料の集計，精算を行う．一般に，電子マネー決済は他決済と同様に取引額に対して一定の割合で取引手数料が発生し，加盟店単位で取引手数料の集計や請求を行う必要がある．

(b) 取引データにおける矛盾検出

プリペイド型の場合，電子マネーカードと IC カード端末間のローカル処理によって決済を実現する一方で，電子マネーセンターへの取引データの収集はバッチ処理によって実現されるため，各会員における電子マネーカードのバリュー値は常にカード内の値が最新となり，バッチ処理のタイミングによっては電子マネーセンターの把握するバリュー値と乖離が発生する．

一方で，電子マネー事業として各電子マネーカードにおけるキャッシュイン，キャッシュアウトの収支計上を行う際に，実際の取引額の総額と取引データから計上される取引額の総額間に矛盾があってはならない．例えば，取引データ上では合計 1 万円の入金がある一方で合計 2 万円の支出が認められるケースでは，一部の取引データの損失，現金の計上誤り，または不正行為が発生している可能性がある．電子マネーセンターでは，取引データにおける矛盾を検出し，特に不正行為と考えられる場合に，当該カードの失効やセキュリティシステムの強化などを行っている．

(c) 会員退会時の返金

プリペイド型の場合，会員退会時にバリュー残高を返金するケースがほとんどであり，電子マネーセンターでは，返金手数料を差し引いた返金額を取引データとして記録する．

また，カード発行（貸与）時に保証金（デポジット）を徴収し，会員退会時（カード返却）にデポジットを返金する電子マネー事業者も存在する．この場合，会員退会時にバリュー残金に加えデポジットも返却する．

(d) 紛失時のネガティブリスト登録や残高保証

記名式の電子マネーの場合，電子マネーが紛失した際に電子マネーセンターが取引データから確認できるバリュー残高を保証し，当該バリューが記録された新たな電子マネーカードを再発行するか，該当バリュー分の現金を返金するなどの対応をとっている．会員が紛失に伴う再発行または返金を希望する場合，会員情報による本人確認を行った後にカード再発行処理または返金処理を行うが，紛失した電子マネーカードはネガティブリストに記録され，端末管理システムを通じて決済端末などの IC カード端末に一斉配布される．

(e) クレジットシステム連携

ポストペイ型の電子マネーの場合，決済時の与信を行わずプリペイド型と同様にオフラインで取引データを生成し，電子マネーセンターに取引データを集約後，クレジットシステムに対しクレジット決済を行っている．クレジットブランドの規定する電子マネーでは，決済時にクレジットネットワークを使い与信を行うものもあるが，いずれの場合も通常のクレジット決済時の取引と類似している．

また，プリペイド型の電子マネーにおいて，オートチャージを行う際に電子マネーセンターにてクレジットシステムとの連携を行っている．一般に，オートチャージを行うためのクレジットカード番号はセキュリティ上の理由により電子マネーカード内には保持されず，電子マネーセンターにて管理されるため，オートチャージを行う際には端末と電子マネーセンター間の連携が必要があり，電子マネーセンターが端末によるチャージ要求に対し当該チャージ額分をクレジット決済することでチャージ処理を実現している．

(f) IC カード発行時のシステム連携

前述 4-1-5 項に示すとおり，印刷会社へ IC カード発行を完全に委託または一部を委託する際に，電子マネーセンターと IC カード発行システム間の連携が発生する．主に IC カード発行時における電子マネーセンターの役割は，IC カード発行システムや発券機に対して IC チップに書き込む発行データの提供と，発券端末からの会員情報やオートチャージ設定などの登録処理である．

(g) ポイント管理サービスにおけるシステム連携

電子マネーセンター内にポイントを管理する電子マネーの場合は，設定端末などからセン

タ内のポイントを取得しバリューをチャージする．また，航空会社のマイルなど他電子マネー事業者とポイント提携を行っている電子マネーの場合は，提携先システムと相互にポイントの交換を行っている．一般に，ポイント交換を行う場合，提携先システムにおいてポイント交換を行う申請を経てバックエンドでポイントデータが連携されるため，交換するポイントを一旦電子マネーセンターに蓄積しておき，バッチ処理で連携させる運用が多い．

また，他会員へポイントを譲渡するサービスを提供する電子マネー事業者もあり，譲渡する会員の電子マネー会員番号を設定端末などで入力し，該当分のバリューを一旦電子マネーセンターに蓄積後，譲渡先の会員が設定端末などからポイントをダウンロードする仕組みも提供されている．

(h) 流通情報システム内の他システムとの連携

電子マネーセンターが保有する会員情報と取引データ，店舗における売上管理システムと連携することで，購買層や地域，店舗単位の詳細なマーケティングデータを分析する．

4-1-7 その他システム

(1) ネット決済システム

電子マネーカードを利用して自宅の PC からネット決済を行うためのシステムである．電子マネーによるネット決済システムでは，決済を行うクライアントとして市販の IC リーダライタを用いることができるが，店舗に配備される専用の IC カード端末のもつセキュリティ機能を利用することができないため，ネット決済のための特別なアーキテクチャが求められる．

前述の IC カード端末や端末管理システムにて述べたセキュリティメカニズムは，主に端末内の相互認証鍵保護や相互認証鍵を設定された端末の不正利用防止を目的としており，端末内に相互認証鍵を保有することが前提となっている．ネット決済で用いる市販の IC リーダライタは相互認証鍵をもたないため，ネット決済システム側で当該鍵を保有し，ネット決済システムと IC カード間で認証処理を行っている．

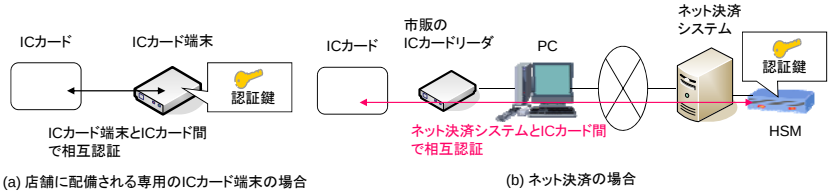


図 4・9 ネット決済システムの概要

(2) TSM（Trusted Sevice Manager）

IC チップ付き携帯電話のモバイル IC チップに対し，無線 IP ネットワーク経由（OTA）で電子マネーアプリケーションの発行や IC チップへの各種書き込みを行う事業者（システム）である．

以下に TSM の概要を示す．

(a) 電子マネーアプリケーションの発行

携帯電話内に各電子マネー事業者の提供する専用の電子マネーアプリケーションモジュー

ルをインストールする．電子マネーアプリケーションは利用者からの操作により携帯電話内で動作し，画面のメニューなどから以下の機能を提供する．

- 前述 4-1-2 項(4)発券機に相当する機能を提供し，モバイル IC チップのユーザ領域に当該電子マネー領域を生成し，個人データの書き込みを行う．これにより，店頭にて電子マネーカードの発行を受けなくても，利用者が時間や場所の制約なく，電子マネー機能を利用できるようになる．
- 前述 4-1-2 項(5)入金機と同等の機能を提供し，現金チャージを除く各種のチャージを行うことができる．
- 前述 4-1-2 項(6)設定端末と同等の機能を提供し，残高参照や各種設定値の確認及び設定変更，ポイント残高の確認などを行うことができる．

(b) OTA によるモバイル IC チップへの IC 処理

上記(a)における電子マネーアプリケーションは，発券機，入金機，設定端末相当の機能を提供するが，これらの処理はモバイル IC チップへのバリュー加算または減算，その他チップの情報の書き換えが発生するため，OTA による IC 処理が必要となる．プラスチックカードの場合は IC カード端末が IC カードと非接触通信を行い IC 処理を実現するが，OTA の場合は IC カード端末を介さず，電子マネーセンターと直接通信を行う必要があることから，前述(1)に示すアーキテクチャと類似したアーキテクチャをとる．

具体的には**図 4･10** に示すとおり，TSM 内の OTA サーバに認証鍵を保有させ，電子マネーアプリケーションからの依頼を電子マネーセンターが受け付け，電子マネーセンターが OTA サーバに IC 処理内容を指示した後に，OTA サーバとモバイル IC チップ間で IC 処理を行うアーキテクチャとなっている．

これらの構成は，携帯電話＝IC カード，TSM＝IC カード端末，電子マネーサーバ＝POS レジと見なすことができ，今後はネットワーク経由で IC 処理を行う基本的なアーキテクチャとして普及が見込まれる．

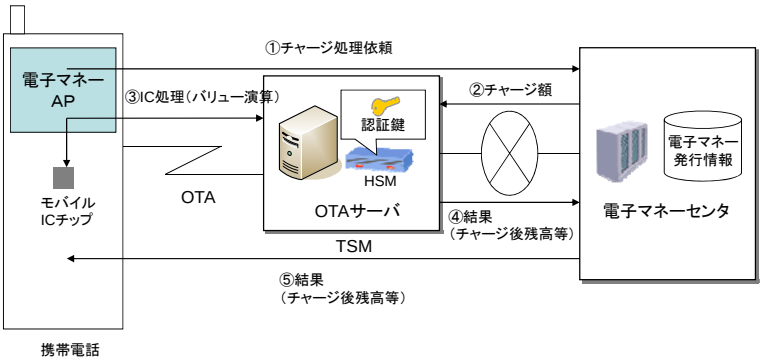


図 4・10　TSM におけるチャージ処理の内容

■11 群 － 6 編 － 4 章

4-2 POS システムなど

（執筆者：長谷川圭一）［2009 年 3 月 受領］

POS（Point of Sale）システムとは，商品や役務の販売に関わる一連の業務（発注，仕入れ，検品，販売）において，それぞれの業務発生時点での情報を捉え，旧来の経験による意思決定だけでなく，得られるデータに基き，予測・マーケティングに活かしたり，在庫管理など，システム連携による業務効率化を実現する総合的な販売情報管理システムである．

なお，POS システムは小売などの販売管理インフラとして定番化されていることもあり，システム全体よりも，もっぱら表に見える店頭での商品登録端末＝POS ターミナル（4-2-1 項(1)）と商品バーコード読取装置＝バーコードスキャナ（4-2-1 項(2)）などの店舗端末の総称とされることが多い．

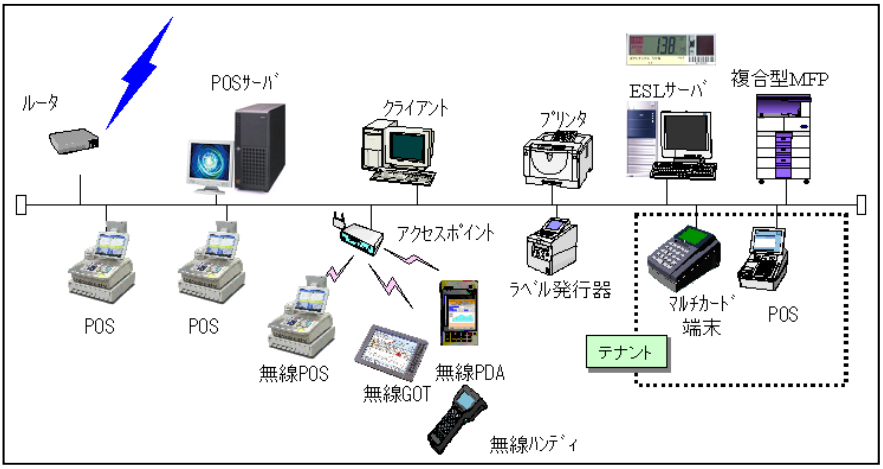


図 4・11　POS システム及び関連機器

4-2-1 チェックアウトシステム

(1)　POS ターミナル

POS ターミナルとは，POS システムにおける商品販売登録と金銭授受の決済処理を行うための入出力装置で，POS（ポス）及び POS レジ（レジ）とも呼ばれる．店頭で消費者と直接接する機器でもあるため店員が必要とする装置（画面，キーボード，レシートプリンタ，ドロワなど）に加え，消費者用の客面表示器をもつ業務専用機器．また，商品販売登録データや決済処理結果はトランザクションデータとして POS システムで共有される．

近年では，この業務専用機器も PC ベースで商品構成されることが一般的となり，商品販売の入出力だけでなく，動画などマルティメディアを活用した情報発信端末としての役目も担うことができるようになってきた．また，自動釣銭機，顧客カード処理端末，電子マネー（IC カード）決済端末など，多くの端末が接続され，かつ使用頻度も高いため，専用オペレータを必要としない機器としては最も過酷な条件で動作している PC といっても過言では

ない．なお，商品販売登録と決済処理という二つの POS ターミナル処理のうち，後者はバーコードスキャナ側の機能充実に伴い，POS ターミナル側ではレシート発行含む決済処理が主な処理となっている．

図 4・12　POS ターミナルの機器構成

(2)　バーコードスキャナ

POS ターミナルに接続されることにより動作する機器で，商品外装に印刷されているバーコードを読み取る装置．なお，店頭に陳列される商品の中でも生鮮品など（青果・鮮魚）はバーコード付加できないケース（もしくは商品マスター登録しにくい商品）が多いため，予め割り付けられたボタンで商品販売登録を行うことが求められる．したがって，バーコードを読取る装置＝スキャナ以外にも商品割付ボタンのある表示装置を搭載したもので構成されるのが一般的である．また，週末などの繁忙時間帯の客捌きを向上させる目的で，POS ターミナル側で決済を行っている間でも，スキャナ側で商品登録処理を重複して行う“2 人制”という処理も多用される．

定置式スキャナ　　定置 2 面式スキャナ　　ハンドスキャナ　　縦型スキャナ

図 4・13　バーコードスキャナの機器構成

POS ターミナル以上に操作する時間が長い機器でもあるため，機器の高さや角度調整機構が搭載されていたり，また，誤ってバーコードを 2 重で読み取ることを防止したり，商品の値引き自動化したりなど，店員操作補助をする機能をも搭載するのが一般的になってきている．

(3)　セルフチェックアウトシステム（SCO）

消費者自ら買い物商品の商品販売登録と決済を行う端末．昨今の買い物スタイルの変化と，厳しさを増す雇用問題への対応から近年急速に普及しつつある新たな形の POS ターミナル．消費者が直接操作する機器でもあることから，操作しやすい環境提供（バーコード化の推進，生鮮品の割付ボタンの整備）とセキュリティ確保機能（商品重量チェック機能，監視カメラ，状況監視モニタ）という今までの POS ターミナルにはない特徴をもつ．

一般の POS システムとは異なり導入すれば効率化が推進されるというものではなく，消費者自身で利用されることによりはじめて効果が出るものでもあるため，顧客サービスレベル（接客，販促）と企業内効率化（人件費削減，雇用難対応）のバランスや，その経営理念や営業戦略により導入店舗や場所，設置台数が決定される機器．

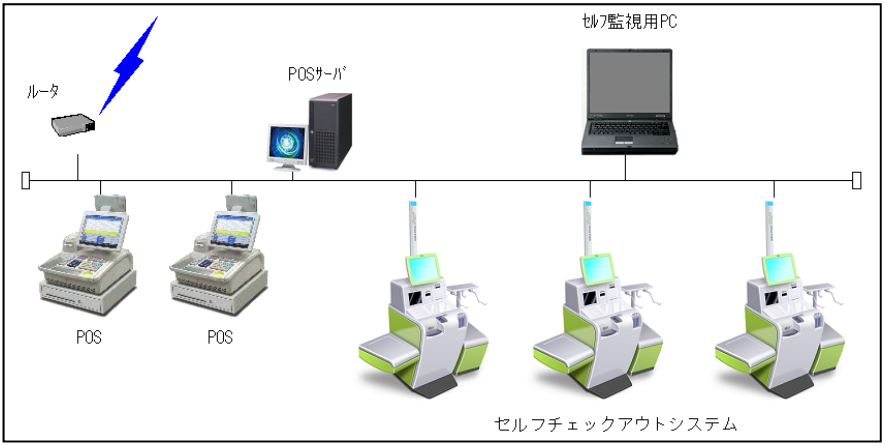


図 4・14　セルフチェックアウトシステムの機器構成

4-2-2 店舗業務システム

(1)　電子棚ラベルシステム（ESL）

昨今急速に導入が加速しているシステムで，棚ラベル（プライスカード）と呼ばれる商品値札に代わり液晶表示化された電子棚ラベル（ESL）と POS システムとを連携させることによって，売価変更ミスの撲滅と，棚ラベルの差し替え作業からの開放を実現することができる新ソリューションシステムである．なお，この電子棚ラベルは売価表示を主とするためセグメント表示の液晶表示器で構成されるのが一般的だが，最近では電子ペーパー的技術（フルドット表示）を応用した製品が数多く開発され，更にはカラー化も見えてきているため，

単なる売価表示だけでなく，商品案内情報表示や商品の販売状況表示が可能になるなど，新たな顧客サービスや店内業務効率化を生み出す可能性を秘めており，発展性を期待されているシステムでもある．

(2) 生鮮管理システム

安全管理・健康志向から食材へのこだわりなど多様化するニーズのなかで，如何に無駄（金額ロス，チャンスロス，廃棄ロス，作業ロス）を減らすかが最大のシステム課題になっており，また，これら課題対応としてはシステム化が立ち遅れている部分でもあったが，生鮮加工機器と POS ターミナルまでもが POS システム全体で連携することにより，今まで解決できなかった課題も対応できるようになってきた．

店内で作業を行う生鮮加工計画の最適化を行うだけでなく，最近では食の安心・安全の消費者意識の高まりから，生鮮加工品のバーコード上に管理データを組み込み（日時），バーコードスキャナ鮮度管理を POS システム連携で行うシステムも導入されてきている．

これにより，万が一，賞味期限を過ぎてしまった商品が店頭に残ってしまった場合でも，それを POS ターミナル側がバーコード上の管理データから販売時賞味期限チェックを行い，消費者の手に渡るのをシステムで防止することも可能になっている．

(3) 決済システム

POS ターミナルの商品販売登録に次ぐ処理が決済処理．現金をはじめ数々の商品券・ギフト券・クレジットカード処理に加え，近年では電子マネー処理も対応されるようになってきた．商品券などの有価証券類はまだ手入力による処理だが，クレジット処理に関しては POS ターミナルから直接与信処理可能なシステム導入が一般化してきた．しかし，近年のセキュリティ対応要求の高まりや非接触 IC 対応とともに，別途に接続されたカード処理端末経由で構成されるケースが多くなってきた．なお，日本国内ではまだ現金決済の比率は圧倒的に高い（特に特に食品スーパー）ため，現金決済もシステム化がされている．最大の課題であった現金の過不足問題は発生要因である手入力ミスを POS 接続された釣銭機により計数できるようになり撲滅の方向に向かっている．また，釣銭用の両替金（棒金）も専用機器で計数する機器も登場し始め，POS システム全体で現金の流れが掌握できるようになった．

4-2-3 まとめ

現在導入がされ始めている POS システム関連の新しい仕組みは，消費者起点ではあるものの店員をはじめ店舗側の効率化や利便性向上を行うものが多く，厳しい雇用状況への対応を反映したものが多く見てとれる．また店員と消費者，オペレータと買い物する人との境目がなくなってきていることも受け入れなければいけない傾向でもある．これから要望されるもの，また創出されるものは，これら“雇用”という視点で自動化・システム化されていくと想定される．