

4Y-1

画面制御におけるアクセス資格管理方式の一検討

松田栄之 菅野政孝
NTT 電気通信研究所

1. はじめに

電子帳票処理においては、同一の帳票を複数の部門(例えば、営業-資材-会計)で持ち回り、一連の処理を進めていく形態が考えられる。このような処理では入力済みのデータに関係者以外の人に見られたくない場合やデータを書き換えられたくない場合がある。本報告では、画面中のデータに対して漏洩の防止、プロテクト等のアクセス制御を可能とする画面制御方式について報告する。

2. 画面制御の概要

2.1 画面制御方式

あらかじめセンタから端末に帳票等を構成する画面構成情報(フォーム)を転送しておく。帳票処理等の業務処理時には、

- (1)センタから画面の識別詞(ID)と出力データを送り、
- (2)端末でそのデータをもとに画面を表示し、
- (3)データ入力後、センタへ画面のIDと入力データのみをセンタへ送り返す。

このように、画面IDとデータのみを送受信で画面入力を可能とする方式を画面制御方式と呼ぶ。図1にその概要を示す。

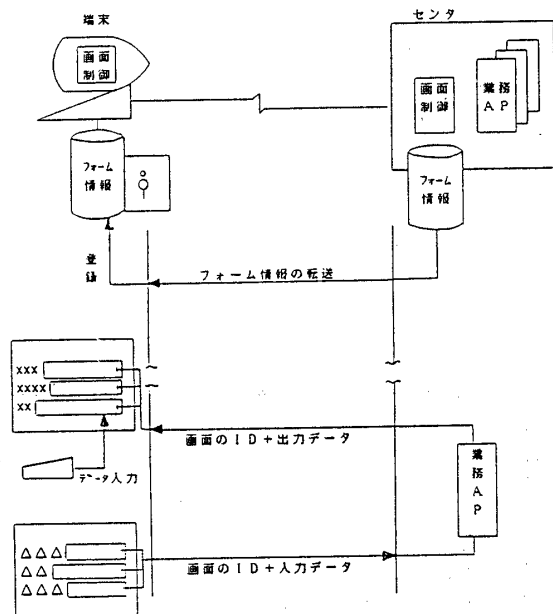


図1 画面制御の概要

2.2 フォームの構成

フォームは以下の要素からなる。

- (1)論理画面：ディスプレイの物理画面にとらわれない仮想的な画面であり、センタとの通信においては、画面のIDと対応する。
- (2)部分画面：論理画面を構成するための要素であり、論理が面上に1つまたは複数の部分画面が存在する。メディアは、部分画面単位に決定でき、文字、およびイメージ等の図形が扱える。
- (3)フィールド：文字を入出力するためのエリア、または、既に入力されたデータを表示するためのエリアであり、部分画面上に存在する。図2にフォームの例を示す。

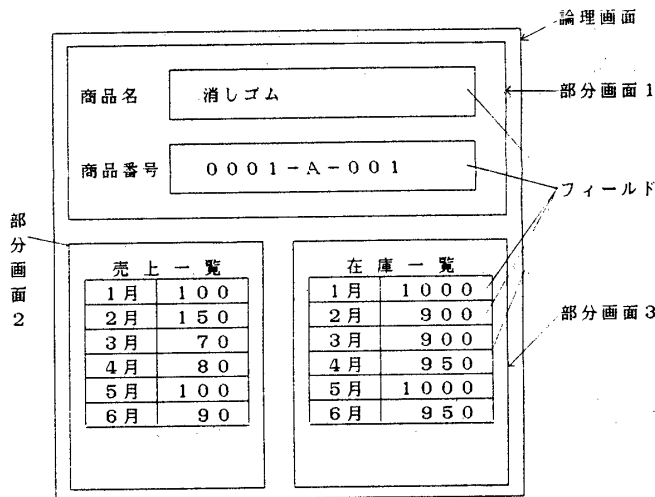


図2 フォームの例

3. 画面処理のアクセス制御

従来、アクセス制御として、パスワードの非表示のように画面のあるフィールドを一律に表示しない制御方式が採られている。一方、帳票処理のような業務処理では、複数の端末から複数の人が帳票処理のルートにそって、順次同一の画面を使用して帳票の入力項目を埋めていき、一枚の帳票を完成していく。このため、帳票処理の過程において以下の処理が必要となる。

- (1)既に入力したデータの参照を禁止する。
- (2)既に入力したデータの更新を禁止する。

これらに対処するために、帳票処理を行う人に対して、データの入出力を許可する等の制御を行う機構が必要となる。以下に、本制御を行うためのアクセス資格管理方式について述べる。

4. 実現方式

4.1 アクセス制御の単位

帳票処理のような定型処理では、それぞれの人が入力する個所は、ある程度定められた比較的単純な領域構成である。そのために、入出力の単位であり、かつ部分画面の構成要素であるフィールドに対してあるまとまった単位で、入出力可否等の制御が可能となる。この単位をアクセス制御領域と呼び部分画面毎に管理する。

4.2 アクセス資格

アクセス制御領域へのアクセス資格管理方式として以下の方法が考えられる。

- (1)個人(グループ)を対象として管理する
- (2)アクセスを許可するレベルにより管理する。

帳票処理の場合、社員、係長、課長、部長というように組織的な階層を経て処理されていく。また、人事異動等による情報の変更に対しても容易に対応できる必要がある。これらの観点から階層的にアクセスレベルを設定できる制御方式とする。

4.3 アクセス制御方式

アクセス制御領域毎に以下のアクセス制御情報を設定する。

(1) 表示制御

情報の漏洩防止等から、特定の人だけにデータを表示するための表示制御機能が必要になる。そこで、表示制御の対象となるアクセス制御領域について、データの表示を認可するアクセスレベルを設定し、表示制御する方式とする。

(2) 入力制御

帳票処理の過程において、部分画面上に既に入力され、表示されているデータについて、特定の人以外には更新をさせたくない場合がある。入力制御の対象となるアクセス制御領域において、データ入力を許可するアクセスレベルを設定して、入力制御を行う方式とする。

(3) 出力制御

入力を許可されたアクセス制御領域においても、入力した文字をエコー出力させたくない場合がある。そこで、エコー出力させたくないアクセス制御領域に対しては、エコー出力させないようにアクセスレベルを設定し、出力制御を行う方式とする。

図3にアクセス資格情報の例を示す。また、図4に実際に表示したイメージを示す。

論理画面	部分画面	アクセス制御領域	アクセス資格情報		
			表示レベル	入力レベル	出力レベル
PPU1	UPS1	A001	0	0	0
		A002	0	0	0
	UPS2	B001	0	1	1
		B002	0	1	5
UPS3	C001	2	2	2	
:	:	:	:	:	:

図3 アクセス資格情報の例

図4 部分画面3のアクセス制御領域を非表示にした例

5. まとめ

画面制御を採用したシステムにおいてデータの漏洩の防止、データの保護等の制御方式について報告した。今後は、本制御方式をシステムに適用し、評価していく予定である。

[参考文献]

- (1)天野他 「分散形画面制御方式」
研究実用化報告 VOL34, NO1, 1985
- (2)家吉他 「端末用画面制御プログラムの構成」
研究実用化報告 VOL34, NO1, 1985