UFJIS株式会社

GUEST SPEAKER

UFJIS 株式会社
取締役
針木 伸佳 氏
Nobuyoshi Hariki
情報システム部 部長
谷本 悟 氏
Satoru Tanimoto
チーフエンジニア
三嶌 琢巳 氏
Takumi Mishima
チーフエンジニア
関 瑞穂 氏
Mizuho Seki
（取材日：2006 年 6 月）

金融機関でエンドユーザ・コンピューティング（EUC）とセキュリティをどう両立させるか。いろいろ考えた末に出した結論は…

旧 UFJ 銀行では、重厚長大な基幹システムのデータを、もっと生き生きと仕事に役立てたいと考え、80 年代後半からエンドユーザ・コンピューティング（EUC※）を推進してきた。ユーザの自由な情報活用とセキュリティをどう両立させてきたのか、詳しく聞いた。

UFJ 銀行は、2006 年 1 月に、東京三菱銀行と合併して三菱東京 UFJ 銀行となりました。
しかし、今回の事例で語られている内容は、すべて旧 UFJ 銀行（旧三和銀行、旧東海銀行）の頃の話です。

ASHISUTO CUSTOMER
UFJIS

UFJISは、どういう会社か

今日はUFJISの皆様に、旧UFJ銀行（現三菱東京UFJ銀行）におけるEUCの歴史を、主にセキュリティの視点から、いろいろお聞きしたいと思います。さて質問に入る前に、まずUFJISの業態についてお聞かせください。

一言で言えば、MUFGグループの情報システムの企画、構築・保守を担っている会社で、その中でも我々「情報システム部」は三菱東京UFJ銀行向けのシステムを担当しております。銀行の情報システムは、一般に勘定系、情報系に大別されます。UFJISが担っているのは、主に情報系の方です。

「MUFGグループ」とは、どの範囲を指すのでしょうか

MUFGは、三菱東京UFJ銀行本体の他、信託銀行、証券会社、カード会社などを含む、総合金融グループです。

旧UFJ銀行はなぜEUCに取り組むようになったか

旧UFJ銀行がEUCに本格的に取り組むようになったのはいつ頃からですか。

80年代後半頃からです。当時は銀行の情報システムの三回目の刷新期、いわゆる第三次オンラインの時期でした。UFJ銀行（旧三和銀行、旧東海銀行）だけでなく、他の銀行でも、EUCに取り組んでいました。

なぜEUCが注目されたのでしょうか。

従来の情報系システムが、現場業務のニーズに合わなくなり、そのギャップを埋めようとして、EUCが注目されたということだと推測します。

銀行の情報システムといえば、いわゆる勘定系。巨大な電算センターに、巨大なメインフレームが、侵すべからざる威容でそびえている。定型的な業務を、定型的な形式で、正確に遂行し、定型的に出力する。正確無比ではあるが、融通は利かない、四角四面の「銀行の基幹システム」というイメージです。こうしたシステムは、1960年代の第一次オンラインでその原型ができあがりました。

しかし80年代も後半にさしかかり、経済環境も激変。与信判断のシステム化を始めとして、様々な意味で情報系システムの比重が高くなってきました。現場としては、様々な情報をリアルタイム収集し、あらゆる角度から分析し、最適な形式で自由に出力したい。そんなニーズが高まってきました。

しかし、ちょっと考えても分かるとおり、こうした「小回り」を求めるニーズと、従来の「重厚長大」な銀行の基幹システムのあり方とは、まったくかみ合いませんでした。

どのようにかみ合わなかったのでしょうか。

例えば、商品開発部が新しい金融商品を開発するために、基幹システムの中のデータを分析、検索したいと考えた場合、当時は、以下の手順を踏まねばなりませんでした。

❶それは通常帳票ではない「臨時帳票」として扱われる。まず、そのような「臨時帳票」を作成することにつき、各部門の承認を得なければならない。さらに分析の形式、帳票の形式などを電算センターに告げねばならない。

❷のみならず、帳票の仕分け手配、必要部署への発送手配など、流通面の手配もしなければならない。

❸手続きには長い時間がかかる。欲しい帳票が届くのは早くて一ヶ月後ぐらい。

※ EUC ?
EUC とはエンドユーザ・コンピューティングの略で、現場で実際に業務を行う者（エンドユーザ）が、自主的に自らコンピュータを操作して、自分あるいは自部門の業務に役立てることをいいます。

しかし、そうして一ヶ月後に帳票が届いた頃には、もうその情報は不必要になっていた、という笑えない話さえ起きていました。

80年代後半にEUCをどのように実現したか

そうした矛盾を解消するために、利用者自らが帳票を構築する、EUCが注目を浴びたと。

そういうことです。80年代後半にもなると、行員のITリテラシーも、だいぶ高くなっていました。自分たちのニーズは自分たちで実現させる方が早い。その方が痒いところにも手が届くだろう。ならば帳票作りは利用者自らにやってもらうことにしようという流れになったのです。

具体的にはどのような形でEUCを実現したのでしょうか。

今までの話を、2006年現在の感覚で解釈して、「なるほど、ユーザのデスクトップから、様々な情報に自由自在にアクセスできるようなシステムを組んだのだな」と想像されたかもしれません。しかし、時代は80年代後半のこと。まだWindows 3.xさえ出ていなかった頃の、汎用機全盛の時代。その頃のEUCは、「ユーザが自らプログラミング言語を駆使して、自分に合う帳票を作っていた」という様態でした。

自らプログラミングとは、具体的にはどういう道具立てで行ったのでしょうか。

情景描写の形で述べてみます。自分オリジナルの帳票を作ろうと考えた行員は、汎用機に繋がった専用端末の黒画面に向かって、簡易プログラミング言語を打ち込みます。すると簡易帳票（罫線もないような黒画面に緑文字が浮かび上がるような帳票）が表示される。それを見ながらデバッグして、上手くいったら完了。紙に打ち出す。そういう光景です。

非常に率直な感想として、ユーザ自らプログラミングを行うなんて、よくそんなことができたなと。

今の感覚ではそうかもしれません。でも80年後半に時計の針を戻して想像してください。電算センターに鎮座する、あの巨大な汎用機から、自分の思い通りのデータを自由自在に取り出せる。もっと露骨に言えば、「メインフレームを思いのままにガンガンまわせる！」という感覚。利用者にしてみれば、モチベーションは高まります。正直言いまして、そのようにマシンリソースを使われるのは、システム部門としては困った話でしたが、それでユーザがやる気を出して、情報を活用して良い仕事をしてくれるのなら、それはそれで良いことかなと。

以上、ここまでが旧UFJ銀行のEUCの第一期の話です。続いて、2004年頃から始まる第二期の話をしようと思います。

「『見せない。牽制する。証跡を残す』が基本コンセプトです」（谷本氏）

性善説から性悪説への転換

第一期と第二期とは、何により区分されるのでしょうか。

平たく言えば、個人情報保護法以前・以後という区分です。その頃は、大手ＩＳＰで大規模な情報漏洩事故が起きたり、個人情報保護法の施行が迫ってきたりするなど、セキュリティに関する外部環境が切迫していました。それに伴いＥＵＣにも見直しが必要になりました。

もちろん個人情報保護法以前の第一期においても、セキュリティに関する必要な対策、手当は行っていました。しかし、それは「社員は悪いことはしない」という性善説に基づいた施策でした。

セキュリティを強化するために、その前提を改めることにしました。「人間は悪いことをすることがあり得る」という性悪説を前提にして、システムを設計し直すことにしたのです。

「性悪説」を前提としたシステム設計での注意点

「性悪説」を前提としたシステムを設計する上で、気をつけたことは何ですか。

以下の三点を基本コンセプトにしました。

❶見せない

「情報は、見てよい人に、見てよい時にだけ、必要な分だけ見せる」を基本思想にしました。

❷牽制する

データベース内の重要情報を、参照・利用した場合は、その利用履歴を、所属部署の管理者に還元します。管理者は、その人が不適切な情報検索をしていないかチェックします。これは事後チェックの効果の他に、「会社は利用履歴を監視している」ということを知らせて、情報の濫用を防ぐ意味合いがあります。性悪説に基づく抑止策です。

❸証跡を残す

万が一、情報漏洩が発生した場合でも、いつどこで誰が漏洩したのかをすぐに事実把握できるよう、利用履歴ログの保存期間をできるだけ長くするようにしました。

「情報は、見てよい人に、見てよい時にだけ、必要な分だけ見せる」

では、3つの基本コンセプトにつき、一つずつお聞きいたします。最初のコンセプト、「見せない」、「情報は、見てよい人に、見てよい時にだけ、必要な分だけ見せる」とは。

このコンセプトをさらに細分化して記述すると以下のようになります。

❶情報を見てよい人

全行員のうち、「データベースにアクセスしてもよい」とされる人を抜き出して定義します。

❷情報を見てよい時

「情報を見てよい人」であっても、いつでも見てよいわけではありません。見てもよい時と、いけない時を定義します。

❸必要な分だけ

データベース内の情報は、基本情報と重要情報に大別できます。「情報を見てよい人」であれば、基本情報はいつでも見られます。しかし「重要情報」は、申請がないと見られません。

「情報を見てよい人」をどう定義したか

細分化した各項目についてさらに詳しくお聞かせください。まず〝情報を見てよい人〟の定義についてさらに詳しく。

〝情報を見てよい人〟とは、以下のように絞り込み定義されます。

❶〝データベースを見てよい人〟という大集団を定義する。

❷「データベース」を、さらに「データベースA種」、「B種」、「C種」に細分定義する。そして各情報のオーナーを定義する。

❸細分定義された「個別データベース」を見てもよい「部署」を定義する。

さらに絞り込んでお伺いします。まず「〝データベースを見てよい人〟という大集団を定義する」とは具体的には。

全行員のうち、業務上データベースを見る必要がある行員１６００人を定義し、

「重要情報を見てもよいかどうかは、管理職かどうかで定義すればいいと思っていたのですが、実際には…」（左から三嶌氏、関氏）

それら行員にユーザＩＤを与えます。重要書類が保管されているビル（＝データベース）への入館証（＝ユーザＩＤ）が与えられているイメージです。ただしユーザＩＤは『入館証』にすぎません。入館証があるからといって、すべての書類が閲覧できるわけではありません。

個別データベースのオーナーをどう定義したか

次の絞り込み定義、「『データベース』を、さらに『データベースＡ種』、『Ｂ種』、『Ｃ種』に細分化する。そして各情報のオーナーを定義する」とは。

先ほどの比喩を引き継いで説明してみます。重要書類保管ビルの中に、Ａ室、Ｂ室、Ｃ室と各部屋がある。各部屋には必ずオーナーがいる。誰がその部屋に入ってよいかはオーナーが決める。そういうイメージです。

それでは具体的に、「法人の取引履歴データベース」を題材にして、説明してみます。

❶そもそも、基幹データベースとは別個に個別データベースが派生するのはなぜか。もちろん自然発生ではない。

❷これは、特定の部署が、情報システム部門に個別データベースの作成を「発注」するから、発生するのである。「法人の取引履歴ＤＢ」の場合は、法人統括部が発注して作った、というように。

❸今使った言葉「発注」は、言葉のアヤではない。法人統括部が、社内取引の形で、情報システム部門に対しコストを支払って、そのデータベースを作るのである。

❹したがって、「法人の取引履歴ＤＢ」のオーナーは法人統括部である。発注者（コスト負担者）がオーナーというのは、シンプルな図式である。

❺しかしながら、「法人の取引履歴データベース」の中の情報は、融資部や審査部としても活用したいところだ。

❻そこで、オーナーである法人統括部は、自分以外のどの部署がデータを閲覧して良いかを定義することができる。許可する・しないの決定権は、オーナーである法人統括部に帰属する（もちろん、ＭＵＦＧグループ全体の利益を考えて、常識的に決定することになるが）。

さて、ここまでで、〝重要情報を見てよい人〟の定義が、「ユーザIDを持つ160人」→「個別データベースのオーナー部門」→「そのオーナーが許可を与えた各部署」まで絞り込まれました。ここまで来れば、もう一段階。部署内の「各個人」というレベルまで絞り込みたいところです。

個人レベルでの「情報を見てもよいかどうか」をどう定義したか

「各個人レベルへの絞り込み」は、どうやって行ったのでしょうか。

最初は、単純に職掌で分ければよいと考えました。管理職なら、情報を全部見てもよい。一般職は、限定された情報しか見てはならないという、よくある手法です。

この手法は「業務の中で重要情報を使う必要が生じるか、生じないかは、職掌と相関関係がある」という仮説に基づいています。次にこの仮説が正しいのかどうか調査を始めました。

どのような調査を行ったのでしょうか。

過去半年分ぐらいのデータ利用ログ数百万件につき、どんな職掌の人が、どんな検索をしているのか、子細に調べました。その際には、WebFOCUSの「リソースアナライザ」という稼働統計・監査証跡オプション機能を使って、分析を行いました。

分析の結果は。

結果として、「業務の中で重要情報を使う必要性と職掌の間には、必ずしも相関関係があるわけではない」ことが分かりました。重要情報を見る人は、管理職のみならず、「その管理職から指示されてデータ検索をしている一般行員」、「データ分析の実務に長けている人。現場実力者」なども含まれていました。

一般職の行員が、普段から重要情報を見ることができるのは適切でない。しかし上司に指示された場合は、重要情報を見るのは問題ない。つまり、「データを見てよいかどうか」を個人に紐付けるのは困難だということになりました。同じ一人の人間であっても、重要情報を見てよい時もあるし、見てはよくない時もあると。

「データを見てよいかどうかは個人に紐付けられない」…では、ある個人がデータを見てよいかどうかは、結局、何を基準に定義するのでしょうか。

結局のところ、昔ながらの「申請制度」にしました。重要情報を見る必要がある場合は、申請してもらう。上長の許可が下りたら、データが見えるようになる。そういう仕組みにしました。つまり、データを見てよいかどうかは人にではなく、行為に紐付けたということです。この部分が、先に述べた〝情報を見てよい時〟の定義」になります。

しかし、「申請→許諾→閲覧」という流れは、いかにも時間がかかりそうです。ユーザのフラストレーションがたまるのではないですか。

おっしゃるとおりです。そこで今回は、「申請→閲覧」までの時間を最短にするよう、実装段階で工夫をこらしました。その工夫は、後ほど説明させてください。

情報は「必要な分だけ見せるようにする」ことをどう実装したか

ここまでで、〝情報を見てよい人〟が、〝情報を見てよい時〟に、〝必要な分だけ〟見る」という3つの基本コンセプトのうち、最初の2つについてご説明いただきました。最後のコンセプト〝必要な分だけ〟についてもお聞きしたいと思います。

〝必要な分だけ〟については、以下のように実装しました。

❶個人（法人）が特定できるデータについては、通常はマスクをかけて見えないようにする。データを匿名的にする。

❷「申請→承認」のプロセスが完了したら、そのデータのマスクが取れて、見えるようになる。

❸つまり、通常は蓋が閉まっていて、承認が下りたら蓋が開くというのがマスクのイメージ。

セキュリティ強化を具現化するにあたり、苦労したこと、工夫したこと

ここまでUFJISの「性悪説」を前

提としたシステムの「設計思想」が分かりました。続いて、その設計思想を具現化するために「苦労した点」や「実装の工夫」についてお聞きしたいと思います。

苦労した点は、セキュリティ制限の導入に対し、銀行内が、総論賛成各論反対に陥ったという点です。

工夫した点は、以下の通りです。

❶申請が通ったらデータがすぐ見られる、「即時性」に気をつけた。
❷期間が過ぎたら、すぐデータを見えなくする「逆即時性」にも気を遣った。
❸数万本の既存のプログラム資産を引き継げるようにした。

銀行内の総論賛成、各論反対にどう対処したか

まず、「苦労した点」についてお聞きしたいと思います。「セキュリティ制限の導入に対し、銀行内が、総論賛成各論反対に陥った」というのは、具体的には。

「これからは、個人情報保護やセキュリティに気をつけなければならない。だから情報系のシステムもセキュリティを強化していく」といえば、反対する人はいません。皆が皆、それは銀行として当然のことだ、ぜひ推進するべきだと言います。総論賛成です。

しかし、いざ自分がこれまでEUCを活用して、自由自在に検索、活用できていたデータが見られなくなるという話、自分の活動に制限がかかるという具体論になると、異議が起きます。「その帳票をスピーディに見られることは業務上、必須だ」等、各論反対に陥ります。

その各論反対にどう対処したのでしょうか。

セキュリティ強化（性悪説）を持ち込む以上、使い勝手は不自由になる。これは避けられません。実装で工夫できるのは、その不自由さを少しでも軽減することです。ゼロにはできない。しかし最小限にするよう努力する。

また、泥臭い話にはなりますが、セキュリティ強化の必要性につき、各部門に出向いて、直接の対面を通じて説明しました。

セキュリティ強化に伴う不自由さを軽減するための工夫

今おっしゃった「不自由さの最小化のための工夫」が、工夫した点の1番と2番、「申請が通ったらデータがすぐ見られる、『即時性』に気をつけた」と「期間が過ぎたら、すぐデータを見えなくする『逆即時性』にも気を遣った」ですね。これらは具体的に、どのような工夫でしょうか。

機密情報は、普段はマスクがかかっており、「申請→承認」のプロセスを経て、見えるようになります。しかし「申請→承認」というプロセスは往々にして、停滞しがちです。データを見たいと思う。申請する。承認が下りるのをじっと待つ。やっと承認が下りて、それから情報システム部に承認が下りた旨を伝え、そうしてやっとデータが見られるようになる。考えただけでも面倒…。そう思うのが人間の自然な感情です。

このまどろこしさを少しでも軽減するために、承認が下りた瞬間に、直ちにデータが見られるような仕組みにしました。

もう一つのポイント「すぐデータを見えなくする『逆即時性』にも気を遣った」とは。

データのマスク解除には期限があります。仮に、「あるデータが見えるのは一日間」と設定した場合には、マスクを解除した日のきっかり24時に、マスクが復活して、データ閲覧は直ちにシャットアウトされます。これが逆即時性です。

数万本の既存プログラム資産を生かすために

工夫した点3番目「数万本の既存のプログラム資産を引き継げるようにした」とは具体的には。

今回、重要データを「カット」するのではなく「マスク」をかけるという手法をとった最大の理由は、既存のプログラム資産を継続活用したかったことが最大の理由です。80年代末にEUCを導入して以来、行員が手作りしたプログラムが積もり積もって数万本。もしデータをカットして、データ構造を変えてしまうと、これらのプログラムが全部使えなくなります。しかしデータのマスクならデータ構造は変わらないので、その心配はありません。

製品としてのWebFOCUSへの評価

続いてWebFOCUSへの評価をお聞きしたいと思います。

「現場でデータ抽出・帳票を簡単に出したい」というEUCの観点から、複数製品を検討した結果、WebFOCUSを行員のデータ抽出・レポーティング標準ツールとして採用しました。また、今回はWebFOCUSをベースとしたデータ・レポートの参照履歴分析、マスク解除申請機能等を作成しました。WebFOCUSは短時間で誰でも簡単に帳票が作れるという触れ込みでしたが、その宣伝通りでした。よい製品だと思います。

帳票というのは、作ってみたはいいけれど、「あ、やっぱりこの項目とあの項目は位置を入れ替えたいな」というように、都度都度、微調整を加えたくなるものです。そういう微調整も、WebFOCUSを使えば簡単にできます。

ちなみに使用者側の実感として、WebFOCUSはどのぐらい簡単だったでしょうか。簡単さを表す言い方として、「Excel・Wordができる人なら使える」という言い方もありますが。

Excelよりは、少し難しいかもしれません。でもAccessより簡単なことは間違いありません。Excel以上Access以下という印象です。

先ほど、WebFOCUSは簡単にデータ抽出、帳票を作れるのがよいと申しました

「私たちの成功体験や失敗体験、気づきを広く世の中のお役に立てられればと考えています」(針木氏)

が、その一方で、複雑な処理の作り込みを許容しているのも魅力の一つです。上級者の場合は、簡単なＧＵＩではなく、直接エディタでプログラミング入力したい場合もあります。WebFOCUSの場合は、それも可能です。つまり、なるべく簡単に済ませたい初心者から、作り込みがしたい玄人まで広くカバーしている点も良いと思います。

会社としてのアシストへの評価

会社としてのアシストの印象はいかがですか。

「小さく打ってもよく響く」ところがよいと思います。こちらが、何となく思いつきレベルで、こんなことができればなと淡くつぶやいたことに対して、濃い目の提案を出してくださいます。さすがにソフトウェア商社だけあって引き出しの多い会社だと思います。一方で「単なる提案屋さん」でない点も評価できます。

「単なる提案屋さん」とはどういうものですか。

ソフトウェア商社の中には、引き出しが多いのをよいことに、5個も6個も提案を持ってきて、どれがいいですか、お客様の方で決めてくださいというところがあります。これが「単なる提案屋さん」。しかし、アシストの場合は、こちらの状況や課題をよく勉強して、一本、濃い提案をドンと持ってきます。そのような提案は、こちらとしても検討しがいがあります。

今後の課題、そしてアシストへの期待

最後に、ＵＦＪＩＳにおける今後の展望について、お聞かせください。

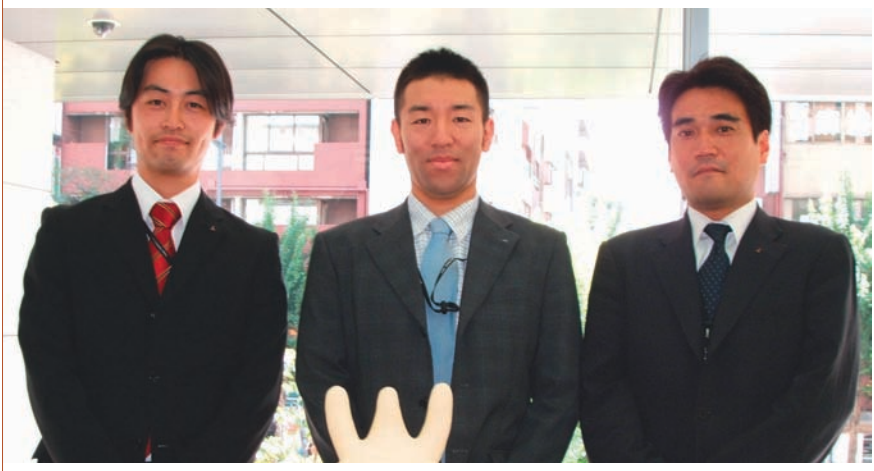
今まで培ってきたノウハウをＭＵＦＧグループのために役立て、グループの事業競争力強化に貢献したいと考えています。

ＵＦＪＩＳでは、銀行、証券等において大型プロジェクトを完遂してきました。その中で、成功体験、失敗寸前のヒヤリ体験、泥臭い運用ノウハウなど、様々な蓄積がなされたと自負しています。そうした蓄積ノウハウを、当面はＭＵＦＧグループの情報活用のために役立てていく所存です。

アシストには、今後もWebFOCUSを始めとする製品群や、その活用ノウハウ、濃い提案などを通じて、弊社の取り組みを下支えいただければと思います。今後もよろしくお願いいたします。

担当者の声
ASHISUTO MEMBERS

お客様とベンダー、さらには
パートナーという関係を超えて、
お客様の一員としてシステム構築に
携わらせていただきました。
お客様のご要望を実現するだけで
なく、お客様が気付いていない、
潜在要望・課題からご提案できる
よう、努力し続けて参ります。



本部EUCシステム構築支援メンバー

現在、UFJIS様で
ご利用いただいている製品、サービス

- BI ツール（設計～実装支援含む）
- データ連携ツール（設計～実装支援含む）
- 負荷テストツール
- 各種保守サポート