

Server Based Computing技術の活用による スルガ銀行殿情報系基盤セキュリティ強化の実現

金子 桃子

大企業で相次いで発生した情報漏えいなどの事件から、情報セキュリティの維持が企業の社会責任の一つとなってきている。特に、企業に対して個人情報の適正な取扱いなどが求められる中、2005年4月「個人情報保護法」が施行された。

金融機関では、お客様の個人データを取り扱わなければならないことから、金融庁のガイドラインに従った個人データの安全管理が必要となり、一層のセキュリティ強化が求められることとなった。

スルガ銀行株式会社殿（以下、スルガ銀行殿）では、情報系PC（パーソナルコンピュータ）の更改検討に併せて、情報漏えい対策に主眼をおいた情報系システムの基盤強化の検討を開始した。同行では、他社に先駆けてIT戦略を展開しており、静岡・神奈川を中心にした地域ビジネスから飛躍し、全国規模の顧客に対するリテール金融ビジネスを実践している。また、お客様のことを第一と考えて行動する『コンシェルジュバンク』として、お客様のく夢をかたちに>するく夢に日付を>いれるお手伝いをすることを使命として、お客様のニーズに一つ一つ誠意を持って接している銀行である。

本稿では、近年そのセキュリティの高さや管理の容易

性などの特長から、新しいシステム基盤として注目を集めているSBC（Server Based Computing）技術を活用した、スルガ銀行殿向け情報系システム基盤について、その特長と効果を記述する。

システム導入の背景

スルガ銀行殿の情報系システムは、既にクライアントサーバシステムで構築されており、約1,500台のWindows NT 4.0 WorkstationベースのPCが稼動中であった。

本システムの構築にあたっては、『既存資産の有効活用』『運用管理面の改善』『PCセキュリティ環境の強化』『最新PCへの更改』の4つの要件を満たす、最適なシステムの構築を求められた。これら銀行殿の要件から、情報系システム全体としてのセキュリティの確保はもちろんのこと、TCO（Total Cost of Ownership）削減など運用面での効率化にも配慮した、新しい情報系システム基盤を検討し構築することとなった。

システムの特長

スルガ銀行殿の情報系システム基盤には、すでにActive Directoryによるドメイン環境が構築され、PCのユーザー

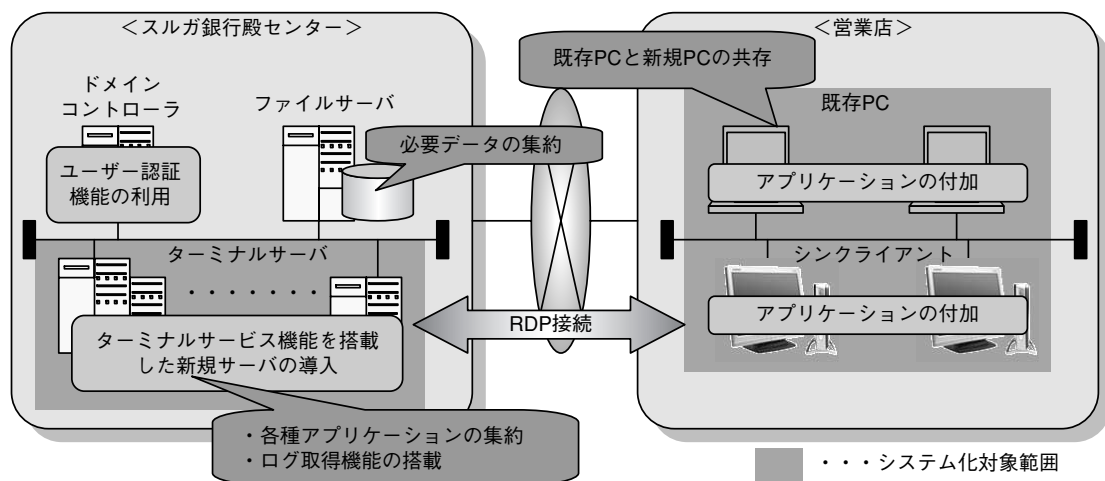


図1 導入後のシステム構成

管理の一元化が実現されていた。また、ブロードバンドネットワークなどのインフラストラクチャも整備されていた。

本システムでは、これらの既存資産を最大限に活用し、かつ銀行殿セキュリティ要件を満たすため、Microsoft Windows Server 2003のターミナルサービス（後述）を採用した（図1）。

また、ターミナルサービスの導入だけでなく、新規アプリケーションの開発も行い、更なるセキュリティ強化を実現した。

以下に、本システムの特長について述べる。

(1) ターミナルサービスの導入

これまで、新たにアプリケーションを導入するには、各拠点に設置されている全ての情報系PCに対し、アプリケーションのインストールやバージョンアップを行う必要があった。また、PCの使用者がアプリケーションを個別にインストールする可能性もあり、アプリケーションの維持管理や運用面での課題があった。

ターミナルサービスでは、各種アプリケーションやデータをすべてサーバにインストールし管理することができる。そして、サーバ上にインストールされるこれらアプリケーションは、最小限の入出力情報（キー情報やマウス情報、画面情報等）のやり取りのみで、遠隔地のPCより実行することができる（図2）。

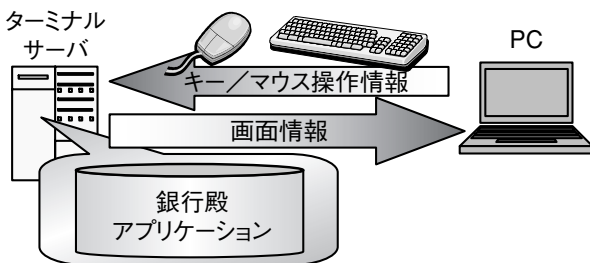


図2 ターミナルサービス動作概念図

以上のような特性より、PCは画面表示に特化した専用端末となり、使用者にはこれまでと同様の利用環境を提供することができる。

これにより、従来全てのPCへインストールしていた各種アプリケーションを、サーバ上で一括管理できる基盤を構築した。

また、PCの使用者の環境を全てサーバに保有することで、どのPCを使用しても、常に同じ環境でPCを利用することが可能となった。

(2) セキュリティの強化

通常のターミナルサービスでは、PCの操作には制限がからず、自由にその機能を使うことが可能である。そのため、PC上にファイルを保管できるなど、セキュリティ面での課題が残っていた。

そこで、新たなアプリケーションを開発し、ターミナルサービスの機能と組み合わせて、銀行殿セキュリティ要件を充足した。

●PCの機能制限

PC環境に制限を加える手段として専用のログインアプリケーションを開発した。これにより、PCの使用者はログイン後に表示される専用画面（図3）のみが操作可能となり、それ以外のPC環境を隠ぺいすることができた。



図3 PC初期画面イメージ

●印刷物の出力管理

印刷物には顧客情報などさまざまな個人情報が含まれるため、厳正な管理が求められる。そこで、PCからの出力処理を検知し、記録を行うためのアプリケーションをターミナルサーバ内に組み込み、印刷物の出力管理を可能とした（図4）。

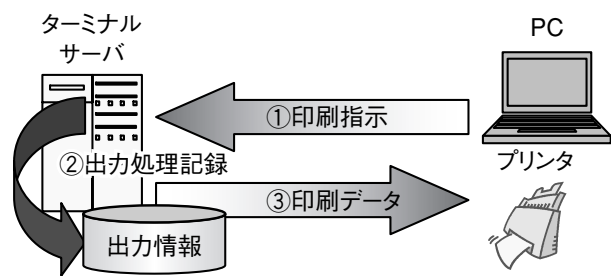


図4 印刷物出力管理概念図

これにより、PCでの印刷履歴がセンターで一括管理できるようになった。

●各種データへのアクセス規制

個人情報を含む各種データは、厳正な管理が求められ、PCの使用者ごとに異なるアクセス管理を実施できる環境が必要であった。

スルガ銀行殿では、営業店ファイルサーバをセンター集約し、データの集中化とデータアクセスの管理を行っていた。

そこで、この権限管理をターミナルサーバでも利用することにより、データへのアクセスに制限をかけられるようにした(図5)。

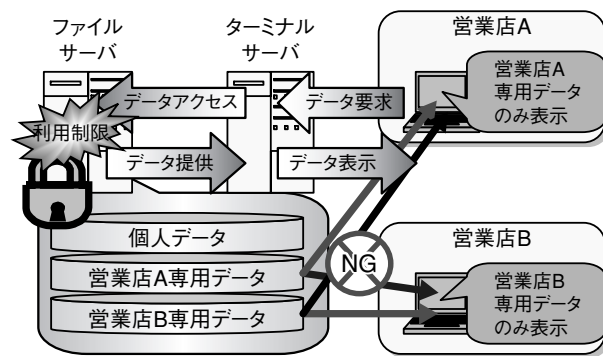


図5 アクセス規制概念図

●ログイン環境の統一によるプリンタの使用

ターミナルサービスの導入により、異なる場所からでも同じ環境でPCを利用することが可能となったが、プリンタの使用に関してのみ、同じ環境で利用できない、という課題が残った。

そこで、サーバに組み込むプリンタ表示用アプリケーションを開発した。たとえば出張などで、一時的に異なるロケーションのPCを使用しても、常に同じ環境で起動

し、表示されるプリンタのみロケーションに適合している、という環境の提供を実現した(図6)。

(3) PCの更改

本システムにより、既存PCでのセキュリティ強化を実現した。しかし、一部の既存PCの老朽化が進んでおり、併せてその更改を検討する必要があった。

そこで、本検討にあたり、通常のPCではなくシンクライアントをその第一候補とした。シンクライアントは、ハードディスクなどを保有せず、画面表示に特化した専用端末である。情報を筐体内に保有できない特長から、個人情報保護対策のための端末としても近年注目を浴びている。

今回、スルガ銀行殿においては、本システムを構築したことで、シンクライアントを導入する環境が先行して構築できていた。そこで、通常のPCからシンクライアントへの更改を、特に新たな対応を行うことなく実現できた。

システム導入による効果

本システムにより、スルガ銀行殿新情報系システム基盤は、既存資産を有効活用しつつ、高いセキュリティを確保することができた。さらには、運用管理面、クライアントPCの処理速度といった性能面でも高い効果を発揮し、銀行殿要件を満たした最適なシステムが実現できた。

(1) セキュリティ管理の向上

SBC技術の導入や各種データのセンター集約により、PC上にはファイルなどのデータが保有されなくなり、各営業店や各部署が保有する個人情報が増減された。管理対象情報の削減はすなわち、情報漏えい防止につながる。

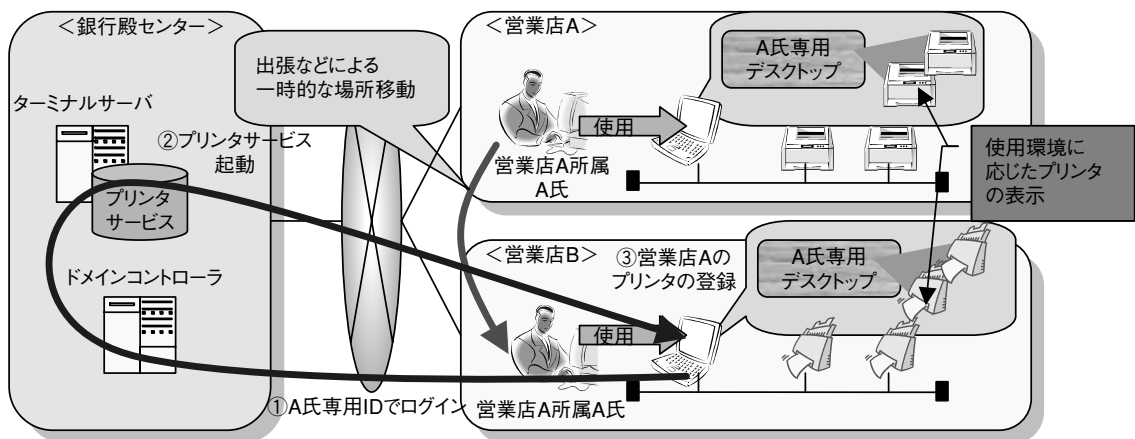


図6 プリンタ表示システムイメージ

さらに、付加機能として提供した各種アプリケーションや仕組みによっても、さまざまなセキュリティ強化が実現されている。

既存PCのローカル環境のロックや、各種データへのアクセス制限により、悪意あるデータの改ざんや、個人情報を含む保護対象のデータの流出といった危険性が極小化され、システム面での課題が解決された。

また、印刷ログ収集機能は、ファイルの不正印刷や不正利用を監視・けん制する効果をもたらす。

さらに、ログイン環境が統一されたことで、ユーザーに対して個別のセキュリティ管理が行えるようになった。たとえば、『取得している印刷ログのユーザー単位での管理』や『ファイルへのユーザー単位でのアクセス制限』などである。

環境面でも、新規PCとしてシンクライアントを導入したことにより、PCの盗難等によるデータの流出の危険性などが削減された。

(2) 運用負荷および管理の軽減

アプリケーションの一元化は、運用管理の負荷軽減にもつながる。

アプリケーションの追加と削除は、センターのターミナルサーバ上へ行うことで、すべてのPCに反映される。また、アプリケーションのライセンスもすべてサーバ上へ登録することになり、メンテナンスやライセンス管理の簡易化とTCO削減を実現した。

(3) クライアント性能の向上

今回のシステムにより、アプリケーションの動作環境をサーバ上に移行することができ、アプリケーションの

処理がサーバの能力に依存する仕組みとなった。そのため、Windows NT4.0という旧式のクライアントPCでも、快適なスピードで最新のアプリケーションを使用できる環境が実現し、クライアントの性能を向上することができた。

これは、従来のPCを、従来環境よりも高い性能を持つ最新の環境で使用できるということであり、ユーザーにとっても大きくメリットのあるシステムが構築できた。

おわりに

2005年3月より本システムは稼働を開始し、セキュリティ強化を特長とする情報系システム基盤構築の成功事例とユーザーから評価されている。

また、本格的な検討から稼働開始まで約3ヶ月という短期間で構築できたことも評価されているが、ユーザーであるスルガ銀行殿の協力無しでは成し得なかったであろう。

本システム稼働後に導入を開始したシンクライアントについても順調に拡大中であり、最終的には全営業店に展開する予定である。

さらに、今後予定されている勘定系端末との“ログイン環境”の統一化でも、本システムの活用により最小限の投資での対応が可能であり、そこでも柔軟性ある情報系システム基盤として最大限の役割を果たす予定である。



● 筆者紹介

金子桃子：Momoko Kaneko. 金融ソリューションカンパニー 金融システム本部 バンキングソリューションSE第二部

TIPS

【基本用語解説】

SBC (Server Based Computing)

アプリケーションとデータをサーバに置くことで、クライアントの処理機能をサーバで代行し、クライアントアプリケーションをサーバで集中的に管理・運用する仕組み。

クライアントサーバシステム

コンピュータをサーバとクライアントに分け役割分担をして運用する仕組み。

RDP (Remote Desktop Protocol)

ターミナルサービス独自のプロトコル。TCP/IPベースのプロトコルで、クライアントPCのマウスやキーボードのユーザ入力情報をサーバ側に伝送したり、サーバ側の画面情報をクライアント側に伝送したりする。

TCO (Total Cost of Ownership)

コンピュータシステムの導入、維持、管理などにかかる費用の総額。

ターミナルサービス

ターミナルサーバ上に仮想的に構成されたWindowsデスクトップを、クライアントPCから利用して、サーバ上のアプリケーションや管理ツールなどを実行するための機能。

Active Directory

ネットワーク上に存在するサーバ、クライアント、プリンタなどのハードウェア資源や、それらを使用するユーザの属性、アクセス権などの情報を一元管理するための仕組み。

*記載されている会社名、製品名は一般に各社の商標または登録商標です。