

次世代金融ネットワークソリューション

鈴木 一義 広重 克典

金融機関は自社の商品・サービスの提供にとどまらず、証券会社等の異業種金融機関や地方自治体と連携し幅広い商品やサービスを提供するようになってきた。またこれらのサービスを実現するソリューションはIP（インターネットプロトコル）ネットワークインフラ上に構築されるのが一般的になってきている。従来は専用線に接続するだけであったが、今後は各々のソリューションに対して最適なサービスレベル、セキュリティレベルの提供が必須となってくる。さらに映像メディアを扱うようになると快適性の提供も必要となる。このような状況から各ソリューションの有効性がネットワークインフラに依存していると言っても過言ではない。

またサービスレベルは低い、従来のデジタル専用線の何十倍もの高速回線が何十分の一という価格で提供されているFTTH（Fiber to the home）接続サービス等の一般家庭向けブロードバンドサービスも法人利用が加速的に進み、今や金融機関でも無視できない回線サービスとなってきている。このように現在ネットワークインフラは大きな転換期を迎えている。

本稿では、これらネットワークインフラ動向を踏まえ次世代の金融ネットワークソリューションに対しての冲電気の取り組みを紹介する。

金融ネットワークの動向

図1に示すように金融ネットワークモデルは、自行の店舗外や営業店を接続する自行ネットワークとネットワーク監視等の運用管理アウトソーシングサービスや他社ASP（アプリケーションサービスプロバイダ）サービスを利用するために接続する外部サービス用ネットワークの2つの大きなネットワークから構成される。自行のセンタには各種ネットワークやサーバなどの機器を接続しIPパケットをルーティングするスイッチ機能とネットワーク上で展開されるさまざまなサービスやシステムをシームレスに連携統合するハブ機能から構成される。ハブ機能は各システム間連携のみならずセキュリティ機能を持たせることによりアウトソーシングサービスなどの外部接続の切り口ともなる。なお図1は論理的な構成を示しており物理的な構成とは異なる。

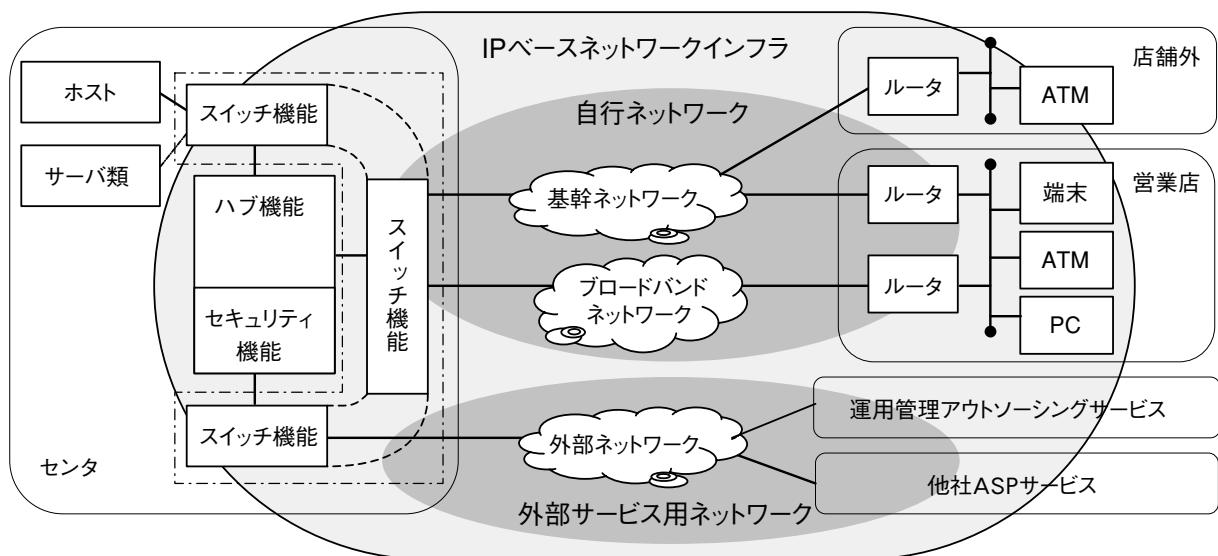


図1 金融ネットワークモデル

さらにネットワークモデル全体がオープンなIPインフラ上で構成されるため、既存システム（メーカ独自の従来型システム）に比べ、セキュリティに対して脆弱であると言われているが、ベンダーにとらわれず機器やサービスなど選択の幅も広がり柔軟な構築が可能である。またIPベースの特徴の一つに物理的なロケーションの制約が少ない点が上げられる。つまりセンタ側のスイッチ機能やハブ機能は、通信事業者のハウジングサービスを利用してネットワーク内に取り込むことも可能である。システムを購入しサービスを実現する方法から今後はIPセントレックスサービスのようにASPからサービスのみ購入する方法も普及してくる。

このような今後のネットワークモデルのポイントとして3点挙げられる。

- ① ブロードバンドネットワーク（BBNW）の導入
- ② セキュリティレベルの導入
- ③ アウトソーシングサービスの活用

ブロードバンドネットワークの導入

世の中のネットワークインフラとして、IPをベースとしたIP-VPNや広域イーサネットといった広帯域のネットワークサービスが普及し、デジタル専用線やフレームリレー網からの世代交代が急速に進んでいる。また個人ユーザ向けにブロードバンド社会を牽引してきたFTTHやADSLの法人利用が増加し、回線サービス選択の幅が大きく広がってきている。

従来の金融機関ネットワークは、信頼性の高い、帯域の保証された専用線を使用してきた。また情報系のトラフィックもそれほど多くなく、高価な専用線を有効利用

する意味でも勘定系、情報系のトラフィックを同じ回線で統合するアーキテクチャが用いられていた。

しかし、回線サービス選択の幅が広がり回線料金の価格破壊も進んでいる現在、IPを基本にその時点での最適な回線サービスに乗り換えていく方法が有効である。従来の高信頼、高価な回線サービスに全てのトラフィックを統合するのではなく、アプリケーションごとにサービスレベルを定め、各レベルにあったネットワークを構築する考え方である。

同じレベルのトラフィックは統合し、異なるレベルは別ネットワークとする。別ネットワークで利便性が損なわれるのであれば、センタや通信事業者内の拠点にて相互接続を行う。セキュリティレベルが同じであればネットワークレベルで接続し、異なるセキュリティレベルであればセキュリティ機能を介して接続する。

一部の都市銀行ではネットワークインフラを将来に向けての戦略的投資と考え高品位/高価な広帯域専用線による統合網構築もある。しかし、新しい回線サービスが次々と提供される現在、コストパフォーマンスを重視しFTTHやADSL等の安価なベストエフォート型のブロードバンドネットワークを活用し、さらに将来への拡張性を持たせたネットワークアーキテクチャがよい。このアーキテクチャのマイグレーションを表したのが図2である。

(1) ステップ1

勘定系、情報系のアプリケーションは数百Kbit/s～1Mbit/s程度のメガデータネットワーク（MDN）等の基幹系NWで構築されている。またWebアクセスやEメール等の用途でBBNWが拠点に敷設されている。

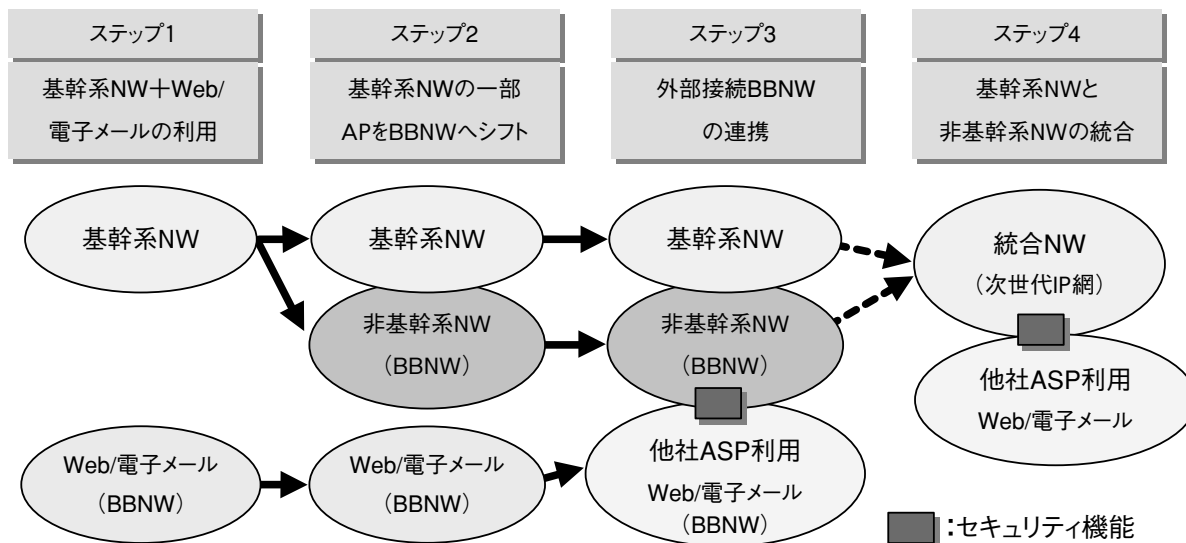


図2 基幹系ネットワークとブロードバンドネットワークの位置づけ

(2) ステップ2

窓口相談端末のように映像やイメージを扱ったアプリケーションの登場により、現在の基幹系NWに統合すると影響が大きいため、別にもう一つBBNWを構築する方法である。広帯域を必要とするが勘定取引ほどの信頼性を要求しないためFTTHを使用したBBNWが最適である。MDN、FTTHとも光ファイバーインタフェースのため将来新たなサービスが出てきても乗り換えることが容易である。つまり営業店に光ファイバーを複数本敷設し、現時点ではサービスレベルにより勘定取引の基幹業務を収容するMDNとそれ以外のデータを収容するBBNWの2レベルの回線サービスを利用する。

(3) ステップ3

他社ASP利用の要求により、外部接続が必要になる。セキュリティ機能を介して接続する。セキュリティ機能を介すことにより、Webアクセスなどに使用されていた単独のBBNWも統合可能となる。QoS（Quality of Service）の確保された基幹網と廉価で高速なBBNWの2網構成とセキュア機能を介した外部接続のためのインタフェースからなる。ステップ3をモデル化したのが先に述べた図1（金融ネットワークモデル）である。

(4) ステップ4

最終的には高速の次世代IP網に統合し、データ、音声、画像のメディアを意識せずに収容できるようになる。

いずれにしてもIPベース、光ファイバインタフェースの網アーキテクチャをとることにより、今後の新しいサービスにも対応できるため、ネットワークインフラ動向に合わせて柔軟なネットワーク構築が可能となる。

セキュリティレベルの導入

従来の金融機関ネットワークは、直接外部とのアクセスを禁止し、高いセキュリティを保っていた。電子メール等外部接続が必要な場合には、アクセス可能な端末を限定しその端末のみ収容する別ネットワークを構築していた。しかし他金融機関ASPの利用や営業店のWebアクセス等、今後外部接続を無視できなくなりつつある。

現在の対応策の延長では営業店に端末が増加することや勘定系端末と相互に連携できないなど利便性で課題があった。また営業店の端末までセキュリティが保たれていないネットワークが構築されることによりリスクが増大し、さらにセキュリティポリシー全体の見直しが必要になり現実的でない。

沖電気では自金融機関内ネットワークのセキュリティをレベル分けし、レベルごとにセキュリティポリシーを定めることによりパフォーマンスのよいセキュリティ対策を実現する。

図3にレベルごとにゾーンを分割した構成例を示す。従来のネットワークおよびシステムをハイセキュアゾーンとし、高セキュアなセキュリティポリシーで運用する。営業店内の端末はこのゾーンに該当するため営業店からの危険拡散が防止できる。

外部接続するためには必ずミドルセキュアゾーンを介して接続する。ミドルセキュアゾーンはセキュリティ機能により囲まれたゾーンである。本ゾーン自体が外部からのアタックを受ける可能性はゼロではないが、本ゾーン内で拡散を防ぐことにより、ハイセキュアゾーンのセキュリティを確保する。外部接続でも共同センタやマルチペイメントなどそのサービス自体のセキュリティが保

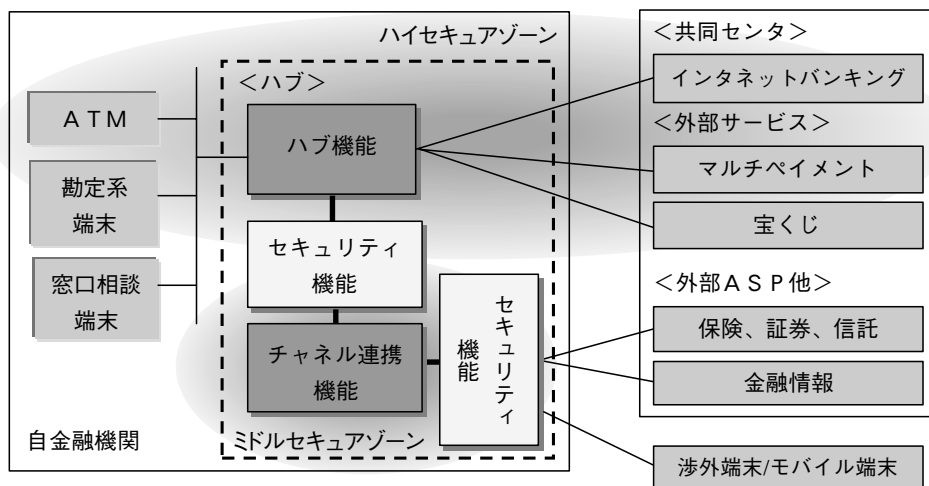


図3 レベルごとのセキュアゾーンモデル

たれている場合はハイセキュアゾーンに直接接続を可能とする。

セキュリティ機能としては、パケットフィルタリング、アンチウイルス、侵入検出、侵入防御と必要に応じて機能を追加していく。ただし現在のセキュリティ製品は特定の機能に注力した製品がほとんどである。そのためアプリケーションに依存せず安全でかつ快適にシームレスな連携を行うとすれば、保護すべき価値以上の投資が必要になり本末転倒である。現在、基幹ネットワークと外部アクセスを連携する場合はWeb画面参照や特定のコンテンツのみのアクセスに制限し、RDP（Remote Desktop Protocol）方式によるアクセスやコンテンツフィルタを介したアクセスにてセキュリティを保っている。今後他社ASP利用の拡大につれセキュリティ対策が的確に行えるかどうかネットワークシステム構築の重要な要件になってくる。沖電気としてもアクセス制限が少なく、よりセキュアな環境が提供できるセキュリティ機能の検討を推進していく。

さらにシステムのセキュリティ対策は構築だけでは不完全であり日々の運用や定期的な診断が不可欠である。構築のみならず、このような日々の運用から診断、企画までをアウトソーシング可能なトータルセキュリティ対策も提供する。

運用管理アウトソーシングの提供

Webサービスの利用や画像トラフィックの増加により、ネットワークの日々のリソース管理が重要になる。また従来の専用線からIPネットワークになることにより、ネットワーク障害自体がネットワーク機器、回線、端末相互に関連する場合があります。障害の原因解析に専門知識やノウハウが必要とされる。セキュリティ面でも日々の運用管理で専門的な技術が要求される。そのため専門の担当

者による運用管理アウトソーシングの要求が高まってきている。

またベストエフォート型のネットワークでは、ネットワークの帯域が保証されないため著しいスループットの低下や遅延の増大が発生する場合がある。従来のpingコマンドによる応答監視ではこのような現象を発見することは困難である。このような現象の発見や、大量のデータがバースト的に発生するBBNWの回線使用率のリアルタイムな把握などがBBNWを使用していく上では非常に重要である。その後の素早いバックアップがBBNWを安心して使用できる要件であり、アウトソーシングに求められる要件でもある。

さらに運用の管理だけでなく、端末やネットワーク機器の資産管理も重要になってくる。資産管理は機器の構成管理以外に端末情報収集やソフト配布などを行うことによりソフトの内部不正使用やパッチの適用状況の管理などセキュリティ面からも今後は欠くことのできないサービスとなる。ネットワークやサーバの日々の監視、管理から予防保全、ハウジングサービスまでを含めてユーザー要求にあったアウトソーシングを提供する。さらにATM運用ノウハウなどの沖電気の強みを生かし顧客サービス向上に結びつく運用提案までをカーバできるアウトソーシングを目指す。

おわりに

今後ネットワークインフラは今まで以上に速いスピードで変革していく。その変革に対して画像などのマルチメディアデータを収容する非基幹系ネットワークの最適な構築、他社サービス利用に伴うセキュリティ確保から日々の運用診断までのトータルセキュリティサービスの提供、ネットワークの構築のみならずその後の運用管理、資産管理までを含めたアウトソーシングサービスの提供、を重点として、柔軟に対応できるネットワークソリューションを金融機関に提供していく。◆◆

参考文献

1) 新田哲二：次世代金融サービスを実現するネットワークアーキテクチャ、沖テクニカルレビュー191号、Vol.69 No.3, pp.11-17, 2002年7月

筆者紹介

鈴木一義：Suzuki Kazuyoshi.金融ソリューションカンパニー 金融ソリューション開発本部 ネットワークソリューション開発部
 広重克典：Hiroshige Katsunori.金融ソリューションカンパニー 金融ソリューション開発本部 ネットワークソリューション開発部

TiPo 【基本用語解説】

IPセントレックスサービス

通信事業者がIP-PBX機能を提供し、ユーザはIP-PBXの設備を持たずに内線通話や外線発着信を実現できるサービス。

IP-VPN

IPパケット単位で通信する仮想閉域網サービス。

広域イーサネット

イーサネットフレーム単位で通信するLAN間接続サービス。