ADSL＋IPSec による自営 VPN 網の構築

―サーバ・ベース・コンピューティングの導入に向けて―

（株）サン・コンピュータ

■ 執筆者Ｐｒｏｆｉｌｅ ■

三　浦　孝　之

2000 年　（株）サン・コンピュータ入社
ネットワーク構築担当
現在 情報技術部所属

谷　川　美津子

1997 年　（株）サン・コンピュータ入社
ホームページ作成担当
Servlet によるページ作成
現在 情報技術部所属

■ 論文要旨 ■

ISDN 及び DA で構築したネットワークを ADSL＋IPSec による自営 VPN ネットワークで再構築し，コスト削減と回線の高速化を図った．全社的には東北４県に広がる支店網であるが，今回はテスト的に青森県内の支店網の ADSL＋IPSec 導入を行った．

グループウェアの利用頻度が高くなったことや，支店の新設が相次ぎ通信費の増大に歯止めがかからない問題，本社 RAS 回線がビジーになるなどの問題解決とともに，サーバ・ベース･コンピューティング（以下 SBC という）へ移行するための広帯域，定額･常時接続のネットワークインフラを構築することが目的である．今回の再構築で，ネットワークの帯域を８倍に，通信費を半分に圧縮することに成功した．今後は，SBC の評価・検証を実ネットワークを使って行う．また，ADSL 回線の障害に備えダイアル・バックアップへの対応も準備しておく必要があるだろう．

■ 論文目次 ■

■ 図表一覧 ■

１．はじめに

１．１　当社概要

当社，㈱サン・コンピュータは，1988 年に設立され，現在従業員 65 名である．主な業務はアプリケーションの受託開発であり，建設業向け総合パッケージ，流通，販売システムなどの開発を行っているほか，パソコンスクール，ホームページ作成も行っている．最近ではインターネット技術を用いた Web ベースのアプリケーション開発や，アプリケーションサーバ構築，運用形態にあったネットワーク構築も含め，情報システムのトータルソリューションを提供している．当社は，三浦建設工業㈱，㈱ほくとうなど八戸地域を拠点とする異業種企業グループ「ほくとうグループ」の一員であり，㈱ほくとうのコンピュータシステムの構築，保守を全面的にバックアップしている．

１．２　㈱ほくとうネットワークの概要

㈱ほくとうは 1961 年に設立され，主に建設及び鉄鋼の機械販売と修理業務を行っていた．1970 年，建設機械のリース業務を開始し，現在では東北４県に 41 の支店及びサテライトオフィスを展開している．1997 年全社を結ぶネットワークを ISDN 回線で構築し，入出庫処理，請求処理のデータ一元化と処理業務のスピードアップを図った．その後一部 ISDN 回線を DA64 回線に切り替えるなどし，**図１**のようなネットワークを構築してきた．本社―支店間は ISDN 接続であり，支店と近隣のサテライトオフィスは，DA64 もしくは ISDN 接続である．支店サーバと本社サーバは，マスタ更新などのバッチ処理と，入出庫などのリアルタイムな更新処理を行っている．サテライトオフィスは最寄の支店のサーバにアクセスし，業務を行っている．最近は，支店，サテライトオフィスの新設が相次いだことや，グループウェアの導入などでネットワークの利用頻度が高まり，本社 RAS 用回線のビジー率が上がりはじめた．また，通信コストが右肩上がりに増えており，通信費の削減が課題になっている．

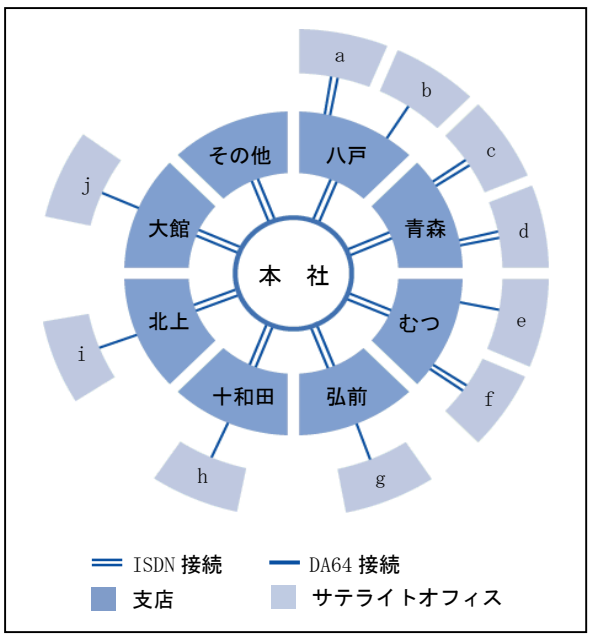


図１　㈱ほくとうネットワーク図

２．問題点と解決手法

２．１　背景と課題

全社を結ぶネットワークの導入は 1997 年に行われたが，専用線費用は高価であったため，従量課金の ISDN が採用された．ISDN とはいえ，本社サーバに支店のクライアントから直接アクセスさせたのでは，回線コストがかかり過ぎる．したがって，各地の支店にサーバを配置し，近隣のサテライトオフィスからは最寄の支店サーバにアクセスする分散型で構築した．

翌年，グループウェアの導入で，通信費用が 1.4 倍に，その後もグループウェア，メール利用頻度が増大を続け，2002 年では，3.5 倍にまで増大した．マイラインで市外通話が安い電話会社に切り替え済みのため，実質的なネットワーク利用頻度の上昇はそれ以上である．後から導入したグループウェアサーバは本社にあるため，距離と接続時間に依存する ISDN の従量課金では通信コストは上がる一方である．

更に，支店，サテライトオフィスの新設も続々と行われたため，本社 RAS の ISDN 回線ポートが不足し，特定の時間帯で，回線ビジー頻度も高まってきた．

ここに ISDN ベースネットワークの問題点を列記すると，以下の四点である．

- 朝夕の特定時間に本社 RAS ポートがビジーになる．
- 距離と接続時間に依存する料金体系であるため，通信費が年々上昇．
- 本社―支店間の ISDN 回線を支店，サテライトで共有しているため，そこがボトルネックになっている．
- 支店―サテライトオフィス間の DA64 回線を高速で安価なものに変更したい．

運用・管理面からは，業務アプリケーションのバージョンアップは全サーバ，全クライアントに対して行う必要があるというクライアント・サーバシステムの管理の煩雑さを経験した．またサーバの障害を復旧するために現地に出向くケースも多々発生し，複数のサーバが各地に分散していることで運用に手間とコストがかかることも体験してきた．

近年，ADSL に代表される広帯域，低価格・定額な常時接続ネットワークの広がりと，SBC の出現で，サーバを本社（一ヶ所）に集中配置することが実現可能となってきた．SBC 実現のための広帯域，定額，常時接続ネットワークインフラを構築し，同時に通信費削減，本社 ISDN 回線ビジー問題の解決をするべく ADSL による VPN の構築を行うこととなった．

２．２　目的と解決手法

目的はSBC導入を前提としたネットワークインフラ構築と，先にあげたISDNベースネットワークの四つの問題を解決することである．それぞれの問題について解決手法を述べる．

２．２．１　朝夕の特定時間に本社RASポートがビジーになる．

本社RASのISDN回線不足であるが，回線不足になるのは，朝夕の特定時間帯である．

単純に回線数を増やす解決策では，その分ランニングコストが上昇し，従量課金体系の脱却を図ることができない．

インターネット経由のVPNを構築し，本社のRASは運用から外す．

２．２．２　距離と接続時間に依存する料金体系であるため，通信費が年々上昇

電話的従量課金体系の脱却をはかる．残念ながら地方では，月額固定料金のサービスのラインナップが限られているのに加え，サービス提供地域も限定されている．IP-VPNや，NTT東日本のフレッツオフィスを利用することは可能であるが，本社側は専用線でIP網に接続しなくてはならないため本社側の専用線コストがかかる．

ほくとう本社が，ISPとLAN接続しているというメリットを活用するため，インターネット経由VPNを構築し，本社分の専用線コストをカットする．支店及びサテライトオフィスでは，コストパフォーマンスの高いフレッツADSLを利用し，月額通信費を削減，かつ固定料金化する．

２．２．３　本社―支店間のISDN回線がボトルネックである．

もともと支店と本社間のISDN回線はサーバ間のデータベース更新処理のためのものだった．しかし，本社にグループウェアサーバが導入されてから，サテライトから本社へのグループウェアアクセスが支店を経由し，ISDN回線を共有する形になっている．

サテライトから本社に直接アクセスするようにルートを変更し，更にADSL化による回線高速化も図る．

２．２．４　支店―サテライトオフィス間のDA64回線を高速化したい．

支店とサテライトは，同一県内にある．同一県内のオフィス間通信は，NTT地域IP網内でのクローズした通信となるため，安定した通信速度が期待できる．

フレッツADSL＋VPNで接続でDA64よりも高速なネットワークを構築する．

３．コストパフォーマンスでADSL＋自営VPNに決定

長距離の専用線を利用していたユーザにとって，IP-VPN，広域Ethernetサービスなど，距離に依存しない料金体系，メッシュトポロジが利用可能なネットワークサービスは，コスト削減につながる．しかし，ISDNユーザの立場からするとコストメリットを出しにくい．なぜならば，IP-VPN，広域Ethernetともに，少なくとも本社とアクセスポイントの接続には専用線を利用するため，その費用だけでも負担増を強いられるからである．

幸い，ほくとう本社はISPとLAN接続しているという利点があった．これを最大限に利用するため，インターネット経由のVPNを利用することとし，本社以外の拠点はコストパ

フォーマンスの高い ADSL 回線を選択，VPN 装置には NetScreen 社の NetScreen シリーズを利用した．

ADSL 化することで，どの程度コスト削減が可能になるのか，**図２**に示すネットワークを例に試算した．試算結果を**表１**に示す．ADSL にすることで通信費を半分以下にできる．しかも，ADSL は固定料金のため，通信量が増えても月額費用は変わらない．

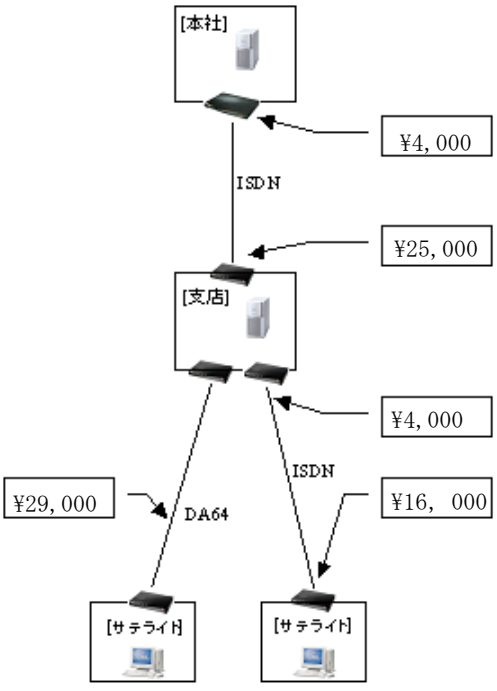
表１　通信コスト比較

ISDN,DA の場合

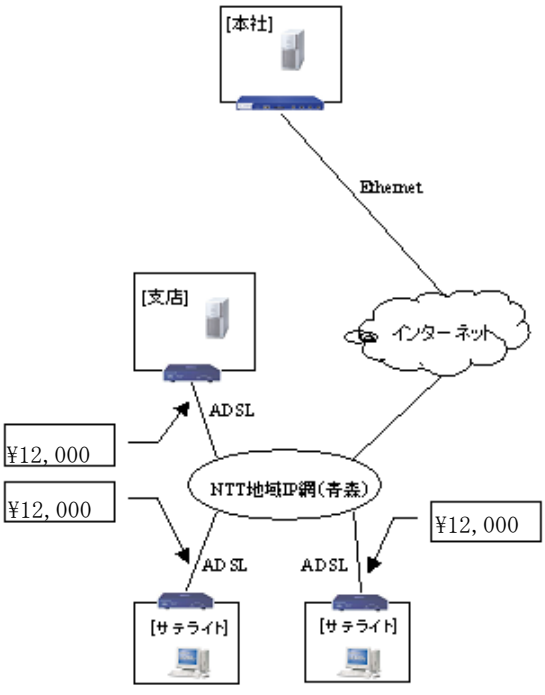
本社	ISDN	¥4,000
支店	ISDN	¥25,000
支店	ISDN	¥4,000
サテライト1	DA64	¥29,000
サテライト2	ISDN	¥16,000
合計		¥78,000

ADSL の場合

本社		－
支店	ADSL	¥12,000
サテライト1	ADSL	¥12,000
サテライト2	ADSL	¥12,000
合計		¥36,000



ISDN,DA の通信費



ADSL の通信費

図２　通信コスト比較モデルネットワーク図

４．VPN 装置の選択

４．１　ユーザ･網インターフェースの主流は Ethernet へ

ADSL のユーザ網インターフェースは Ethernet で提供されている．今回使用した NetScreen5XP は，２ポートの Ethernet を有し，網側の Untrusted，LAN 側の Trusted ポートで構成される．Untrusted ポートは PPPoE に対応しているため，別途ブロードバンドルータは不要である．Ethernet 機器は最も普及しており扱いやすいインターフェースであり，L3 スイッチも安価に購入できるようになった．広域ネットワークのユーザ・網インターフェースは Ethernet が主流になると思われる．

IP-VPN，広域 Ethernet 以外にも今後便利で安価なネットワークサービスが出現すると思われるが，ユーザ・網インターフェースが Ethernet であれば，機器を変更せずにサービスを切り替えられる．ユーザがより有利な広域ネットワークサービスへ比較的容易に切り替えができる環境になると予想する．

４．２　NetScreen5XP のパフォーマンス

NetScreen 導入前の簡易テストで得られた NetScreen5XP のパケット転送スループットを**表２**に示す．簡易テストは，**図３**に示すネットワークにて PC1 から PC2 に FTP 接続し，データをダウンロードして計測した．

NetScreen5XP の性能としては VPN なしの IP ルーティングの場合で，約 7 Mbps，VPN（IPSec 3DES/SHA）の場合で約 740kbps [1]となった．フレッツ ADSL8M では，上り最大 1Mbps であるため，NetScreen5XP を VPN で利用する場合はフレッツ ADSL 8M タイプまでならボトルネックとはならないだろう．VPN 利用時のスループットに関してはやや不満ではあるが，NetScreen5XP を VPN なしのルーティングモードで利用すれば 7 Mbps のスループットであるため，広域 Ethernet を利用すれば同製品で高速通信が可能である．

表２　NetScreen5XP パケット転送スループット

VPN なし(ルーティング)	7,149 kbps
VPN (IPSec 3DES/SHA)	743 kbps

[1] 2002 年 7 月に新製品 「NetScreen 5XT」が発表された．VPN 時のスループットは 20Mbps．

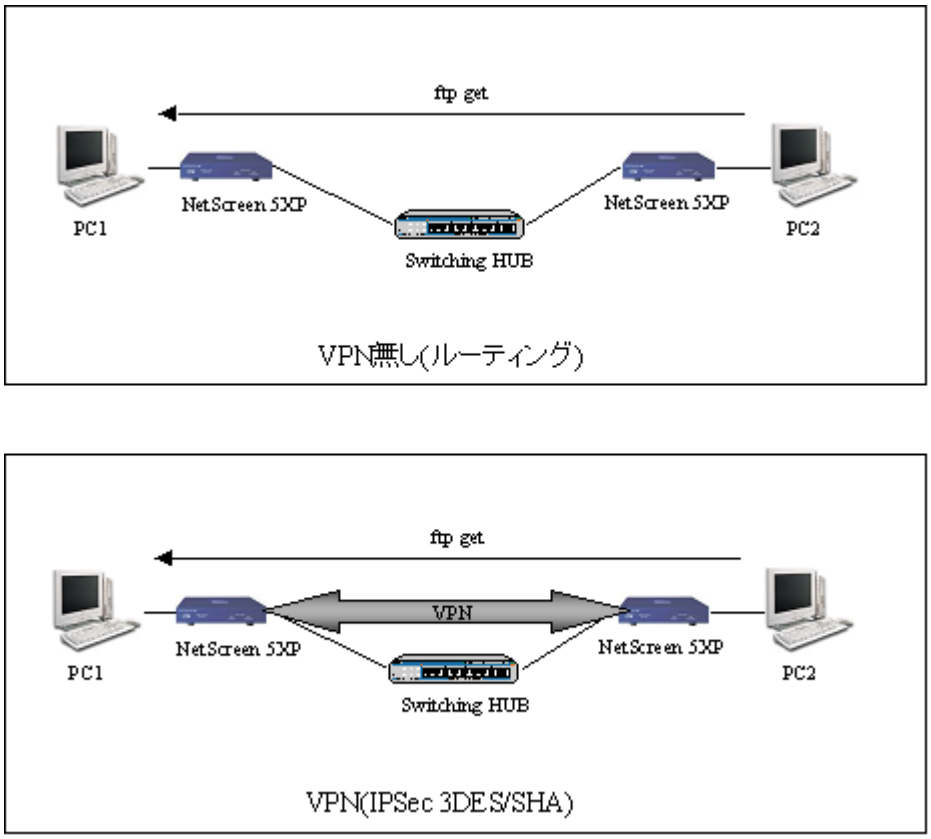


図３　テスト用ネットワーク図

５．構築における工夫

５．１　設定作業の効率化

ADSL への移行にあたって各拠点での機材設置，設定作業が伴う．今後の全拠点への展開に備え，最低限の人件費，交通費で行えるよう，既存 ISDN ネットワークを活用して設定作業を行った．下記手順に従い，一人で作業を進めることができる．

１．本社に NetScreen を設置し，支店，サテライトへの IPSec トンネルの設定を完了させる．
２．支店の ADSL 回線に，設定済みの NetScreen を接続する．
３．本社 RAS に PIAFS ダイアルアップし，本社から支店へのルーティングを VPN 経由に変更する．（本社への VPN 接続がうまくいかない場合も，本社 RAS に PIAFS ダイアルアップすることで本社側の NetScreen の設定変更が可能．）
４．サテライトの ADSL 回線に，設定済みの NetScreen を接続する．
５．本社 RAS に PIAFS ダイアルアップし，本社からサテライトへのルーティングを VPN 経由に変更する．（本社及び支店への VPN 接続がうまくいかない場合，本社 RAS に PIAFS ダイアルアップすることで本社はもちろん，支店の NetScreen の設定変更も可能．）

５．２　安全対策，効率化のために

各店で加入する ISP を共通にすることで，VPN トンネルの経路を特定の ISP のバックボーンネットワークにとどめることができる．インターネット VPN のリスクを軽減させられるうえ，拠点間のネットワークホップ数が少なくなるなど，他者のトラフィックによる遅延の影響も抑えられる．

６．導入の効果

サイト間通信速度が８倍に

支店―本社間のネットワーク帯域の比較を FTP にて行った．
ISDN の場合は，61.5kbps であったが，ADSL(1.5M)+IPSec の場合，約 8 倍の 500kbps になった．サテライトオフィスから本社のグループウェアサーバへのアクセスレスポンスは明らかに高速になったことが体感できるほどだ．LiveHelp にて本社から行っている支店サーバの遠隔サポートも快適に動作するようになり，サポート業務の効率化も期待できる．ただし ping によるレイテンシ計測では，ADSL+IPSec の方が 20ms ほど遅かった．おそらく，地域 IP 網内での L2TP による遅延によるものだと思われる．

表３　ISDN と ADSL+VPN のネットワーク速度比較

	FTP 転送レート	ping レイテンシ
ISDN	61.5kbps	60ms
ADSL+IPSec	500.0kbps	80ms

通信コストが半分に

試算どおり通信コストは半分になった．フレッツ ADSL は月額通信料が固定のため，ある月に限って高額な通信費の請求を受けることがないので安心である．

RAS 回線ビジーが解消

ISDN 回線を利用しなくなったため，本社 RAS 回線のビジーから開放された．また，最終的には本社 RAS は撤去できるため，RAS 用に用意していた ISDN 回線利用を休止することで，ISDN 基本通話料の削減もできる．

VPN を用いて VoIP を試用

NetScreen5XP との入れ替えで不要となった YAMAHA RT54i ルータを用いて VoIP の試用を行っている．PBX と連携した VoIP ではないため，内線電話への転送ができないのが難点であるが，通話品質には問題ない．ADSL の導入で比較的広帯域で支店間常時接続ができるようになったため積極的にネットワークを利用することが可能となった．

常時接続，定額ネットワークを活用

1997 年には常時接続ネットワークは高価だったため，サーバを分散せざるを得なかったが，今回の ADSL＋VPN の導入で，本社と支店・サテライトオフィス間の帯域が 500kbps の常時接続回線となり，サーバを本社に集約できるネットワークが整った．今後はこの VPN ネットワークを利用し，SBC の検証を行っていく．

以下に SBC について簡単に説明を加える．

ここでは，Windows2000 のターミナルサービスに Citrix 社[2]製 MetaFrame をアドオンしたもので説明する．**図４**に SBC のモデルを示す．

- MetaFrame サーバ

  クライアント用のアプリケーションをインストールしておく． MetaFrame サーバのリソース（CPU，メモリ，HDD）を使ってクライアント用アプリケーションが動作し，画面だけがクライアントに表示される．

  画面ビットマップ転送は，変化のあった差分だけ送られるため，色数 16 色なら，WAN 回線が 64kbps でもクライアントがデータベースサーバと同一 LAN に接続しているのと同等のレスポンス速度が得られる．

  複数台の MetaFrame サーバを用意し，ロードバランスすることで MetaFrame サーバのスケールアップと，冗長性を高めることができる．

- クライアント

  クライアントには ICA クライアントソフトウェア（MetaFrame のビットマップ転送，マウスキーボードの入力情報転送などの処理を行う）をインストールするだけで，そのほかのアプリケーションは不要．MetaFrame サーバの端末といった位置付けになる．

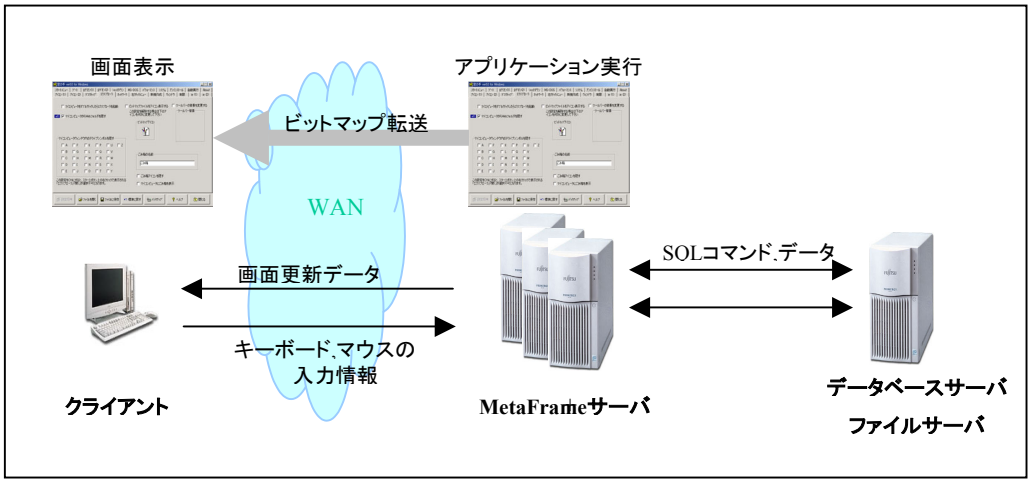


図４　SBC のモデル

[2] シトリックス・システムズ・ジャパン株式会社 http://www.citrix.co.jp/

SBC がもたらすメリットを以下に挙げる.

1. 支店のサーバを廃止できる
   １ヶ所にサーバを集約し管理が楽になる（障害，バックアップなど）

2. クライアントのアプリケーションを展開したり更新するのが容易になる
   MetaFrame サーバにアプリケーションをインストールすれば，即クライアントで利用可能になる．バージョンアップも同様である．
   ロードバランス機能を利用すれば１台づつサーバを停止し，サーバメンテナンスをオフラインで実施できる．

3. 低スペックな PC も使いつづけられる
   アプリケーションはクライアントで動作しないため，クライアントにハイスペックな PC を必要としない．

4. 既存の Windows アプリケーションを利用できる
   既存アプリケーションを Web 版に開発しなおすことなく，サーバサイドでアプリケーションを実行させることが可能であり，Windows アプリケーションの操作性を失わない．

７．おわりに

コストパフォーマンスの高い ADSL を利用することで，通信費を約半分に圧縮し，しかもネットワークの帯域は８倍にすることができた．また，常時接続･固定料金のネットワークになったことで，ネットワークを動脈としたシステムづくりを加速させることができる．本 VPN を用いて SBC を評価･検証し，ユーザに対しては，レスポンスのよい業務システムを提供し，管理者側としては，メンテナンス性の高いシステムの構築を目指す．更に，いままで個別に行っていたウィルス対策を，エンタープライズ版のアンチウィルスソフトに切り替えることで，本社で集中管理していくことも検討する．

SBC では，ネットワークの安定運用が非常に重要になる．ネットワークダウンはシステムの致命傷になるため，今後導入する支店では，ADSL 回線障害時のバックアップとして，モデムや TA によるダイアルアップが可能な NetScreen 5XT などを利用してゆく．

また，ADSL＋自営 VPN に固執することなく， 新しい広域ネットワークサービスの登場に注意を払い，より有利なネットワークサービスに切り替えたり，複数のネットワークサービスを組み合わせて利用するなど柔軟な対応ができるようにする．

参考文献

［１］ “MetaFrame XP 実践ガイド” CQ 出版社