I−6 作業所接続に対応したインターネットＶＰＮシステムの開発

Development of Internet VPN system between construction sites

渡邉 英一[1]　古田 均[2]　佐藤 郁[3]
Eiichi Watanabe,　Hitoshi Furuta,　Iku Sato

【抄録】ADSL に代表される高速で安価なインターネット接続が急速に普及しているが，建設現場の現場事務所（作業所）と本支店等とのネットワーク接続は ISDN が主流であり高速化が図れていない．まず，作業所のネットワーク接続の特性を分析し，一般消費者向けインターネット利用に必要とされる要件をまとめた．次に，セキュリティーや安定性が不足しているため企業には不向きとされていた InternetVPN をセキュリティーと安定性を確保した方策について説明する．約 200 拠点の接続を実施した結果，通信速度を従来の ISDN の 5 倍以上に，コストを従来の 28%に削減することを可能とした．

【Abstruct】The high speed and cheap Internet connectivity have spreaded quickly by ADSL. But the network connection between construction sites and branches still use ISDN line, and cannot attain improvement in speed. First, since the characteristic of network connection of a work place is analyzed, and the requirements needed for the Internet use for general consumers are summarized. And the method of InternetVPN System is described to be sufficiently secured and stabile to a company. As a result of connecting about 200 sites, this made it possible to increase transmission speed to 5 or more times of the conventional ISDN, and to cut cost to 28% .

【キーワード】ネットワーク，VPN，インターネット，作業所，セキュリティ，認証

【Keywords】Network, VPN, Internet, Construction site, Security, Certification

1．はじめに

驚異的なスピードで高速なインターネットが普及し，2003 年 3 月時点において，DSL 加入者数は 650 万世帯を突破している[1)]（図-1）．企業内のコンピュータも電子メールやホームページの普及に伴いほとんどのコンピュータはネットワーク化され，資本金 1000 億円以上の建設会社のうち 6 割以上が 8 割以上の作業所でネットワークを整備している（図-2）．

一方，ブロードバンドの普及に伴い，交換されるデータ量は増大している．図-3 に示すように，日本最大のインターネット接続拠点（IX：Internet exchange）である，JPIX においては，2003 年 3 月 28 日に 1 秒間の

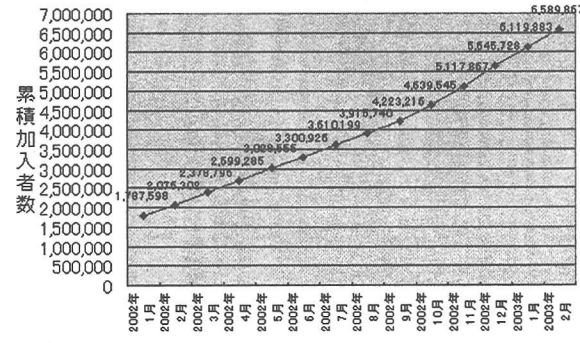

図-1　DSL加入者数

1 工博 京都大学教授，京都大学大学院工学研究科土木工学専攻（〒606-8501 京都市左京区吉田本町）
2 工博 関西大学教授，関西大学総合情報学部総合情報学科（〒569-1095 大阪府高槻市霊仙寺町 2-1-1）
3 戸田建設株式会社　本社　土木企画室（〒104-8388 東京都中央区京橋 1-7-1 新八重洲ビル）

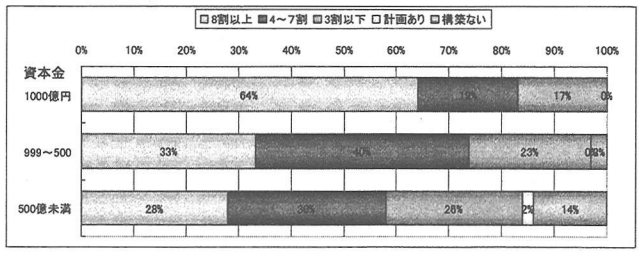

図-2　作業所ネットワーク整備状況 (2002年) [2)]

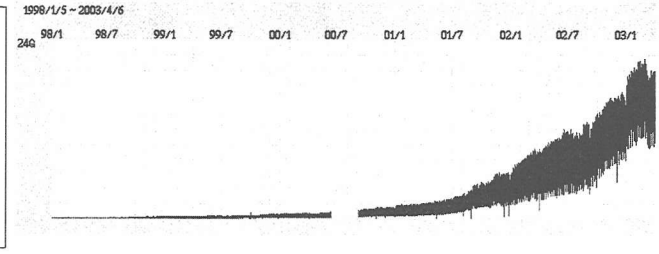

図-3　JPIXトラフィック [3)]

最大通信量 20Gb を突破し，インターネットは日本の主要なインフラの一つと言っても過言ではない．

インターネット接続費用が一般消費者の利用拡大に伴って，急速に低価格化する一方で，建設作業所（以下作業所）を初めとする企業向けネットワークの費用の低価格化は進んでいない．これは，インターネットが誰でも利用できる共有設備であることに対し，企業向けのネットワークはセキュリティー確保のために，インターネットから切り離された占有設備を利用しているためである．

そこで，セキュリティーを確保しながら，一般消費者向けのインターネットを利用することが可能になれば，大幅なコストダウンが可能となるため，利用技術の開発が求められていた．本論文では，まず，作業所ネットワーク接続に必要とされるセキュリティーと利便性の要求条件を定義し，これらの条件を満足する接続技術の開発とその実証結果について報告する．

2．作業所ネットワークの要求条件

作業所は顧客から依頼を受けた，建設に関る情報が集中する場所であるとともに，小人数で運営されるため，

- セキュリティー
- 利便性

が要求される．

(1) セキュリティー

作業所ネットワークにおいて，セキュリティー上必要となる外部への対応は，

- 共同企業体への対応
- 外部からの情報受取への対応

の２点である．

a) 共同企業体への対応

作業所の形態には，１社単独の場合と共同企業体（以下 JV）の場合がある．JV は作業所に多く用いられる企業形態であり，JV の構成会社である複数の企業の社員（以下　JV 構成員）が同一事務所内において共同で業務を行う．構成会社ごとに担当工区を定めて単独で業務を行う場合もあるが，構成会社の区別なく業務を遂行するケースが多く，JV 構成員間において様々な情報の共有が行われている．

日常業務のほとんどにコンピュータを利用している現状においては，JV 構成員間で工事にかかわる多くの情報をネットワーク経由で交換する必要がある．一方，JV 構成員は本来所属する会社の情報も取得する必要があるため，それぞれの会社のネットワークへのアクセス環境も同時に整備する必要があるため，JV を構成する作業所（以下 JV 作業所）のネットワークは，構成会社のネットワークが混在する特殊な環境となる．このため，構成会社ネットワークが相互に接続されないための制限と，JV 構成員による他社ネットワーク接続の制限が必要となる．

従って，JV 作業所においては

- ＪＶ構成員の相互接続
- ＪＶ構成員の自社ネットワーク接続
- ＪＶ構成会社のネットワーク相互接続の制限
- ＪＶ構成員の他社ネットワークへの接続制限

が必要となる．

b) 外部からの情報受取への対応

作業所においては，作業所内の他に，

- 発注者
- 業者
- JV 構成会社

等との情報交換が発生する．交換方法としては，電子メール，CD-ROM 等のメディア，ASP に代表される情報共有サーバによるファイル共有等がある．電子メールは各 JV 構成会社のメールシステムより取得され，メディアは郵送等で直接作業所に持ち込まれ，ファイル共有サーバにはインターネットや専用線ネットワークにより接続される．

セキュリティー上の問題としては，

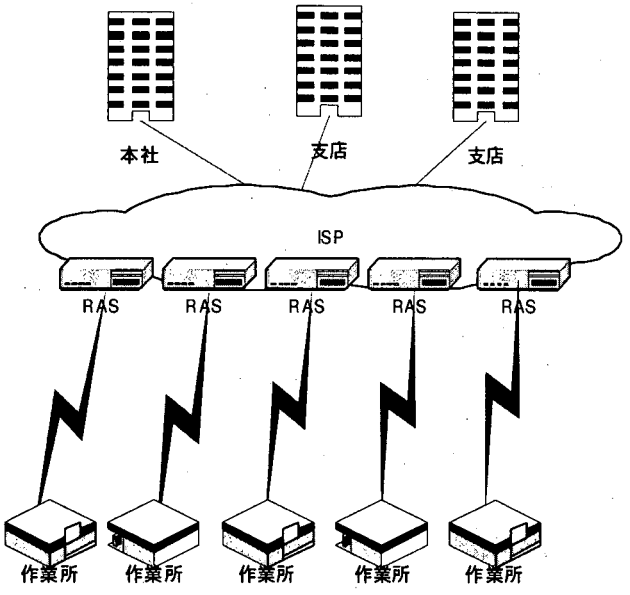

図-4 ISPを利用したダイアルアップ接続

- ウィルスへの感染
- 不正アクセス（ワーム，スパイウエアなど）
- 機密データの流出

があげられる．

また，経路としては，

- 電子メール
- インターネット
- CD-ROM などのメディア

があげられる．

作業所にウィルスなどが進入した場合，その影響範囲は，作業所内にとどまらず，発注者，業者，構成会社と広範囲に及ぶため，十分な対策が必要である．同時に被害が生じた場合においても影響を作業所内部に留める方策が必要である．

(2) 利便性

建設作業所の特性として，

- 開設期間が工事の工期に準ずるため，数ヶ月～数年の短期間である
- 都市部に限らず，地方や山間部での立地が多い
- 数人～数十人規模と小人数である

といった特徴がある．従って，利便性の高い作業所ネットワークを構築する条件としては，

- 短期間で設置，移動が可能
- メンテナンスが容易
- 専門家が不要

があげられる．つまり，半年間の工期で設置手続きに１ヶ月必要とするシステムでは，工事当初にネットワークが利用できない．また，地方都市や山間部でシステムをサポートする業者の確保は困難であり，遠方から人員を派遣するためには膨大なコストを必要とするため，メンテナンスが容易なシステムが必要である．また，人員が限られた作業所においては，情報技術を習得した専門家を配置することは困難であるため，専門家が不在でも対応できるシステムにする必要がある．

3．現状と課題

(1) 現状

作業所との接続は，接続の都度アクセスポイント(AP)へ電話をかけて接続を行う，ダイアルアップ接続が主流である．通信頻度が多く，接続費用が高額になる場合は，ダイアルアップから専用線による常時接続へ移行するケースも見受けられる．AP は自社の支店などに設けるケースもあるが，営業範囲が広域に及ぶ場合には，インターネット接続事業者（ISP）の AP を利用するケースも多い（図-4）．

接続の種類としては，アナログ，ISDN の他，PHS や携帯電話を利用している．PHS は利用可能範囲が狭いこと，携帯電話は通信速度が遅いことから，ISDN を利用するケースが多い．この他の選択支としては，

表-1　接続種類

	速度(bps)	費用	接続エリア
アナログ	56k	10円/分～	全国
ISDN	64～128k	10円/分～	ほぼ全国
INS1500	～1.5M	45,000円/月 ＋10円/分～	都市部
PHS	～128k	10円/分	都市部
携帯電話 (FORMA)	384k	1,638円/MB	ほぼ全国
ATM	0.5～600M	74,200円/月*	都市部
FR	64K～6M	162,400円/月**	都市部

* ATMシェアリンク　15km 最高速度1Mbps，保証速度200kbps 双方向で試算　**スーパーリレーFR　15km　1.5Mbpsで試算

フレームリレー（FR），広域 LAN，IP-VPN 等があるが，費用が高いこと，接続拠点が限られていることから，作業所での利用は少ない．表-1 に接続種類別の速度，費用，接続エリアを示す．

(2) 課題

高度情報通信ネットワーク社会推進戦略本部 e-Japan 戦略[4]の後押しにより，一般消費者向けのサービスである ADSL，CATV，FTTH などは価格が急速に低下し，接続可能エリアも急速に拡大している．このように高速インターネット接続の重要度が増加する一方，作業所の接続速度はほとんど改善していない．

一般消費者向けのインターネット接続サービスが作業所接続に利用されない理由には，

- インターネットが盗聴などセキュリティー上の危険性があること
- 通信速度が保証されないベストエフォート型のサービスであること

があげられる．ISP のアクセスポイントのある電話局まで ADSL などを利用して接続するサービスも始まっているが，提供エリアは一部地域に限られている．

ダイアルアップ接続は利用時間に応じて課金される従量制が一般的であるため，ISP の利用料金が定額であっても，アクセスポイントまでの通信料金は，専用線接続を用いない限り距離と接続時間に応じた通常の電話料金が必要となる．表-2 に 2002 年 3 月の接続料金の実績を示す．1 拠点あたりの平均通信時間は 90 分/日，接続料は 3.2 万円/月で，通話料が全体の 62%を占めている．通信量は効率を 60%としても 300MB/月発生している．従って，表-1 を考慮に入れても現状では ISDN が最も低価格な選択肢であることがわかる．

表-2 作業所接続料金実績（2002 年 3 月）

拠点数:782
千円/月

項目	金額(千円)	比率
通話料金	15,610	62%
ISDN基本料金	1,040	4%
ISP基本料金	4,242	17%
ISP超過料金	4,431	17%
合計	25,323	

4．VPN の利用方法

(1) InternetVPN について

VPN の一般的な利用方法としては，

- IP-VPN
- InternetVPN

の 2 種類がある．

IP-VPN とは，単一の通信事業者が保有するネットワークを複数の企業（利用者）で共有するために VPN を用いるものである．専用線や FR に比べ安価にネットワーク構築が可能なため，採用例が増加している[7]（図-7）．IP-VPN のメリットとしては，

- 回線を単一の事業者が管理するため，盗聴などの危険性が少ない
- 利用者数や接続速度を制限できるため，安定した接続が可能

があげられる．一方，デメリットとしては，

- 提供エリアが限定される
- InternetVPN に比べコストが高い

といった点があげられる．

InternetVPN とは，インターネット上に VPN により仮想の私的なネットワークを構築する方法である．IP-VPN との相違点は利用するネットワークを単一事業者が保有するネットワークではなく，複数事業者や個人が自由に利用するインターネットを利用する点である．

インターネットは，

- インターネットが盗聴などセキュリティー上の危険性がある
- 通信速度が保証されないベストエフォート型のサービスである

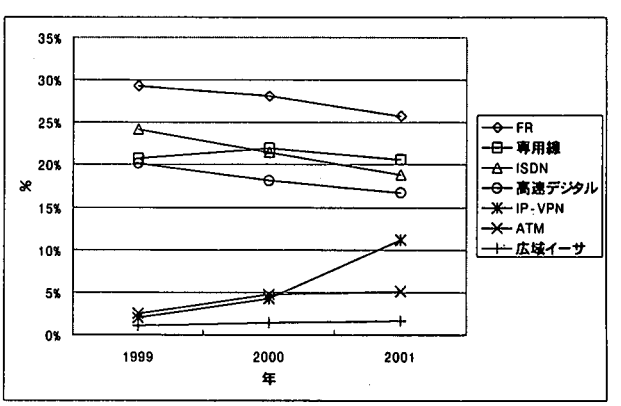

図-7 WANサービスの推移

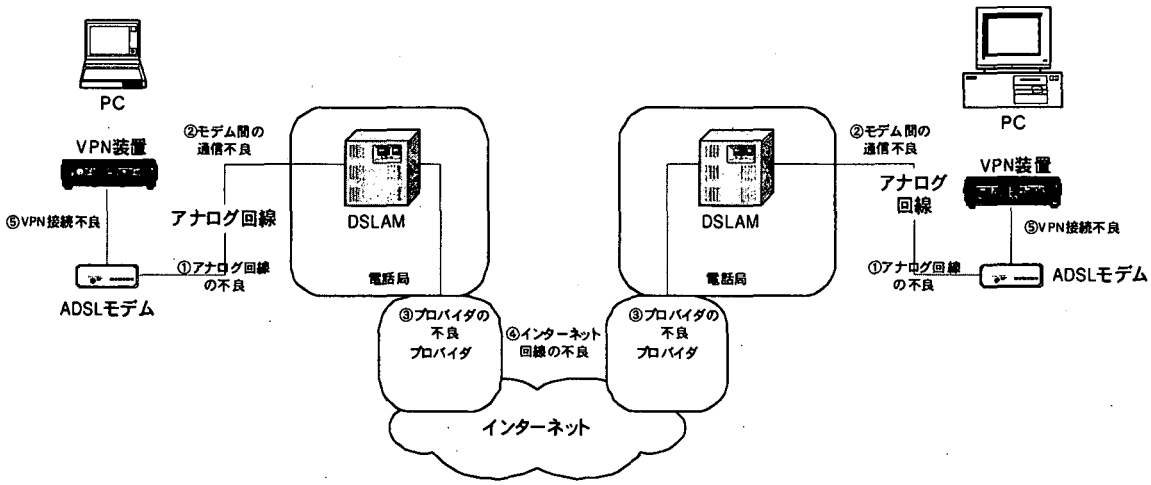

図-8　VPNによる接続と障害要因

といった特徴をもつため，InternetVPN は

- セキュリティーの確保が困難である
- 安定的な接続の確保が困難である

といったデメリットがあるため，ビジネスを目的とした利用には適さないとされていた．しかし，一方で，

- 安価である
- インターネット接続環境があれば地域が限定されない

といったメリットがあるため，作業所のように多数の拠点が全国に散在する場合には利用価値が高く，実用化が求められていた．

(2) セキュリティーの確保

前述のように，InternetVPN を建設作業所に利用するためには，セキュリティーの確保と安定性の確保といった２つの課題を克服する必要がある．ここではまず，InternetVPN においてセキュリティーを確保するための方策について述べる．

VPN においてセキュリティを確保するためには，

- 機密性(confidentiality)
- 正当性(authentication)
- 完全性(integrity)
- 秘匿性(concealment)
- 認否不能性(nonrepudiation)

を保証する必要があり，

- 認証
- 暗号化
- MAC

の技術が有効である．これらを実現する方法として，電子メールの場合は PGP や S/MIME，Web の場合は SSL が一般的に利用さている．しかし，ネットワークを接続する VPN の場合，様々なアプリケーションで利用可能な環境を構築する必要があるため，パケットレベルでの実現が必要となる．そこで，InternetVPN では IPsec を利用する．

IPsec とは暗号化技術や認証技術を利用して IP パケット化された情報を安全に伝達する方式であり，インターネット技術の国際標準を議論策定している IETF によって，RFC2401,2006[5)6)]等として標準化され，ている．IPsec の特徴として，

- RFC として仕様が公開され，常に検証が行われているため安全である
- 通信を保護すべき区間の始点と終点に機器を設置すればよく，中間点は通常の設備が利用可能である
- パケットレベルで保護されるため，個々のアプリケーションの修正が不要
- IETF により標準化されているため，対応している機器が多い

等があげられる．デメリットとしては，セキュリティーを確保するために複雑な手順が必要であり，実装が困難でるため，IPsec 対応機器間においてもメーカが異なると接続が不安定になるといった点があげられる．

(3) 安定性の確保

次に，InternetVPN において安定性を確保するためには，

- 接続回線の安定
- 接続状態の安定

を実現する必要がある．

InternetVPN により拠点間を接続するケースについて ADSL を例に説明する．まず，図-8 のように，両拠

点からまず，アナログ電話回線により電話局に接続し，拠点側ADSLモデムと電話局側のADSLモデムであるDSLAM(Digital Subscriber Line Access Multiplexer)間で通信を確立する．次に電話局内のプロバイダの回線に接続し，プロバイダの回線を利用してプロバイダのインターネット接続ポイントまで接続する．このインターネット接続により拠点同士の通信を確立し，VPNによりトンネリングを確立する．

InternetVPNにより接続が不良となる要因としては，

1. 電話局と拠点間のアナログ回線の不良
2. 拠点側ADSLモデムと電話局側DSLAM間の通信不良
3. 電話局 DSLAM よりプロバイダのインターネット接続ポイントまでの接続不良
4. インターネット回線の接続不良
5. VPN 接続不良

があげられる．両拠点でADSLを利用する場合，1~3は両拠点に発生する可能性があるため，その要因は8箇所に及ぶ．

1.については，ダイアルアップ，IP-VPN等においても同じ条件である．2.については，ISDN回線やAMラジオ等による干渉により発生するものであり，ADSL回線共通に発生する問題である．3.については，全国展開を行っているeAccecss[8]，アッカ[9]，YahooBB[10]の3事業者では2003/04/01~2003/04/07 の1週間で局内における通信障害が9件発生している．4.については，上記期間において，Biglobe[11]，@nifty[12]，OCN[13]の3プロバイダで2件発生している．5.については，VPN機器の故障や設定上のミスによる要因が考えられる．

上記の問題をクリアし，接続回線の安定性を確保するため，

1. 回線の自由な選択
2. プロバイダの自由な選択
3. IX(Internet eXchange)の直接利用
4. VPN の自動復旧システム

の対策を行った．それぞれについて以下に解説する．

a) 回線の自由な選択

ADSLで発生する回線不良の問題は，InternetVPNに限らず，ADSL で接続を行う接続を利用する場合には共通に発生する．ISDN，FTTH，CATV など様々な回線に対応することで，回線不良による障害を最小限に抑えることが可能となった．また，障害が長期に及ぶ場合にも利用可能な回線から選択することで早期復旧が可能となる．

b) プロバイダの自由な選択

大手プロバイダの場合，プロバイダを原因とする障害は非常に少ないが，プロバイダが大規模な停止に陥った場合，全ての拠点が接続不能となる．プロバイダを自由に選択可能とすることで，地域で最も信頼性の高いプロバイダを選択できるだけでなく，障害時においても，プロバイダを変更することで早期復旧が可能となる．

c) IX(Internet exchange)の直接利用

IX(Internet eXchange)とは，ISPなどのネットワークの相互接続を目的とした，インターネットの相互接続点である．インターネットを構成するISP間で無駄な中継をすることなく，経済的に相互接続を行う拠点であり，インターネットにおけるバックボーンを下支えする役割を果たしているため，無停止での運用が図られている．VPNを構成する拠点の片方をIXに直接接続することで，様々なISPからの安定的な接続が可能となり，接続不良の要因を8箇所から5箇所に減少させることができる．

d) VPNの自動復旧システム

前述のように，VPNによる接続は様々な外的要因によって断絶する可能性がある．プロバイダや局舎内における通信障害の発生件数も1週間で 11 件に達している．また，ADSL を利用した場合には雑音等による通信の断絶も高い頻度で予想される．

従って，通信断絶を前提とし，断絶時の自動復旧システムを搭載することにより，安定性を向上させることが可能となる．

(4) コストの削減

VPNにより双方向の通信を可能とするためには，両拠点をインターネット上で特定する必要がある．従来の技術では両拠点に固定的にグローバル IP アドレスを付与する必要があった．しかし，固定のグローバルIP アドレスは，大手通信事業者の場合，月額 3,000～10,000 円程度の追加料金が必要となるため，拠点毎の通信費が倍増することになる．

そこで，VPN の自動復旧システムを応用し，ADSL接続で一般的に利用されている，接続毎にIPアドレスの変化する動的IPアドレスを利用可能とした．この方法により，固定グローバルIPアドレス取得費用が不要となり，拠点あたりの回線費用のさらなる削減を可能

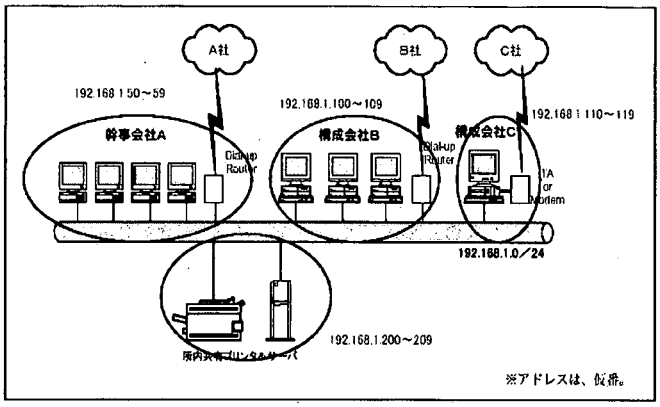

図-9　JV作業所ネットワーク構成例

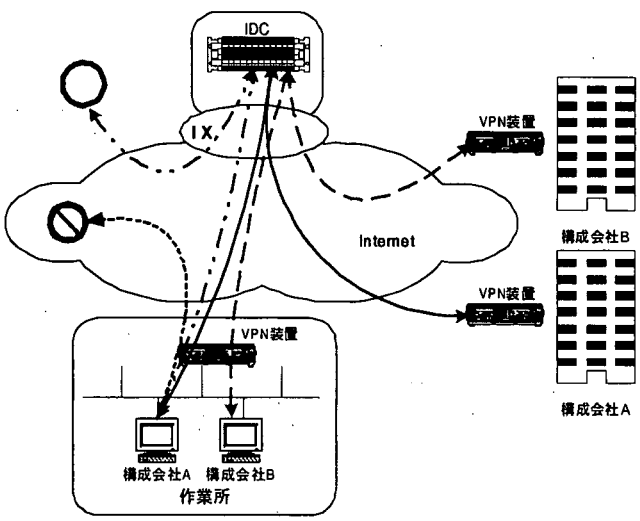

図-11　InternetVPNによるJV作業所ネットワーク

とした.

5．建設作業所を考慮した構築方法

(1) セキュリティー

a) 共同企業体への対応

現在のJVネットワークは図-9のように，JV作業所内より各構成会社へダイアルアップや専用線で接続されている[14]．しかし，ADSL等の低価格化に伴い，図-10のような接続方法が用いられるケースも増加している[15]．しかし，前者の方法では作業所内のPCを介した構成会社間の直接接続が可能であり，セキュリティー上重大な問題となる可能性がある．さらに，後者の方法では構成会社だけでなく，インターネットより容易に第三者へ情報漏洩する危険性がある.

そこで，本システムでは，図-11のように，作業所内の全ての接続を，ウィルスチェックやファイアウォールのなど十分な対策を行ったIDCを経由した接続とし，IDC内部で各構成会社に通信を切り分けることにより，安全性の高いネットワーク構築を可能とした.

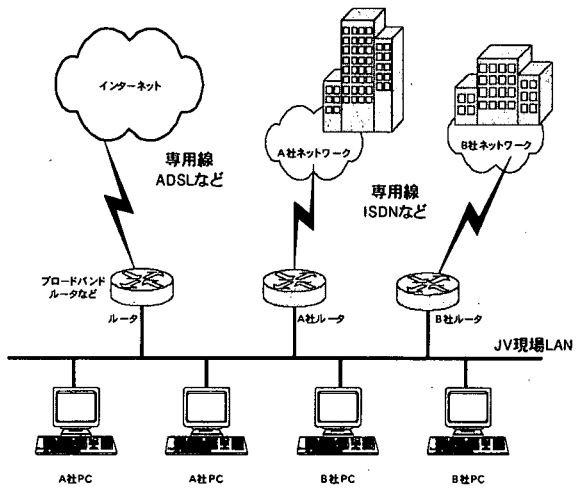

図-10　インターネットに接続したJV作業所ネットワーク

b) 外部からの情報受取への対応

外部からの情報受取に対しても，電子メールやインターネットのASPサービス等により取得する場合においては，IDCにより一括してウィルス等のチェックを行う．また，作業所内に持ち込まれたCD-ROM等のメディアによって作業所内が感染した場合にも，IDCにおいて集中的にウィルスチェックを行うことで，構成会社への感染を防止することも可能とした.

(2) 利便性

前述のように，作業所にはITに関する専門家の設置が困難であるため，高度なセキュリティーと利便性を両立させる必要がある．そこで，

- VPN装置のブラックボックス化
- 透過プロキシ

の利用により，セキュリティーと利便性の両立を実現させた.

a) VPN装置のブラックボックス化

VPNの確立のためには，非常に複雑な設定が必要となるため，高度な知識が必要となる．また，認証局を利用しない安価なプレシェアードキーの利用は，「プレシェアードキーが外部へ漏洩しないこと」が前提となる.

また，固定IPアドレスを利用しない接続でプレシェアードキーが漏洩した場合，世界中のどこの接続拠点からでも接続可能となるため，セキュリティー上の重大な問題を生じる危険性がある.

そこで，VPN装置を集中的に設定して送付し，ブラ

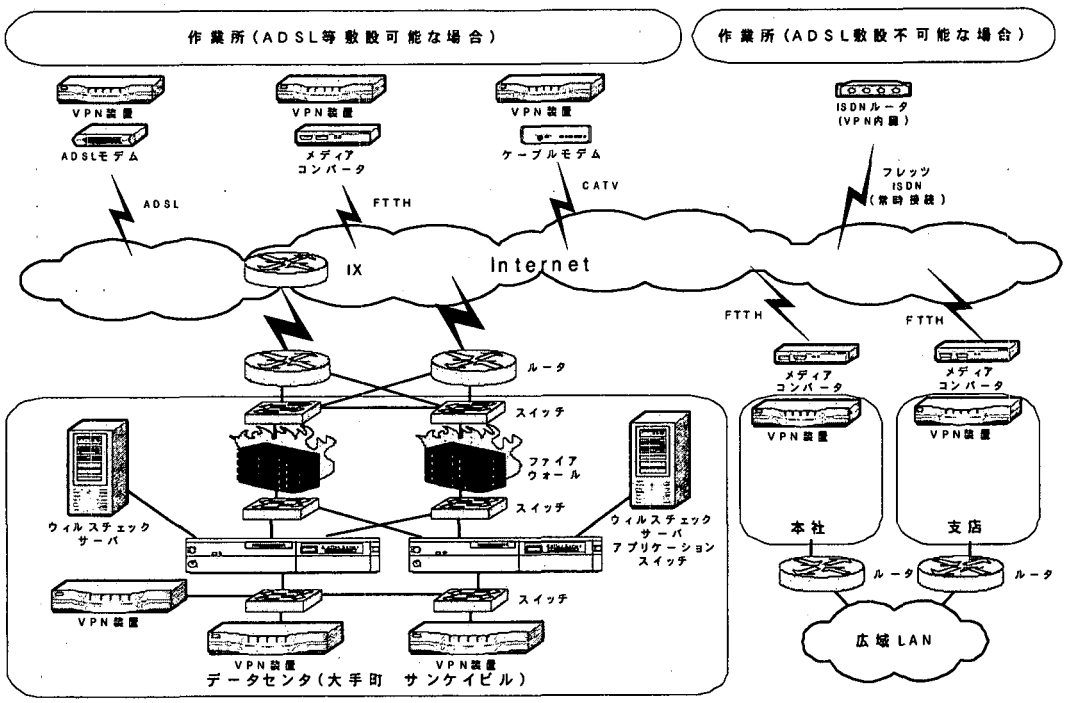

図-12 InternetVPN構成

ックボックス化することで，建設作業所の負担を軽減し，安全性を向上させることが可能となった．

b) 透過プロキシ

作業所内で発生する作業所外部へ向けた全ての通信を，IDC を経由して行うためには，IDC にあるプロキシサーバ（proxy server：代理サーバ）を経由させる必要がある．IDC にあるプロキシサーバを経由せずに，作業所内からインターネットに接続するためには，VPN 装置から直接インターネットに接続する必要があり，セキュリティー上重大な問題となる．しかし，Windows に代表される OS においては，プロキシサーバの設定はアプリケーション毎に行う必要があるため，接続のための作業量が増加する．また，「ネットワークが繋がらない」といった障害要因にも繋がる可能性があり，回避する必要がある．

そこで，IDC 内に透過プロキシを設置し，作業所からの全ての通信を，強制的に透過プロキシを通過させることによって，個々の PC へのプロキシの設定を不要とした．

6．実施内容

(1) システム構成

作業所を考慮した，InternetVPN のシステム構成を図-12 に示す．

インターネット回線は，国内インターネットの中心であり海外インターネットの玄関口である，JPIX，NSPIXP2 を収容している大手町 KDDI ビルの JPIX に，同一敷地内で隣接するサンケイ大手町ビルの CRC OiDC（大手町インターネットデータセンター）より 10Mbps で直結している．OiDC には，ルータ 2 台，スイッチ 6 台，ファイアウォール 2 台，ウィルスチェックサーバ 2 台，VPN サーバ 3 台を冗長構成により設置している．OiDC，KDDI ビルともに，自家発電設備を備え，電源，空調設備が冗長構成となっており，災害時にも十分に機能する．

また，作業所側は，ADSL による接続を標準としているが，回線の状況により，FTTH，ISDN による常時接続環境を選択可能としている．

(2) 構築方法

構築は，2002 年 12 月に IDC の機器準備が完了し，2003 年 1 月より 100 拠点/月で接続を行っている．開設手順は，

- ADSL の申請
- ADSL 接続確認（ADSL 開通日確定）
- VPN 接続申請
- VPN 機器送付
- ADSL 開通（VPN 接続）

であり，ADSL の申請から接続まで概ね 2 週間程度で完了する．

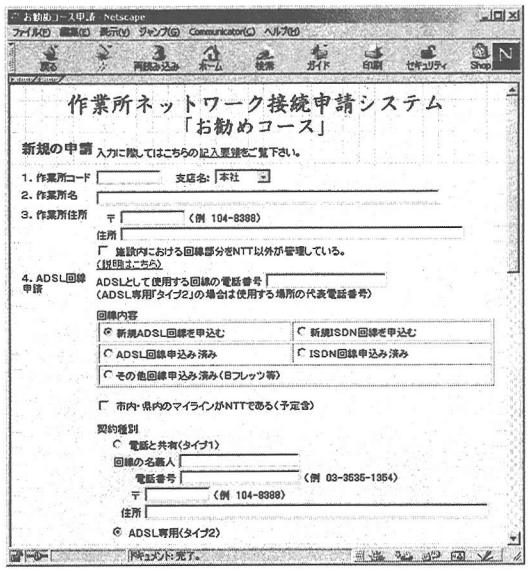

図-13 接続申請画面

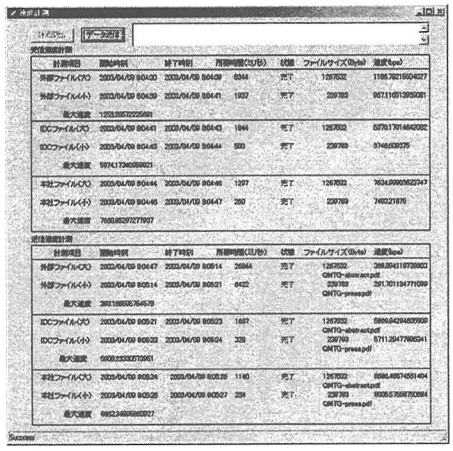

図-14　速度計測ソフト

なお，申請から開通までは全てOnlineで行い，開通状況の確認も可能となっている（図-13）.

(3) 実施対象

実施対象は，

- 営業所　68箇所
- 作業所600箇所

の計668箇所であるが，機器性能としては，1000箇所以上の対応が可能な構成となっている.

7．実施結果と課題

(1) 実施状況

2003年4月1日現在で，222箇所の設置が完了している．表-3に構築状況を示す．3月末現在，作業所の整備率は33%，営業所の整備率も33%となっている.

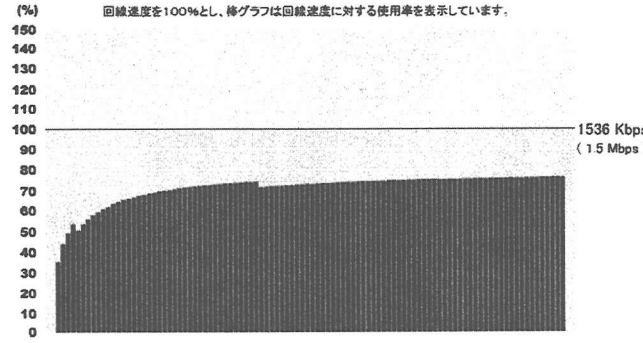

図-15　httpによるデータ転送速度変化

また，回線はADSLが81.5%，ISDNが17.5%，FTTHが1%である.

(2) 実効速度調査

VPNによる実効速度は，計測用のソフトウエア（図-14）を独自に開発し，拠点側のPCにより計測を行った．このソフトウエアは，IDC，本社，外部ホスト(biglobe)に対してhttpによるデータのアップロード，ダウンロードを行い，データの転送時間により，転送速度を計測するものである．転送速度は，各ホストに対し，1.2MB，200kBの大小2種類のデータを転送し，データ量の差をその所要時間の差で除することにより，速度を算出している．httpのデータ転送の場合，図-15のように初期速度が遅いためこの影響を排除するための措置である.

契約別平均速度を表-4に示す.

本社，IDCのダウンロード速度はADSLの場合それぞれ平均1,167kbps，1,141kbpsとなった．また，アップロード速度はそれぞれ，526kbps, 596kbpsとなった．インターネットへの接続は，ダウンロード302kbps，アップロード423kbpsであるとなった．また，ISDNの場合はアップロード，ダウンロードとも50~60kbpsとなった.

ADSLにおいて，12Mの契約よりも8Mの契約のほ

表-3　InternetVPN開設累計

(件)

年/月	作業所			営業所			計
	ADSL	ISDN	FTTH	ADSL	ISDN	FTTH	
2002/12	10	1	0	1	0	0	12
2003/ 1	63	5	0	3	0	0	71
2003/ 2	112	20	1	9	1	1	144
2003/ 3	160	38	1	21	1	1	222

うが平均速度が早いという結果になった．契約電話番号より電話回線の線路情報検索[18)19)]により算出した伝送損失とIDCまでの実測速度，理論値[20)]の関係とを図-17 に示す．今回の計測データは電話局から離れているため，伝送損失30~50dbの範囲が多く，平均速度が低下していることがわかる．また，8Mと12Mの平均速度の逆転は，12Mの契約が伝送損失が高い場合に利用されているケースが多いことが原因と考えられる．

また，インターネット上のホームページへのアクセス速度が内部に比べ低下している原因としては，

- ウィルスチェックサーバ等の処理速度が遅い
- ホームページを掲載しているサーバまでの回線が混雑している
- インターネット上のホームページを掲載しているサーバの処理速度が遅い

という原因が考えられる．個別に契約しているADSL回線からの計測によれば，1Mbps以上の計測データも取得されているため，ウィルスチェック等による影響が大きいと考えられる．

また，伝送損失が25db未満の測定点について8M，12Mの契約で速度が低下してあいるが，

- ISDN等による干渉やノイズ
- 拠点側ネットワークの混雑
- 計測サーバの負荷の増大
- IDC側ネットワークの混雑

などの原因が考えられる

全体的な速度分布では（図-17），ダウンロードは外部が150~350kbps，IDC，本社からは250k~1.5Mbps，アップロードは外部が250~650kbps，IDC，本社が300~700kbpsにまとまっており，最低でもISDNの5

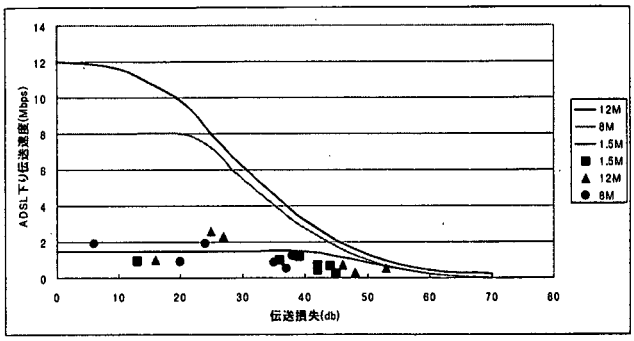

図-16 下り伝送理論値と実績

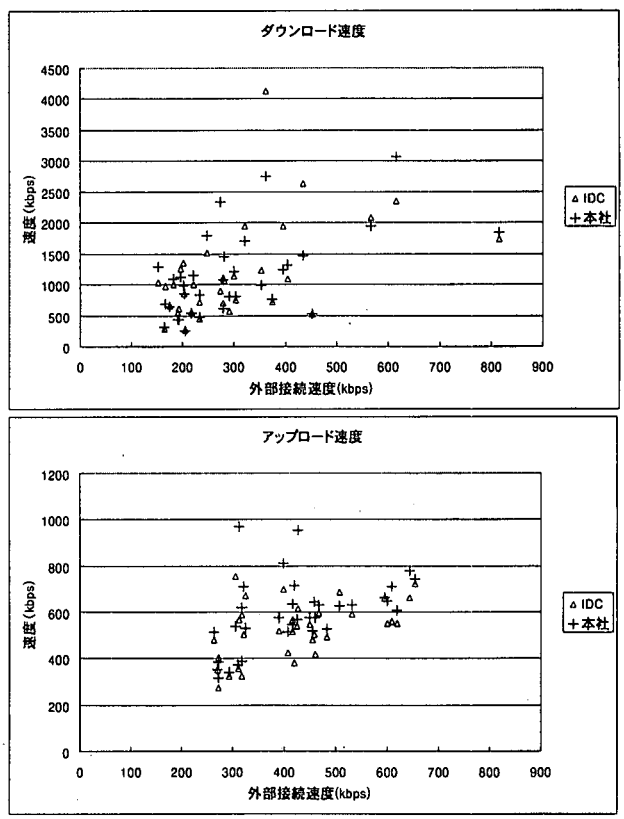

図-17 速度分布

表-4 契約別平均速度

ダウンロード (kbp)

	Internet	IDC	本社	最高/最少*
ADSL 12M	316	1,282	1,293	3,058 / 281
ADSL 8M	344	1,413	1,390	4,132 / 522
ADSL1.5M	257	722	729	1,223 / 264
ISDN 64k	55	58	58	60 / 56

アップロード (kbp)

	Internet	IDC	本社	最高/最少*
ADSL 12M	490	561	662	952 / 324
ADSL 8M	434	538	600	810 / 358
ADSL1.5M	408	522	569	716 / 382
ISDN 64k	50	52	55	59 / 46

* 最小値はIDCまでの接続速度

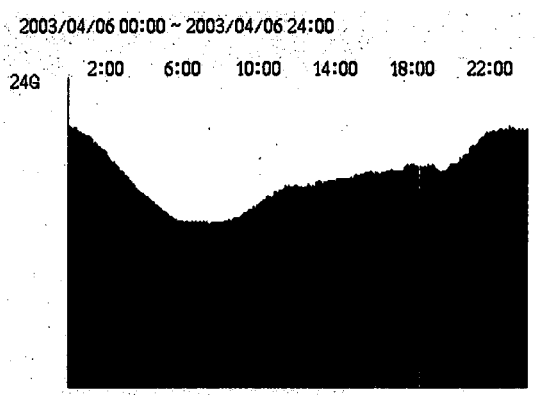

図-18 JPIXトラフィックの日変化

倍程度の速度が確保されている．

(3) 利用状況

まず，インターネットの混雑状況を把握するために，JPIX のトラフィックの日変化を図-18 に示す．19 時から翌 2 時まで利用のピークを迎え 3~11 時までの利用が少ないことがわかる．日本国内のインターネットの幹線はピーク時の利用量を想定して構築されているため，8~18 時までのビジネスタイムは余裕があり安定的な接続が期待できる．

IDC におけるトラフィックのうち，

- 全体：　VPN を通過したトラフィック
- 社外：　ウイルスゲートを経由したトラフィック

を MRTG[16]（Multi Router Traffic Grapher）により計測した．

計測結果を図-18 に示す．それぞれ，年データは日平均，月データは時間平均，週データは分平均，日データは秒平均により算出している．

まず，VPN を通過するトラフィックを検証する．VPN サーバは作業所から IDC に向けた全てのトラフィックを表す．就業時間中は概ね 2 Mbps 程度で推移し，始業時（8~9 時），昼休み（12~13 時），終業時（17~18 時）にピークを迎えている．就業時間外の 22~23 時にピークが見受けられるが，データのバックアップ等の作業と考えられる．日変化では土曜日も開所している作業所が多いためか，トラフィック量の減少は少ない．また，日曜日は 0.5M 程度とトラフィックが少ないことがわかる．年変化では，3 月に向けてトラフィックが上昇しているが，これは接続拠点数の増加が原因と考えられる．

次に，ウィルスチェックサーバのトラフィックを検証する．ウィルスチェックサーバは社内より Internet に向けた全てのトラフィックを表し，VPN を通過するトラフィックとの差が作業所から本社等の拠点への通信となり，その量は概ね 20%程度にあたることがわかる．

(4) 費用比較

InternetVPN による費用は，全体にかかる費用と拠点側接続費用で構成される．内容を列記する．

一方，従来のダイアルアップネットワークの場合，2002 年 3 月の実績は，

- 全体にかかる費用：　4,175,000 円/月
- 拠点側接続費用　：25,323,000 円/月（782 拠点）

であり，全体で 29,498,000 円/月であった．

InternetVPN によるネットワーク費用は 782 拠点の場合，

3,120,000 円/月+4,950 円/月/拠点×782 拠点

＝6,990,900 円/月

であり，22,507,100 円/月（年間約 2.7 億円　72.4%）のコスト削減が可能となる．

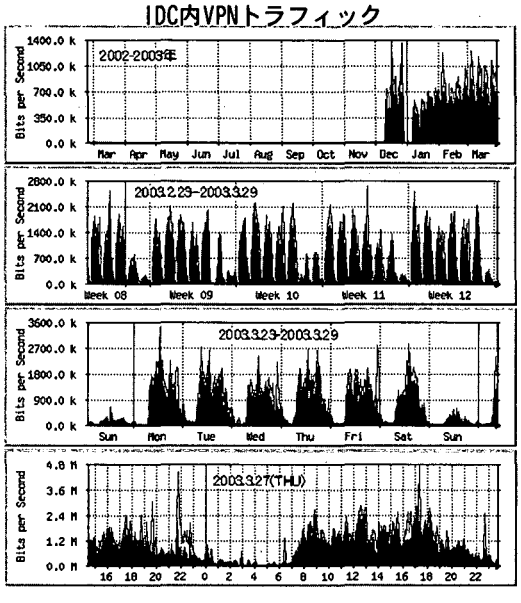

図-19 IDCトラフィック

8．まとめと今後の課題

セキュリティーや安定性が不足しているため，作業所等の他拠点遠隔地接続に不向きであったInternetVPNを，

- IPsecの利用
- IXの直接利用
- VPNの自動復旧システム
- VPN装置のブラックボックス化
- 透過プロキシ

の技術を統合し，セキュリティーと安定性を確保し利用可能とした．

約200拠点の接続を実施した結果，通信速度を従来のISDNの5倍以上に，コストを28%に削減することが可能となった．

一方，残された課題として，

- ADSL 高速接続地域における速度低下の現象解明
- InternetVPNによるモバイル接続の実用化
- InternetVPNを利用した音声通信の統合
- 高速常時接続を前提とした新たな拠点向けサービスの提供

があげられる．

情報技術は時々刻々と進化し続けており，SSH（Secure Shell）やSSL（Secure Socket Layer）を利用したIPsecに代わる技術も開発されている．また，Internetの利用状況も変化しており，今後は接続費用の低下に加え，ADSLのさらなる高速化やFTTHの普及が見込まれる．

本システムは任意の接続回線を選択できるため，これらの技術動向に対しても十分に対応可能であると確信している．（以上）

表-5　InternetVPN費用

◆全体にかかる費用　　3,120,000円/月

IDC利用料	1,860,000円/月
IX接続料	960,000円/月
機器管理料	300,000円/月

◆拠点側接続費用　　4,950円/月/箇所 *

ADSL回線利用料	2,650円/月
ADSLモデムレンタル	550円/月
プロバイダ利用料	1,750円/月

* フレッツADSL8Mの場合

参考文献

1) 総務省：ＤＳＬ普及状況公開ページ，http://www.soumu.go.jp/joho_tsusin/whatsnew/dsl/index.html

2) 土木工業協会:2002年度土工協情報化実態調査報告書，pp. 2，2002

3) 日本インターネットエクスチェンジ株式会社：JPIX トラフィック，http://www.jpix.co.jp/jp/technical/traffic.html

4) 高度情報通信ネットワーク社会推進戦略本部：e-Japan 戦略（要旨），http://www.kantei.go.jp/jp/it/network/dai1/0122summary_j.html

5) IETF：RFC2401, http://www.ietf.org/rfc/rfc2401.txt

6) IETF：RFC2006, http://www.ietf.org/rfc/rfc2006.txt

7) 桑津浩太郎：拡大する次世代ネットワーク・アウトソース戦略，NRI データサービス第一回アウトソーシングセミナー，2003

8) イー・アクセス株式会社:eAccess 障害情報，http://www.eaccess.net/support/support_info/obstacle/service_outage_th.html

9) 株式会社アッカ・ネットワークス:アッカ障害情報，http://www.acca.ne.jp/support/user_supporttrouble_info/index.html

10) ソフトバンクBB株式会社:YahooBB障害情報，http://www.bbtec.net/support/report/trouble/

11) 日本電気株式会社:Biglobe 障害情報，http://support.biglobe.ne.jp/cgi-bin/shogai/guest2.cgi?action=search&area=99

12) ニフティ株式会社:@nifty障害情報，http://www.nifty.com/supinfo/trouble_bb.htm

13) エヌ・ティ・ティ・コミュニケーションズ株式会社:OCN テクニカルサポート障害情報，http://customer.ocn.sphere.ne.jp/cgi-bin/trouble/report.cgi?mode=1

14) 土木工業協会：JV 現場ネットワークの構築と運用ガイドライン初版，pp. 5，2001

15) 土木工業協会：JV 現場ネットワークの構築と運用ガイドライン補足版，pp. 6，2002

16) Tobias Oetiker,Dave Rand : MRTG, http://people.ee.ethz.ch/~oetiker/webtools/mrtg/

17) イー・アクセス株式会社:距離判定結果，http://www.eaccess.net/tools/area/result_dst.html

18) NTT西日本株式会社:線路情報開示システム，http://www.ntt-west.co.jp/open/senro/senro_user_info.html,

19) NTT東日本株式会社：線路情報開示システム，http://www.ntt-east.co.jp/line-info/

20) NTT 東日本株式会社：ADSL 下り伝送速度と伝送損失の関係，http://flets.com/misc/adspeed.html