「建物・設備の遠隔監視システムの動向」

ミタカ通信株式会社　井出正彦

【はじめに】

近年、地球環境保全にともない、温暖化防止（二酸化炭素削減）・エコロジー・省資源・省エネルギー・運用コストの削減等、建物・設備管理の分野でも様々な削減が求められてきております。しかしながら防災・防犯・情報セキュリティも含め建物・設備・情報の保全維持管理の要求や要望は年々高まっており、管理側には一層の努力が必要となってきております。そこで最近、特に注目されてきているのが遠隔監視システムです。遠隔監視システム自体は、以前より様々な物があり、特に目新しいものではありませんが、最近の通信インフラのブロードバンド化、低価格化にともない、接点データやアナログデータだけではなく、画像や映像・音声までリアルタイムに情報を伝送することが可能となりました。回線の選択肢も一層広くなり、様々な機器・ユニット・モジュール等を組み合わせることで、目的にあったベストな遠隔監視システムを構築することが可能となります。今後、サービスの向上を計りながら、少人数で効率よく運営・維持管理を行うためには、必要不可欠なツールとなることでしょう。遠隔監視システムといっても、監視対象も多種多様で用途ごとに様々なシステムが考えられますが、ここでは建物や建物に関連する設備に的を絞って、遠隔監視システムの基本的な事柄や、導入時のポイントなど

を解説します。

【１、遠隔監視システムの目的や種類・分類・対象物】

（１）建物・設備の遠隔監視の目的とは

「監視側」では建物・設備の一元管理及び少人数化・無人化による建物・設備管理の効率化の推進。「建物オーナー側」へは的確な情報の提供やプランニング、さらに低コストでの維持管理を実施。「テナントの利用者」へは設備異常などの即時適切な対応を行い快適で安心・安全に利用できるようなサービスの提供などを総合的に実施する事により、建物そのものの付加価値を高める事にあると考えます。

（２）遠隔監視の種類・分類・対象物としては大まかに次のようなことが考えられます。

①円滑な維持管理のための監視（故障や異常、警報の通知により即時適切な対応を行う）

a)設備の故障監視（対象設備例：受変電、電気、ガス、給排水、各水槽、自火報、空調、冷凍、ボイラー、照明、通信、エレベータ、エスカレータ、駐車場、インターホン、電気錠、その他）

b)設備の異常監視（対象異常例：電気「電流・電圧・トリップ」、動力盤、発電機「電圧・電流、各水槽水位、給排水、空調「温度・湿度」、冷凍「温度」、熱源、排煙、排気ファン、照明、通信、輸送、駐車場、その他）

c)設備の警報監視（対象警報例：停電、漏電、高圧地絡、低圧地絡、火災、ガス漏れ、ガス緊急遮断弁作動、漏水、エレベータ、エスカレータ、侵入、地震、扉・ゲート長期開放、メールボックス長期開放、その他）

②省エネルギー・経費削減のための監視（空調や照明の ON、OFF や温度設定等をリアルタイムに監視、夜間時や休日・季節などによる設備や機器の遠隔制御を行う）

a)設備のリアルタイム計測監視（対象計測例：電気「電流・電圧」、照明「ON/OFF、調光」、空調「稼動時間、温度・湿度」、冷凍「温度」、各水槽「水位」、その他）

b)設備の遠隔制御（対象制御例：照明「ON/OFF、調光」、空調「ON/OFF、温度・湿度」、冷凍「温度」、電気錠「開・閉」、その他）

③建物マネージメントのための監視（収集したデータにより、フィルターの清掃や消耗品等の交換や設備機器の入換え等の長期的なマネージメントを行ない、計画的な維持管理を行う）

a） 設備の計測収集監視（対象設備例：電気、空調、照明、その他）

b） 設備の稼働状態監視（対象設備例：電気、空調、照明、給排水、各水槽、冷凍、ボイラー、その他）

④資産保全管理ための監視（監視カメラ・防犯センサー及び自火報・防災センサーによる防犯・防災管理、さらに通信・情報のセキュリティ管理を行う）

a)監視カメラによる監視（対象物例：生物、入口・出口、エレベータ、エスカレータ、駐車場、倉庫、各種設備、その他）

b)防犯センサーによる監視（対象物例：生物、ゲート、扉、窓、建物外周、エレベータ、駐車場、倉庫、各種設備、その他）

c)自火報・防災センサーによる監視（対象物例：建物全体、各種設備、その他）

d)情報・通信のための監視（対象物例：建物内外の通信網、サーバー、各種データ、個人情報等）

【２、遠隔監視システム導入時のポイントⅠ　システム・設備機器】

（１）遠隔監視システム導入の大まかな流れ

①監視対象の規模を含めたシステム設計（全体的な大よそのボリュームやデータ量の把握）

↓

②監視対象側に適合する機器及び通信回線の選定（設置場所や設備との接続を考慮）

↓

③監視側の機器及び通信回線の選定（データ量に見合う、またはそれ以上のスペック、冗長化）

↓

④遠隔監視システム全体のセキュリティ対策（データの管理及びシステム関係者への教育等）

↓

⑤運営・維持管理（システムを生かした監視マネージメントの運用）

（２）監視対象側（端末側）の大まかなポイント

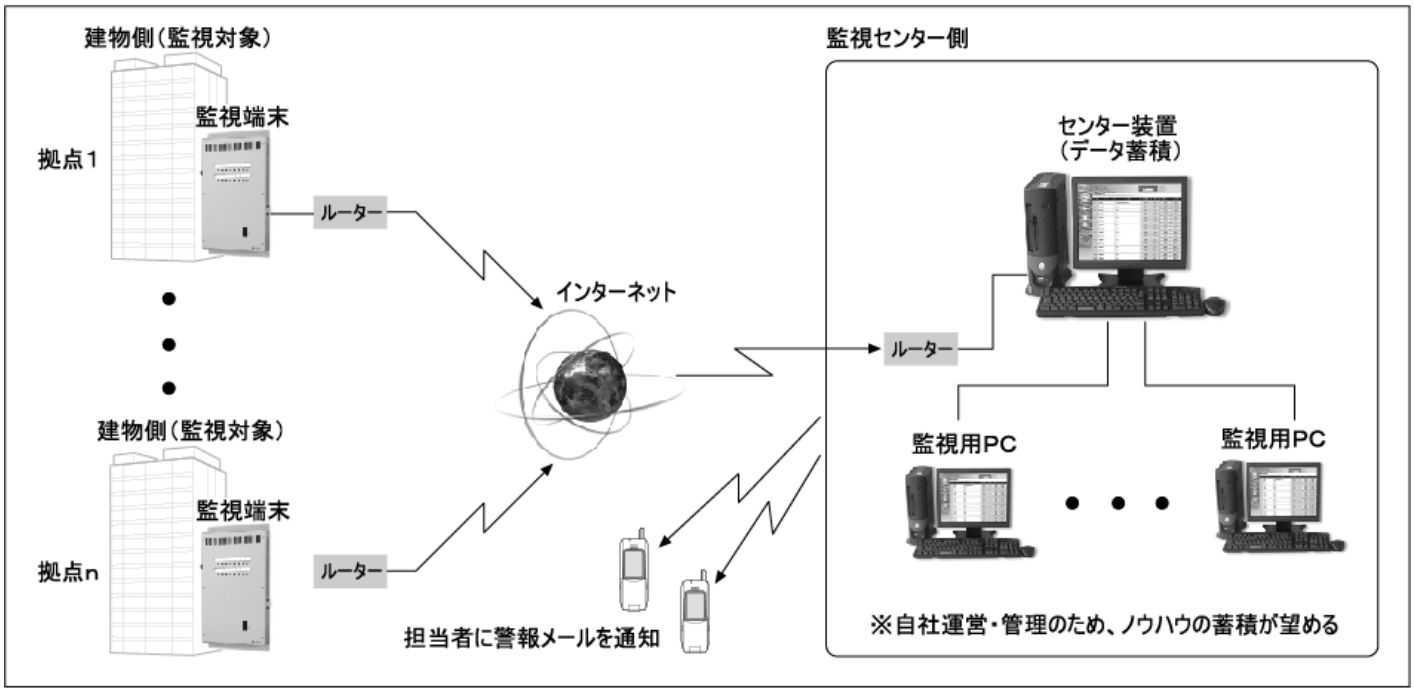
①監視対象側の監視対象種別（警報などの接点の内容・点数及び温度や電源などのアナログデータの内容・点数）
②監視対象側からの警報及びデータの受け渡しの確認（たとえばエレベータ設備側から故障の接点出力は可能か、電源盤から電流や電圧等のデータ出力が可能か、どんな信号内容か等々）
③監視対象側端末の設置場所の状態確認（設置スペースや固定方法、温度・湿度や埃などの環境、他設備との信号の取り合いや電源・ＵＰＳ等の有無）
④監視対象側の通信回線の有無及び種類（新たな敷設は可能か）
※設備側からの接点や情報が必要な場合、各設備側で接点やデータを外部に出せるような端子台やコネクタなどをそれぞれの設備メーカーへ追加工事依頼の必要があります。（責任の分解点、切り分けをハッキリさせる事、相手設備に影響を与えないようにシステムを構築する事が必要です）

（３）監視側（センター装置）の大まかなポイント（システムとして監視側にパソコンまたはサーバーを想定）

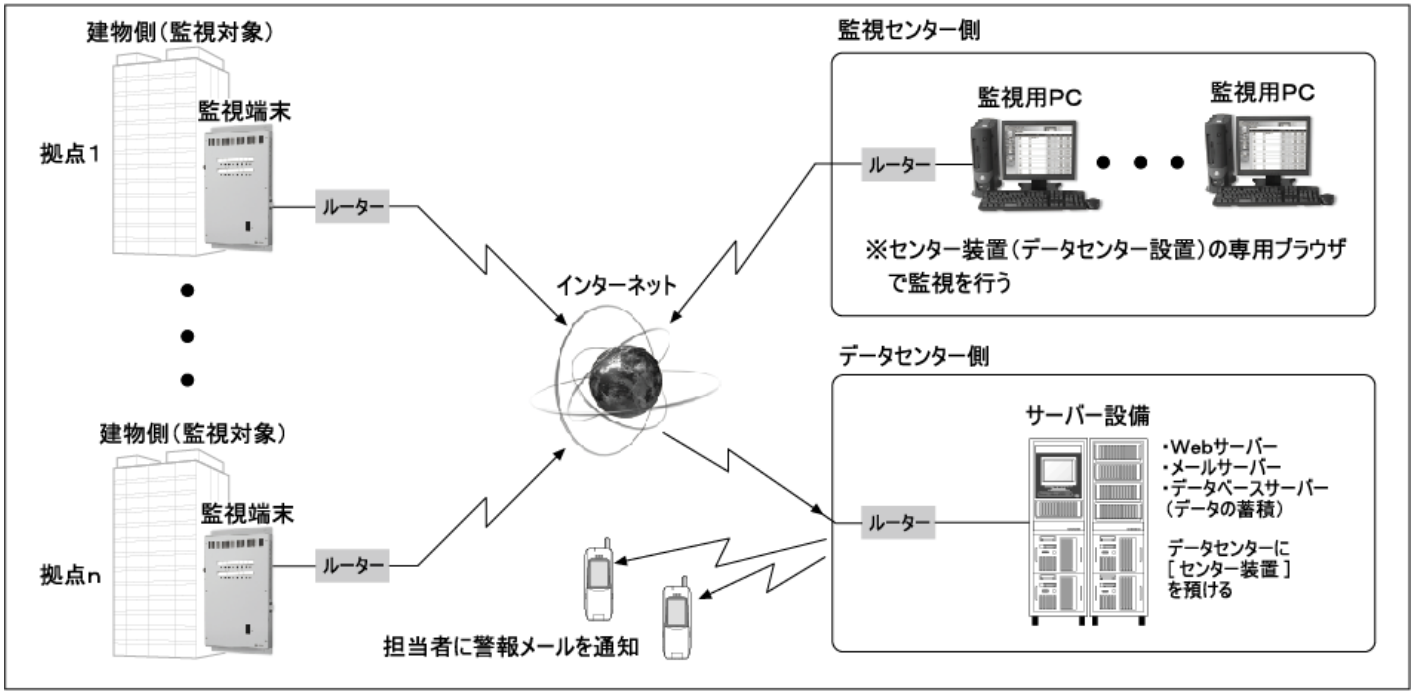
①監視対象側の把握（建物の棟数や設備情報の点数、監視カメラ設備等の大まかな想定数）
②監視対象側の接点数や各種データの想定数に見合う、またはそれ以上のスペックの受信設備（パソコン・サーバーのハードウェアのスペックはもちろんの事、警報点数や各種データ等を蓄積して検索やソートを行うデータベースの処理能力や容量なども考慮）
③監視対象側との通信用の受信機器（モデム、ＴＡ、ルータ等及び通信回線の安定性・安全性を考慮）
④センター装置の設置場所（パソコン・サーバー等の機器を設置するためのラックまたはデスク等、固定・防振を考慮）
⑤センター装置の電源（電源容量の確認やＵＰＳ等の冗長化対策を考慮）
⑥センター装置の空調設備（温度・湿度の管理する為、センサーの設置も考慮）
⑦センター装置の耐震や防災対策（耐震の建物が望ましいが、耐震対策の機器収納架でも良い）
⑧センター装置の通信回線、パソコン・サーバー、データバックアップ等の冗長化の対策（緊急時の対策として他地点でのデータバックアップ設備等も考慮する）
⑨総合的なセキュリティ対策（ファイアーウォール、ウイルス、通信回線、各種データ、個人情報等の管理対策）
※監視側設備（サーバー及びソフトウエアを除く）を外部（データセンター等）に委託する事も可能です。

a)自社で監視センターを運営する場合[図１].（メリットとしては、自社資産で自社運営の監視センターでなければ受注できない物件などもある事と自社で運営することにより、付加価値やノウハウの蓄積がある。デメリットとしては、サーバーを設置する場所及びサーバー、回線、電源、UPS、空調、耐震などの管理等の手間がかかる）
b)外部（データセンター等）に委託する場合[図２].（メリットとしては、物理的サーバーの管理が一切必要なくセキュリティ面でも安心がある。デメリットとしては、自社にセンター設備のノウハウの蓄積がない）
※センター設備を外部委託する場合の通常監視は、インターネットに接続できるパソコンにより（ID やパスワードによりログイン）専用のホームページにアクセスして監視を行なうイメージです。

[図1]
自社で監視センター設備を運営する場合のイメージ図



[図2]
外部(データセンター等)に監視センター設備を委託運営する場合のイメージ図



【３、遠隔監視システム導入時のポイントⅡ　通信回線について】

遠隔監視システムを導入するにあたり、最も多く質問を受けるのが通信回線です。遠隔監視にとって通信回線はいわば生命線です。通信回線の選択によっては、使用する機器等も含め、システム全体にも大きく影響します。使用内容や情報量や設置場所、安全性や安定性、さらにコスト等を総合的に見て慎重に選択することが重要です。現在インターネット回線の普及にともない、回線の種類やサービスが増えてきておりますので、ここでは一般通信回線（一般電話網や専用回線）とイーサーネット回線（イーサーネット接続やインターネット回線）とを大きく２つに分類して説明します。

（１）一般通信回線の種類と分類　［図３］

一般通信回線は専用回線（直通回線）と交換回線（公衆回線）の２種類に分類されます。

①専用回線（直通回線）は、２拠点間を直接結び、途中に交換機を置かない回線のことをいいます。監視側（センター側）と監視対象側（拠点側）との１対１での通信となりますので、監視対象側が多地点の場合には、同じ数量の回線が監視側にも必要となります。回線は常時接続されており、安全性・安定性に特に優れ、リアルタイムでの監視が可能です。回線の費用は、毎月の定額制です。（拠点間の距離及び品目により費用は異なります）

※重要な監視対象や、拠点間が近く、通信の頻度が多い場合向き

②交換回線（公衆回線）は、必要な時（警報の発報等）だけ相手側と接続して、通信を行う回線のことをいいます。代表的な品目としては、一般の電話回線や ISDN 回線です。監視側（センター側）へ監視対象側（拠点側）からのダイヤルアップで接続し通信終了後回線を切断します。監視対象側が多地点の場合には、同じ数量の回線が監視側にも必要となります。決まった相手先の接続に限定すれば、安全性・安定性は比較的良いです。回線の費用は、接続する度に料金が加算される従量制です。（拠点間の距離により費用が異なります）

※データ量が少なく通信の頻度が少ない場合向き

（２）イーサーネット通信回線の種類と分類　［図４］

イーサーネット通信回線は、大まかに、専用回線（イーサーネット直結型）とギャランティー回線（バックボーン直結型）及びベストエフォート回線（各種インターネット網接続型）の３種類に分類されます。

①専用回線（イーサーネット直結型）は、拠点間をイーサーネットで LAN のように直接結ぶ回線のことをいいます。監視側（センター側）と監視対象側（拠点側）を直接結ぶ事によりプライベートネットワークに近い形での利用が可能となります。回線は常時接続されており、安全性・安定性に特に優れ、リアルタイムでの監視が可能です。回線の費用は、毎月の定額制や従量制です。（拠点間の距離及びネットワークの組み方や回線の種類や品目により費用は異なります）

※プライベートなネットワークを必要とし、重要な監視対象物や拠点間の情報量が多い場合向き

②ギャランティー回線（バックボーン直結型）は、各キャリア（通信事業者）のバックボーン（基幹回線）に直結したインターネット回線です。ほとんどの品目が、バックボーン回線・設備の二重化や通信速度・帯域・品質などを保証しており、さらに LSA というサービス品質保証制度（可用性、遅延時間、故障回復時間、障害通知時間等）に対応した高信頼性の回線です。常時接続が可能で、安全性・安定性に優れ、リアルタイムでの監視が可能です。回線の費用は、毎月の定額制です。（回線の種類や品目と収容局までの距離により費用は異なる場合があ

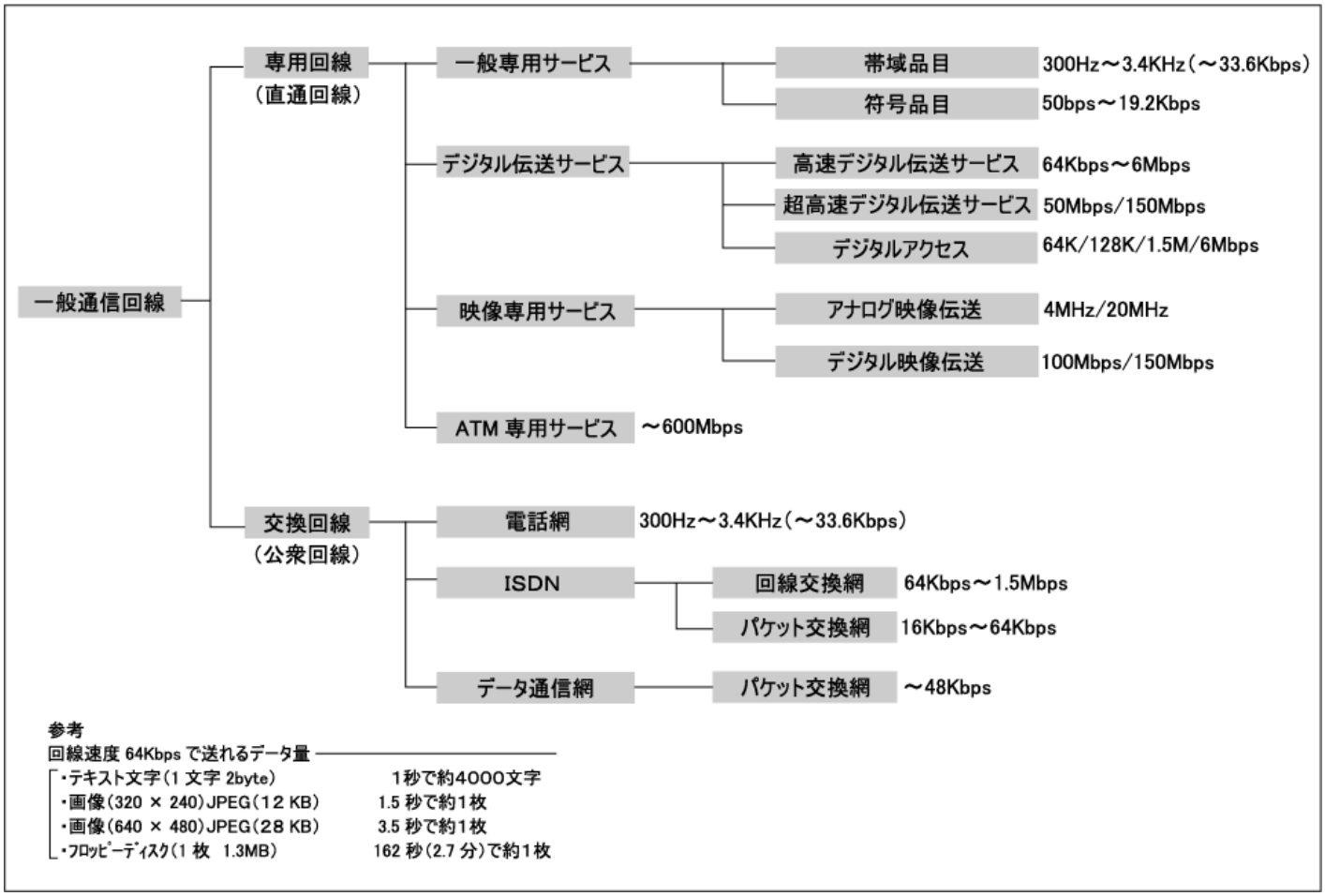
ります)
※回線コストが見合うようであれば、監視センター側の基幹回線向き

③ベストエフォート回線（インターネット網接続型）は、一番多く使用されている一般的なインターネット回線です。低コストでのサービスを目的とした回線で、インターネット網を利用し、一つの回線を不特定多数で使用しています。そのため同時に通信するユーザ数やトラフィックの増加などにより実質的な通信速度は低下します。通信速度に関しては、「最大限の努力をするが速度保証のない」回線です。しかしながら、低コストのため、最近では遠隔監視等への利用も増えてきております。常時接続が可能で、安全性・安定性は良く、リアルタイムでの監視が可能です。回線の費用は、毎月の定額制です。(回線の種類や品目及びサービス地域や固定 IP サービス等さまざまですので、各通信業者に事前に確認が必要です)
※低コストをいかして、特に監視対象側の回線向き

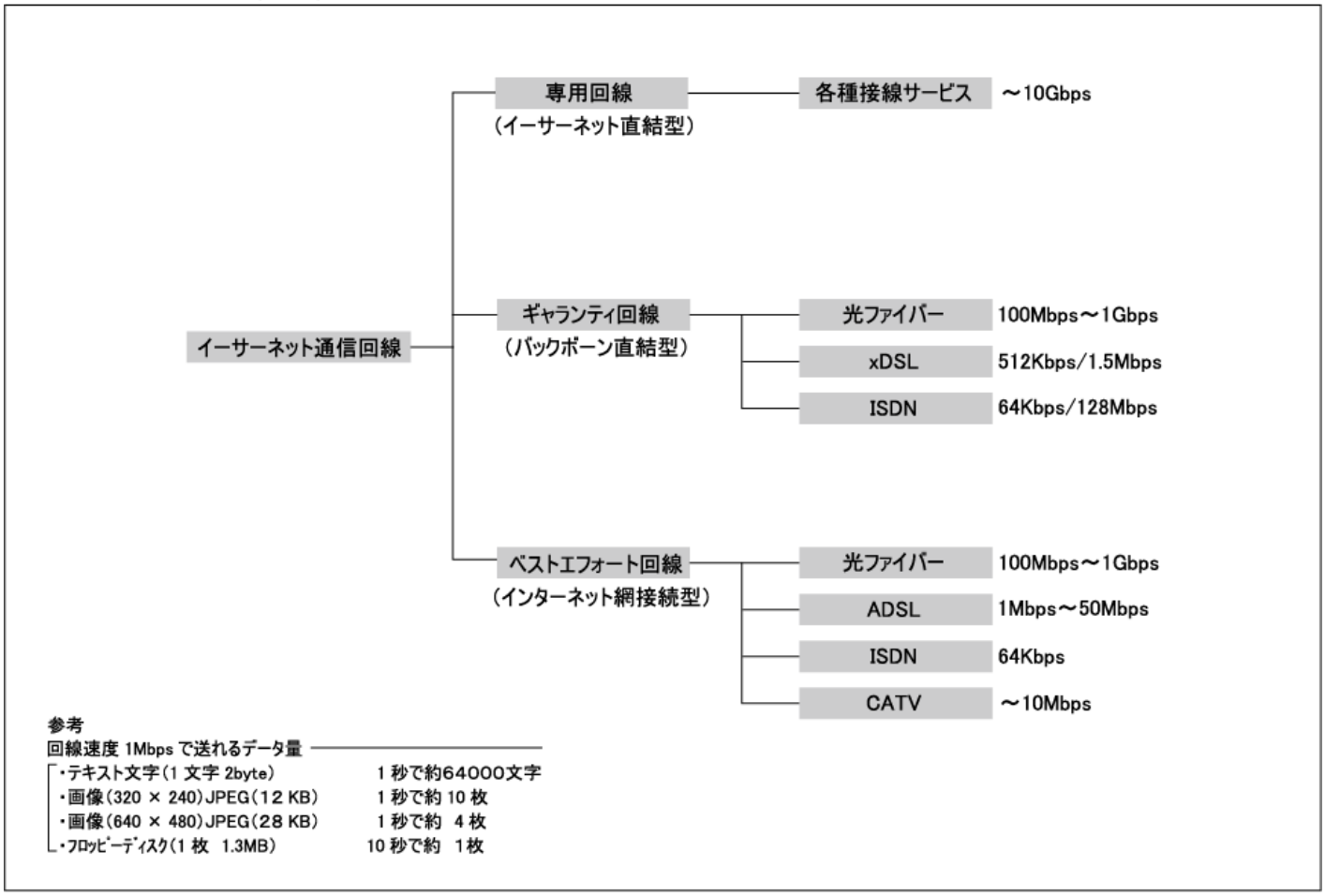
「通信回線備考」

その他の通信回線としては、有線回線（CATV、構内 LAN、構内回線他)、無線回線（無線 LAN、DoPa、PHS、携帯電話、SS 無線他)、衛星回線など、記述した以外にも多数ありますので、用途や目的、システムに適合する回線や機器・モジュール等を選択することでさらに幅の広い遠隔監視が可能となります。

[図3]
一般通信回線の種類と分類



［図４］
イーサーネット通信回線の種類と分類



【４、遠隔監視システム導入時のポイントⅢ　情報セキュリティ】

昨今、情報の流出、サイト攻撃、ウイルス・ワーム等による被害が毎日のように騒がれています。それら外部、内部からの攻撃や侵入等により重要なデータ情報、個人情報なども盗難や漏洩、改ざん、消失等の被害の恐れがあります。さらには、自社のパソコンやサーバー等が踏み台（ウイルスやワームに侵され攻撃プログラムを入れられる）にされ被害者のはずが攻撃する加害者側になる場合や、内部の情報がウイルスメールによりバラ撒かれたり等、社会的信用にも大きくかかわります。遠隔監視システムを構築するにあたり情報セキュリティは非常に重要な要素となりますのでしっかりと対策することが必要です。

（1）セキュリティポリシーについて

セキュリティポリシーとは企業（各組織）が情報資産に対してどのように取り組み、脅威から何故、何を、どのような方法で保護するのか等の「明文化」、さらには従事する社員がどのように行動すべきかという規定を設けた「方針」の事をいいます。遠隔監視事業を行なうという事は、さまざまな顧客のデータを所有・共有する事になります（遠隔監視システムにより受信したデータは顧客のデータであると共に大切な資産です）信頼されて監視・管理を行なうには、それ相応のセキュリティポリシーが必要です。企業資産は「ひと」・「もの」・「かね」の３要素があるといわれておりますが、現在では、もうひとつ４番目の要素として「情報」が重要な位置をしめており

ます。それだけに「情報」へのセキュリティ対策が重要となります。

（2）セキュリティポリシーの３要素

①機密性（許可された者だけが情報にアクセスできる事を確実にすること）
②完全性（情報が正確・完全に保存・維持されること）
③可用性（情報が定められた方法でいつでも利用可能なこと）

（3）セキュリティの種類と分類

①物理的セキュリティ（遠隔監視システム・設備等の物理的な保護や監視センターへの侵入による盗難や破壊等の被害からの保護）
a)自然災害（地震、洪水や火災などの防災対策）
b)侵入対策（入室制限や入出退管理、生体認証、ケーシングによる保護、鍵などの対策）

②システムセキュリティ（システムへの不正アクセスによる、プログラムの改ざん、システムダウン、破壊等からの保護）
a)ファイアウォール等による保護（システムへの侵入を防止）
b)パスワードや生体認証等による保護（パスワードや認証にアクセス権限を適用し、システムへの侵入を防止）
c)システムの二重化等、冗長化による保護（システムを二重化、冗長化することによりリスクの低減を図る）
d)システムソフトのバックアップによる保護（システムソフトを更新ごとにバックアップし問題発生時に速やかに復旧できるような対策をする）

③データセキュリティ（データベースへの不正アクセスによる、データ情報、個人情報の改ざん、漏洩、消去、破壊等からの保護）
a)ファイアウォール等による保護（データベースへの侵入を防止）
b)パスワードや生体認証等による保護（パスワードや認証にアクセス権限を適用し、データの不正な改ざん、盗難や消去を防止）
c)社員の教育による倫理的保護（従事する社員に、データ情報、個人情報の重要性、機密性、情報倫理の教育を徹底し、データの不正な改ざん、盗難や消去を防止）
d)ウイルス対策等による保護（対策ソフトによりウイルスやスパイウエア、ワームなどの侵入を防止）

「セキュリティー備考」

インターネットの普及にともない、ネット犯罪も多様化してきております。高額な対策機器やセキュリティソフトの導入も効果はありますが、それよりもシステムに見合ったセキュリティ対策と、日々のデータチェックやバックアップなどを的確に実施すること、さらにセキュリティポリシーに基づき、従事する社員等への徹底した教育がもっとも有効な対応策です。

【５、監視カメラによる遠隔監視の最新動向】

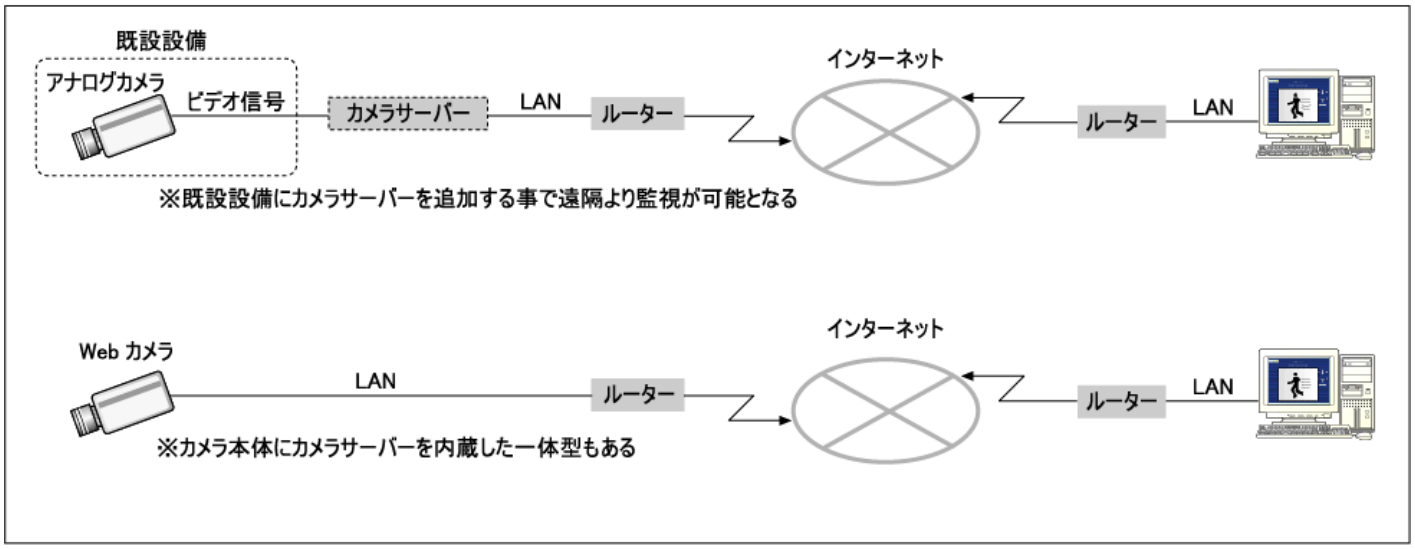
監視カメラも最近の通信機器や回線のブロードバンド化にともない、アナログ（同軸）からディジタル（ＬＡＮ）へと移行してきております。現状では既設カメラも含め、アナログカメラが大半を占めておりますが、それらのカメラにも対応できるカメラサーバー（アナログカメラ信号をＬＡＮに変換）等も多数出てきており、監視カメラのＬＡＮ化、インターネット化は勢いを増してきております[写真１]. カメラサーバー内には専用のＷｅｂブラウザが標準で搭載されており、パソコンでホームページを見る感覚で簡単に利用することができます[写真２]. 既設のカメラ等にも接続が可能なため、監視したいカメラのケーブルの途中に接続することで、既設システムを変更することなく容易に遠隔監視をすることが可能となります[図５]. また専用ソフトやカスタムソフトにより、一度に複数の映像を見ることや、画像の変化をとらえ記録することも可能となり、今後の監視カメラシステムも大きく変わろうとしております[写真３]. ＬＡＮ化、インターネット化により手軽に利用できることもあり、建物・設備の遠隔監視システムでは、今後情報と映像・音声の融合がますます進むと予想されます。

［写真１］

［写真２］

［図 5］

インターネットを利用した遠隔監視カメラシステム



［写真３］

【６、遠隔監視システムの最新の動向・今後の展開】

米国の GE 社が近年、サービス事業の一環として遠隔診断（リモート・ダイアグノスティックス）を実施し効果を上げています。内容としては、はるか 10000m 上空を、1000km 近い速度で飛ぶジェット旅客機のエンジンを、地上のノートパソコンで、24 時間リアルタイムに遠隔監視を行うというものです。警告レベルでは、即時警報メール等で連絡を行ない修理対応する。その他、監視データの分析を基にメンテナンスを行ないます。これによるトラブル回避で、運行の遅延や中止が減少し、カナダの航空会社では年間 30～35%のコスト削減に成功しているというケースもあるそうです。また同社では航空機の他に電気機関車や船舶のエンジン、発電タービン、さらに医療機器などの製品にもセンサーを取り付け、常にベストの状態を保つというサービスを行なっています（注１）。この事により「保守契約」、「メンテナンス契約」を結ぶ事ができ、機器や部品の販売（他社との競争で低利益、低付加価値になってきている）の他に遠隔診断サービスという高付加価値なサービスの展開を実現しています。サービスを提供している側、受ける側、双方共にコストを削減でき、安全・安心と信頼度も向上し、さらに双方共に利益があるという良い事例です。いまや飛行機の中でもインターネットができる時代になり、国内のインターネット普及率は６割を超え７，７３０万人が利用しています（注２）この爆発的なインターネット普及の要因の一つには、インターネット回線のブロードバンド化と低価格化があり、高速な ADSL 回線では、月額通信コストが世界最安水準といわれております。これからの遠隔監視システムは、より多くの情報とリアルタム性を必要と

し、コネクションレスで多拠点を同時に複数箇所から監視できることが求められ、イーサーネット接続・インターネット接続は遠隔監視システムには欠かせないインフラになると考えます。既設設備固有の通信ネットワークも、上位にはイーサーネット接続を想定しているものも多く、今後益々LAN 化、インターネット化し、他設備との統合、融合そしてよりシームレスになり、本当の意味でのオープンネットワークになるであろうと推測されます。それゆえにセキュリティ面や安定性の面、コスト面での一歩踏み込んだシステム設計・構築及び運用・マネージメントが必要となる事でしょう。

（注１）「企業間 EC 実用化の動向」2000 年 JECALS EC/CALS 調査委員会しらべ
（注２）「平成 15 年通信利用動向調査」2004 年 4 月総務省しらべ
※参考文献「通信・ネットワーク入門講座」井上伸雄 著 発行：(株) 電波新聞社 2003 年 12 月

「設備と管理」特別企画掲載記事
ミタカ通信株式会社　井出正彦