＜特集＞

遠隔監視技術の現状と今後の展望

Present and Future of Technology on Remote Operation System

新　誠一 *

東京大学大学院情報理工学系研究科システム情報学専攻

Seiichi Shin*
Course of Information Physics and Computing, School of Information Science and Technology, the University of Tokyo

Abstract

This article presents a present status and future view of technology on the remote operation system. The requirements for the system become very complex and a solution by information technology is inevitable. Especially, safety and security are two big requirements. Duplication of a communication line is requested, however it is too expensive. Therefore, a new type of duplication is needed. This way leads to the use of Internet Protocol and Web service.

Key Words :remote operation, IP, web service, VPN, XML

1. はじめに

20 世紀はフォードの生産方式で幕を開けた．これは，T 型と呼ばれる規格品の大量生産である．同じものを全ての住民に届けるという発想だった．しかし，21 世紀は，個人の趣向を尊重する時代である．製造業でいえば受注生産であり，少量多品種の生産である[1]．

同じことが環境施設にも当てはまる．これまでの百年は均質なサービスをできるだけ多くの住民に提供することが公のサービスであった．しかし，技術の発達は土地ごとの事情に応じたサービス，個々の住民に応じたサービスを可能にし始めている．このため，環境施設の運用も多様化し始めている．

この多様化を支える技術の一つが遠隔監視技術である[2]．この技術の登場により，環境設備の無人運転やメーカによる遠方からの保守，危険地帯での環境活動などが可能となる．もっとも技術の進歩は裏腹である．良い面と悪い面がある．遠隔監視技術の登場は，これまで考慮されてこなかった問題を浮上させつつあることも認めざるをえない．ここでは，この遠隔監視技術の動向を紹介するとともに，浮上した問題点およびその対策について解説する．

* 〒 113–8656　東京都文京区本郷 7–3–1
TEL: 03–5841–7666　　FAX: 03–5841–7674
E-mail: shin@axis.t.u-tokyo.ac.jp

2. 遠隔監視

監視という業務を考えると，測定と表示という二つの機能に分かれる（**Fig. 1**）．測定はセンサが中心の機能であり，表示は人が中心となる機能である．計測の歴史の初期は，その二つが同一の場にあったが，現在は監視室と呼ばれる場所に施設の情報が集約されている．つまり，監視室という言葉が使われ始めたときから遠隔監視は始まっていた．これと近年の遠隔監視との違いは，事業所内か事業所を越えるかにある．ここでは，事業所内のデータ伝送をテレメータリングとよび，事業所を越えたものを遠隔監視とよぼう．最近の遠隔監視システムとして想定されているものは，一つの事業所を無人化し，その無人化された事業所の情報を別の事業所で監視するものである．

情報通信技術から見れば通信路が構成できれば近くても遠くても同じであるが，組織としてみると違う．違いの最たるものは，異常時に職員が駆けつけるまでにかかる時間である．もう一つの違いは，事業所を跨ぐことによる通信路のセキュリティの問題である．

しかし，これらの問題は遠隔としたから顕在化したの

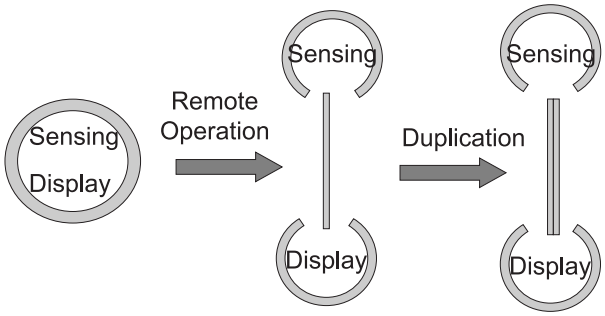

Fig. 1 Remote Operation and Duplication.

であり，テレメータリングでも問題のはずである．つまり，事業所内での遠隔監視は一つの施設内で行われてきたので，異常時の対応やセキュリティに十分な配慮をしなくても許されてきたということが実態ではないかと推測する．異常時には誰かが対応するし，施設内の人間が遠隔監視システムに悪さはしないという考え方である．

この考え方は，事業所を跨ぐ遠隔監視では通用しない．実は，テレメータリングでも通用しない．事業所を跨ぐ遠隔監視をする，しないに関わらず，全ての遠隔監視システムの異常時の対応とセキュリティを見直すべきである．

それでは，どのような対策が必要か考えてみよう．まず，指揮系統のリスクマネージメントを整えるべきである．誰が異常時の対応に責任を持つかをはっきりさせる必要がある．もちろん，設備の長が責任者である．しかし，その長が出張や不在の時の責任者は誰か，その者が代理をしていることを設備内で周知されているかとなると怪しくなる．そして，その代理が急病や怪我をしたときの対処となると，明文化されていない事業所が大半かもしれない．

常に代替をおくこと．これが，リスクマネージメントである．そのマネージメント無しで，遠隔監視システムの異常時の挙動を論じても意味がない．賢い方は，最後には代替を置けなくなることに気がつくだろう．判断できる責任者がいない状態，それが無人施設である．つまり，遠隔監視システムの問題点の一つは情報技術の問題ではなく，管理技術の問題である．これは緊急に見直す必要がある．

話を情報技術に戻すと，遠隔監視システムで異常が起きた場合の通知，代替手段が焦点となる．多くの監視システムでは，この通知に電子メールを利用する．たとえば，携帯電話へのメールを利用すれば，担当者に自由度が生まれる．もっとも，携帯電話のメールは遅延するとか，圏外にいたら届かないとか，携帯電話システムがダウンしたらどうするとか，問題点が挙がってくる[3]．

これはリスクマネージメントの問題である．最初の課題は，メールを送信して一定時間の内に返答がなければどうするかである．そのときは，代理の代理に連絡するということが一つの手段である．別な手段としては，メールが駄目なら電話するである．少なくとも，このような機能が搭載されていない遠隔監視システムは不完全な商品である．

第二の課題は，代理の代理にも連絡がつかない．または，電話しても出ない場合にはどうするかである．その対処シナリオはメーカではなく，遠隔監視システムを運用する側が作成しなければならない．つまり，無人設備で異常がおき，遠隔監視ができない場合という最悪ケースにおける無人設備側の対応である．被害の拡大を食い止めるには，どのようにすべきかである．

現在，ダムの監視制御用システムで採用されているFL-net は自律分散ネットワークと呼ばれる ADS-net をベースとするものである．両者とも，2004年春にISO15745 として国際標準化された[4]．このネットワークを紹介するとき，「分散」の方は見れば分かるので，「自律」の定義が問題となる．この標準化を進めてきた FA オープン推進協議会では，自律をネットワークから切断されても生存する機能と定義した．遠隔監視システムの良否は，この自律性を持つか否かで判断すべきである．つまり，ネットワークが正常に稼動しているときの性能より，切断されたときの性能を論じるべきである．多くの遠隔監視システムは，その順序が逆転している．この逆転は，遠隔監視システムのコストを膨大にしてしまう．その問題と対策を次節で考えてみよう．

3. 二重化

測定と監視を分断すると，両者の通信路の脆弱性に眼が行く．リスクマネージメントが出来てないシステムの場合，切断はあってはならない．つまり，「自律」していない無人施設の維持を考えるとネットワークは切断されてはいけない．それで，二重化ということになる．もっとも，監視には複数のセンサシステムが関わっている．そのため，全ての通信路を二重化するという結論に至る．しかし，これではコストは膨大となってしまう．この信頼性とコストのギャップを埋めるものが情報技術である．たとえば，三つの通信路があり，それを全て二重化すると **Fig. 2** に示すように六つの通信路が必要になる．

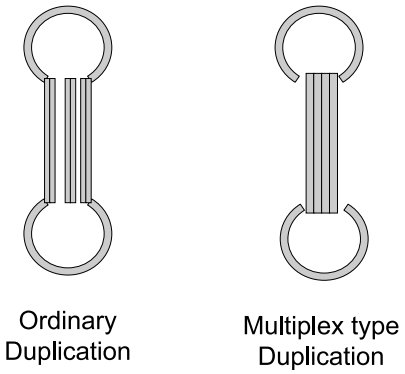

Fig. 2　Two types of duplication.

一つの通信路がダウンする確率を 0.1 とすると，二重化によりダウンする確率は 0.01（＝0.1 × 0.1）まで減少する．しかし，同じ信頼性は四つの通信路でも確保できる．ただし，予備の 1 本は他の三本の通信路のどれとも代替できなくてはならない．そして，一本の通信路がダウンしたら，直ちに修復できるという前提が必要である．このように通信路を多用途化することで，信頼性の向上とコスト削減という一見，背反する問題を解決できる．これが情報技術の活用である．

以上の例の鍵は多用途化である．どの通信路も他の通信路の代替ができるなら，通信路が増えるほど予備を置くコストは問題とならなくなる．もちろん，通信路だけの問題ではなく，全ての予備問題に通じる．電気屋，機械屋，通信屋と分かれていれば，それぞれに予備が必要だが，皆が全てを扱えれば，予備は一人で OK である．これは専用から汎用という流れである．人材では難しいかもしれないが，GHz で動作するマイコンに Mbps で情報交換する通信路，GB の要領を飲み込む記憶装置に支えられた情報技術には朝飯前の仕事である．この流れに専用線中心の環境施設における遠隔監視も大きな影響を受けている．その流れにそって先ほどの冗長化を見直すと，汎用線を使った遠隔監視という形態にたどり着く．

先に述べた冗長化は通信路の多目的化であり，通信の世界では多重化と呼ばれている．時分割や周波数分割など多様なものがあるが，現在は IP（Internet Protocol）に集約されつつある[5]．つまり，IP 化である．IP に対応することで，伝送線，接続装置，ミドルウェアなどが汎用品となり，大幅なコストダウンが可能である．もっとも，IP は大容量通信基盤を前提とした通信方式であり，十分な容量を確保できないと能力を発揮できない．もっとも，家庭でも ADSL で数十 Mbps，光ファイバーで 100 Mbps の容量で通信可能である．戸外では携帯電話を使って数百 Kbps から数 Mbps で通信できるインフラが整っている．そこで，専用線さえも IP に基づいた通信が行われ始めている．

4. インターネット化

このように考えると，遠隔監視の IP 化とインターネット利用が視野に入ってくる．もっとも，公共設備では信頼性とセキュリティの問題があるので，IP 化とインターネット化が受け入れ難いと考える方も多い．しかし，数百億円にも上る電子決済がインターネット上で行われていることを考えると，これらの技術の現状が正確に認識されていないとも思える．そこで，信頼性とセキュリティに関する現状に少し触れよう．

まず，インターネットの原点は米国の軍事技術である ARPAnet であり，従来の技術では確保できない信頼性を維持する目的で開発された．基本は，全てのノードが他のノードの通信を中継できることと，複数の中継先を持つことである（**Fig. 3**）．つまり，常に選択肢を持つという自律分散原理に通じる構成である．この構成により，一つの通信路やノードが原子爆弾などによって破壊されても，別ルートを使って通信を確保する仕組みである．

そうすると，中継器が大事であることが分かる．これは，ルータと呼ばれるものである．通信路にも信頼性の高いものと，そうでないものがある．常に信頼性の高い通信路を割り当てるようにルータを設定すれば，単なる専用線の二重化より信頼性の高い通信が可能である．

次にセキュリティである．専用プロトコルでなく，IP ならば誰でもが簡単に接続できる．しかし，通信内容を暗号化すれば盗み見することはできない．この仕組みを総合的に提供する枠組みが VPN（Virtual Private Network）である[6]．VPN は汎用ネットワーク上に専用のネットワークを構築するものである．汎用ネットワーク上で暗号化された通信路のほうが，専用線上で暗号化されていない通信路よりセキュリティは高いとも考えられる．遠

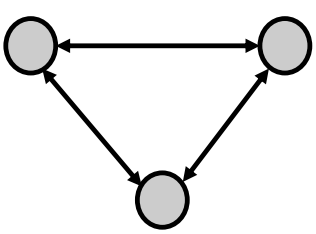

Fig. 3　ARPAnet.

隔化でセキュリティの問題に気がついたのなら，所内のテレメータリングのセキュリティにも目を配るべきである．そこにも，VPN が提供する各種の情報技術が有効である．

以上のように，信頼性の確保，セキュリティの確保の技術が高度化してきており，現在のテレメータリングで使われている旧式の通信路より安全になりつつある．その意味で，遠隔監視システムのインターネット化は急速に進むと思われる．

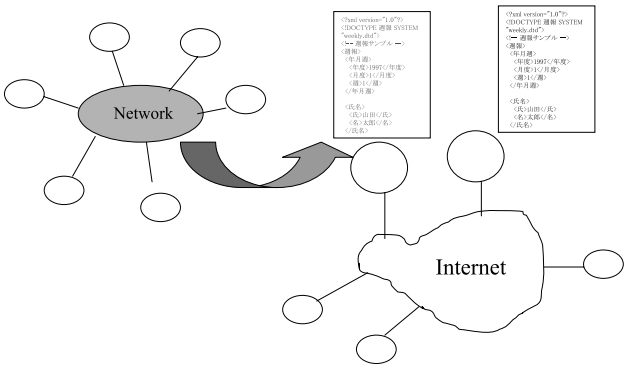

Fig. 4 To Web Service.

5. Web サービス化

VPN はセキュリティの切り札と見られてきたが，最近は悪意を持った攻撃も視野にいれなければいけない．特に，コンピュータウィルスによる攻撃は遠隔監視システム乗っ取りという事態まで発展する可能性がある．ウィルスはメールの添付ファイルで広まるだけでなく，ポートスキャンとバッファオーバーフローを組み合わせることで侵入する手段が顕在化している．

IPでは，サービスごとに予めポート番号を決めている．たとえば，ファイル交換の FTP は 21 番，ホームページ閲覧の HTTP は 80 番，メールを送る SMTP は 25 番，メールを受ける POP3 は 110 番という具合である．ポートスキャンは，このポートを順番にアクセスして，使用可能なポートを見つけることである．そして，そのポートに大量のデータを送信して飽和させ，その隙をついて計算機に侵入する仕組みがバッファオーバーフローである．特に問題となるのは Active X や CORBA などの RPC（Remote Procedure Call）なるサービスである．これは，外部から計算機内のソフトウェアを操作する仕組みであり，現在のネットワークサービスには不可欠の機能である．しかし，この機能を悪用して他人の計算機に不正に侵入できれば，後は思いのままである．

この侵入を避けるために，ファイヤーウォールと呼ばれる守りを設けてHTTPのポート以外を閉じてしまう対策が取られてきている．しかし，閉じたままではネットワークサービスが使えない．そこで，**Fig. 4** に示すような RPC を HTTP で行う Web サービス化が進んでいる．ここで交換されるデータは XML（eXtensive Markup Language）である．これはインターネットのホームページ記述に使われるデータ名とデータ内容を対に表記する HTML を拡張した記述であり，XML スキーマーなどを使ってデータ名を好きに定義できる点が特徴である．

データが 2 進数ではなく，XML のように文字であれば悪意のあるメッセージを検出しやすい．また，Active X などのように計算機内のサービスを直接駆動するのではなく，文字を理解して，それに基づいて駆動するというプロセスが介在することによりバッファオーバーフローによる乗っ取りを回避しやすい．しかも，Web サービスを使うことにより，Windows のパソコンも非 Windows の計算機も連携できることが重要である．このことは，プラットフォーム（OS，通信方式，開発言語）に依存しない計算機連携を提供するものであり，複数のプラットフォーム，新旧のシステム，多種類の端末が混在する各種設備に，正にジャストフィットする技術である．このような理由から，遠隔監視も Web サービス化が急速に進むものと見ている[7]．

XML はデータ毎にセキュリティや暗号化を設定できる．しかも会社の情報系であるイントラネットで文書標準となっているHTML形式とマイクロソフト社のオフィス形式とを統合することもできる．これは，同社の製品であるオフィス 2003 が XML 対応になったためである．

遠隔監視が測定データの監視だけでなく，そのデータに基づいた報告や引継ぎ，当直情報との連携などの合理化まで視野にいれるのならば XML が連携のキーワードである．我々は，製造業 XML 推進協議会を 2002 年に設置し，XML を用いた設備の連携と文書の連携の技術開発に着手している[8]．それだけでなく，XML に関わる各種団体と連携し，XML を製造業で活かす枠組み作りを行っている．複数のデータベース，複数のネットワーク，複数のシステムを手軽に糊付けできる仕組みのキーワードが XML である．

6. グローバル化

さて, インターネット上で遠隔監視システムを作ると, 測定現場と監視所との二点を結ぶ専用線以上の世界が開ける．具体的には，測定値は誰でも読むことができ，監視所は何処でも見ることができる. つまり, インターネットは公開が原則であり，非公開とするには追加の技術が必要である．追加の技術とは，これまで紹介したファイヤーウォール，VPN，暗号化などの技術である．つまり，公開するほうが簡単で，非公開には追加投資が必要である．

このような基本的な特性に目を向けると，遠隔監視業務が違ったものに見えてくる．それは，特定の施設の状態監視だったシステムが，もっと多種類の，もっと広範囲な情報と統合した監視業務が行える（**Fig. 5**）．浄水所や処理場内だけの情報で監視業務をするのではなく，天気予報，近くの降雨状況，住民の様子，西方の天気，ダムの貯水量，工場の稼働状況などを見ながら総合的な判断ができるということである．しかも，それらの測定点が公開されていれば，追加投資無しで可能である．正に世界中を照らしながら，自らの進む方向を決められる環境を提供するものが開かれた監視システムである．

逆も，また真である．測定場所の情報を公開の場に簡単に掲示することも容易である．ゴミ処理場の状況，配水所の情報，ポンプ場の状況を住民を含む不特定多数の方々に見てもらうことができる．公共施設は情報公開法の施行にともない，基本は情報公開，特に理由のあるものだけを秘匿することになっている．この趣旨にもっとも合致しているものが，インターネットを用いた監視システムである．

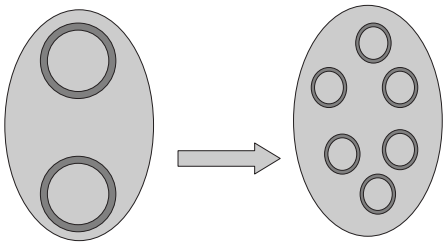

Fig. 5　Globalization.

7. まとめ

以上，見てきたように，情報技術は夢を現実にかえつつある．良いことも，悪いことも何でも可能な状況になりつつある．だから，使う側が問われている．「これで何をしたいのか」，「本当は何をしたいのか」を見つめなおすことが，情報技術活用の一番の早道である．遠隔監視のシステム設計の前に，環境設備のリスクマネージメントとセキュリティ対策を見つめなおそう．所内に侵入した悪者に乗っ取られない仕組みはあるのか，所内の誰かが裏切っても大丈夫なのか，所内の責任者や担当者が急病で倒れても監視業務が続けられるのかを問い直そう．その問いに答えられれば，遠隔監視を始め，設備を維持管理している方々の夢を情報技術は適えてくれるはずである．

［参考文献］

1) 新誠一：信頼性の新たな動き－保障から補償へ―，日本信頼性学会誌，vol. 26, no. 8, pp. 898–905（2004）
2) 新誠一：インターネット応用計測制御システム，水道協会雑誌，vol. 20, no. 10, pp. 2–8（2001）
3) 新誠一：ユビキタス計装再考，計測技術，vol. 31, no. 8, pp. 18–22（2003）
4) 新誠一：ADS-net と国際標準化活動，計測と制御，vol. 39, no. 3, pp. 209–215（2000）
5) 新誠一：オール IP 化の世界，電気協会報，no. 944, pp. 28–31（2003）
6) http://www.atmarkit.co.jp/fsecurity/special/22fivemin/fivemin00.html
7) 新誠一：XML が製造ビジネスを変える！，Plant Engineer, vol. 35, no. 9, pp. 14–18（2003）
8) http://www.mstc.or.jp/mfgx/