

高度情報通信危機管理研究施設の構築 (1)KVMスイッチを核としたオペレーション室の設計と実装

大野 浩之* 松本 文子* 山崎 靖博†

本報は、全部で5つの報文からなる「高度情報通信危機管理研究施設の構築」の第1報にあたる。一連の報告は、独立行政法人通信総合研究所情報通信部門非常時通信グループが2001年度から遂行中の「情報通信危機管理研究」の成果の一つである。「高度情報通信危機管理研究施設」についての研究報告になっており、第1報である本報告では、KVMスイッチを核としたオペレーション室(SD室)の設計と実装について述べている。SD室は、情報通信や拡張現実感の分野で培われた技術を採用入れた、危機管理への適用を主眼においた施設で、危機管理のための機器のオペレーションと、危機管理に伴う意志決定を支援する機能を持つが、本報告では、パーソナルコンピュータ用に製造販売されているKVMスイッチのうち、大規模用途向けの機種種の活用が高度情報通信危機管理に有用であることを報告する。

Constructing of the Integrated Telecommunication Crisis Management Research Facility

Part1: A design and implementation of the KVM switch centric operation room

Hiroyuki Ohno † Fumiko Matsumoto‡ Yasuhiro Yamazaki§

Emergency Communications Group, Communications Research Laboratory (ECG/CRL) has started the research on Info-communication Crisis Management in 2001 and has been developing the facility for the Integrated Telecommunication Crisis Management (ITCM) since then. This thesis is a part 1 of 5 series of report on the design and implementation of ITCM facility and especially describes the importance of KVM switch centric operation center. Note that the operation facility has named SD room and it contains two major roles. One is to support operation for many servers and their related equipment for crisis management, the other is to support the decision making for crisis management

1 はじめに

1.1 高度情報通信危機管理研究施設

独立行政法人通信総合研究所情報通信部門非常時通信グループでは、危機管理分野とインターネット

技術を中心とする情報通信関連分野の境界領域に注目し、この境界領域における研究を「情報通信危機管理研究」と名付けて2001年度から研究を続けている [1].

情報通信危機管理研究においては、「インターネットの危機管理 (crisis management for the internet)」と「インターネットで危機管理 (crisis management by management)」の二つをサブテーマが存在する。前者では、インターネットなどの情報通信システム自身の危機管理をどうやって実現するかを議論して

*独立行政法人 通信総合研究所 情報通信部門 非常時通信グループ

†KDDI 株式会社 ソリューション技術 1部 1グループ

‡Emergency Communications Group, Communications Research Laboratory, Japan

§Engineering Section 1, Solutions Design Department, KDDI CORPORATION

おり、後者では、インターネットなどの情報通信システムを駆使し、大規模災害やテロリズムなどの非常事態が発生した場合の危機管理を通信の立場から支援する体制をどうすれば構築できるかを議論している。

前者は、「情報セキュリティ(Information Security)」「コンピュータシステムセキュリティ(Computer System Security)」などと呼ばれている研究分野と近く、後者は、「非常時通信(Emergency Communication)」あるいは「災害復旧通信(Telecommunication for Disaster Relief)」と呼ばれている研究分野と近いが、これらの研究分野では、必ずしも危機管理あるいは安全保障という視点からの議論が明確にされているわけではない。これに対し、著者らは、(1)情報通信システムと危機管理の双方の重要性を強く意識した研究者集団を組織し、(2)日頃から最新情報の蓄積と分析および適切なシステムの研究開発を行い、万一の事態に際しては、適切な応策を立案しうるだけの実績を備えた研究体制が必要であると考えた。幸い、平成12年度公共事業等予備費、平成13年度補正予算などの予算を得られたため「情報通信危機管理研究施設」の整備を続けており、2002年度末の段階で以下の機能を保持するに至った。そして、2003年度には、これらの施設を統合的に運用する体制を整え「高度情報通信危機管理研究施設」に発展させる方針である。

- 不正アクセス再現実験装置や脆弱性データベースを中心とした「ネットワークセキュリティ研究施設」
- 関東地区と関西地区に分散配置した大型サーバを中心とした「非常時通信用高信頼性ネットワーク検証実験施設」
- 大型ディスプレイや拡張現実感等を用いたオペレータ支援環境を有する「情報通信危機管理オペレーション実験施設」
- 電子機器から漏洩する電磁波や侵入する電磁波の脅威を調査する実験システムを有する「電磁波セキュリティ研究施設」

1.2 一連の報告の概要

「高度情報通信危機管理研究施設の構築」は、全部で5つの報告の報告からなり、その概要は下記のとおりである。

第1報 オペレーション室の設計と実装(本報)

第2報 オペレーション室を中心に、本研究施設内外の設備を効率的に連携させる機構の設計と実装(仮題)

第3報 本研究施設を活用した実践の高度情報通信危機管理演習訓練環境の整備と運用(仮題)

第4報 本研究施設全体の総括と評価(仮題)

第5報 最新の状況報告と今後の展開(仮題)

本報告は第1報で、KVMスイッチを活用したオペレーション室の設計と実装について述べる。なお、同施設は歴史的経緯でSD室と呼ばれており、本報告でもそれに従う。

2 情報通信危機管理オペレーション実験施設(SD室)の設計と実装

2.1 SD室に必要な機能

SD室は、情報通信危機管理研究施設の運用(オペレーション)の中核をなす施設である。本施設施工以前は、階段教室状の座席と120インチスクリーン3面を擁する、床面積約300m²の70名ほどを収容可能な会議室であったが、SD室を下記のように実装するにあたり大幅に改修した。改修後の外観を図1に示す。

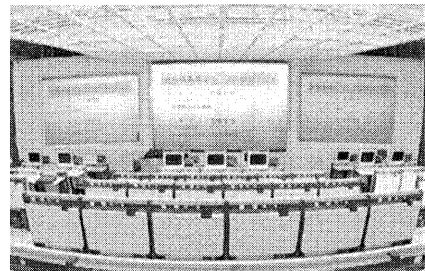


図1: SD室の外観

SD室は、情報通信危機管理のための「機材運用拠点」という性格と、危機管理に伴う「意志決定のための会議室」という性格をあわせ持っている¹。

¹ 通信総合研究所は研究組織であって危機管理対応組織ではないので、危機管理支援が可能な環境が整っていても、実際の事案発生時に危機管理を実施することは現状ではできない

2.2 大型ディスプレイを用いた映像情報表示機能

SD室の前面(正面)の3面の大型ディスプレイと、これを活用する機材群を導入し、下記を実現した。

1. 従来の120インチ3面をあらため、200インチ1面、150インチ2面という構成にした。
2. 200インチの画面は、100インチ×4台あるいは50インチ×16台の独立したディスプレイとしても利用できる。150インチディスプレイは、分割利用はできない。
3. ただし、主に予算上の制限から、画像の解像度は、200インチの画面であってもXGA相当(1024×768)相当となった。それ以上の解像度の場合、コンバータがXGA相当に変換するため、画質が劣化してしまう。
4. 表示できる映像は、(1)階段状座席のPCの映像(後述)、(2)情報通信危機管理研究に参画している各種サーバのコンソール、(3)VHSビデオをはじめとする各種ビデオ機器、(4)テレビ映像(地上波・衛星波)放送などがある。

2.3 協調作業支援機能

既に述べたように、SD室の利用者として想定しているのは、危機管理用機材を運用するオペレータか、意志決定に携わる人々である。どちらであっても、SD室の利用者が協調して作業するため、下記を用意した。

1. 従来の階段状の座席には、特段の設備がなかったが、全ての座席に下記を用意しノートパソコン等の利用を容易にした。
 - 電源(AC100V)
 - 有線LAN(100BASE-Tイーサネット)無線LANのアクセスポイントも別途配備した。
 - VGA出力接続口(次項)
2. プレゼンテーション時に、自席から移動することなくプレゼンテーションが実施できるよう、座席にはノートパソコン等からのVGA出力を取り込むためのコネクタを用意し、最大8ユーザの画面を前面のディスプレイに同時に表示できるようにした。この機能は、迅速な情報の交換や意志決定に寄与すると考えられる。

3. 前二列(7席/列)は、上記に加えてキーボード、マウス、液晶ディスプレイ(以下、KVM)を各座席に一組ずつ別途用意した。各座席のKVMは、特定のパソコン等に接続されているのではなくKVMスイッチ群に接続されている。KVMスイッチに関しては、次項で詳しく述べる。

階段状座席の外観を図2に示す。

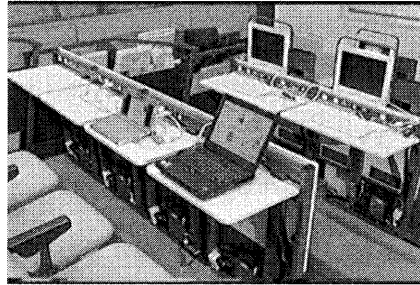


図2: 階段状座席近傍

2.4 KVMスイッチの活用

情報通信危機管理にかかわるサーバ類やパソコンの種類は多岐に及び数も多く、総台数は200台を超える。これらの機材を10名に満たない操作者で効率よく管理しなければならない。

これらのパソコン等のうち、特にサーバ類の多くは、オペレータが常にその画面を監視したり、なんらかの操作を施し続ける必要はない。正常に立ち上がってしまえば、ネットワーク経由で自動的に管理できるしかけが用意できているのが普通だからである。加えて、最近のMacintoshを含むUNIX系OSを搭載する機材であれば、sshのような遠隔シェルが有効に使えるし、Windows系OSであってもVNCのような遠隔操作ソフトウェアが開発されているので、遠隔地のサーバに動作変更を施すような操作であってもそのほとんどはネットワーク経由で問題なく処理できる。しかし、システムの起動に失敗した場合や、OSがクラッシュしてハングアップしてしまったり、PCがBIOSモードになってしまった場合、あるいはPCのBIOS設定のようにOSを停止させなければ対処できない操作は、もはやネットワーク経由では対応できない。

このため、PCアーキテクチャではない多くのサーバ類には、以前からシリアルコンソール機能が備わっ

ていた。最近では PC アーキテクチャであってもシリアルコンソールをサポートしている場合がある。この場合、シリアル回線 (RS-232C) を介して起動前設定 (PC で言えば BIOS 設定) を実施できるので、ターミナルサーバなどを配して、ネットワーク経由での起動前設定を実現してきた。

しかし、PC アーキテクチャの機材、いわゆるパソコンでは、シリアルコンソール機能がないため遠隔からの BIOS 設定はできない。また、シリアルコンソールがある機材であっても、シリアルコンソールからはウィンドウシステムにはアクセスできないため、ひとたびウィンドウシステムが立ち上がってしまうと、シリアルコンソールからはシステムの制御が事実上できなくなり、ネットワーク経由でウィンドウシステムにアクセスしなければならないなど、作業が複雑になる。

この問題への解決策として、CPU 切替器あるいは KVM スイッチと呼ばれる機材 (以下では KVM スイッチと表記) の有効利用がある。KVM スイッチは 1990 年代中ごろから盛んに利用されるようになってきた機材で、当初は、単一のキーボード (K)、ビデオディスプレイ (V)、マウス (M) で 4 台程度 PC を切替えて利用するための単純な切替器であったが、この数年間に以下の発展があった。

- 接続可能な PC 等の数の上限が増加した。カスケード接続すれば、1000 台を超える PC が接続可能になった。
- 多数の PC 等を複数のオペレータが協調して操作できるようになった。
- OSD (on screen display) 機能が導入され、PC 等の切替えが画面上で実施できるようになった。
- 当初は KVM それぞれに 1 本ずつケーブルが必要であったが、Category 5 ケーブル 1 本で KVM 信号を送れるようになった。
- 従来、スイッチと PC 等の距離は 10 数 m が限界であったが、遠隔地の PC に対しても、光ファイバによる KVM 信号の伝送あるいは、KVM over IP といったプロトコルでアクセス可能になった。

今回、SD 室でも KVM スイッチを活用することにした。KVM スイッチは多種多様な機種が流通しているが、今回採用した機種には PS/2 規格のキーボードおよびマウスを持つパソコン等の機材を最大

64 台まで収容でき、カスケード接続によって台数を増やせる。また、これらを最大 16 人のユーザが協同的にあるいは排他的に利用できる。KVM スイッチ群の概略を図 3 に示す。

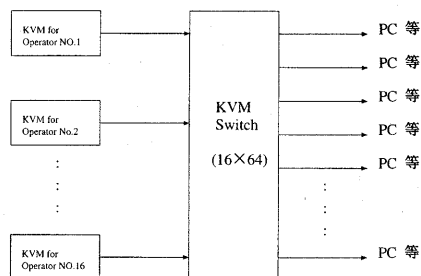


図 3: KVM スイッチの周辺の構成 (1)

この KVM スイッチの特徴を整理すると下記になる。

- KVM スイッチ単体で 64 台までの PS/2 規格のパソコン等を収容できる。カスケード接続で 1000 台以上のパソコン等を収容可能。実際に、不正アクセス再現実験系の約 130 台の PC 等は 2 段カスケードのあと、図 3 の KVM スイッチに収容されている。
- 16 人のユーザは、別々の PC 等を利用できるだけでなく、同じ PC 等に複数のユーザが接続することも可能なので、共同作業や作業状況を見守るといった対応が可能。
- KVM スイッチと PC 等の間は、Category 6 の UTP ケーブルで接続でき、距離も 200m まで延長できる (現実的には、アナログ伝送のビデオの品質劣化の問題があるので 100m 程度が限界)。
- 100m を越え 1000m 以下のケースでは、光ファイバを用いて KVM 信号を伝送する手段が用意されている。
- 関東と関西のように離れた場所にある PC 等については、KVM 信号をネットワーク経由で送る手段が用意されている (KVM over IP)。

最後の KVM over IP は、ビデオ信号を含む KVM 信号をキャプチャして TCP/IP で送る方式で、現時点では以下のような問題があるが、本質的な問題ではない。

- プロトコルの標準化が行われていないので、今後の動向が不透明(メーカー間の互換性はないし、クライアントソフトウェアが特定の OS の特定のブラウザ用しか存在しないなどの問題が生じている)
- 回線速度が遅いと、画質や色数を落とすなどしてなんとか対応しようとするが、それでも最低でも数 100kbps の帯域が必要(仕様上では、画面のキャプチャをモノクロにするなどして情報量を減らして、V.90 のアナログモデムでも対応できる。PC 等の画面が、テキスト画面などであれば問題ないが GUI の場合、背景色を慎重に選ぶなどしないとイケない)
- フルカラー(24bit)や、大画面(1280x1024 を越えるサイズ)に対応できない

しかし、昨今では ADSL などの普及の結果、数 100kbps 程度の速度であれば、ssh や SSL や socks などの技術と併用することで、事実上の専用線と同様に使える回線を安価かつ安全に取得できるので、帯域の問題はあまり問題にならない場面が増えている。モバイル環境で数 100kbps の通信が普通になれば、移動先からも PC 等のハングアップ対応が可能になるので、遠隔地の PC 等の BIOS 設定を変更したり、ハングアップしてしまった際の強制的再起動に対応できる数少ない手段として注目に値する。

ところで、SD 室には、大型ディスプレイの画面分割の仕方や入力信号を選択する作業をする制御卓(図 5)があり、階段状の座席にのどの座席からの VGA 信号を大型ディスプレイのどの場所に表示するかといった操作を実施できる。図 3 では、KVM スイッチと大型ディスプレイ制御卓の関係を省略してあるが、その関係を示すと図 4 のようになる。すなわち、KVM スイッチの利用者(オペレータ)の画面は、制御卓のビデオスイッチに送られ、大型ディスプレイに随時表示できる。これにより、KVM スイッチの利用者の操作画面を SD 室の利用者全員で共有することが可能である。

KVM スイッチの利用者は、KVM スイッチにあらかじめ決められたシーケンスの文字列を送って、KVM スイッチを切替えて、操作する PC 等を選択するが、この切替えは制御卓側から制御できる方が効率的な場合もある。すなわち、KVM スイッチ利用者が、操作する PC 等を捜し出し接続する作業を省略できるからである。このためのもっとも簡単な方法は、KVM スイッチの制御ポートにコマンドを

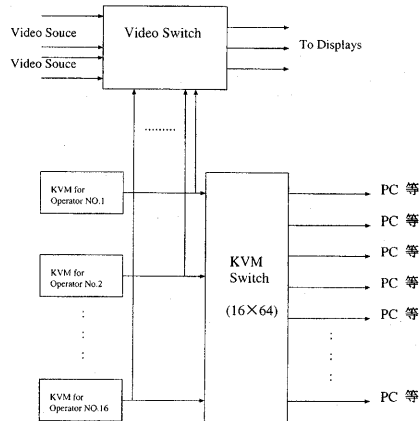


図 4: KVM スイッチとビデオ制御卓の関係



図 5: コンソール卓の外観

送って KVM スイッチを操作することである(図 6)。しかし、現在利用している KVM スイッチにはこの機能はない。

改善の策が、図 7 と図 8 である。図 7 は、パソコン教室用のインストラクタモジュールと学生用モジュールを使う方法である。あるオペレータの操作する PC 等を他のオペレータが強制的に割り当てたり変更する操作を実現する場合、もっとも近い環境を提供しているのが、パソコン教室用の機材群である。すなわち、インストラクターは、学生のパソコンに何が表示されるかを変更することができ、たとえばインストラクターの画面を見せたり、他の学生の画面を見せたりできる。また、インストラクターは学生の操作を支援できる。インストラクターと学生の間をオペレータを統括する者とオペレータと考えれば、パソコン教室用の機材が利用可能であるこ

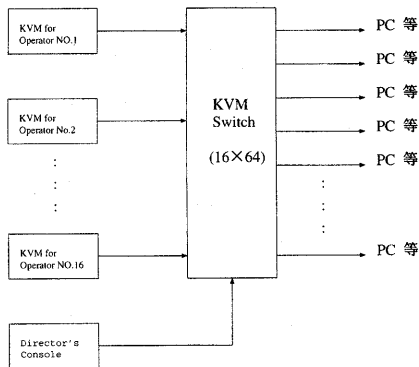


図 6: KVM スイッチの周辺の構成 (2)

とが予想できる。図 8 は、これを少し簡便にした方式で、パソコン教室用機材に代えて、2 台目の KVM スイッチを用いる。オペレータを統括する者はこの KVM スイッチを介して、オペレータの操作を支援する。これら二つの方式は、いずれも試作とを評価終え、前者が SD 室に導入されることになった。

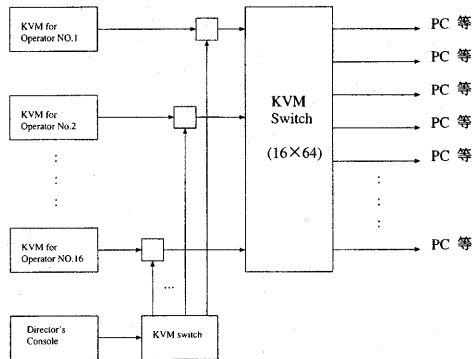


図 8: KVM スイッチの周辺の構成 (4)

であることがわかってきた。そのためには、SD 室が単にその機能があるがままに提供するだけでなく、それぞれの時点で、各担当者にどのような操作や処理が求められているかを、各担当者に伝えるしかけが必要になってきている。これについては第 2 報で報告する。

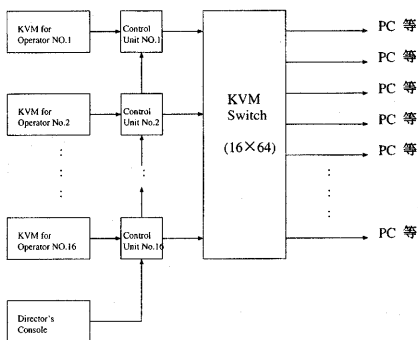


図 7: KVM スイッチの周辺の構成 (3)

3 評価と今後の展開

現在、SD 室の KVM まわりは実戦的な試験運転を繰り返している。設計どおりの動作をしているが、前述のように改定したい点が見出されているのも事実である。

検討の結果、緊急対応時に SD 室がその能力を発揮するには、緊急対応スタッフがいかに適切に役割りを分担をし、自分の分担を的確にこなすかが重要

4 おわりに

本報告では、通信総合研究所に設置した高度情報通信危機管理研究施設のうち、SD 室という名称の情報通信危機管理オペレーション実験施設の設計と実装について述べた。現状でも、情報通信危機管理に大きな威力を発揮すると定性的に評価しているが、今後は定量的な評価を行うとともに、シナリオシステムを導入し、オペレーション機能の一層の充実を進めており、その結果は第 2 報以降で報告する。

参考文献

- [1] 戸村 哲, 三輪 信介, 大野 浩之, “我が国政府におけるネットワークセキュリティ確立への取り組み”, 情報処理学会, 情報処理, Vol.42, No.12, Dec. 2001.
- [2] 大野 浩之, 武智 洋, 永島 秀己, “インターネットの脅威に対抗しうる脆弱性データベースと検証システムの構築”, 情報処理学会, DSM シンポジウム 2001, Feb. 2001.
- [3] 大野 浩之, 松本 文子, 山崎 靖博, “高度情報通信危機管理研究施設の設計と実装”, 情報処理学会, DPS/CSEC 合同研究会, Feb. 2003.