高度情報通信危機管理研究施設の構築
(3) 危機管理対応支援シナリオシステムの実装と運用

大野 浩之* 馬場俊輔† 山崎 靖博‡ 松本 文子*

本報は「高度情報通信危機管理研究施設の構築」の第 3 報である.「高度情報通信危機管理研究施設」は，大規模不正アクセス等の事案 (incident) に対処する方法を見出す研究や大規模災害時の情報交換を支援する方法の研究といった「情報通信危機管理研究」を支援するための施設で，独立行政法人通信総合研究所が 2001 年度から導入を開始し，情報通信部門非常時通信グループが中心になって整備を進めてきた．高度情報通信危機管理研究施設には，危機管理時のオペレーション及び意思決定支援のありかたを研究するための，専用オペレーション室がある．この部屋をわれわれは SD 室と呼んでおり，第 1 報および 2 報でも報告した．本報告では，SD 室内の研究施設相互接続システムを利用し，今回新たに構築した，情報通信危機管理オペレーションを支援するための，シナリオシステムの設計と実装について報告する．

Constructing of the Integrated Telecommunication Crisis Management Research Facility
Part3: A design of the scenario system to assist crisis management operations

Hiroyuki Ohno § Syunsuke Baba¶ Yasuhiro Yamazaki‖
Fumiko Matsumoto§

This is the part 3 of the series of reports on the integrated telecommunication crisis management research facility. This research facility has been constructing and expanding in the Communications Research Laboratory Japan (CRL) since 2001 under the leadership of the Emergency Communications Group in the laboratory. In this facility, we have been developing and researching on the incident responding mechanism against various threats on the internet and the special communication supporting systems in case of an emergency such as natural disasters like huge earthquakes. In this facility, there is a special operation room prepared for both type of crisis management operations and decision making assistance. We call the special room the SD room. In this report, “the scenario system” which has been developing for assisting crisis management operation in the SD room, has been discussed.

*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
†横河電機株式会社 技術開発本部 セキュリティプロジェクトセンター
‡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
¶Security Project Department, Corporate Research and Development Headquarters, Yokogawa Electric Corporation
‖Engineering Section 1, Solutions Design Department, KDDI CORPORATION

1　はじめに

独立行政法人通信総合研究所が 2001 年度から整備を続けている高度情報通信危機管理研究施設では，われわれが SD 室と呼ぶ「情報通信危機管理オペレーション室」の整備を通じて情報通信危機管理に適したオペレーションセンターのありかたを探っている．SD 室では，SD 室と同一建物内に設置した情報通信危機管理研究用機器の操作を全て実施できるだけでなく，遠隔地にある他の関連研究施設の機器を SD 室から操作したり，あるいは関連研究施設と連携したオペレーションを実施し，さらに互いの研究施設が持つ情報を共有できる機構を構築している．この連携機構の要素技術のうち，特に KVM スイッチの有効性については，すでに第 1 報，第 2 報等 [1, 2, 3] で報告した．ところで，SD 室で実際の事案に対するオペレーションを行ったり，事案発生を想定した訓練を実施する場合，全体を統括する者が，複数のオペレータに対して的確な操作指示を出す機構が必要になってくる．われわれは，この操作指示を出す機構を「危機管理対応支援シナリオシステム」と名付けた．本報告では，主としてこの「危機管理対応支援シナリオシステム」の実装と運用について述べる．

2　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の小金井本所 (東京都小金井市) 内の高度情報通信危機管理研究施設は，情報通信の研究と危機管理の研究の境界領域の研究とわれわれが位置付けている「情報通信危機管理研究」の一貫として 2001 年度から整備が開始されたもので，以下の 3 施設が最初に整備された．

1. ネットワークセキュリティ研究施設
2. 非常時通信用高信頼性ネットワーク検証実験施設
3. 情報通信危機管理オペレーション実験施設

このうち 1 は，SIOS システム (Security Intelligence Operation Studio) [4, 5](不正アクセス等の事案を再現させてその影響を調べたり対策を調査研究するための不正アクアセス再現実験装置と，情報通信システムの脆弱性に関するさまざまな情報を集めた脆弱性データベースから構成されるシステム) を中心とした施設で，「情報通信システムの危機管理」についての研究を行っている．

上記 2 は，「大規模 IAA システム」(大規模災害時等に被災者情報の登録や検索を可能にする IAA システム [6] の中でも一番能力と規模が大きなシステム [1] を中心とした施設で，「情報通信システムで危機管理」についての研究に利用されている．なお，本報告では詳細は述べないが，「大規模 IAA システム」は，2003 年度からは，東京都小金井市の通信総合研究所小金井本所だけでなく，大阪府内の大阪府立インターネットデータセンターにも設置し，二拠点での運用を開始している．

上記 3 は，大型多面ディスプレイによる画像映像表示機能，東京地区地上波テレビ放送全チャネル 24 時間連続自動録画機能，本実験施設専用構内 PHS による音声会議 (意志決定支援) 機能，さらに AR(拡張現実感) 技術等を用いたオペレータ支援環境等を有する施設である．この施設は，「情報通信システムの危機管理」[2] や「情報通信システムで危機管理」[3] を実施する際にどのようなオペレーション環境をどのように提供するのがよいかを検討し，あらたな手法を研究開発するための施設である．この施設，すなわち「情報通信危機管理オペレーション室 (SD 室)」についての議論を行っているのが本報告を含む一連の報文である．

なお，2002 年度以降には，これらの施設の機能拡張が行われると同時に，新たな研究設備を通信総合研究所小金井本所のみならずそれ以外の拠点に設置しつつある．以下はその一例である．

- SIOS システムの考え方を踏襲しつつ，高機能パソコン上に多数の仮想マシンを配置して，不正アクセスの再現実験を仮想的に実施する「VM nebula」 [7, 8] を中心とした「ネットワークセキュリティ研究施設」の拡張 (通信総合研究所関西先端研究センター)

- 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」の新規導入 (同小金井本所)

これらの施設を，通信総合研究所小金井本所や関西先端研究センターからのみならず，必要な場合には「いつでもどこからでも」「確実に」運用できるようにしてゆく必要に迫られている．このため，「情報通信危機管理オペレーション室 (SD 室)」のオペレーション環境をどのように発展させてゆくかの議論は，以前にも増して重要になってきている．

[1] 開発名は「モンスター IAA システム」
[2] あるいは「インターネットの危機管理」
[3] あるいは「インターネットで危機管理」

3　オペレーション室 (SD 室) の機能

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．実際の SD 室は，床面積約 $300m^2$ で 約 60 名を収容可能な階段教室状の座席を備えた部屋で，室内には大型多面ディスプレイ，KVM スイッチに接続されたキーボード，マウス，液晶ディスプレイを持つ 14 名分のオペレータ席，持込み PC を接続できる一般席，全体の指揮をとるディレクタが着席するディレクタ席がある．また，大型多面ディスプレイの裏手には，AR(拡張現実感) 実験装置，地上波テレビ録画装置，SD 室専用の構内 PHS 装置を用いた音声による意志決定支援装置，対外接続設備 (ルータやファイアウォール) などが設置されている．

3.1　SD 室で実施可能な活動

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[4]．

SD 室では，下記の実施が考えられる．

3.1.1　ネットワークセキュリティ研究関連

1. 不正アクセス再現実験装置や脆弱性データベースを用いた事案の解析作業や対処方針策定手法の開発

2. 外部の情報を積極的に獲得しつつ対策を立案する，セキュリティ情報集約分析センターの構築．

    - 平常時は，主に上記 1 を実施する．
    - 実際に不正アクセス等の事案が発生した場合には，事案対処のためのスタッフが集まり，不正アクセス再現実験装置や脆弱性データベースの運用を実施しながら，外部の情報も積極的に獲得して対策を立案する，いわばセキュリティ情報集約分析センターとなる．この場合，機材運用拠点としての性格と意志決定のための会議室という性格の双方が同時に現れることになる．

[4] 第一報でも述べたように，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．よって，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．しかし，実際の事案発生に十分対処できる能力を持つことを目標にしている

3.1.2　非常時通信用高信頼性ネットワーク検証実験関連

1. 被災者情報登録検索システム (IAA システム) の運用監視手法の研究開発

2. 大規模災害時の情報の集約と対策の立案を行う，非常時情報集約分析センターの構築

    - 平常時は，著者らが以前から開発を続けている被災者情報登録検索システム (IAA システム) の運用状況の監視と動作監視手法の研究開発を実施する．
    - 実際に大規模災害等の事案が発生した場合には，事案対処のためのスタッフが集まり，IAA システムを運用しながら，外部からの情報も積極的に獲得するいわば非常時情報集約分析センターとなる．

上記以外にも，SD 室は下記に活用可能である．

- 上記に関連する学習，演習，訓練．
- マルチメディア技術を必要とする演習，プレゼンテーションあるいは会合

これらの用途に供するため，本節の冒頭でも言及したように，われわれは以下の機能を導入してきた．

- 大型多面ディスプレイを用いたさまざまな画像映像情報を表示する機能
- KVM スイッチを活用した，オペレータの協調作業を支援する機能
- AR(拡張現実感) 技術を利用した三次元画像情報を共有する機能
- SD 室内でのみ有効な構内 PHS を用いて複数のグループがそれぞれ独立してグループ内会話をする機能

導入にあたっては，情報通信分野や拡張現実感分野の研究で培われた技術を積極的に導入し，従来の危機管理用会議室に欠けているものが何で，何をどのように改善するとよいかといった，危機管理用会議室のありかたを検討することも念頭においた．

4　危機管理対応支援シナリオシステム

複数のスタッフが連携を取りながら作業を行う場合，各オペレータが自分の役割りをよく理解してい

るのはもちろんのこと，誰がいつオペレータに対してどういう指示を出したかを明確にでき，かつそれを随時チェックできる機構を持つ必要がある．例えば，人工衛星の運用など，ミスの許されない作業においては，ヒューマンエラーをなくすために，３重のチェック体制や，操作時の読み上げ２人体制，作業指示と操作の分業化などが以前から行われている．

情報通信危機管理においても，状況把握や対策立案，復旧作業の着手を素早く実施することは，被害を減らし信頼を保つ面からも重要な課題であり，こうしたオペレーションを支援するためのシステムが必要となる．

SD 室の機能を最大限に生かすためには，SD 室においてシステムを操作する多数の操作者 (オペレータ) に的確な指示を与える機構が必要である．

この要求に対処するために，今回設計と実装を開始したのが「危機管理対応支援シナリオシステム」である．

危機管理対応支援シナリオシステムで取り扱う情報通信危機の範囲には，インシデントや大規模災害時の発生の対策オペレーション支援，また，これらの危機対応のための教育啓蒙や訓練のためのオペレーション支援を含むものとする．

シナリオシステムで対応するのは，各オペレータが何をすべきかの指示を主とする．各オペレータは，施設の機器に関する基本的知識を有することを前提とし，各機器の詳細な操作方法については，特に作業に影響を与えること以外は，詳細に説明しないものとする．

4.1　シナリオシステムの機能要件

緊急対応を，効率よく行うためには，以下の要件が必要とされる．

1. 各オペレータへの役割分担
2. 作業ごとの優先順位づけ
3. 時系列ごとの処理手順や実行結果
4. 各オペレータが行うべき操作や処理の支持
5. 各処理の終了状況や現状のチェック
6. 処理状況などの情報共有
7. 作業実施後の報告

4.2　シナリオシステムの構成

これらの要件を満たすため，オペレータへの対処方針を明記した「シナリオ」を発生させる「危機管理対応支援シナリオシステム」の検討を行った．検討の結果，ハードウェア構成としては図 1 のようになった．

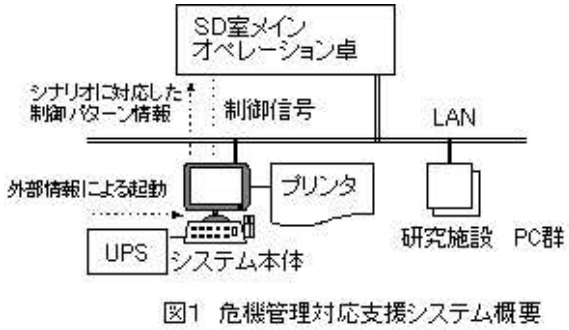

図1　危機管理対応支援システム概要

図 1: 危機管理対応支援システム概要

すなわち，UPS(無停電電源装置) から電源供給を受けるパソコンがシナリオシステムの要となる．このシステムには，事案発生時には事案の種類や発生時刻などの事案発生に関する最初期情報が自動あるいは手動で入力される．システムは，この最初期情報をもとに動作を開始する．

自動入力の情報源には，他のシステムからネットワーク経由で送られて来る信号やセンサから送られて来る信号がある．前者の一例には，不正アクセス等の事案発生を検知するためにインターネット上に設置されつつある広域早期警戒網がある．後者の例には，地震計，地上波テレビ放送を使って津波発生を知らせる緊急警報放送などがある．手動入力の一例は，SD 室全体を統括する者が着座するコンソール卓からの指示である．コンソール卓からの指示は，自動検知できなかった事案発生時や，訓練や演習時などの自動検知はありえない状況下でオペレーションを開始する場合には，特に有効である．また，具体的な手順はまだ決めていないが，遠隔からも起動指示を与えられるようにする方針である．

このパソコン上には，シナリオシステムの中核をなすソフトウェアが用意されており，与えられた最初期情報が事前に与えられたシナリオの原型 (テンプレート) のどれに最も近いか判断し，シナリオの原型をもとに当該事案用のシナリオを自動発生させる．

シナリオには，オペレータ全員の操作をすべて記した「全体シナリオ」と，シナリオシステムが自動

実行する内容を記したシナリオおよび各オペレータごとに与えられる「個別シナリオ」がある．内容的には，「全体シナリオ」は，全ての「個別シナリオ」をひとつにまとめただけである．

シナリオは，オペレーションの途中からは，本システムの運用関係者用の専用の WEB ページ上でも参照できるようになるが，時案発生直後の状態では，オペレータがオペレータ席に着席して専用 WEB ページにアクセスできるようになる前に，以下をオペレータ伝えなければならないため，オペレータごとに個別の「個別シナリオ」を作成し，プリンタで印刷して配布する．

- オペレータの氏名あるいは ID(誰に対して発行された個別シナリオなのかを明確にする必要があるため)
- 個別シナリオ作成日時と有効期限
- 個別シナリオ作成者
- 事案の種別
- 事案の名称 (仮称)
- 事案発生日時
- 事案対応の概要
- 事案対応の責任者
- 事案対応の全担当者
- 事案対応者 (個別シナリオを受け取ったオペレータ) の役割り
- 事案対応者の着席場所
- KVM スイッチの接続先 (利用するコンピュータの指定)
- 当該オペレーションの専用 WEB ページの URL
- 当該個別シナリオについての問い合わせ先
- 当該オペレータの作業手順 (シナリオ本体)．下記が時系列に沿ってくりかえし記載されている．
  - 作業開始条件 (作業開始時刻あるいは同期をとる必要がある作業項目)
  - 作業項目
  - 具体的な作業内容
  - 注意事項
- その他の参考になる情報

4.3 危機管理対応シナリオのパターン

危機管理対応支援シナリオのパターンとしては，危機の種類によりいくつかのパターンが考えられる．

情報セキュリティに関連した事案発生に伴うオペレーションでは，SIOS（シミュレーション装置と脆弱性データベース）システムとの連携を行いつつ，原因究明のためのインターネット上での情報収集や状況分析が主なオペレーションとなる．一方，大規模災害時には，テレビ放送のニュース映像などからの情報収集がオペレーションの重要な柱のひとつとなる．危機の種類により，オペレーションの方法は，機器利用も含め異なるが，シナリオ生成と対処流れはいずれも，図 2 に示すような手順となると考えられる．

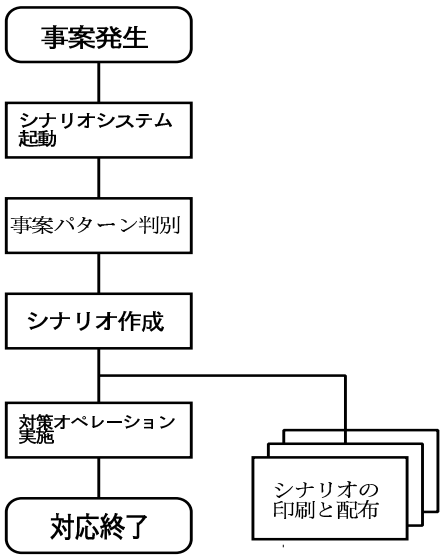

図 2: 危機管理対応シナリオ生成と対処の流れ

4.4 他のシステムとの連携

既に述べたのように，シナリオシステムの個別シナリオには，各オペレータに配布するものと，シナリオシステムが自動実行する内容を記したシナリオとがある．このうち後者については，シナリオに基づいて諸作業を順次実行する何らかのシステムが必要である．「シナリオに基づいて諸作業を実行する」際には，他のコンピュータ上の他のサービスと連携する必要が予想される．そこで，このような目的に合致したエージェントシステムを導入することにした．当初は，新たにエージェントシステムを開発することも検討してが，幸い，SIOS システムにおい

て不正アクセスを再現したり，データを回収したりする際に用いられているエージェントシステム[5]が利用に適していることがわかった．

このエージェントシステムは，JAVA で書かれているため移植性に優れている．また，動作を XML で記述する．XML による動作記述は，専用のスクリプト言語を用意する場合よりも場合によっては柔軟性に欠けるが，エージェントの動作記述は，時系列に沿って作業内容を記したシナリオ状になっており，動作記述ファイルを作成するフロントエンドは作成しやすいだけでなく，本報告で述べているシナリオシステムと相性がよい．

4.5 シナリオシステムの実装状況

現在，シナリオシステムは FreeBSD をインストールしたパソコンの上で，各種のスクリプト言語および上記のエージェントシステムを組み合わせて暫定的に実装している．シナリオの原型もまだごく限られた内容のものしか用意できていない．それでも，事案の内容を簡易なものに限定的すれば，シナリオを発生は可能である．現在，ソフトウェアの開発を継続しつつ，自動入力できる情報源の新たな確保に努めている．また，さまざまな状況を想定してシナリオの原型の種類を増やす準備をしている．

5 今後の展開

「危機管理対応支援シナリオシステム」の実装はまだプロトタイプの段階だが，これを安定した実装にする作業を急いで行いたい．前節で述べたように，現時点での実装では，各種スクリプト言語とエージェントシステムが混在した状態になっているが，極力エージェントシステムのみで記述する方針である．エージェントシステム自体は，SIOS システムの研究開発の中で改良作業が続いており，あと 2-3ヵ月で完成の域に達する予定である．エージェントシステムを中核とする次版のシナリオシステムも今年度中には連続して運用できる状態にまで実装を進めるとともに，実際の事案対応や災害対応に即した複数のシナリオを用意して，模擬訓練を行うことを検討している．また，現在はエージェントシステムが直接操作できないために，オペレータに指示を出してオペレータに操作させている，空調制御，照明制御，KVM スイッチの制御，構内 PHS の制御などもエージェントシステムが直接操作できるように改造可能なものから順次可能にしてゆきたい．

[5] このエージェントシステムの詳細は，現在別の報文にまとめている．

6 おわりに

本報では「危機管理対応支援シナリオシステム」の実装方針とプロトタイプの運用状況について述べた．「高度情報通信危機管理研究施設の構築」についての報告は，当初全 5 報を予定していたが，4 報構成に縮退させることになった．よって次報が最終報であり，高度情報通信危機管理研究施設について総合的な評価与え，今後の類似施設構築の際に参考なるよう総括を行う．

参考文献

[1] 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, 情報処理学会研究会報告 (DSM 研究会) 2003-DSM-29, No.29, (社) 情報処理学会 (2003)

[2] 大野 浩之, 山崎 靖博, 松本 文子, 三輪 信介: 高度情報通信危機管理研究施設の構築　(2) 研究施設間接続方式の設計と実装, 情報処理学会研究会報告 (DSM 研究会) 2003-DSM-30, No.30, (社) 情報処理学会 (2003)

[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, 情報処理学会研究会報告 (DPS/CSEC 合同研究会) 2002-DPS-111, No.111, (社) 情報処理学会 (2003)

[4] 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, DSM シンポジウム 2001 予稿集, (社) 情報処理学会, pp.121-126 (2001)

[5] 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, Vol.42, No.12, (社) 情報処理学会 (2001)

[6] 井澤 志充, 木本 雅彦, 多田 信彦, 三輪 信介, 大野 浩之, 篠田 陽一: IAA システムの現状とその課題, コンピュータソフトウェア, Vol.18, No.6, ソフトウェア科学会, pp.27-42 (2001)

[7] 三輪 信介, 大野 浩之: 再現実験環境『VM Nebula』を用いたウィルス・ワームの解析, IC2003 (Internet Conference 2003) 予稿集, インターネットコンファレンス (2003)

[8] 三輪信介，滝澤修，大野浩之: 仮想 PC インターネットセキュリティ実験環境『VM Nebula』の設計と構築, 2003 年暗号と情報セキュリティシンポジウム (SCIS2003) 予稿集, (社) 電子情報通信学会 (2003)