

ネットワークのコンフィギュレーションの高度化に関する考察と一提案

下 條 敏 男[†] 新 麗^{††} 新 善 文^{†††}
門 林 雄 基[†] 山 口 英[†]

現在の IP ネットワークでは、ネットワーク全体を直接設定するための手段が存在しないために、ネットワーク機器の人為的設定ミスを引き起こし問題となっている。この問題に対処するために XML によるネットワーク設定が提案されている。しかし、この XML によるネットワーク設定のアーキテクチャは詳細化されていないので、本論文ではこの XML によるネットワーク設定のアーキテクチャの詳細な設計を行った。そして、柔軟性、拡張性、Scalability という観点で考察を行い、問題点と対策を示す事ができた。

Consideration about advancement of the network configurations

TOSHIO SHIMOJO,[†] REI ATARASHI,^{††} YOSHIFUMI ATARASHI,^{†††}
YOUKI KADOBAYASHI[†] and SUGURU YAMAGUCHI[†]

Current IP-based networks lack effective means to configure networks as a whole, thereby causing human errors in the configuration of individual network devices. Although the concept of XML-based network configuration has been developed, the XML-based configuration architecture is still under development. This paper elaborates the architecture of XML-based network configuration. We then evaluate the proposed architecture from various perspectives, e.g., flexibility, extensibility, and scalability.

1. はじめに

昨今のブロードバンドの加入者回線は着実に普及している。特に、日本では DSL (Digital Subscriber Line: デジタル加入者回線) の普及は総務省公開のデータによると 2002 年度の 1 年間で約 3.6 倍に推移している。DSL 以外にも FTTH (Fiber To The Home: 光ファイバによる加入者回線) も既に商用サービスが行われており、DSL の加入者回線数までではないにしても着実に普及しつつある。また、ホットスポットと呼ばれる公共施設における無線 LAN によるインターネットアクセス可能な場所も増加している。

このような加入者回線のブロードバンド化にともない、動画配信サービス、個人の間でのビデオデータのやり取り、英会話教室のようなビデオ通話、オンラインゲームなど今までになかったようなブロードバンド

を有効利用したアプリケーションやサービスが展開されつつある。このように現在のインターネットにおいて新たなネットワーク技術が次々と開発されていく中で、ネットワークも変化し続けている。

上記のようなネットワークの変化のために加入者回線に対してインターネットへの接続サービスを行う ISP (インターネット接続事業者) のバックボーンネットワークもより高速化されている。

一方、現在の IP ネットワークではネットワーク全体を直接設定する手段が存在しない。ネットワーク全体を設定するために、ネットワークオペレータはネットワーク内の各ネットワーク機器に対して個別に設定を行っている。

大規模なネットワークにおいて、ネットワーク・オペレータが直接各ネットワーク機器を設定することは、設定すべきネットワーク機器も多数存在し、それぞれのネットワーク機器間での設定の関係も存在する。このため、設定すべき内容も多く存在し、設定するためのコストが大きく、設定の人為的なミスも発生する可能性が高い。

ネットワーク設定には、大きく分けてネットワーク機器の初期導入時のためのネットワーク機器設定と個

[†] 奈良先端科学技術大学院大学 情報科学研究科
Graduate School of Information Science, Nara Institute
of Science and Technology
^{††} (株) インターネットイニシアティブ 技術研究所
Research Laboratory, Internet Initiative Japan Inc.
^{†††} 株式会社日立製作所 IP ネットワーク事業部
Global IP Network Division, Hitachi, Ltd.

別のサービスを提供するためのネットワーク機器設定の二種類が存在する。ネットワーク機器の初期導入時のネットワーク機器設定は、ネットワーク機器初期導入時の一回のみ設定が行われ、導入時に運用を行う前に接続確認も行われる。このため、設定ミスがあっても実際のネットワーク運用に与える影響は小さい。しかし、個別のサービスを提供するためのネットワーク機器設定では、サービスの設定の要求が発生する度にネットワーク機器設定を行わなければならない。その上、ネットワーク機器を設定する対象が実運用を行っている動作中のネットワークであるために、設定ミスによる影響も大きい。

上記のように、設定する内容が多く、その設定項目間の整合性を考慮して設定することは、設定するためのコストとも大きい。このことから、何らかの方法にて、ネットワーク機器に対する設定の自動化を行う仕組みが必要である。

このネットワーク設定の自動化のための仕組みとして、XML¹⁾を使用したネットワーク設定^{3)~5)}がIETFなどで提案されている。同一ネットワーク内に存在するネットワーク機器は様々なベンダの製品から構成されており、その設定のためのコマンドは各ネットワーク機器に異なる。ネットワークオペレータが直接ネットワーク機器を設定するためには、同一ネットワーク内に存在するすべてのネットワーク機器の設定コマンドを理解する必要がある。ネットワークオペレータが多くのネットワーク機器の設定コマンドを理解するためには、ネットワーク機器の設定コマンドなどを理解するための学習コストがかかる。このため、XMLを使用したネットワーク設定では、それぞれのネットワーク機器の設定コマンドの代わりに、ネットワーク機器共通の設定コマンドを規定するためXMLを使用する。

しかし、現在提案されているXMLによるネットワーク設定では概念、要素技術などが規定されているが、詳しいアーキテクチャが規定されておらず、実装にあたっては様々な問題が存在する。このため、本論文ではXMLによるネットワーク設定のより具体的なアーキテクチャについて考察し、XMLによるネットワーク設定での目的であるネットワーク機器のベンダに依存しないネットワーク設定の実現に向け、その問題点などを明らかにし、その対策について述べる。

2. XMLによるネットワーク設定の概要

XMLによるネットワーク設定は、主としてネットワーク設定のためにかかるコストを削減することを目的として提案されている。現在、XMLによるネッ

トワーク設定では、基本的なアーキテクチャとネットワーク機器にコンフィグレーションを配布するためのプロトコルであるXMLCONFがIETFで提案されている。

2.1 XMLによるネットワーク設定のアーキテクチャ

現在提案されているXMLによるネットワーク設定の基本的なアーキテクチャは、図1に示すように、ネットワーク設定とネットワーク設定内容の管理を行うXML Configuration System、ネットワーク設定の対象であるNetwork Nodeに分けられる。XML Configuration Systemは、Visual Design Tool, XML Configuration Controller, DataBaseに分かれている。Visual Design Toolは、ネットワーク・オペレータに対してネットワーク設定のための情報の入力をGUIにより提供し、入力された情報をXMLで表現される特定ベンダに非依存なネットワーク設定情報に変換する。XML Configuration Controllerは、DataBaseに格納または取り出しを行い、各Network Node対するの設定情報をXMLCONFプロトコル⁴⁾にて各Network Nodeへ配布する。DataBaseはネットワークの設定情報を格納する。

XMLによるネットワーク設定の対象は、設定対象のネットワークが運用状態においてネットワーク設定内容の追加と削除、そのネットワーク設定の実施状態の監視を動的に行うことである。

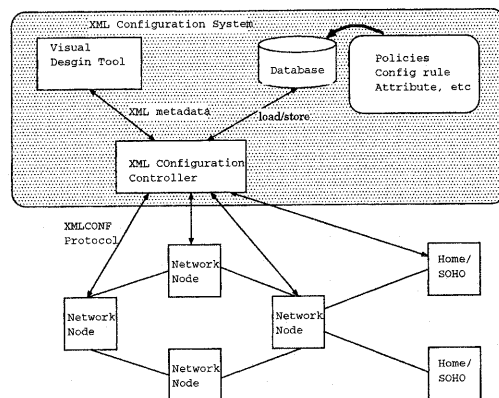


図1 XMLによるネットワーク設定のアーキテクチャ

2.2 XMLCONF プロトコル

XML Configuration System と Network Node 間のプロトコルは、XMLCONF プロトコルを使用する。XMLCONF プロトコルのプロトコル階層は、次の図2のように上位層から Contents layer, Operations

layer, RPC layer, Transport layer に分かれている。Contents layer と Operations layer は、XML を利用した RPC (Remote Procedure Call) である XML-RPC²⁾ のメッセージとして encode される。XML-RPC の実行上で発生したエラーは XML-RPC のエラーメッセージで返される。以下に各プロトコル階層について詳述する。

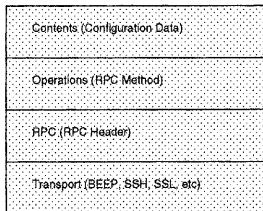


図2 プロトコル階層

Contents layer: この Layer は、XML-RPC のメッセージに encode される。Operation layer で指定されている XML-RPC 関数により異なるが、主に各 Network Node のコンフィグレーション情報とその応答、参照する状態情報の項目とその内容に分類できる。XMLCONF プロトコル仕様では、この Layer の内容を規定していない。

Operation layer: この Layer は、XML-RPC のメッセージに encode される。実行する XML-RPC 関数を指定する。主に、Network Node からコンフィグレーション情報を得る get-config, Network Node にコンフィグレーション情報を設定する edit-config, Network Node 全体のコンフィグレーション情報を設定する copy-config, Network Node にコンフィグレーション情報を削除する delete-config, Network Node の状態情報を得る get-status, XMLCONF プロトコルのセッションを切断する kill-session などの XML-RPC の関数が規定されている。

RPC layer: 上記の二つの Layer の内容を encode する。XML-RPC メッセージの最小単位である。XML-RPC の処理は、このメッセージ単位に行われる。例えば、RPC の実行時にエラーが存在した場合には、要求メッセージ単位に、XML-RPC 要求元に返される。

Transport layer: 上記三つの layer の内容をカプセル化し、XML Configuration System と Network Node 間の実際の接続を行う。Transport protocol として、BEEP⁹⁾, SSL, SSH などを使用する。

3. XML によるネットワーク設定のアーキテクチャの設計

現在の XML によるネットワーク設定の基本的なアーキテクチャは、各 Network Node の内部構造に関しては示されておらず、XML Configuration System の内部構造については簡単な要素だけが示されているだけである。このため、どの部分が標準化されているの機能がベンダ依存の機能が分からない。この章では、ネットワーク設定の基本的なアーキテクチャに対して標準化に必要な機能がベンダ依存の機能を分類し、以下に示す要件にしたがって各 Network Node と XML Configuration System の内部構造についてのアーキテクチャについて設計を行う。

- システムの柔軟性
- システムの拡張性
- Scalability

3.1 XML Configuration System の内部構造

XML Configuration System の内部は、機能毎に分割すると図3のように次の4つのブロックに分けることができる。

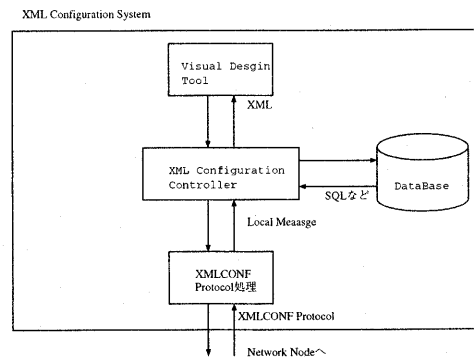


図3 XML Configuration System の内部構造

Visual Design Tool: ネットワークオペレータのネットワーク設定の入力の処理を行い、入力された情報を XML で表現されたネットワーク機器のベンダに非依存なネットワーク設定情報に変換する。この機能部分は、ネットワークを運用するユーザによって要求する詳細な機能(入力方法など)が異なるため、ベンダ依存ではなくとも標準化すべき機能ではない。

XML Configuration Controller: XML で表現されたネットワーク機器のベンダに非依存なネッ

トワーク設定情報を DataBase に登録する。さらに Network Node に対する設定のためにネットワーク設定情報の内容を XML-RPC で encode した設定情報に変換し、変換した設定情報を XMLCONF Protocol 処理に渡す。

XMLCONF Protocol 処理: XML Configuration Controller で変換した XML-RPC で encode された Network Node に対する設定情報を XMLCONF プロトコル・メッセージにカプセル化して送信する。XMLCONF プロトコルのための処理であり、Network Node のベンダの実装に依存しない。

DataBase: XML Configuration Controller の要求にしたがって、Network Node のベンダに非依存なネットワーク設定情報の登録、削除、保持をおこなう。使用する DataBase の実装としては、Network Node のベンダに非依存なネットワーク設定情報の永続性に必要であるだけなので特定しない。

3.1.1 Visual Design Tool, XML Configuration Controller 間インタフェース

このインタフェースでは、XML で表現されたネットワーク機器のベンダに非依存なネットワーク設定情報を Visual Design Tool から XML Configuration Controller に渡す。

3.1.2 XML Configuration Controller, XMLCONF Protocol 処理間インタフェース

このインタフェースは、標準的なプロトコルや encoding を使用しない関数呼び出しか、ローカルなフォーマットのメッセージパッシングで実現できる。この間で渡されるデータは、XMLCONF プロトコルメッセージにカプセル化可能な各 Network Node に対する設定情報である。

3.1.3 XML Configuration Controller, DataBase 間インタフェース

このインタフェースは、使用する DataBase の実装するに依存しているので特定なものを指定しない。例えば、DataBase として RDB (Relational DataBase) を使用する場合には、XML で表現されたベンダに非依存なネットワーク設定情報から SQL に変換するために XML 文書を RDB に登録するためのインタフェースである XML-DB を使用することができる。

3.2 Network Node の内部構造

XML Configuration System が管理する対象の各 Network Node を機能別にモジュールに分割すると、図 4 のように、主に次の 3 つのモジュールに分割で

きる。

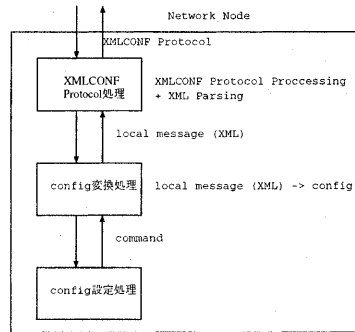


図 4 Network Node の内部構造

XMLCONF Protocol 処理: XMLCONF プロトコルのための処理であり、XML Configuration System から受信した XMLCONF プロトコルメッセージを解析し、XML-RPC 部分を取り出し、config 変換部に渡す。config 変換処理から受け取った一連の処理結果を XMLCONF プロトコルメッセージにして XML Configuration System へ送信する。XMLCONF プロトコルのための処理であり、Network Node のベンダ依存する変換処理を行わないので、Network Node のベンダに非依存である。

config 変換処理: XMLCONF プロトコルメッセージの XML-RPC 部分から Network Node の設定に必要なデータ部分の内容を取りだし、Network Node 固有のコンフィグレーションの形式に変換する。また、config 設定処理における実行結果を解析し、XML-RPC の形式に変換して XMLCONF Protocol 処理に渡す。この変換の方式は Network Node のベンダ毎に機器のコンフィグレーションが異なるのでベンダ依存である。

config 設定処理: Network Node に対する XML によるネットワーク設定のための拡張を行う以前から実装されている既存機能である。この部位は Network Node のベンダにより実装が異なるベンダ依存である。

次に、上述の 3 つのモジュール間のインタフェースについて述べる。

3.2.1 XMLCONF Protocol 処理、config 変換処理間のインタフェース

このインタフェースは、標準的なプロトコルや encoding を使用しない関数呼び出しもしくは、ローカルなフォーマットのメッセージパッシングで実現する

(例えば、UNIX のローカルメッセージインタフェースである Domain Socket など)。この間で交換されるデータは、XML-RPC の関数名と XML-RPC の内容に含まれるネットワーク設定情報だけを持つ内部形式のデータである。

3.2.2 config 変換処理、config 設定処理間のインタフェース

このインタフェースは、Network Node の config 設定処理の実装に依存である。例えば、この間で交換される内容は、Network Node に固有のコマンドもしくは、コンフィグレーションファイルである。

4. XML によるネットワーク設定のアーキテクチャの考察

次に、本論文でのアーキテクチャ設計を柔軟性、拡張性、Scalability という観点から考察し、見つかった問題点とその対策を述べる。

4.1 柔軟性

4.2 XML Configuration System

XML Configuration System がネットワークオペレータの入力情報の内容から Network Node に対する設定情報に変換するためとネットワーク状態が変化しても設定可能にするためには、どの Network Node がネットワーク上のどこに配置されているかを知っておく必要がある。

ネットワークのトポロジを表現する情報を XML Configuration System で持つようにし、ネットワークの状態が変化した場合にはこの情報を更新する。オペレータによりネットワークトポロジの情報を作成することは可能であるが、ネットワークの情報が増加した場合に対応するのが難しいため、Routing Protocol の持つ経路情報を Network Node から SNMP¹⁰⁾ で取得し、この情報から XML Configuration System で扱うネットワークトポロジ情報を自動で作成する。

4.3 Network Node

XML によるネットワーク設定での設定対象である Network Node (router, switch, など) に対する設定情報を特定のベンダ製品を想定して仕様を決めると、別の製品に対応することが難しい。

XML によるネットワーク設定での設定対象である Network Node (router, switch, etc) をベンダ非依存に扱うために、仮想的な Network Node を定義して Network Node に対する設定情報を定義する。

4.4 拡張性

4.4.1 Network Node の将来の機能拡張に対する対応

インターネットは現在も次々と新たな技術開発が行われており、将来において新たな機能が XML Configuration System の管理対象である Network Node に対して追加する必要性が発生する可能性がある。このため Network Node に新たな機能追加がなされた場合に XML Configuration System においても柔軟に対応できる必要がある。しかし、Network Node は通常、組み込み機器であるため Network Node 側のプログラムは簡単には修正できないという性質がある。このことから、プログラムでない方法で拡張するなんらかの手段が必要である。

プログラムでない方法でテキストデータ変換のための仕組みとして W3C にて XSLT⁸⁾ が規定されている。XSLT はテキストデータ変換処理を XSLT スタイルシートと呼ばれる形式の XML 文章で記述可能であり、テキストデータ変換処理の拡張が容易である。Network Node の config 変換モジュールの処理でこの XSLT を使用することにより、将来の Network Node に対する機能追加に対応する。

4.4.2 新しいネットワークサービスへの対応

将来、インターネットにおいて新技術が登場し、その新技術を使用したサービスが必要となった場合において、XML Configuration System においてもその新ネットワークサービスへの対応が必要となることが予想される。このため、新しいベンダに非依存であるネットワーク設定情報に対して大幅な変更なしに対応できるような構造にしなければならない。

Network Node の config 変換モジュールの処理同様に、XML Configuration System の XML Configuration Controller においても、XSLT を使用することで新しいネットワークサービスに対応する。

4.5 Scalability

4.5.1 XML Configuration System

XML Configuration System が多数の Network Node を管理する場合には、XML Configuration System が一台のマシンで実装されていると処理性能不足になると考えられる。そこで、4 つあるモジュールブロックを別々のマシンで動作させることにより負荷分散を行う。

Visual Design Tool と XML Configuration System の間は、特定ベンダに依存しないネットワーク設定情報のデータ形式として XML を使用することを規定しているだけで、使用する transport protocol を規定

していないため、使用する適切な transport protocol を規定する必要がある。また、XML Configuration System と DataBase の間は、DataBase をアクセスするためのプロトコルを使用するか、別のプロトコルを使用して、別々のマシン上でそれぞれを動作させることが可能である。

4.5.2 管理領域の階層化

管理対象のネットワークが大規模で Network Node 数が多数存在する場合には、管理領域を区切って管理することが考えられる。また、異なった管理ポリシーを持つネットワークが接続している場合において、XML Configuration System で管理を行う場合にはそれぞれのネットワークを管理している XML Configuration System の間でやり取りを検討する必要がある。

5. 関連研究

ネットワーク設定の自動化のための仕組みとしては、XML によるネットワーク設定のほかに、IETF の SNMPCONF (Configuration Management with SNMP) Working Group で提案されている SNMP による設定⁶⁾ や DMTF (Distribute Management Task Force, Inc.) で標準化を行っている CIMxml⁷⁾ が存在する。

既存の SNMP では、管理装置である NMS (Network Management System) がネットワーク機器から MIB (Management Information Base) を取得して、NMS で人間が見ることのできる形式に加工し、表示を行っている。SNMP による設定では、既存の SNMP の MIB をネットワーク機器に対して設定を行えるように拡張したものである。しかし、MIB のすべての定義が一つのツリー構造になっていて、設定に必要な項目がツリーのいろいろな場所に配置されている。このため、ネットワーク設定を行う場合には、ツリーのいろいろな部分に存在する複数 MIB に対して設定を行う必要があり、設定の効率が悪い。また、SNMP プロトコルは一つの項目の設定要求に対して一つの応答が必要である。このため、ネットワーク機器に対して複数の MIB の項目を設定するとオーバーヘッドが大きい。

CIMxml は、CIM を xml で規定したものである。しかし、CIMxml はその XML の型定義に DTD (Document Type Definition) を使用しているため、XML の name space が使用できないなど、XML の有用な機能を有効利用できない。

6. まとめ

本論文では、XML によるネットワーク設定より詳

細な設計を行った。XML Configuration System では、機能ブロックを Visual Design Tool, XML Configuration Controller, XMLCONF Protocol 処理と DataBase に分割し、それぞれの詳細な機能を提示し、それぞれの間のインタフェースを規定した。また、Network Node では、XMLCONF Protocol 処理、config 変換処理、config 設定処理に分割し、それぞれの詳細な機能を提示し、それぞれの間のインタフェースを規定した。

本論文で提示した XML Configuration System と Network Node の詳細機能を柔軟性、拡張性、scalability という観点から考察した結果、柔軟性、拡張性、scalability のそれぞれの問題点を見つけ、それぞれの対策案を提示できた。

今後は Network Node のベンダに非依存なネットワーク設定情報の定義、仮想 Network Node の XML での定義などを行い、実際に動作可能なシステムを実装する。

参考文献

- 1) "Extensible Markup Language (XML) 1.0 (Second Edition)", W3C, <http://www.w3.org/TR/2000/REC-xml-20001006>
- 2) Dave Winer: "XML-RPC Specification", <http://www.xmlrpc.com/spec>
- 3) Ray S. Atarashi, Toshio Shimojo, Yoshifumi Atarashi, Shigeru Miyake, Makoto Kitani, Fred Baker, Margaret Wasserman: "XML Configuration Architecture", Internet-Draft, IETF, Oct., 2002.
- 4) Rob Enns: "XMLCONF Configuration Protocol", Internet-Draft, IETF, Feb., 2003.
- 5) 新麗, 三宅 滋, 新 善文, 木谷 誠, 下條 敏男: "メタデータによるネットワーク制御", 第 23 回 デジタル図書館ワークショップ, Nov., 2002.
- 6) M. MacFaden, D. Partain, J. Saperia, W. Tackabury: "Configuring Networks and Devices With SNMP", Internet-Draft, IETF, Jan., 2003.
- 7) Jim Davis: "CIM-XML", DMTF, Jun., 2002.
- 8) "XSL Transformations (XSLT) Version 1.0", W3C, <http://www.w3.org/TR/xslt>
- 9) M. Rose: "The Blocks Extensible Exchange Protocol Core", IETF, RFC3080, Mar., 2001.
- 10) D. Harrington, R. Presuhn and B. Wijnen: "An Architecture for describing Simple Network Management Protocol (SNMP) Management Frameworks", IETF, RFC 3411, Dec., 2002.

11) "SOAP Version 1.2 Part 0: Primer", W3C,
<http://www.w3.org/TR/soap12-part0/>

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* 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