

# 総合行政ネットワーク(LGWAN)実証実験

## Demonstration Experiments on LGWAN

### あらまし

近年、インターネットを始めとしたネットワーク上で様々なデータ交換が行われている。政府もこの現状を受け、「ミレニアム・プロジェクト」として「2003年度までに電子政府の実現のための基盤を構築する」という目標が掲げられた。この基盤こそが「総合行政ネットワーク」であり、すでに運用を開始している霞が関WANとの接続を始め、近い将来実現するであろう住民・企業からの電子申請の基礎を築くものである。総合行政ネットワークについては、3年間の調査研究期間を終え、この研究結果を踏まえた実証実験を行った。

本ネットワークシステムは全国規模でのネットワークをはじめ、セキュリティ技術や暗号技術、認証技術を有機的に結合することを特徴としている。

この実証実験は今後の電子政府実現のための礎になるものであり、これを実現するための有効性、課題などについて実験を通して検証を行った。

### Abstract

There have been various data exchanges over the Internet in recent years. Taking this into consideration, the Japanese government has formed the Millennium Project, which aims to establish the base for Electronic Government by fiscal year 2003. This base, called the Local Government Wide Area Network System, will enable connection to the Kasumigaseki WAN and enable citizens and businesses to do all their administrative procedures over the Internet. The aim of this system is to establish a nationwide network that integrates security, encryption, and authentication technologies. We have completed three years of advanced research on this project and have conducted various demonstration experiments on the Local Government Wide Area Network to prove the system's validity and identify problems. These demonstration experiments are an essential step towards realizing Electronic Government in the future. This paper describes these demonstration experiments.



寺田満明（てらだ みつあき）

e-Japanソリューション事業部電子  
行政第二ソリューション部 所属  
現在、地方公共団体システム開発  
に従事。



樋口寿徳（ひぐち ひさのり）

e-Japanソリューション事業部電子  
行政第二ソリューション部 所属  
現在、総合行政ネットワーク構築  
に従事。

## まえがき

近年、インターネットを始めとしたネットワーク技術の進歩あるいは低コスト化に伴うコンピュータネットワークが急速に発展し、従来のオフライン媒体（紙・電話・FAXなど）での情報交換の仕組みがオンラインによる電子データへと大きく変貌してきている。

こうした世の中の変革を受け、政府においては、1994年12月25日に閣議決定した「行政情報化推進基本計画」を「電子政府」実現に向けた行政情報化を更に推進するため、同計画の改定を1997年12月20日に行った。

また、1999年12月19日に内閣総理大臣が決定した「ミレニアム・プロジェクト」において、「2003年度までに電子政府実現のための基盤を構築する」という目標が掲げられ、その実現のために地方公共団体の電子化を先導することになった。政府はこれを受けて、中央省庁間の霞が関WANが構築され、1997年1月から運用が開始された。

この電子政府実現のための基盤として、「総合行政ネットワーク（LGWAN）」と呼ぶ全国の地方公共団体約3,300を収容するネットワークについての調査研究が開始された。

「総合行政ネットワーク」の調査研究は1997年度から3か年実施され、ネットワーク構築・運営手法、行政情報の定義、行政情報を電子的にネットワーク上で流通させる場合の技術面・運用面などの諸課題などが整理された。この調査報告を受け、2000年度に47都道府県と12政令都市を対象に「総合行政ネットワークに関する実証実験」が行われ、諸々の検証が行われた。

本稿では、この「総合行政ネットワークに関する実証実験」を題材に電子政府実現の足掛かりについて考察する。<sup>(1)～(3)</sup>

## 実証実験の目的

総合行政ネットワークは既に地方公共団体が構築している組織内ネットワークを相互に接続し、高度情報流通を可能とする通信ネットワークとして整備し、地方公共団体相互のコミュニケーションの円滑化、情報共有による情報の高度利用促進などを図ることにより、各地方公共団体と国の各府省および将来的には住民や企業との情報交換基盤とすることを目的に実験環境の構築を行った。

構築に当たっては、以下のコンセプトが掲げられ、この実現を目的に実験環境の構築が進められた。

- ・すべての地方公共団体を収容可能な行政内に閉じたネットワーク
- ・電子メール、電子文書交換などの業務横断的サービスの提供
- ・高いセキュリティの確保（ISO/IEC15408準拠を目標）
- ・霞が関WANとの接続
- ・情報通信分野におけるデファクトスタンダード技術活用によるネットワーク構築
- ・地方公共団体ごとのネットワークを含めた既存設備の有効利用およびネットワーク形態の相違を吸収
- ・運用可能な低コストでの構築、運用

また、構築に当たっては47都道府県および12政令都市をベースに既に県域でWANを構築運用している2県から12市町村が選ばれ、県域WANとの接続性、霞が関WANとの接続性あるいは実験から得られるトラヒックの種別や量を測定し、ネットワークの最適化を得るための様々なパラメータ収集を実験の目的とした。

実験に際しての技術目標として以下が掲げられた。

- ・拡張性（スケーラビリティ）
- ・信頼性（アベイラビリティ）
- ・ネットワーク性能
- ・セキュリティ
- ・マネージャビリティ
- ・柔軟性（アダプタビリティ）
- ・費用対効果（TCO：Total Cost Ownership）

## 実証実験の概要（実験内容）

実証実験は主に五つのレイヤに分け、それぞれのレイヤごとに本運用をにらんだ実験環境の構築を行い、技術検証、運用時の課題などの洗い出しを行った。

五つのレイヤは、以下のとおりである。

### (1) 物理層・データリンク層

MPLS（Multi Protocol Label Switching）網によるネットワーク回線の検証と都道府県WAN形態ネットワークの接続技術検証。

### (2) ネットワーク層

TCP/IPプロトコルをベースに通信途中のデータ暗号化、セキュリティ、ルーティング、全地方公共団体を収容するためのIPアドレスデザインなどの技術検証。

### (3) 基本プロトコル群

アプリケーション基盤が使用する基本的なインターネットプロトコル（DNS、SMTP、NTPなど）について実装上の技術検証。

## (4) アプリケーション基盤

総合行政ネットワーク上で構築されるアプリケーションに共通的に必要となる認証基盤、ディレクトリ基盤、証明書検証、公証基盤、XML電文交換基盤についての整備。

## (5) 基本サービス

アプリケーション基盤と連動し、サンプルアプリケーションとして、電子文書交換とWebアプリケーションを整備。

それぞれのレイヤ構成について、さらに実験の詳細を以下に述べる。

### ● 物理層・データリンク層

MPLS網の利用範囲としては、図-1に示すようなNOC (Network Operation Center) 設備を階層的に構築し、ネットワーク全体の信頼性・可用性を考慮した構築を行った。

#### (1) 全国NOC

全国NOCとは、総合行政ネットワーク専用の施設・設備として設置されるNOCを指し、各都道府県単位に設置されるNOCを接続し、総合行政ネットワーク全体の運用管理を行うセンタ。

#### (2) LGWANバックボーン回線

LGWAN (Local Government Wide Area Network) とは、総合行政ネットワークのことである。バックボーン回線は、全国NOCと都道府県NOCを相互に接続する

MPLS網。

#### (3) 都道府県NOC

都道府県NOCとは、総合行政ネットワークの施設として各都道府県に設置されるNOCであり、管下の市町村ネットワーク (LAN) を收容、集線して全国NOCに接続するとともに、管下の市町村を相互にネットワーク接続する施設。

#### (4) LGWANアクセス回線

LGWANアクセス回線とは、都道府県NOCと地方公共団体の接続を中継するLGWANサービス提供設備とを接続する回線。

LGWANアクセス回線は、MPLS網を使用する県域アクセス回線と都道府県WANの2種類に分類される。

本レイヤでは総合行政ネットワークにおけるバックボーン回線に求められる閉域性、大容量帯域、スケーラビリティ、SLA (Service Level Agreement)、回線料金の均一化を目指したネットワーク構築を行った。また、アクセス回線についてはフレームリレー伝送方式とし、PCR (Peak Cell Rate : 上限転送速度)、SCR (Sustainable Cell Rate : 保証転送速度) を設定したMPLS網接続環境が構築された。

### ● ネットワーク層

本レイヤでは、先にも触れたとおりTCP/IPプロトコルをベースに通信途中のデータ暗号化、セキュリティ、ルーティング、全地方公共団体を收容するためのIPア

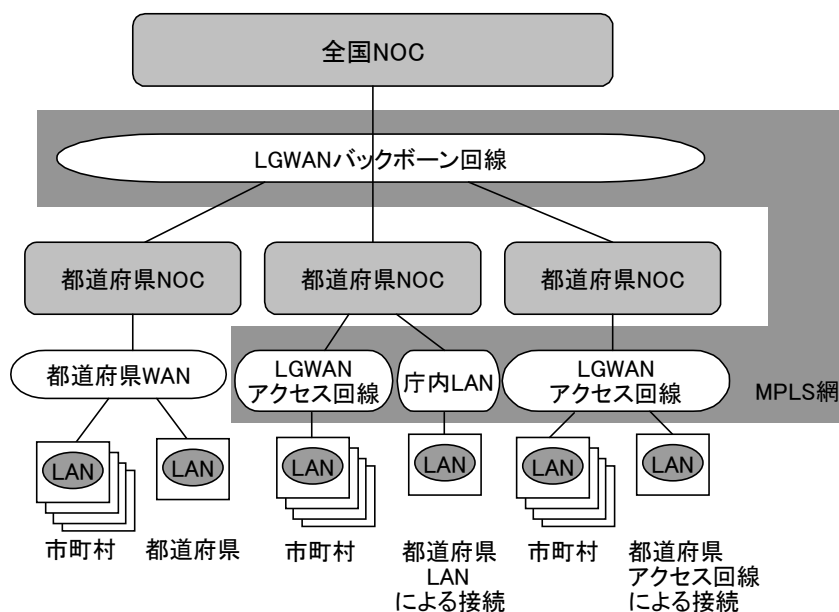


図-1 MPLS網の利用範囲  
Fig.1-Scope of utilization of MPLS network.

ドレスデザインなどを目的に実証実験検証が行われた。

### (1) 暗号化

暗号化においてはトリプルDES (Data Encryption Standard) 方式を採用し、性能、コストパフォーマンスを考慮し、それぞれのネットワークパスにおいて最適な機器で暗号化処理環境の構築を目的とした。

### (2) セキュリティ

セキュリティに関しては、総合行政ネットワークに求められる信頼性を確保するために、それぞれのネットワークパスごとにファイアウォールを設置することにより、外部からの侵入を極力遮断する構成をとっている。また、併せてIDS (Intruder Detection System) を設置し、不正侵入検知を行う構成をとっている。実験では、この構成に対して第三者機関によるペネトレーションテストを行い、問題がないことを確認した。

### (3) ルーティング

ルーティングでは、ダイナミックルーティングを試行し、NOC-NOC間、NOC-LAN間は経路情報を交換し、障害検出時に予備回線へ切り替わる構成とした。

また、図-1によると同一管内の市町村間はアクセス回線を通じて直接通信することも可能であるが、上述のセキュリティを担保するため、必ず都道府県NOCのIDSを経由したルーティング設定が施された。

### (4) IPアドレスデザイン

IPアドレスデザインにおいては、総合行政ネットワーク内では、インターネットアドレス（グローバルアドレス）を採用し、ネットワーク内で一意性を保つためのデザイン設計が行われた。ただし、全国約3,300の団体やその接続機器を収容するためのアドレス確保ができなかったため、本運用に当たっての課題とした。

本運用に当たっては、適切なアドレスブロックの割当てを行わなければルーティングテーブルの肥大化を招き、遅延を引き起こす可能性がある。

## ● 基本プロトコル群

総合行政ネットワーク内で使用される基本的なプロトコルとして、DNS (Domain Name System)、SMTP (Simple Mail Transfer Protocol)、NTP (Network Time Protocol) の各サーバを設置した。

これらのプロトコル群は、インターネット上でも標準的に利用されているものであるが、行政内に閉じた閉域ネットワークとして、以下のような特性を持つものとした。

### (1) DNS

インターネットとの接続を持たないため、総合行政ネットワーク内で用いられるドメイン以外の解決処理は行わないこととした。したがって、Rootサーバを全国NOCに設置することとした。

### (2) SMTP

図-1のような階層的なネットワーク構成をとったため、メールの配送経路も階層分けを行った。また、総合行政ネットワーク内のNOC設備では、SMTPによる中継サービスのみを提供することとし、POP (Post Office Protocol) などのユーザデータを扱うサービスは行わないポリシーで構築を行った。さらに、すでに稼働している霞が関WANとのメール交換においては、相互のネットワーク間で送達確認が行えるよう、X.400プロトコルによる中継処理およびX.400⇄SMTPのゲートウェイ処理を行い、異種プロトコル間通信の検証を行った。

### (3) NTP

後に述べる公証基盤や総合行政ネットワーク内の時刻を一定に保つために、NTPサーバを設置した。時刻は日本標準時間を刻み原子時計に直結しているStratum1を設置し、それを参照するStratum2の構成をとっている。

## ● アプリケーション基盤

アプリケーション基盤では、総合行政ネットワーク内で使用されるであろう以下の基盤機能について検証が行われた。

### (1) 認証基盤

認証基盤 (PKI: Public Key Infrastructure)、および認証基盤から発行された証明書を検証する検証機能であるVA (Validation Authority) を構築した。これにより、総合行政ネットワーク内を通過する電文の保証（なりすまし、改ざん、盗聴などのネットワーク被害からの保護）を担保する仕組みとした。

これらは、近年EC (Electronic Commerce: 電子商取引) などで利用されている手法と基本的な考え方を一にするものであるが、総合行政ネットワーク内で使用する証明書フォーマットはITU (International Telecommunication Union: 電気通信に関する国際標準の策定を目的とする、国際連合の下位機関) -TX.509 Version3をベースにその拡張領域を使用した総合行政ネットワーク専用の証明書の発行を行い、この証明書はICカードに格納され、認証、署名を伴う実験項目に利用することとした。



## (2) ディレクトリ基盤

統合ディレクトリを全国NOCに設置し、認証基盤から発行される認証情報を公開する機能を構築し、ディレクトリ機能の検証を行った。

## (3) 公証基盤

公証基盤は、論理的トランザクション単位にXML化されたレシート原文にNTPから受信した標準時間を刻印し、秘密鍵を専用のハードウェア装置を用いてデジタル署名のうえ管理を行う仕組みとした。

## (4) XML電文交換基盤

XML電文交換基盤は上述の公証基盤にも記したように、アプリケーション基盤におけるトランザクション処理の基盤を構築した。この基盤を用いることにより、各アプリケーションの差異を吸収し、各トランスポート層の通信プロトコルによって通信を行うことが可能となる。したがって、トランスポート層がアプリケーションから分離されているため、クライアントやアプリケーション間の通信では通信プロトコルを自由に使い分けることが可能となる基盤とした。

## ● 基本サービス

総合行政ネットワークにおける基本サービスとして、基本プロトコル、アプリケーション基盤上で動作する以下のアプリケーションを実装し、有効性の検証が行われた。

### (1) 公文書交換

公文書交換とは、行政間でやり取りが行われる行政文書(以下、公文書)を送受する仕組みである。SMTP/POPなどのメールプロトコルで送受される電子データ交換と同様の考え方であるが、公文書交換では、その性格上当該文書の取扱いについて、図-2で示すような事務フローが発生することから、メールプロトコルでの電子データの送受信だけでは機能的に不足が発生する。

図-2からも分かるとおり、公印付与、受領確認などのプロセスにおいて、メールプロトコルが適していないことが分かる。したがって、公文書交換ではアプリケーション基盤を用いて公文書の送受信中に発生するトランザクション(送信、受信、受領確認、受領否認など)を公証基盤に委ねながら稼働するアプリケーションとしての構築を行った。また、公文書起案後の公印付与は認証基盤より発行される証明書を用い、デジタル署名を行うなど公文書の真正性確保を行い成果を確認した。ただし、現実的には公文書の取扱いについては、紙媒体を基本とする条例、規則などが各地方公共団体ごとに定められており、これがすぐに従来の手法に変わるものではな

～文書発信時～



～文書受信時～



図-2 行政文書の事務フロー概略  
Fig.2-Outline of administrative document procedure flow chart.

いことは「総合行政ネットワーク構築に関する調査研究最終報告」にも記されているとおりである。

### (2) Webアプリケーション

Webアプリケーションでは各種データベースの検索システムなどを構築したが、これに関しては、総合行政ネットワーク内でしか閲覧できないことを除けば取り立てて論ずるものではない。ただし、総合行政ネットワークの発展のためにWebアプリケーションは欠かせないアイテムとして注目されており、今後、様々なアプリケーションを展開していく中でアプリケーションの作りに極力影響を与えない仕組みについて環境構築を行った。具体的には、ReverseProxy技術を利用した利用者認証の仕組みがこれに当たる(図-3)。

通常のWebコンテンツは不特定多数の閲覧者に情報を発信するために規制を設けることは少ないが、業務アプリケーションをWeb技術を用いて構築する場合はアクセスコントロール(利用者を特定した、資源へのアクセス制御)の概念が非常に重要となる。

一般的に行われているのはBASIC認証と呼ばれるユーザID/PASSWORDによる利用者認証であるが、この方式はネットワーク上をユーザID/PASSWORDクリアテキストとして電文が流れるため盗聴の恐れがあり、総合行政ネットワークのセキュリティポリシーには合致しない。そこで今回の実証実験では、認証基盤から発行される証明書をベースに認証を行う仕組みとした。また、この方式を採用することにより、異なるWebアプリケーションへのアクセスの際、煩雑なログオン処理が不要となり、シングルサインオン環境が構築できることになる。

なお、ReverseProxy方式のほかにGetAccess方式も考えられたが、アプリケーション開発のしやすさの観点から今回の実証実験での採用は見送った。

以下は、ReverseProxyによる利用者認証の動作概要である(図-3 ①～⑥)。

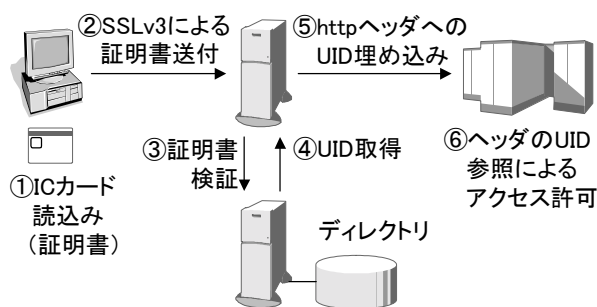


図-3 ReverseProxyによる利用者認証  
Fig.3-User electronic authentication through ReverseProxy.

- ① 利用者はアクセス制限されているWebアプリケーションにアクセスする際、ICカードから証明書をブラウザ内に取り込む。
- ② ブラウザ内で取り込まれた証明書はSSLv3 (Secure Socket Layer Version 3) プロトコルによるクライアント証明を行う。
- ③ ReverseProxyサーバは、送信されてきた証明書の検証をディレクトリに問い合わせる。
- ④ 検証結果に問題がなければ、証明書発行時に登録されたUIDがディレクトリサーバから返される。
- ⑤ ReverseProxyサーバはディレクトリサーバから応答されたUIDをhttpヘッダに埋め込み、当該Webアプリケーションサーバへのコネクションを要求する。
- ⑥ コネクション要求を受けたWebアプリケーションサーバはクライアントとのコネクションを確立し、サービスを開始する。

## 実証実験結果

本実証実験で掲げた七つの技術目標について、それぞれにつき実証を行った結果、ほぼすべての項目において正当性および有効性が確認できた。しかし、同時に技術・運用面からいくつかの重大な課題も露呈した。

### (1) 拡張性 (スケーラビリティ)

実証実験では、ある想定した規模でのネットワーク設定やサーバ設置を行った。今後、計画されている2003年度までに全地方公共団体を収容するために必要なパラメータの抽出および設計を行ったが、回線容量 (バックボーン: 1.5 Mバイト, LGWANアクセス: 0.5 Mバイト) を含め、構成についての見直しなどの課題が残った。

### (2) 信頼性 (アベイラビリティ)

総合行政ネットワークは24時間365日稼働を目指しているが、実証実験の限られた資源と時間の中ではファシ

リティも含めたすべての資源を2重化することはできなかった。(7) の費用対効果との兼ね合いも含め、SLAレベルの策定など、運用設計を更に進める必要がある。

### (3) ネットワーク性能

本運用時のネットワークトラフィックについては、想定での設計・構築を行ったが、接続団体数の増加やWebアプリケーションサービスが立ち上がるごとに、加速度的にトラフィックが増加することが予想される。これに関しても(7)の費用対効果に影響する部分であるが、ネットワーク性能、QoS (Quality of Service) を含めた設計変更を余儀なくされることが予想される。

### (4) セキュリティ

先にも述べたとおり、ファイアウォールやIDSの冗長構成により、現時点ではかなりハイレベルなセキュリティネットワークが構築された。ただし、使いやすさとは相反する部分もあることや、今後更なる技術進歩により新たなプロトコルなどが規定された場合への対応など、セキュリティポリシーに関しても継続して検討する必要がある。

### (5) 運用管理 (マネージャビリティ)

運用監視のシステムとしては、一定の評価を出したが、これもネットワークの増大化に伴い管理対象の増加が見込まれる。これに対応できる運用面も含めた管理体制についても課題を残した。

### (6) 柔軟性 (アダプタビリティ)

ネットワークの観点からは、都道府県WANとの接続性をもとに、とくにEthernet接続による技術検証を行ったが、日本の地理特性を考えた場合、管下に島嶼を抱える都道府県も多数あることから、無線などを含まないいくつかの収容技術についても検討が必要であると考えられる。

### (7) 費用対効果 (TCO)

先にも述べてきたとおり、全地方公共団体を収容するためには、回線種別を含めた容量の見直し、信頼性を担保するための設備の2重化、これに伴う管理システムや体制の確立など、費用に直結してしまう問題を多く抱える結果となった。

実証実験はこれらの結果と課題を残して終了したが、これらの課題解決をどう行っていくかが、総合行政ネットワークの有効活用の観点からも重要である。

## む す び

本稿の執筆時点では、これらの課題解決に向け関係各

位が検討を開始している。全国規模のネットワークという観点では、ISP (Internet Service Provider) などがこれと同じ悩みをクリアしながら、我々にサービスを提供していると考えられるが、ISPの技術が総合行政ネットワークにすぐに直結するものではないかも知れない。しかし、要素技術あるいは解決手法として得るものは多くあることもまた事実である。

総合行政ネットワークは電子政府を実現するためのインフラストラクチャとして、非常に意義のあるネットワークであり、地方公共団体を始めとした行政体の情報化が加速度的に発展するトリガでもある。今年度には約

400団体、2003年までに全団体に展開を予定している。

早期にこれらの問題をクリアし、政府のIT戦略本部が標榜する「e-JAPAN戦略」の礎となることを期待する。

### 参考文献

- (1) ー：ミレニアム・プロジェクト（新しい千年紀プロジェクト）について。内閣総理大臣決定，1999.12.
- (2) 自治大臣官房情報政策室：総合行政ネットワーク構築に関する調査研究 最終報告。平成12年3月.
- (3) 総務省 自治行政局 地域情報政策室：総合行政ネットワーク構築に関する実証実験報告書。平成13年3月.