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

総務省　自治行政局　地域情報政策室

はじめに

２１世紀を迎え、さらに社会・経済活動の構造変化の加速度が増し、インターネットの爆発的普及や電子商取引の発展に代表されるように急速にデジタル・ネットワーク化が進行している。その変化を推進しているのがＩＴである。こうしたいわゆるＩＴ革命の進展は、行政の在り方にも大きな影響を及ぼしつつある。

我が国においては、平成６年１２月２５日に閣議決定した「行政情報化推進基本計画」を平成９年１２月２０日に改定し、２１世紀初頭に高度に情報化された行政、すなわち「電子政府」の実現を目指すという方針が示された。また、「ミレニアム・プロジェクト（新しい千年紀プロジェクト）」（平成１１年１２月１９日内閣総理大臣決定）により、「平成１５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、地方公共団体の電子政府化を先導する実証実験として「総合行政ネットワークに向けた実証実験等」が平成１２年度のプロジェクトの一つとして挙げられた。

平成１２年度に実施した「総合行政ネットワークに関する実証実験」は、平成９年度から平成１１年度にわたり「総合行政ネットワーク構築に関する調査研究」によって進められてきた、ネットワーク構築・運営手法、ネットワークを流通させる行政情報の定義、既存の紙を主体とした行政情報の流通をネットワークによる電子的な流通に置き換えた場合の技術面・運用面等の諸課題の検討結果を検証し、「総合行政ネットワーク構築仕様書」として提示するために実施したものである。この成果を踏まえ、平成１５年度末までに、各地方公共団体の自主的な取り組みにより、総合行政ネットワークが整備されるとともに、これと国の霞が関ＷＡＮとの接続が図られることを期待する。

本実証実験が地方公共団体の情報化推進と併せ、行政サービス向上の一助になることを期待するとともに、本実証実験を進めるに当たって御協力いただいた多数の方々に対し、心から御礼申し上げる次第である。

平成１３年３月

総務省自治行政局
地域情報政策室長　髙﨑一郎

総合行政ネットワーク構築に関する実証実験推進委員会

1　委員会開催日

第1回　平成12年8月25日

実証実験の基本設計、セキュリティ設計及び、スケジュールについての検討

第2回　平成12年10月30日

実証実験の設計概要、実施要領についての方向性及び実現性の検討。
システム監査実施計画の検討。

第3回　平成13年2月28日

基盤系実証実験構築報告、電子文書交換デモンストレーション及び、認証システムについての評価・検討。地方公共団体のドメイン名についての検討。

第4回　平成13年3月27日

実験結果、実験報告書の評価及び、本構築スケジュールについての検討。
システム監査報告。

2　推進委員名簿(敬称略)

委員長	
須藤　修	東京大学大学院情報学環教授
委員長代理	
新免　國夫	岡山県企画振興部情報政策課参与(情報政策課長)
委員	
森田　宏樹	東京大学大学院法学政治学研究科教授
芝　勝徳	神戸市外国語大学助教授
髙﨑　一郎	自治大臣官房情報政策室（H12.7.10～H13.1.5）
	総務省自治行政局地域情報政策室室長（H13.1.6～H13.3.31）
清水　孝治	北海道総合企画部情報政策課課長補佐
菅原　嘉男	青森県企画部情報政策課参事（情報政策課長）
古澤　眞作	岩手県企画振興部情報科学課課長
高橋　幸夫	宮城県企画部情報政策課課長
五嶋　青也	秋田県企画振興部情報企画課課長
三澤　雄一	山形県企画調整部情報企画課課長
尾形　憲一	福島県企画調整部情報政策課課長
坂本　理	茨城県企画部情報政策課課長
高橋　祐司	群馬県企画部情報政策課課長
西村　和純	埼玉県総務部情報政策課課長
大村　禎一	千葉県総務部情報システム課課長

小林　正樹	東京都総務局総務部情報システム管理課副参事
三角　秀行	神奈川県企画部情報システム課課長
中野　雅至	新潟県企画調整部情報政策課課長
棚瀬　佳明	富山県情報企画課課長
高本　隆	石川県企画開発部情報政策課課長
青山　秀四郎	福井県総務部情報政策課課長
林野　旻	山梨県企画部情報政策課課長
牛越　徹	長野県企画局情報政策課課長
川出　達恭	岐阜県経営管理部情報システム課電子県庁推進室室長
村松　靖則	静岡県企画部高度情報総室総室長
長崎　栄一	愛知県企画振興部情報企画課課長
西村　真哉	三重県地域振興部情報政策課技師
永谷　正夫	滋賀県企画県民部情報統計課管理監（情報統計課長事務取扱）
里中　純一	京都府企画環境部情報システム課課長
明石　亮一	大阪府総務部情報システム推進課課長
熊田　和仁	兵庫県企画管理部教育・科学技術局情報政策課課長
樫根　成憲	奈良県総務部情報システム課主査
蟹江　健一	和歌山県企画部情報システム課課長
岡村　俊作	鳥取県企画部情報政策課課長
月森　憲三	島根県総務部情報システム課課長
日當　康典	広島県総務企画部情報政策課課長
佐本　敏朗	山口県企画振興部情報企画課課長
一宮　省一	徳島県企画調整部情報政策室室長
森高　勝	香川県企画部情報政策課課長
佐伯　満孝	愛媛県企画情報部情報政策課課長
大庭　孝之	高知県企画振興部情報企画課課長
出嶋　大介	福岡県企画振興部高度情報政策課課長
赤司　邦昭	佐賀県企画県民部地域・情報政策課課長
池田　和明	長崎県総務部電算システム課課長
中川　芳昭	熊本県企画開発部情報企画課課長
河野　功	大分県企画文化部統計情報課情報企画室室長
日高　義郎	宮崎県企画調整部情報政策課部参事兼課長
納山　栄樹	鹿児島県企画部新技術情報課課長
儀間　朝昭	沖縄県企画開発部情報システム課課長

加藤	正晴	札幌市情報化推進部情報調整課情報化推進担当課長
秋山	博信	仙台市企画局情報統計課課長
林	光春	千葉市総務部情報管理課課長
手塚	誠	横浜市総務局事務管理部情報化推進課課長
栗山	久史	川崎市総務局情報管理部システム企画課課長
恒川	平章	名古屋市総務局企画部主幹
小林	正雄	京都市総合企画局情報化推進室室長
金森	幹仁	大阪市総務局行政部情報企画課情報企画課長代理
多田	淳	神戸市企画調整局情報企画部ﾏﾙﾁﾒﾃﾞｨｱ推進課高度情報化担当主幹
西村	斉時	広島市企画総務局情報システム課情報担当課長
井上	憲八郎	北九州市総務局総務部情報管理課課長
四宮	祐司	福岡市総務企画局総務部課長（全庁ＯＡシステム推進担当）

専門委員

竹内	雅彦	自治大臣官房情報政策室理事官（H12.7.10～H13.1.5）
高井	龍一	自治大臣官房情報政策室管理係長（H12.7.10～H13.1.5）
海老原	諭	総務省自治行政局地域情報政策室課長補佐（H13.1.6～H13.3.31）
三和	英治	総務省自治行政局地域情報政策室地域情報専門官（H13.1.6～H13.3.31）

総合行政ネットワーク構築に関する実証実験ワーキンググループ

1　ワーキンググループ開催日

第1回　平成12年7月28日

実証実験の概要説明。総合行政ネットワークの接続条件とセキュリティポリシィの検討。実証実験に係る参加団体の共通的課題の抽出。

第2回　平成12年8月23日

実証実験の基本設計、セキュリティの考え方及び、スケジュールについての検討。

第3回　平成12年10月25日

実証実験の基本設計、詳細設計及び、セキュリティ設計についての検討。

第4回　平成13年2月21日

基盤系実証実験構築報告、電子文書交換デモンストレーション及び、認証システムについての検討。地方公共団体のドメイン名についての検討。

第5回　平成13年3月23日

実験結果、実験報告書の検討及び、本構築スケジュールについての検討。

2　ワーキンググループ委員名簿(敬称略)

委員長

芝　　勝徳　　神戸市外国語大学助教授

委員長代理

国枝　信男　　岐阜県経営管理部情報システム課電子県庁推進室課長補佐

委員

竹内　雅彦　　自治大臣官房情報政策室理事官（H12.7.10～H13.1.5）

高井　龍一　　自治大臣官房情報政策室管理係長（H12.7.10～H13.1.5）

海老原　諭　　総務省自治行政局地域情報政策室課長補佐（H13.1.6～H13.3.31）

三和　英治　　総務省自治行政局地域情報政策室地域情報専門官（H13.1.6～H13.3.31）

村山　卓　　総務省自治行政局地域情報政策室主査（H13.1.6～H13.3.31）

黒川　恵司朗　自治大臣官房情報政策室自治事務官（H12.7.10～H13.1.5）
総務省自治行政局地域情報政策室総務事務官（H13.1.6～H13.3.31）

酒井　隆　　北海道総務部法制文書課主任

高田　英明　　北海道総合企画部情報政策課主任

池田　浩彰　　福島県総務部文書学事課主事

山村　浩一　　福島県企画調整部情報政策課副主査

水野　康夫　　神奈川県総務部法務文書課副主幹

加藤　友義　　神奈川県企画部情報システム課主幹

浅井　寛　　新潟県総務部文書私学課副参事
明間　聡　　新潟県企画調整部情報政策課主任
内藤　玉樹　岐阜県経営管理部法令政策課課長補佐兼文書係長
土屋　順広　静岡県総務部私学文書管理室文書管理主幹
平井　隆一　静岡県企画部情報システム室主査
小林　巖　　愛知県総務部総務課主査
大野　智靖　愛知県企画振興部情報企画課主任
世登　武　　大阪府総務部法制文書課主査
平田　博文　大阪府総務部情報システム推進課主査
久長　正和　兵庫県企画管理部管理局文書課課長補佐兼文書管理・公益法人係長
土井　博雅　兵庫県企画管理部教育･科学技術局情報政策課主査（H12.7.10～9.30）
横山　淳　　兵庫県企画管理部教育･科学技術局情報政策課事務吏員(H12.10.1～H13.3.31)
渡辺　謙二　岡山県総務部総務学事課主査
小田　敬三　岡山県企画振興部情報政策課主事
若林　清美　広島県総務企画部総務課専門員
坂本　信義　広島県総務企画部情報政策課主任
山崎　隆志　高知県総務部文書学事課課長補佐
西岡　輝幸　高知県企画振興部情報企画課主幹
坂本　秀文　大分県総務部総務課主幹兼文書係長
渡辺　文隆　大分県企画文化部統計情報課情報企画室主査
坪水　満　　鹿児島県総務部学事文書課主幹兼文書係長
加世田　登　鹿児島県企画部新技術情報課OA推進係長
大木　将彰　横浜市総務局事務管理部情報化推進課課長補佐
山口　健太郎　横浜市総務局事務管理部情報化推進課技術吏員
久保田　幸三　京都市総合企画局情報化推進室情報化推進課担当係長
清水　和孝　京都市総合企画局情報化推進室情報化推進課（H12.7.10～10.31）
長村　邦弘　京都市保健福祉局衛生公害研究所（H12.11.1～H13.3.31）
古田　隆　　神戸市行財政局行政部新行政システム課主査
神木　与治　神戸市企画調整局情報企画部マルチメディア推進課技術職員

目次

1. 実証実験概要と目的

1.1 総合行政ネットワークの目的

総合行政ネットワーク（以下、「LGWAN[注1)]」という。）は、政府のミレニアムプロジェクト（平成11年12月19日内閣総理大臣決定）において、地方公共団体における電子政府の基盤と位置付けられている。LGWANは、地方公共団体の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、情報の共有による情報の高度利用等を図ることにより、各地方公共団体と国の各省庁及び住民等との間の情報交換手段の確保のための基盤とすることを目的とする。

注1) LGWAN：Local Government Wide Area Network

1.2 実証実験の概要

総務省（旧自治省）において、平成9年度から平成11年度まで行われた「総合行政ネットワーク構築に関する調査研究」において、実際にネットワークを構築・運営することにより初めて明らかになる技術面・運用面等の課題も存在することが予想されたため、これらの課題の洗い出し及び解決を図るため下記のようなコンセプトと目的のもとに「総合行政ネットワーク構築に関する実証実験」（以下、「実証実験」という。）を行った。

- 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、電子文書交換等の業務横断的サービスを提供。
- 高いセキュリティを確保（ISO/ISE 15408等準拠を目標）。
- 霞が関WANとの相互接続。
- 情報通信分野における標準的な技術を採用。
- 各市町村や都道府県におけるネットワーク規模、多様な情報化の進度や方法の違いを吸収。
- すべての地方公共団体が現実的に負担できる費用で運用。
- 地方公共団体が持つ既存設備の有効利用。

また、実証実験は、平成12年4月から、本構築時のネットワークの最大規模を前提とした運営主体と、58団体（都道府県46団体、政令指定都市12団体）の地方公共団体による拡張性を十分にもつ小規模な実証実験ネットワークを設計し、構築を行った。更に、実験主体を組織し、具体的な業務の模擬的な運用や、ネットワーク内で提供される意義が高いコンテンツを選定しつつ、段階的に実験運用を行っていくこととした。その結果のトラフィックの種別や量を測定し、ネットワークの最適化を図り、また、本構築・本運用に必要な規定類を文書化し整備することとした。

実証実験と本構築・本運用時との違いは、以下のようになる。

〇実証実験（平成12年度）

・接続地方公共団体数：58団体

・運用時間：基本的に勤務時間内

〇本構築・本運用（平成13年度以降）

・接続地方公共団体数：47都道府県を始め、順次すべての地方公共団体の接続を予定

・運用時間：原則として24時間運用（定期点検など計画停止については別途考慮）

なお、地方公共団体を相互に接続する総合行政ネットワークと国の行政機関のネットワークである霞が関WANとの相互接続の要件等については、今後国の行政機関と検討・調整する予定である。

1.3 実証実験の技術目漂

実証実験における技術目標は以下のとおりとした。

・拡張性（スケーラビリティ）

当初58団体から始めてすべての地方公共団体を収容できることを目標に設計・構築した。また、団体の規模にかかわらず同等のサービスができることを目標とした。

・信頼性（アベイラビリティ）

原則として24時間運用可能なネットワークを目標とした。また、各主体間での具体的なサービスレベルの合意や、業務アプリケーションの要求を根拠に稼働率を設定することとした。

・ネットワーク性能

すべての業務アプリケーション運用に十分な性能を確保し、また、アプリケーションの要件に応じた通信路分離や品質保証ができることを目標とした。

・セキュリティ

総合行政ネットワークに対して考えられる脅威を確定し、それらに対応した暗号化、信号／経路分離、ファイアウォール機能、監視、リアルタイム追跡、代替え経路等の技術要素を実装した。また、検証、監査／検査、ペネトレーションテスト等の運用技術も確立することとした。

・マネージャビリティ

性能管理、故障管理、ネットワークデバイスを遠隔操作できる技術を導入することとした。

・柔軟性（アダプタビリティ）

将来の新技術の採用を妨げない設計とし、また、後述するASPの概念と技術を取り込むことにより多彩なアブリケーションが展開されるようにした。

・費用対効果

アベイラビリティやネットワーク性能とセキュリティのバランスをとりながら各団体の規模に応じた適切な費用で運用できることを目標とした。

1.4 実験項目概要

⑴物理層・データリンク層

MPLS網により、LGWANバックボーン回線、LGWANアクセス回線を構築した。また、LGWANアクセス回線として都道府県WANを利用する場合の技術検証を行った。

⑵ネットワーク層

TCP/IPをベースにネットワーク整備を行い、暗号化、セキュリティ、ルーティング、IPアドレスデザインなどの技術検証を行った。

⑶基本プロトコル群

アプリケーションが使用する基本的なプロトコルサービス（DNS、NTP、SMTP等）についてサーバ配置を行い、実装上の技術検証を行った。

⑷アプリケーション基盤

各アプリケーション共通に必要な機能である、認証基盤、ディレクトリ基盤、証明書検証、公証基盤、XML電文交換基盤を切り出し、統一的にサービスする基盤として整備した。

⑸基本サービス

アプリケーション基盤と連動し、運営主体が提供するサービスのサンプルアプリケーションとして、電子文書交換とWWWアプリケーションを構築した。基本サービスの構築に基づき、ＡＳＰガイドラインの作成を行った。

⑹管理システム

ネットワーク監視、セキュリティ監視を行う管理システムの構築を行った。

2. 総合行政ネットワークの構成概要

2.1 全体構成

総合行政ネットワークは、全体の施設設備である全国NOC[注2)]、
都道府県に設置される施設設備である都道府県NOC[注2)]、
及び地方公共団体により構成される。
これらは、LGWANバックボーン回線、LGWANアクセス回線によって接続される。

[注2)] NOC (Network Operation Center)：ネットワーク・オペレーション・センター

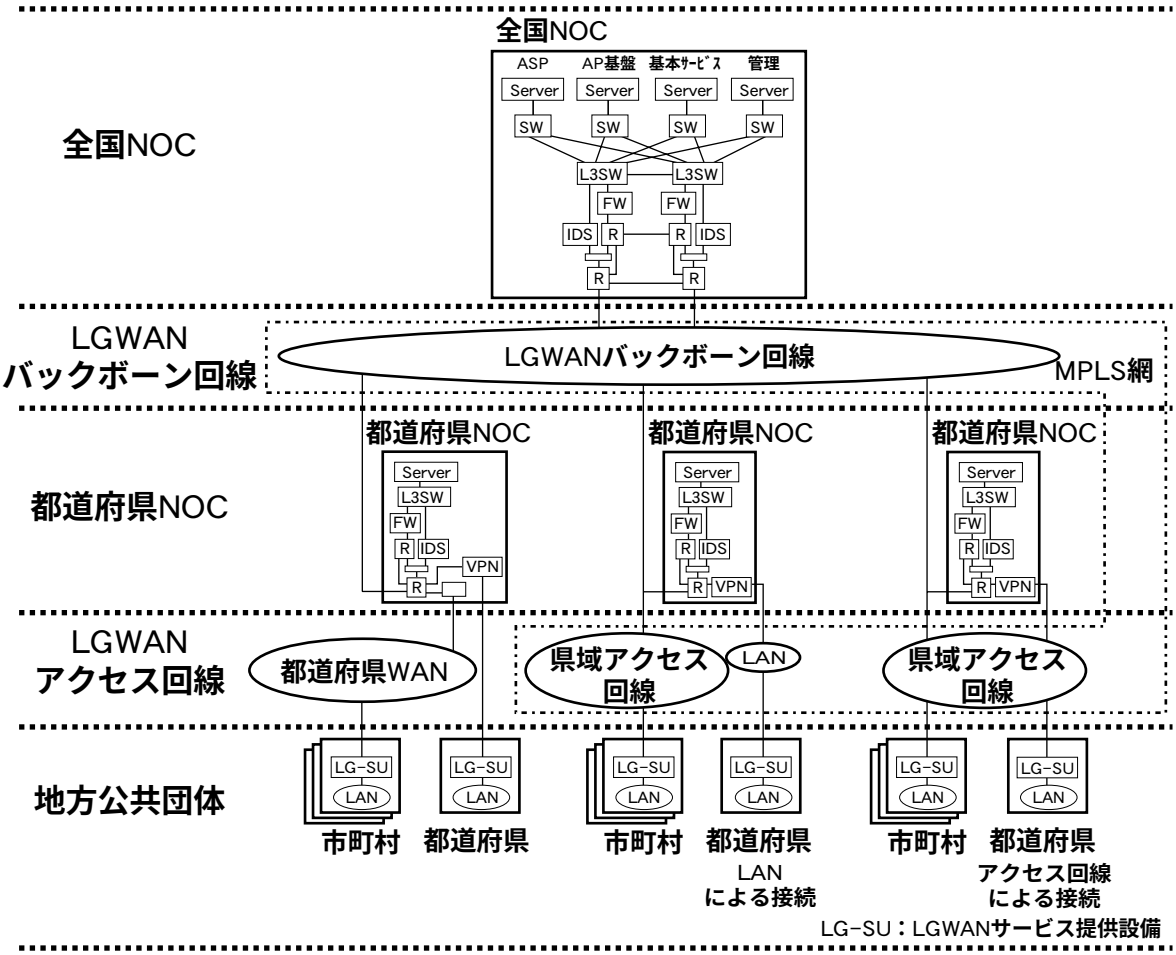

図 2-1 全体構成

2.2 全国NOC

全国NOCとは、総合行政ネットワーク専用の施設として設置されるNOCである。各都道府県に設置される複数の都道府県NOCを接続し、総合行政ネットワーク全体の運用及び管理を行う施設である。

2.3 LGWANバックボーン回線

LGWANバックボーン回線とは、全国NOCと各都道府県NOC間を接続するMPLS網である。

2.4 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都道府県に設置されるNOCである。管下の市町村のLANを収容、集線して全国NOCに接続するとともに、都道府県管内の市町村の相互ネットワーク接続を行う施設である。

都道府県NOCは、別途運営主体から示される「都道府県NOC設置ファシリティ条件」を充足する施設を、原則都道府県の庁舎内に用意するものとする。ただし、施設が準備できない場合は、「都道府県NOC設置ファシリティ条件」を充足する施設を有する事業者等のハウジングサービスを利用することも可能とした。

実証実験においては、具体的な設置場所の選定基準として表2-1に示す条件を満たすことを前提とした。

表 2-1 都道府県NOC設置ファシリティ条件

No	要件
1	機器設置予定場所は専用の情報システム機器設置設備（マシンルーム）であること
2	隣接建物、回線等からの延焼防止措置が施されていること 建物の構造は鉄筋コンクリートであること 屋外からの引きこみ口には延焼防止処置が施されていること
3	機器設置室の出入口には入退室管理システム等を設置し、不正侵入等に対する 監視・管理処置等の防止措置が施されていること 機器設置場所の出入り口は２箇所以下であること
4	水を使用した消化設備や配水管設備（空調設備を除く）が無いこと 屋外側の窓、外壁、天井及び床からの雨水等の浸入が無いこと
5	室内は延焼防止区画であること 床、壁、天井等の内装には不燃材を使用していること
6	床、壁等の内装には帯電防止材を使用していること
7	照明器具は固定され、落下防止措置が施されていること 天井は固定され、落下防止措置が施されていること
8	室内の環境は、腐食性ガス、振動、塵埃が発生しないこと
9	消火設備はハロゲン（又は新ガス）方式であること
10	情報システム機器、データ保管設備、電源設備、空調設備、通信設備等に対しては 以下のいずれかの転倒防止処置が出来ること ①架台の使用　②耐震ベースの使用　③床に直接固定
11	供給電源はAC100V±5%以内の電圧と所要電力を安定的に供給できること
12	空調設備が必要な能力を安定的に保持し、24時間稼働であること

なお、表2-1中No12における空調設備の能力にあっては、サーバの自動電源遮断の温度センサーが40°Cに設定されていることから、ラック内外の温度差を最大13°Cとすると、室内温度は27°C以下が必須であり、室内の温度分布差を考慮すると20°C程度に保つことが求められる。

2.5 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LGWANサービス提供設備とを接続する回線である。

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種類がある。

(1) 県域アクセス回線

都道府県NOCと各地方公共団体間を総合行政ネットワークが利用するMPLS網を使用して接続する場合には、LGWANアクセス回線に使用されたMPLS網を県域アクセス回線と呼ぶ。

(2) 都道府県WAN

都道府県が独自の網を用意して各地方公共団体間を接続する場合にはLGWANアクセス回線として使われる都道府県の独自網を都道府県WANと呼ぶ。

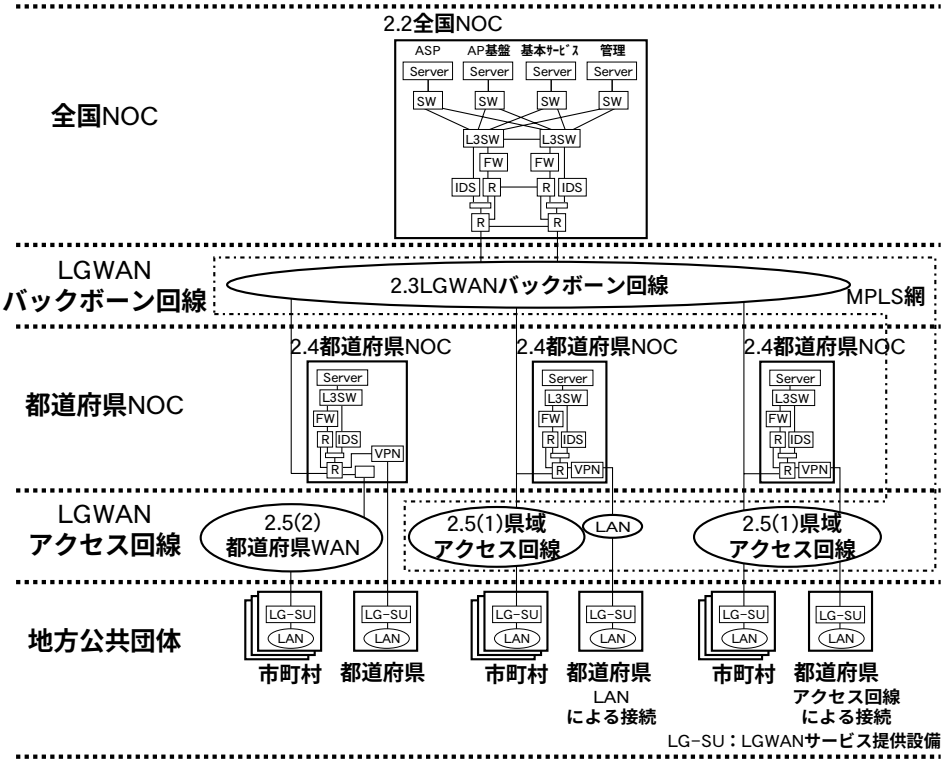

図 2-2 全国NOC・LGWANバックボーン回線・都道府県NOC LGWANアクセス回線

2.6 総合行政ネットワーク全体構成

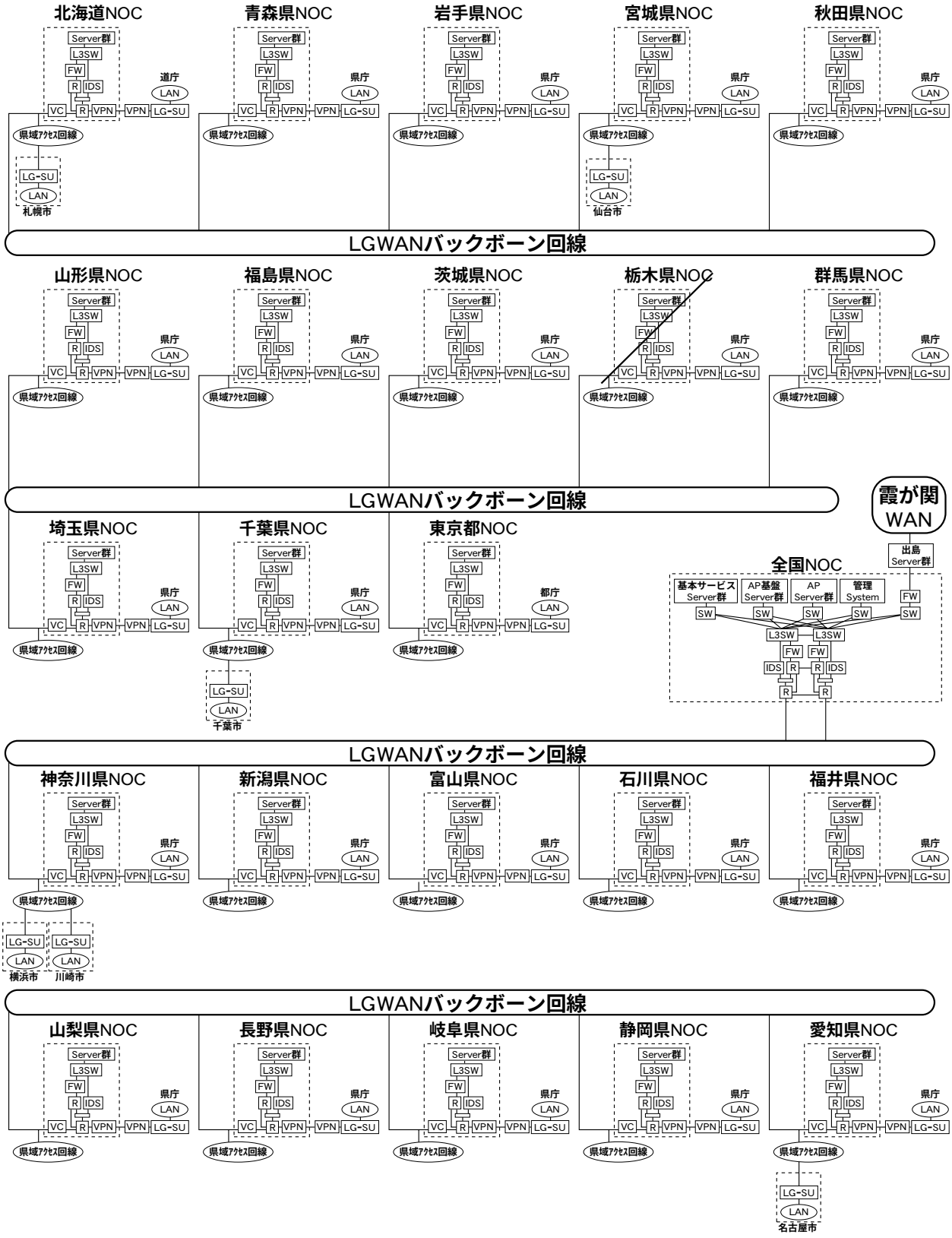

図 2-3 総合行政ネットワーク全体構成(1/2)

図 2-4 総合行政ネットワーク全体構成(2/2)

2.7 セキュリティ境界面

(1)セキュリティ保護の考え方

総合行政ネットワークのセキュリティ保護対象となる機器の集合は、LGWANの構造にしたがい、以下の領域に分割した。

1）全国NOC設備

2）都道府県NOC設備

3）LGWANサービス提供設備

また、以下の外部ネットワークをLGWANと接続することとした。

1）霞が関WAN

2）地方公共団体LAN

総合行政ネットワーク内の分割された各領域は、同じセキュリティレベルに属するものであり、各要素間をまたがるアクセスはセキュリティポリシーに従いコントロールすることとした。

具体的には、全国NOCと都道府県NOC 、また都道府県NOCとLGWANサービス提供設備の間、すべてにセキュリティ上の障壁を設けた。万一、特定の領域でセキュリティ侵害行為が発生した場合にも、障壁により他領域に被害が広がることを防止できる階層的な構造とした。

(2)セキュリティ境界面

保護対象とセキュリティ領域を更に詳細に規定したものを、図2-5に示す。AからIのシステム層を縦軸座標とし、０から１０の領域層を横軸座標とした。この座標空間では、総合行政ネットワークの範囲は網掛けで示す領域である。総合行政ネットワークと外部との境界面は以下のものがある。

・境界面１：地方公共団体と総合行政ネットワークとの境界面。
・境界面２：総合行政ネットワークと霞が関WANとの境界面。
・境界面３,４：地方公共団体へのLGWANアクセス回線に都道府県WANを使用した場合の境界面。
・境界面５：地方公共団体が、広域行政ネットワーク運営主体の管理下において、ASPの提供するアプリケーションサービスを受ける場合の境界面。
・境界面６：都道府県NOC設備を設置するファシリティに関する境界面。
・境界面７：広域行政ネットワーク運営主体が地域の地方公共団体に対して、アプリケーションサービスを実施する場合の境界面。
・境界面８：総合行政ネットワーク上でサービスを提供するアプリケーション開発等の共 通のアプリケーション開発基準を定める境界面。
・境界面９：広域行政ネットワーク運営主体が地域の地方公共団体に対して、アプリケーションサービスを実施する場合の境界面。

セキュリティ境界面と組織の関連を図2-6に示す。

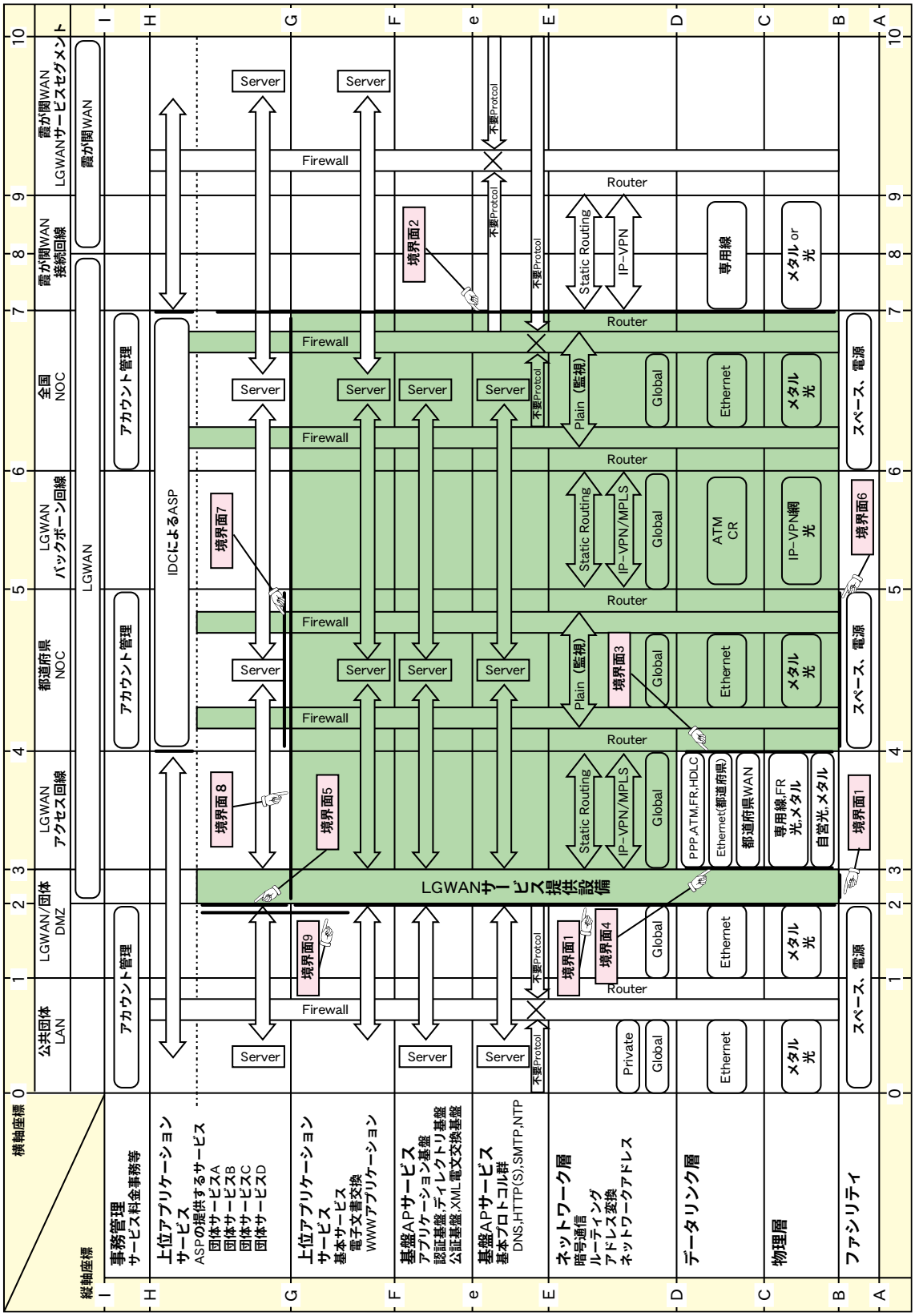

図 2-5 セキュリティ境界面

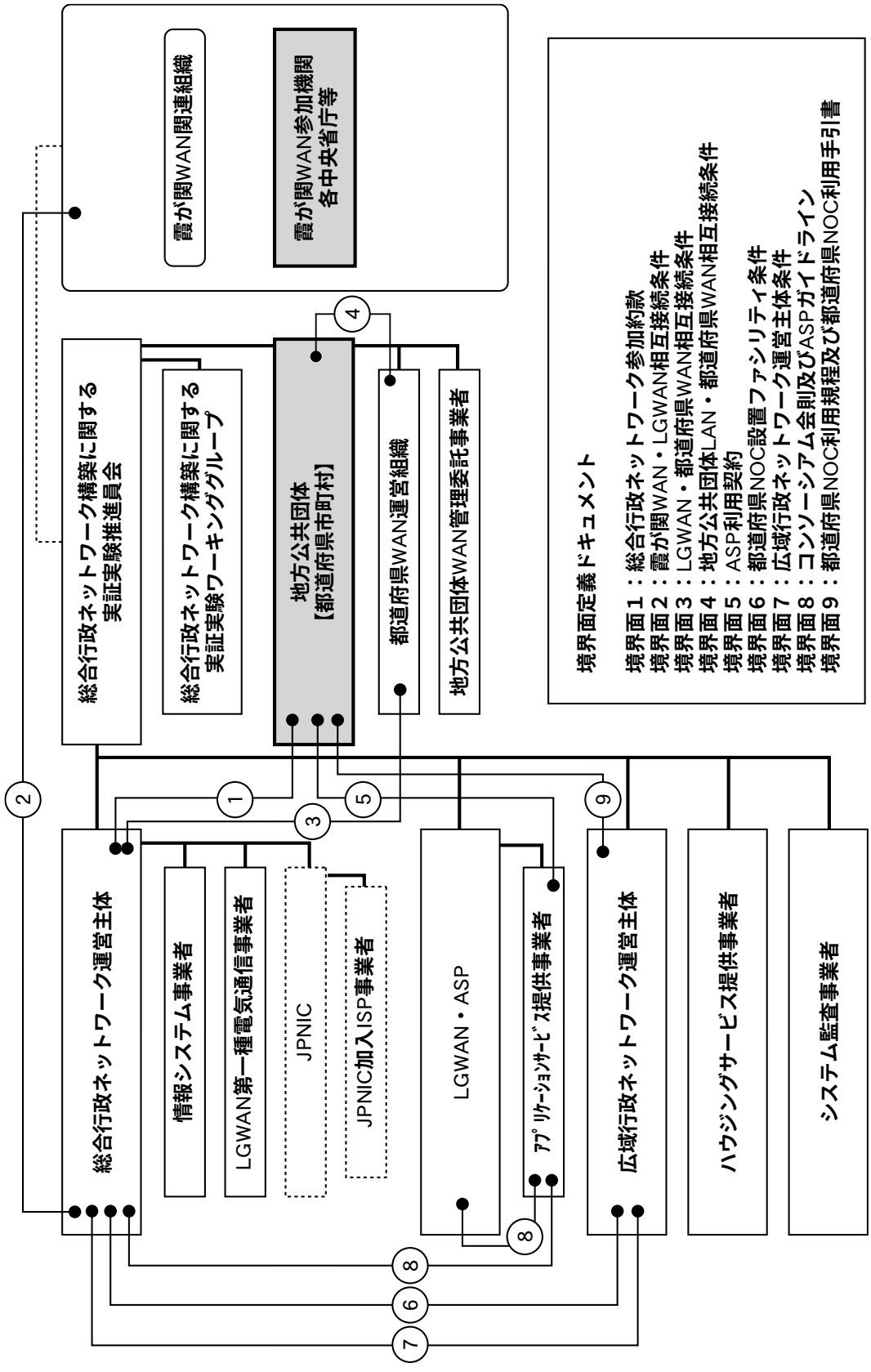

図 2-6 セキュリティ境界面と組織の関連

2.8 アプリケーションの区分

総合行政ネットワーク上で提供されるアプリケーションサービスの区分は以下のとおりである。

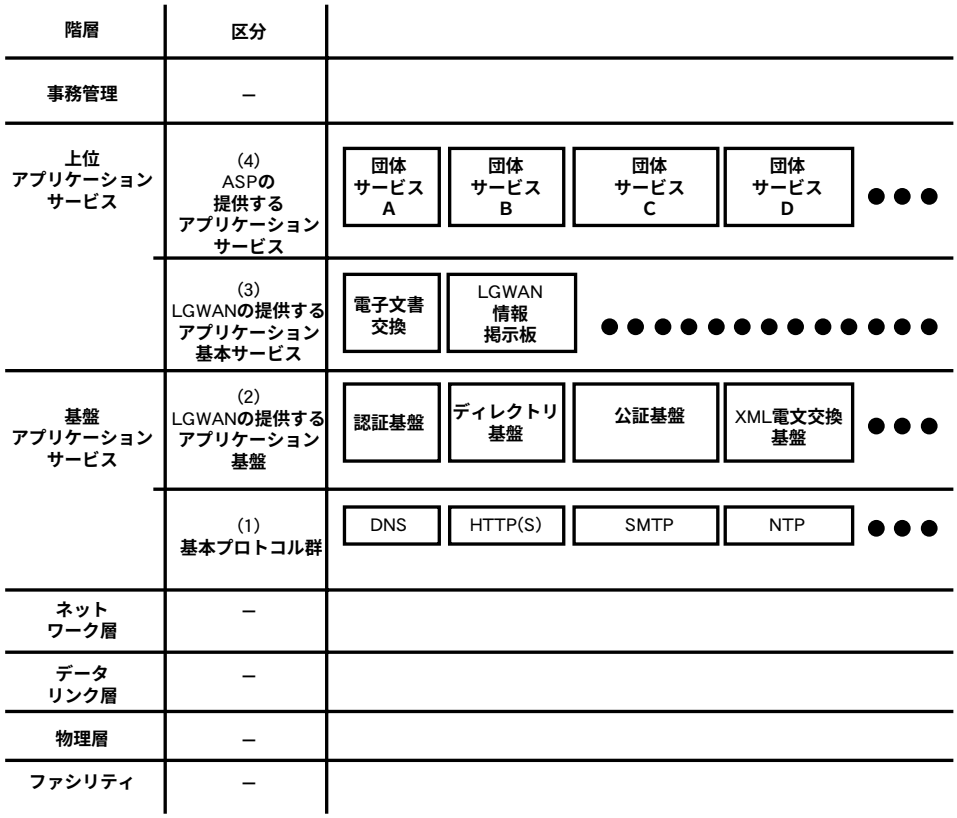

図 2-7 アプリケーションの区分

(1)基本プロトコル群

一般的なインターネットプロバイダーが提供する基本的なサービスと同様のサービスとして、DNS、HTTP(S)、SMTP、NTPなどのプロトコルをサービスする。

(2)アプリケーション基盤（AP基盤）

アプリケーション基盤は、各アプリケーションに共通の機能を切り出して統一的にサービスする基盤であり、認証基盤、ディレクトリ基盤、公証基盤、XML電文交換基盤などが含まれる。

(3)基本サービス（LGWANの提供するサービス）

アプリケーションサービス基盤と連動して、総合行政ネットワーク運営主体が提供するサービスであり、電子文書交換、WWWアプリケーション（LGWAN情報掲示板など）がある。

(4)ASPの提供するサービス（アプリケーションサービス）

総合行政ネットワークの利用団体が独自に提供するアプリケーションサービスはASPを通じて提供される。

3. 物理層・データリンク層

3.1 実験項目と内容

(1)LGWANバックボーン回線

総合行政ネットワークで必要となるバックボーン回線は、閉域性、全国均一料金体系、大容量帯域、スケーラビリティ、SLA（Service Level Agreement）提示を持つネットワークである必要がある。

これらの要件を満たすものとして、閉域IPネットワークサービス（MPLS（Multi Protcol Label Switching）の技術を用いた回線サービス）を利用し、全国NOCと各都道府県NOC間を結ぶ実証実験用ネットワークの構築を行った。

(2)LGWANアクセス回線

都道府県NOCと地方公共団体のLGWANサービス提供設備とを結ぶLGWANアクセス回線は、次の 2 ケースを対象に実証実験用ネットワークの構築を行った。

・MPLS網である県域アクセス回線を利用するケース

・各都道府県が独自に構築整備を行っている都道府県WANを利用するケース

都道府県WANについてはアクセス回線技術仕様の実証実験を行った。

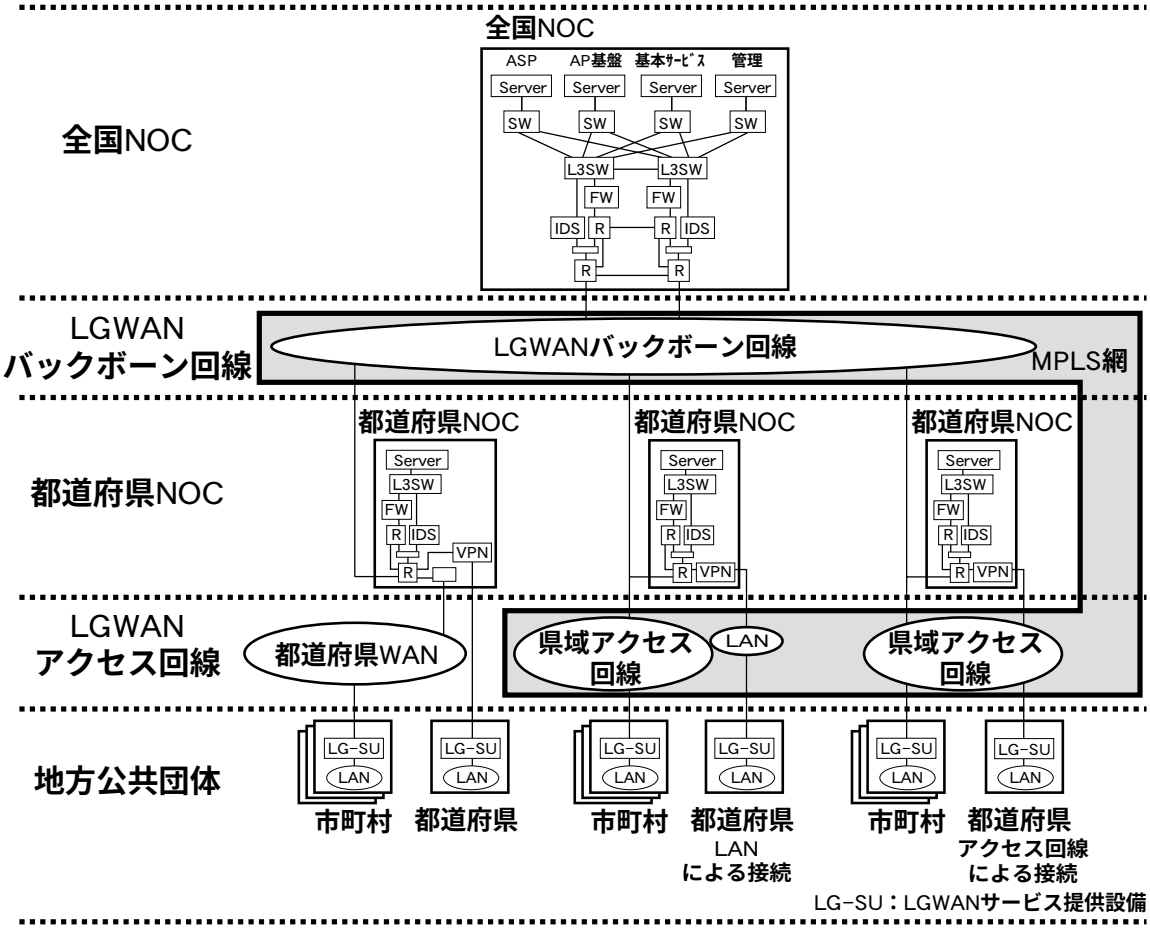

図 3-1 MPLS網の利用範囲

3.2 LGWANバックボーン回線の実証実験結果

LGWANのMPLS網は、物理的には都道府県及び市町村をフラットに接続し、論理的にはVPN-IDによる識別を行うCUGで、LGWANバックボーン回線と各県域アクセス回線を区分する構成とした。

全国NOCと各都道府県NOCが、LGWANバックボーン回線に接続する回線は、ATM伝送方式を採用した。

各都道府県NOCはPCR（Peak Cell Rate：上限転送速度）0.5Mbps，SCR（Sustainable Cell Rate：保証転送速度）128kbpsでMPLS網と接続した。

全国NOCはPCR3Mbps,SCR1.5MbpsでMPLS網と接続した。

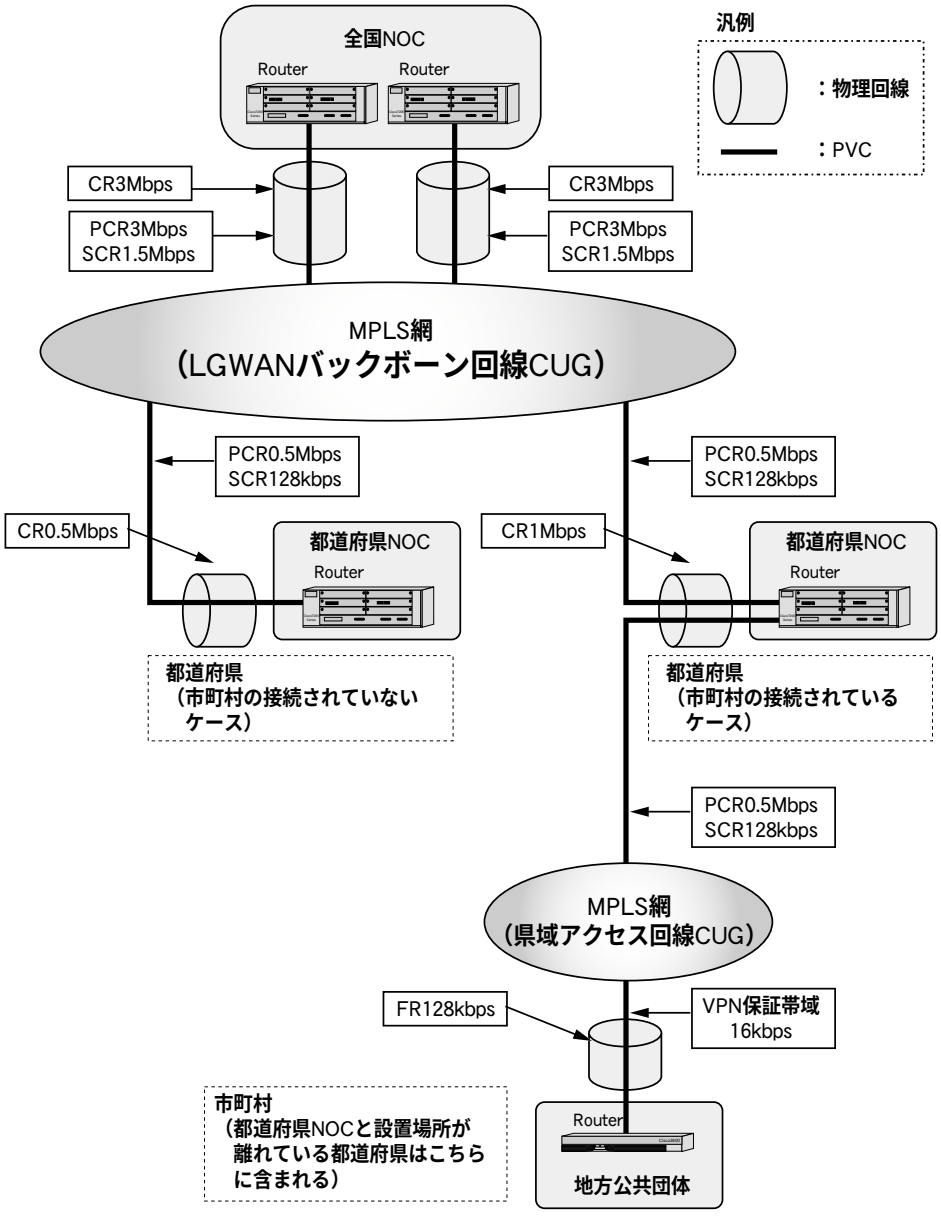

図 3-2 MPLS網による実証実験網の構成

3.3 LGWANアクセス回線の実証実験結果

(1)県域アクセス回線（MPLS網）

各都道府県NOCがLGWANアクセス回線に接続する回線は、ATM伝送方式を採用した（物理回線はLGWANバックボーン回線と兼用した。）。各市町村がLGWANアクセス回線に接続する回線はフレームリレー伝送方式を採用した。

都道府県NOCの回線帯域はPCR（Peak Cell Rate：上限転送速度）0.5Mbps, SCR（Sustainable Cell Rate：保証転送速度）128kbpsでMPLS網と接続した。

各市町村の回線帯域は、128kbps、VPN保証帯域は、16kbpsでMPLS網と接続した。

(2)都道府県WAN

岡山県、広島県にて都道府県WANを使い、LGWANアクセス回線の接続を行った。実際の接続を行う上で、LGWANアクセス回線に都道府県WANを利用する場合、次の要件を満たすことを前提とした。

ア．閉域性

既存データ通信チャネルとは異なる、LGWAN専用チャネルをレイヤ2以下で用意すること。また、接続対象とする地方公共団体以外からはアクセスできないこと。

イ．帯域保証

上記で割り当てたLGWAN専用チャネルは帯域を保証すること。

ウ．常時接続性

都道府県NOC設置場所と地方公共団体を結ぶ回線は、常時接続性を確保すること。

エ．インタフェース条件

都道府県NOC設備及び地方公共団体に設置するLGWANサービス提供設備に対し、Ethernet接続（10BASE-T又は100BASE-TX）方式のインタフェースを提供すること。都道府県NOCには都道府県WANに対してEthernetのポートを一つのみ準備する。

オ．アドレス割当て条件

物理層、データリンク層については、都道府県側の管理となるが、ネットワーク層より上位に関しては、LGWAN側の管理となる。従って、都道府県WANに必要なIPアドレスについては、LGWAN側で用意することを原則とする。

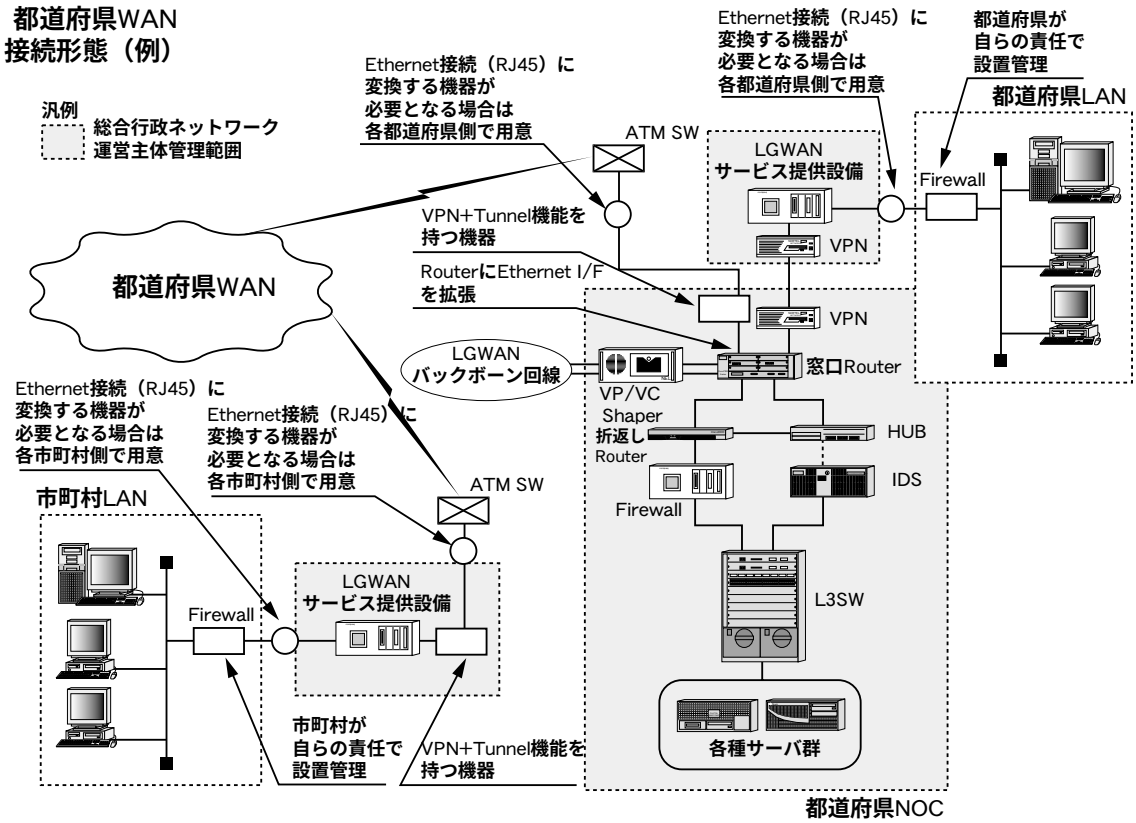

図 3-3 都道府県WANとの相互接続図(例)

3.4 実証実験の考察

(1)LGWANバックボーン回線について

現在の設計では、各県下に10団体程度の接続を想定している。本運用の過程で接続団体数の増加に合わせて、全国NOC～都道府県NOC間の帯域拡大やネットワーク機器の増強を行う必要がある。

(2)LGWANアクセス回線（県域アクセス回線）について

県域アクセス回線では、県域下すべての市町村が、都道府県NOCルータの同一ハードウェアI/Fに同時接続する構成である。ハードウェアI/Fの同時セッション数には限度があり、概ね100セッション単位に物理ポートを設ける必要がある。

よって、市町村が多い都道府県は参加団体の増加に併せてルータ本体の増設を行う必要がある（例、北海道3台、長野・新潟2台等）。また、複数ルータを接続可能な構成とするため、都道府県NOCにおけるネットワーク機器の接続構成を見直す必要がある。

(3)LGWANアクセス回線（都道府県WAN）について

都道府県WANは都道府県域ごとに全く異なった技術で構築されることが予想される（例えば、ダークファイバを使い自営構築、第一種キャリアサービスを活用といった分類以外に、無線技術の利用など通信媒体も様々なケースがありうる）。よって単純なパターン化はできず、LGWANアクセス回線としての技術仕様を満たすか否かについて、判定するための技術審査を行う必要がある。

今後、様々な接続パターンを取りうることを考慮し、より柔軟な構成が取れるように、都道府県NOCにおけるネットワーク機器の接続構成を見直す必要がある。

現時点の都道府県NOCの機器構成では、都道府県WANとの接続用のインターフェース（実証実験の前提ではEthernetポート）は標準状態で装備せず、接続が必要な都道府県のみに追加装備とした。本運用の過程で、新たに都道府県WANにより接続する都道府県域があれば、その時点で、都道府県NOCの窓口ルータに必要なインターフェースの増設を行う必要がある。

4. ネットワーク層

4.1 実験項目と内容

広域ネットワークを構築するためのプロトコルとしてTCP/IPの採用を前提とした。前記の「3.物理層・データリンク層」上で、暗号化、セキュリティ、ルーティング、IPアドレスデザインについて実際にネットワークを構築し、実証実験を行った。

4.2 暗号化の実証実験結果

全国NOCと都道府県NOC間の通信経路及び都道府県NOCと地方公共団体間の通信経路をIPSecで暗号化した。暗号化方式はトリプルDESを採用した。

暗号化処理は機器によって性能が大きく異なり、以下のように使い分けた。

・全国NOC間−都道府県NOC間：ルータに暗号処理アクセラレータを追加

・都道府県NOC−都道府県庁間：VPN専用装置を対向で設置

・都道府県NOC−市町村間：ルータのCPUのみで処理

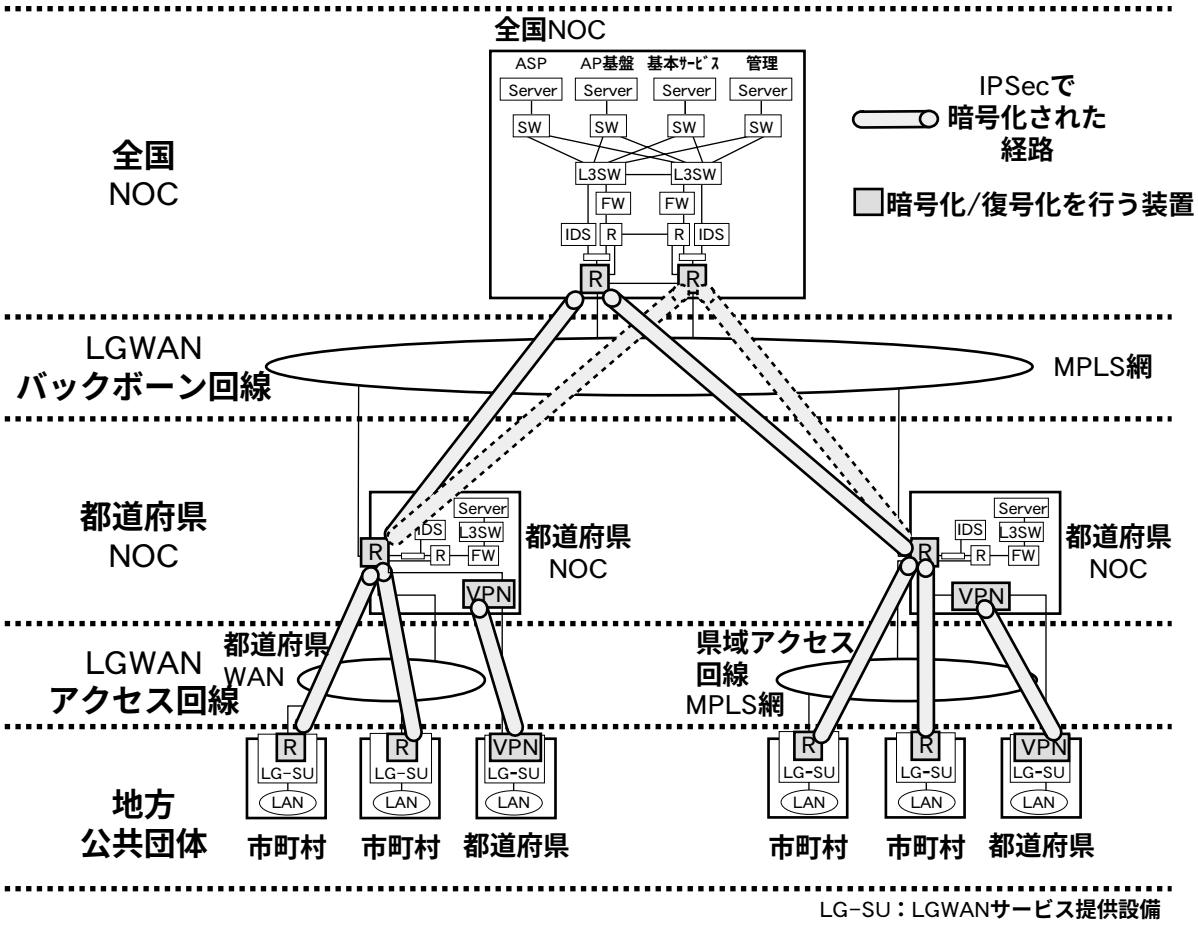

図 4-1 暗号化構成

4.3 セキュリティの実証実験結果

(1)Firewallの設置

セキュリティ上の境界となる場所に原則としてFirewallを配置し、侵入の脅威から防御する。具体的には、全国NOC及び都道府県NOCの各種サーバ群の入り口にFirewallを設置した。また、都道府県NOCと地方公共団体の接続点であるLGWANサービス提供設備にFirewall機能を持たせた。

図4-2に示すようなペネストレーション試験（疑似アタック試験）を行ったが、Firewallなどネットワークセキュリティには全く問題は無く、一部のサーバソフトに些細な問題が見つかったが、それも対処済みである。

(2)IDS（Intrusion Detection System）による監視

各地方公共団体間及び地方公共団体とサーバ間の通信をIDSにより監視することとした。具体的には都道府県下の地方公共団体間の直接通信は制限し、すべて都道府県NOCを経由し、IDSで監視することとした。また、都道府県NOC間の直接通信は制限し、すべて全国NOCを経由し、IDSで監視することとした。

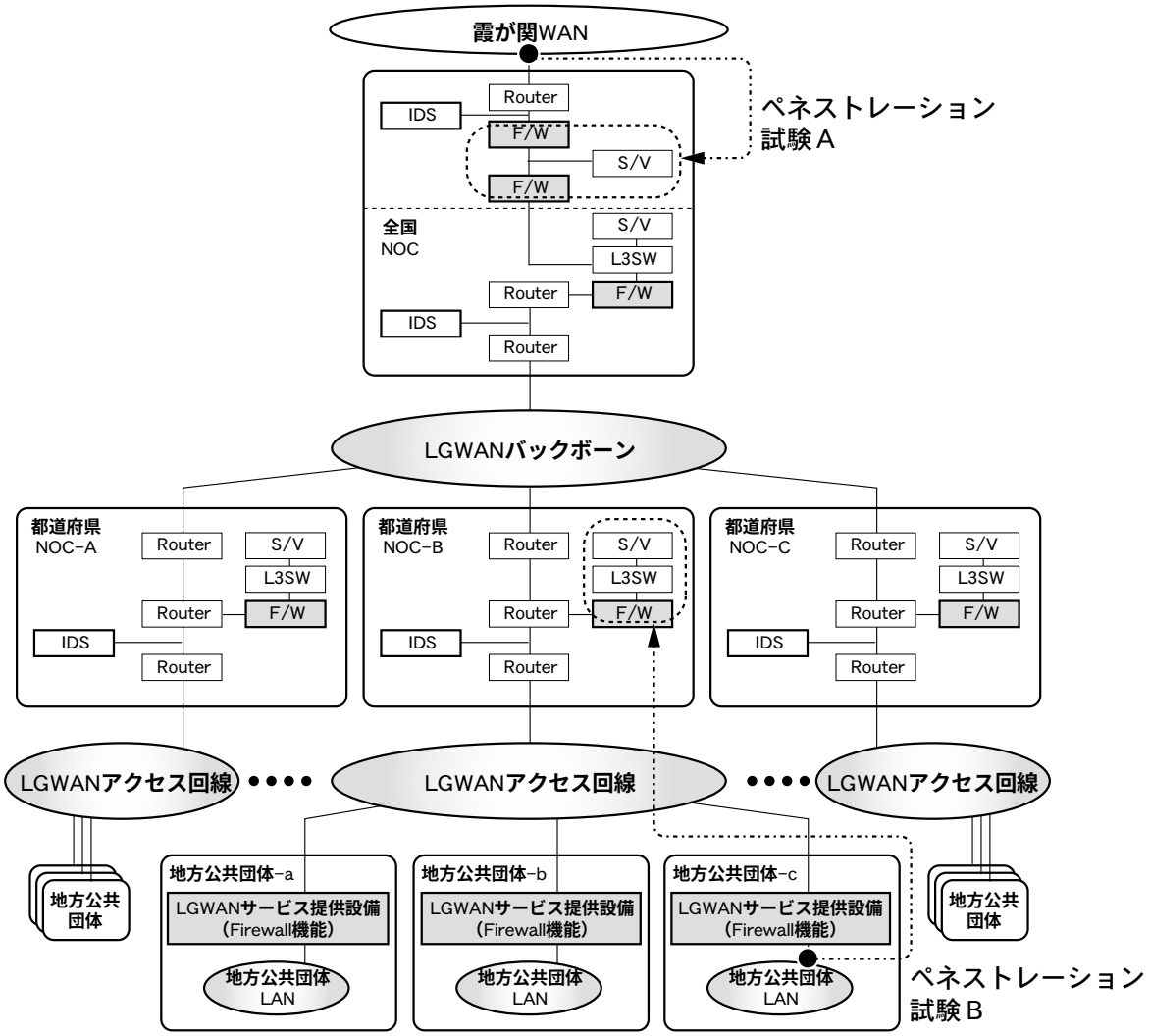

図 4-2 FirewallとIDSの論理的な配置構成

4.4 ルーティングの実証実験結果

(1)ダイナミックルーティング

スタティックルーティングでは、全国NOC回線の２重化経路の自動切換えが行えないため、ダイナミックルーティングを試行した。全国NOC−都道府県NOC間、都道府県NOC−市町村間はEIGRPで経路情報を交換し、全国NOCの１系統の回線ダウン時に２系統の回線に切り替わる構成とした。

(2)IDS監視のためのポリシールーティング

地方公共団体間の通信に不正がないか検出するため、暗号が解かれるIDS検出用セグメントを窓口ルータの内側に設けて一旦そのセグメントを強制的に経由させる。ポリシールーティング機能を使い、折返し用ルータを設けることで図 4−3に示すように折返しルーティングを実現した。

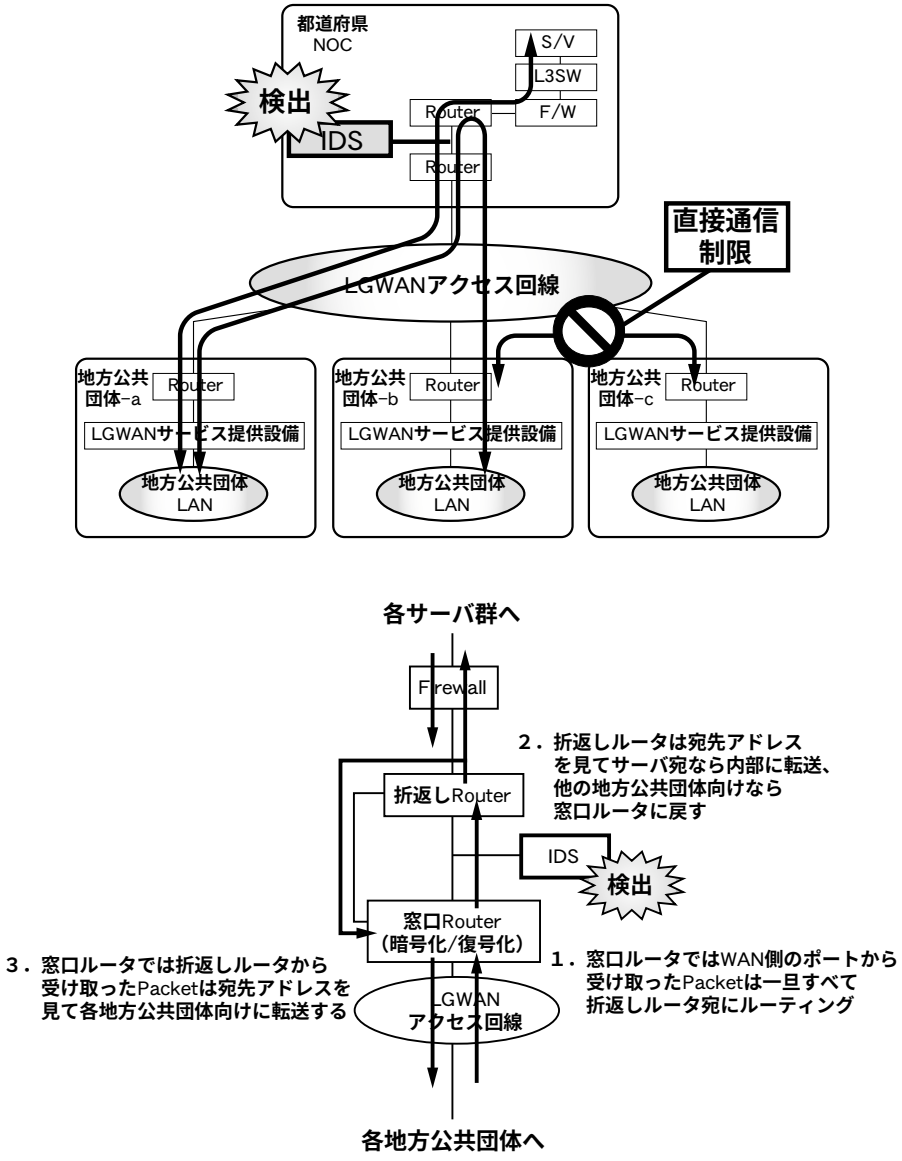

図 4−3 ポリシールーティングの構成イメージ

4.5 IPアドレスデザインの実証実験結果

総合行政ネットワーク内のアドレスは正式なInternetアドレス（グローバルアドレス）を採用した。既にプライベートアドレスで運用している地方公共団体LANとの相互接続は、LGWANサービス提供設備にてNAT(アドレス変換機能)を用いて総合行政ネットワークのグローバルアドレスに変換した。

実証実験では、全国NOCにはクラスC一つ、都道府県NOCには25ビットマスクを割り当て、地方公共団体には28ビットマスクを割り当てた。都道府県WANは、別途その構成に応じた追加割り当てが必要であった。

具体的なアドレス割付では、ルーティングテーブルの最適化のため、各都道府県域単位にクラスC相当のアドレスブロックを割り付け、県域下の団体はそのアドレスブロックの中から割り振った。

3300団体を対象にする場合は、全く拡張性を見込まず、かつ、アドレスブロックを考慮せず割り振ったとしても、クラスBのIPアドレスをほぼ一つ分消費することになる。

表 4-1 割り振ったサブネット数とホスト数

Subnet Mask	全国NOC		都道府県NOC		地方公共団体	
	実使用数	消費ホスト数換算	実使用数	消費ホスト数換算	実使用数	消費ホスト数換算
30ビット	13		7		2	
29ビット	2		2		1	
28ビット	3		0		0	
27ビット	2		1		0	
合計	20	180	10	76	3	16

表 4-2 LGWANで最低限必要なクラスCの数

	SubnetMask	数量	ClassCの数
全国NOC	24	1	1
都道府県NOC	25	47	24
地方公共団体	28	3300	207
合計			232

4.6 実証実験の考察

(1) 暗号化について

暗号化処理性能は機器構成によって性能が異なるため、都道府県WANの帯域によって機器構成を選択できるようにする必要があった。今後、必要に応じて暗号化処理を高速化するハードウェアを追加可能な機器構成とした。

ASPの形態によって、論理的に独立した通信路（トンネリング）を使うケースが想定されるが、その技術仕様については今後、追加評価が必要である。

(2) セキュリティについて

今回の実証実験では、都道府県NOC間の通信については、全国NOCと都道府県NOCで２重にIDSで検出し、全国NOCで集中監視する構成とした。しかし、全国NOCのネットワーク機器は、可用性向上のため２重化しており、IDS検出機能とあいまって、構成が複雑になってしまった。その結果、障害時の切り分け操作の簡便化など運用面の検討が必要となった。

今後、都道府県NOC間の通信については各都道府県NOC側のIDSのみで検出するようにし、構成を単純化するよう見直しを行う必要がある。集中監視機能については構成見直し後も担保する。

(3)ルーティングについて

以下の理由から、全国NOCと都道府県NOC間及び都道府県NOCと地方公共団体間のWAN接続部分はダイナミックルーティングを採用するべきと考える。

- 全国NOCのLGWANバックボーン回線を２重化し、全国NOCと都道府県NOC間の通信回線障害時に自動切り替えをする。
- 今後の団体追加やASPの接続により、経路情報が追加されても、ルータへの個別定義が最小限に済むようにする（人為的な設定ミスの予防も考慮）。

(4)IPアドレス

付加サービス用サーバ（ASPサービス）の追加分や都道府県WAN用回線分のIPアドレスは含まれていないため、最終的にはその利用見通しを含めたグローバルIPアドレス帯域を確保することが必須である。

3300もの地方公共団体を収容するため、適切なアドレスのブロック割り当てを行わないとルーティングテーブルサイズが大きくなり、遅延を引き起こす恐れがある。実際のIPアドレスの割付ではこの点を考慮する必要がある。

本構築の過程で上記の点を考慮したIPアドレス体系に振り直しを行う必要がある。

5. 基本プロトコル群

5.1 実験項目と内容

個別業務アプリケーションが利用しなければならない基本的なプロトコルサービス（DNS(Domain Name System),NTP(Network Time Protocol),SMTP(Simple Mail Transfer Protocol)）を実装した。サーバ配置やプロトコル実装上の問題について実証実験を行った。

5.2 DNSの実証実験結果

総合行政ネットワークで実証実験期間中に管理するドメインは、正引きでは「lgwan.go.jp」、逆引きでは「2.157.in-addr.arpa」とした。また、本ネットワークはInternetに接続されていないので、Internet上のドメイン名の処理はできないため、LGWANドメイン以外のドメイン名の解決処理はしないものとした。

結果としてZone Fowording機能を持たないDNS製品しかない団体があり、うまく処理ができないケースが発生した。

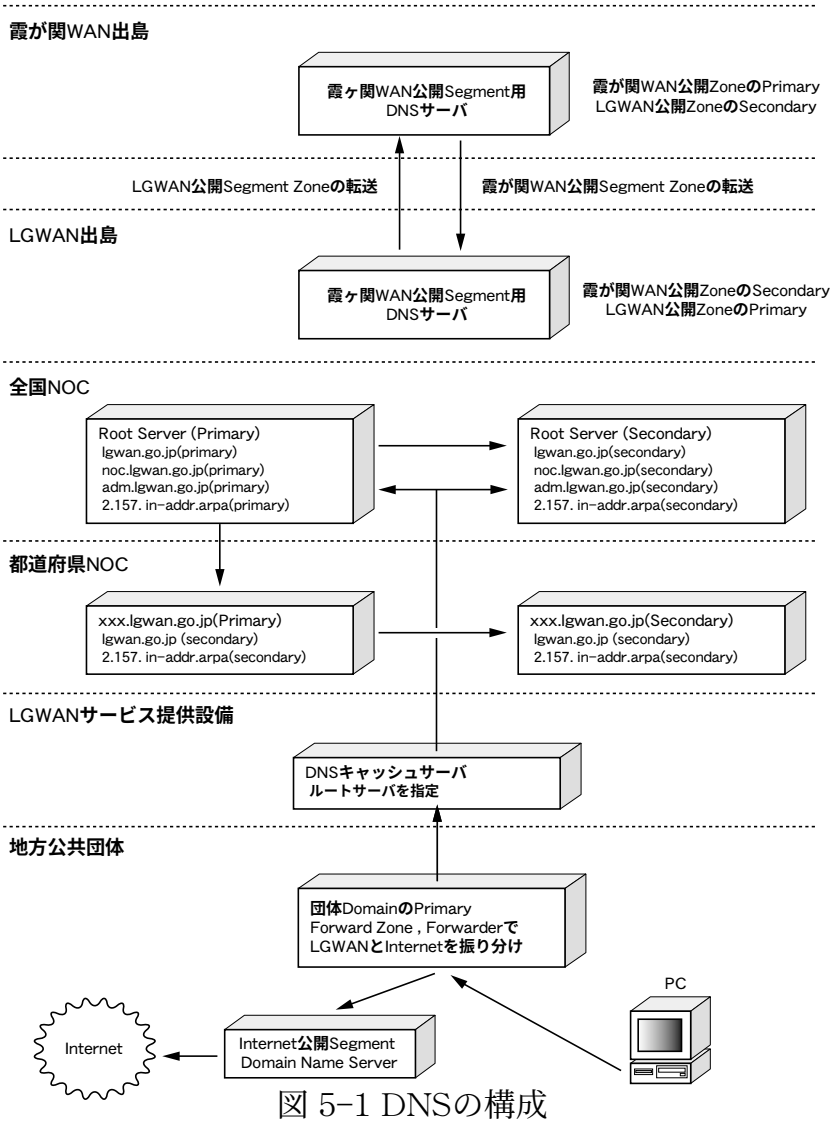

図 5-1 DNSの構成

5.3 NTPの実証実験結果

総合行政ネットワーク上の各機器は、階層構成によりNTPプロトコルを利用して正確な時刻を取得し、ネットワーク内の時刻（時分秒）同期を実現した。

全国NOC、都道府県NOCのタイムサーバ間で問題となるような時刻のずれが生じることがないか計測した。また、LGWANのNTPで時刻同期を取っている試験PCが標準時刻とどの程度の誤差があるか、実際にいくつかの団体側で実際の時刻とのずれを計測することとした。

その結果、全国NOC、都道府県NOCのタイムサーバ間のずれは数ミリsecの範囲であり、問題のない精度であった。試験PCの時間の誤差も数秒の範囲で収まっていた。

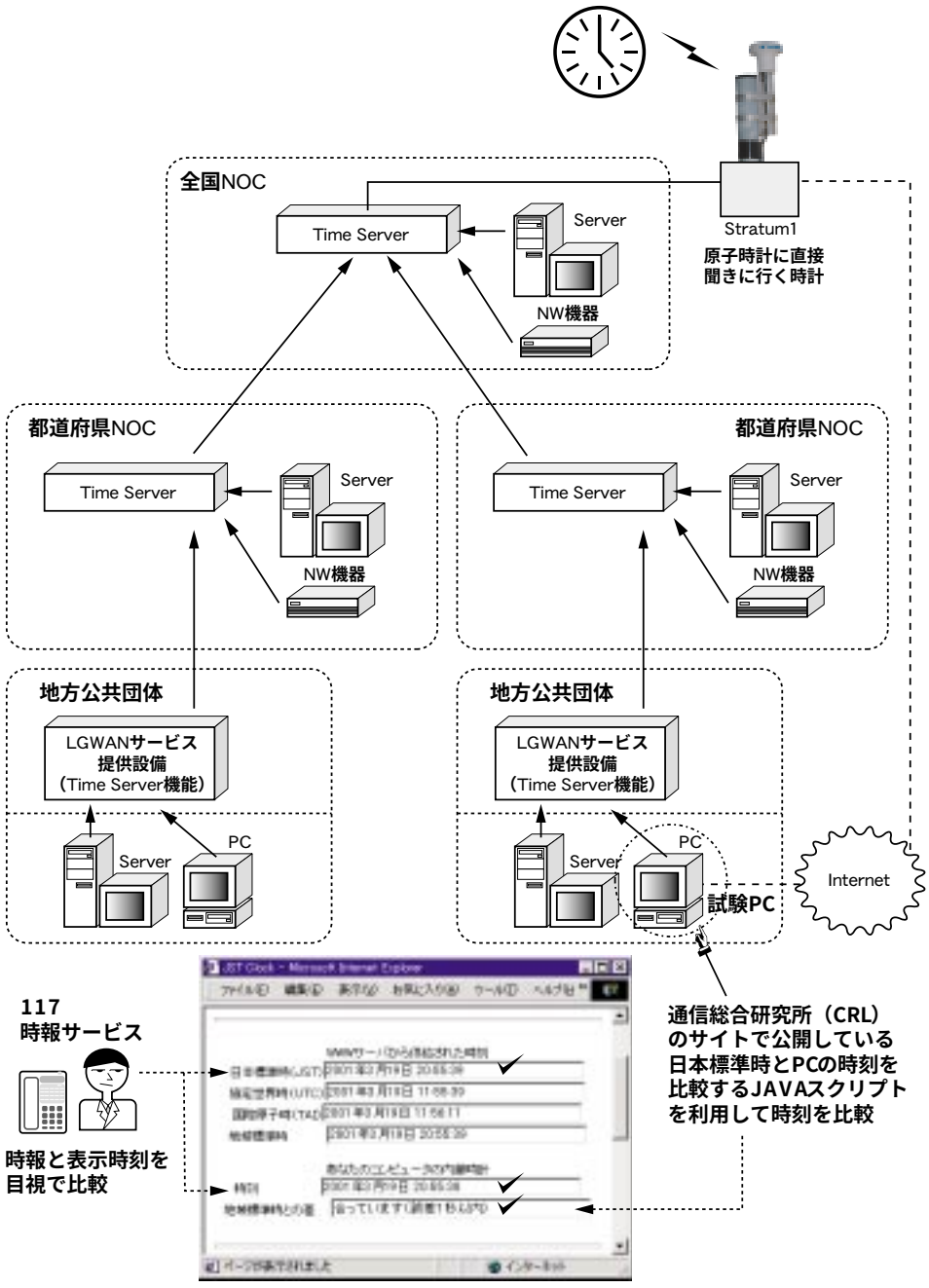

図 5-2 タイムサーバの構成

5.4 SMTPの実証実験結果

ネットワークの階層に合わせて、電子メールの配信経路は全国NOC、都道府県NOC、地方公共団体の３階層で構成した。地方公共団体と総合行政ネットワーク間はすべてSMTPプロトコルによる配信とした。全国NOCと霞が関WAN NOC間はX.400プロトコルによる送受信とし、X.400/SMTP変換GWによりX.400とSMTPのプロトコル変換を行うこととした。

霞が関WANとのメール試験では、総務省とLGWAN参加3団体間で、Asciiコード以外に漢字・カタカナを件名や本文に使ったメールや添付ファイルの容量を10MB×1個、1MB×10個、10KB×10個としたメールを実際にやりとりし、問題なく送受信できることが確認できた。

LGWAN内のメール試験では地方公共団体で実際に使っているMUA（Mail User Agent）から電子メールを送信してもらい、Internet標準（STD10,RFC821,822他）に適合しているか調査を行った。

その結果、Internet標準の仕様を満たしていないMUAを使っている団体があった。また、標準仕様以外にも、最大メールサイズの制限を行っており、大容量のメール試験（10MBの添付ファイル）を受け取れない団体も多かった。

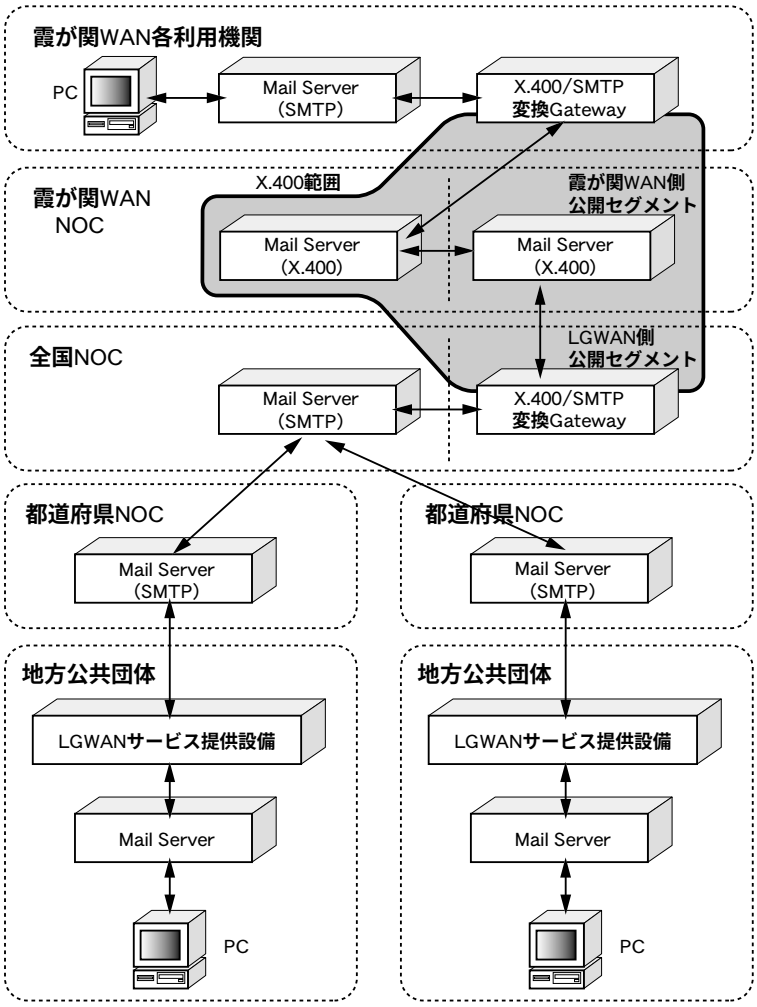

図 5-3 メールシステム構成

5.5 実証実験の考察

(1)DNSについて

実験団体のDNSがZone Forwardingに対応できないケースが見受けられ、DNSサーバの仮設置など暫定的な個別対応を行っている。どこまでをLGWAN標準の接続仕様とするか決める必要がある。

本運用時のドメイン名の考え方は、地方公共団体専用のドメイン名「xxx.lg.jp」を指向している。汎用ドメインとの併存などを含む設計の見直しが必要である。

都道府県NOCドメインDNSの代替え（Secondary）は同一サイト内で持たせる設計となっているが、全国NOCのDNSで各都道府県NOCドメインDNSの代替えを持たせるなど最適化の余地がある。

(2)NTPについて

実証実験では時刻情報ソースは一つしかないので、今後、複数の時刻情報ソースを取り込み、相互補完させる必要がある。

(3)SMTPについて

災害時の緊急連絡など緊急性や、同報性がどの程度保証できるかなど、業務への適応性を検討し、メールの配信遅延に対して、SLAを定めるべきである。

電子メールはスタティック配信で実証実験を行ったが、ドメイン名の移行を考慮しMXレコードによるダイナミック配信を行えるようにする必要がある。

MUAの仕様は団体ごとに異なっており、Internet標準に準拠してないものも多い。また、標準ではないが慣例となっている仕様の扱いについても、実際にどのレベルを許容範囲とするか検討が必要である。

添付ファイルのロングファイル名の可否やメールの最大サイズなど本来のメールの技術仕様と直接関係がない部分についても、同様に取り決めをする必要がある。

実証実験終了段階では上記のサーバ群はすべてシングル構成となっているので、２重化構成とし、可用性を担保する必要がある。

6. アプリケーション基盤

6.1実験項目と内容

アプリケーション基盤は、各アプリケーションに共通の機能を切り出して統一的にサービスする基盤である。アプリケーション基盤としては、認証基盤、ディレクトリ基盤、公証基盤、文書保管基盤、XML電文交換基盤を構築し、実証実験を行った。

6.2 認証基盤の実証実験結果

6.2.1 認証基盤構築

認証局（CA：Certification Authority）は登録局（RA：Registration Authority）と発行局（IA：Issueing Authority）の機能を併せ持っているが、実証実験の構成では、登録機能（RA）と発行機能（IA）を分離し、地方公共団体が、LGWAN運営主体の運営する認証局に証明書の発行を依託することを想定した（都道府県IAを47に分割したのは次に示す独自認証局への移行の容易性を考慮。）。

更に、都道府県の独立性の保証と他の組織などとの相互認証のために、ブリッジ認証局を全国NOCに設置した。証明書の有効性の問い合わせに即時に答える証明書検証サーバ（VA：Validation Authority）を全国NOCと各都道府県NOCに設置した。

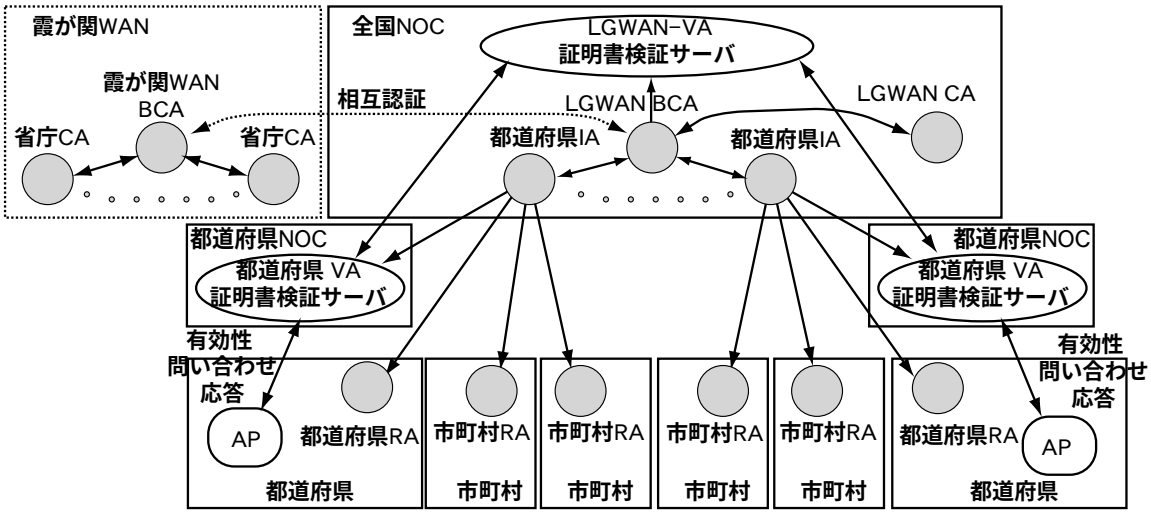

図 6-1 実証実験の認証基盤の構成

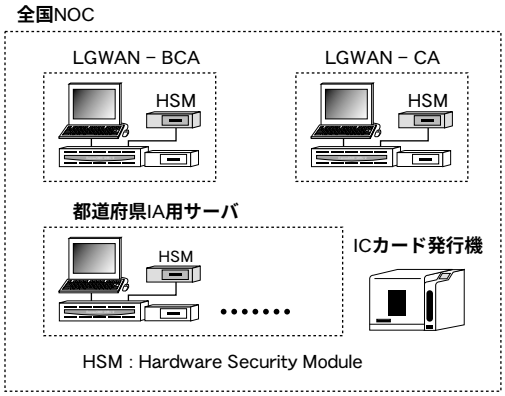

図 6-2 実証実験の認証基盤のシステム構成

6.2.2 LGWAN認証局

LGWAN認証基盤で構築した認証局とその正式名称（ディレクトリのDN）を以下に示す。

・DNが日本語表記の場合はすべての文字を全角とした。

・都道府県NOC CAは論理的には47あるが、物理的な装置は10台とした。

・都道府県NOC CAは、現状ではすべて全国NOCに収容することとした。

表6-1 LGWAN認証局（その１）

番号	認証局名	発行者名(Issure)			
		C	O	OU	OU
－	－	JP	Local Government	Zenkoku NOC	－
			地方公共団体	**全国ＮＯＣ**	－
48	LGWAN-BCA	JP	Local Government	Zenkoku NOC	LGWAN-BCA
			地方公共団体	**全国ＮＯＣ**	**ＬＧＷＡＮブリッジ認証局**
49	LGWAN-CA	JP	Local Government	Zenkoku NOC	LGWAN-CA
			地方公共団体	**全国ＮＯＣ**	**ＬＧＷＡＮ認証局**
1	**北海道**	JP	Local Government	Zenkoku NOC	Hokkaido NOC CA
			地方公共団体	**全国ＮＯＣ**	**北海道ＮＯＣ認証局**
2	**青森県**	JP	Local Government	Zenkoku NOC	Aomoriken NOC CA
			地方公共団体	**全国ＮＯＣ**	**青森県ＮＯＣ認証局**
3	**岩手県**	JP	Local Government	Zenkoku NOC	Iwateken NOC CA
			地方公共団体	**全国ＮＯＣ**	**岩手県ＮＯＣ認証局**
4	**宮城県**	JP	Local Government	Zenkoku NOC	Miyagiken NOC CA
			地方公共団体	**全国ＮＯＣ**	**宮城県ＮＯＣ認証局**
5	**秋田県**	JP	Local Government	Zenkoku NOC	Akitaken NOC CA
			地方公共団体	**全国ＮＯＣ**	**秋田県ＮＯＣ認証局**
6	**山形県**	JP	Local Government	Zenkoku NOC	Yamagataken NOC CA
			地方公共団体	**全国ＮＯＣ**	**山形県ＮＯＣ認証局**
7	**福島県**	JP	Local Government	Zenkoku NOC	Fukushimaken NOC CA
			地方公共団体	**全国ＮＯＣ**	**福島県ＮＯＣ認証局**
8	**茨城県**	JP	Local Government	Zenkoku NOC	Ibarakiken NOC CA
			地方公共団体	**全国ＮＯＣ**	**茨城県ＮＯＣ認証局**
9	**栃木県**	JP	Local Government	Zenkoku NOC	Tochigiken NOC CA
			地方公共団体	**全国ＮＯＣ**	**栃木県ＮＯＣ認証局**
10	**群馬県**	JP	Local Government	Zenkoku NOC	Gunmaken NOC CA
			地方公共団体	**全国ＮＯＣ**	**群馬県ＮＯＣ認証局**
11	**埼玉県**	JP	Local Government	Zenkoku NOC	Saitamaken NOC CA
			地方公共団体	**全国ＮＯＣ**	**埼玉県ＮＯＣ認証局**
12	**千葉県**	JP	Local Government	Zenkoku NOC	Chibaken NOC CA
			地方公共団体	**全国ＮＯＣ**	**千葉県ＮＯＣ認証局**
13	**東京都**	JP	Local Government	Zenkoku NOC	Tokyoto NOC CA
			地方公共団体	**全国ＮＯＣ**	**東京都ＮＯＣ認証局**
14	**神奈川県**	JP	Local Government	Zenkoku NOC	Kanagawaken NOC CA
			地方公共団体	**全国ＮＯＣ**	**神奈川県ＮＯＣ認証局**
15	**新潟県**	JP	Local Government	Zenkoku NOC	Niigataken NOC CA
			地方公共団体	**全国ＮＯＣ**	**新潟県ＮＯＣ認証局**
16	**富山県**	JP	Local Government	Zenkoku NOC	Toyamaken NOC CA
			地方公共団体	**全国ＮＯＣ**	**富山県ＮＯＣ認証局**
17	**石川県**	JP	Local Government	Zenkoku NOC	Ishikawaken NOC CA
			地方公共団体	**全国ＮＯＣ**	**石川県ＮＯＣ認証局**
18	**福井県**	JP	Local Government	Zenkoku NOC	Fukuiken NOC CA
			地方公共団体	**全国ＮＯＣ**	**福井県ＮＯＣ認証局**
19	**山梨県**	JP	Local Government	Zenkoku NOC	Yamanashiken NOC CA
			地方公共団体	**全国ＮＯＣ**	**山梨県ＮＯＣ認証局**
20	**長野県**	JP	Local Government	Zenkoku NOC	Naganoken NOC CA
			地方公共団体	**全国ＮＯＣ**	**長野県ＮＯＣ認証局**

表 6-1 LGWAN認証局（その２）

番号	認証局名	発行者名(Issure)			
		C	O	OU	OU
21	岐阜県	JP	Local Government	Zenkoku NOC	Gifuken NOC CA
			地方公共団体	全国ＮＯＣ	岐阜県ＮＯＣ認証局
22	静岡県	JP	Local Government	Zenkoku NOC	Shizuokaken NOC CA
			地方公共団体	全国ＮＯＣ	静岡県ＮＯＣ認証局
23	愛知県	JP	Local Government	Zenkoku NOC	Aichiken NOC CA
			地方公共団体	全国ＮＯＣ	愛知県ＮＯＣ認証局
24	三重県	JP	Local Government	Zenkoku NOC	Mieken NOC CA
			地方公共団体	全国ＮＯＣ	三重県ＮＯＣ認証局
25	滋賀県	JP	Local Government	Zenkoku NOC	Shigaken NOC CA
			地方公共団体	全国ＮＯＣ	滋賀県ＮＯＣ認証局
26	京都府	JP	Local Government	Zenkoku NOC	Kyotofu NOC CA
			地方公共団体	全国ＮＯＣ	京都府ＮＯＣ認証局
27	大阪府	JP	Local Government	Zenkoku NOC	Osakafu NOC CA
			地方公共団体	全国ＮＯＣ	大阪府ＮＯＣ認証局
28	兵庫県	JP	Local Government	Zenkoku NOC	Hyogoken NOC CA
			地方公共団体	全国ＮＯＣ	兵庫県ＮＯＣ認証局
29	奈良県	JP	Local Government	Zenkoku NOC	Naraken NOC CA
			地方公共団体	全国ＮＯＣ	奈良県ＮＯＣ認証局
30	和歌山県	JP	Local Government	Zenkoku NOC	Wakayamaken NOC CA
			地方公共団体	全国ＮＯＣ	和歌山県ＮＯＣ認証局
31	鳥取県	JP	Local Government	Zenkoku NOC	Tottoriken NOC CA
			地方公共団体	全国ＮＯＣ	鳥取県ＮＯＣ認証局
32	島根県	JP	Local Government	Zenkoku NOC	Shimaneken NOC CA
			地方公共団体	全国ＮＯＣ	島根県ＮＯＣ認証局
33	岡山県	JP	Local Government	Zenkoku NOC	Okayamaken NOC CA
			地方公共団体	全国ＮＯＣ	岡山県ＮＯＣ認証局
34	広島県	JP	Local Government	Zenkoku NOC	Hiroshimaken NOC CA
			地方公共団体	全国ＮＯＣ	広島県ＮＯＣ認証局
35	山口県	JP	Local Government	Zenkoku NOC	Yamaguchiken NOC CA
			地方公共団体	全国ＮＯＣ	山口県ＮＯＣ認証局
36	徳島県	JP	Local Government	Zenkoku NOC	Tokushimaken NOC CA
			地方公共団体	全国ＮＯＣ	徳島県ＮＯＣ認証局
37	香川県	JP	Local Government	Zenkoku NOC	Kagawaken NOC CA
			地方公共団体	全国ＮＯＣ	香川県ＮＯＣ認証局
38	愛媛県	JP	Local Government	Zenkoku NOC	Ehimeken NOC CA
			地方公共団体	全国ＮＯＣ	愛媛県ＮＯＣ認証局
39	高知県	JP	Local Government	Zenkoku NOC	Kochiken NOC CA
			地方公共団体	全国ＮＯＣ	高知県ＮＯＣ認証局
40	福岡県	JP	Local Government	Zenkoku NOC	Fukuokaken NOC CA
			地方公共団体	全国ＮＯＣ	福岡県ＮＯＣ認証局
41	佐賀県	JP	Local Government	Zenkoku NOC	Sagaken NOC CA
			地方公共団体	全国ＮＯＣ	佐賀県ＮＯＣ認証局
42	長崎県	JP	Local Government	Zenkoku NOC	Nagasakiken NOC CA
			地方公共団体	全国ＮＯＣ	長崎県ＮＯＣ認証局
43	熊本県	JP	Local Government	Zenkoku NOC	Kumamotoken NOC CA
			地方公共団体	全国ＮＯＣ	熊本県ＮＯＣ認証局
44	大分県	JP	Local Government	Zenkoku NOC	Oitaken NOC CA
			地方公共団体	全国ＮＯＣ	大分県ＮＯＣ認証局
45	宮崎県	JP	Local Government	Zenkoku NOC	Miyazakiken NOC CA
			地方公共団体	全国ＮＯＣ	宮崎県ＮＯＣ認証局
46	鹿児島県	JP	Local Government	Zenkoku NOC	Kagoshimaken NOC CA
			地方公共団体	全国ＮＯＣ	鹿児島県ＮＯＣ認証局
47	沖縄県	JP	Local Government	Zenkoku NOC	Okinawaken NOC CA
			地方公共団体	全国ＮＯＣ	沖縄県ＮＯＣ認証局

6.2.3 LGWANが発行する証明書の構造

構成要素		説明
バージョン番号		証明書のバージョン。（Version 3）
シリアル番号		各CAが発行した証明書に対して 一意に割り振る番号。
デジタル署名 アルゴリズム識別子		CAが本証明書の電子署名に使用した アルゴリズム（例：SHA-1+2048bit RSA）
(1) 発行者名（CA） （Issuer name）		本証明書を発行したCAの名前 DN（Printable String：英数字）
有効期間 （開始日時、終了日時）		本証明書の有効期間
(2) 所有者名 （Subject name）		本証明書によって証明される公開鍵の所有者名 DN（Printable String：英数字）
所有者の公開鍵情報		本証明書によって証明される公開鍵の情報
	アルゴリズム識別子	公開鍵のアルゴリズム（例：1024it RSA）
	所有者公開鍵	公開鍵自身

	要素名	重要／非重要 フラッグ
V3拡張	発行者鍵識別子（Authority key identifier）	非重要
	所有者鍵識別子（Subject key identifier）	非重要
	鍵利用（Key usage）	未使用
	秘密鍵利用期間（Private Key Usage Period）	非重要
	証明書ポリシー（Certificate policies）	非重要
	ポリシーマッピング（Policy mappings）	未使用
	(3) 所有者代替名（Subject alternative name）	非重要
	(4) 発行者代替名（Issuer alternative name）	非重要
	所有者ディレクトリ属性（Subject Directory Attribute）	非重要
	基本制限（Basic constraints）	未使用
	名前制限（Name constraints）	未使用
	ポリシー制限（Policy constraints）	未使用
	CRL配布点（CRL distribution point）	未使用

CAのデジタル署名

CAの署名	アルゴリズム識別子	電子署名に使用したアルゴリズム
	CAの電子署名	証明書データをCAがハッシュ暗号化した署名

図 6-3 LGWANが発行する証明書の構造

LGWANの発行する証明書のフォーマットは ITU-T X.509 Version 3に定められた形式を用いた（図 6-3）。

証明書の構成要素の内「(1) 発行者名（Issuer name）」「(2) 所有者名（Subject name）」はディレクトリのDNを指定し英数字（Printable String）で表現した。

エンドユーザによる証明書の 発行者及び所有者の識別を容易にするため、「(3) 所有者代替名（Subject alternative name）」「(4) 発行者代替名（Issuer alternative name）」に日本語（漢字）表現の一般的な名称をUTF-8で格納した。

6.2.4 証明書構造詳細（基本領域）

1） 証明書形式のバージョン（Certificate format version）

Version 3を指定。

2） シリアル番号（Certificate serial number）

新しく発行した証明書に対してCAが生成し、割り振る一意の番号。

3） 電子署名アルゴリズムの識別子（Signature algorithm identifier for CA）

CAが証明書の電子署名に使用するアルゴリズムの識別子。

本証明書ではハッシュアルゴリズムSHA-1、暗号化アルゴリズム2048bit RSA。

4） 発行者名（Issuer X.500 name）

証明書を発行したCAのユニークなX.500識別名DN（Distinguished Name）。

5) 有効期間（Validity period）

証明書の有効期間。

6) 所有者名（Subject X.500 name）

本証明書によって証明される公開鍵の所有者のユニークなX.500識別名DN（Distinguished Name）。

7) 所有者公開鍵情報（Subject Public Key Information）

アルゴリズム識別子と公開鍵。

8) 認証システムの署名（CA signature）

証明書本体のデータをアルゴリズム識別子に示された方法で、CAがハッシュ暗号化した電子署名の値と、アルゴリズム識別子（本体内と電子署名内に 電子署名アルゴリズムの識別子が重複して存在するがこれは仕様である。）。

6.2.5 証明書構造詳細（ X.509 Version 3 による証明書形式の拡張領域）

X.509 Version 3 による証明書形式の拡張領域として下記要素を証明書中に含める。未使用の要素は証明書に存在しない。

1) 発行者鍵識別子（Authority key identifier）：非重要

発行者（CA）が複数の鍵ペアを持っている場合に、証明書の電子署名に使用する秘密鍵（或いは秘密鍵の対となる公開鍵を含む証明書）が特定できる識別子を格納する。

2) 所有者鍵識別子（Subject key identifier）：非重要

所有者が複数の鍵ペアを持っている場合に、証明書に記載された公開鍵と対になる特定の秘密鍵を示す。

3) 鍵利用（Key usage）：未使用

鍵を使用する目的（署名、暗号化等）を示す。

4) 秘密鍵利用期間（Private Key Usage Period）：非重要

秘密鍵を使用する期間を示す。（証明書の有効期間と鍵の使用期間が異なった場合）

5) 証明書ポリシー（Certificate policies）：非重要

発行された証明書のポリシー（発行の方法、利用の目的や提供範囲）の識別子を示す。

6) ポリシーマッピング（Policy mappings）：未使用

相互認証したところとの間で証明書ポリシーが等価であると見なせるかを示す。

7) 所有者代替名（Subject alternative name）：非重要

証明書の所有者の一般名称（日本語・漢字名称をここに入れる。）。

8) 発行者代替名（Issuer alternative name）：非重要

発行者（認証システム）の一般名称（日本語・漢字名称をここに入れる。）。

9) 所有者ディレクトリ属性（Subject Directory Attribute）：非重要

利用者の証明書に含ませることが可能である付加的なディレクトリ属性（所属・役職・住所・電話番号など）を示す。

10) 基本制限（Basic constraints）：未使用

証明書が認証システムに対して発行されたものかどうかを示す。認証システムに対して発行されたものであれば、認証経路の長さに対する制限を示す。

11) 名前制限（Name constraints）：未使用

相互認証時の信頼できるドメイン制限の機構を示す。

12) ポリシー制限（Policy constraints）：未使用

相互認証時の受け入れることのできるポリシーを示す。

13) CRL配布点（CRL　distribution point）：未使用

本証明書の証明書廃棄リスト（CRL）はCRL-DPではなく、一つのCRLを使用。

6.2.5 証明書の発行配布

本実験では、参加団体に対して、文書交換の実験用として以下の証明書及びICカードを発行配布した（次ページに発行リストの一部を示す。）。

1) ＸＸ県文書取扱担当１：文書交換業務、正常用（有効）

2) ＸＸ県文書取扱担当２：文書交換業務、異常用（失効）

3) ＸＸ県公印１：公印業務、正常用（有効）

2) ＸＸ県公印２：公印業務、異常用（失効）

表 6-2 LGWAN発行の証明書例（一部分）

証明書番号	発行対象団体番号	発行対象団体名	所有者名							備考
			C	O	L	OU	CN	別名(otherName)	別名（title）	
1	1	北海道	JP	Local Government	Hokkaido Area	Hokkaido	Bunsyo Toriatsukai Tantou 1	**北海道文書取扱担当１**	none	
			JP	**地方公共団体**	**北海道域**	**北海道**	**文書取扱担当１**	－	－	
2			JP	Local Government	Hokkaido Area	Hokkaido	Kouin 1	**北海道公印１**	none	
			JP	**地方公共団体**	**北海道域**	**北海道**	**公印１**	－	－	
3			JP	Local Government	Hokkaido Area	Hokkaido	Bunsyo Toriatsukai Tantou 2	**北海道文書取扱担当２**	none	
			JP	**地方公共団体**	**北海道域**	**北海道**	**文書取扱担当２**	－	－	
4			JP	Local Government	Hokkaido Area	Hokkaido	Kouin 2	**北海道公印２**	none	
			JP	**地方公共団体**	**北海道域**	**北海道**	**公印２**	－	－	
5	2	福島県	JP	Local Government	Fukushimaken Area	Fukushimaken	Bunsyo Toriatsukai Tantou 1	**福島県文書取扱担当１**	none	
			JP	**地方公共団体**	**福島県域**	**福島県**	**文書取扱担当１**	－	－	
6			JP	Local Government	Fukushimaken Area	Fukushimaken	Kouin 1	**福島県公印１**	none	
			JP	**地方公共団体**	**福島県域**	**福島県**	**公印１**	－	－	
7			JP	Local Government	Fukushimaken Area	Fukushimaken	Bunsyo Toriatsukai Tantou 2	**福島県文書取扱担当２**	none	
			JP	**地方公共団体**	**福島県域**	**福島県**	**文書取扱担当２**	－	－	
8			JP	Local Government	Fukushimaken Area	Fukushimaken	Kouin 2	**福島県公印２**	none	
			JP	**地方公共団体**	**福島県域**	**福島県**	**公印２**	－	－	
9	3	神奈川県	JP	Local Government	Kanagawaken Area	Kanagawaken	Bunsyo Toriatsukai Tantou 1	**神奈川県文書取扱担当１**	none	
			JP	**地方公共団体**	**神奈川県域**	**神奈川県**	**文書取扱担当１**	－	－	
10			JP	Local Government	Kanagawaken Area	Kanagawaken	Kouin 1	**神奈川県公印１**	none	
			JP	**地方公共団体**	**神奈川県域**	**神奈川県**	**公印１**	－	－	
11			JP	Local Government	Kanagawaken Area	Kanagawaken	Bunsyo Toriatsukai Tantou 2	**神奈川県文書取扱担当２**	none	
			JP	**地方公共団体**	**神奈川県域**	**神奈川県**	**文書取扱担当２**	－	－	
12			JP	Local Government	Kanagawaken Area	Kanagawaken	Kouin 2	**神奈川県公印２**	none	
			JP	**地方公共団体**	**神奈川県域**	**神奈川県**	**公印２**	－	－	
13	4	新潟県	JP	Local Government	Niigataken Area	Niigataken	Bunsyo Toriatsukai Tantou 1	**新潟県文書取扱担当１**	none	
			JP	**地方公共団体**	**新潟県域**	**新潟県**	**文書取扱担当１**	－	－	
14			JP	Local Government	Niigataken Area	Niigataken	Kouin 1	**新潟県公印１**	none	
			JP	**地方公共団体**	**新潟県域**	**新潟県**	**公印１**	－	－	
15			JP	Local Government	Niigataken Area	Niigataken	Bunsyo Toriatsukai Tantou 2	**新潟県文書取扱担当２**	none	
			JP	**地方公共団体**	**新潟県域**	**新潟県**	**文書取扱担当２**	－	－	
16			JP	Local Government	Niigataken Area	Niigataken	Kouin 2	**新潟県公印２**	none	
			JP	**地方公共団体**	**新潟県域**	**新潟県**	**公印２**	－	－	
17	5	岐阜県	JP	Local Government	Gifuken Area	Gifuken	Bunsyo Toriatsukai Tantou 1	**岐阜県文書取扱担当１**	none	
			JP	**地方公共団体**	**岐阜県域**	**岐阜県**	**文書取扱担当１**	－	－	
18			JP	Local Government	Gifuken Area	Gifuken	Kouin 1	**岐阜県公印１**	none	
			JP	**地方公共団体**	**岐阜県域**	**岐阜県**	**公印１**	－	－	
19			JP	Local Government	Gifuken Area	Gifuken	Bunsyo Toriatsukai Tantou 2	**岐阜県文書取扱担当２**	none	
			JP	**地方公共団体**	**岐阜県域**	**岐阜県**	**文書取扱担当２**	－	－	
20			JP	Local Government	Gifuken Area	Gifuken	Kouin 2	**岐阜県公印２**	none	
			JP	**地方公共団体**	**岐阜県域**	**岐阜県**	**公印２**	－	－	

6.3 ディレクトリ基盤の実証実験結果

6.3.1 ディレクトリ基盤構築

統合ディレクトリを、全国NOCに置き、LGWANの認証情報及びLGWANに接続する各都道府県CAの認証局の認証情報を公開する機能を提供した。

統合ディレクトリにより、LGWAN-CAとLGWAN-BCAの自己署名証明書・相互認証証明書ペア・CRL・ARL、各都道府県CAの自己署名証明書、職責証明書及びこれらの失効情報を登録、格納、管理するための機能を提供した。

認証ドメイン内に含まれるすべてのエンティティは、全体として矛盾のない一つのディレクトリ情報ツリー(DIT)として構成した。また、証明書内のsubject、issuerは、ディレクトリ上で各々に対応するエントリの識別名と一致させた。

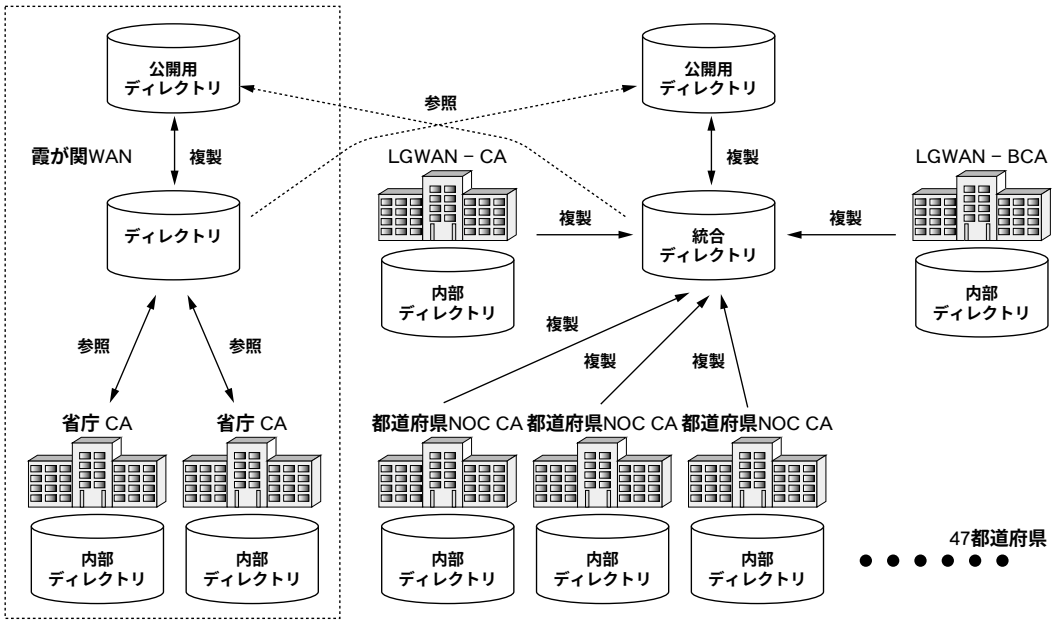

図 6-4 ディレクトリ配置

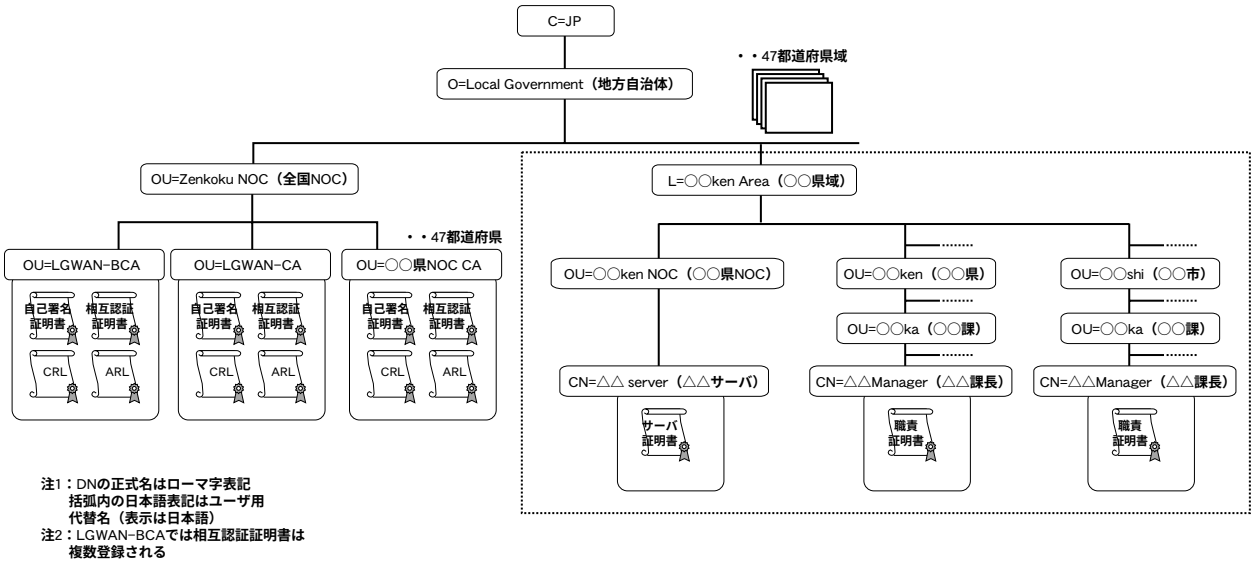

図 6-5 DIT構成

6.3.2 システム用ツリー

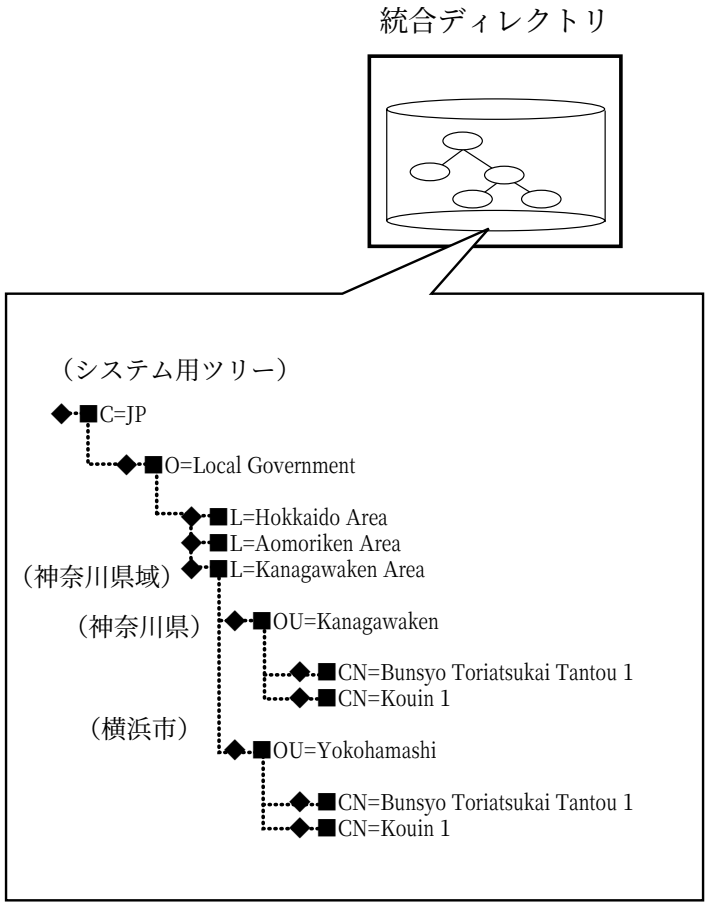

図 6-6 システム用ツリー

LGWANで発行された証明書は統合ディレクトリに収容される。ディレクトリのDNは証明書の所有者名（Subject name）と一致し、英数字（Printable String）で表現される。この英数字（Printable String）で表現されたツリーを「システム用ツリー」と呼ぶ。

6.3.3 エンドユーザ用ツリー

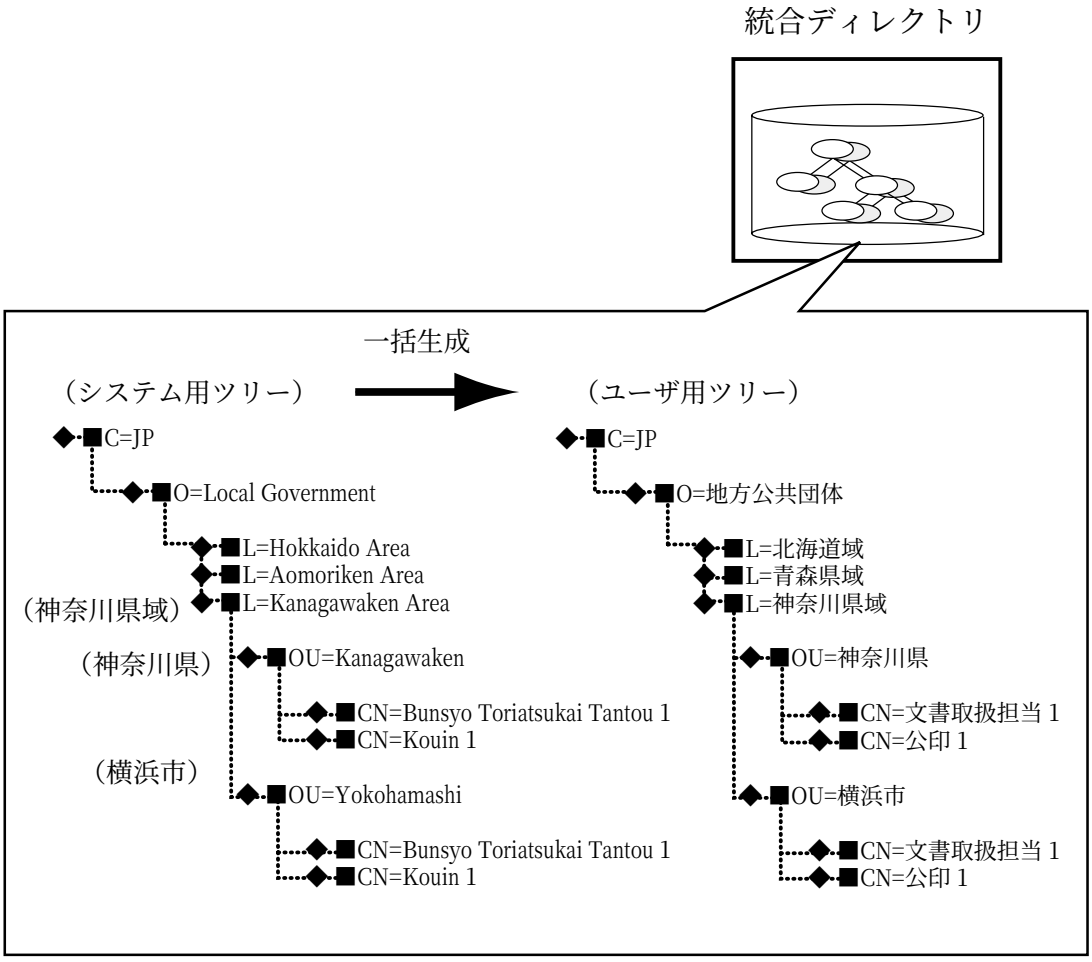

図 6-7 エンドユーザ用ツリーの生成

「システム用ツリー」のDNは証明書の所有者名（Subject name）と一致し、英数字（Printable String）で表現される。このため、エンドユーザがこのツリーを直接利用して宛名等を選ぶことは困難であり、使い勝手を著しく低下させると考えられる。このため、DNを日本語（漢字）で表現した「ユーザ用ツリー」を作成して、エンドユーザの利用を容易にする必要がある。

「ユーザ用ツリー」は「システム用ツリー」から一括して生成し、「ユーザ用ツリー」と「システム用ツリー」は一対一に対応させる。

6.4 証明書検証の実証実験結果

他の地方公共団体から電子文書を収受する際には、都道府県NOCに設置された証明書検証サーバに証明書の有効性確認の問い合わせ要求をする。この時、証明書検証サーバは全国NOC内の統合ディレクトリから証明書、失効情報を取得し、認証パスの構築及び有効性の検証を行い、検証結果を応答する。

証明書検証サーバを構築し、これらの機能を実現させ、有効性を確認できた。

霞が関WAN接続を考慮し、BCAを介した証明書検証も行った。証明書検証サーバのアクセスプロトコルはOCSP（RFC2560）の規定に準拠するものとした。

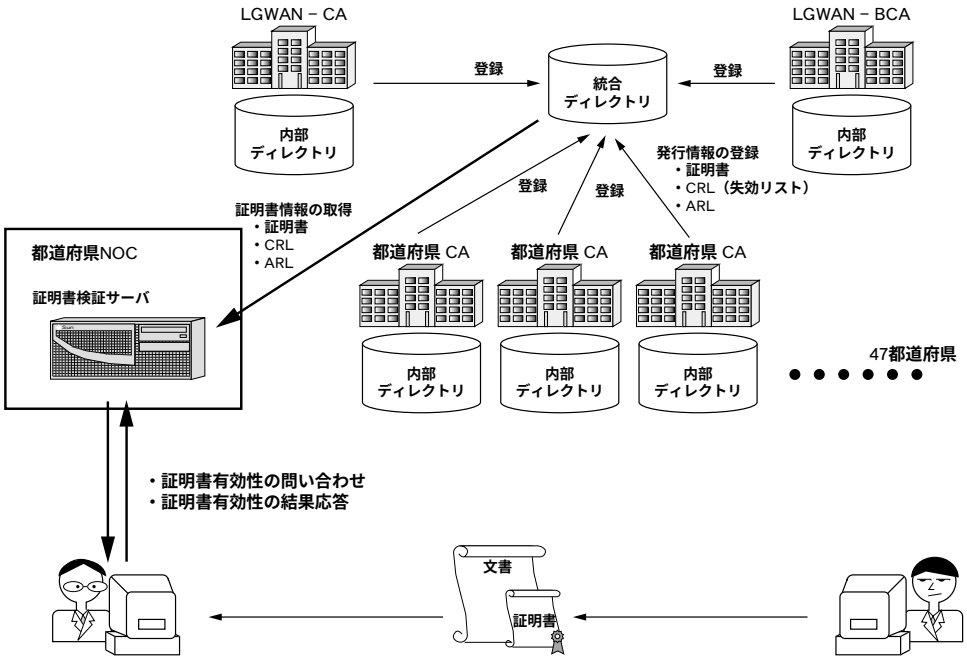

図 6-8 証明書検証の概要図

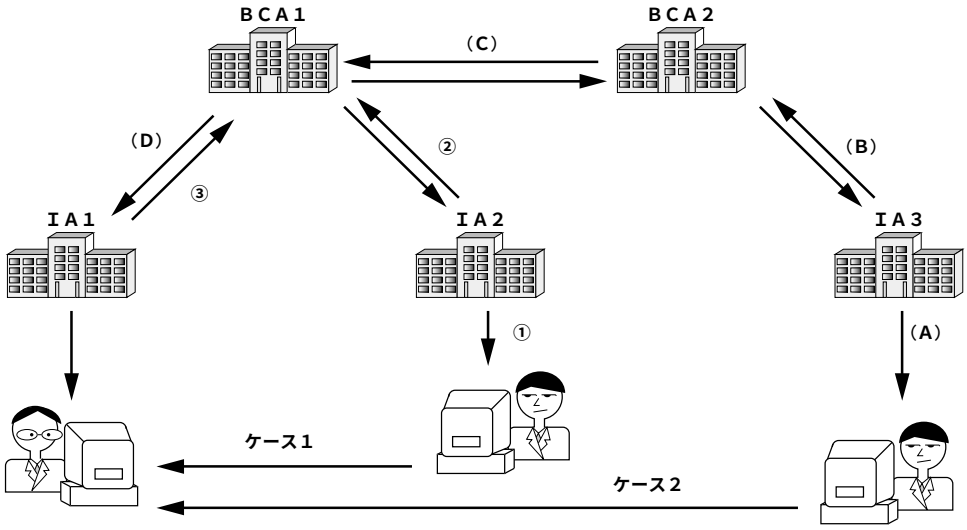

図 6-9 認証パス構築のイメージ

6.5 公証基盤の実証実験結果

確認証サーバは、確認証の発行を行う。確認証は確認したい内容（確認証発行リクエスト）をXML化した原文に、正確な基準時計からの時刻を刻印し、それらのハッシュ値に対して確認証サーバの秘密鍵によってデジタル署名を行ったものである。確認証自体の存在によって、データが存在した日時を特定することが可能となるが、更に、確認証サーバが確認証発行の事実の問い合わせに答えることができるようにした。

文書交換サーバは、文書自体を安全に交換・保管して完全性を保証する文書保管（アーカイブ）の機能を実現する。LGWAN文書交換は文書交換サーバの文書交換機能と保管の機能を使って文書交換を実現した。

確認証サーバの確認証及び文書交換サーバの文書の実体は データベースサーバに納めることとした。データベースサーバの内容は改ざん・盗用できないよう保護される。

データベースサーバの重要な情報は、光磁気技術を使った書き換え不可能なWORM（Write Once Read many）ディスクにバックアップし、監査及び障害に備える。

各サーバの秘密鍵はHSM（Hardware Security Module）内に納められ、安全な運用を確保した。

各都道府県NOCの公証基盤サーバ群は全国NOCの公証基盤サーバ群と補完し合って、サービスレベルとセキュリティレベルを保つようにした。

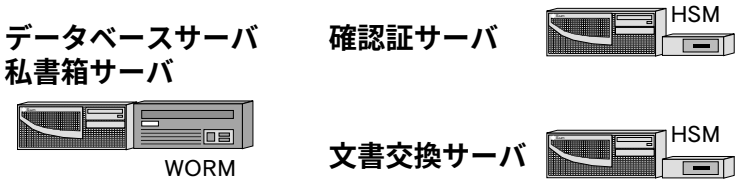

図 6-10 公証基盤サーバ群

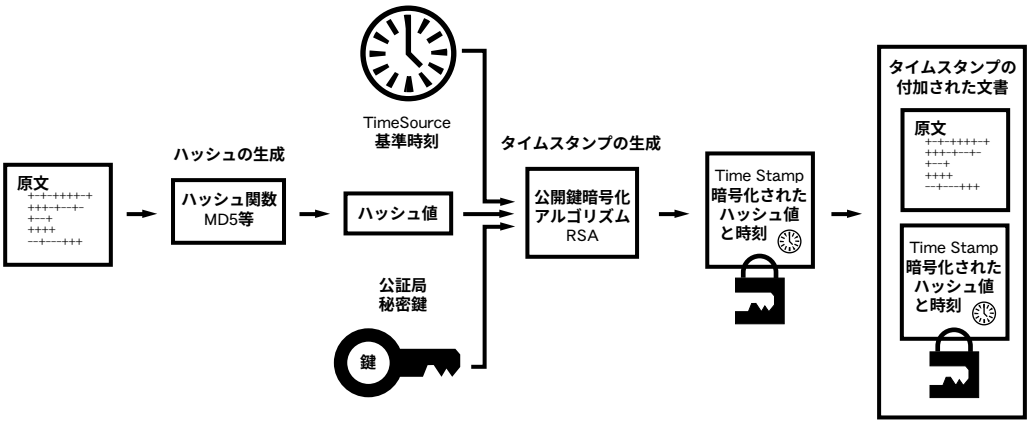

図 6-11 確認証の発行（タイムスタンピング）

6.6 XML電文交換基盤の実証実験結果

XMLを本アプリケーション基盤におけるトランザクション処理基盤に採用した。

動作概念は次のとおりである。XML電文ルータはXML電文を目的のXML G/Wに届ける。XML電文交換基盤ではXML G/Wによって、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。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できる。

全国NOCにXML電文交換サーバを設置し、共通情報のサービスを行うこととした。各都道府県NOCにXML電文交換サーバを設置し、各都道府県NOCのXML電文交換サーバをメッシュ状に接続することによって、障害が発生した場合の影響を局所化し、各地方公共団体へのサービスを行う構造とした。

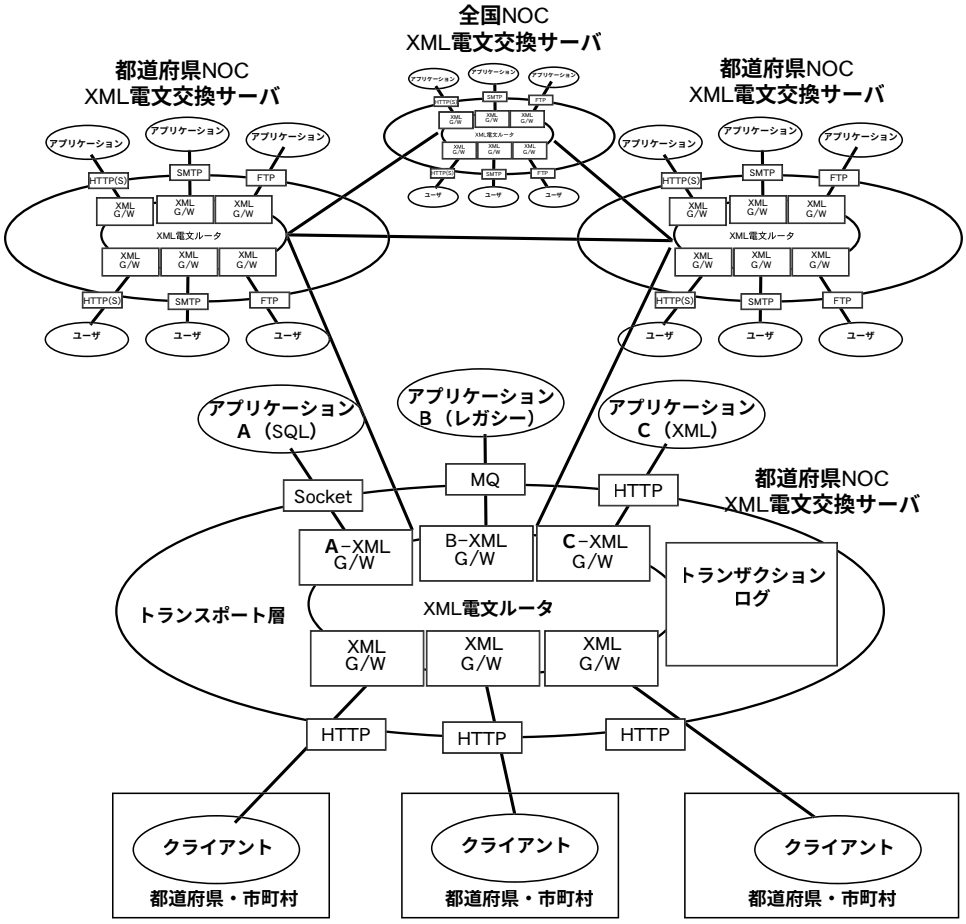

図 6-12 XML電文交換基盤の構築

6.7 実証実験の考察

6.7.1 アプリケーション基盤全般

アプリケーション基盤全般として、以下の課題がある。

(1)リダンダンシー問題

サーバの構成が冗長化されていないため、原則として24時間運用ではサービスの 一時的な停止が起こる可能性がある。

(2) スケーラビリティ問題

サーバの性能及びディスク容量などの性能設計が、最小構成となっているため、 今後の使用頻度やデータ量及びユーザ数の増加に対して対策を取る必要がある。

解決策

・複数のサーバハードとソフトウェア機能のたすき掛け運用によって、単純にサー バハードを２重化（２倍化）することなく、上記の問題は解決可能である。

・複数のNOCのたすき掛け運用などによって（一か所のNOCを強化するのではなく）解決する方向が望ましい。

(3) ディスク容量の問題

サーバのディスク容量が最小構成となっているため、今後の使用頻度やデータ量及びユーザ数の増加に対して対策を取る必要がある。

解決策

・クラスターディスクサーバの活用によって解決する。

(4) ユーザアカウント管理問題

各サーバにおけるアカウント管理が統一化されていないため、管理が煩雑で負荷が高い。今後、多数のユーザに対してサービ スを提供する際、アカウント管理の統一が必要となる。

解決策

職員個人認証、ディレクトリ基盤の活用方法の工夫、ディレクトリ基盤の機能強化 などの方法を考慮して、この問題は解決可能である。

(5) 規格の問題

規格に対して、各製品間での実現方法や解釈方法の不一致な点があり、多くの問題が発生した。

解決策

規格の詳細を厳密に定義し、解釈方法の徹底を行い、相互運用試験プログラムによる実証試験を前提とした認定制度を設けるといった手段によって解決可能である。

6.7.2 認証基盤

(1) 認証プロファイル

認証プロファイルの解釈方法が各製品間で不一致な点があり、認証動作が安定してないことがあった。

解決策

認証プロファイルの厳密な定義をし、相互運用試験プログラムによる実証試験を前提とした認定制度を設けるといった手段によって解決可能である。

(2) ICカードの規格の問題

ICカードの規格、ICカードリーダ及びドライバーの不統一のため、今後の文書交換に困難が生じる可能性が高い。

解決策

・規格の詳細を厳密化し公開することで、より多くの製品が動作可能な環境を用意する（マルチベンダー化）。ICカードやICカードリーダに関して相互運用試験プログラムを用意し、実際の製品採用の際に実証試験を義務付ける。

6.7.3 ディレクトリ基盤

(1) 構成

ディレクトリサーバは全国NOCに集中配置の構成になっているため、今後の使用頻度の増大、ユーザ数の増加に対して対策を取る必要がある。

解決策

・ディレクトリサーバを都道府県NOCなどに分散配置を行う。

(2) LDIF解釈

製品間でLDIFファイル（ディレクトリ間情報交換規格）の解釈の不一致により、ディレクトリ間の情報交換が直接できず、手動操作により加工が必要となるなど困難が見られた。

解決策

・LGWANとしての仕様を明確にし、該当製品のフォーマットを合わせてもらう、又は、変換するためのツールを開発することで解決可能である。

6.7.4 検証

(1) CRLプロファイル

CRLプロファイルの作成方法や解釈方法の不一致による、問題発生が見られた。

解決策

・CRLプロファイル作成方法を厳密に定義し、解釈方法の徹底を行い、相互運用試験プログラムによる実証試験を前提とした認定制度を設けるといった手段によって解決可能である。

6.7.5 公証基盤

「7.4.1 電子文書交換」を参照。

6.7.6 XML電文交換基盤

「7.4.1 電子文書交換」を参照。

7. 基本サービス

7.1 実験項目と内容

基本サービスはアプリケーション基盤と連動して、総合行政ネットワーク運営主体が提供するサービスであり、電子文書交換、WWWアプリケーションについて実証実験した。この実証実験の結果を基に、ASPガイドラインを作成した。

7.2 電子文書交換の実証実験結果

7.2.1 電子文書交換構築

文書の送信処理は、起案、回議/合議、決裁、校合、公印付与を行った後、送信を行うという流れになる。受信側は、収受、受信審査、保管した後、送信側に受領確認（受領否認）を行い、回覧/閲覧、廃棄の処理となる。

電子文書交換システムの構築範囲は、送信側文書取扱主任が公文書を受信側の文書取扱主任に送信し、受信側文書取扱主任が受取った文書を確認、保管し、送信側文書取扱主任に受領確認(受領否認）を行うところまでとした。

文書の起案、回議/合議、決裁、校合といった地方公共団体における文書管理システムについては対象としていないので、必要な機能は、各地方公共団体で準備する必要がある。また、文書フォーマットなど実際に団体間で文書交換を行うための取り決めも今後必要である。

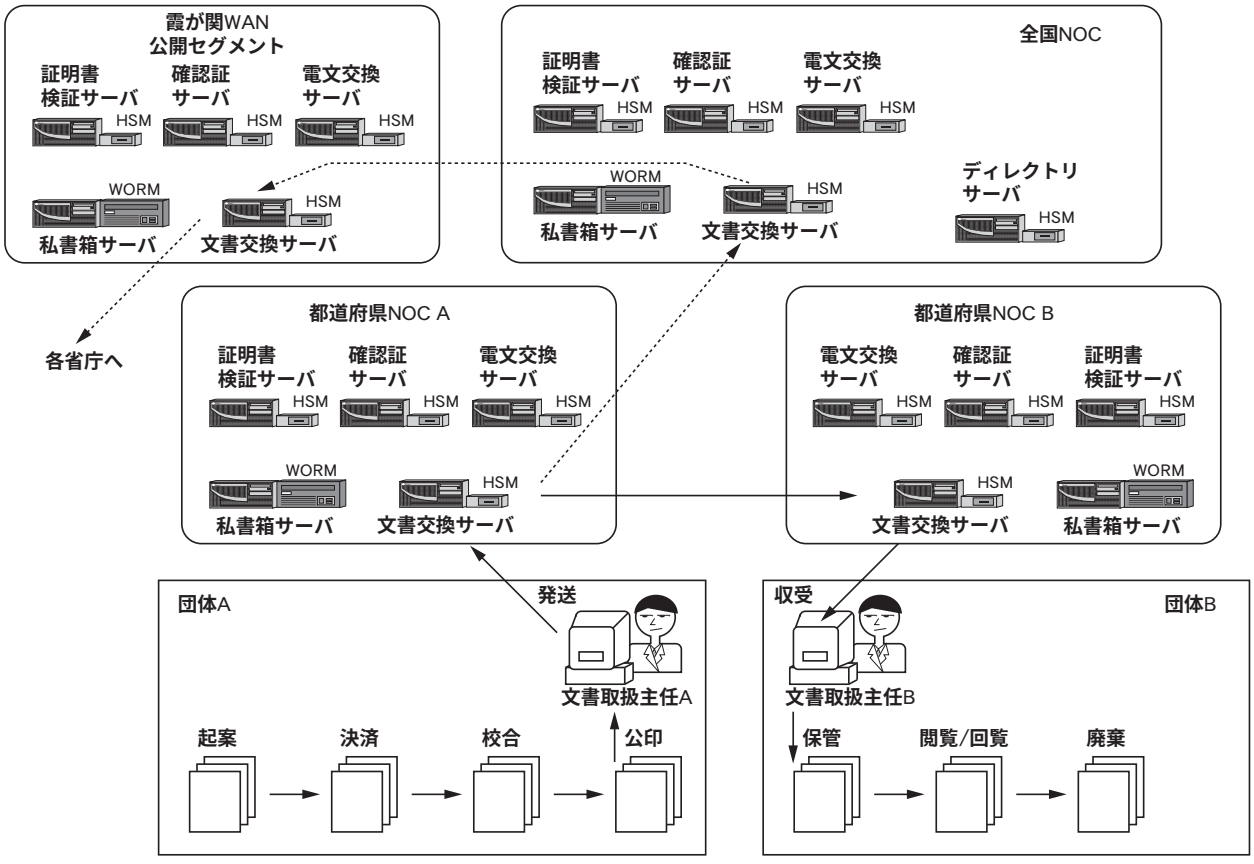

図 7-1 電子文書交換システム構成

7.2.2 エンドユーザの宛名選択

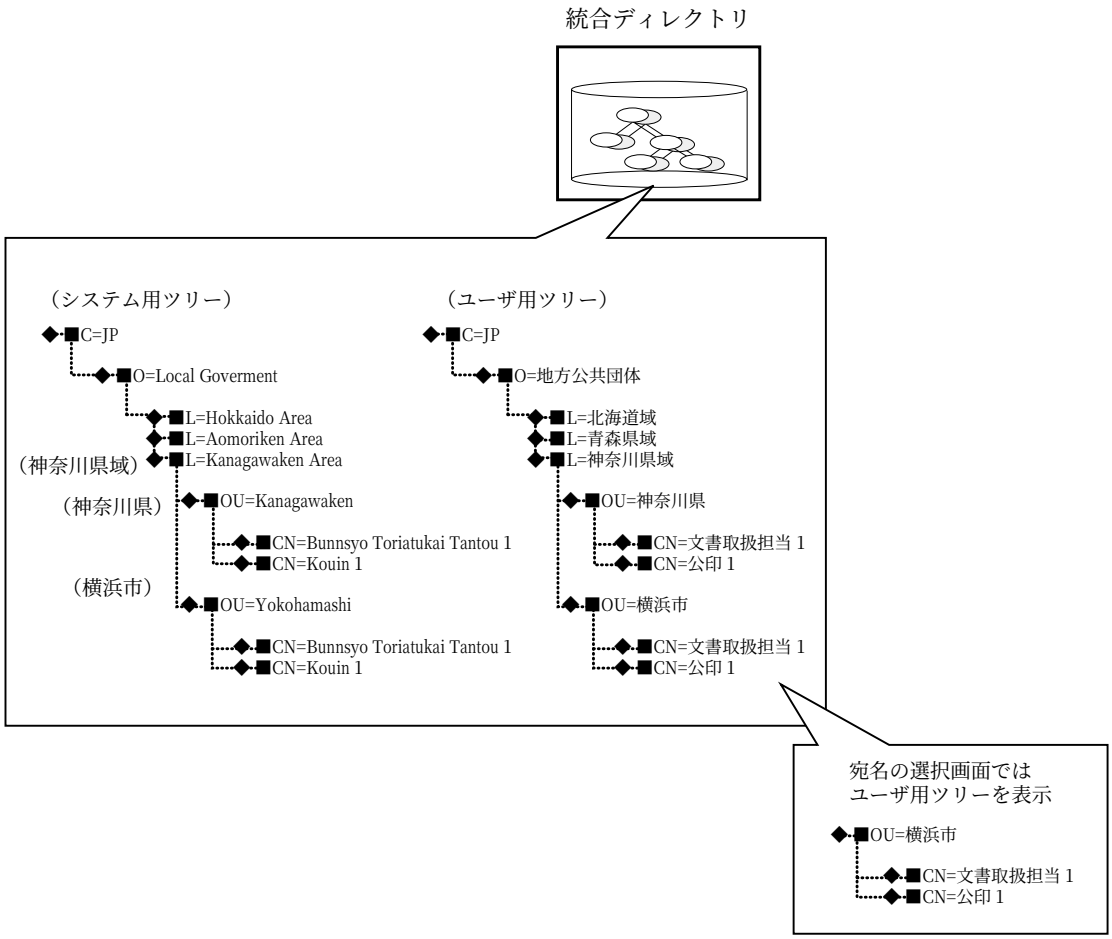

図 7-2 エンドユーザの宛名選択

LGWAN文書交換の宛名選択画面では、統合ディレクトリのユーザ用ツリーを使用して宛名選択を行うため、ユーザはシステム用ツリーの英数字のDNを意識する必要はない構成とした。

7.2.3 証明書の表示

構成要素	内容
・・・・・・	・・・・・・・・・・・
(1) 発行者名（CA） （Issuer name）	C=JP,O=local Goverment,OU=Zenkoku NOC, OU=Kanagawaken NOC CA
・・・・・・	・・・・・・・・・・・
(2) 所有者名 （Subject name）	C=JP,O=local Goverment,L=Kanagawaken Area, OU=Yokohamashi,CN=Kouin 1
・・・・・・	・・・・・・・・・・・
(3) 所有者代替名 （Subject alternative name）	横浜市公印１
(4) 発行者代替名 （Issuer alternative name）	神奈川県NOC認証局
・・・・・・ ・・・・・・	・・・・・・・・・・・ ・・・・・・・・・・・

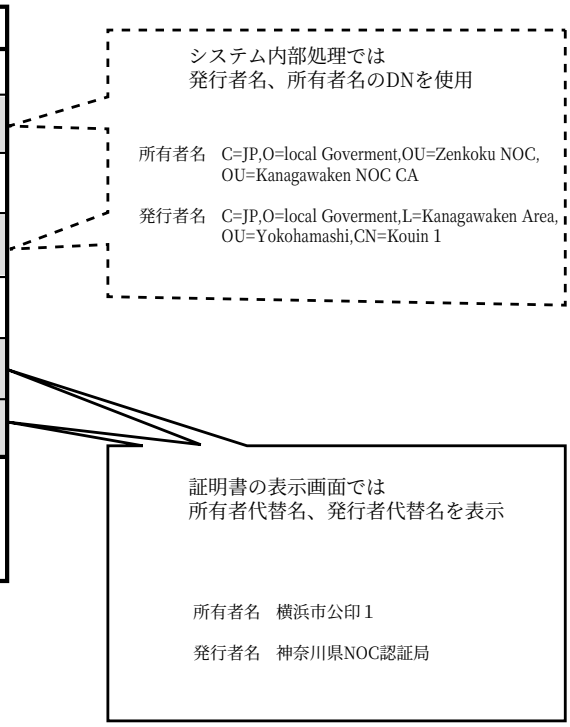

図 7-3 エンドユーザへの証明書の表示

証明書の表示には、証明書内の所有者代替名、発行者代替名にある日本語表記を使用し、所有者名、発行者名のDNはシステムの内部処理でのみ使用することで、エンドユーザーに違和感の無い使い勝手となるようにした。

7.2.4 電子文書交換の実験

(1) ICカードによる公印付与の確認

各実験参加団体が事前に配布したICカードを使い、テスト用公文書にて公印付与の確認を行った。事前に配布したICカードは、正常なカードと失効しているカードとし、正常時・異常時の両ケースについて確認、検証作業を行った。

(2) 文書交換サーバへの接続確認

各実験参加団体がブラウザ（今回の実証実験においては、NetScapeを利用）を利用して文書交換サーバに接続し、事前に配布した文書取扱主任用ICカードによるログインの確認を行った。ICカードは、正常なカードと失効しているカードの両方を使った。失効しているICカードでのログインは失敗し、正常なICカードでのログインは成功したことを確認した。

(3) 文書交換サーバから全国NOCへの公文書の送信確認

各実験参加団体が文書交換サーバを利用して作成した公印付の公文書を全国NOC宛に送信できることを確認した。

(4) 全国NOCからの公文書の受信確認

全国NOCから各実験参加団体に対してテスト用の公文書を送信し、各実験参加団体が文書交換サーバを利用してテスト用の公文書を全国NOCから受信した。受信した公文書を開封し、内容を確認した。

(5) 受信公文書の公印確認

各実験参加団体が受信した公文書に付与されている公印の確認を行った。

(6) 受領確認の送信確認

各実験参加団体が受信した公文書に対して受領確認を送信し、全国NOCで受領確認を行った。

(7) 確認証の表示確認

各実験参加団体が確認証の表示を行い、確認証が発行され、内容が正しく表示されていることを確認した。

(8) 複数種類の公文書の送受確認（各実験参加団体主体作業）

実際の文書作成で使用されている様々な形式のファイル（テキスト、既存のワープロソフト、イメージなど）を添付して、実際に送受し、正しく送受できていることが確認できた。

7.2.5 霞が関WANとの電子文書交換

霞が関WANとの電子文書交換試験はLGWANと基本的に同様であるが、以下の点が異なる。

・霞が関WANで既に導入済みのICカードを使用する。

・宛先情報の問い合わせは霞が関WAN標準のX.500サーバを使用する。

実証実験の結果、証明書フォーマットの違いによる問題が顕在化した。図7-4に示すように、文書交換システムではWWWブラウザ（Netscape）をクライアントソフトとしているが、証明書に日本語など２バイトコードが入っている場合には、証明書の情報がWWWブラウザに取り込めず、サーバとの接続ができなかった。

霞が関WAN仕様のICカードは証明書に日本語が含まれているため使用できず、ローマ字のみを使ったLGWAN仕様のICカードでのみ文書交換が可能であった。今後、WWWブラウザの日本語証明書対応化を行う必要がある。

暫定処置としてLGWAN仕様のICカードを使用した場合には、問題なく文書交換が可能であった。

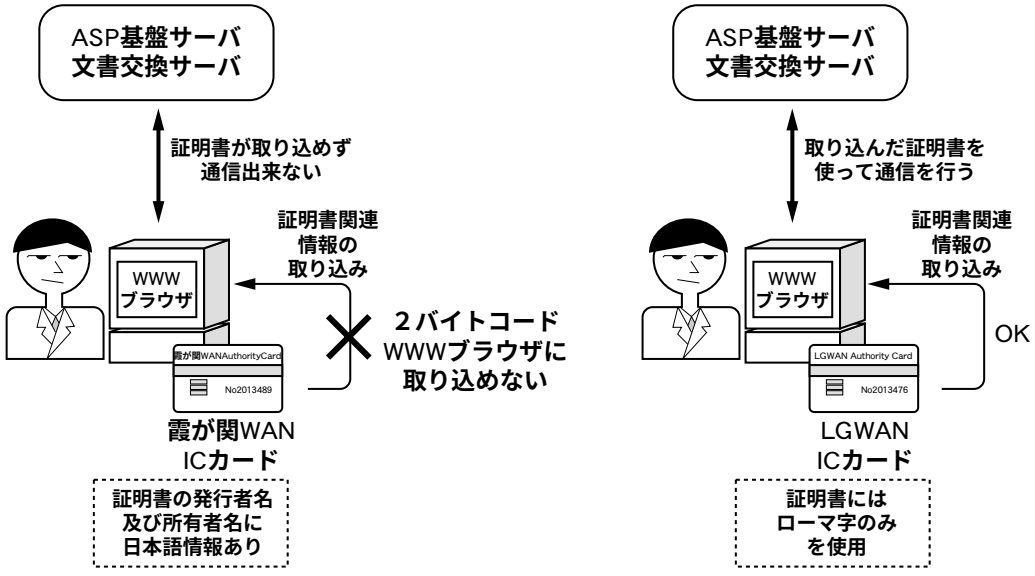

図 7-4 電子文書交換とICカード

7.3 WWWアプリケーションの実証実験結果

WWWアプリケーションサーバを導入し、実証実験用のサンプル掲示板やデータベースを構築した。

今回用意したサンプルアプリケーションは、ICカードによって認証を行うケースと認証が不要なケースを用意した。

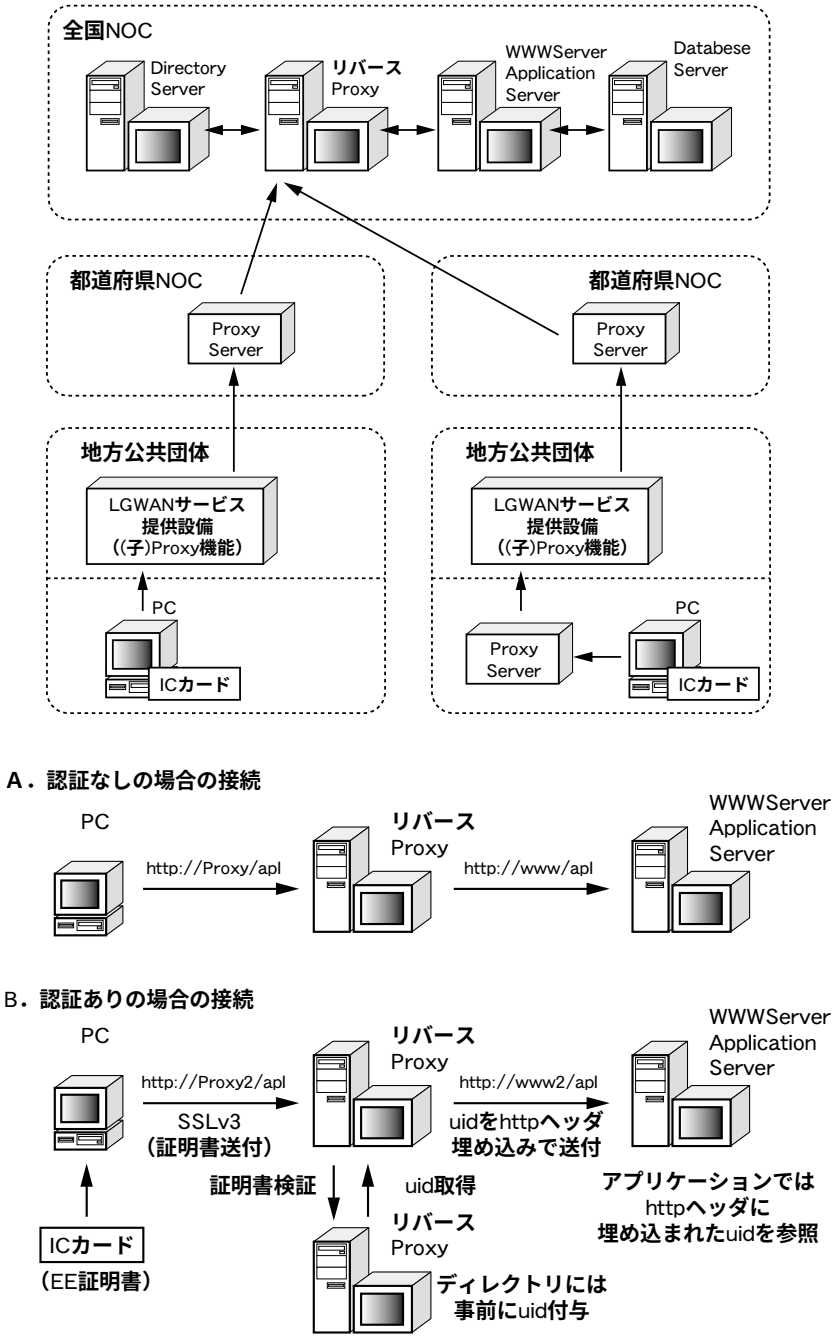

図 7-5 情報共有掲示板システムの構成

7.4 実証実験の考察

7.4.1 電子文書交換

今回の実証実験では文書の配送部分を構築した。文書の作成や管理についてはサンプルアプリケーションを提供したものの、文書のフォーマットなど実際に団体間で文書の交換を行うための取り決めがなされていない。また、文書の管理や検索性を高めるためのヘッダファイルについても同様に規定していない。

団体間での文書交換についての方向性を検討する必要がある。

(1) 確認証の問題

確認証の内容、表記方法が適切でない。

解決策

・文書規則などに則った形式、内容、表現に改める。

以下は、アプリケーション基盤全般が持つ問題と同様である。

(2)リダンダンシー問題

サーバの構成が冗長化されていないため、原則として24時間運用ではサービスの 一時的な停止が起こる可能性がある。

(3) スケーラビリティ問題

サーバの性能及びディスク容量などの性能設計が、最小構成となっているため、 今後の使用頻度の増大、データの増大、ユーザの増加に対して対策をとる必要がある。

解決策

・複数のサーバハードとソフトウェア機能のたすき掛け運用によって（単純にサー バハードを２重化（２倍化）することなく）、解決可能である。

・一か所のNOCを強化することなく、複数のNOCのたすき掛け運用などによって、解決する方向が望ましい。

(4) ディスク容量の問題

サーバのディスク容量が最小構成となっているため、今後の使用頻度の増大、データの増大、ユーザの増加に対して対策をとる必要がある。

解決策

・クラスターディスクサーバなどの活用によって解決する。

(5) ユーザアカウント管理問題

各サーバにおけるアカウント管理が統一化されていないため、管理が煩雑で負荷が高い。今後、多数のユーザに対してサービスを提供する際、アカウント管理の統一が必要となる。

解決策

職員個人認証、ディレクトリ基盤の活用方法の工夫、ディレクトリ基盤の機能強化などの方法を考慮して、この問題は解決可能である。

(6)ブラウザの日本語証明書取り込み不可問題

Netscapeでは日本語を使った証明書の取り込みが出来ない。

解決策

AOL社に日本語対応をしてもらうよう働きかける、また、Internet ExploreなどNetscape以外のブラウザ用ICカードドライバを開発することで対応可能である。

7.4.2 WWWアプリケーション

今回構築したアプリケーションはあくまでサンプルであり、実際には、どのようなサービスを標準として用意するか検討し、必要に応じて手直しをする必要がある。

また、利用量の増加に対して、ポータルとなるサーバの分離や負荷分散など機器の増設が必要となる。

8. 管理システム

8.1 実験項目と内容

実証実験ネットワークの管理を行うためのシステムを構築し、総合行政ネットワークの運用管理の方法を検討した。

8.2 監視システムの実証実験結果

snmp及びpingによるネットワークノードの生死を監視する稼働監視システム、FirewallとIDSのログ収集、分析によるセキュリティ監視システムを構築した。

3300団体への展開を想定し、都道府県NOC単位に稼働監視システムを設け、県域内の各市町村のLGWANサービス提供設備までを遠隔で監視する構成とした。全国NOCの監視サーバで一元監視を行えることを確認した。

ファシリティ監視を行う装置は、検討の結果、市販の製品では必要機能を満たせないため、仕様設計までを行い、実装は見送った。

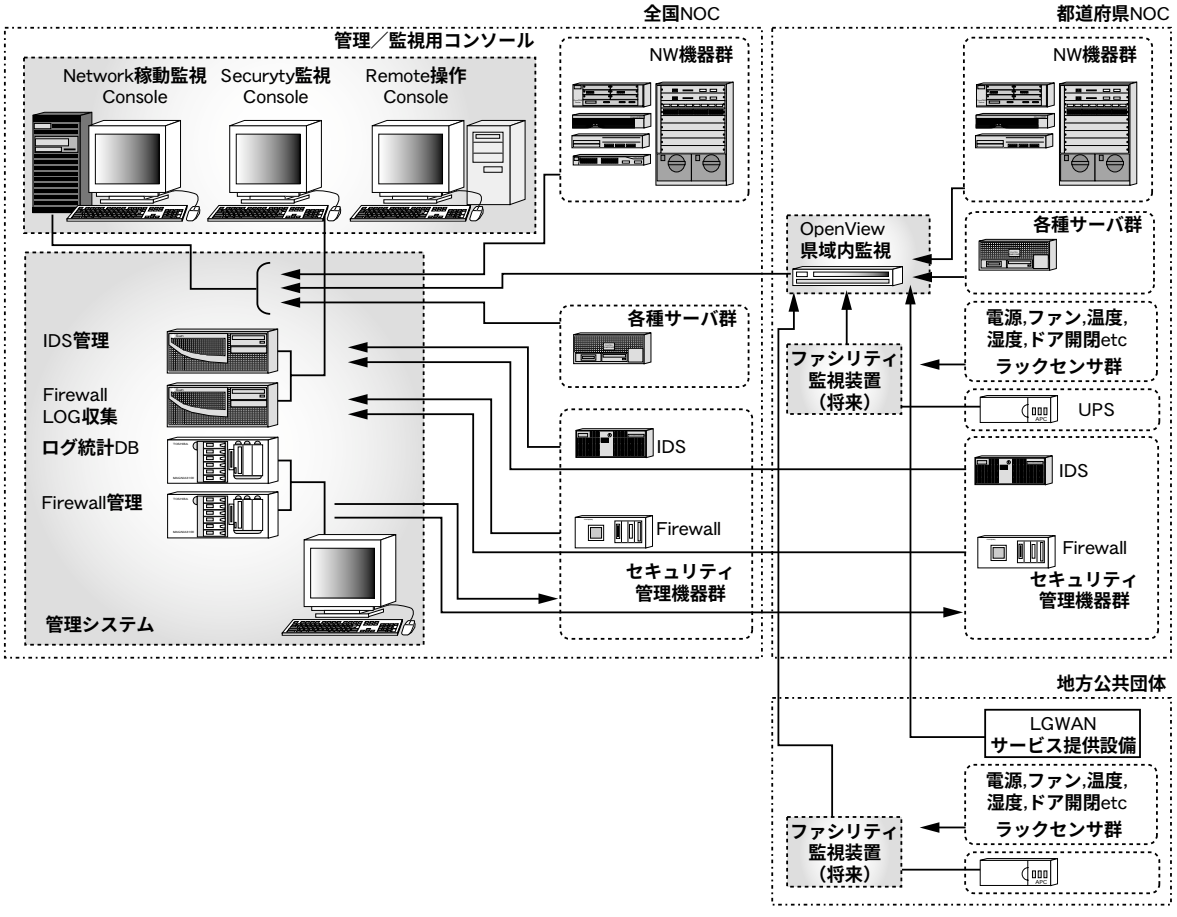

図 8-1 管理システムの構成

8.3 電子メールウィルス対策機能の実証実験結果

電子メールのウィルス対策を行うための方式として、電子メールの配信がスタティックである場合を前提に全国NOCでの集中監視方式を設計した。しかし、電子メールの配信は、今後、MXによる動的な配信（N:N）にしていくべきとした。その場合は、各地方公共団体のメールサーバ同士が直接接続してメール交換を行うため、地方公共団体側のメールサーバにウィルス監視機能を持たせる必要がある。よって、本実験では実際の導入は見送った。

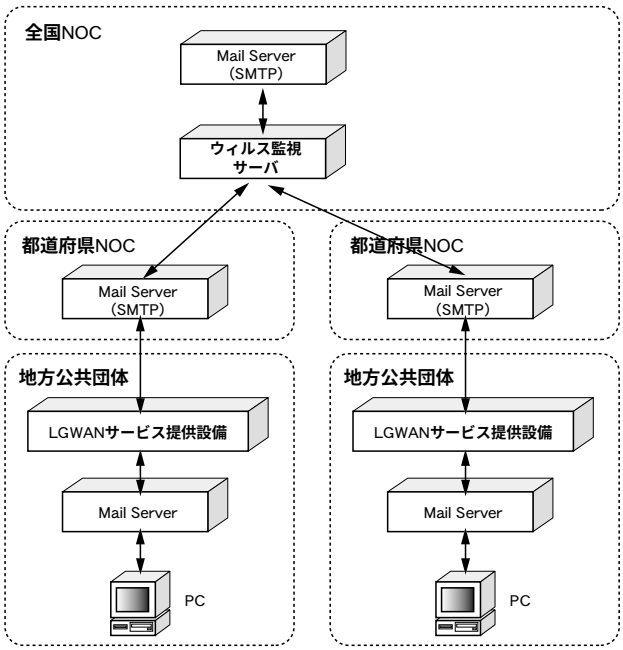

図 8-2 電子メールのウィルス監視システムの構成

8.4 遠隔からの電源制御機能の実証実験結果

各サーバやFirewall、VPN装置など、手動で電源停止処理の必要な機器の遠隔からの電源停止処理を行う機能の設計を行った。UPSの電源監視情報を取り出し、停電時に自動的に電源を停止・復電時に自動起動する機能を持たせるとともに、計画停止に対応したマニュアル停止機能も持たせる構成とした。

なお、既製品では仕様を満たせず、ハードからの開発が必要となったため、導入は見送った。

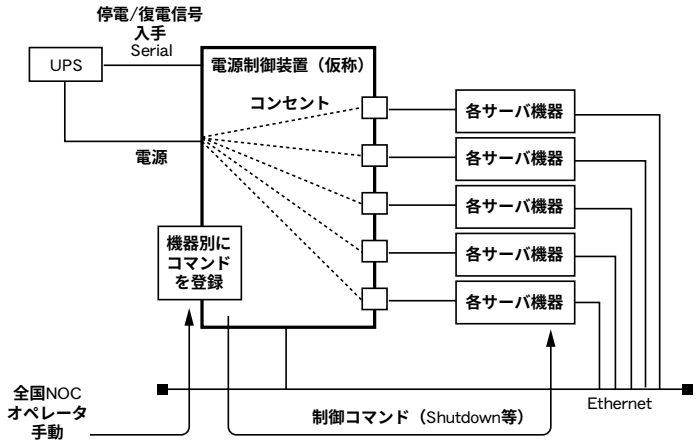

図 8-3 遠隔からの電源制御機能の構成

8.5 実証実験の考察

⑴監視対象の拡充

実証実験では必要最小限の監視にとどめている。

本運用の内容を明確にした上で、ファシリティ監視やサーバリソース監視など監視対象を拡充する必要がある。

⑵各機器の管理用アカウントの統一管理化

管理対象機器が膨大な数となるので、パスワードの更新作業も簡単に行うことができない。統一的な認証機構の導入を検討する必要がある。

⑶管理機能の追加

本運用の内容の明確化に合わせ、以下のような機能を追加装備することを検討する必要がある。

・遠隔からの電源制御機能

・ヘルプデスク支援機能

・トラフィック分析機能

⑷セキュリティ監視に関するアクション

セキュリティ監視時の緊急切り離し対応など、総合行政ネットワーク運営主体に委ねる権限の範囲や基準を検討する必要がある。

9. 実証実験総括

9.1 拡張性（スケーラビリティ）

(1)実証実験の結果と課題

実証実験では、各都道府県下に１０団体程度の規模までを想定したネットワーク設計を行い、第一種キャリアのMPLS網を利用して、都道府県域ごとに階層化したネットワークを実際に構築し、今後拡張する上でボトルネックとなりうる部分を確認した。3300団体を最終的に接続するために今後必要となるネットワーク機器の増設パターンを検討し、それに対応する設計を行った。

当面の課題として、都道府県NOCの窓口ルータが複数になるケースに対応するため、増設が容易な機器接続構成に見直しを行う必要がある。

(2)今後継続的に発生する課題

都道府県域ごとに接続する団体数の増加に合わせて、回線の増速や複線化、窓口ルータの増設などネットワーク機器の増設、各種サーバの増設を行う必要がある。

電子メールのメッセージ量や文書交換の送受信量の増加傾向を見て、LGWANバックボーン回線・LGWANアクセス回線の増速や、アプリケーション基盤サーバなど関連サーバの増強・増設を適宜行う必要がある。

また、新たなASPサービスの追加の際には、サービス開始の時点で予測されるトラフィック量に見合った設備投資をするとともに、利用量の増加に対応し、回線の増速及びネットワーク機器・各種サーバの増設を行う必要がある。

9.2 信頼性（アベイラビリティ）

実証実験では、全国NOCのネットワーク機器の２重化やディレクトリサーバの２重化など、部分的な信頼性向上対策については、実際に構築し、動作確認を行った。原則として24時間稼働を目標としたが、電源などファシリティに依存する点も解決されていないという意味からも完全に２重化するには至っていない。現実的に必要な要件（SLA）を検討し、不足する部分について対策を行う必要がある。

電源設備の定期点検などによる長時間な計画停止に対しては、他のNOCとの相互バックアップを取れる構成にするなど技術的に解決すべき課題として検討する必要がある。

今後、新たなASPサービスの追加などにより、SLAが変更となる場合、不足部分について対策を行う必要がある。

9.3 ネットワーク性能

実証実験では、網内の時刻同期機能の遅延測定、電子メールの到達時間測定などを行い、問題がないレベルに収まっていることを確認した。また、電子メールの配信や電子文書交換、WWWアプリケーションの利用について、動作することは確認できた。ただし、各アプリケーションでやりとりする最大データ量とその時の応答性要求を明確に定義していないので、現時点の回線容量は、十分とは言い切れない。今後、電子メールや文書交換のデータ量など具体的な利用条件の検討をした上で、必要に応じて増強を行う必要がある。

今後、新たなASPサービス追加の際には、その利用条件に合わせて、回線の増速及びネットワーク機器・各種サーバの増設を行う必要がある。

9.4 セキュリティ

実証実験では、暗号化とトンネリングによる経路分離、Firewall機能、IDSによる侵入検知を組み合わせたﾈｯﾄﾜｰｸを実際に構築し、擬似アタック試験などを行い、問題がないことを確認した。IDSについては、２重・３重に検知をする仕組みとした部分が複雑すぎて、運用負荷が高くなると考えられるため、見直しを行う必要がある。

また、セキュリティ監視時の緊急切り離し対応など運営主体に委ねる権限の範囲や基準を検討する必要がある。

今後、新たなASPサービス追加の際には、セキュリティ上問題がないか、審査を行う必要がある。また、サービス内容に応じて通過対象プロトコルを増やすなどFirewallの設定ポリシーの見直しを行う必要がある。

9.5 運用管理（マネージャビリティ）

実証実験では、3300団体に展開する機器の監視を行うため、階層構造を持たせた監視システムを構築し、技術的に問題がないことを確認した。監視項目や管理機能は必要最小限とした。ファシリティ監視と遠隔からの電源制御については、要求機能を満たす市販の製品がなく、設計までに止めた。重要度の高い機能から優先して、追加整備を行う必要がある。また、アカウント管理については現時点では機器やサーバごとに個別に管理しており、統一化対策を検討する必要がある。

今後、運用状況を見て、サーバリソースの監視など監視対象の追加やトラフィック分析機能など機能追加についても、必要に応じて追加整備を行う必要がある。

9.6 柔軟性（アダプタビリティ）

(1)都道府県WANとの接続

都道府県WANを実際に接続し、技術検証を行い、ATMによる仮想LAN技術を前提とした技術仕様（物理的な接続I/FやIPアドレスの割付など）を確立した。実験では接続仕様はEthrenetのみとしたが、今後、無線やダークファイバなど様々な技術を使うケースがありうる。そのため、全国の各都道府県域で実際に計画している内容を調査し、適切な仕様を定める必要がある。また、接続点となる都道府県NOCのネットワーク機器は、より柔軟性のある構成に見直しを行う必要がある。

今後、実際に都道府県WANとの接続を行う際にはセキュリティなどの問題がないか技術審査を行う必要がある。

(2)ASP接続セグメント

サービス提供者として、各運営主体、地方公共団体、第三者機関（ASPコンソーシアム参加者）を想定し、物理的な接続方法やIPアドレスやドメインの割り当てなどの接続仕様を検討した。物理的な接続点として、全国NOCや都道府県NOCにASPサーバを設置するケース以外に、IDC（Internet Data Center）を利用する場合や各地方公共団体に設置する場合を想定した。

実験では仮想ASPを構築し、ASP接続時の技術仕様について、NOCにサーバを設置するケースと団体側にサーバを設置するケースについて、技術仕様（物理的な接続I/FやIPアドレス・ドメインの割付など）を確認した。物理的な接続点である、各NOCのネットワーク機器構成やLGWAN ASP接続装置については、今後サービス提供形態が多様化することが予想されるので、より柔軟性のある構成に見直しを行う必要がある。

今後、ASPサービス提供者との接続を行う際に、技術審査を行い、必要に応じてネットワーク機器を増設する必要がある。

9.7 費用対効果（運用コスト）

各参加団体にとって適切なコストとなることを考慮し、本運用当初は参加団体が少ないことから、性能や信頼性は必要最小限の構成に止めている。

今後、参加団体の増加による追加投資が可能となった時点で、順次追加整備を行っていく必要がある。また、回線の増速及びネットワーク機器・各種サーバの増設を行う際には、コスト面の評価を行う必要がある。

9.8 霞が関WANとの相互接続

霞が関WAN側及びLGWAN側に相手側の参加団体から接続可能な公開セグメントを設け、電子メールの交換、電子文書の交換、WWWサーバによる情報の共有化を行った。

(1)電子メールの交換

X.400とSMTPのゲートウェイ接続を使い、一般的な電子メールの交換が正常に行えることは確認できた。但し、電子メールの容量は霞が関WANでは10MByteまでの伝送を保証しているが、LGWANでは2MB程度までしか送受信できないように制限をかけている団体もあった。作法について調整が必要である。

霞が関WANでは各省庁毎にX.400による到達確認を行う規則であるが、LGWANの実証実験ではX.400サーバは全国NOCに１台としたので、そこでしか到達確認が返せない。制度面を含む検討が必要である。

霞が関WANではX.400を使用しており、変換が必要となる。その際にすべてのLGWANのドメイン名を変換するための登録を行う必要がある。逆に各団体には霞が関WAN接続省庁のドメインを振り分けできるように定義してもらう必要がある。実証実験期間中は実験用の仮想ドメインを使ったが、本運用向けに実際に使うドメインを定義する必要がある。

(2)電子文書の交換

電子文書の交換では霞が関WAN仕様のICカードには証明書の一部に日本語を使っているため、WWWブラウザからサーバに接続できない問題が発生した。今後、WWWブラウザの日本語証明書対応化を行う必要がある。

LGWANの仕様のICカードでは文書交換を行うことができた。本運用に向け、公文書のフォーマットでどうするか、今後検討が必要である。

(3) WWWサーバによる情報の共有化

LGWAN側のPCから霞が関WAN側のWWWサーバを利用した場合、霞が関WAN側のPCからLGWAN側のWWWサーバを利用した場合のいずれも問題なく動作が確認できた。

今回はICカードによる認証は対象外であり、本運用に向け、認証が必要なサーバについてのユーザ登録方法など、実際の運用を踏まえた検討を進める必要がある。

9.9 その他特記事項

(1) ファシリティ要件

都道府県NOCのファシリティ条件として、実証実験では「都道府県NOC設置ファシリティ条件」を示し、導入に当たり調査を実施したが、すべての項目を満たしていない団体も多かった。許容範囲はどこまでとするのが適当か検討の必要がある。

また、市町村のLGWANサービス提供設備のファシリティ要件は都道府県NOCと同等レベルを満たすことは実質困難であった。どこまでを前提とすべきか検討の必要がある。

(2) 地方公共団体内LANとの整合性

NTP、SMTPについて、LGWANの中では問題なく機能することは確認できたが、各地方公共団体内LANの時刻同期をどうするか、また、LGWANのメール形式の標準仕様やマナーなどについては、制度面の整備を含めて今後の課題とした。

表9-1 実証実験の結果及び検討課題一覧

	実証実験の結果	実証実験における課題	本運用後、継続的に発生する課題
拡張性	第一種ｷｬﾘｱのMPLS網を利用して、都道府県域ごとに階層化したﾈｯﾄﾜｰｸを実際に構築し、今後拡張する上でﾎﾞﾄﾙﾈｯｸとなりうる部分を確認した。 3300団体を最終的に接続するために今後必要となるﾈｯﾄﾜｰｸ機器の増設ﾊﾟﾀｰﾝを検討し、それに対応するための設計を行った。	都道府県NOCのﾈｯﾄﾜｰｸ機器の接続構成を拡張が容易な構成に見直しを行う。	接続団体数の増加に合わせてLGWANﾊﾞｯｸﾎﾞｰﾝ回線の増速及びﾈｯﾄﾜｰｸ機器・各種ｻｰﾊﾞの増設を行う。 新たなASPｻｰﾋﾞｽの追加や利用量の増加に対応し、LGWANﾊﾞｯｸﾎﾞｰﾝ回線の増速及びﾈｯﾄﾜｰｸ機器・各種ｻｰﾊﾞの増設を行う。
信頼性	全国NOCのLGWANﾊﾞｯｸﾎﾞｰﾝ回線及びﾈｯﾄﾜｰｸ機器の２重化を行い、障害時に自動的に切り替えを行えることを確認した。 同様に、統合ﾘﾎﾟｼﾞﾄﾘなど一部のAP基盤は２重化構成での動作を確認した。	現実的に必要な要件（SLA）を検討し、不足する部分について対策を行う。 計画停止に対応するための技術検討を行う。	新たなASPｻｰﾋﾞｽの追加などにより、SLAが変更となる場合、不足部分について対策を行う。
性能	網内の時刻同期機能の遅延測定、電子メールの到達時間測定などを行い、問題がないレベルに収まっていることを確認した。	具体的な利用条件の検討を行い、必要に応じて回線の増速及びﾈｯﾄﾜｰｸ機器・各種ｻｰﾊﾞの増設を行う。	新たなASPｻｰﾋﾞｽの利用条件に合わせて、LGWANﾊﾞｯｸﾎﾞｰﾝ回線の増速及びﾈｯﾄﾜｰｸ機器・各種ｻｰﾊﾞの増設を行う。
セキュリティ	暗号化、IDS、Firewallを組み合わせたﾈｯﾄﾜｰｸを実際に構築し、擬似ｱﾀｯｸ試験などを行い、問題がないことを確認した。	IDS監視構成の見直しを行う。 緊急切り離し権限など運用基準の検討を行う。	都道府県WAN接続の際に、技術審査を行う。 新たなASPｻｰﾋﾞｽの内容によって、技術審査を行う。必要に応じてFirewallのﾎﾟﾘｼｰを見直す。
運用管理	3300団体に展開する機器の監視を行うため、階層構造を持たせた監視ｼｽﾃﾑを構築し、技術的に問題がないことを確認した。	遠隔からの電源制御やファシリティ監視など追加整備を行う。 アカウント管理の統一化対策を検討する。	運用状況を見て、監視項目や管理機能を追加する。 新たなASPｻｰﾋﾞｽの内容によって、必要があれば見直しを行う。
柔軟性	都道府県WANを実際に接続し、技術検証を行い、ATMによる仮想LAN技術を前提とした技術仕様（物理的な接続I/FやIPｱﾄﾞﾚｽの割付など）を確認した。 仮想ASPを構築し、ASP接続時の技術仕様について、NOCにｻｰﾊﾞを設置するｹｰｽと団体側にｻｰﾊﾞを設置するｹｰｽについて、技術仕様（物理的な接続I/FやIPｱﾄﾞﾚｽ・ﾄﾞﾒｲﾝの割付など）を確認した。	都道府県WANの計画についてヒアリングを行い、接続仕様に反映する。 都道府県NOCのﾈｯﾄﾜｰｸ機器の接続構成を拡張が容易な構成に見直しを行う。	都道府県WANとの接続を行う際に、技術審査を行う。 また、接続仕様に合わせ、ﾈｯﾄﾜｰｸ機器のｲﾝﾀｰﾌｪｰｽを増設する。 ASPｻｰﾋﾞｽ提供を行う際に、技術審査を行う。必要に応じてﾈｯﾄﾜｰｸ機器を増設する。
費用対効果	参加団体にとって適切なコストとなることを考慮し、当初は参加団体が少ないことから、信頼性等は必要最小限の構成に止めた構成とした。		回線の増速及びﾈｯﾄﾜｰｸ機器・各種ｻｰﾊﾞの増設に対して、ｺｽﾄ面の評価を行う。
その他	都道府県NOCを対象にﾌｧｼﾘﾃｨ要件を検討し、各都道府県及び市町村に対して調査を行った。条件を満たすことが困難な団体では、ﾊｳｼﾞﾝｸﾞ方式を一部の団体で実行し、要件を満たせることを確認した。	都道府県NOC及び市町村のﾌｧｼﾘﾃｨ要件について満たすべき範囲を検討する。 時刻同期やメールの利用マナーなど団体側の制度に関する取り決め範囲を検討する。	