セキュア地域イントラネットデザイン

佐藤 修二*

A secure regional intranet design

Shuhji Satoh*

地方自治体では, 住民記録, 戸籍, 税, 公的個人認証, 住基ネットなど, 個人情報にかかわる情報を広域にまたがって取り扱うためセキュリティ確保を考慮したネットワーク設計が必要である. 本論文では, 筆者が現在構築を行っている広域ネットワークをモデルとしてセキュリティ, プライバシーを考慮したネットワークソリューションとCWDMを採用したネットワークアーキテクチャを, 広域にまたがってセキュリティを確保するための仕組みとして提案する. ネットワークとセキュリティは, サーバーとともにシステム基盤設計の基幹となるものであり, システムの安定性, 拡張性, 信頼性, 完全性に強く影響を与える. 本論文で取り扱うように, 計画段階からセキュリティ対策をネットワーク方針として組み込むことが重要である.

Local governments' networks must be designed to insure security as they handle personal information, such as residents' records, family registers, taxes, public individual certifications, and Juki Net (resident registry network). In this paper, using as a model the regional intranet network which the author is currently building, the network architecture which applies the network solution and CWDM in consideration of security and privacy is proposed as mechanism for securing security over a wide area. Together with the servers, networks and security are key ingredients of the basic design of a regional system, and significantly affect its stability, extendibility, reliability, and completeness. It is important to incorporate the security measure as a network policy in the planning stage as exemplified in this paper.

Key Words & Phrases：ネットワークアーキテクチャ, CWDM, 地域イントラネット, ネットワークメソドロジー, セキュリティ
network architecture, CWDM, regional intranet, network design methodology, security

1. はじめに

「e-Japan重点計画」（平成13年3月IT戦略本部決定）[1]のもと総務省では, 教育・福祉などの住民サービスの向上, 行政の効率化, 情報格差（デジタル・ディバイド）の是正などの観点から, 総合的に地域の情報化を推進している.

特に, 電子自治体の構築などのための地域公共ネットワークの整備推進については, 平成13年10月に作成・発表した「全国ブロードバンド構想」の中で, 学校, 図書館, 公民館, 市役所などを接続する地域公共ネットワークについて, 平成17（2005）年度までの全国整備を提唱している.

この実現に向けて, 地域の教育, 行政, 福祉, 医療, 防災などの高度化を図るために,「地域イントラネット基盤施設整備事業」などの補助事業を充実するとともに, 地方単独事業の活用も図ることとし, 補助事業, 単独事業ともに適切に地方財政措置を講じるなど, 総務省全体として地方公共団体などを支援している.

そして, 行政サービスを行う単位である市町村は, 行政財政基盤の確立のために合併を行う必要がある. 平成の市町村合併は, 約3300ある市町村を約1000の自治体に統合するために, 広域にまたがった合併となる. 行政事務のためのネットワークを広域利用するために, 地域公共ネットワークの構築が合併にともない促進される.

地域情報化計画にあたって使用する設計方法は,

提出日：2003年8月27日
*shu2@jp.ibm.com

企業における計画, 設計と同様な方法になるが, 考慮すべきビジネス要件, 制約は自治体特有なものとなる. 個人情報保護法, 住基ネットや今後展開される公的個人認証, 戸籍ネットワーク, マルチペイメントなど電子自治体を想定したネットワーク構築には, ワンポイントでなく全体的にセキュリティを考慮したネットワーク設計が必要となる.

本論文では, 2章で地域イントラネットのセキュリティ要件を紹介し, 3章でセキュリティ強化のために検討したネットワークソリューションについて述べ, 4章でその要件を実現するネットワークアーキテクチャを述べる.

2. 地域イントラネットのセキュリティ要件

セキュリティ要件の分類と地方自治体における利用形態別セキュリティ要件を述べる.

2.1 セキュリティ要件の分類

セキュリティ要件の分類はIBMのe-Riskというセキュリティアセスと目標策定のためのメソドロジーに基づき以下の五つとしている.

① 機密性(秘匿性)は,「アクセスを認可された者だけが情報にアクセスできることを確実にすること」(JIS X5080:2000 [2])である. 外部に公開しないプライバシーに関する情報は機密性が高くなる. 対策としてはデータや通信の暗号化や, ネットワークの分離, VPN(Virtual Private Network)などによるトンネル, NAT(Network Address Translation)などによるアドレス隠ぺいがある. 物理セキュリティや, セキュリティ教育などによるソーシャル・エンジニアリングへの対応や情報漏えいへの対応も重要である.

② 完全性は,「情報及び処理方法が、正確であること及び完全であることを保護すること」(JIS X5080:2000 [2])である. 誤りや意図によりまちがった変更がなされないことが重要である. 対策としては, 変更管理, コード改ざん防止, データ更新のログ管理や更新されたデータが正しいかの比較情報の保存がある.

③ 可用性は,「認可された利用者が、必要なときに、情報及び関連する資産にアクセスできることを確実にすること」(JIS X5080 :2000 [2])である. システムの計画外停止を減らし, 安定サービスを提供することが必要である. 対策として, DoS(Denial of Service Attack:サービス不能攻撃)対策, ウイルス対策, サーバーやネットワークの冗長化による高可用性化がある.

④ 否認不能性は,「通信を行った当事者が通信を行った事実を不正に否定できないことを保証すること」である. 対策として責任逃れを防止するために認証システム, セキュリティ管理システムやアプリケーションでのアクセスログなどを管理し, アクセス違反の監査に利用する.

⑤ 識別認証は,「個人を特定し認証すること」である. ユーザーIDと一般パスワード認証の利用以外にデジタル証明書, スマートカード(ICカード)方式や指紋, 網膜パターン, 手の静脈など身体的特徴を利用したバイオメトリックス認証がある. ネットワークを流れるパスワードの取り扱いとしては, 平文以外にハッシュしたチャレンジアンドパスワードや認証システムを利用したワンタイムパスワード方式がある.

⑥ アクセス制御は,「認証を受けた利用者/グループ/アプリケーションなどに対して、情報資源へのアクセスの認可を与え, アクセスの権限を制御する」ことである.

オペレーティング・システムやセキュリティ管理システムによるオペレーティング・システム資源, データへのアクセス制御がある. ネットワークを利用する場合, セキュリティ区分による分離(ゾーニング)やファイアウォール, ルータでのACL(Access Control List)を利用したアクセス制御が可能である.

2.2 地方自治体の利用形態別セキュリティ要件

地方自治体では, セキュリティ, プライバシーに関して重要度が高く, 個人情報保護法の適用を迎え, 重点的に取り込むことが必要である.

表1. 利用形態別セキュリティ要件

セキュリティ要件	利用形態別重要度					脅威との対応
	インターネット情報公開	LGWAN	住民情報系	内部情報系	OA系	
機密性		○	◎	◎	○	情報の盗難,漏えい,ソーシャルエンジニアリング
完全性	◎	◎	◎	◎	◎	悪意を持ったコード,改ざん
可用性	○	○	◎	◎	◎	DOS,ウイルス
否認不能性		◎	◎			アクセス違反,否認
識別認証		◎	◎	○	○	アクセス違反,否認
アクセス制御	○	○	◎	○	○	アクセス違反

業務セキュリティ要件の調査と計画セッションでの分類の結果, **表1**のように利用形態別セキュリティ要件を五つに分類した.

① インターネット情報公開

インターネットにおける行政情報や市広報などの公開情報で, 公開した内容の完全性が重要である.

② LGWAN

政府・自治体間でのメール, 文書交換に利用されるLGWAN(Local Government WAN:総合行政情報ネットワーク)を利用した情報で, 完全性や識別認証や, 侵入防止のためアクセス違反からの防御が重要である.

(LGWANによる公的個人認証サービスのための証明書発行は, 当初要件としてはなく, あとから追加されたものである. メール, 文書交換とは別の分類として, 住民情報系と同じ取り扱いにしている. 今後戸籍ネットワークなどLGWANの基盤を利用すると考えられるサービスも同様な取り扱いになると考えられる.)

③ 住民情報系

自治体内で住民サービスを提供するための住民情報系システムでは, 住基ネット以外にも税などの個人収入や, 福祉情報, 戸籍情報などを取り扱い, プライバシーに強くかかわる自治体としての基幹業務であり, すべてのセキュリティ要件が重要である. 不正アクセス禁止, 目的外利用禁止, 利用権限の制約などの要件があり, アクセス制御と, だれがどの情報をアクセスしたかという管理が求められる. データへのアクセス制御と, その監査に関してはネットワークセキュリティ以上に, サーバー, アプリケーションのセキュリティで検討することが必要であり, セキュリティポリシー策定や, 職員教育によるセキュリティ意識向上も, 重要な課題である.

④ 内部情報系

自治体内部の業務として人事・給与, 財務, 土木積算, 地図情報など, 行政内部のための情報で, 完全性, 機密性, 可用性のために, 外部からの侵入防止や, ウイルス対策, 信頼性の確保が重要である.

⑤ OA系

OA系情報としてメールや文書管理などの業務で, 完全性, 可用性のために, ウイルスに対する対応や侵入による改ざん防止, スパム対策が重要である.

3. セキュリティ強化のためのネットワークソリューション

セキュリティ強化のために検討したネットワークソリューションは, 以下の四つである. これ以外に検討したウイルス対策は実施済みであることと, メインフレーム, サーバー, アプリケーションのセキュリティなどは, 重要な項目ではあるが, 本論文の範囲ではないので省略する.

① 無線LANのセキュリティ
② 認証LANとレイア2・アタック対応
③ ダークファイバ利用とCWDM
④ ファイアウォールと侵入検知システム

3.1 無線LANとセキュリティ

無線LAN利用は, 配線工事が不要なため部門移動の多い自治体においては, 利便性が高く広く用いられている. しかし, 無線LANの鍵交換および暗号方式であるWEP(Wired Equivalent Privacy)の脆弱性や, 公共の場所での電波の到達という点は不正アクセスの絶好の対象となっている. 後継として出てきた規格であるWPA(Wi-Fi Protected Access)は, 標準化が進められている無線LAN規格IEEE802.11iのサブセットに位置付けられる. WPAでは, 鍵の漏えい防止のために鍵の一定期間における変更の仕組みであるTKIP(Temporal Key Integrity)とユーザーの個別認証のための方式としてIEEE802.1Xを採用している. 無線LANは, イーサネット・ハブと同様に共有メディアであり, 暗号強度という論点以前に, 電波が到達する場所からデータ収集が可能であるという問題を持っている. 無線LANの利用では外部からのアクセスと同様に, アクセス用のセグメントを作り限定した利用法を取る必要があり, イントラネット全体に採用することは不可能である. 計画当時は, WPA対応の製品も出ておらず, 追加の暗号としてIPsec(IP層を暗号化して送る業界標準の通信プロトコル)やSSL(Secure Sockets Layer: WebサーバーとWebブラウザ間のHTTP通信を暗号化して送受信する業界標準の通信プロトコル)を利用する選択があったが[3][4], IPsecはIPだけに対応し(SNAを利用した基幹業務がある), SSLはさらに利用できるアプリケーションが限られているためすべての業務, サーバーにわたって適用することはできない.

一般者の出入りが多いことと, 公共機関における無線LANの見直しの指針が出たことに合わせて, 当プロジェクトでは無線LANの廃止を打ち出している.

3.2 認証LANとレイヤー2・アタック対応

IP層, アプリケーション層でのセキュリティ対策は一般化してきているが, 無防備であるレイヤー2(layer 2)への攻撃が, ネットワーク攻撃として取り上げられはじめた. 具体例がN+I Network[5], CISCO SAFE[6]で述べられている.

LANスイッチCPU負荷上昇・機能停止をねらい, 大量のMACアドレス情報を送りLANスイッチ上のテーブルあふれを発生させる攻撃や, あて先MACアドレス解決のためのプロトコルの偽装や, 偽装MACアドレ

スによる成りすまし, 偽装ブリッジ情報排出によるブリッジのスパニング・ツリー・トポロジーの破壊, DHCP要求(Dynamic Host Configuration Protocol：IPアドレスなどを自動的に割り振る仕組み)の大量発生によるDHCPサービス停止など, 盗聴のみならずネットワーク全体を停止させる攻撃がある. これ以外にも, エンドユーザーが島ハブ用にLANスイッチを接続したものがスパニング・ツリーのルートブリッジになってしまい, 設計時のトポロジーを維持できなくなりパフォーマンス劣化や障害になるケースもある. ウイルスに汚染された個人のPCを接続しウイルスを広めてしまうこともある.

これらの対策として, LANスイッチの不正ブリッジ情報防止機能など以外に, IEEE802.1Xを利用した認証LANを検討した. IEEE802.1Xは無線LANのために標準化された機能であるが, 無線のアクセス・ポイント以外にも有線のLANスイッチなどでも利用できるポートセキュリティの機能である.

PCの認証クライアントから要求があると, イーサネット・スイッチはEAP(Extensible Authentication Protocol)により代理で個人別にRADIUS(Remote Authentication Dial In User Service)サーバーと認証し, 認証されたユーザーのみが該当イーサネットポートを開き, ネットワークに入れるため, レイヤー2でのセキュリティを確保できる. 認証方式は, EAP-MD5(Message Digest 5), EAP-TLS(Transport Layer Security), EAP-MS-PEAP(Protected EAP)などがある.

EAP-MD5は, ユーザーIDが暗号化されずに流れること, 認証用データベースが平文であることと, RADIUSサーバーと認証用データベースが別マシンの場合には, パスワードも平文でネットワークを流れることから, あまり強いセキュリティではない.

EAP-TLSは電子証明書を利用してクライアントとサーバーの間で相互認証する. 認証局の構築とクライアントに電子証明書が必要となるため, 金額面および運用での工数がかかる.

EAP-PEAPは認証サーバーが電子証明書を持ち, クライアントはパスワードのみで認証する. サーバー側はTLSで、クライアント側はMSCHAPv2 またはEAP-TLSで認証する. 認証局を必要とするが, クライアントに電子証明書をインストールする必要はない.

これ以外にもベンダー独自の方式としてLEAP(無線LAN専用)やTTLSなどがある. IEEE802.1Xを利用しない独自の認証LANの仕組みを持っているベンダーもある. 認証LANはベンダー独自の機能が多いが, Windows® XP, 2000で認証クライアントを標準装備しており, ネットワークベンダーもIEEE802.1X対応の製品をそろえてきている. 認証サーバーについても, アプライアンス・タイプの製品出荷や, Windows2003サーバーでの標準機能搭載などから, 今後の社内セキュリティ対策の要となる.

認証による動的VLAN(Virtual LAN：仮想LAN)と組み合わせることにより, 組織や権限に応じて決めたユーザーグループをVLANに対応付けることが可能となる.

そのため、セキュリティポリシーに応じたネットワーク配置ができACLなどにより内部強化と管理に貢献する. 今回のプロジェクトでは, PC更改時期との兼ね合いのため当初からの利用を変更し合併後の利用を予定している.

3.3 ダークファイバ利用とCWDM

WDM(wavelength division multiplexing：光ファイバを利用した波長分割多重)として, CWDM(Coarse Wavelength Division Multiplexing)とDWDM(Dense Wavelength Division Multiplexing)がある. どちらも異なる光波長を利用し伝送転送密度を上げる方式である. CWDMは, 多重密度は粗く廉価に構築できる. DWDMは, 高密度の多重度を実現でき光ファイバ上の情報転送量を飛躍的に増大できる.

CWDMの別波長を利用することにより, 住基ネットや, 戸籍システムを別ネットワークとして各支所まで展開することが容易となる. 光伝送の層での分割ができることにより, レイヤー2・アタックの心配も無くネットワークを物理的に分割できる.

庁内LANのために検討したネットワークの物理分割および論理分割を反映した設計と認証LANの仕組みを, そのまま支所までLANの延長として展開できるため, CWDMの採用を決めた.

3.4 ファイアウォールと侵入検知システム

インターネットとの接続以外にもLGWANやマルチペイメント, 公的個人認証など外部との接続が増える. 行政サービスも外局(市の外部施設)利用が増える. 今まで, 閉じられたネットワークであったものがオープンになるため, セキュリティ区分に応じたアクセス制御を行うことが必要となる. そのため, インターネット, DMZ(DeMilitarized Zone：非武装地帯)以外にもルータでのACLやファイアウォールを配置して, セキュリティ確保が必要になる.

ファイアウォールを越えてくる侵入準備は, 以下の手順を踏むことが通常である. [7] [8]

ターゲット決定のため, 公開情報を入手する. ホームページや検索エンジン, メールなどから入手する. ping, traceroute, nslookupなど各種コマンドおよびJPNIC(Japan Network Information Center)や各地域のIPアドレス情報管理のためのホームページなどを利用しネットワークの概要を調べる.

侵入準備の段階では, ツールを使用して侵入経路を調査する. pingスイープやポートスキャンによりネットワークの詳細情報や, 利用しているオペレーティング・システム, ルータ, ファイアウォールを特定する. 利用しているサービスをチェックし, 脆弱性のある項目を列挙しそのテストを行う.

これらの調査, 準備の後に侵入者は, セキュリティホールに基づく侵入方法を決定し, 侵入することになる. これらの準備を検知し, 対策するためにネットワークタイプの侵入検知システムを利用する. アクセス制御だけでは守ることのできないファイアウォールを通過する不正アクセス, 情報収集のためのポートスキャン, サーバー・オペレーティング・システムやミドルウエアの脆弱性をねらった攻撃や, ウイルス感染した機械からのワームなど関しては, 侵入検知システムにより検知できる.

4. ネットワークアーキテクチャ

4章では, セキュリティ要件(2章)とネットワーク要件とセキュリティ強化のためのネットワークソリシューション(3章)を考慮し設計に反映した内容を概要設計中心に述べる.

4.1 概要設計

要件に基づき, どのようにネットワーク設計に組み込むかを示すために概念を表すセキュリティ区分(**図1**), イントライメージ(**図2**)と、ネットワークの詳細設計に展開するために概念論理図(**図3**), ロケーション図で表現した.

セキュリティ区分の検討として, 2.2節で述べた利用形態分類だけでなく, 個別業務での分類を行った. ネットワークセキュリティのためのゾーニングに対応しやすくするため, 業務別サーバーに合わせてグループ化した.

各業務の取り扱う情報をもとにセキュリティ区分を検討すると, 図1のように, 戸籍が一番高く, 個人情報を取り扱う住民情報系の中核となる. 住基ネットは, 取り扱う情報は4情報だけであり, 税や住民基本台帳より扱う情報は少ないが, 外部と接続するため, 独立したセキュリティ区分になる. 次に人事・給与, 財務, 都市計画など業務システムである内部情報系がくる.

文書管理, メールなどのOA系システムと外部公開のためのインターネット接続となる.

クライアントからサーバーへのアクセスを制御するために, セキュリティ要件の分類に合わせて組織による利用業務と場所による利用業務を検討した. 図2のように, 部門ごとのVLANで論理分割し, 業務グループごとのサーバーセグメントへのアクセス制御をレイヤー3・スイッチでのACLで行い, ネットワークのパフォーマンスを犠牲にすることなくセキュリティを確保できるようにした. 3.2節で検討したようにPC更改の時期に合わせIEEE802.1Xの認証を利用することにより, 認められたVLANのみへの参加を制御できるようにする.

戸籍および住基ネットは, その他のネットワークと分離することが必要である. 構成する2町が自営の

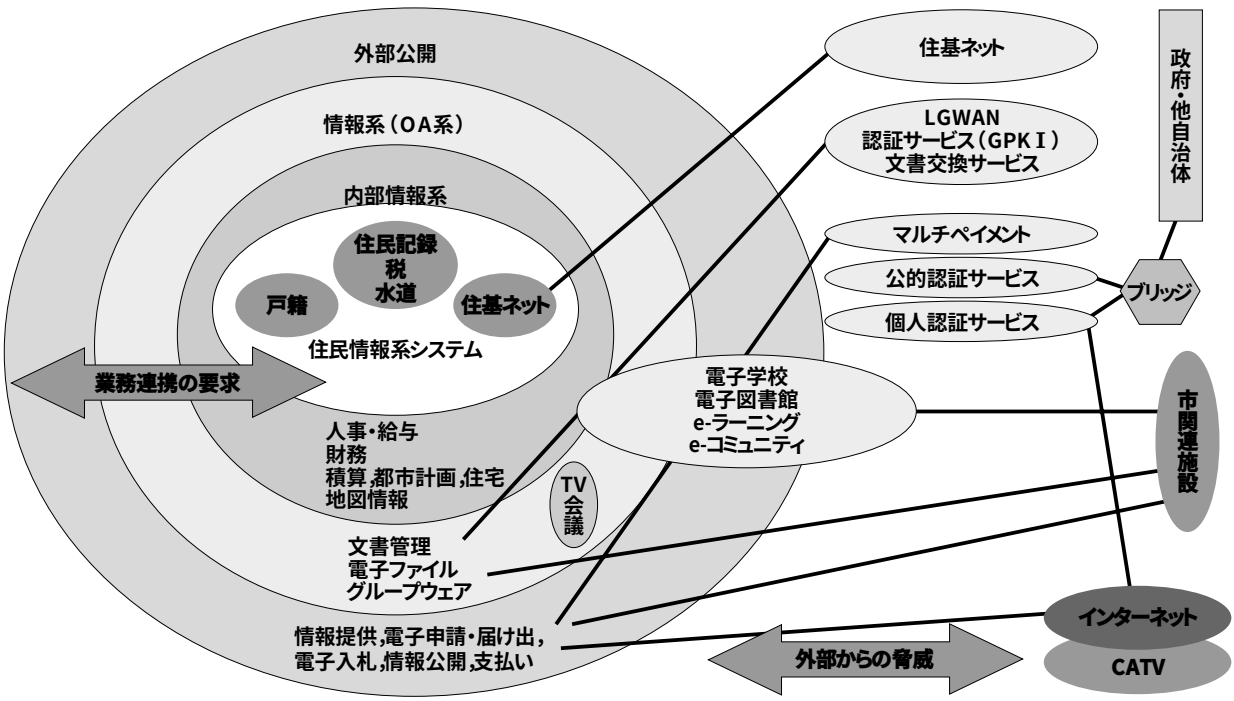

図1. セキュリティ区分

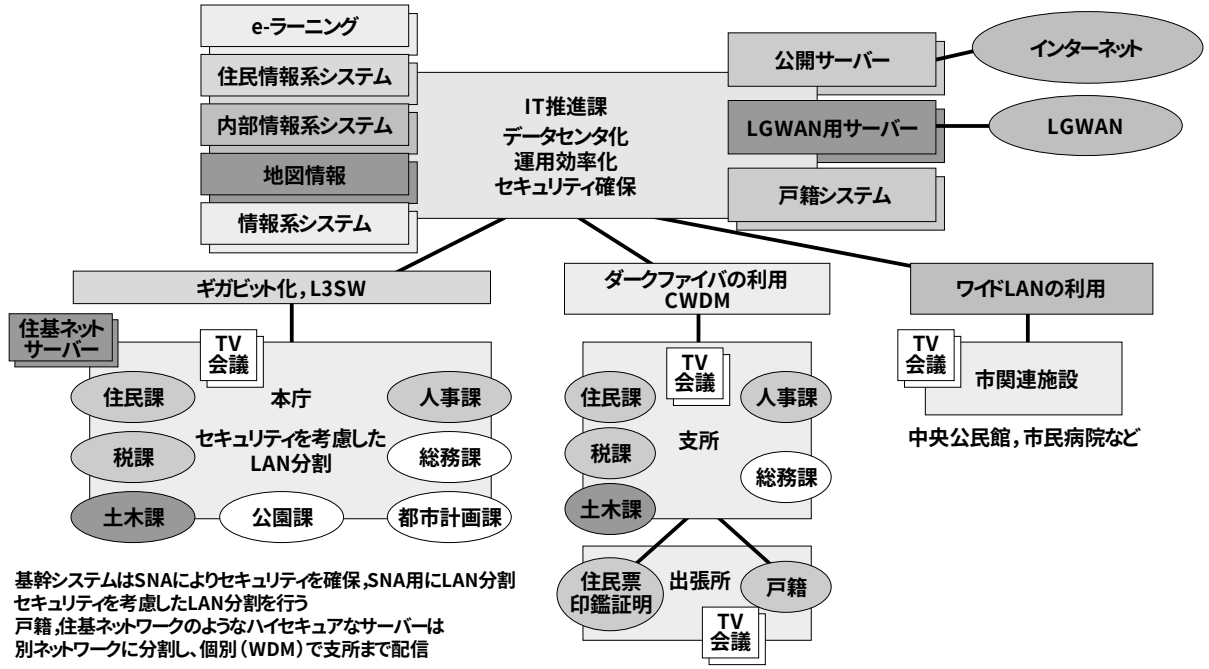

図2. イントライメージ

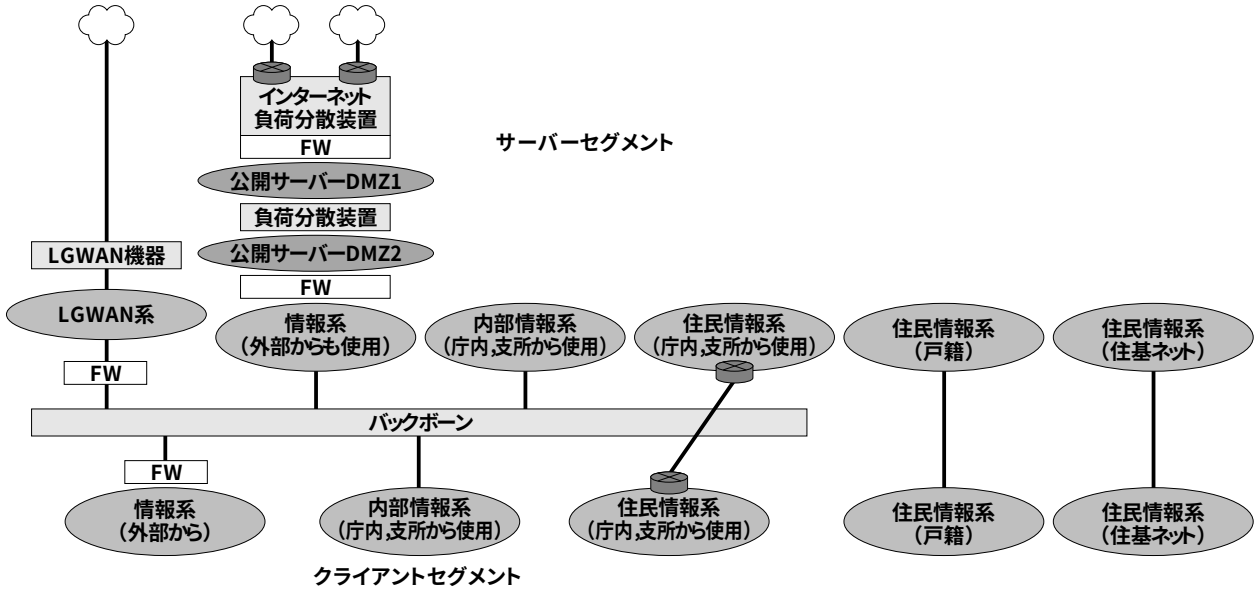

図3. 概要論理図

CATV施設を持ち, すでに物理的ネットワーク分割を行っているため, 広域に関しても物理分割することにした.

分割の方法としてCWDMの波長による分割にした. 3.3節で検討したようにCWDMを使うことにより, レイヤー2での分離より区分けを強固にできる. LANスイッチも, 機器のレベルで分割することとした（図3）.

3.4節で検討したように, LGWANやインターネットとの境界部分にはファイアウォール, 侵入検知システムを配置した. また市の外局となる外部施設は, 庁内よりも公共の場として, 複数の一般の人々の出入りが多いため, 準パブリックスペースからのアクセスという位置づけになる. アクセスが庁内LANに比べ少ないことと, アクセス記録を保存する目的からルータACLによるアクセス制御ではなく, 図3のようにファイアウォールを配置し, 特定のサーバーへのアクセスに限定し, ログを残すことにした. 3.1節で検討したように脆弱性のある無線LANは廃止し, 当初はLANスイッチのポートセキュリティで利用できるPCを限定した. PC更改時に, 本庁と同様にIEEE802.1X認証によるアクセス制御を検討している.

3.4節で検討した内部、外部からのサーバーセグメ

ントへの不正侵入検知のために, 侵入検知システムをDMZのみでなく内部ネットワークにも配置した.

4.2 機能仕様設計

以下の内容を, 3章で述べたセキュリティ関連技術のほかに検討した.

CWDMの波長と距離の要件を整理し、WANトポロジーも冗長経路で策定した. CWDMは, スター形状とリング形状のトポロジーを取ることが可能であるが, 機器の機能上からスパニング・ツリーによる制約を受けるため, 障害時の収束時間問題のためにスター形状を採用した. 冗長構成をとるために2系統のダークファイバを借り受け3角形のトポロジーを採用し信頼性を確保した. LANに置いて実績のあるスパニング・ツリーを利用し3角形のトポロジーを採用しているため, WANの展開においてもLANの延長として考えることができる. これにより, セキュリティ区分によるネットワーク分割を支所に延長することが可能となっている.

5. おわりに

本論文では, セキュリティ対策をネットワークソリューションとして計画段階から検討し, 実際の設計として組み込む方法を実例を通じて示した. ネットワークとセキュリティは, サーバーとともにシステム基盤設計の基幹となるものであり, システムの安定性, 拡張性, 信頼性, 完全性に強く影響を与える. ネットワーク方針として, ワンポイントのセキュリティ対策ではなく全体として対策を組み込むことが重要である.

ネットワークソリューションとして取り上げた項目は, 近年になり強く脆弱(ぜい)性が指摘されている部分への対策であり, セキュリティ対策として広い分野で有効である. 広域にまたがったネットワークにおいてはCWDMを用いたアーキテクチャが有効である.

ネットワークセキュリティへの要求は, ワームやインターネットからの脅威の増大から日増しに強くなってきており, 今後の課題としてオペレーティング・システムへの自動的なパッチ適用, ウイルス対策およびネットワーク認証の仕組みを併用して, 安全なPCしかネットワークに接続しないことを強制する仕組みが求められている. ネットワーク技術, セキュリティ技術の進歩は早く, 組み合わせにより解決方法は各種におよぶが, 計画段階から進めるにあたって本論文が進め方の一助となれば幸いである.

参考文献

[1]「e-Japan重点計画」, 高度情報通信ネットワーク社会推進戦略本部, 2001年

[2] JIS X 5080:2000(ISO/IEC17799:2000)「情報技術―情報セキュリティマネジメントの実践のための規範」(財)日本規格協会, 2002年2月

[3] Tom fault, Warren Barkley,「ワイヤレス LAN テクノロジとWindows XPホワイトペーパー」, Microsoft, 2001年11月

[4] Sean Convery, Darrin Miller, Sri Sundaralingam : SAFE: Wireless LAN Security in Depth version2, 2003年, Cisco

[5]「社内セキュリティをスイッチで守れ」, N+I Network, 2002年10月号pp.60-80

[6] Sean Convery ,Bernie Trudel: SAFE: A Security Blueprint for Enterprise Networks,2003年,Cisco

[7] Joel Scambray他,「クラッキング防衛大全」, 翔泳社, ISBN4-7981-0026-9,2001

[8] Stephen Northcutt, Judy Novak:「ネットワーク不正侵入検知」, 翔泳社, ISBN4-7981-0142-7, 2001

日本アイ・ビー・エム株式会社
ITアーキテクト
佐藤 修二 Shuhji Satoh

[プロフィール]
1983年日本アイ・ビー・エム入社. システムエンジニアとして, 製造業・流通業・金融業・公共機関のお客様を担当し, お客様のシステム構築・安定運用に従事してきた. 現在公共機関担当のITアーキテクトとして, システム構築, 合併プロジェクトおよびアウトソーシングに従事. 情報処理学会正会員.