INTEC IT Holdings Group Go Beyond

総務省 Ministry of Internal Affairs and Communications

総務省平成25年度請負事業
インターネット利用環境の変化に伴う情報セキュリティ対応推進事業

IPv6導入の早わかり

-こうやればできるIPv6導入-

平成26年11月17日

株式会社インテック
先端技術研究所　廣海緑里

目次

本題に入る前に

- 電話番号10桁化
  - 電話帳、短縮ダイヤルの更新（ソフトウェア対応）
- 11桁電話番号の登場
  - 携帯電話。設備、端末が固定とは違う新しい技術。（ハードウェア、ソフトウェアどちらも対応）
- IPv4ネットワークにIPv6
  - 新しい機器はソフトウェア設定のみ
  - 古い機器はハードウェアとソフトウェアどちらも確認が必要

Ⅰ．企業や地方自治体のネットワークの現状

Ⅱ．IPv6対応ガイドラインと調達仕様書モデルの背景

Ⅲ．IPv6対応ガイドライン

Ⅳ．IPv6調達仕様書モデル

Ⅴ．ケーススタディ

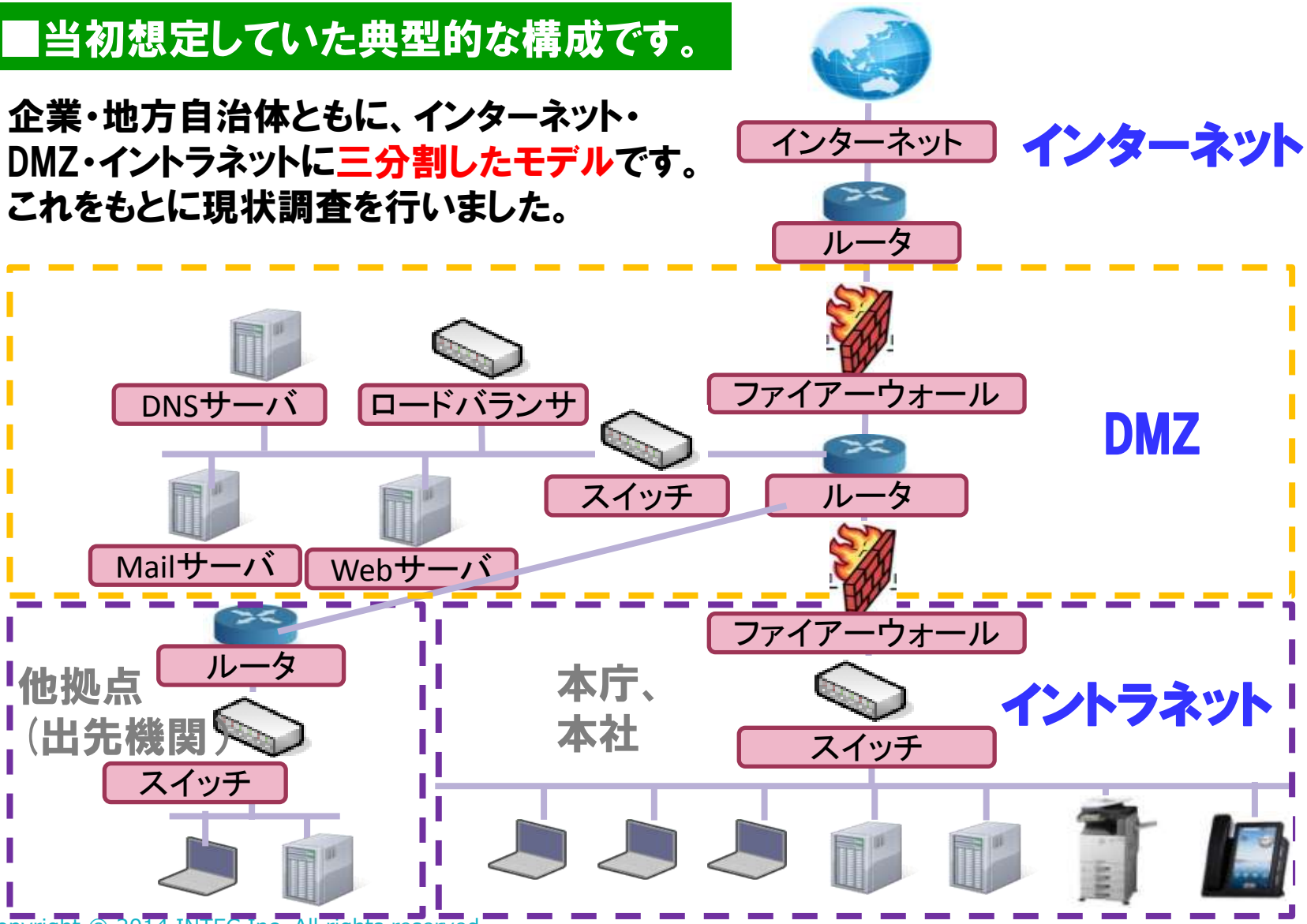
おわりに

（付録） IPv6の基礎知識

1．想定モデル

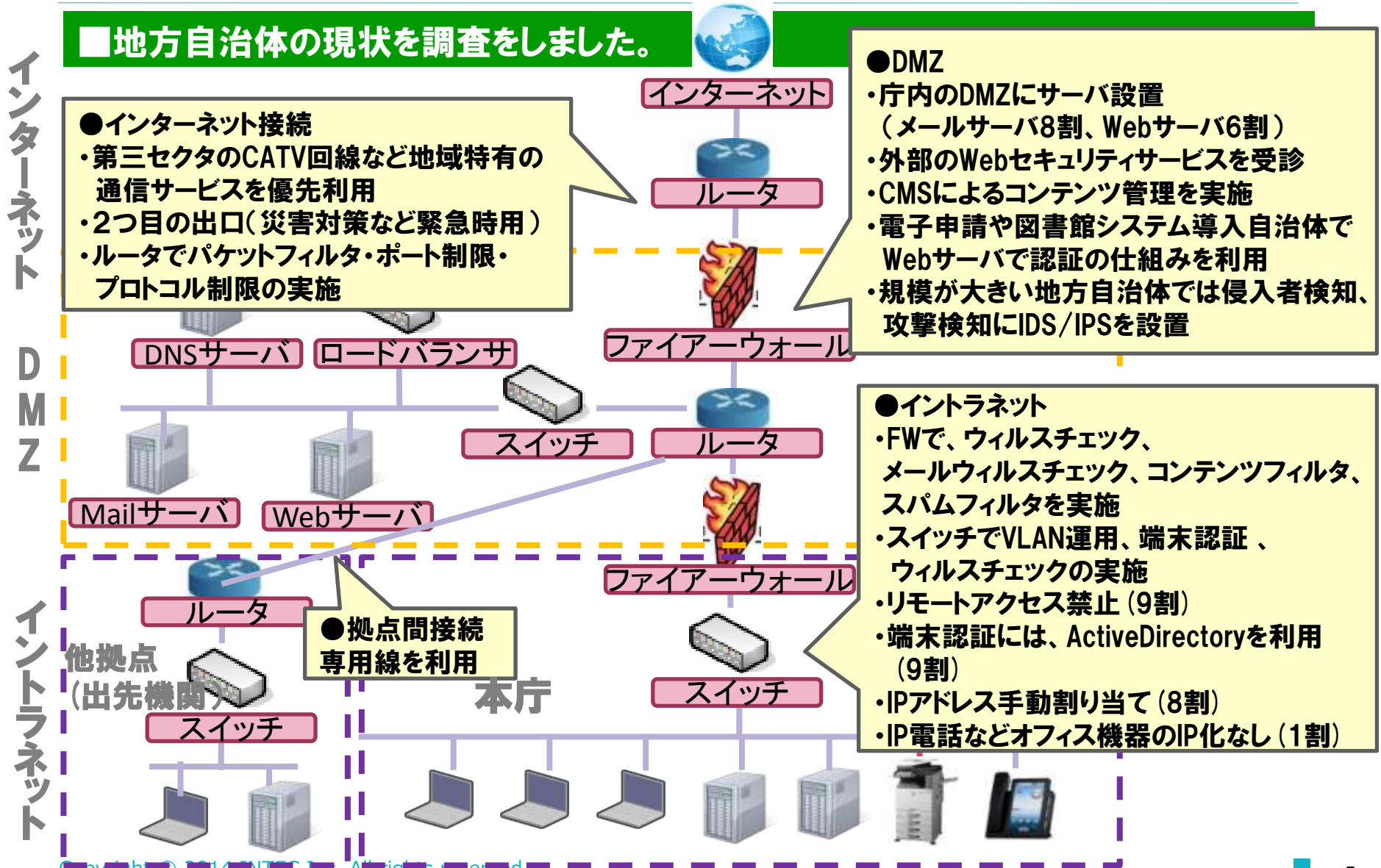
■当初想定していた典型的な構成です。

企業・地方自治体ともに、インターネット・
DMZ・イントラネットに三分割したモデルです。
これをもとに現状調査を行いました。



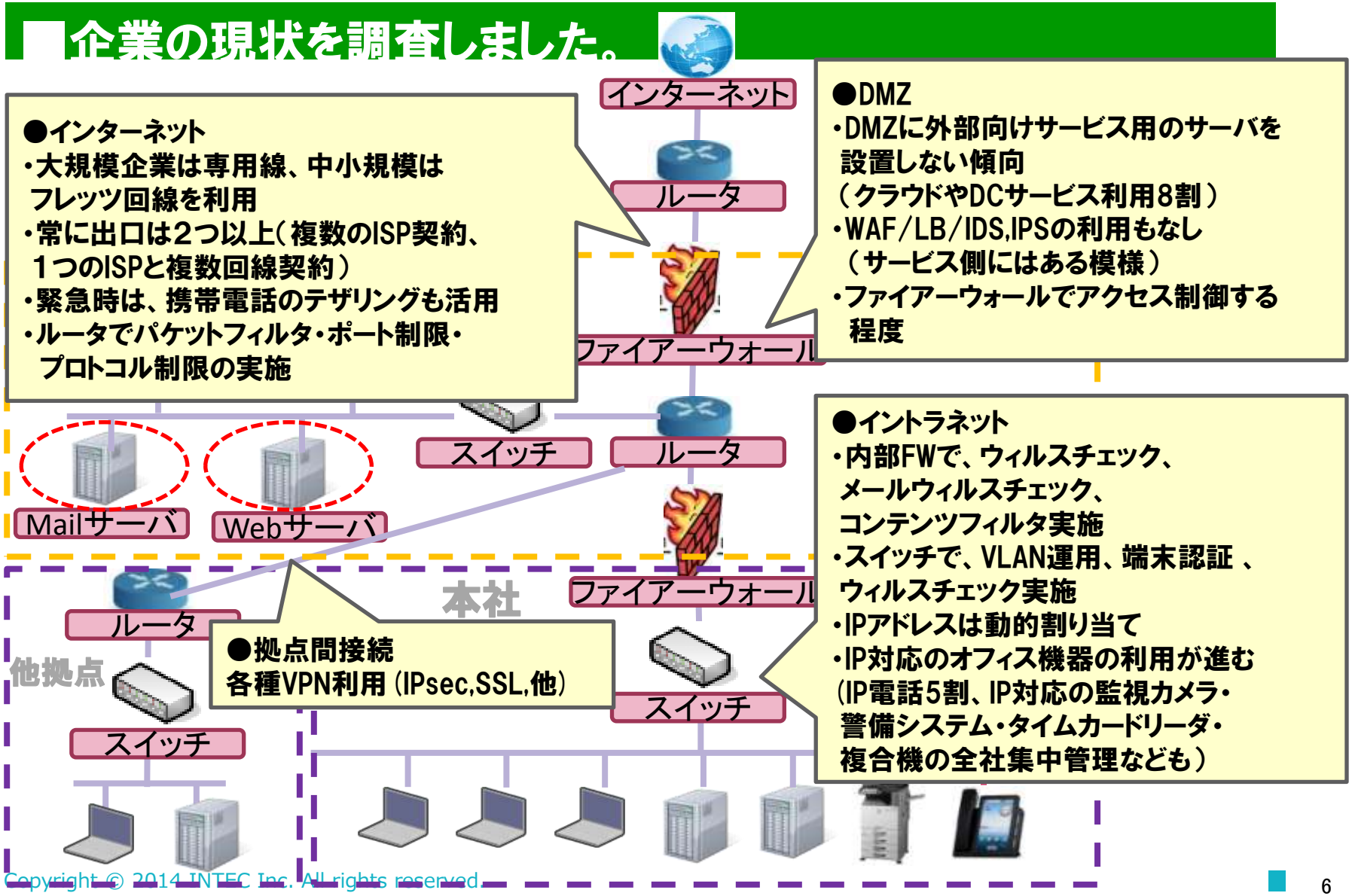
2. 地方自治体の調査結果

■地方自治体の現状を調査をしました。



3. 企業の調査結果

企業の現状を調査しました。



●インターネット
・大規模企業は専用線、中小規模は
フレッツ回線を利用
・常に出口は2つ以上(複数のISP契約、
1つのISPと複数回線契約)
・緊急時は、携帯電話のテザリングも活用
・ルータでパケットフィルタ・ポート制限・
プロトコル制限の実施

●DMZ
・DMZに外部向けサービス用のサーバを
設置しない傾向
(クラウドやDCサービス利用8割)
・WAF/LB/IDS,IPSの利用もなし
(サービス側にはある模様)
・ファイアーウォールでアクセス制御する
程度

●イントラネット
・内部FWで、ウィルスチェック、
メールウィルスチェック、
コンテンツフィルタ実施
・スイッチで、VLAN運用、端末認証 、
ウィルスチェック実施
・IPアドレスは動的割り当て
・IP対応のオフィス機器の利用が進む
(IP電話5割、IP対応の監視カメラ・
警備システム・タイムカードリーダ・
複合機の全社集中管理なども)

●拠点間接続
各種VPN利用 (IPsec,SSL,他)

4. 管理、マネジメント等

■構成以外にわかったこともいくつかあります。

① Webサイト構築は、広報部門が手掛けていてICT部門が不介在である。
Webサイトのセキュリティ対策、ITネットワーク技術は広報部門のポリシーの場合がある。

② ３－５年でシステム更改している。

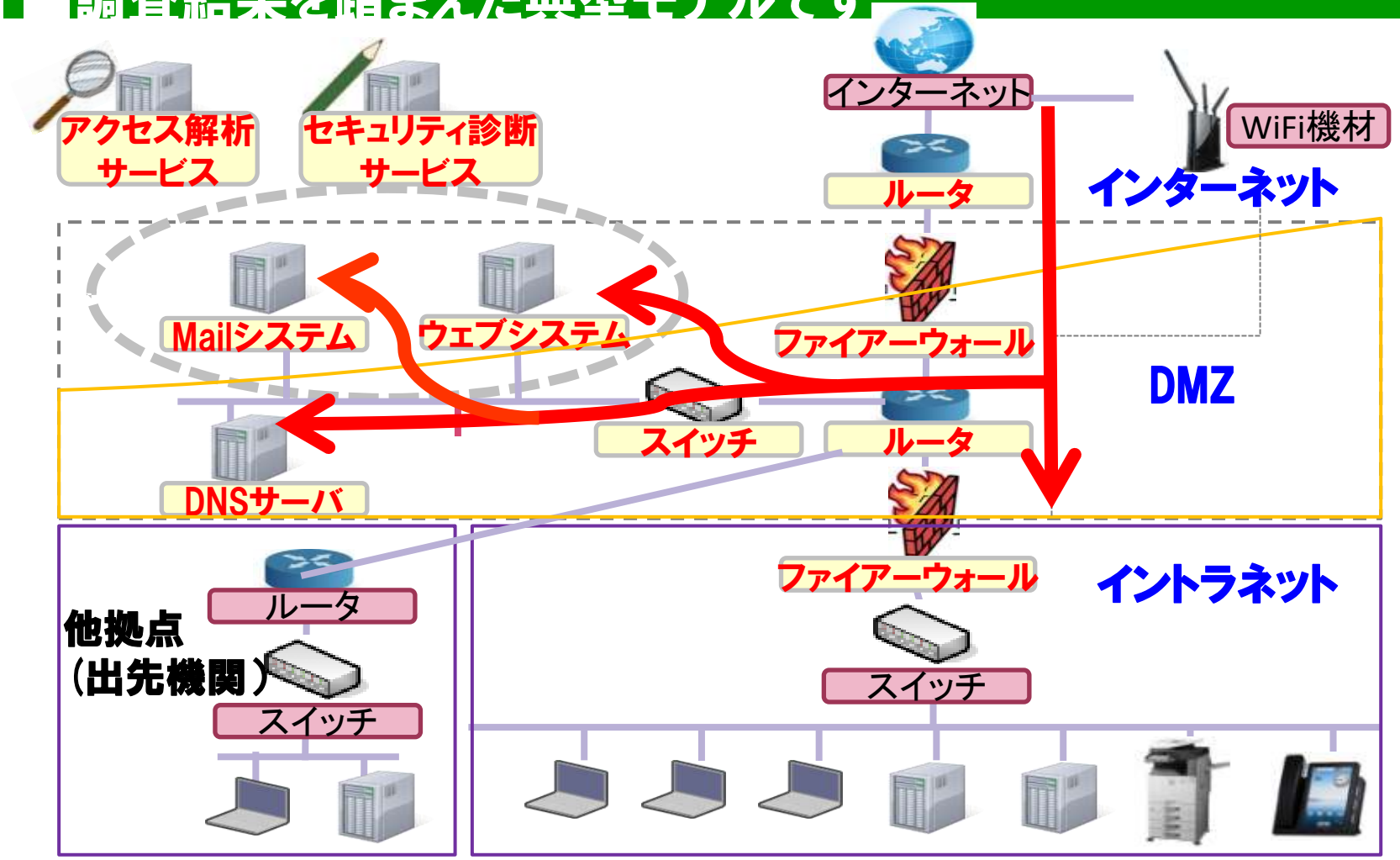
③ 地方自治体、企業ともにデータセンター（場所利用）から
データセンターサービスや クラウドサービス（サービス利用）への移行に
意欲が大である。

④ 情報セキュリティは、外部の診断サービスの組み合わせ利用が増加中である。
（監査の影響）

⑤ IPv6対応は情報収集段階。IPv6対応機材に気づかず運用しているケースもある。

5. 企業や地方自治体の典型モデル

調査結果を踏まえた典型モデルです



インターネット側からアクセスされる部分（赤字→）をIPv6対応します。

Ⅰ．企業や地方自治体のネットワークの現状

Ⅱ．IPv6対応ガイドラインと調達仕様書モデルの背景

Ⅲ．IPv6対応ガイドライン

Ⅳ．IPv6調達仕様書モデル

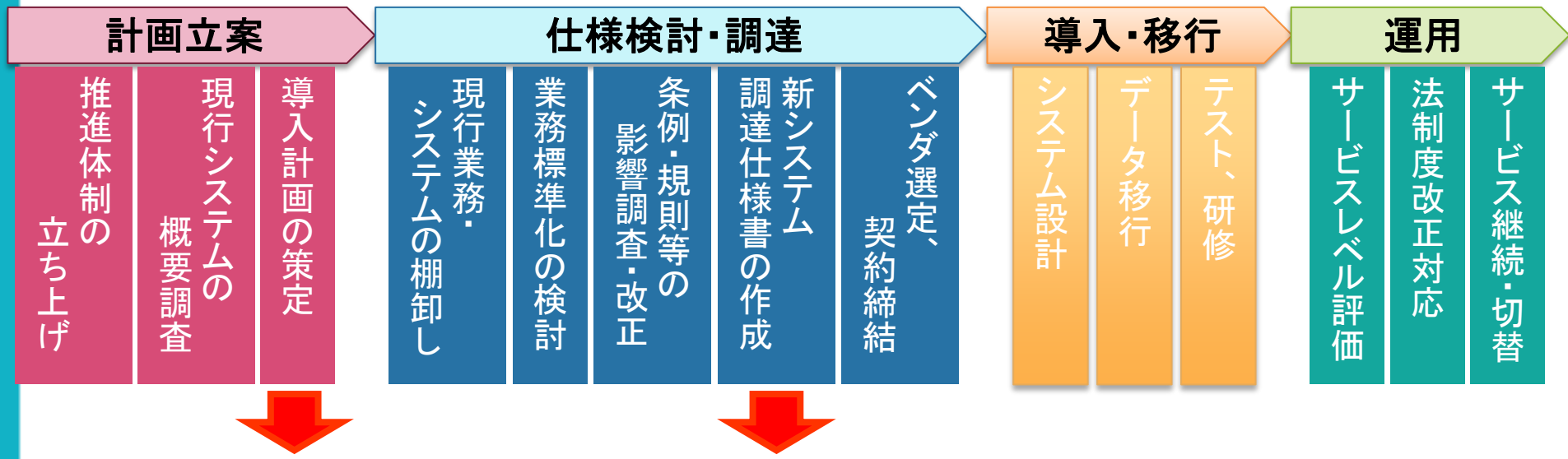
Ⅴ．ケーススタディ

おわりに

（付録）　IPv6の基礎知識

1．IPv6対応ガイドラインと調達仕様書モデル

■IPv6対応ガイドラインと調達仕様書モデルの利用想定です。



①IPv6対応ガイドライン　②IPv6対応調達仕様書モデル

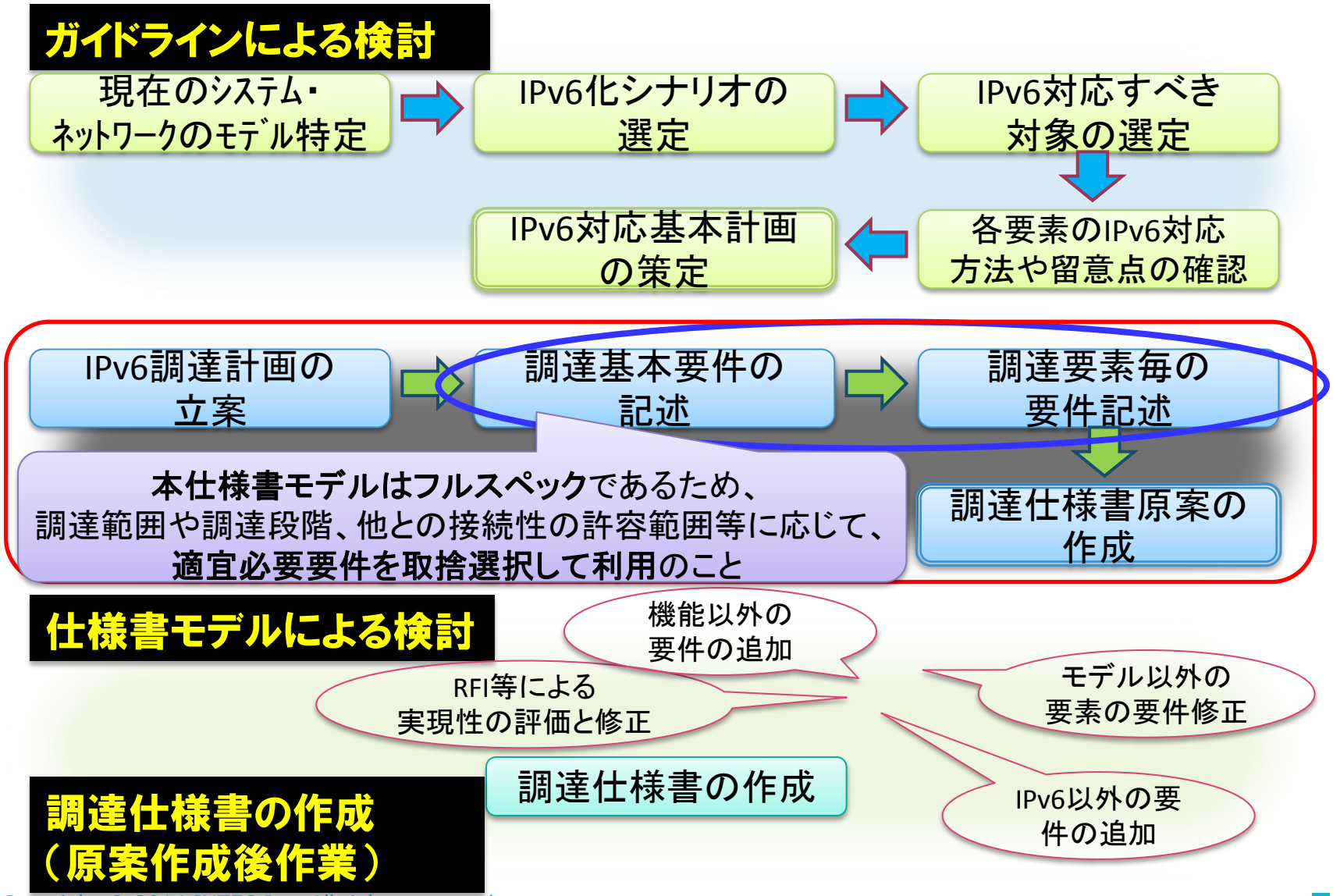
①　IPv6対応ガイドライン

- IPv6対応の方法や対応を検討していく上での留意点をまとめてあります。
- これをもとに、一定レベルの基本計画の策定をすることを目指しています。
- 基本方針をつくることで、組織の意思決定に役立ちます。

②　IPv6対応調達仕様書モデル

- 調達時の手引きとなります。
- 基本計画をもとに、調達上の要件を整理したものです。
- 各企業・地方自治体の実態に合わせたカスタマイズをしてご活用ください。

2. IPv6対応ガイドラインと調達仕様書モデルによる検討



Ⅰ．企業や地方自治体のネットワークの現状

Ⅱ．IPv6対応ガイドラインと調達仕様書モデルの背景

Ⅲ．IPv6対応ガイドライン

Ⅳ．IPv6調達仕様書モデル

Ⅴ．ケーススタディ

おわりに

（付録） IPv6の基礎知識

1．目的

■ガイドラインは以下の3点を目的としています。

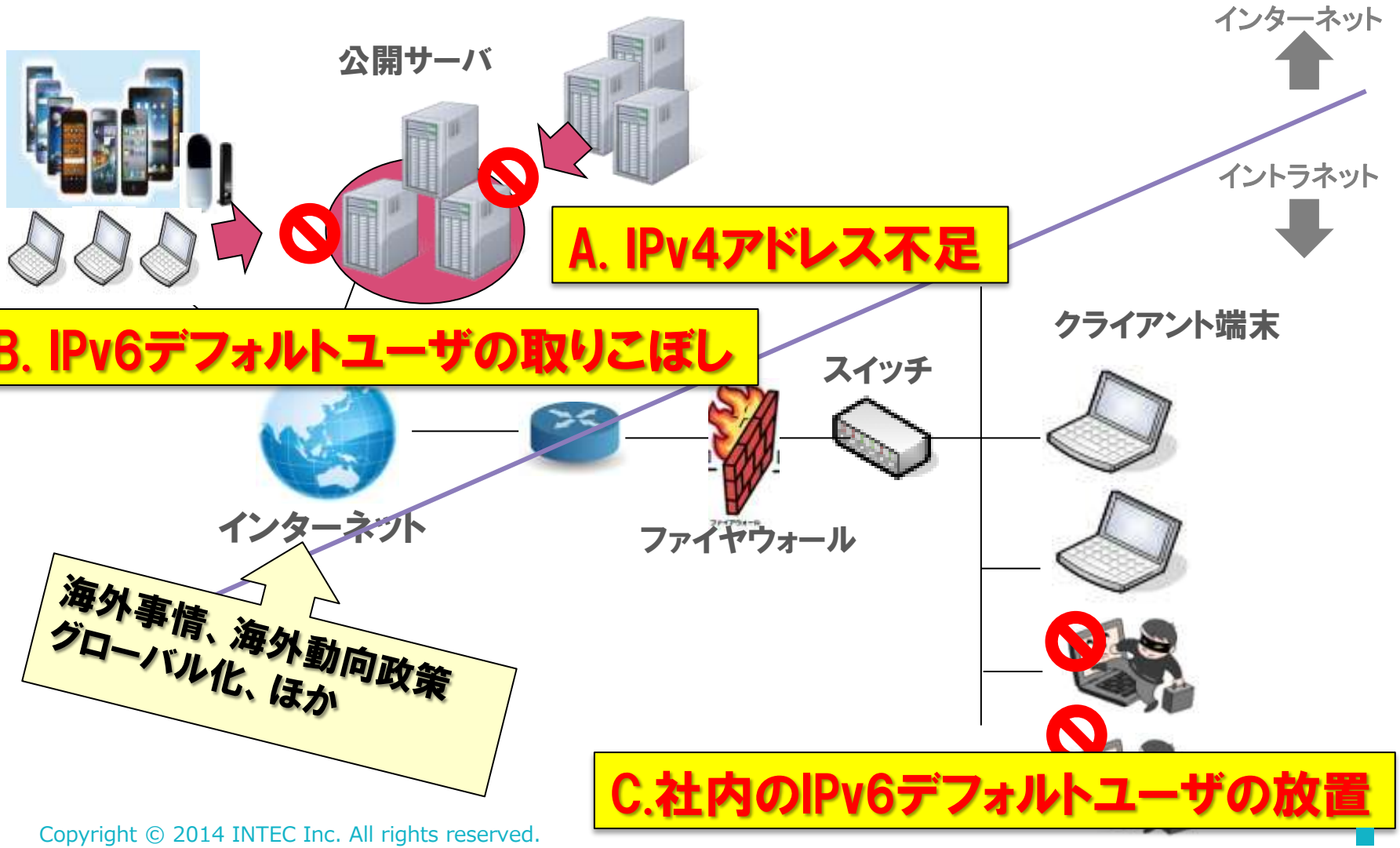
① 企業や地方自治体のWebサイトなど外部向けサービスのIPv6対応促進

② IPv6対応を考える際の全体像、IPv6対応にあたっての基本的な考え方や方針、具体的に検討すべき箇所、検討の方法等について解説

③ 調達仕様書サンプルと合わせた利活用の促進

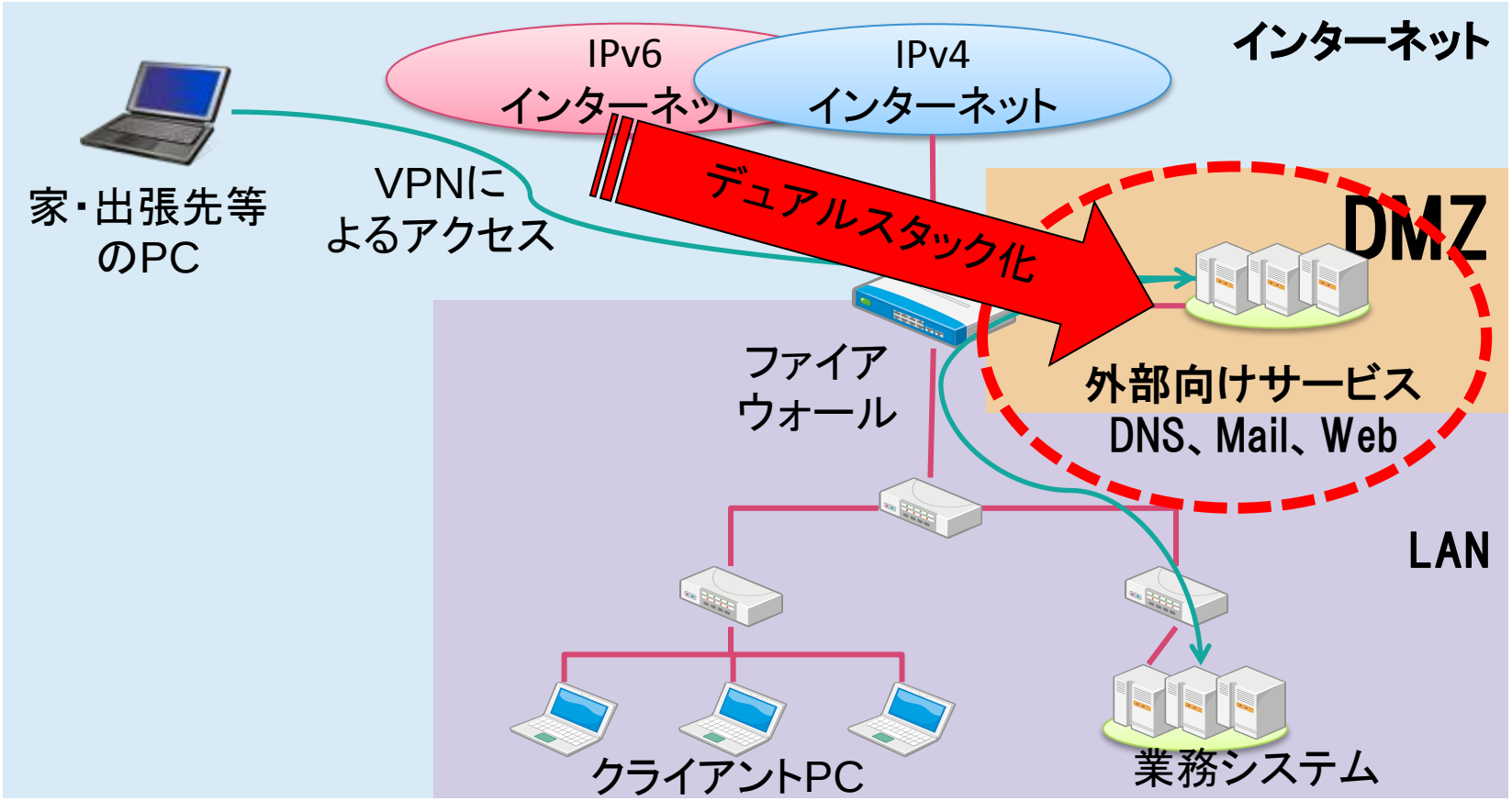
2. IPv6対応の背景

■ガイドラインの提供は、次の問題状況を背景としています。



3. システムモデル

■ガイドラインでは、以下のようなシステム・ネットワークモデルを想定しています。



4. 基本計画

■想定するモデルに従って「IPv6対応に向けた基本計画（基本方針）づくり」を行います。

①DMZ/LANともにフルデュアルスタック化	–	全体最適化が図れる
②DMZのみデュアルスタック化	–	必要最低限の対応が可能
③DMZをトランスレータ等でIPv6対応	–	既存設備に手を入れずに部分的対応が可能
④ネットワークで提供されるサービス利用のみIPv6対応	–	設備や手間をかけずに対応が可能

5. IPv6アドレス設計方法（1）

■基本計画ができあがったら、IPアドレス設計について考えます。
アドレス設計では、以下の2点をポイントとして解説しています。

①IPv6アドレスをどこからもらうか

A)　アドレス管理組織（JPNICなど）から組織専用のグローバルアドレス

- ルーティング情報の広告や外部接続性などを構築、運用
- ISP依存しないで運用可能

B)　ISPからISPのグローバルアドレス（の一部）

- ルーティング情報の広告や外部接続性をISPに任せられる

※　IPv6インターネットへの接続予定がない場合、ユニークローカルグローバルユニキャストアドレス（ULA）が利用可能

- IPv4プライベートアドレス相当、無料、特殊な計算方法
- IPv6グローバル接続時にどうするか検討必要

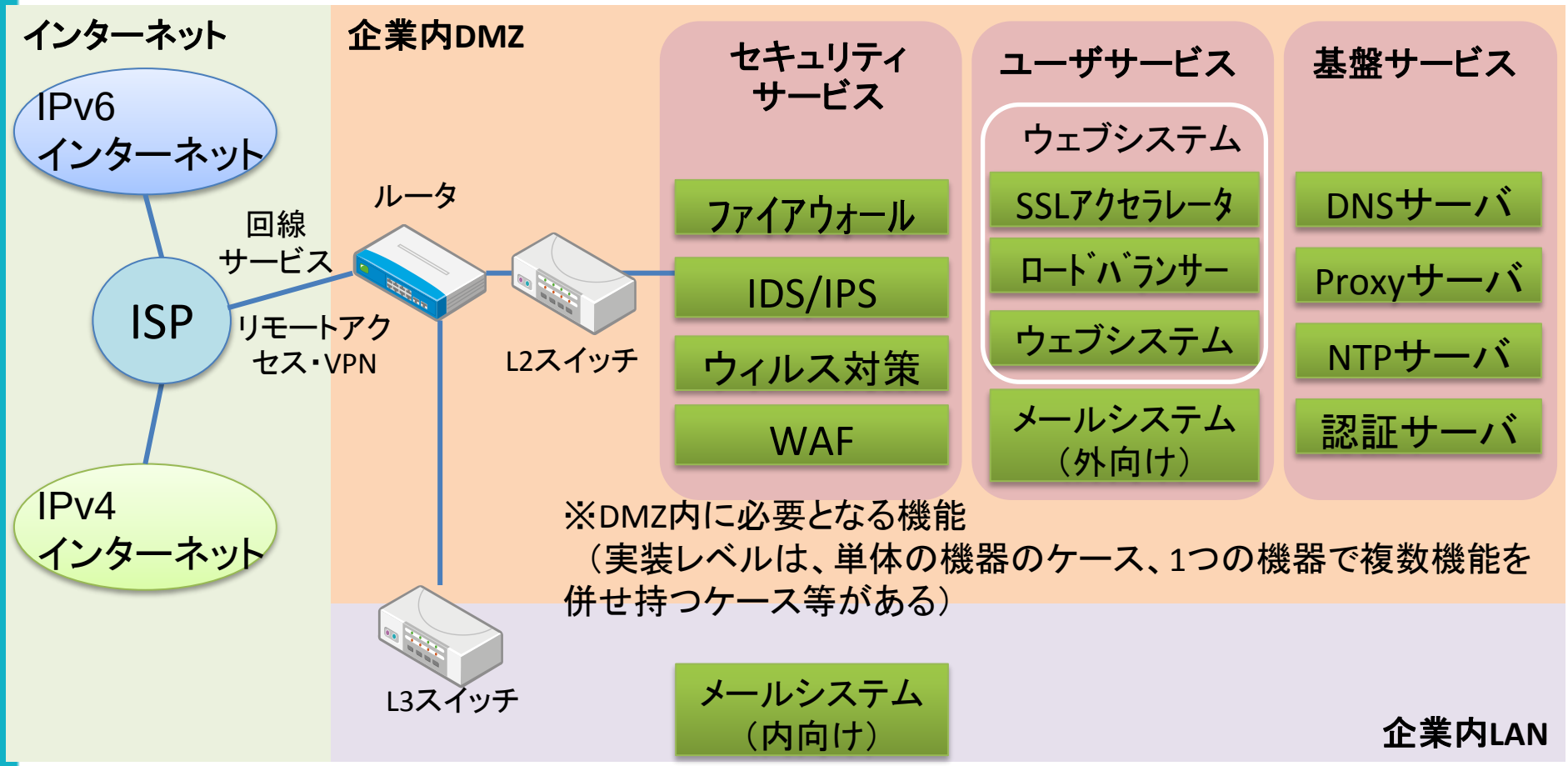
5. IPv6アドレス設計方法 (2)

②IPv6アドレスの割り当て管理方法をどうするか

- IPv4と違うアドレス体系のため、**サブネット数の算出や階層管理の考え方**の整理が必要
- 管理ツールの利用の(再)検討
- ルータ、スイッチ、ファイアウォールには固定アドレス
- サーバにも固定アドレス
- クライアントには動的アドレス(自動設定プロトコル利用)

6. 外部システムのIPv6対応（1）

■ガイドラインの「6. 外部向けサービスのIPv6対応方法」に従って、DMZ上の外部サービスのコンポーネントを抽出し、対応方法を検討していきます。



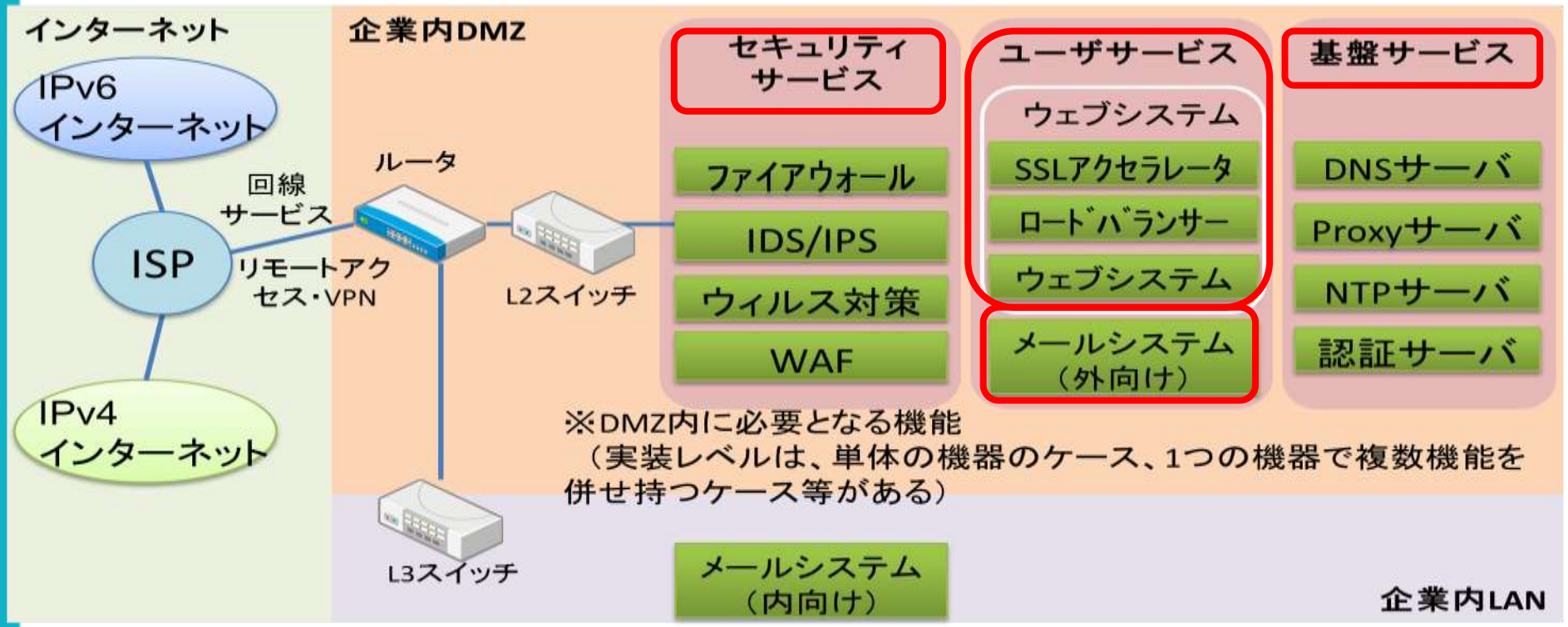
6. 外部システムのIPv6対応 (2)

INTEC IT Holdings Group Go Beyond

■DMZの外部向けサービスでどこをIPv6対応するのかと、対応方法の整理をします。

- 外部向けサービスのコンポーネント毎に機能要件と非機能要件
- IPv4との共存部での、IPv4とIPv6の冗長利用と優先処理順序、IPアドレス認証、IPアドレス埋め込みなどに注意
- DNSのzoneデータやログデータなどの移行や移行後の整合性確認も重要

IPv6対応させる箇所



7．セキュリティ

INTEC Go Beyond
IT Holdings Group

■ガイドラインの「7．IPv6環境におけるセキュリティ対応方法」で、セキュリティ上のリスクと対応方法を整理します。

IPv6導入によって気をつけたい3つのポイントは以下の通りです。

① 機器に関するセキュリティ課題

基本的にIPv4と同等の対策を講じる

IPv6ではICMPv6を全てフィルタすると不具合発生するため、ICMPv6メッセージタイプごとに取捨選択することに注意

IPv4と実装方法が異なる機材もあるので、提供機能と性能を確認

② 運用に関するセキュリティ課題

IPv4のアドレス管理手法や静的設定、逆引きの認証・存在確認利用、IPv4では使っていない機能の温存などを見直し

③ システム環境に起因する予期せぬセキュリティ課題

IPv6が有効化されている端末の放置対策

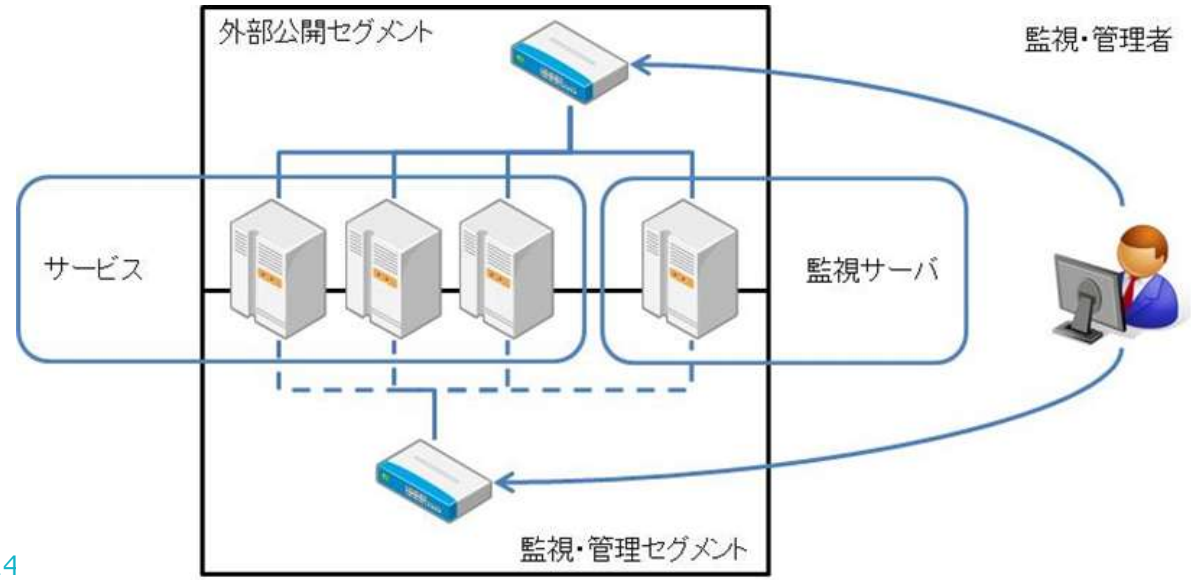
管理情報やデータ処理の未整備状況の放置対策

8. 保守・運用・監視

■ガイドラインの「8. 保守・運用・監視に関するIPv6対応方法」に従って、保守・運用・監視のIPv6対応も検討しておきます。

保守、運用、監視のIPv6対応も必要

- 監視ツールや管理ツールの見直し
- 保守条件や運用条件への組み入れ
- 障害切り分けや対応方法の見直し
  - IPv6対応によってIPプロトコルの冗長化が図れるため、可用性があがるケースも。前向きに取り組んだ方がよい



9. IPv6人材の確保

■基本計画の実行を行う人材については、ガイドラインの
「9. IPv6対応人材の確保」を参照してください。
人材の育成も検討しておきます。

IPv6の基本知識の習得は必要、さらに

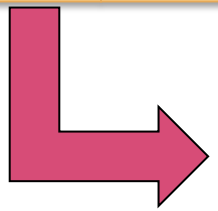
- 最新情報（技術刷新があるので最新であることに注意）の収集
- 信頼できる情報源から取得
- IPv6資格試験認定済みのプログラム受講者の積極的採用
  - 大学や専門学校でIPv6の教育を受けた人材もそろそろ巣立ち出している（エキスパートを教育するより新人を活用）

10. コスト

■調達に向けて、ガイドラインの「10. IPv6対応に伴う調達及びコストについての考え方」として、機材・設計、構築・運用のそれぞれの考え方を整理しておきます。

整理のポイント

	機器	設計・構築	運用
対応方法	IPv6デフォルト搭載機材の利用	対応できる人材の確保	IPv6導入をきっかけにした見直し
注意点	追加費用が発生するケース（高度なセキュリティ対応など）の必要性を確認	工期の延伸の可能性に注意	統合管理や各種対応手順の再検討



- **IPv4で利用していない機材や機能の削減など全体最適化によって、コストダウンが可能に**
- **「IPv6の単体導入」ではなく、「インターネット環境の見直し」**

11.（付録）チェックシート

■巻末に「チェックシート」をつけました。

- ガイドラインで示した工程に沿ったチェックシート
- 各工程でのポイントをチェックできます
- チェックシートで漏れがないか確認しながら、基本計画を作成

Ⅰ. 企業や地方自治体のネットワークの現状

Ⅱ. IPv6対応ガイドラインと調達仕様書モデルの背景

Ⅲ. IPv6対応ガイドライン

Ⅳ. IPv6調達仕様書モデル

Ⅴ. ケーススタディ

おわりに

（付録） IPv6の基礎知識

0. はじめに

■調達仕様書には以下のような内容を記載します。

1.概要
2.想定するシステム・ネットワークの全体像
3.調達範囲
4.調達にあたっての基本的考え方
5.回線サービス
6.リモートアクセス・VPN
7.機能及びサービス
8.保守要件
9.その他の留意事項

1．概要

■概要で記載する内容は以下の通りです。

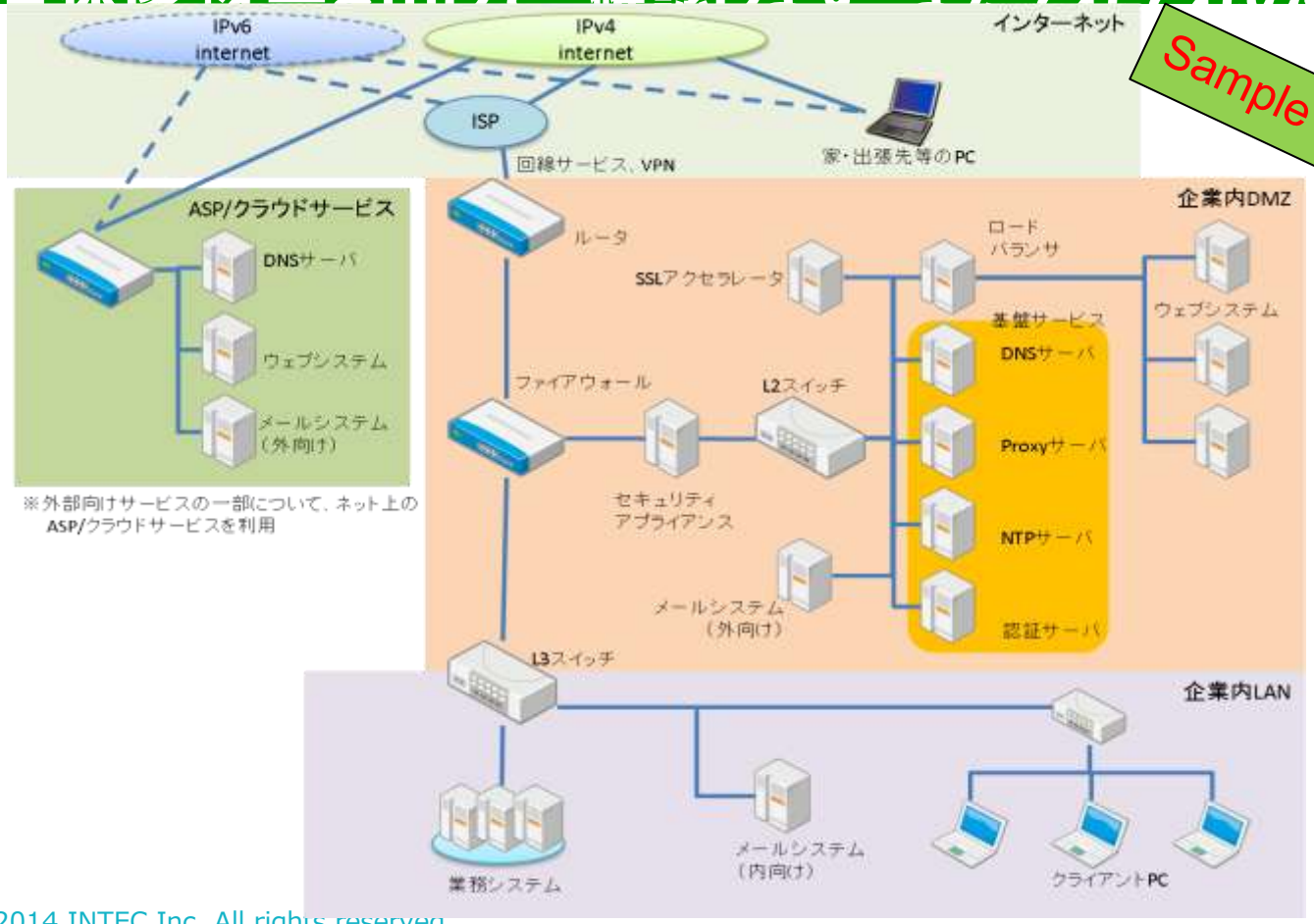
IPv6対応させる背景認識、対象とする調達によって実現される目標への認識、調達仕様書として何を記しているのか等について記載します。

具体的には、案件の名称や目的などを記載します。

2. 想定するシステム・ネットワークの全体像

■調達対象、対象外を含めて、調達後に構築を目指すシステム・ネットワーク

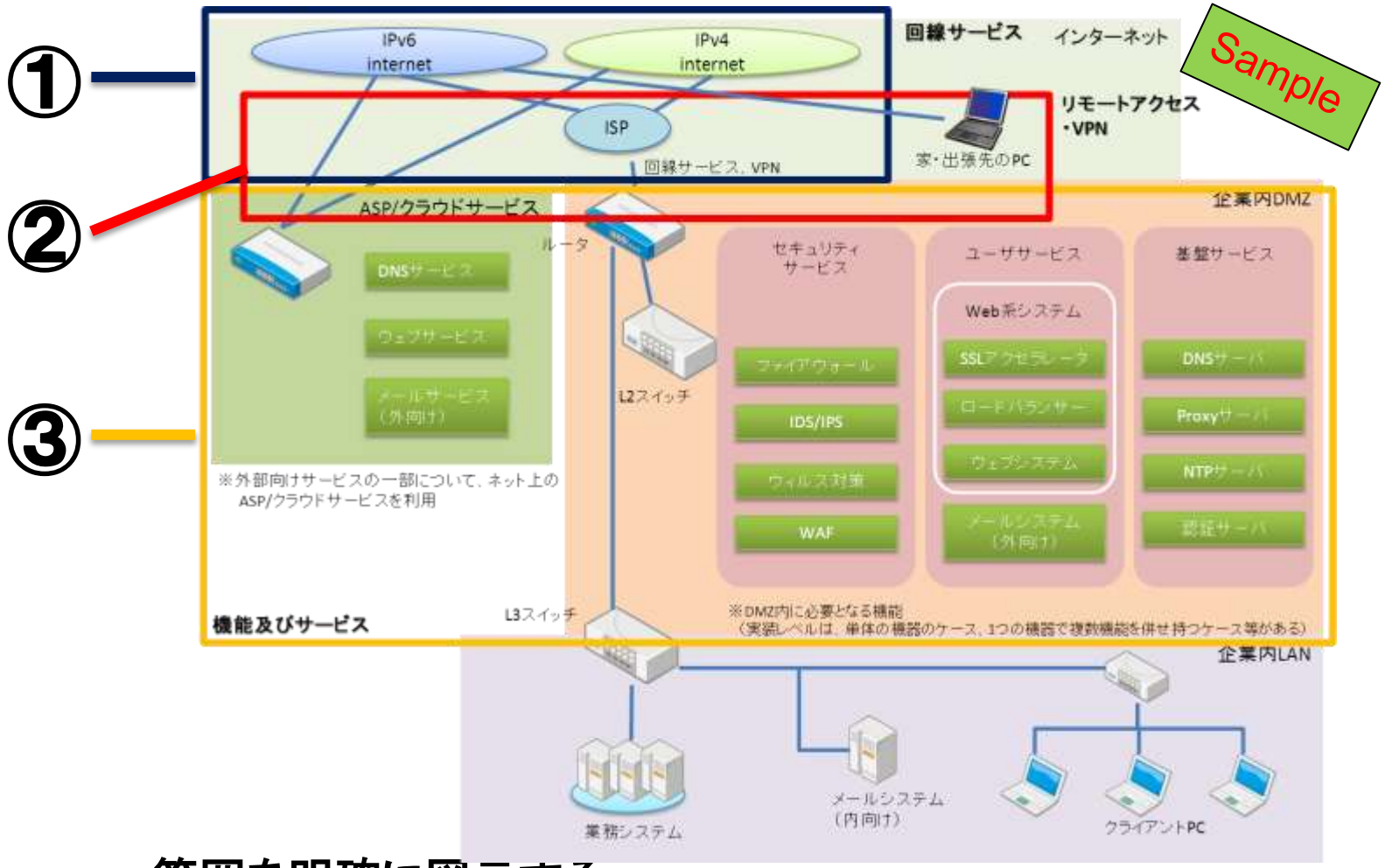
の「全体像」を書き出して、確認します。またそれぞれの構成



Sample

3. 調達範囲

■調達の範囲を記載します。



- 範囲を明確に図示する。

4. 調達にあたっての基本的考え方(1)

■調達の基本的な考え方を記載します。

NO	記載項目	記載内容	記載例
1	調達単位と 調達スケジュール	調達の範囲や、調達項目・期間について記載する	・調達単位は、「回線サービス」「リモートアクセス・VPNサービス」「機器及びサービス」とし、これらは一括して調達する（ASPは考慮しない）。
2	構築要件	設置対象機器や 設置場所を記載する	・「機器及びサービス」のうち、DMZを構成する各機器は自社内サーバ室に設置することとする。 ・システム構築に際し、ラックスペース、電源容量、空調能力が十分に用意 されている。
3	非機能要件	規模、性能、信頼性、 セキュリティを記載する	詳細は次頁参照
4	移行要件	移行期間、現行システムと新システムの並行稼働、教育等を記載する	・並行稼働を可能とし、移行は1ヶ月で終了すること。 ・新コンテンツ管理者向け教育を事前に行うこと。

4. 調達にあたっての基本的考え方（2）

■非機能要件の記載例は以下の通りです（ウェブシステム更

①規模に対する要求要件

Sample

要求項目	内容
データ検索回数	1,000件／時
データ閲覧回数	1,000件／時
ログデータ保管期間	5年間
登録利用者数	100,000人

②性能に対する要求要件

要求項目	内容
オンラインレスポンス	最大で5秒程度
オンラインスループット	100件／時

4. 調達にあたっての基本的考え方(3)

③信頼性に対する要求要件

Sample

要求項目	内容
運用スケジュール	24時間稼働
	故障時には24時間以内に要員を派遣出来る体制を確保すること
稼働率	全体として98%以上の稼働率を実現すること
拡張性	標準的なパーツを使用し、容易にシステムを拡張可能であること
事業継続性	故障時には代替機器／代替サービスを用いることで24時間以内に再開可能であること
	バックアップにより障害発生時にもログを回復可能であること

④セキュリティに対する要求要件

要求項目	内容
利用者の権限	システム管理者、登録利用者、一般利用者を区別して権限管理できること
利用制限	システム管理者は、システムの全ての機能及びデータにアクセスできること
	登録利用者は、一般利用者が利用可能なコンテンツ及び登録利用者向けに制限された機能及びデータにアクセスできること
認証・認可	OpenID及びOAuth2.0を用いた認証・認可機能であること
権限管理	認証情報、認可情報には、システム管理者のみがアクセス可能であること
	認証情報、認可情報は毎日完全なバックアップを取得すること

5. 回線サービス

■回線サービスに対する技術/運用要件やIPv4/IPv6共存に対する稼働条件を記載します。

NO	記載項目	記載内容	留意点
1	技術要件	IPv6で通信ができることやルーティングができること等を記載	IPv6アドレスに対するセカンダリDNSの提供
2	運用要件・信頼性要件	通信帯域や、サービス適用条件等を記載	品質保証がされる場合には、サービス提供条件（最大遅延時間等。いわゆるSLA）でIPv4/IPv6間での差異がないこと
3	接続要件	IPv6アドレスの払い出しの要件等を記載	
4	IPv4/IPv6共存環境に関する稼働条件	必要に応じて、IPv4アドレスの払い出し等を記載	

6. リモートアクセス・VPN

■リモートアクセス・VPNに対する技術/運用要件やIPv4/v6共存に

NO	記載項目	記載内容	留意点
1	技術要件	IPv4/IPv6双方での 通信が可能である等を 記載	
2	運用要件・ 信頼性要件	IPv4/IPv6とも同じ サービスレベルで 提供できること等を 記載	・不正アクセスなどの 監査でIPv6を識別できる ・アクセスコントロールに関し IPv6で制御できる
3	接続要件	IPv4/IPv6双方で接続 できることを記載	接続クライアントの認証は IPv4/IPv6両方で可能である
4	IPv4/IPv6共存環境 に関する稼働条件	IPv6に対応していない アプリケーションへの 接続性等について記載	

7. 機能およびサービス

■調達の範囲に示した各機能およびサービスの具体的な仕様を

NO	大分類	中分類	留意点
1	ルータ・スイッチ	・ルータ ・L3スイッチ ・L2スイッチ	・各機器及びサービスで備えるべき基本機能（ルーティング、フィルタリング、ログ出力等）を有することを記載 ・性能要件は、IPv4と同等のスループットを処理できる能力を有することを記載
2	セキュリティサービス	・ファイアウォール ・アプリケーションファイアウォール ・セキュリティアプライアンス（IDS/IPS) ・UTM	
3	ユーザサービス	・SSLアクセラレータ ・ロードバランサー ・ウエブシステム ・メールシステム	
4	基盤サービス	・DNSサーバ ・Proxyサーバ ・NTPサーバ ・認証サーバ	

- **必要に応じてバックアップ等のバックエンドのサービスも記載する。**

8. 保守要件、その他の留意事項

■システム・ネットワークの保守に関する要件を記載します。

①運用要件

②保守要件

特に、監視ツールのIPv6対応について、運用要件に含めます。

■その他留意事項について記載します。

①LAN上の端末からDMZへアクセスする通信

②WANの情報

等について記載を行います。

Ⅰ. 企業や地方自治体のネットワークの現状

Ⅱ. IPv6対応ガイドラインと調達仕様書モデルの背景

Ⅲ. IPv6対応ガイドライン

Ⅳ. IPv6調達仕様書モデル

Ⅴ. ケーススタディ

おわりに

（付録） IPv6の基礎知識

1．概要

■民間企業A社をケーススタディとして取り上げます。

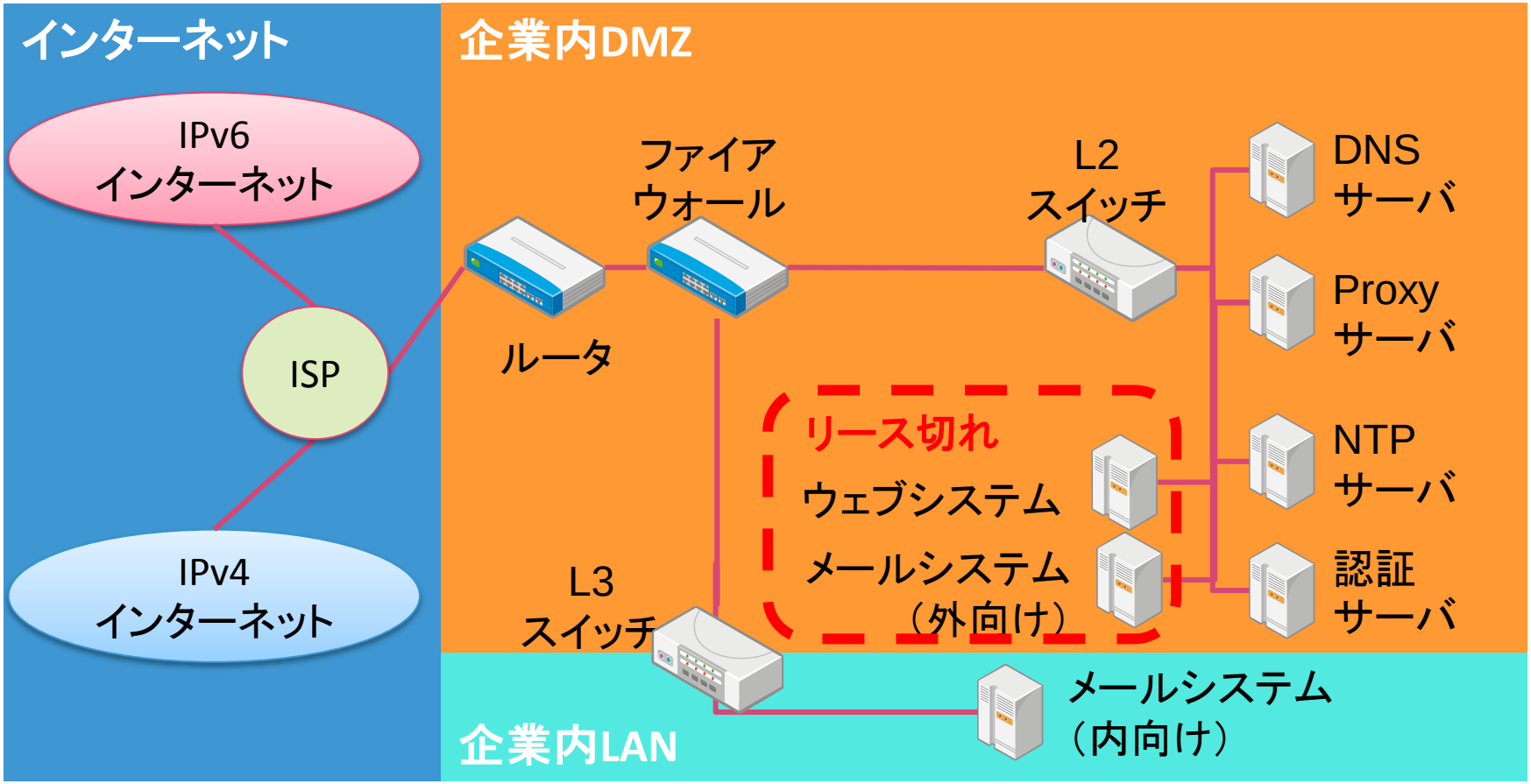
A社：

- インターネットは、ウェブシステム（企業のウェブサイト）、社員のメールシステムの利用にとどまっており、ECサイトなどは持っていない
- 外部向けインターネットサービスで使用しているウェブシステム及びメールシステムの機器がリース切れ、将来的に新たなインターネットサービスの展開を考慮して、IPv6への対応を決定
- ただしIPv6対応の必要性や喫緊性、またコストの観点から、社内LANまで含めてA社ネットワーク全体をIPv6対応するのではなく、外部向けインターネットサービス（ウェブシステム、メール）及びそれに必要となる機器のみをIPv6対応とすることに決定

それではA社における調達をケースに、調達仕様書原案の作成プロセスをみてみましょう。

2. システム・ネットワーク構成

■A社は、自社内のサーバ室にインターネット回線を引き込み、自らシステムやネットワークの運用を行っています。

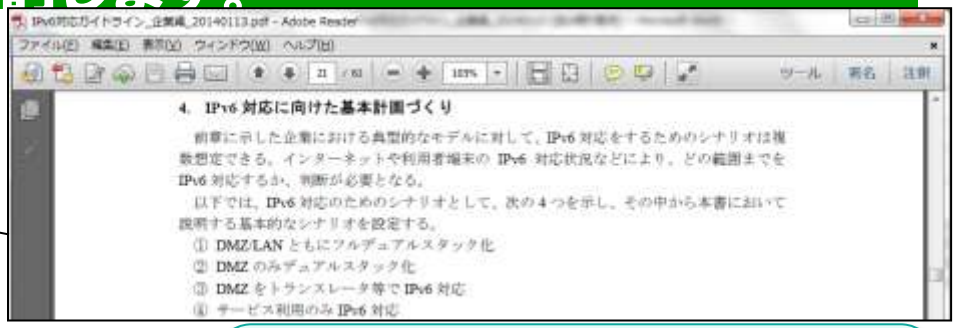


3. IPv6対応シナリオの検討（1）

INTEC IT Holdings Group Go Beyond

まず、IPv6対応シナリオを検討します。

ガイドライン企業編
「4. 基本計画づくり」18ページ



①DMZ/LANともに フルデュアルスタック化

→ 外部向けインターネットサービスのみをIPv6対応とするため対象外

②DMZのみデュアルスタック化

③DMZをトランスレータ等で IPv6対応

④ネットワークで提供される サービス利用のみIPv6対応

→
- DMZ内のサービス調査
- 利用している機器・システムの調査

この調査結果から、②～④のシナリオのどれを採用するか、または組み合わせて使うかを決定

3. IPv6対応シナリオの検討（2）

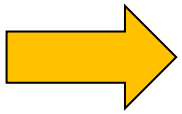
■DMZ内のサービスと、利用している機器・システム、ISPを調査

- ◆ DMZ内のサービス調査
  - ✓ 外部向けインターネットサービスは、ウェブシステム（企業のウェブサイト）、社員のメールシステムのみ
- ◆ 利用している機器・システムの調査
  - ✓ ウェブシステム及びメールシステムは新たにIPv6へ対応
  - ✓ **ウェブシステム及びメールシステムのIPv6化にあわせてIPv6化が必要となる機器・システムはすでにIPv6に対応済み**
- ◆ ISPの調査
  - ✓ **ISP側はIPv6に対応済み**

②DMZのみデュアルスタック化

③DMZをトランスレータ等でIPv6対応

④ネットワークで提供されるサービス利用のみIPv6対応

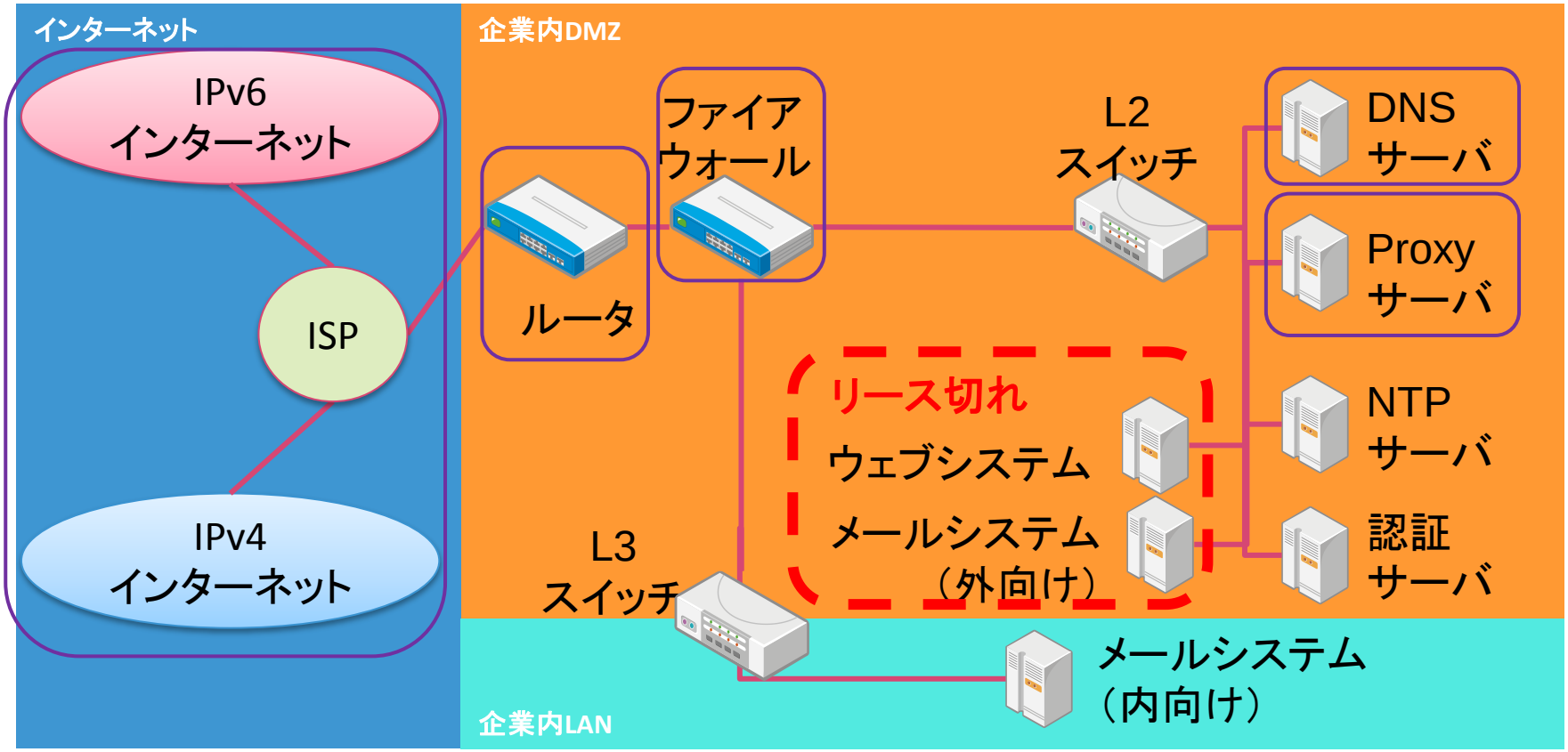


既存資産の有効活用（IPv6対応済み）の観点から、②DMZのみデュアルスタック化とすることに決定

4. IPv6対応範囲

調達仕様書モデル企業編「3. 調達範囲」(8ページ)

■ウェブシステム及びメールシステムのIPv6対応に際し、ルータ・ファイアウォール、DNS、Proxyには、設定変更の必要があることがわかりました。



次からは、システムやサービスごとの要求仕様を確認しましょう。

5. 調達にあたっての基本的考え方(1)

調達仕様書モデル企業編「4. 調達にあたっての基本的考え方」(10ページ)

■調達仕様書モデルを参照し調達仕様書を作成します。

4.調達にあたっての基本的考え方

4.1　調達単位とスケジュール

4.1.1　調達単位

①「WEBサーバ」、「メールサーバ」の新規調達
　それに伴う、既存機能/サービスの設定変更を範囲とする。

②調達単位は、一括でも分割でも良いが、対象が少ないので一括とする。

4.1.2　調達スケジュール　　省略

4.2　構築要件

①既存DMZがオフィス内にあるため、オフィス内のサーバを入れ替え。

②設置スペース、電源などは現状の設備を利用する。

※4、4.1・・・は、調達仕様書モデルの項番です。

5．調達にあたっての基本的考え方（2）

調達仕様書モデル企業編「4．調達にあたっての基本的考え方」（11ページ）

4.3　全体として確保すべき非機能要件

新たな追加要件はないため、現行のIPv4での非機能要件を記載する。

4.4　移行要件

4.4.1　移行に係る要件

①WEBサーバ

・どれくらいの期間で移行できるかを記載する。

・一括移行か段階移行なのかを明確にする。

②メールサーバ

・切り替えタイミングについて記載する。

4.4.2　教育に係る要件

①説明会やマニュアルについて記載する。

6. 回線サービス

調達仕様書モデル企業編「5. 回線サービス」（14ページ）

■回線サービス

すでにISP側はIPv6対応済みなのでIPv6オプションの申請を行い、

5. 回線サービス

本章では、調達対象である回線サービスに対する技術／運用要件を具体的に記述する。また、IPv4／IPv6 共存環境に対する稼働条件等を提示する。なお、回線サービスとしてはインターネット接続サービスを対象とし、IPv4 と IPv6 双方に対応した回線を調達することを想定する。

5.1 技術要件

- インターネットとの IPv4/IPv6 通信が可能であること。
- 静的経路（デフォルトゲートウェイ）を提供すること。
- IPv6 アドレスに対応したセカンダリ DNS サーバを提供すること。またセカンダリ DNS サーバ自身も IPv4/IPv6 通信が可能なこと。

5.2 運用要件・信頼性要件

- 回線サービスで品質が保証される場合には、通信帯域（帯
びサービス提供条件（最大遅延時間、利用時間に対する
いて IPv4/IPv6 間での差異がないこと。

7. リモートアクセス・VPN

調達仕様書モデル企業編「6. リモートアクセス・VPN」（15ページ）

6.リモートアクセス・VPN

IPv6でのリモートアクセス・VPN要件がないため、今回の調達仕様書では

6. リモートアクセス・VPN

本章では、調達対象であるリモートアクセス・VPN サービスに対する技術／運用要件を具体的に記述する。また、IPv4／IPv6 共存環境に対する稼働条件等を提示する。

6.1 技術要件

- リモートアクセス[illegible]終端装置[illegible]IPv4 終端装置の[illegible]ワークインタフェースの双方（インターネット[illegible]のクライアント接続、DMZ または LAN 側接続）で IPv4/IPv6 通信が可能なこと。
- インターネット側のクライアント接続、DMZ または LAN 側の接続の双方で IPv4/IPv6 通信が可能なこと。
- 外部認証装置を利用可能な場合、その装置との接続について IPv4/IPv6 通信が可能なこと。

記載の必要なし

8. 機能およびサービス（1）ルータ・スイッチ①

調達仕様書モデル企業編「7. 機能及びサービス　7. 1ルータ・スイッチ」（16ページ）

■調達仕様書モデルには以下の通り記載されています。

7.機能及びサービス

7.1　ルータ・スイッチ

7.7.1　ルータ

- ルータとして備えるべき基本機能を有すること。
- インターネットとIPv4/IPv6通信が可能なこと。
- ルータからISPに接続する回線上にIPv4/IPv6パケットを通過させること。
- IPv4/IPv6のルーティング機能を有すること。
- IPv4/IPv6のフィルタリング機能を有すること。
- 【OP】IPv4/IPv6のパケットシェーピング機能を有すること。
- 【OP】IPv4/IPv6の優先制御機能を有すること。

【OP】はオプション項目のことです。

次ページに続く

8. 機能およびサービス（1）ルータ・スイッチ②

前ページより

- IPv4通信とIPv6通信が同等のスループットを処理できる能力を有すること。
- IPv4/IPv6通信による運用管理端末からのリモート保守を可能とする機能を有すること。
- 【OP】IPv4/IPv6通信による構成定義情報のバックアップを可能とする機能を有すること。
- IPv4/IPv6通信による時刻設定を常時正しい状態に保つことを可能とする機能を有すること。
- 【OP】IPv4/IPv6のMIBに対応すること。
- MIBの設定や情報取得のための転送にIPv4/IPv6通信が利用できること。
- IPv4/IPv6情報をログ出力できること。
- ログ出力の通信にIPv4/IPv6通信が利用できること。

WEBとメールをIPv6対応するに際し、赤字の部分は、既存機器での設定変更が必要となります。これら「設定変更」を考慮した調達仕様書が次ページとなります。

8. 機能およびサービス（1）ルータ・スイッチ③

★調達仕様書モデル企業編「7．1　ルータ・スイッチ」（16ページ）をA社向けカスタマイズ後

■調達仕様書には以下のように記載を行います。

7.機能及びサービス

7.1　ルータ・スイッチ

7.7.1　ルータ

既存機器で以下のIPv6対応の設定変更を実施する事

- 通信設定
- パケット通過
- ルーティング設定
- フィルタリング設定
- パケットシェーピング
- 優先制御
- MIB出力
- ログ出力

L3スイッチやL2スイッチに関しても同じような視点で記載を行います。

8. 機能およびサービス(2) セキュリティサービス①

調達仕様書モデル企業編「7. 2 セキュリティサービス 7. 2. 1 ファイアウォール」(17ページ)

■調達仕様書モデルには以下の通り記載されています。

7.2 セキュリティサービス

7.2.1 ファイアウォール

- ファイアウォールとして備えるべき基本機能を有すること。
- IPv4/IPv6通信が可能なこと。
- IPv4/IPv6のルーティング機能を有すること。
- IPv4/IPv6のフィルタリング機能を有すること。
- IPv4/IPv6のTCP/UDPが監視できること。
- IPv4/IPv6のステートフルインスペクション機能を有すること。
- IPv4/IPv6のIPヘッダチェック機能を有すること。
- IPv4/IPv6のDoS攻撃防御機能を有すること。
- IPv4/IPv6のフラグメンテーションアノマリ機能を有すること。
- IPv4/IPv6のIPアドレスアノマリ機能を有すること。
- IPv4/IPv6のTCPアノマリ機能を有すること。

次ページへ

8. 機能およびサービス (2) セキュリティサービス②

前ページより

- IPv4/IPv6のUDPアノマリ機能を有すること。
- IPv4通信とIPv6通信が同等のスループットを処理できる能力を有すること。
- IPv4/IPv6通信による運用管理端末からのリモート保守を可能とする機能を有すること。
- IPv4/IPv6通信による構成定義情報のバックアップを可能とする機能を有すること。
- IPv4/IPv6通信による時刻設定を常時正しい状態に保つことを可能とする機能を有すること。
- IPv4/IPv6のMIBに対応すること。
- MIBの転送にIPv4/IPv6通信が利用できること。
- IPv4/IPv6情報をログ出力できること。

WEBとメールをIPv6対応するに際し、赤字の部分は、既存機器での設定変更が必要となります。これら「設定変更」を考慮した調達仕様書が次ページとなります。

8. 機能およびサービス(2) セキュリティサービス③

★調達仕様書モデル企業編「7．2．1　ファイアウォール」(17ページ)をA社向けカスタマイズ後

■調達仕様書には以下のように記載を行います。

7.2.1　ファイアウォール

既存機器で以下のIPv6対応の設定変更を実施する事

- 通信設定
- ルーティング設定
- フィルタリング設定
- 監視設定
- ステートフルインスペクション機能設定
- IPヘッダチェック機能設定
- DoS攻撃防御機能設定
- フラグメンテーションアノマリ機能設定
- IPアドレスアノマリ機能設定
- TCPアノマリ機能設定変更
- UDPアノマリ機能設定変更
- MIB出力
- ログ出力

8. 機能およびサービス (2) セキュリティサービス④

調達仕様書モデル企業編「7. 2. 2 ～ 7. 2. 3」(18ページ)

7.2.2 アプリケーションファイアウォール

未導入の為記載の必要なし

7.2.3 セキュリティアプライアンス(IDS/IPS)

未導入の為記載の必要なし

7.2.4 UTM

未導入の為記載の必要なし

7.2.3

セキュリティアプライアンス（IDS/IPS）

- IDS/IPS として備えるべき基本機能を有すること。
- IPv4/IPv6 通信が可能なこと。
- 電子メールのウィルス検出など、アプリケーションレベル（L7）の検査が IPv4/IPv6 通信に対して可能であること。
- パターンファイル、エンジンモジュールを設定したスケジュールで納入元のサーバに IPv4/IPv6 でインターネット等を経由してアクセスし、自動的に更新できること。
- IPv4 通信と IPv6 通信が同等のスループットを処理できる能力を有すること。
- 冗長構成を取ることで IPv4／IPv6 通信の冗長化を可能とする機能を有すること。
- IPv4/IPv6 通信による運用管理端末からのリモート保守を可能とする機能を有すること。

記載の必要なし

8. 機能およびサービス (3) ユーザサービス (1)

調達仕様書モデル企業編「7. 3. 1 ～ 7. 3. 2」(19ページ)

7.3 ユーザサービス
7.3.1 SSLアクセラレータ
未導入の為記載しない
7.3.2 ロードバランサ
未導入の為記載しない

7.3 ユーザサービス

SSL アクセラレータ

- SSL アクセラレータとして備えるべき基本機能を有すること。
- IPv4/IPv6 通信が可能なこと。
- サーバ証明書を[illegible] IPv4/IPv6 通信で SSL や TLS プロトコルで暗号化できる機能を有すこと。
- IPv4 通信と IPv6 通信が同等のスループットを処理できる能力を有すること。
- 冗長構成を取ることで IPv4／IPv6 通信の冗長化を可能とする機能を有すること。
- IPv4/IPv6 通信による運用管理端末からのリモート保守を可能とする機能を有すること。
- 【OP】IPv4/IPv6 通信による構成定義情報のバックアップを可能とする機能を有するこ

記載の必要なし

8. 機能およびサービス(3) ユーザサービス②

調達仕様書モデル企業編「7. 3. 3 ウェブシステム」(20ページ)

■調達仕様書モデルには以下の通り記載されています。

7.3.3 ウェブシステム

- ウェブシステムとして備えるべき基本機能を有すること。
- IPv4/IPv6通信が可能なこと。
- Web ブラウザ等のクライアントからのIPv4/IPv6通信による要求に対して、Web サーバ上に格納されたコンテンツを返送できること。
- サーバ証明書をインストールし、IPv4/IPv6通信をSSL やTLS プロトコルで暗号化できる機能を有すること。電子政府推奨暗号リストに対応する暗号強度を有するものを適用すること。
- ウェブシステムのCMS(コンテンツ・マネジメント・システム)等が備える外部との連携機能において、IPv4/IPv6の双方に対応すること。

次ページへ

8. 機能およびサービス(3) ユーザサービス③

前ページより

- IPv4通信とIPv6通信が同等のスループットを処理できる能力を有すること。
- IPv4/IPv6通信による運用管理端末からのリモート保守を可能とする機能を有すること。
- IPv4/IPv6通信による構成定義情報のバックアップを可能とする機能を有すること。
- IPv4/IPv6通信による時刻設定を常時正しい状態に保つことを可能とする機能を有すること。
- IPv4/IPv6情報をログ出力できること。
- ログ出力の通信にIPv4/IPv6通信が利用できること。

青色の部分は現在その機能を有しないため割愛し調達仕様書に記載します。

8. 機能およびサービス(3) ユーザサービス④

調達仕様書モデル企業編「7. 3. 4 メールシステム」(21ページ)

■調達仕様書モデルには以下の通り記載されています。

7.3.4 メールシステム

- メールシステムとして備えるべき基本機能を有すること。
- IPv4/IPv6通信が可能なこと。
- インターネットとのIPv4/IPv6通信による送受信要求はSMTPに対応すること。送信ドメイン認証が可能なこと。
- IPv4通信とIPv6通信が同等のスループットを処理できる能力を有すること。
- IPv4/IPv6通信による運用管理端末からのリモート保守を可能とする機能を有すること。
- IPv4/IPv6通信による構成定義情報のバックアップを可能とする機能を有すること。
- IPv4/IPv6通信による時刻設定を常時正しい状態に保つことを可能とする機能を有すること。
- IPv4/IPv6情報をログ出力できること。
- ログ出力の通信にIPv4/IPv6通信が利用できること。

このまま記載します。

8. 機能およびサービス(4) 基盤サービス①

調達仕様書モデル企業編「7．4　基盤サービス」(21ページ)

■調達仕様書モデルには以下の通り記載されています。

7.4　基盤サービス

7.4.1　DNSサーバ

- DNSサーバとして備えるべき基本機能を有すること。
- IPv4/IPv6通信が可能なこと。
- IPv4/IPv6通信によるDNS の名前(アドレス)解決機能を有すること。
- IPv4/IPv6通信による順引き及び逆引きに対応していること。
- 上位又は下位のDNS サーバとIPv4/IPv6通信で連携する機能を有すること。
- IPv4及びIPv6に関連するレコードを保持できること。

次ページへ

8. 機能およびサービス(4) 基盤サービス②

前ページより

- IPv4通信とIPv6通信が同等のスループットを処理できる能力を有すること。
- IPv4/IPv6通信による運用管理端末からのリモート保守を可能とする機能を有すること。
- IPv4/IPv6通信による構成定義情報のバックアップを可能とする機能を有すること。
- IPv4/IPv6通信による時刻設定を常時正しい状態に保つことを可能とする機能を有すること。
- IPv4/IPv6情報を**ログ出力**できること。
- ログ出力の通信にIPv4/IPv6通信が利用できること。

WEBとメールをIPv6対応するに際し、赤字の部分は、既存機器での設定変更が必要となります。これら「設定変更」を考慮した調達仕様書が次ページとなります。

8. 機能およびサービス(4) 基盤サービス③

★調達仕様書モデル企業編「7．4．1　DNSサーバ」(21ページ)をA社向けカスタマイズ後

■調達仕様書には以下の通り記載します。

7.4.1　DNSサーバ

既存機器で以下のIPv6対応の設定変更を実施する事

- 通信設定
- DNS の名前(アドレス)解決機能設定
- 順引き及び逆引きに対応設定
- 上位又は下位のDNS サーバとの通信設定
- 関連するレコードを保持設定
- ログ出力設定

8. 機能およびサービス(4) 基盤サービス④

調達仕様書モデル企業編 「7. 4. 2 Proxyサーバ」(21ページ)

■調達仕様書モデルには以下の通り記載されています。

7.4.2 Proxyサーバ

- Proxyサーバとして備えるべき基本機能を有すること。
- IPv4/IPv6通信が可能なこと。
- IPv4/IPv6通信によるアクセスをProxy サーバが中継できること。
- IPv4通信とIPv6通信が同等のスループットを処理できる能力を有すること。
- IPv4/IPv6通信による運用管理端末からのリモート保守を可能とする機能を有すること。
- IPv4/IPv6通信による構成定義情報のバックアップを可能とする機能を有すること。
- IPv4/IPv6通信による時刻設定を常時正しい状態に保つことを可能とする機能を有すること。
- IPv4/IPv6情報をログ出力できること。
- ログ出力の通信にIPv4/IPv6通信が利用できること。

WEBとメールをIPv6対応するに際し、赤字の部分は、既存機器での設定変更が必要となります。これら「設定変更」を考慮した調達仕様書が次ページとなります。

8. 機能およびサービス(4) 基盤サービス⑤

★調達仕様書モデル企業編 「7. 4. 2 Proxyサーバ」(21ページ)をA社向けカスタマイズ後

■調達仕様書には以下の通り記載します。

7.4.2 Proxyサーバ

既存機器で以下のIPv6対応の設定変更を実施する事

- 通信設定
- ログ出力設定

8. 機能およびサービス(4) 基盤サービス⑥

調達仕様書モデル企業編「7. 4. 3 ～ 7. 4. 4」(22ページ)

7.4.3 NTPサーバ

特にWEB、メールサーバとIPv6で時刻同期する必要がないため、記載しない

7.4.4 認証サーバ

認証機能はないため記載しない

7.4.4 認証サーバ

- 認証サーバとして備えるべき基本機能を有すること。
- IPv4/IPv6 通信が可能なこと。
- IPv4/IPv6 通信を使用する Web アプリケーションに対して、指定された認証方式による認証と、URL [illegible] 機能を提供すること。
- 【OP】外部の認証サーバと IPv4/IPv6 通信で連携できること。
  - 外部の認証サーバと連携する場合。
- IPv4 通信と IPv6 通信が同等のスループットを処理できる能力を有すること。
- 冗長構成を取ることで IPv4／IPv6 通信の冗長化を可能とする機能を有すること。

記載の必要なし

8. 機能およびサービス(5)その他の必要な機能及びサービス

調達仕様書モデル企業編「7．4．3 ～ 7．4．4」(22ページ)

7.5 その他の必要な機能及びサービス

7.5.1 トランスレータ

未導入の為記載の必要なし

7.5.2 仮想化基盤

未導入の為記載の必要なし

7.4.3 運用監視機能

運用監視はIPv6化しないため記載の必要なし

9. 保守要件（1）

調達仕様書モデル企業編「8．1　運用要件」（25ページ）

■調達仕様書モデルには以下の通り記載されています。

8.1 運用要件

- システムは原則として24時間365日運用とする。
- システム障害の予防と早期発見のため、IPv4及びIPv6に対応した監視ツールを使用し、集中管理ができることとする。
- プログラム、データ、各種ログ等の特性に応じ、定期的にバックアップ出来ること。
- バックアップにあたっては、システムを停止しないオンライン・バックアップが出来ること。
- 監視・運用に用いるシステムはオフィス内のサーバ室に設置する。なおその一部は、ASP/クラウドサービスにより提供するものでも可とする。
- システム運用体制、障害時の対応体制、連絡窓口、ヘルプデスク、保証品質について明示した運用計画書を予め提出し、承認を得ること。

青色の部分は現在その機能を有しないため割愛し調達仕様書に記載します。

9. 保守要件 (2)

調達仕様書モデル企業編「8. 2　保守要件」（25ページ）

■調達仕様書モデルには以下の通り記載されています。

8.2 保守要件

- システムの機能的な不具合の修正及び設定の変更等を保守の対象とする。
- 不具合発生時の早急な修正を可能とする計画を用意すること。
- 設計情報、定義情報等のドキュメントを整備し、障害や改訂の際に対象箇所を容易に識別出来るようにすること。
- バージョン管理を適切に行える仕組を提供すること。
- 保守対応時間は、平日9時から17時までとする。なお、これ以外の対応時間においても、緊急度の高い不具合に対して臨時の対応を可能とする仕組を提供すること

このまま記載します。

10. 最後に

- これで、仕様書の原案ができあがりました。チェックシートで記載項目に漏れがないか確認してみましょう。

- 漏れがない事を確認し、調達仕様書を作成します。

おわりに

資料のダウンロード

○総務省

http://www.soumu.go.jp/menu_seisaku/ictseisaku/ipv6/

- IPv6対応ガイドライン(中小通信事業者編)
- IPv6対応ガイドライン(企業編)
- IPv6対応ガイドライン(地方自治体編)
- IPv6対応調達仕様書モデル(企業編)
- IPv6対応調達仕様書モデル(地方自治体編)

ご清聴ありがとうございました

（付録） IPv6の基礎知識

1．IPv6対応の必要性

INTEC IT Holdings Group Go Beyond

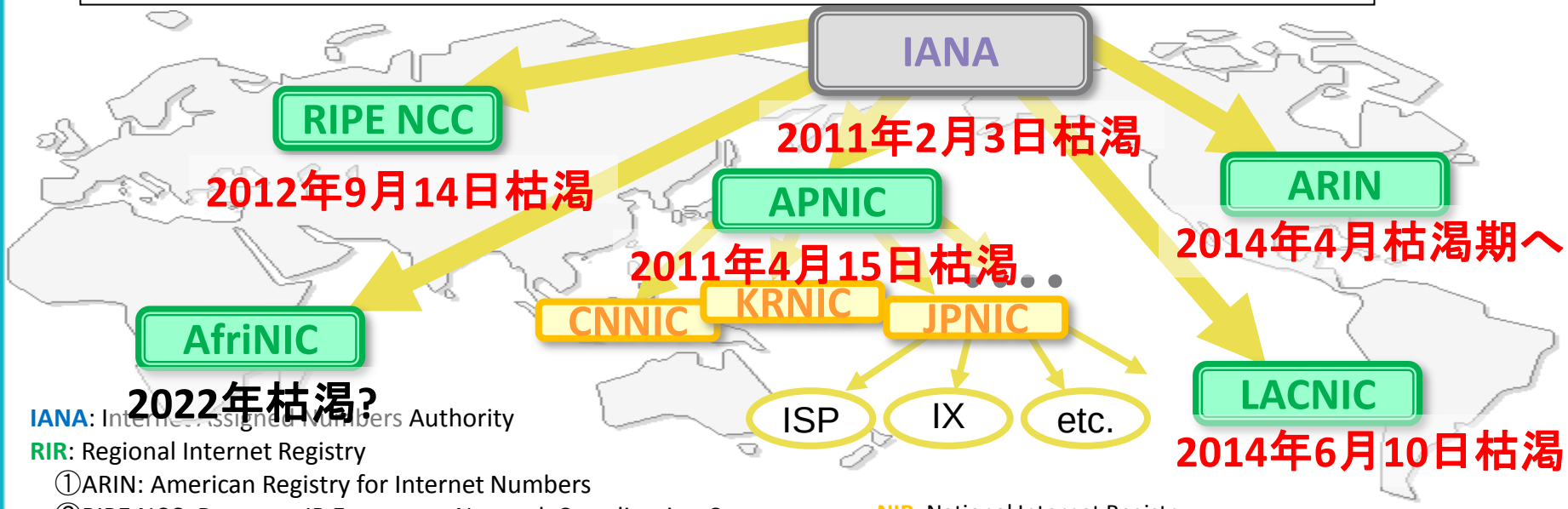
■そもそもIPv6対応は必要なのか？の疑問にお答えします。

IPv4アドレスの在庫は枯渇しました。

① 既存のIPv4サービスの拡張が困難（NATでの品質維持も困難）

② IPv4を利用した新規サービスの開発・提供が困難

→ 次世代プロトコル「IPv6」へ



IANA: Internet Assigned Numbers Authority

RIR: Regional Internet Registry

①ARIN: American Registry for Internet Numbers

②RIPE NCC: Resource IP Europeans Network Coordination Centre

③LACNIC: Latin American and Caribbean Internet Address Registry

④AfriNIC: African Network Information Centre

⑤APNIC: Asia Pacific Network Information Center

NIR: National Internet Registry

JPNIC: Japan Network Information Center

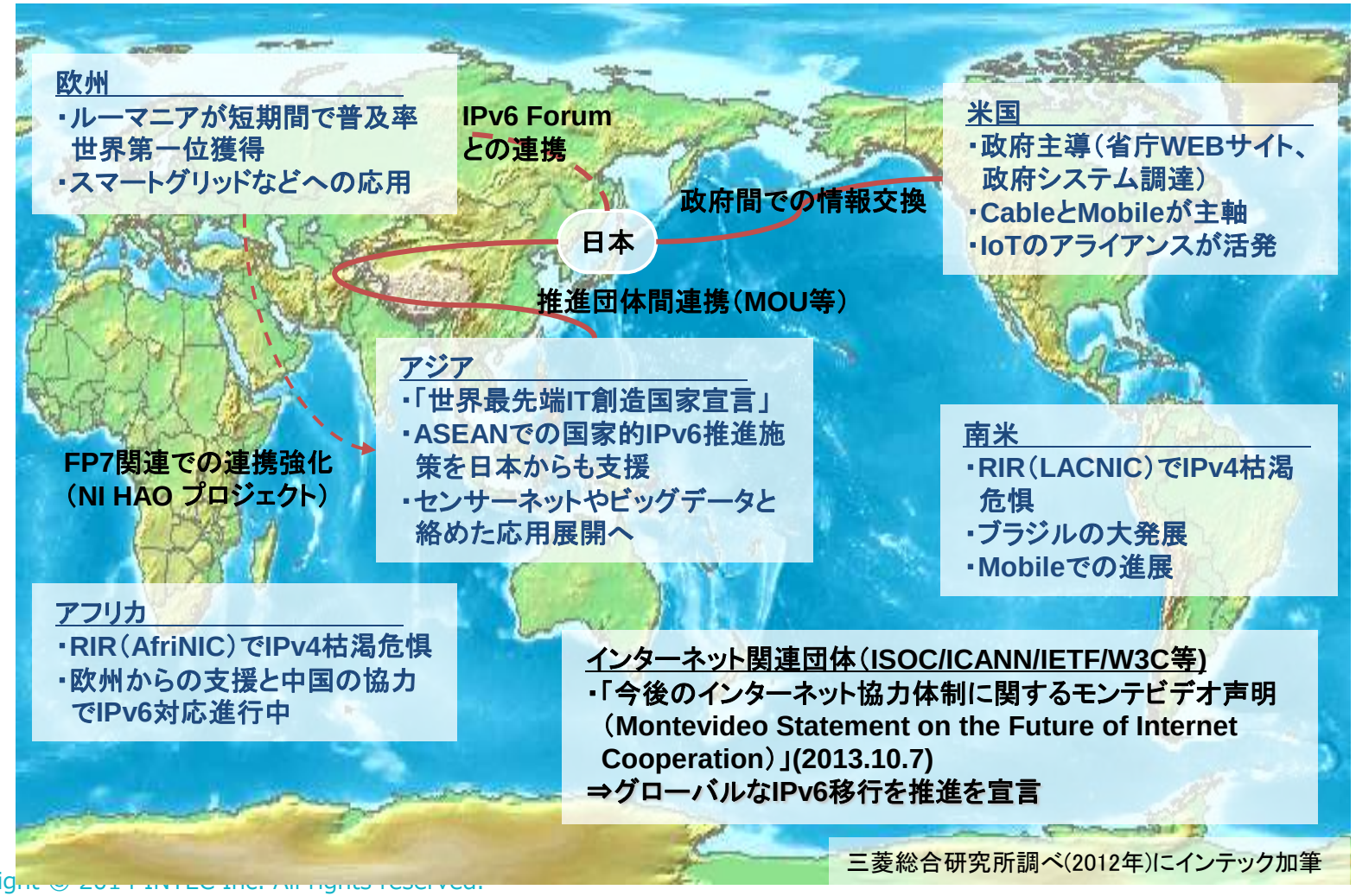
KRNIC: Korea Network Information Center

CNNIC: China Internet Network Information Center…他

2. IPv6の普及状況

■世界中でIPv6対応が進展中です。

日本では「世界最先端IT創造国家宣言」でIPv6推進。企業や地方自治体のWebサイトの対応が課題



3. IPv4とIPv6の違い（1）

INTEC IT Holdings Group Go Beyond

■IPv4とIPv6は何が違うのか？にお答えします。

①IPv4とIPv6ではアドレスの長さや表記方法が違います

・IPv4を前提としているとIPv6ではエラーになります

IPv4　192.168.0.1
IPv6　2001:db8:fa0:4000::1

②パケット形式やプロトコルが備える機能が違います

・IPv4プロトコルの再設計。運用管理が楽になる工夫が必要です
・パケットフィルタなどのセキュリティ対策に注意が必要です

③IPv4とIPv6は互換性がありません

・IPv4とIPv6は直接やり取りできません
・共存環境にしない場合は、どこかに変換装置を入れる必要があります

④IPv4とIPv6の共存環境では処理順序に注意が必要です

・「IPv6優先、IPv6が使えないときはIPv4へ」が基本（アプリケーションに依存）
・サーバ側ではIPv4とIPv6をパラレルに待受けさせる等して、独立運用も可能です

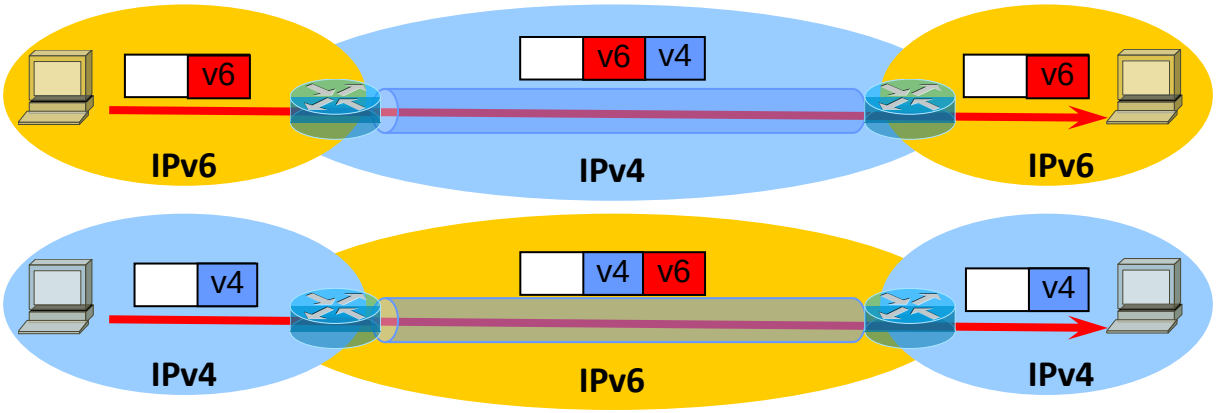
3. IPv4とIPv6の違い（2） ①アドレスの長さや表記の違い

■IPv4アドレスとIPv6アドレスの長さや表記の違いです。（赤字が変更点）

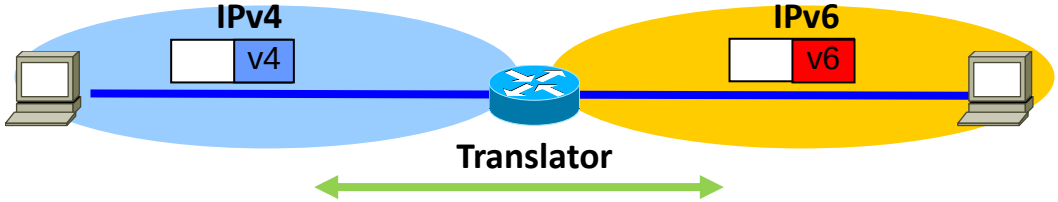
3. IPv4とIPv6の違い（3） ③互換性がないことへの対策

■IPv4とIPv6の非互換性対策として、ネットワーク接続方法が2通りあります。

- トンネリング
  - 端末やセグメント間でカプセリングして中継網を通過



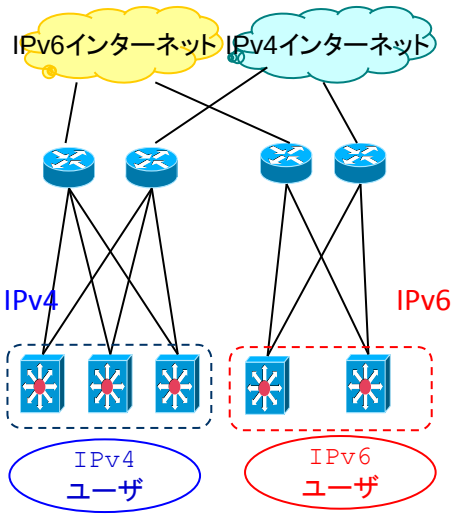
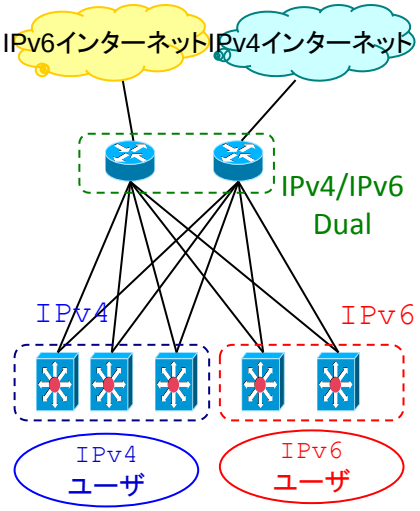
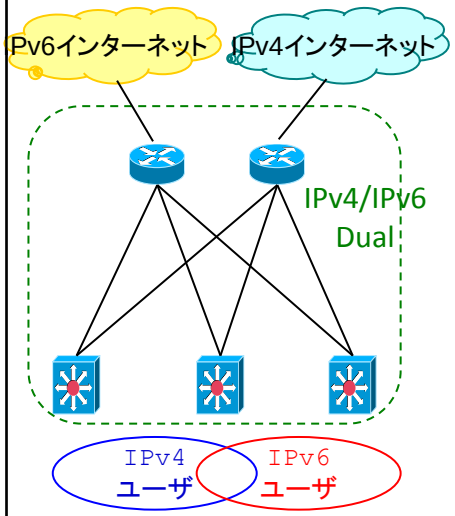
- トランスレータ
  - IPv4 ホストと IPv6 ノード間の通信におけるプロトコル変換



トランスレータには、NAT64・TransportRelay・ALGなどの方式があります。
トランスレーションできないアプリケーションもあります。（一部のIP電話やVPNなど）

3. IPv4とIPv6の違い(4)
④組織でのIPv4/IPv6共存パターン

■組織内をIPv6対応する方法には3つのパターンがあります。

	完全別ネットワーク構成	一部別ネットワーク構成	完全デュアルスタック構成
			
既存IPv4への影響	なし	限定的	あり
障害切り分けの難易度	低	中	高
コスト	高	中	低

※コストは機材台数で比較した場合

4.「IPv6に対応しない」リスク（1）

■「IPv6に対応しない」場合にはリスクがあります。

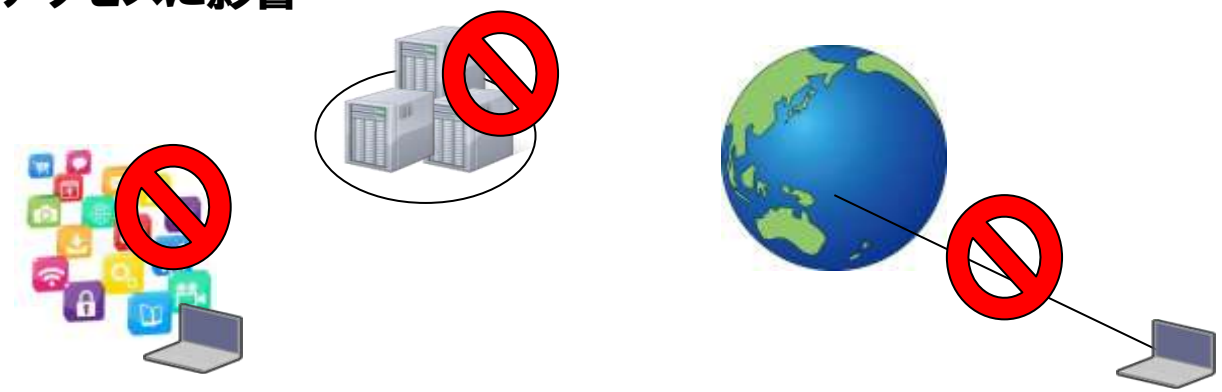
ビジネスへの影響

① IPv4アドレスの枯渇により、データセンター事業、クラウド事業の拡大に影響

② **動かないWebアプリケーション**が出現し、コンテンツ事業に影響

③ IPv6サイトとのシステム連携に不具合が発生し、ネットからの情報収集に影響

④ IPv4アドレス割り当が少なくIPv6で拡大する中国、インド等の海外ユーザからのWebサイトへのアクセスに影響

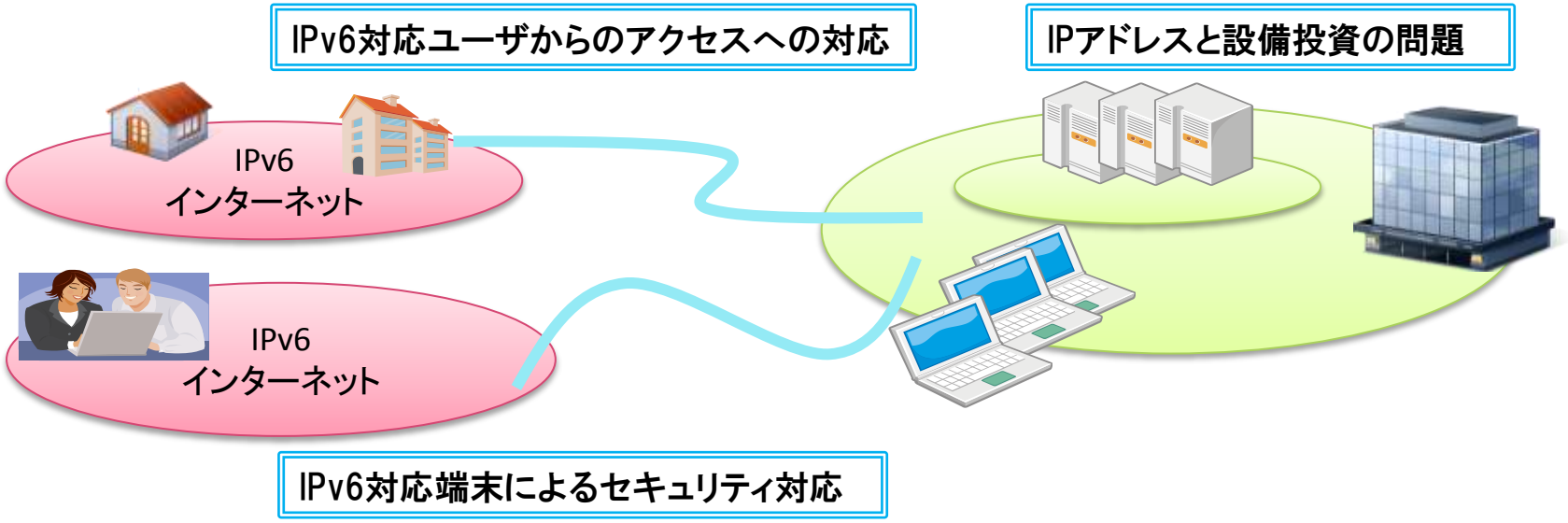


4.「IPv6に対応しない」リスク(2)

■「IPv6に対応しない」場合にはリスクがあります。

地方自治体や企業内ネットワークへの影響

① Webサイト閲覧機会損失の可能性
② 社内のユーザ対応が増える
③ 意図しない通信などの**セキュリティリスクが増える**
④ **ビジネス機会損失**の可能性
⑤ IPアドレスコストが増える可能性
⑥ 新技術対応への遅れ



5. IPv6のメリット、デメリット

INTEC Go Beyond
IT Holdings Group

■一般的なIPv6導入のメリット、デメリットです。

	メリット	デメリット
ビジネス機会	・広大なアドレス空間が利用できる ・接続対象を飛躍的に増やせる	導入事例が少ない
セキュリティ	・NATを使わないシンプルな セキュリティモデルが実現される ・アドレス空間が広大なので、 攻撃の早期発見が可能	・セキュリティ対策の見直しが必要 ・NATを利用しないため、 端末アドレスや利用機材情報 （MACアドレス）が漏洩する 可能性がある
アドレス管理 コスト	・/64の固定サブネット長でLANの サブネットアドレス細分化の 管理労力が低減 ・NATの導入と管理コストが低減	・表計算ソフトでのアドレス 管理は難しくなる ・管理方法の見直しが必要
可用性向上	・シンプルな設計が可能 ・アドレス自動設定や死活監視等が 充実 ・共存環境では、冗長性確保が できる	IPv4との互換性がなく、並行運用になる

6. IPv6の先行事例

■IPv6対応取り組み事例の背景とメリットの抜粋です。

① 大手電機メーカー

※DC＝データセンタ

- ✓ ネットワーク運用管理部門がIPv6ネットワークとDCの整備を決定
- ✓ 業務システムやアプリケーションサーバのDC集約
- ✓ 標準端末やシステム導入・改修の共通ガイドラインの提供開始
  - → NATやプライベートアドレス重複管理などの導入・運用管理コストの削減
  - → 管理強化によるセキュリティリスクの軽減
  - → 数千ものシステムの見直しによる不要なシステムの削減

② 地方自治体

- ✓ 防災センサーネットワークの整備
  - → IP対応機材を優先導入し、専用機材より安価に導入
  - → ゼロコンフィグで多数のセンサーの配備、運用管理を簡単に実現
  - → IPv6マルチキャストの一斉情報発信利用で、特別な配信システムなしで実現