別添13

資料２－１－４

クラウド時代の自治体ネットワーク最適化方法

－ネットワークに求められる要件－

（案）

平成２１年１２月９日

総　務　省

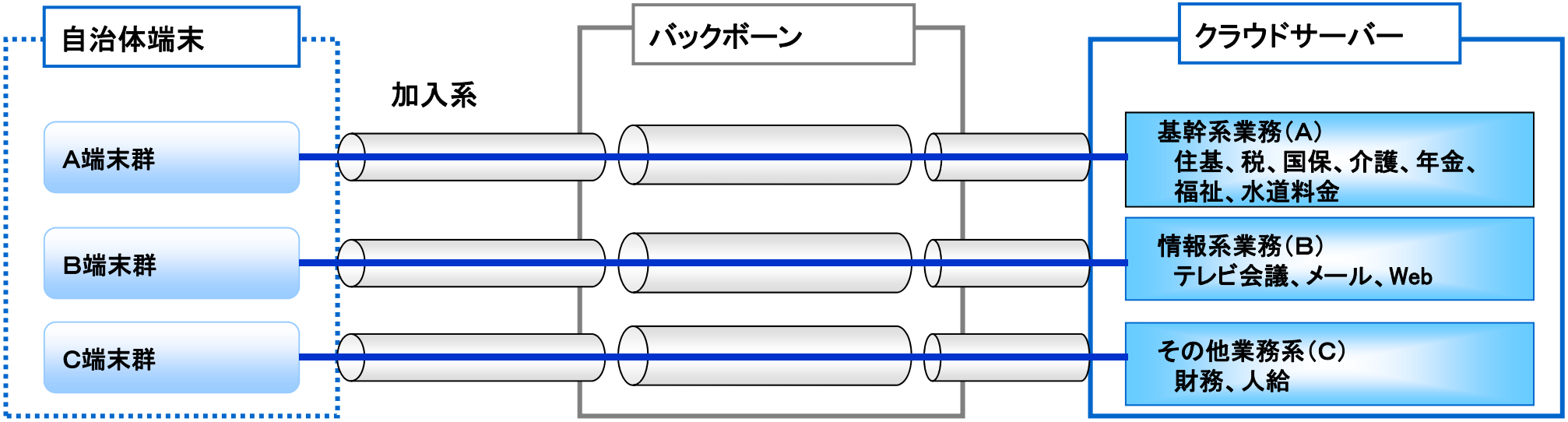
自治体業務へのクラウドサービス導入にあたっての機能分担案（例）

前提
- ✓クラウドサーバーの障害による業務停止の可能性は低いと想定されるが、万が一に備えて自治体内での証明発行や受付などの窓口業務は対応可能とする。
- ✓全データのバックアップはクラウドサーバー側で取得するものとする。

項目		機能分担	自治体側	クラウドサーバ側
各種データ管理と業務	1	マスタデータ管理、バックアップデータ管理		○
	2	縮退運転時（センタ障害時）の窓口業務用データ管理（証明書データ等）と証明発行	○	
	3	過去（過年度、改製原等）データ管理と証明発行	○ （移行不可の場合）	○ （移行可の場合）
業務機能	4	通常業務		○
入力データ取込	5	自治体に送付される外部からのデータ取込(*1)	○ （両立もあり）	○ （両立もあり）
帳票印刷	6	バッチ帳票の印刷機能(*2)	○ （少量）	○ （大量）
窓口対応	7	縮退運転時の各種データ照会	○	
自庁内システム連携機能	9	自庁内システムとの連携機能	○	

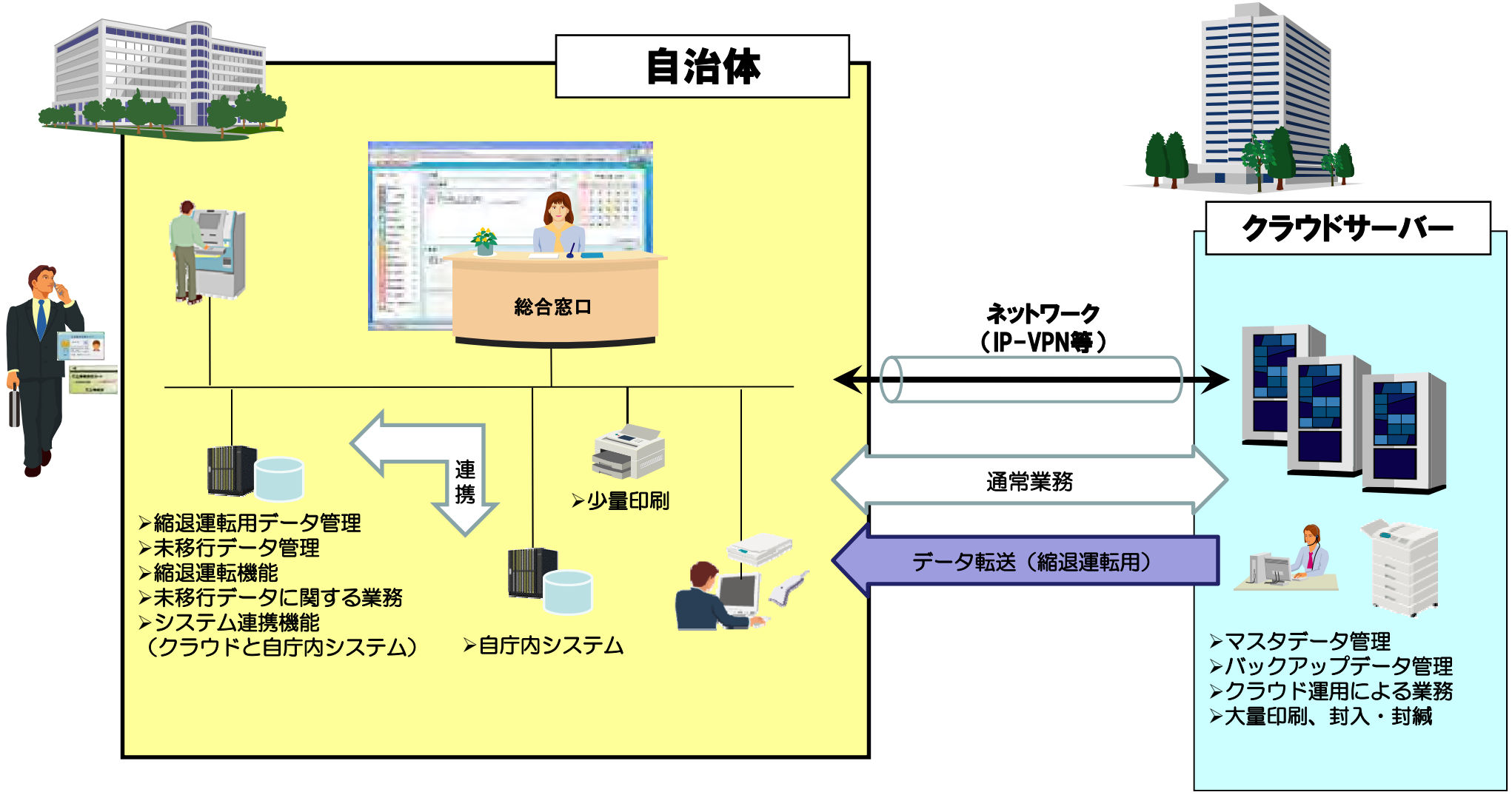
*1、*2：その他付随業務
**：自治体によってネットワーク未接続業務として、投票時の選挙人名簿の確認、住民税の申告等の業務が自治体側にある。

ブロードバンドを活用した公共ネットワークサービス（例）



	セキュリティ（a）	容量（b）	安全性（可用性）（c）	（a）＋（b）＋（c）望ましいネットワークサービス案（例）		コスト	備考
				加入系	バックボーン		
Aライン	高	中	高	イーサアクセス、ATMアクセス、専用線	IP-VPN	高	・帯域保証型 ・経路設定・管理は通信事業者側で実施するためユーザ負担小
					広域イーサ	中	・帯域保証型 ・経路設定・管理はユーザ側で実施
Bライン	低	大	低	一般ユーザ向けFTTHサービス	エントリーVPN	低	・ベストエフォート型
					インターネットVPN（SSL-VPN、IPSec）	低	・ベストエフォート型
Cライン	中	小	中	イーサアクセス、ATMアクセス、専用線、事業所向けFTTHサービス（IP-VPNのみ）	IP-VPN	高	・帯域保証型（事業所向けFTTHはベストエフォート型）
					広域イーサ	中	・帯域保証型

機能分担案のイメージ


自治体
総合窓口
ネットワーク
（IP-VPN等）
クラウドサーバー
連携
通常業務
データ転送（縮退運転用）
➢縮退運転用データ管理
➢未移行データ管理
➢縮退運転機能
➢未移行データに関する業務
➢システム連携機能
（クラウドと自庁内システム）
➢少量印刷
➢自庁内システム
➢マスタデータ管理
➢バックアップデータ管理
➢クラウド運用による業務
➢大量印刷、封入・封緘

どの程度のトラフィックが必要なのだろうか？

・Web系や情報系システムの集約でトラフィックが増大
・ネットワーク越しでもLANのように使える環境が必要

業務種別	システム種別	データ量	頻度	トラフィック
基幹業務	クライアントサーバアプリ	数KB程度（文字データ）	中程度（入力完了時）	少ない
	Webベースのシステム	10～100KB程度	多い（画面遷移時）	中程度
情報系	Web／グループウェア	10～100KB程度	多い（画面遷移時）	中程度
	電子メール	数KB～数MB	中程度	中～多い
	ファイルサーバ	数MB～数十MB	少ない	多い

従来からのシステム

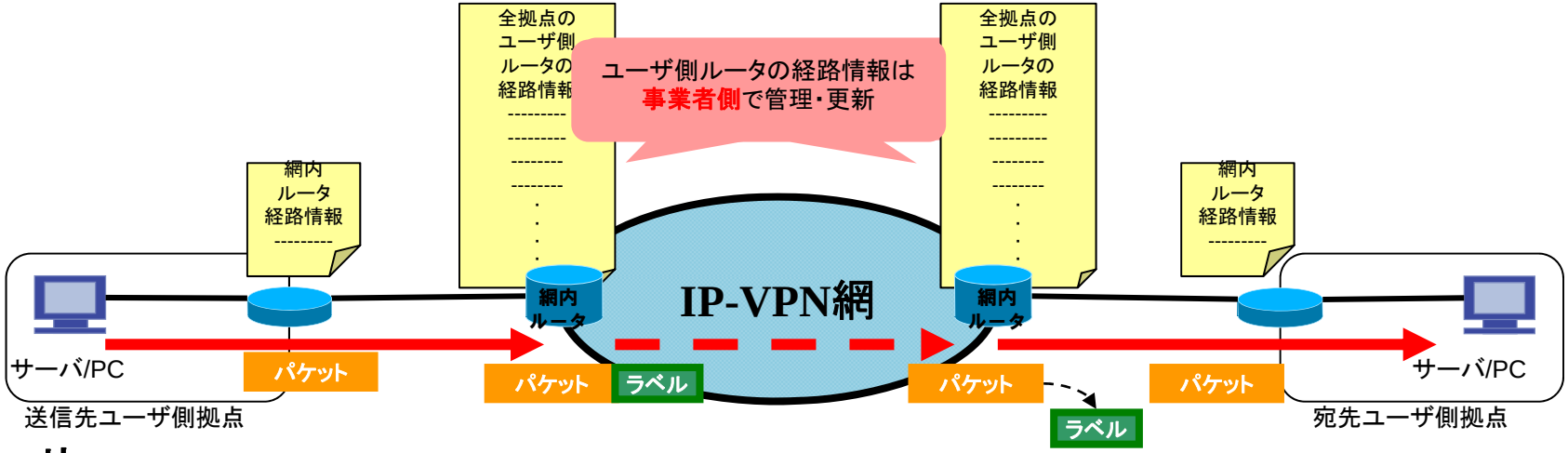
Webベースのアプリケーション増大に伴ない、
非定期かつ、変動の大きいトラフィックが増える傾向
今後は動画コンテンツ（教育コンテンツ）などで更に増大へ

【バックボーン毎の特徴】

バックボーン 種別	セキュリティ 技術	バックボーンの 帯域	SLA	特徴
IP-VPN	MPLS	帯域確保	有	**・経路設定・管理は通信事業者側のルータにより実施。** -アクセス回線からIP-VPN網に入る地点で受け取ったパケットに対し、網内ルータで、ルーティング（経路選択）情報として行き先を示す「ラベル」と言われる短い固定長の識別標識を付け、そのラベルによって経路を識別し、網の出口のルータまで転送する。ラベルはパケットが網の外に出る地点で外され、宛先ユーザ側ルータまで通常パケットとして送信される。 **・インターネット網とは完全分離された、事業者の閉域網として構成されている。** **・ラベルに係る優先制御機能により音声/データ/映像を1回線で提供する事が可能。**
広域イーサ	VLAN	帯域確保	有	**・経路設定・管理はユーザ側のルータにより実施。** -アクセス回線から広域イーサ網に入る地点で受け取ったイーサネットフレームに対し、網内スイッチで、行き先を示すVLANタグを付与し、そのVLANタグによって経路を識別し、網の出口のスイッチまで転送する。タグはフレームが網の外に出る地点で外され、宛先ユーザ側ルータ（もしくはスイッチ）まで送信される。 **・インターネット網とは完全分離された、事業者の閉域網として構成されている。** **・VLANタグに係る優先制御機能により音声/データ/映像を1回線で提供する事が可能。**
エントリーVPN	IPsec	ベストエフォート	無	**・経路設定・管理は通信事業者側で実施。** -送信元ユーザ側ルータにおいて、パケットをIPsecによりカプセル化（暗号化した上で行き先を記したヘッダを付与）し、事業者の閉域網であるエントリーVPN網の網内ルータを経由し、宛先ユーザ側ルータまでの通信を行う。カプセル化の際に付与したヘッダは宛先ユーザ側ルータにて外される。 **・インターネット網とは完全分離された、事業者の閉域網として構成されている。** **・優先制御機能は無い。**
インターネットVPN	IPsec	ベストエフォート	無	**・経路設定・管理はユーザ側で実施（事業者は関与しない）。** -送信元ユーザ側ルータにおいて、パケットをIPsecによりカプセル化（暗号化した上で行き先を記したヘッダを付与）し、インターネット網を経由し、宛先ユーザ側ルータまでの通信を行う。カプセル化の際に付与したヘッダは宛先ユーザ側ルータにて外される。 **・インターネット網を経由する為、ユーザ側ルータが第三者から攻撃を受ける可能性はあるが、通信内容を解読されることは無い。** **・優先制御機能は無い。**
インターネット	SSL	ベストエフォート	無	**・経路設定・管理はユーザ側で実施（事業者は関与しない）。** **・インターネット網を経由するが、SSLにより暗号化されている為、通信内容を解読されることは無い。** **・優先制御機能は無い。**

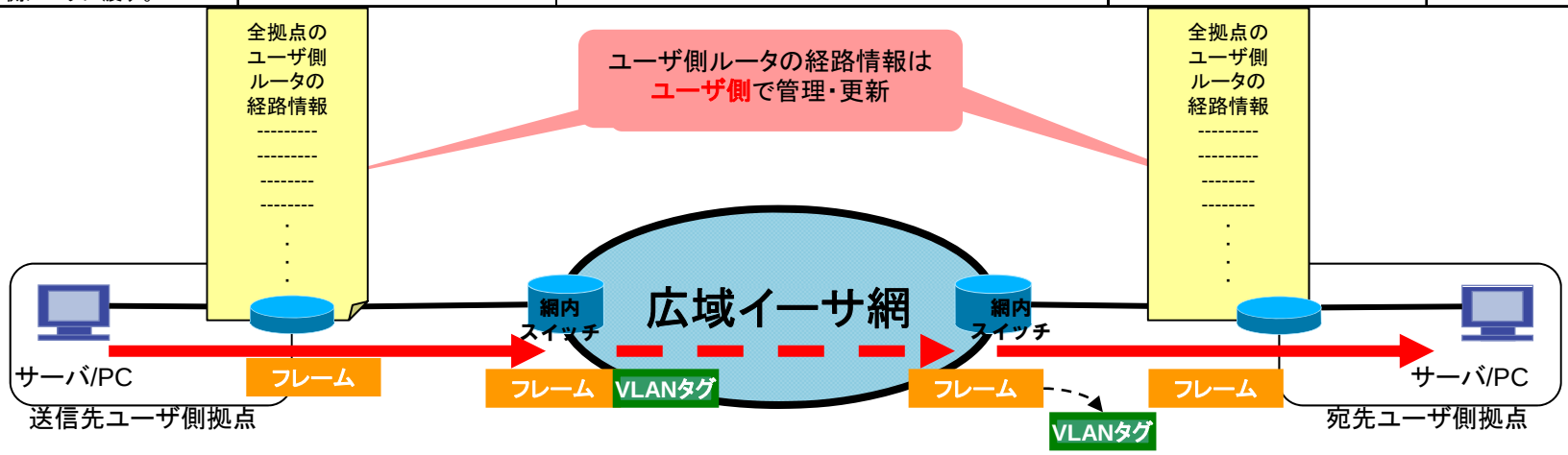
●IP-VPN

中継ポイント	送信元ユーザ側サーバ(PC)	送信元ユーザ側ルータ	事業者側ルータ(事業者の閉域網内)	宛先ユーザ側ルータ	宛先ユーザ側サーバ(PC)
所持情報	・自拠点ユーザ側ルータのIPアドレス	・事業者側ルータまでの経路情報 ・自拠点サーバ・PCのIPアドレス	・全拠点のユーザ側ルータまでの経路情報	・事業者側ルータまでの経路情報 ・自拠点サーバ・PCのIPアドレス	・自拠点ユーザ側ルータのIPアドレス
役割	・パケットに宛先情報(宛先ユーザ側サーバアドレス)を入れて、送信元ユーザ側ルータに渡す。	・経路情報を参照し、事業者側ルータに渡す。	・IP-VPN網の出入り口で「ラベル」を付与/除去 ・経路情報を参照し、宛先ユーザ側ルータに渡す。	宛先情報を参照し、宛先ユーザ側サーバ(PC)に渡す。	―



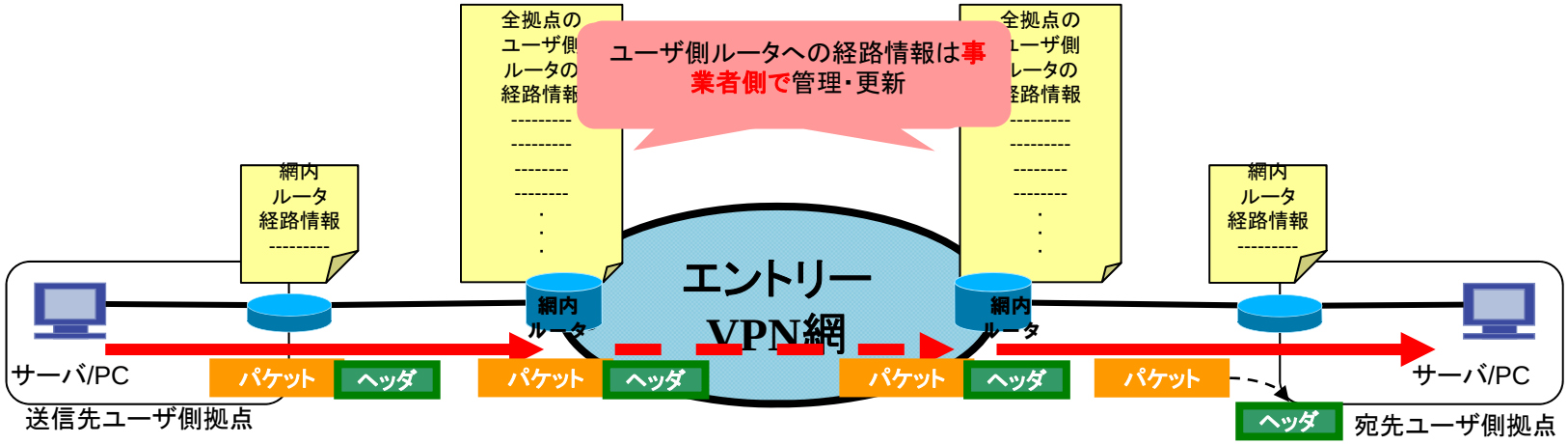
●広域イーサ

中継ポイント	送信元ユーザ側サーバ(PC)	送信元ユーザ側ルータ	事業者側スイッチ(事業者の閉域網内)	宛先ユーザ側ルータ	宛先ユーザ側サーバ(PC)
所持情報	・自拠点ユーザ側ルータのIPアドレス	・全拠点のユーザ側ルータまでの経路情報 ・事業者側スイッチのMACアドレス ・自拠点サーバ・PCのIPアドレス	・経路情報は持たない。	・全拠点のユーザ側ルータまでの経路情報 ・自拠点サーバ・PCのIPアドレス	・自拠点ユーザ側ルータのIPアドレス
役割	・フレームに宛先情報(宛先ユーザ側サーバアドレス)を入れて、送信元ユーザ側ルータに渡す。	・経路情報を参照し、事業者側ルータに渡す。	・広域イーサ網の出入り口で「VLANタグ」を付与/除去 ・VLAN情報を識別し、宛先ユーザ側ルータに渡す。	・宛先情報を参照し、宛先ユーザ側サーバ(PC)に渡す。	―



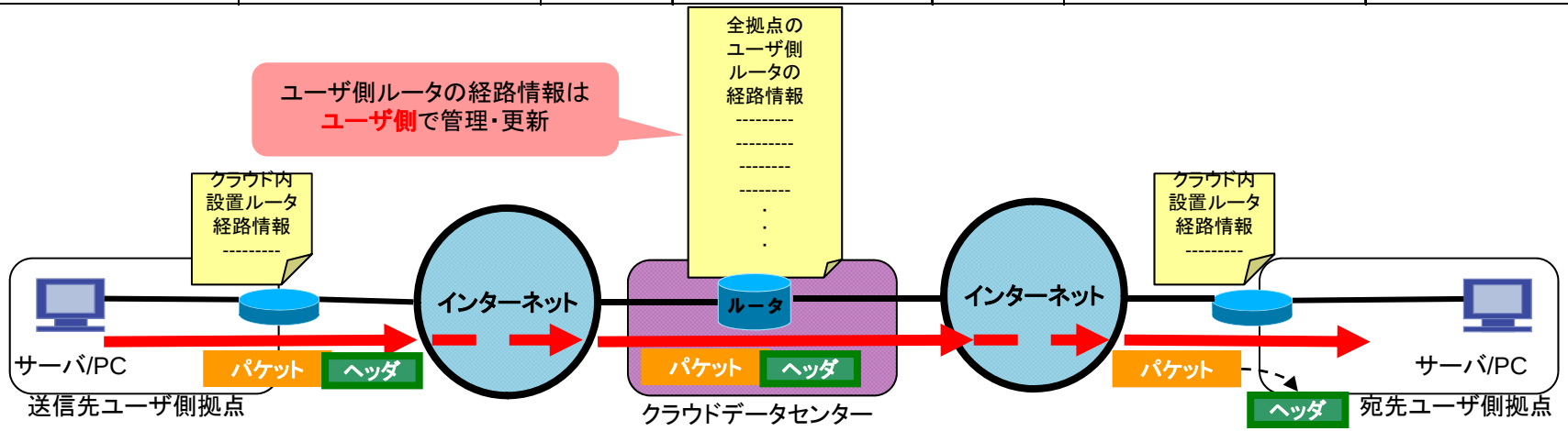
●エントリーVPN

中継ポイント	送信元ユーザ側サーバ(PC)	送信元ユーザ側ルータ	事業者側ルータ(事業者の閉域網内)	宛先ユーザ側ルータ	宛先ユーザ側サーバ(PC)
所持情報	・自拠点ユーザ側ルータのIPアドレス	・事業者側ルータまでの経路情報 ・自拠点サーバ・PCのIPアドレス	・全拠点のユーザ側ルータまでの経路情報	・事業者側ルータまでの経路情報 ・自拠点サーバ・PCのIPアドレス	・自拠点ユーザ側ルータのIPアドレス
役割	・パケットに宛先情報(宛先ユーザ側サーバアドレス)を入れて、送信元ユーザ側ルータに渡す。	・受け取ったパケットをIPsecでカプセル化。 ・経路情報を参照し、事業者側ルータに渡す。	・経路情報を参照し、宛先ユーザ側ルータに渡す。	・受け取ったパケットのIPsecのカプセル化を解除する。 ・宛先情報を参照し、宛先ユーザ側サーバ(PC)に渡す。	―



●インターネットVPN

中継ポイント	送信元ユーザ側サーバ(PC)	送信元ユーザ側ルータ	インターネット	クラウド内設置ルータ	インターネット	宛先ユーザ側ルータ	宛先ユーザ側サーバ(PC)
所持情報	・自拠点ユーザ側ルータのIPアドレス	・クラウド内設置ルータまでの経路情報 ・自拠点サーバ・PCのIPアドレス	―	・全拠点のユーザ側ルータまでの経路情報	―	・事業者側ルータまでの経路情報 ・自拠点サーバ・PCのIPアドレス	・自拠点ユーザ側ルータのIPアドレス
役割	・パケットに宛先情報(宛先ユーザ側サーバアドレス)を入れて、送信元ユーザ側ルータに渡す。	・受け取ったパケットをIPsecでカプセル化。 ・経路情報を参照し、クラウド内設置ルータに渡す。	―	・経路情報を参照し、宛先ユーザ側ルータに渡す。	―	・受け取ったパケットのIPsecを外す。 ・宛先情報を参照し、宛先ユーザ側サーバ(PC)に渡す。	―



【アクセス回線毎の保証帯域と特徴】

アクセス回線種別	保証帯域	特徴
イーサアクセス	0.5Mb/s～10G	・ユーザ側のインタフェースはイーサネット。 ・光ファイバー回線のみを利用。 ・宅内装置からバックボーンまで専用線方式またはVLAN技術によりセキュリティを担保。
STM[注1]アクセス	64kb/s ～1.5Mb/s	・ユーザ側のインタフェースはSTM。 ・64kb/s、128kb/sはメタル回線、それ以上の帯域は光ファイバー回線を利用。 ・宅内装置からバックボーンまで専用線方式でセキュリティを担保。
ATM[注2]アクセス	0.5Mb/s～135M	・ユーザ側のインタフェースはATM。 ・光ファイバー回線のみを利用。 ・宅内装置からバックボーンまでVP/VC[注3]技術によりセキュリティを担保。
一般ユーザ向けFTTH サービス	ベストエフォート	・ユーザ側のインタフェースはイーサネット。 ・光ファイバー回線のみを利用。 ・一般ユーザ向け回線であり、複数ユーザが共有している為、帯域は他ユーザの影響を受けやすい。 ・稼働率は上記の回線種別と比較すると低い。 ・ユーザ側でIPsecかSSLによりセキュリティを担保する（事業者は関与しない）。

一般的には安価なイーサアクセスを選択するが未提供エリアが存在するため、STMアクセスやATMアクセスを選択することがある

注1:時分割多重(TDM)方式の一種で、通信速度(転送レート)が固定化されたネットワークで使われる方式。伝統的な通信サービスである(アナログ)電話回線やISDN回線、DDX網などがSTMを利用している。

注2:1本の回線を複数の論理回線(チャネル)に分割して同時に通信を行なう多重化方式の一つ。
ATMで送受信されるデータは48バイトごとに分割され、5バイトのヘッダ情報を付加した53バイトの「ATMセル」という単位の固定長データで送受信される。

注3:ATM網でルーティング処理するための論理コネクション。1本のVP（仮想パス）の中に、1本以上のVC（仮想チャネル）が存在する。1つのエンド・ツー・エンドの通信に対応して1つのVCを設定し、これを識別するための識別子（VCI）を割り当てる。また、VCを束ねたものがVPであり、これに割り当てる識別子がVPIである。
ネットワークでチャネルをまとめて取り扱う場合（同じ経路を通過する場合など）の便宜のためにチャネルのほかにパスを定義しており、VPIとVCIはATMセルのヘッダ（セルの制御情報が書かれる部分）に書き込まれ，セルの転送の時に利用する。

【バックボーン毎の利用可能なアクセス回線種別】

アクセス回線 / バックボーン種別	イーサアクセス	STMアクセス	ATMアクセス	一般ユーザ向けFTTH サービス
IP-VPN	○	○	○	○
広域イーサ	○	○	○	×
エントリーVPN	×	×	×	○
インターネットVPN	×	×	×	○

クラウドモデルで想定される業務アプリケーション

行 政 事 務

基幹系業務	・住民基本台帳、印鑑登録、外国人登録、選挙/投票 ・市民税、法人税、固定資産税、軽自動車税、たばこ税、収滞納事務、宛名 ・国民健康保険、後期高齢者医療、年金、介護 ・障害者福祉、児童手当、生活保護、就学、乳幼児医療、ひとり親医療、健康管理
内部系事務	・電子申請、電子調達、財務会計、庶務事務、文書管理、人事/給与 ・IP電話、電子メール ・ホームページ公開、情報検索

医　　療

双方向映像	・遠隔診療支援（遠隔画像診断、遠隔病理診断、遠隔医療指導） ・遠隔健康管理（健康相談、健康指導） ・災害時のトリアージ
情報共有	・診断記録、検査記録、処方記録

教　　育

動画像配信	・デジタルコンテンツ（教材）、デジタルアーカイブ（質疑応答） ・e-Learning（遠隔授業、遠隔交流学習、試験、課題提出）
登録・管理	・入学登録、学生認証、履修登録、授業評価、学生間コミュニケーション

クラウドモデルにおけるネットワーク機能要件

項　　目	課　　題	対応方針
データ集中処理と大容量化への対応	シンクライアント方式によるレスポンスの低下 データバックアップ等のバーストトラフィックによるNWの圧迫	業務トランザクションは確保した上でバーストに対応したネットワークを整備
データセンター間通信の安定	ロケーションフリーで分散処理するサーバの故障切替え切り離し時の業務中断	仮想化と分散処理を実現するグリッドサーバに対応した多重化
セキュリティ統制	異なるポリシーで運用される業務間や団体間でプライバシー確保に懸念	各団体・各業務ごとのポリシーに対応するネットワーク制御機能の実装