資料3－5

# クラウドサービスに求められるネットワーク要件と対応する技術動向

平成22年1月21日

NTTコミュニケーションズ株式会社
第二法人営業本部 u-Japan推進部
馬場　覚志

# アジェンダ

1. 情報システムの変遷とネットワークが果たしてきた役割と課題

2. クラウドサービスに求められるネットワークの要件

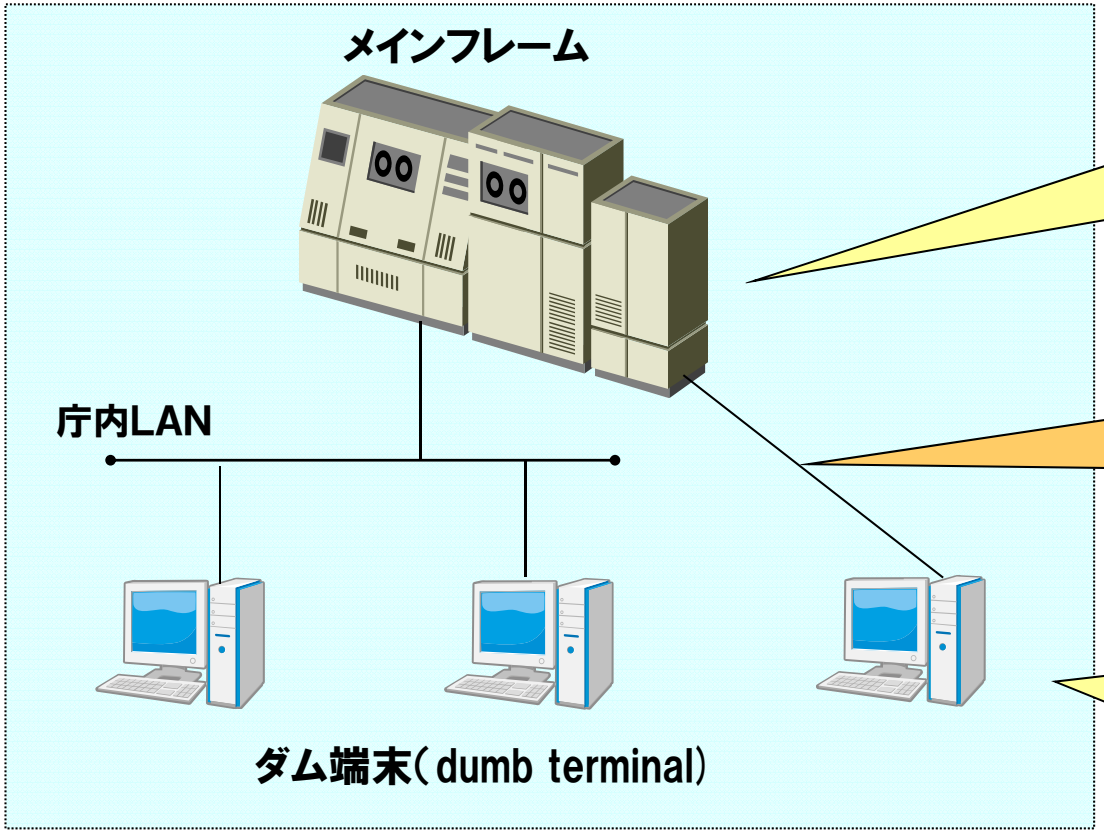
3. 新たに求められるネットワーク要件に対応した技術動向

# 1. 情報システムの変遷とネットワークが果たしてきた役割と課題

# 1-1. メインフレーム時代

## 集中モデル

・アプリケーションもデータも全てメインフレーム（大型汎用コンピュータ）に集中させて処理
・端末は入力と出力表示機能のみ




データの処理や保存は、すべてメインフレーム（大型汎用コンピュータ）で集中処理

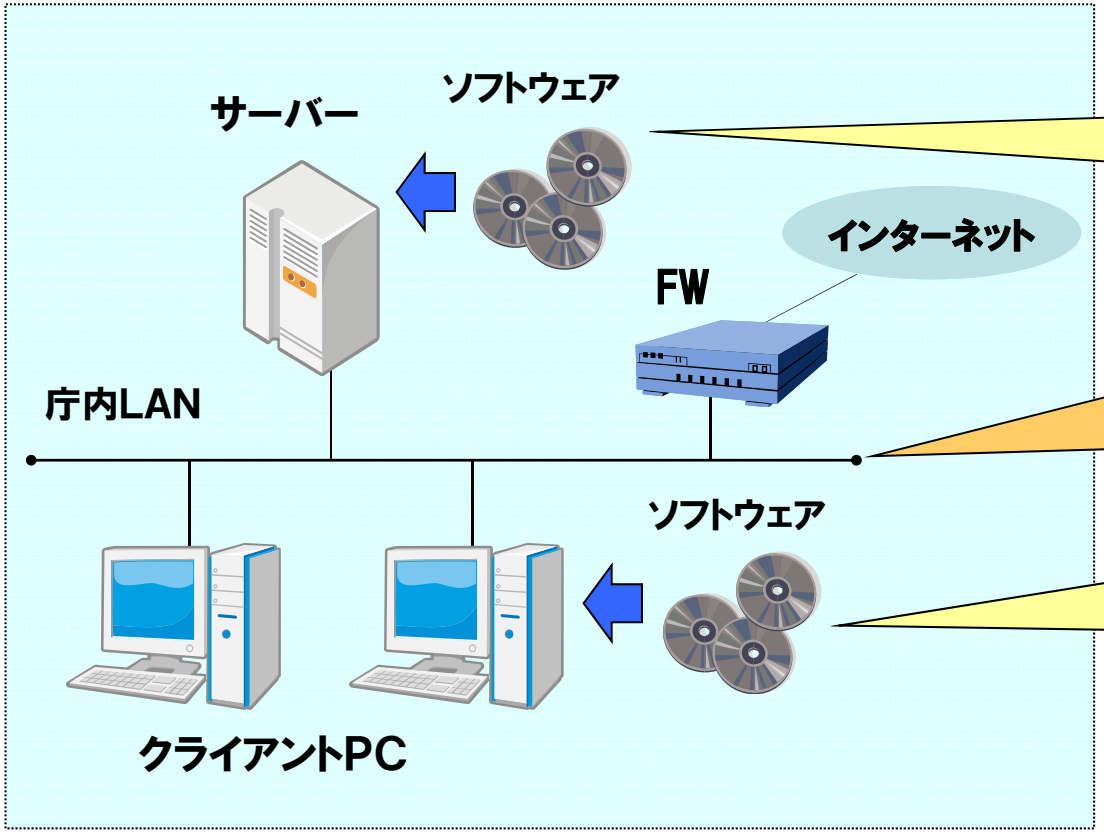
ネットワークは専用線で低遅延が求められたが狭帯域で十分

ダム端末は、処理や記憶機能はなく、入力と表示機能のみ

# 1-2. クライアントサーバ時代

## 分散モデル

・イントラネット上のクライアント端末にも処理機能を実装
・クライアントへ多数のソフトをインストール




ダウンサイジングによりコスト低減化

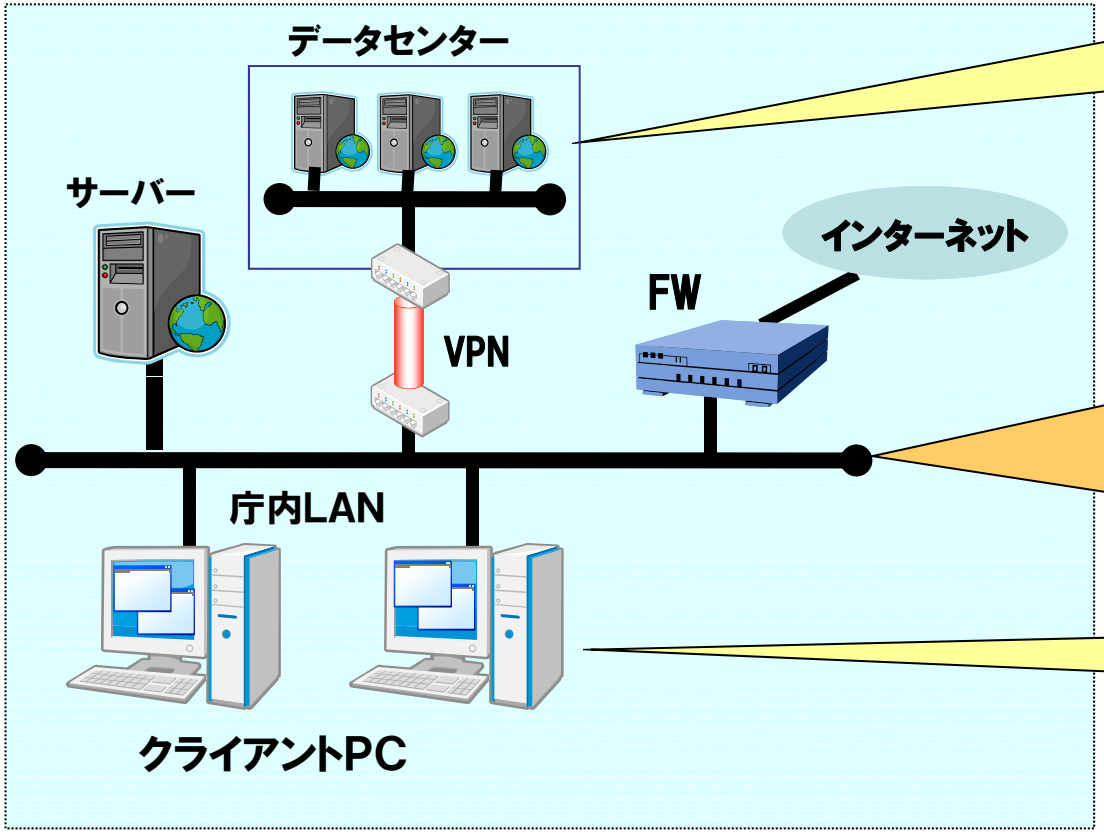
ネットワークはIPとなり高速化、外部ネットワークへの接続が増え、セキュリティ対策が重要に

クライアントへ多数のソフトをインストールし管理コストが増大

# 1-3. Web時代

## オープン型の集中モデル

・ウェブブラウザを利用したアプリケーションが主流に




サーバーをデータセンターへ移し、アウトソーシングするケースが増加

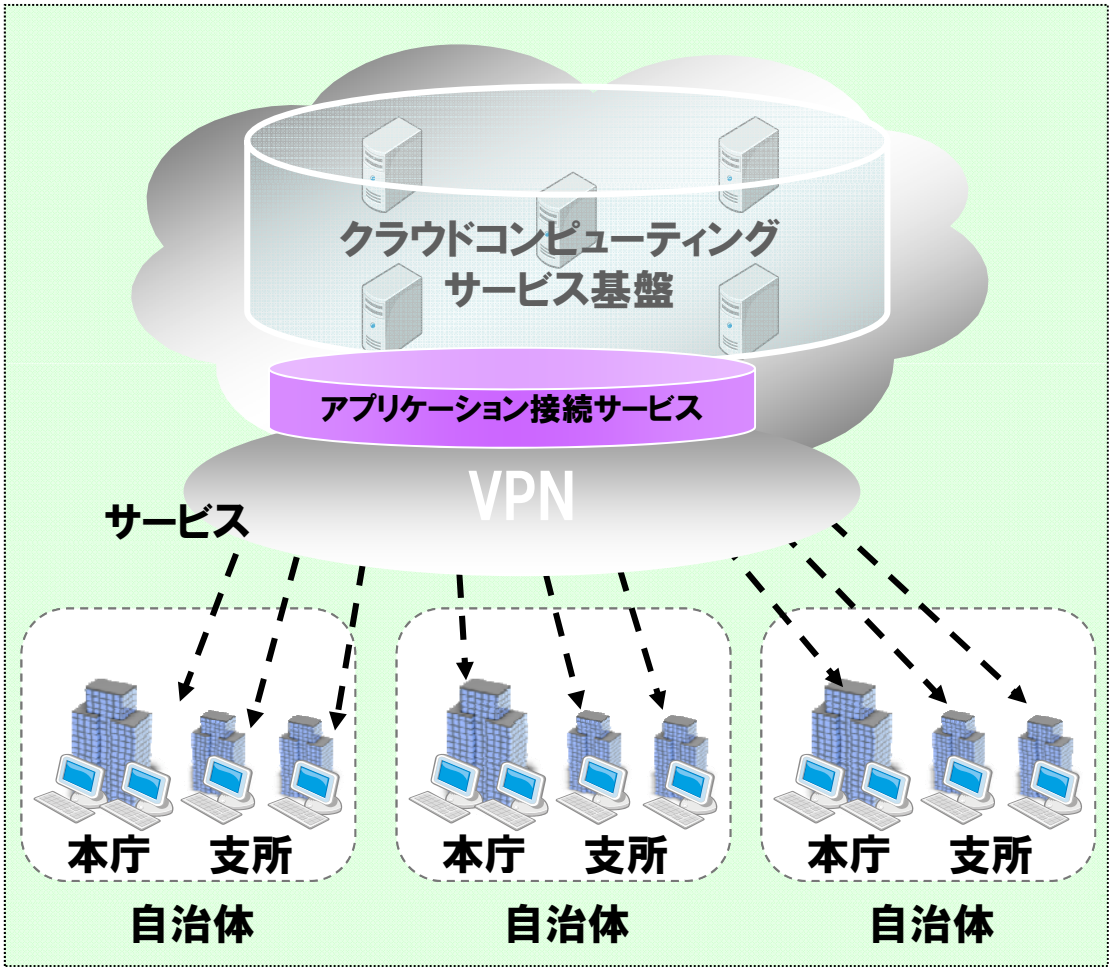
ネットワークを介したアプリケーション利用の拡大により、更なる高速化、ウィルスや情報漏洩などの脅威が増し、セキュリティ対策がますます重要に

WANはVPNでセキュリティ対策

クライアントはブラウザベースが主流へ

# 1-4.「クラウドコンピューティング」の登場

・光ブロードバンドの普及と分散処理技術や仮想化技術の発展により、ネットワークを介した大容量の集中処理が進展




**利用者は、サーバを所有せず、利用するのみ**

・ネットワーク上にあるソフトウェアを「サービス」として利用

・コンピュータはブラウザさえ操作できればよく、高性能なCPUやソフトウェアを必要としない

・ソフトウェアはサービス提供者が常に最新バージョンを提供

# 2. クラウドサービスに求められるネットワークの要件

# 2-1. 想定される主な課題

## ①安定性(可用性)の確保

ex.) システムダウンによる業務停止の防止。

## ②信頼性(完全性)の確保

ex.) システムが提供する情報の誤りによる業務トラブルの発生の防止。

## ③安全性(情報セキュリティ)の確保

ex.) ハッカーによる不正アクセスなどの防止。

## ④効率性(低コスト)の確保

ex.) システム保守のための莫大なコストの削減。

## ⑤柔軟性の確保

ex.) 最新テクノロジーへの対応、制度変更に伴うアプリケーション改修への対応。

# 2-2. 各システム運用形態における課題整理

## 各システム運用形態の特色

| | メインフレーム | クライアントサーバ | クラウド |
|---|---|---|---|
| 安定性 | ○ | △ | ○<br>サービス停止時の波及大 |
| 信頼性 | ○ | △ | ○<br>アプリケーション障害の波及大 |
| 安全性 | ○ | △ | ○<br>セキュリティ事故発生時の波及大 |
| 効率性 | × | △ | ○ |
| 柔軟性 | × | △ | ○ |

# 2-3. クラウドサービスにおける課題

**安定性の確保**

- ✓ 仮想化技術
- ✓ 冗長化
- ✓ バックアップ
- ✓ トラヒック変動への対策

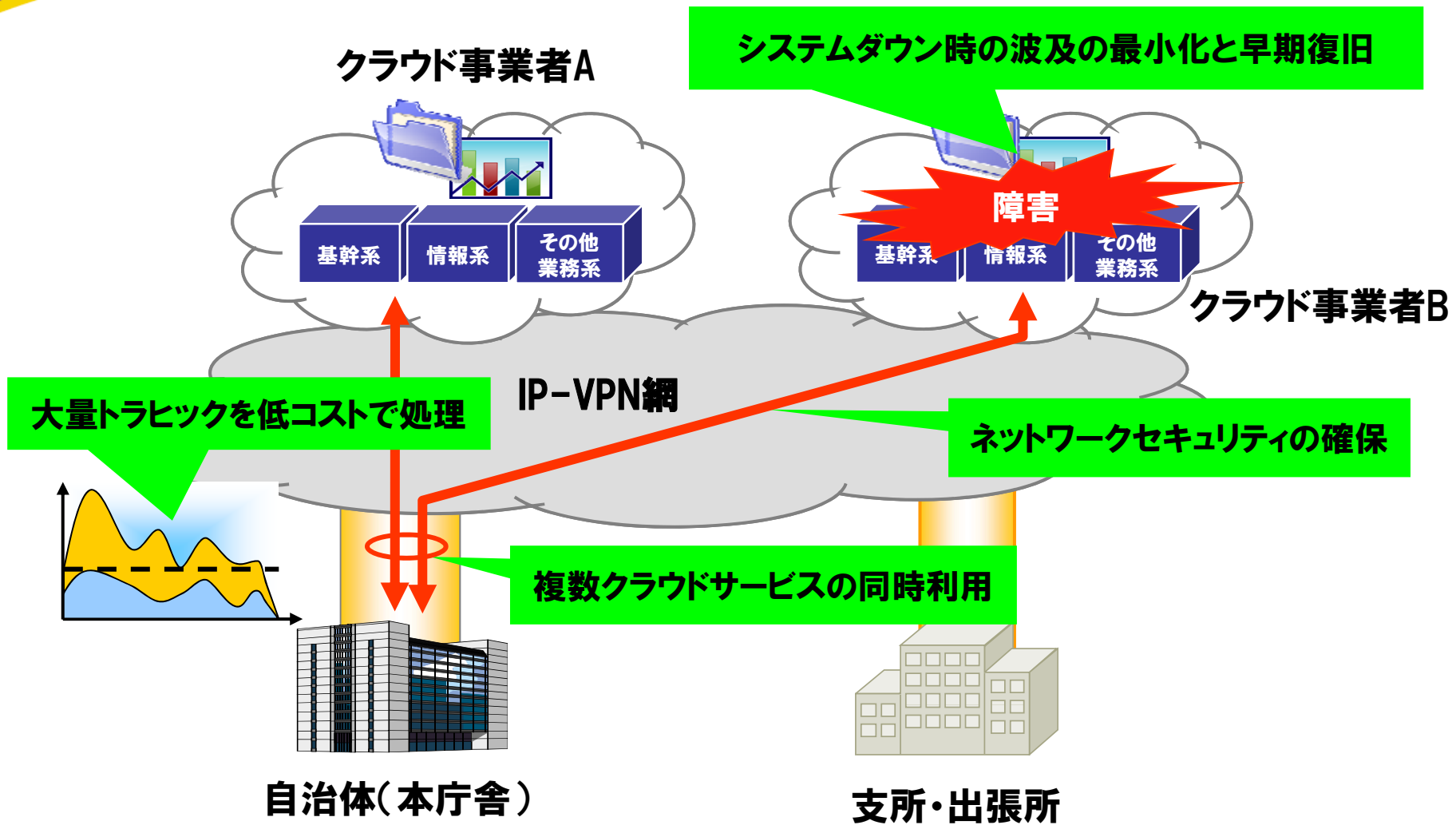
**信頼性の確保**

- ✓ データの複数バックアップ
- ✓ 質の高いアプリケーションの共同利用

**安全性の確保**

- ✓ 閉域網（ネットワーク）の利用
- ✓ 業務特性に応じた認証方式の適用
- ✓ ログ管理

# 2-4. クラウドサービスに求められるネットワークの条件



# 3. 新たに求められるネットワーク要件に対応した技術動向

# 3. ネットワーク要件毎の対応方策

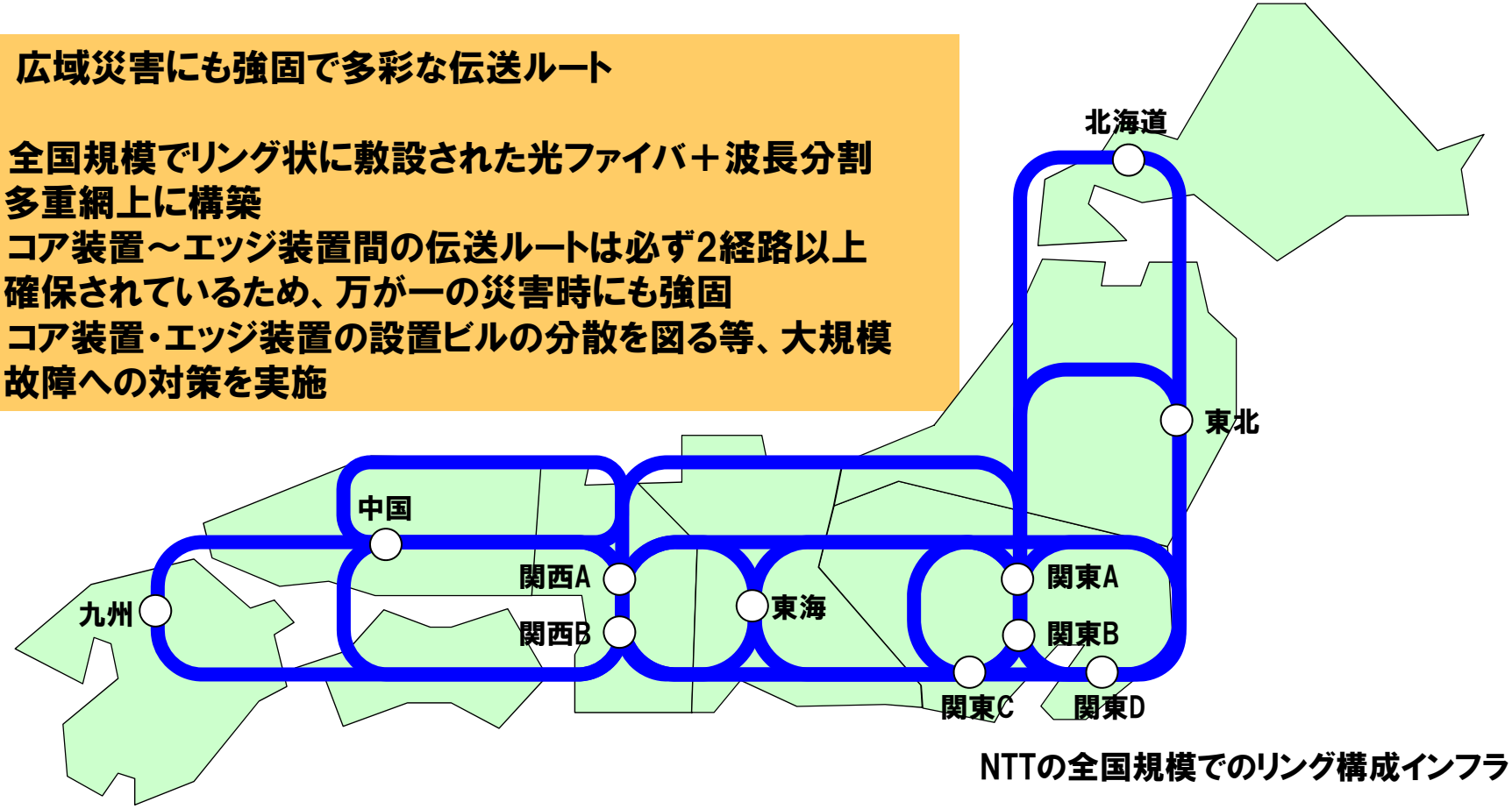
| クラウドを有効に機能させるための要件 | 対応方策 |
| --- | --- |
| 大容量トラヒックへの対応 | • Arcstar IP-VPN<br>• バーストイーサアクセス |
| ネットワークセキュリティの確保 | • Arcstar IP-VPN<br>• eVLAN<br>• セキュアコネクティビティ 多要素認証 |
| システムダウンへ備えた対策 | • Bizホスティング<br>• Bizストレージ<br>• Group-Ether |
| 複数クラウドサービス利用時の安全性と利便性の確保に向けた対策 | • セキュアコネクティビティ SSO機能（シングルサインオン） |

# 3-1. 大容量トラヒックへの対応/ネットワークセキュリティの確保

## Arcstar IP－VPN / eVLAN

■ 広域災害にも強固で多彩な伝送ルート

- ✓ 全国規模でリング状に敷設された光ファイバ＋波長分割多重網上に構築
- ✓ コア装置～エッジ装置間の伝送ルートは必ず2経路以上確保されているため、万が一の災害時にも強固
- ✓ コア装置・エッジ装置の設置ビルの分散を図る等、大規模故障への対策を実施



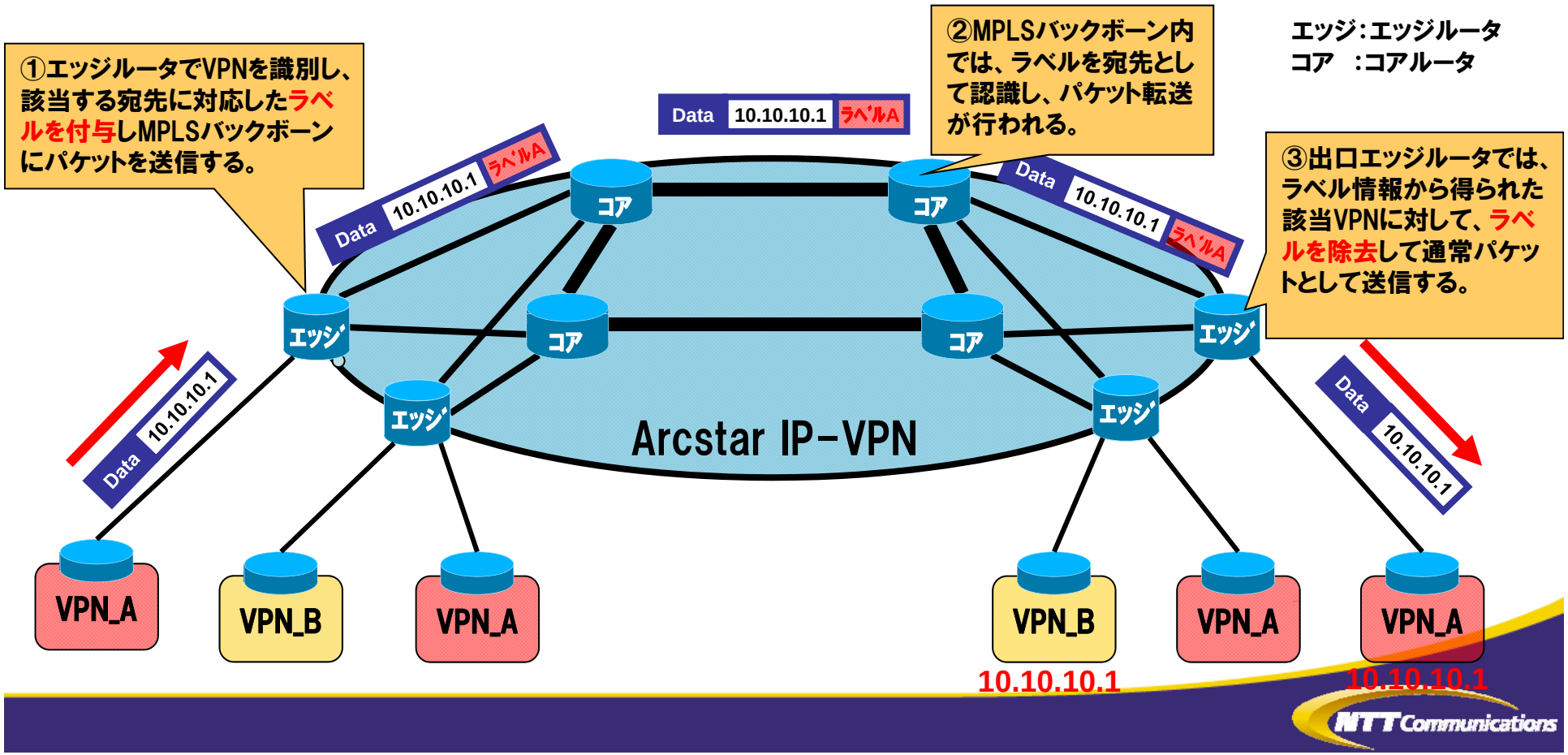

NTTの全国規模でのリング構成インフラ

リング状に構成された豊富な設備で中継伝送路区間の二重化と自動切替を実現

# 3-1. 大容量トラヒックへの対応/ネットワークセキュリティの確保

## Arcstar IP-VPN

基幹技術にMPLS (Multi Protocol Label Switching) を採用し、MPLSのラベルよりVPNを実現する技術(MPLS-VPN)により、高速かつ高い安全性の高いサービスを提供

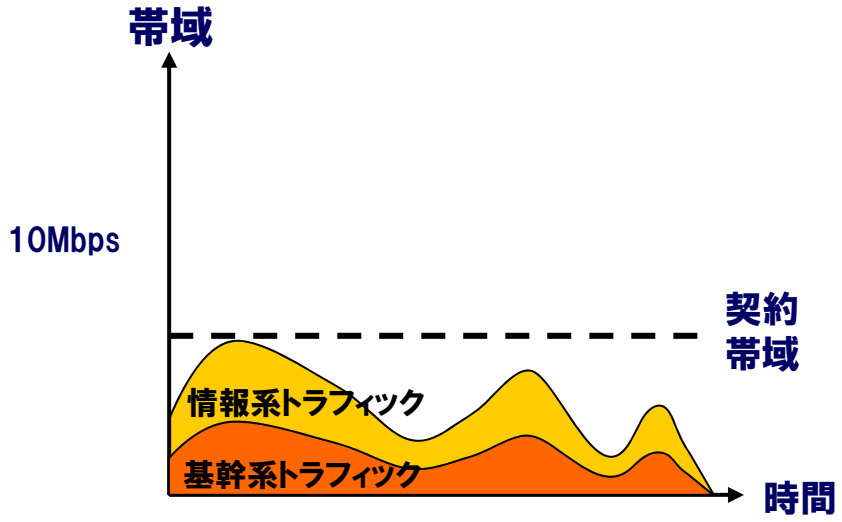


# 3-1. 大容量トラヒックへの対応/ネットワークセキュリティの確保

## バーストイーサアクセス

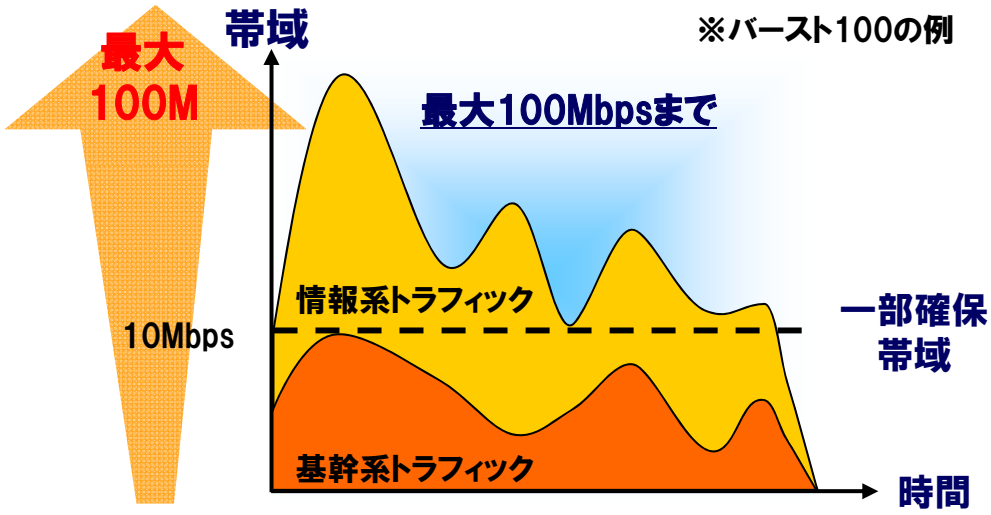
一部(10%)の帯域を確保しつつ、10Mbpsもしくは100Mbpsの
物理インタフェース速度までバースト可能なイーサアクセス回線

### ギャランティ型アクセス




- ✓ クラウドの進展で高速化が必須
  増速には高価な高速回線の準備が必要
- ✓ フレッツ等の低廉アクセスでは品質・運用面でビジネスニーズに適さない

### バーストイーサアクセス




- ✓ 一部確保部分で基幹データを確実に通信、
  クラウドからの大量データはバースト利用
- ✓ リーズナブルな料金
- ✓ ギャランティ型同様、高い運用品質

# 3-2. ネットワークセキュリティの確保

## セキュアコネクティビティ　多要素認証

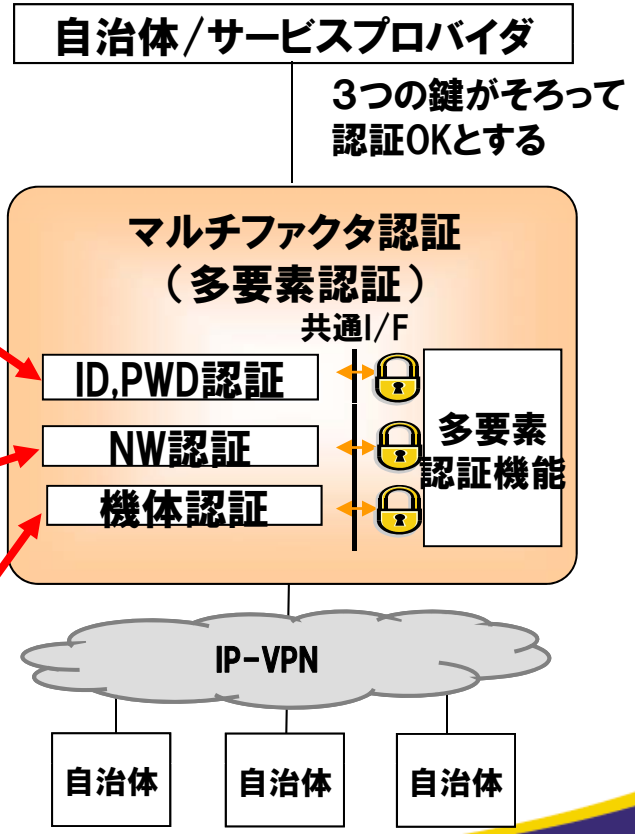
**さまざまな認証要素を組み合わせて、お客様ニーズに合わせた認証強度を実現する認証方式**

ex）端末認証＋NW認証＋アプリケーション認証

【カテゴライズ例】

| | レベル3 | レベル2 | レベル1 |
|---|---|---|---|
| アプリケーション | ・静脈<br>・虹彩<br>・指紋 | ・音声<br>・筆跡 | ・ID/PW<br>・リマインダクイズ（質問と回答） |
| NW | ・回線番号（NGN）<br>・回線番号（フレッツ）<br>・発番号 | ・OCN上の発IPアドレス | ・インターネット上の発IPアドレス |
| 端末 | ・ハードウェア証明書/鍵（ICカード、TPMなど） | ・ソフトウェア証明書/鍵（PKI）<br>・ワンタイムパスワード | ・機体番号<br>・Cookie |

松　　竹（組合せ）　　梅



# 3-3. システムダウンへ備えた対策

## Bizホスティング / Bizストレージ

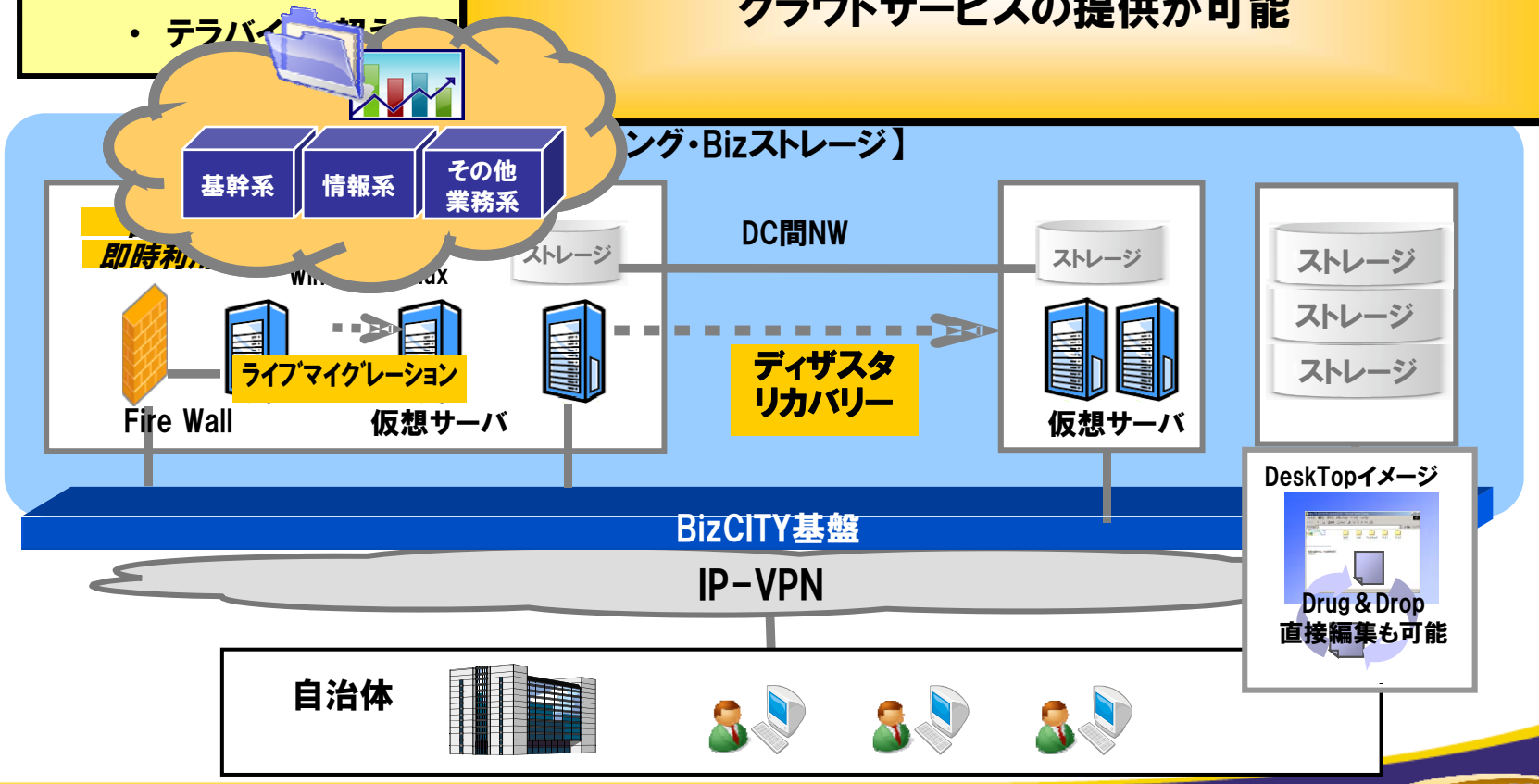
**Bizホスティング**

- 必要な時、必要なだけ
- サービスは仮想サー

**Bizストレージ**

- ファイルサーバ機能を
- テラバイ

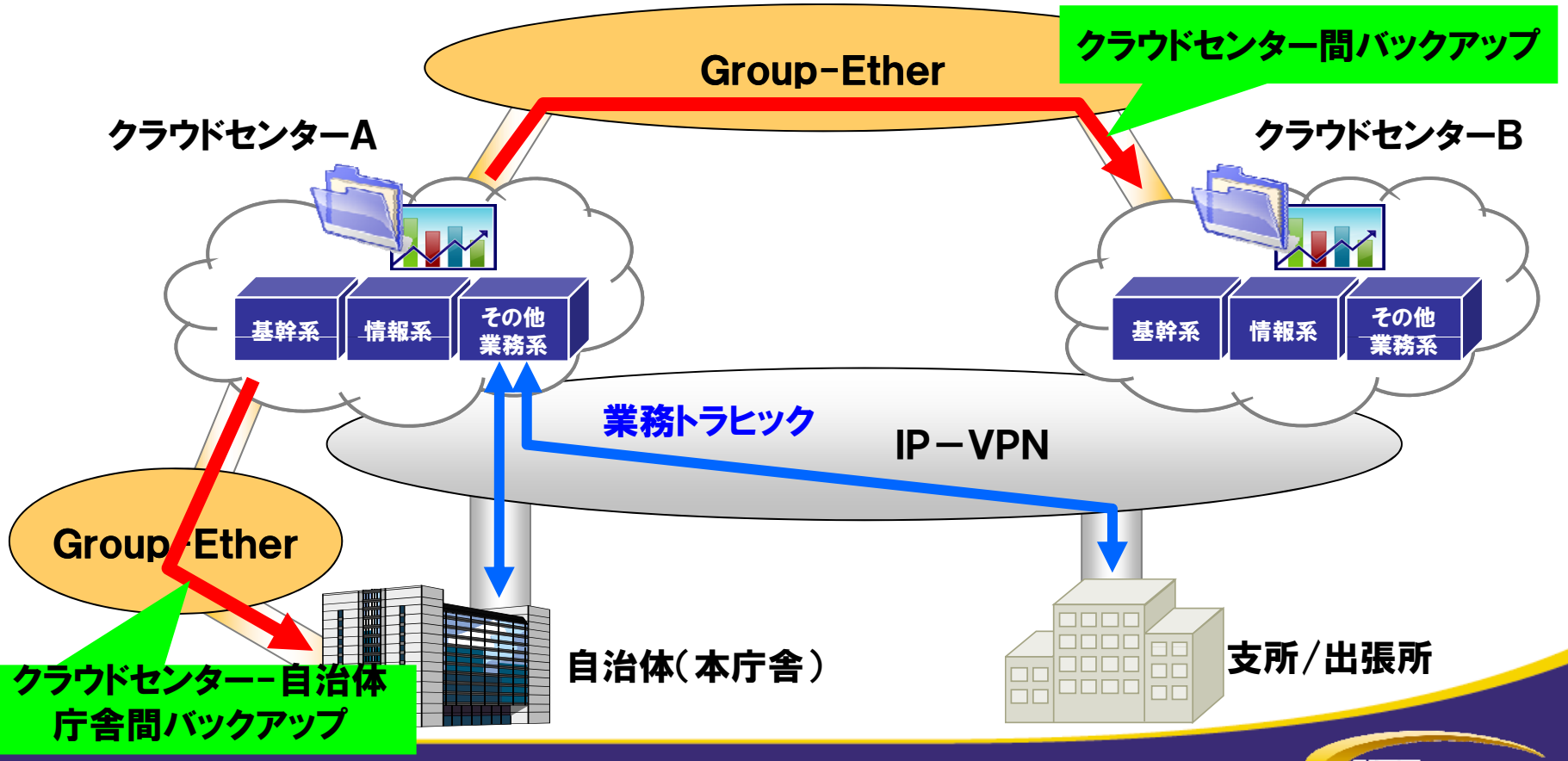
**Bizホスティング上にアプリケーションを構築するだけで**
**クラウドサービスの提供が可能**



# 3-3. システムダウンへ備えた対策

## Group-Ether（エントリー型広域イーサネット）

**ブロードバンド回線を利用した低廉なベストエフォートタイプのエントリー型広域イーサネットサービス**
**⇒基幹系ネットワークのバックアップ対策（バックアップ回線用メニュー）**

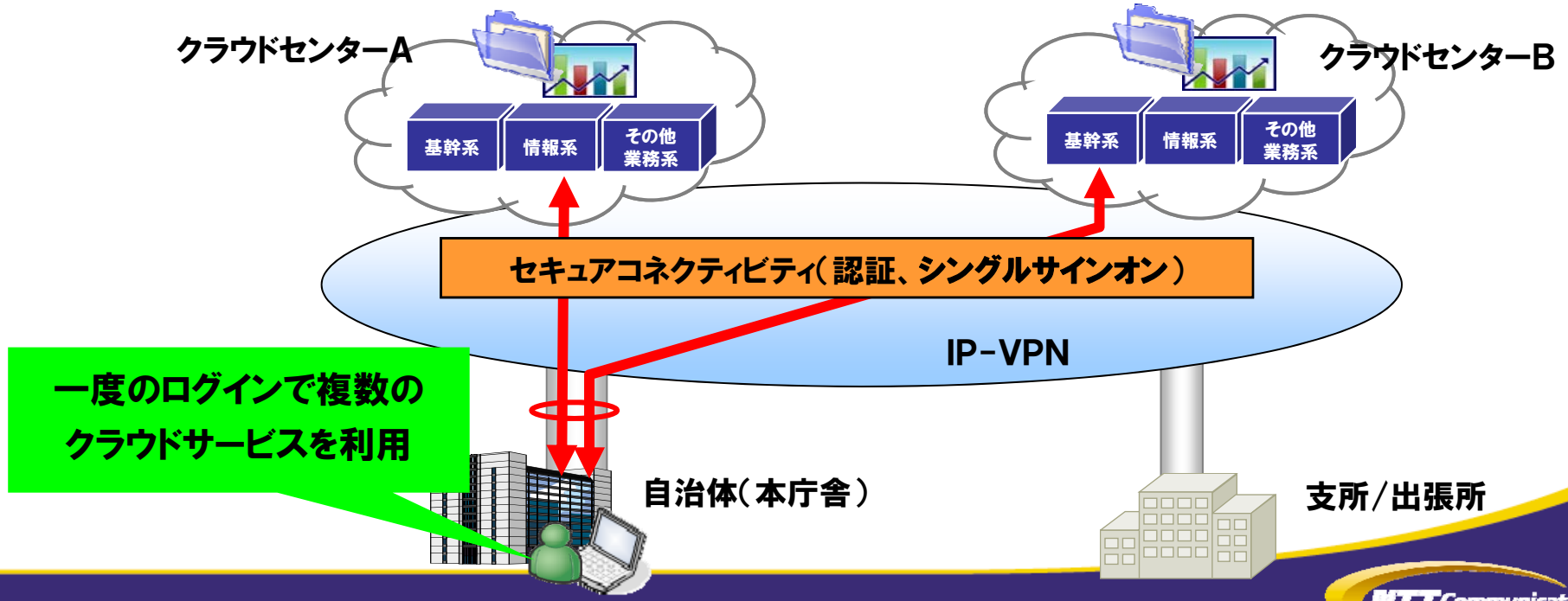


# 3-4. 複数クラウドサービス利用時の安全性と利便性の確保に向けた対策

## セキュアコネクティビティ　SSO機能

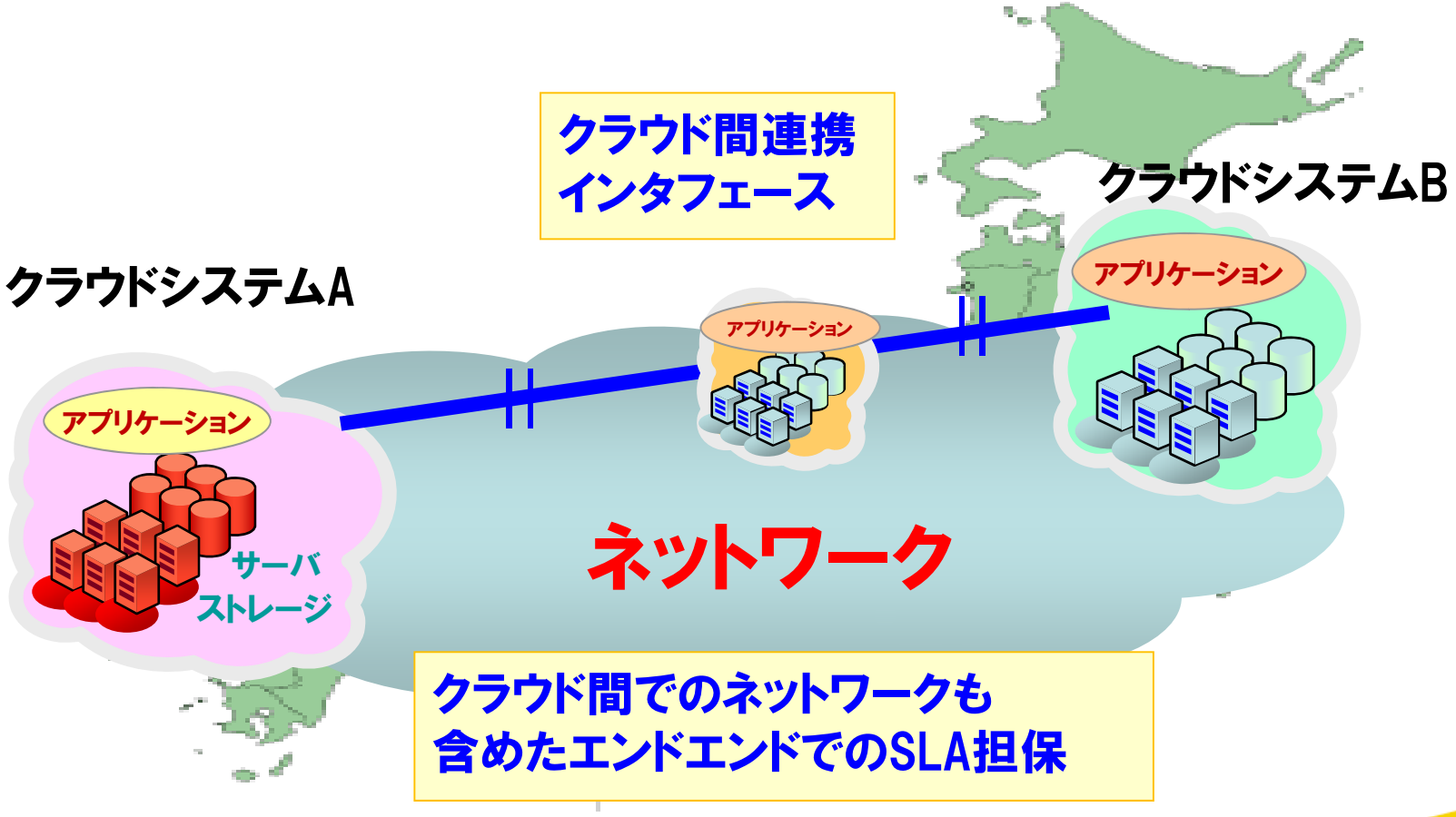
**シングルサインオン(SSO)機能として3方式を提供**

| 認証連携種別 | 機能概要 |
|---|---|
| SAMLタイプ | 標準化団体OASISによって策定された、IDやパスワード等の認証情報を安全に交換するためのXML仕様 |
| エージェントタイプ | システムにエージェントを導入することによりSSOを実現 |
| リバースプロキシタイプ | Webサーバのフロントエンドでリバースプロキシがアクセスを受け付け、Webサーバへリクエストを中継 |



# （参考）クラウド間連携に向けた研究開発

- クラウド間連携のインタフェースの確立
- クラウド間でのネットワークも含めたエンドエンドでのSLA担保



ご清聴ありがとうございました。