FreeBitのIPv6への取り組み
仮想化によるIPv6の利用と実例

FreeBit R&D
H.Oizumi

IPv6への取り組み

インターネットインフラへのニーズ
の把握と早期実現を計画 (2002年)

インターネットからの到達性確保
(インターネットからの固体認識)

膨大な個体数への対応

セキュリティの確保

トンネリング技術を利用した、
IPv6 over IPv4テクノロジーの開発に着手

IPv6への取り組み

2002年～ Feel6 テクノロジー

・IPv6 over IPv4トンネルを採用。
・DTCP (Dynamic Tunnel Configuration Protocol)をメインプロトコルに選定。
・数千～数万の規模に対応可能なサーバシステムの構築。
・SONY、日立、YAMAHA、日本のISP51社、IPv6推進協議会、
WIDEプロジェクトと「Feel6 Farm」実証実験を開催。
(SONYのIPv6対応HDDレコーダー「Cocoon」の開発、実験に参加)
・共立メンテナンスによる27000台のIP Centrex採用。

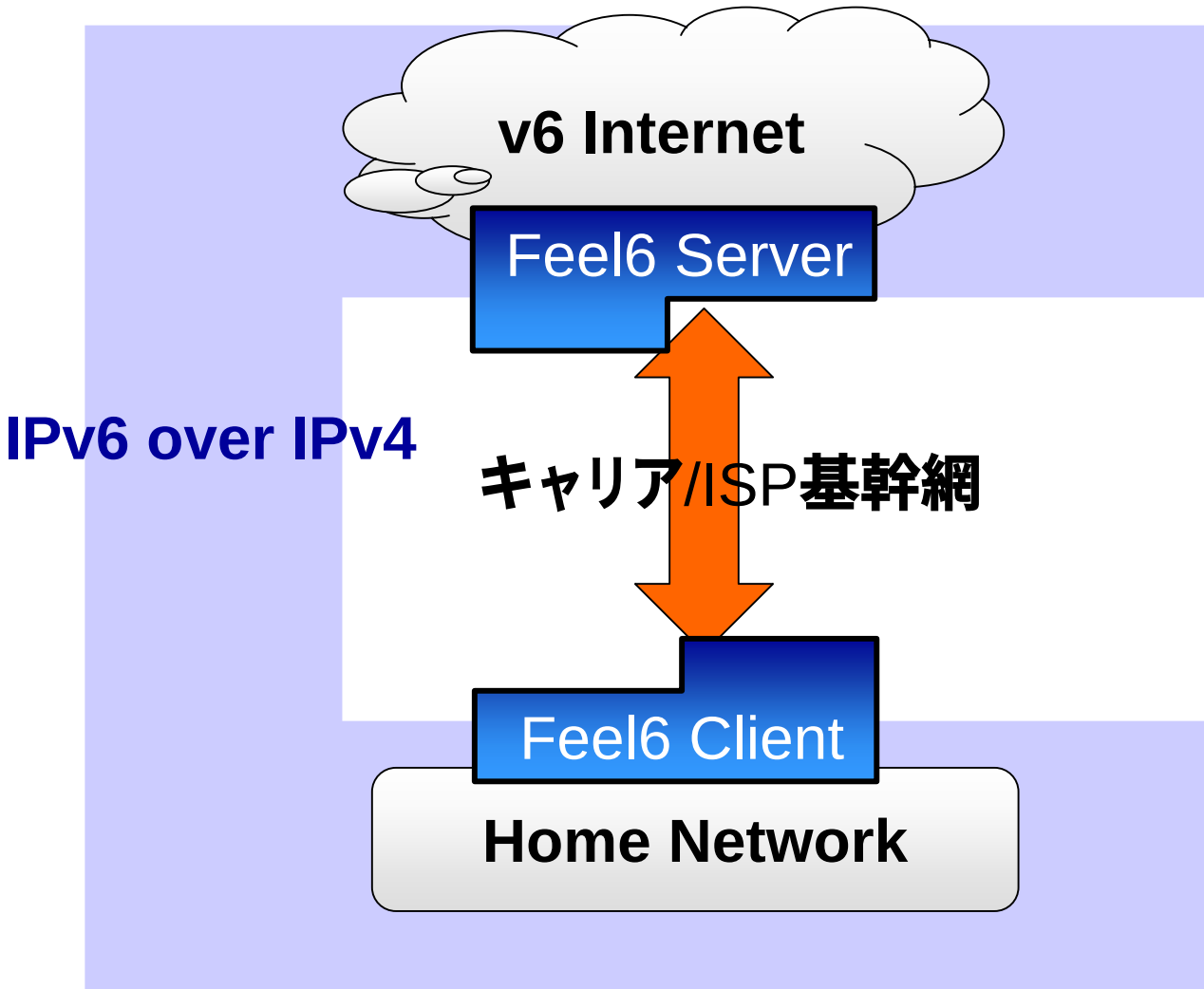
2004年～ Emotion Link テクノロジー

・Feel6 の問題点を改善、IPv4グローバルアドレスなしでトンネルを作成可能。
(L2,L3の2つのバージョン)
・Emotion Link Active Node ライブラリで、TCP/IPスタック自体を内包。
OSのTCP/IPスタック(ex.winsock)ではなく、専用ライブラリをリンクして
アプリケーションを作成することで、アプリケーション自体がIPアドレスを
持つノードとしてネットワーク上に存在できるようになる。
・オムロンのセキュリティ機器、OBCのUSBによるVPN、楽天メッセンジャーにて
広範囲に採用。

IPv6への取り組み

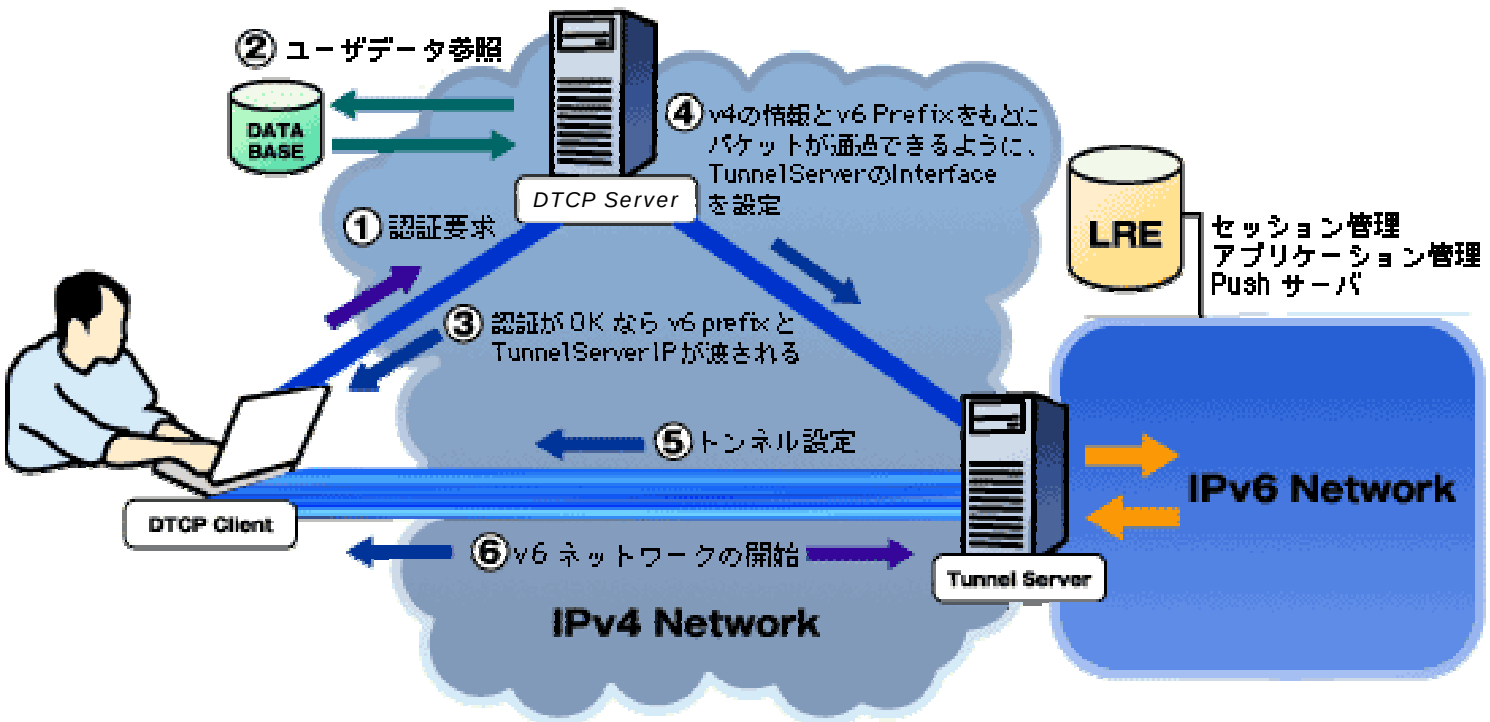
2002年～
Fee16テクノロジー

IPv6への取り組み (Feel6 Technologyとは)



IPv6への取り組み (Feel6 Technologyとは)

トンネルブローカモデルを採用。
動的にトンネルを制御するためのプロトコルはDTCPを採用。



DTCPについて(1)

トンネル構成時における問題

IPv6 over IPv4 トンネルは、トンネルの終端のIPv4アドレスを指定してトンネルを構築する。

PPPoE等でISPからIPをもらっている場合、IPアドレスはダイナミックに割り当てられ、アクセスの度に変更されてしまう。

この問題に対処する方法として

Trumpet社が1999年ごろ提唱したDTCP(Dynamic Tunnel Confituration Protocol)。
Freenet6が提唱したTSP(Tunnel Setup Protocol)
などが存在。

DTCPについて(2)

DTCPはv4/TCPを利用したプロトコルで、クライアント側のIPv4アドレスが動的に変化するような接続環境においてもサーバ側がこれに追随し、トンネルを適切に設定可能。
また、v4/TCPのコネクション自体をKeep-Aliveセッションとすることで、このコネクションが生きている間はトンネルが維持されるというシンプルな管理を行っている。

非常にシンプルなプロトコル仕様

■APOPに準拠した、challenge and response方式による認証。

■Perl等のスクリプト言語でも、容易に記述可能。
→Net::POP3 ,Digest::MD5

■ルーターメーカに実装をお願いしやすい(かった)。
→YamahaさんのIAD(RTV-700)　BBR(RTA-55i)

■すでにBSD系の実装(server/client)などがあって、利用者が存在した。

DTCPについて(3)

telnetでつないでみる

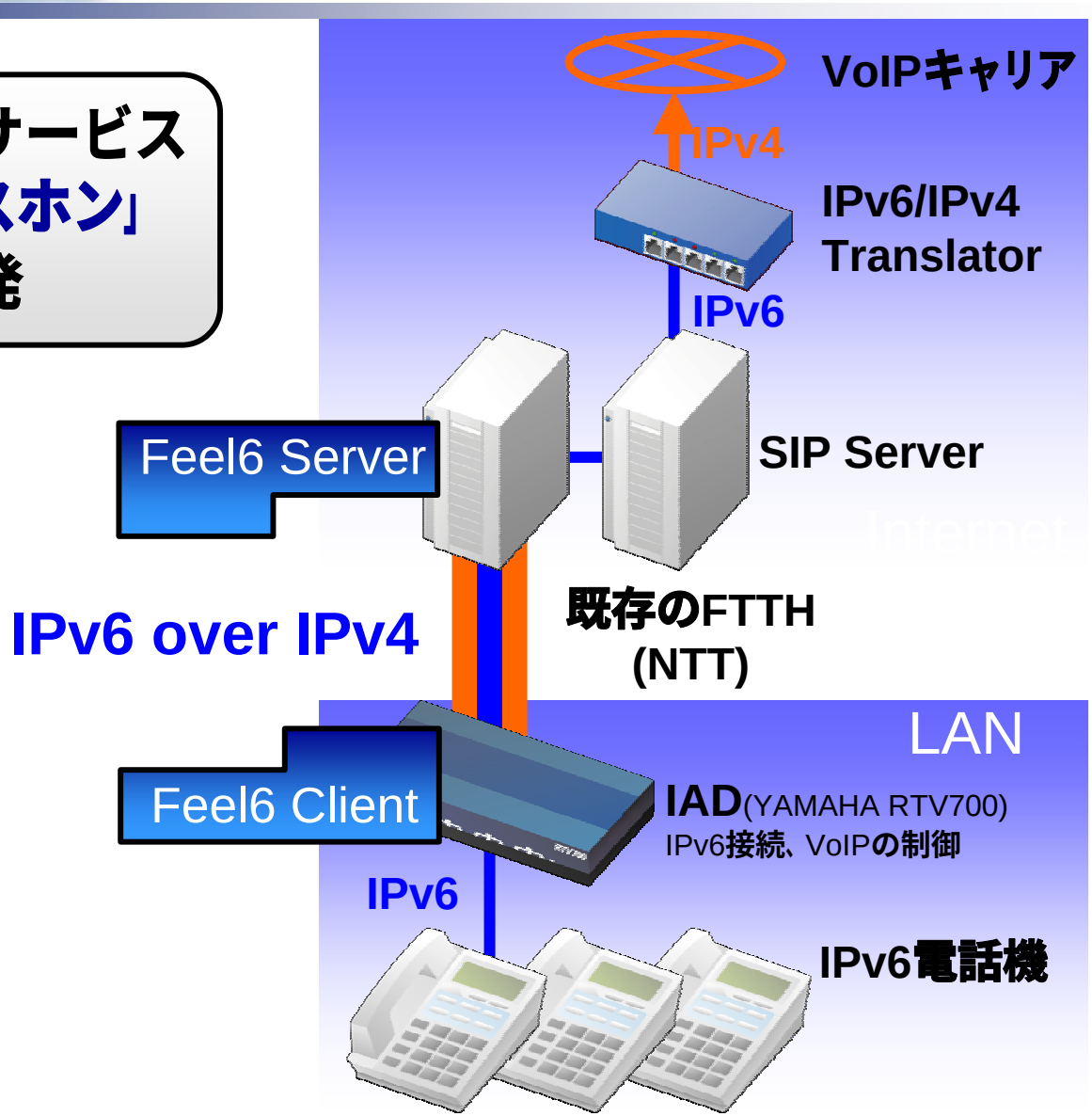
```
air:/>telnet dtcp.feel6.jp 20200
Trying 43.244.255.120...
Connected to dtcp.Feel6.jp.
Escape character is '^]'.
+OK e8be78a04561197f1e0c5b0f321e7026 FBDC TunnelBroker (version 0.2) Ready.
tunnel testuser 8f427154dc34a055275dcf47bca12b62 network
+OK 210.143.144.163 43.244.255.37 2001:03e0:01fe::/48
..
ping
+OK pong
..
quit
+OK tunnel server quitting
```

hashの計算

MD5(**ユーザ名+チャレンジ文字列+パスワード**)

IPv6への取り組み（実サービスへの展開）

IP Centrexサービス
「IPビジネスホン」
の開発



IPビジネスホン導入事例

全国寮グループ「共立メンテナンス」による全面採用（2004年3月）

日本全国	300拠点
IPv6Node数	27000台以上

共立メンテナンスからのオーダー

- ○ 運用コストを削減したい
- ○ 短期間（9ヶ月）で導入したい
- ○ 拡張性のあるシステムにしたい

寮電話システム導入段階

- 寮側のネットワークを考えた場合、IPv4でも同じ構成が可能か？可能だとしたらどのように構築するべきか、IPv6を採用する場合にはIPv6 over IPv4トンネルを使用することが決まっていたため、IPv4でも同様の構成を構築し、実際のモデル寮にて実験を行った。結果として、

→工事段階における設定に関する問題の表面化。
→IPv6を使用したCentrexシステムとの接続が非常に面倒
　プロトコルトランスレータ、B2BUA等が接続に必要となる
→IPv4グローバルを端末に振る場合、27000個以上もアドレスが
　取得可能か？

IPv6にするのがシンプルかつ現実的

サービスインまでの流れ

短期間で20,000台のサービスインを実現

サービス仕様の策定 システム設計	テスト稼動	設置工事 （入退寮に伴う工事休止期間を含む）

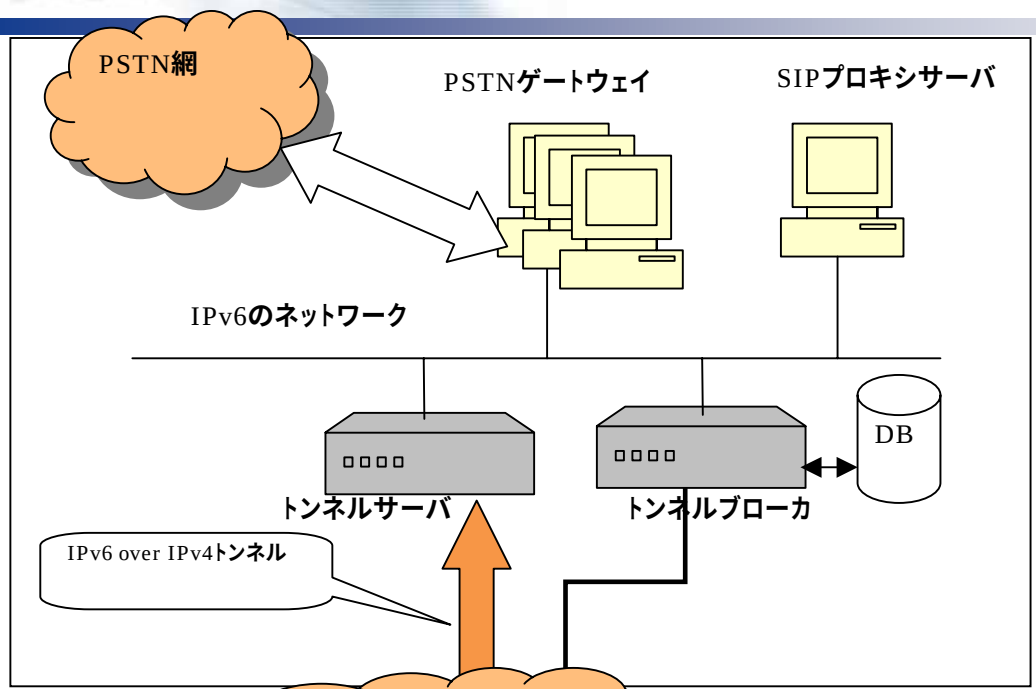
2004/3　6　9　2005/4

「アドレス設計の利便性を活かし、入居者数に応じて3パターンに工事内容を抽象化。」

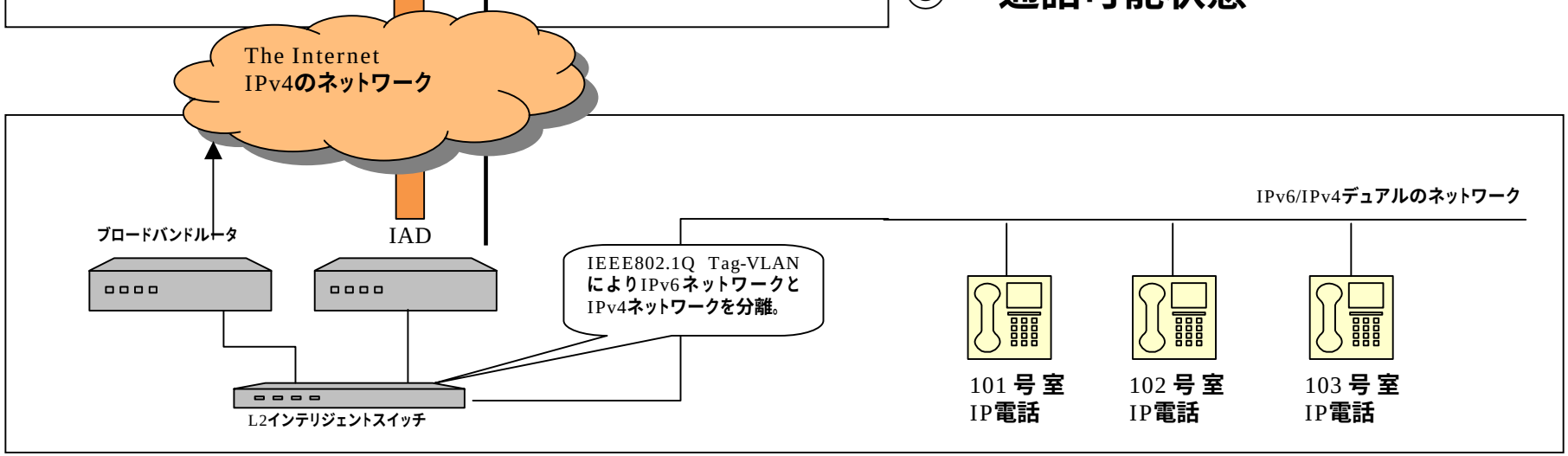
「アドレスの自動取得により、設置工事は専門知識が不要。」

「各端末の状況は固定IPv6アドレスを利用して、リモートで監視。迅速な障害対応を実現。」

寮電話システム構成概要



① IADがインターネット接続開始
② IADがブローカへ認証 (DTCP)
③ ブローカよりIPv6-prefixを取得
④ IADは下流でprefixを広告 (RA)
⑤ IADは対向のトンネルサーバを自らに設定
⑥ 電話機は個別にアドレスを自動生成
⑦ 電話機がSIPサーバへREGIST
⑧ 通話可能状態



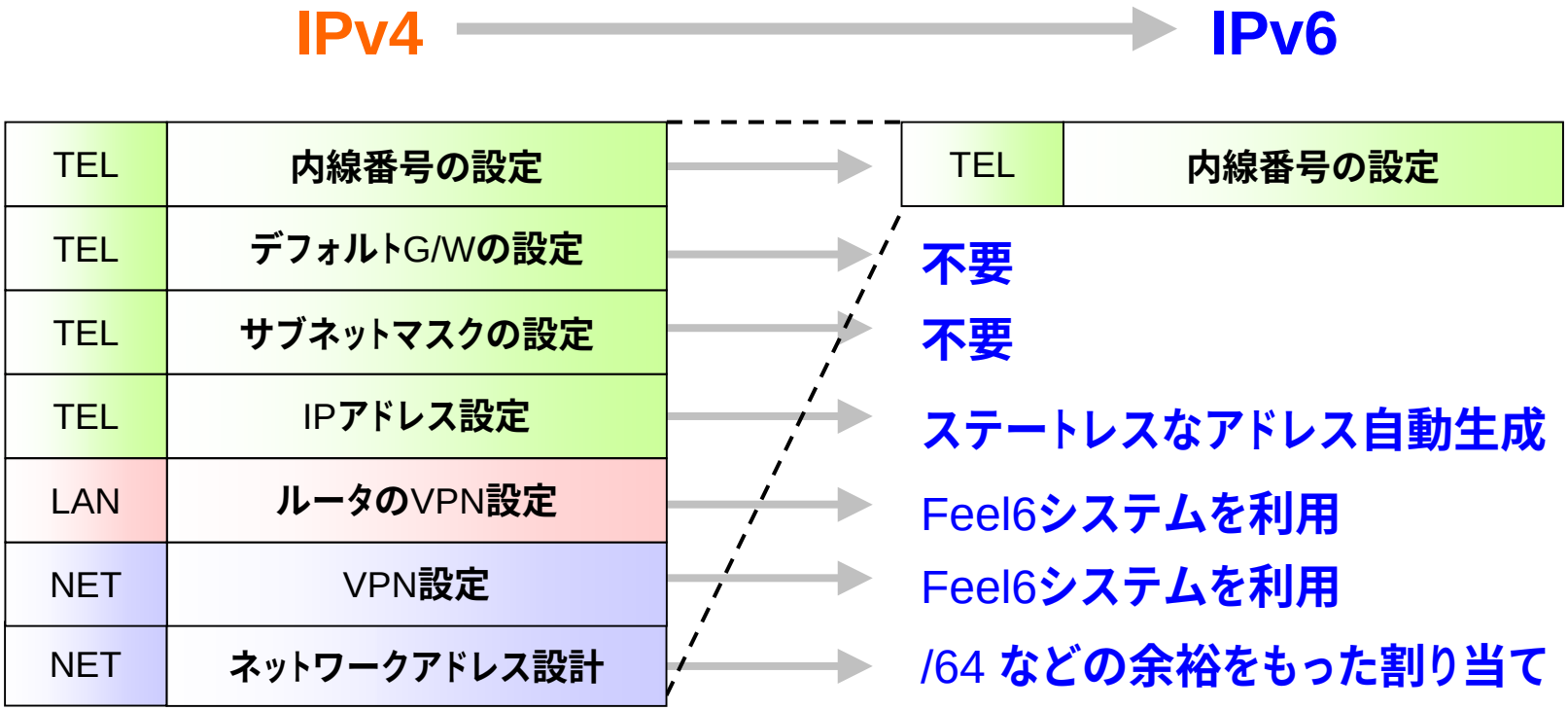
コストについて

IPv6でコストダウンを実現

	設計段階	工事段階	運用段階
IPv4	割り当てるIPアドレスの範囲を細かく決める必要がある。	各端末にサブネット・マスクやデフォルトゲートウェイの設定が必要。	センター側から端末を特定するのが難しい。
	拠点ごとのアドレス設計が必要。	アドレス設定のミスが多発。	障害時の原因特定が遅れる。
IPv6	余裕を持ったアドレス数を確保。 階層化で設計可能。	ステートレスなアドレス自動生成。	固定IPv6アドレスがセンター側で分かるため、各端末の状態を簡単に確認、設定できる。
	拠点ごとのアドレス設計が不要。	工事に専門知識が不要。電話工事業者でも工事可能。	メンテナンス作業の負荷を軽減。

設計、設定工数の圧縮

ネットワーク設計と設定工数を大幅に削減



導入にあたって苦労した点

- 外線発信のための相互接続における問題
  →SIP用IPv6 / IPv4 のトランスレータのパフォーマンス問題
  接続されるDBのパフォーマンスや、同時に数百のSIP/RTP/RTCPを終端し変換する能力が求められた。
  このような高負荷をどのように分散するかの手法の構築はトライアンドエラーを繰り返して煮詰めた。

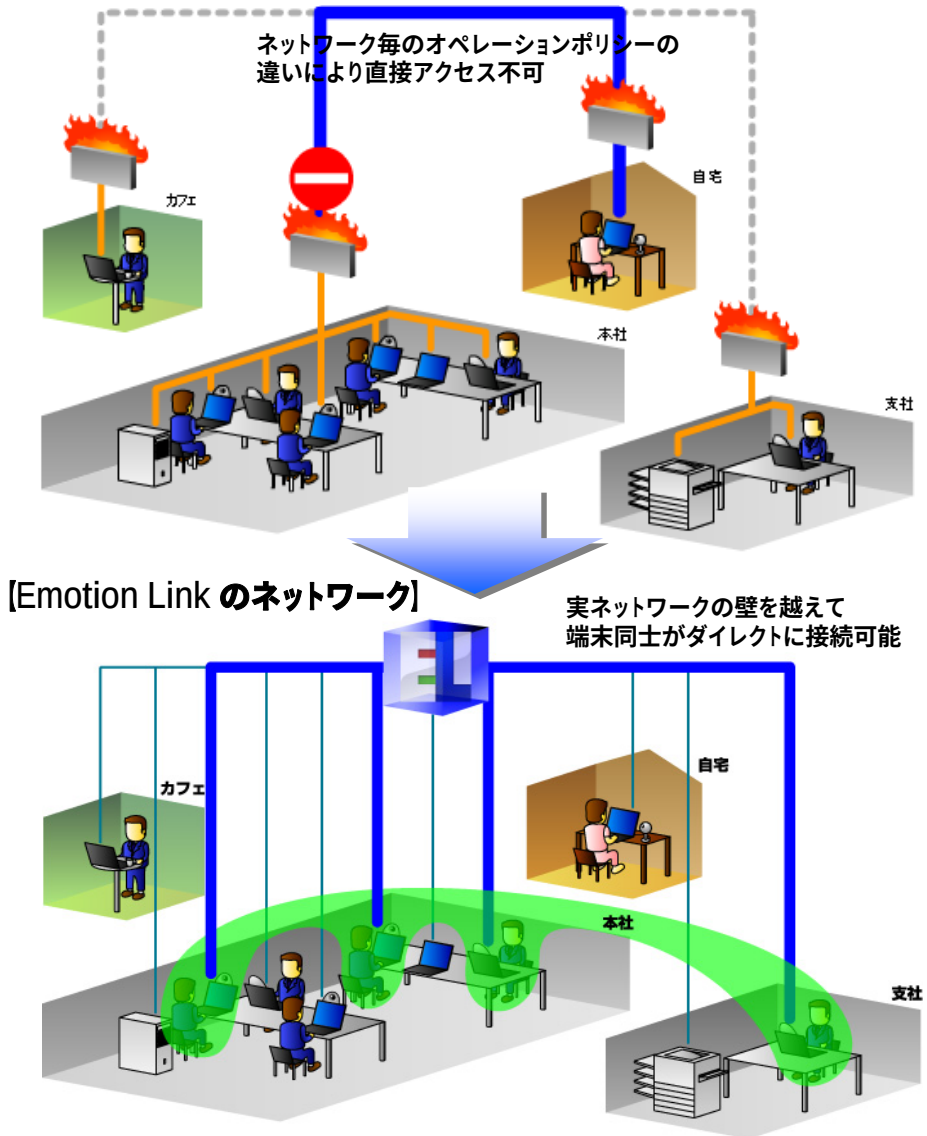
- 比較的小規模では発現しなかったような不具合の顕在化
  →寮側に導入するIPv6対応ルータの不具合。
  近隣探索の結果IPv6アドレスを保持するテーブルがあふれ、一定数以上の端末の通信が不能になった。

IPv6への取り組み

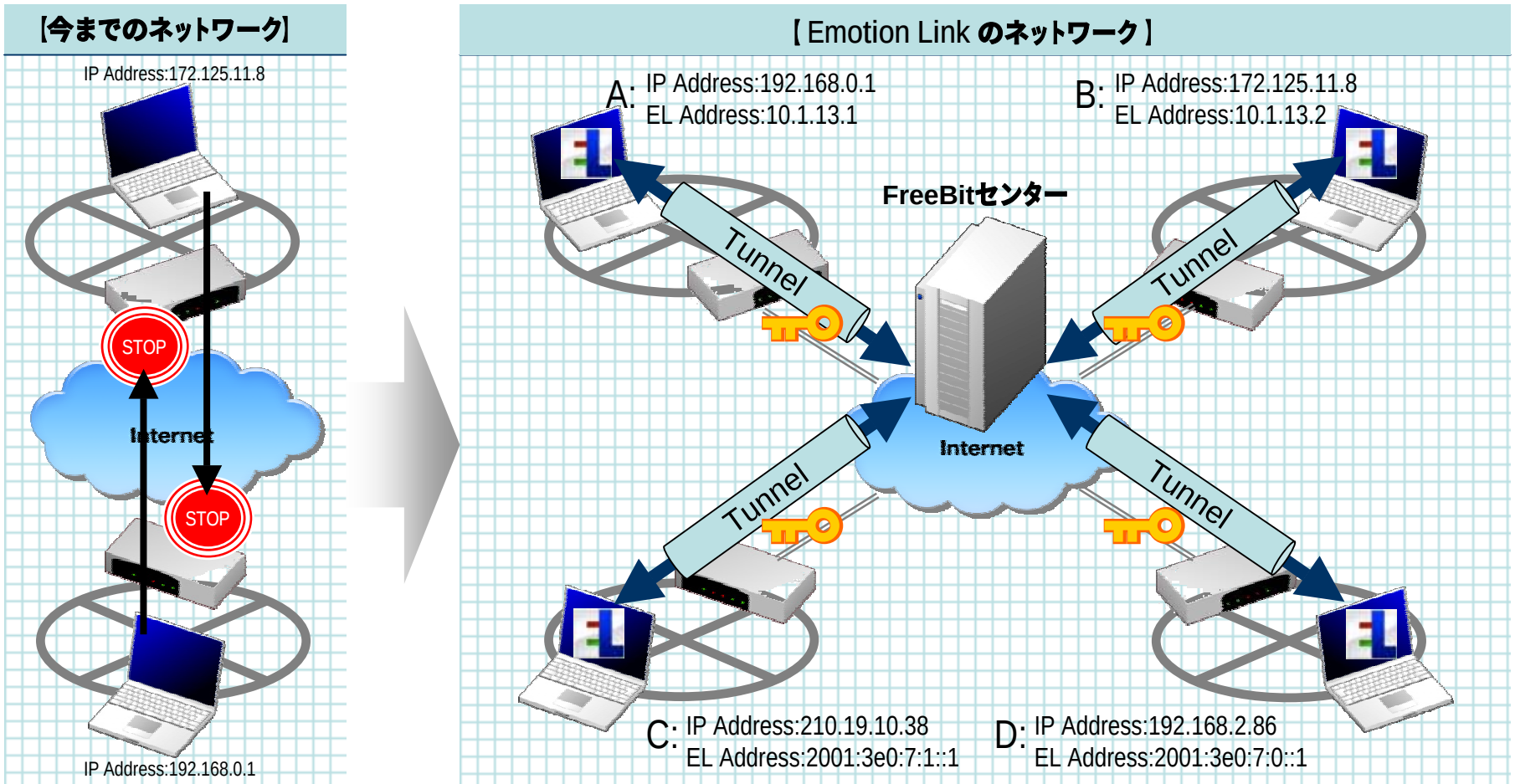
2004年～
Emotion Linkテクノロジー

『Emotion Link』とは

- 導入が容易である
  - 個々の端末側に特別なネットワークの設定が必要なく、接続用ソフトウェアを導入するだけの簡単設定
  - 通信経路上のルータ等に特別な設定を行う必要が無い為、ユーザ負担が軽い
- セキュアな通信
  - 通信経路は暗号化されるため、セキュアな通信を確立できる
  - 拠点同士のVPNと違い、LAN内も含め各端末まですべての経路で暗号化
- シームレスなダイレクトアクセス
  - 端末同士が仮想IPアドレスベースでNATを超えた通信ができる(IPv4/IPv6に対応)
  - どのようなプロトコルでも通信する事が出来る為、アプリケーションの制約が無い
  - L2までのアクセスを扱えるため、ブロードキャスト等に依存したアプリケーションも動作可能
- クライアント実装を選べる
  - OSに仮想ネットワークドライバをインストールする提供パターン
  - 仮想ネットワークを構築するためのライブラリ形式での提供パターン



『Emotion Link』のシステムモデル概要



Internet上にセキュアなプライベートネットワークを構築。
端末同士はEmotion Linkで割り当てられたIPアドレスを用いて通信を行う。
※EL-IPは実際のIPアドレスとは別に付与される。

Emotion Link プロトコル（1）

■IPv4/TCPをキャリアに採用した、独自のVPN方式。

■TCPをつかうため、既存のv4-NATやPROXYともなじみがよく、Feel6で実現できなかったNATを越えた通信を実現している。

■Ether（L2）フレームを扱うモードと、L3以上を扱うモードの2種類の製品が存在。

■SSLを利用した暗号化に対応。OpenSSLが実装している暗号化プロトコルを任意に選択して利用できる。

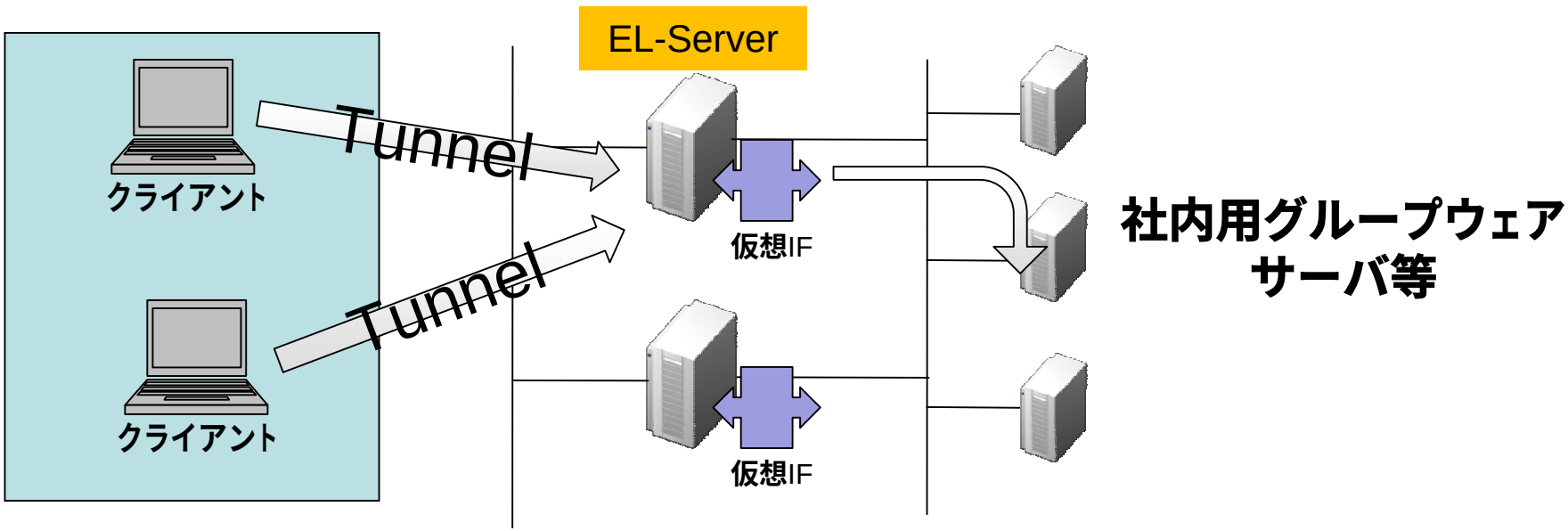
■IPv6とIPv4の仮想ネットワークアドレスを扱える（現在排他的）。

■冗長化と負荷分散を実現するためにブローカーモデルを採用。
このためプロトコルの実際の動作は
1．ブローカープロトコル
2．ELプロトコル
の2フェーズに分かれる。

Emotion Linkサーバ

ネットワーク上に存在するEmotionLink用のスイッチングハブのような存在。
接続されたクライアントを仮想的なひとつのネットワーク（もしくはセグメント分けされた）にまとめる役割をもち、クライアントからのv4/TCPを直接終端する。

仮想ネットワークインターフェースを持ち、サーバと同一もしくは指定されたセグメント上のサーバ機器と仮想IPを使った通信が可能。



Emotion Linkクライアント

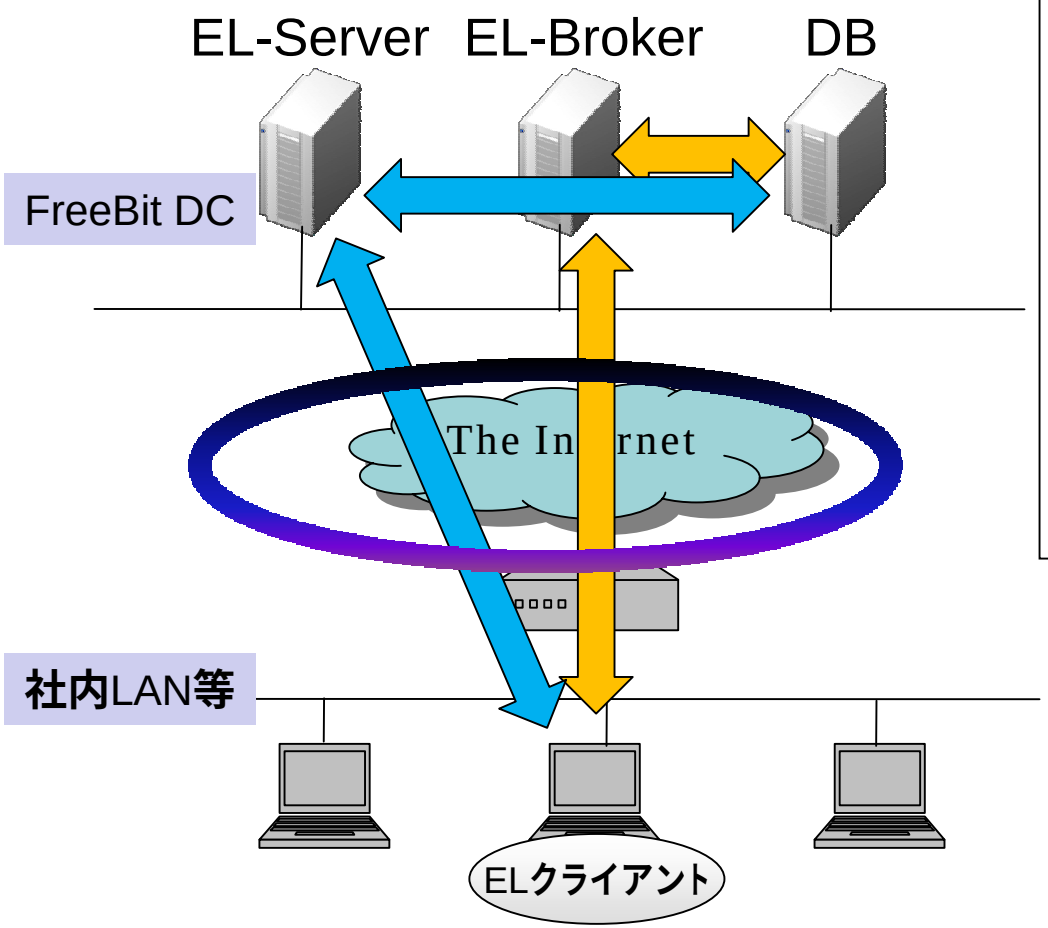
・クライアントの種類

OS	モード
WindowsOS	カーネルモード、ユーザモード
MacOSX(iPhone)	(カーネルモード)、ユーザモード
Linux (組み込み等)	(カーネルモード)、ユーザモード
T-Engine	カーネルモード

カーネルモード： 専用の仮想ネットワークデバイスドライバのインストールが必要。OSがTCP/IPの面倒をすべて見る。
ifconfig / ipconfig 等で仮想IPが確認できる。

ユーザモード ： TCP/IPスタックを内包したライブラリ形式のクライアント。
仮想ネットワークデバイスドライバのインストールなしにEmotion Linkネットワークと接続可能。

VPN確立までの流れ



1. クライアントがブローカへアクセスし
   ユーザ認証を行い、接続可能な
   ELサーバを選択する。

2. クライアントは紹介されたELサーバ
   に対しIPv4/TCPのコネクションを
   確立（SSL）。

3. サーバから接続に必要なIP、Netmask
   ルーティング情報等を取得。

4. リンク確立。

Emotion Link Stack Library 2006～

■TCP/IPスタックを独自に実装し、Emotion Linkネットワークへのアクセス能力を備えた独自ライブラリ。IPv6/IPv4に対応。

■BSD Socketのようなインターフェースで利用可能なAPI群。

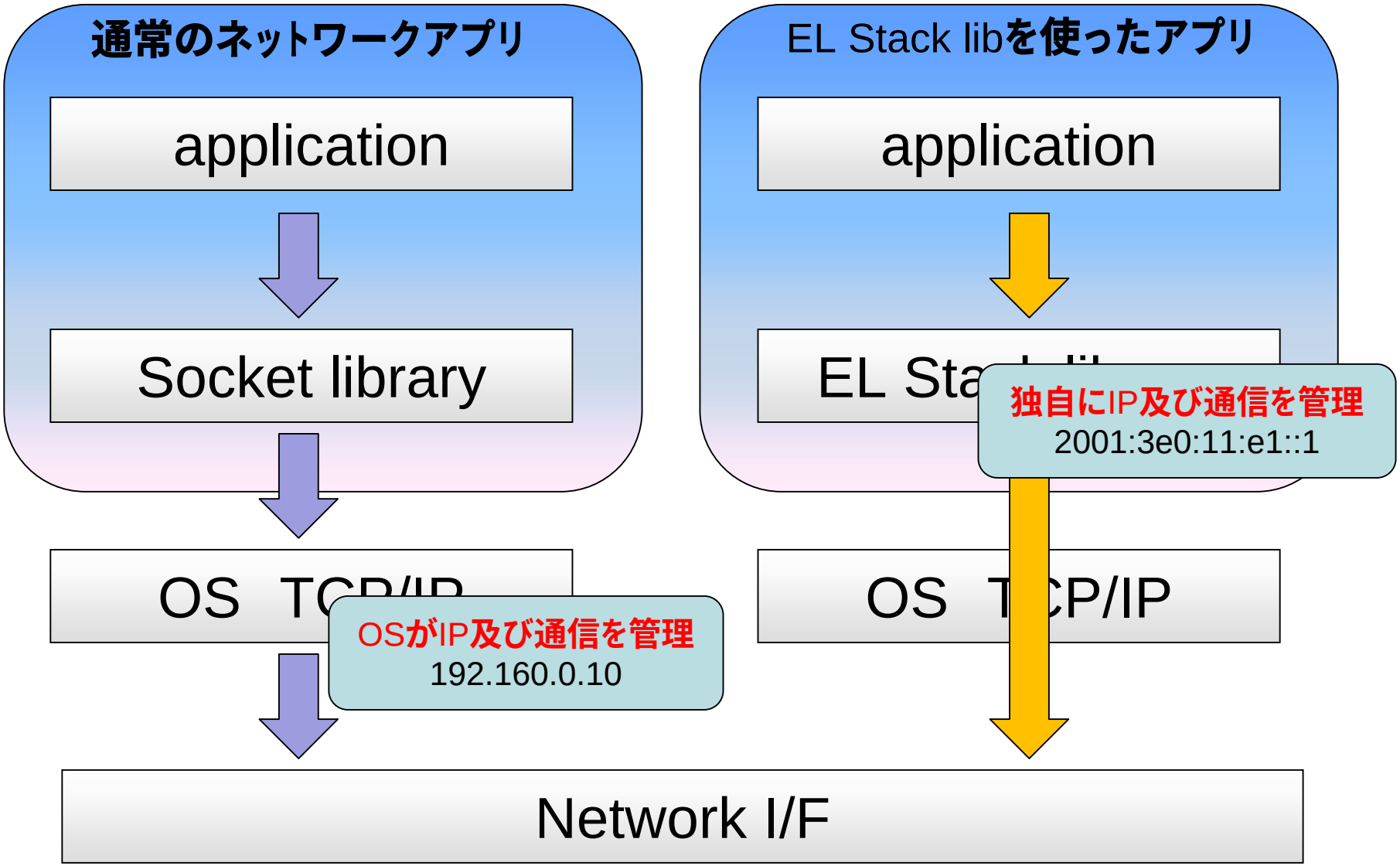
■ライブラリが直接Emotion Linkを終端し、IPやルーティングなどの管理を行うためこのライブラリを組み込んだアプリケーションは、アプリ単体でIPを保持する。

■OSからみると、v4/TCPをしゃべるひとつのネットワークアプリにしか見えない。このため、OSの持つネットワークアーキテクチャと分離できる。
例） IPv6未対応のOSでIPv6対応のアプリケーションを動作させる。

■既存のネットワークアプリケーションのsocketアクセス部分を、このライブラリを使用して書き直すと、そのアプリケーションは直接Emotion Linkネットワークに接続されるようになる。

■ユーザモードで動作するので、ドライバインストールなどの必要がない。

Emotion Link Stack Library（比較）



Emotion Link Stack Libraryの利用に際して

■OSがIPv6に対応しているかどうかに関係なく、アプリケーションをIPv6対応することができるため、アプリケーション製作者はIPv6のことだけを考えていればよい。

■仮に実ネットワークがIPv6対応した場合には、Emotion Link Stack Libraryを外して、普通にsocketを使うようにすればよい。
→APIがBSDソケットに近い使い方ができるので、変更も容易

■トンネルデバイス（デバイスドライバ等）を作成するのが困難な状況、またはOS自体がIPv6対応が難しい場合においても、アプリケーションレベルでVPNが実装できるので、様々なOS環境に対応できる。

Emotion Link Active Nodeを利用したアプリケーション導入例

楽天メッセンジャー

EL ActiveNodeを使いインスタントメッセンジャーが直接IPv6のアドレスを持ち、SIPを使ったメッセージや音声をやり取りする。

楽天メッセンジャーの特徴

- IPV6自律ノード型アプリケーション。
- Emotion Linkにより、IPv4の環境に一切手を加えずにIPv6の動作を実現。
- シグナリングプロトコルとしてスタンダードなSIP(IPv6) を採用。
- チャットのメッセージも含め通信内容はすべて暗号化。

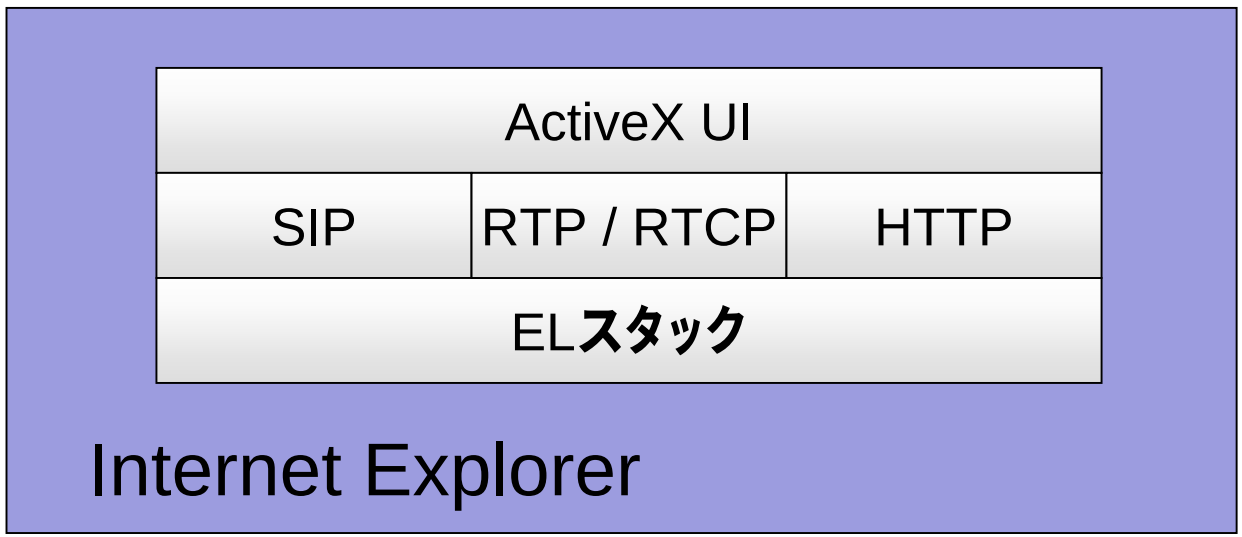
現在はサービス停止中

楽天IMの構成

■ActiveXモジュールとして配布することで、WEBサイトと密接にサービスを展開。

■SIPスタック等のネットワークアクセスを行う部分を、ELスタックに対応させることで、すべての通信をEmotion Linkネットワーク経由で行う。

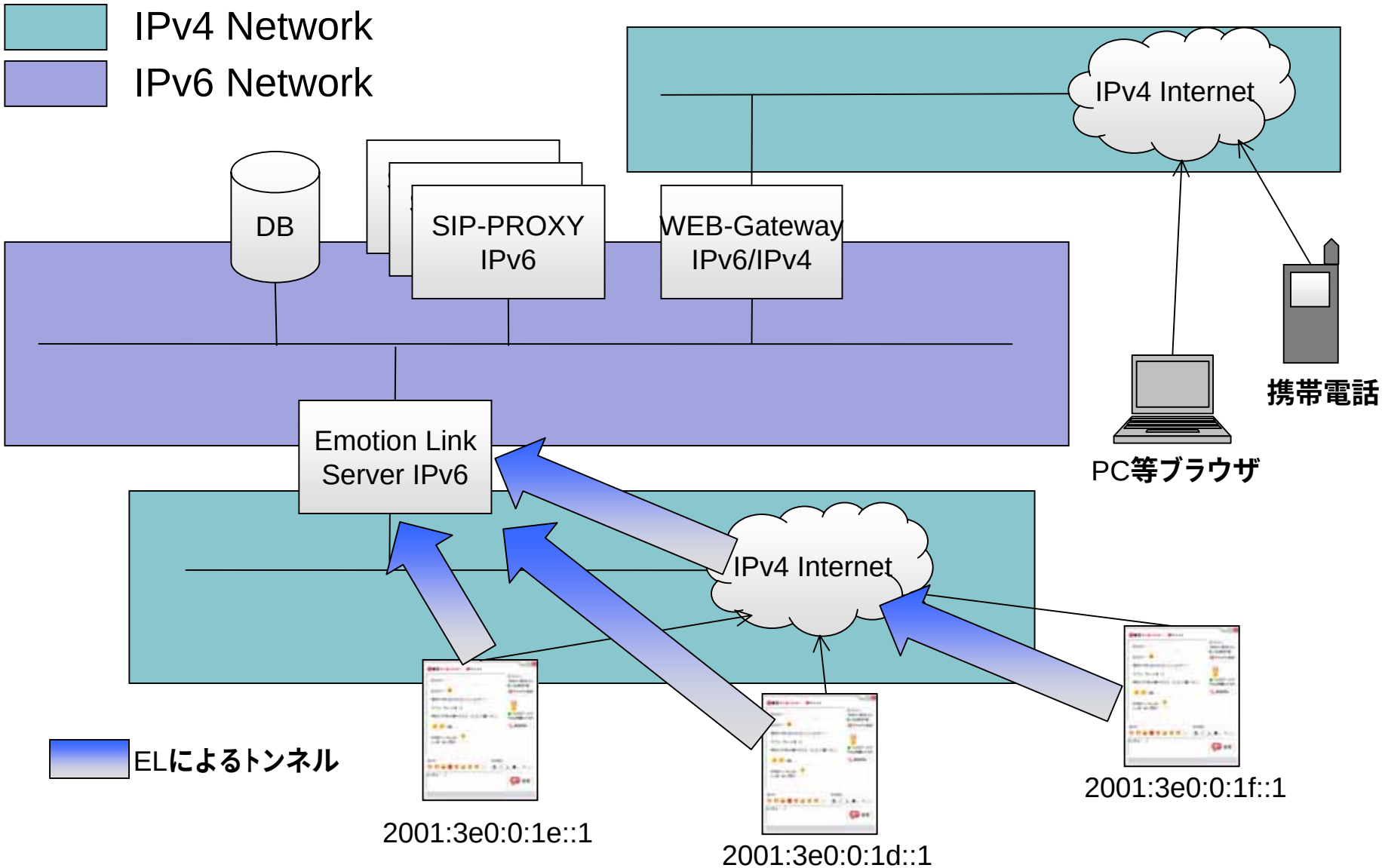
■暗号化を行う部分をすべてELスタックに任せることで、プロトコル設計が楽に。



楽天IMのネットワーク構成概要

- バックエンドサーバ群をすべてIPv6ネイティブ対応で構築。IPv4は必要に応じて利用。基本的なアクセス部分はすべてIPv6を使う。
- メッセージング及びシグナリング、プレゼンス通知などはすべてSIP（IPv6）で行う。
- エンドユーザにIPv6を利用したIMアプリケーションを利用して もらうためにEmotion Link（IPv6運用）を採用する。
- 将来的にPSTNに接続する場合はIPv6/IPv4トランスレータを介して接続する。
- IMクライアントはActiveXプログラムで提供されるため。WindowsPCでIEが動いている環境であれば動作する。

楽天IMネットワーク概念図

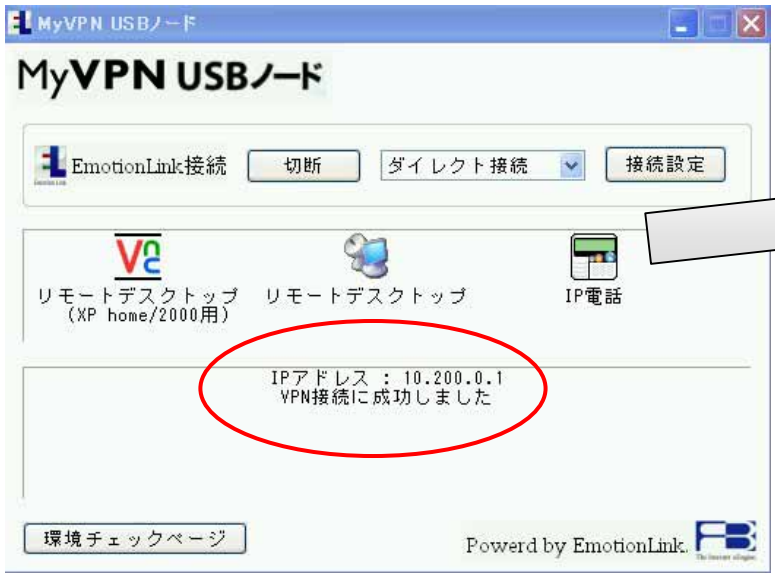


最近の事例　総務省　テレワーク実証実験

- 総務省主催によるテレワーク推進のための実証実験に参加。
- VPN部分Emotion Linkを利用したアプリケーションを提供。
  IPv4とIPv6の仮想ネットワークを同時に利用可能に。
- IPv4での提供部分：　IPv4のみのWEBアクセス、リモートデスクトップ等既存のOSのIPv4に頼ったアプリケーションを使う要望があるため、部分的にIPv4を提供。
- IPv6での提供部分：　IPv6を使ったソフトフォン（内線網の構築）。電話（ソフトフォン）に関しては、弊社のIP-Centrexシステムに直接収容するために、IPv6対応。

最近の事例　総務省　テレワーク実証実験

メインアプリケーション



起動

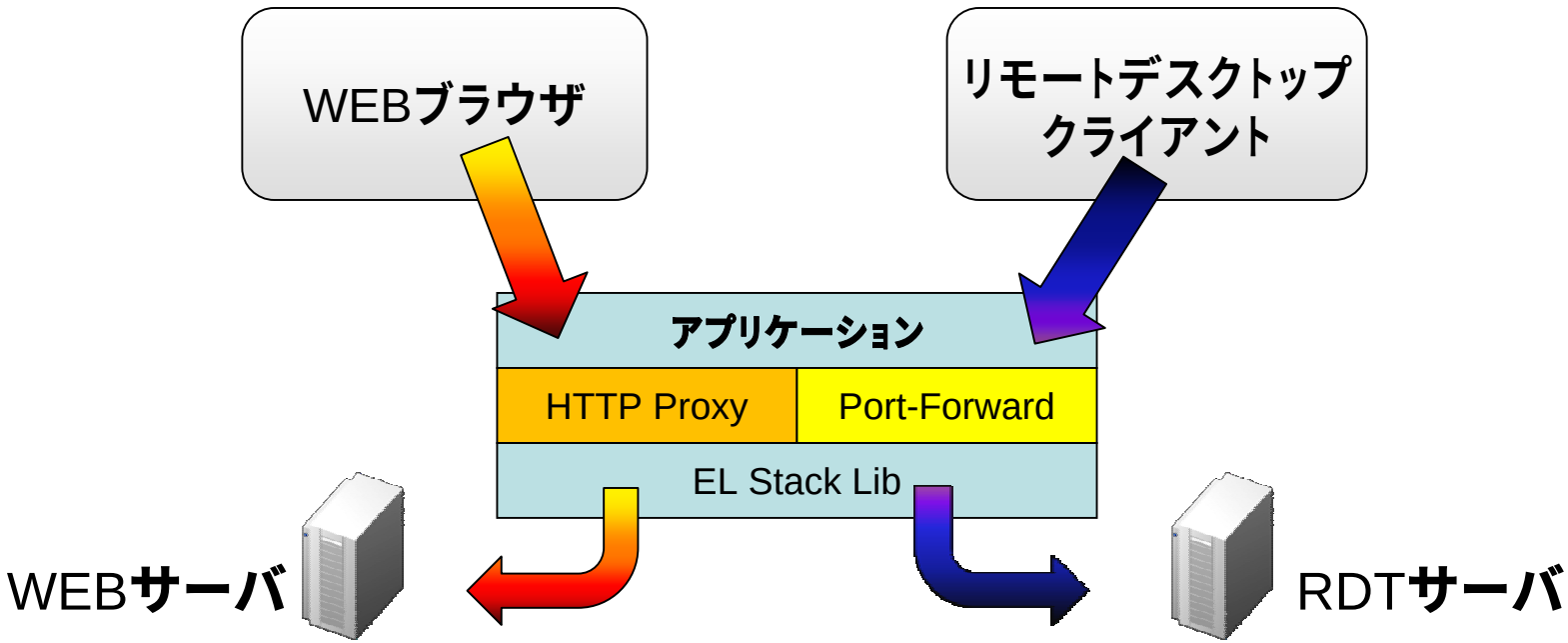
生体認証（指紋）に対応した
USBキーデバイス

メインアプリケーションの機能

■アプリケーションはELネットワークを経由できる、HTTP Proxy機能とポートフォワード機能を持っている。

■通常のWEBブラウザ等はPROXYをローカルホストに指定することでHTTP Proxy機能がEL Stack Libraryを経由したアクセスに変換する。

■リモートデスクトップ等のアプリケーションもPort-Forward機能により、指定された宛先IPとPORTに対するアクセスをEL Stack Library経由に変換する。



SemantiqNode　2007~

■2007年よりDTI(Dream Train Internet)からリリースされた新サービス。
専用クライアントをPCにインストールすることで、ブラウザさえあれば場所を問わずに、どこからでもPC内のリソースにアクセス可能になる。

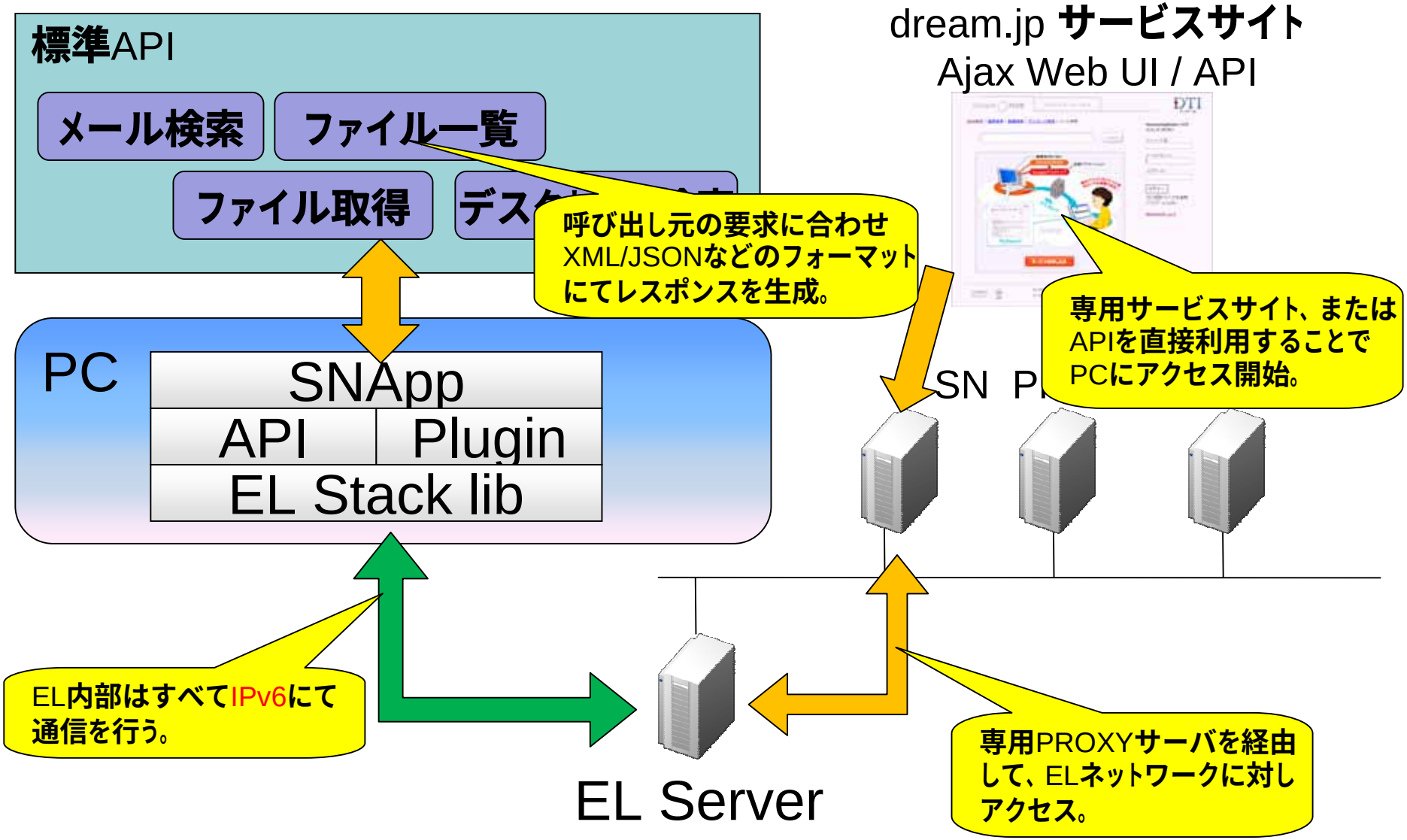
■PC上のリソースをすべてURLで表現する。＝API化。
例）ファイルリストAPI、ファイル取得API、ファイル検索API、etc..

■PCへのアクセス機能は、カテゴリ別にAPI化されており、XMLやJSONといった標準的なデータ形式でレスポンスを返す。

■このため、既存のWEBサービスとも連携が可能となり、独自のマッシュアップ等が可能。

■プラグインによる機能拡張が可能(現在はWindowsのみ）で、独自のAPIを実装可能。
例）Webカメラ＋Webカメラプラグイン　＝ 映像をリアルタイムに取得するAPI。

SemantiqNode アーキテクチャ



SemantiqNode API (1)

■SemantiqNodeとの通信にはhttpを使用します。APIを呼び出す場合はCGI等にアクセスするのと同様の方法を用います。APIの実行結果はレスポンスのBODY部で受け取ることができます。現在下記のAPIが提供中です。

API名	機能
認証	SemantiqNodeをインストールしたPCに対して認証を行ないます。
ファイル一覧	指定したフォルダ内のファイル一覧を取得します。
ファイル取得	特定のファイルを取得します。
ファイル検索	Googleデスクトップと連携し、検索結果を取得します。
メール検索	OutlookExpressやThunderbird 2で受信したメールを検索します。

■APIには組み込み型とplugin型が存在し、plugin型APIは今後公開予定のplugin-SDKを利用することでSemantiqNodeの機能を直接拡張することが可能となります。

SemantiqNode API (2)

■APIアクセスURLフォーマット

http://snapi.dream.jp/sn/<node-name>/do?action=<API>&param=value..

■Public / Privateの概念

SemantiqNodeには、広くInternet上に公開できる場所としてのPublicエリアと、SemantiqNodeを実行するPCのオーナーのみが、アカウントとパスワードで識別されアクセスが許される、Privateエリアという2つのアクセス概念が存在します。

通常、Publicエリアは、ブログパーツなどの、不特定多数に公開してもいい画像などのコンテンツを格納する場所で、それに対してPrivateエリアは他人には公開しないファイルなどを格納します。

SemantiqNode用のアクセスPROXYサーバは、この公開状態を把握し、適切に認証を行います。APIを利用することで、これらのエリアを自由にアクセスすることが可能です。

SemantiqNodeの今後

■今後の取り組みとして、PCの電源を積極的にコントロールするモードの開発を進めています。この機能が実装されると、PCの電源がOffである状態から自動復帰させ、SemantiqNodeAPI等を呼び出し利用することが可能になります。

■また、常時通電型のデバイス上にSemantiqNodeを実装することで、上記のデバイスコントロール対象をLAN上の家電製品にまで拡大することが可能です。

これらを制御するためのアクセス経路はすべてEmotion LinkおよびIPv6の特質を生かしたネットワーク構成になるでしょう。

FreeBitではこれからも、仮想化とIPv6を推し進めていきます。

SemantiqNode API デベロッパプログラム

■開発者向けに特別なプランを用意してます！
DTI Ubiqプランのアカウントを無料で提供。すぐにSemantiqNodeをインストールし、開発環境であるAPI使ってみることができます。

http://dream.jp/ubiquitous/snode/developer/

おわりに、IPv4アドレス枯渇に際して

- IPアドレスの消費動向をwatchしていると、近い将来なくなるのだなぁと漠然と思う段階は過ぎている。
  →危機感

- 近い将来ネットワークはIPv6とIPv4の混在した環境になっていく。IPv4があまり利用されなくなって、IPv6に置き換わるまでは共存していく必要がある。
  →いきなりは変えられない。

- 広い意味でのトンネリング技術を適用して、なるべく早い段階で、エンドユーザにIPv6を届ける努力をする。
  →新しいサービスを考えるときにIPv6を考慮する。

- IPv4の枯渇が現実的になってくると。IPv6のビジネスが必ず立ち上がってくるはず！　→なるべく早く始めましょう。