

インターネットにおけるプレゼンテーション、セッション層相当、

汎用プロトコルの開発

一次世代インターネットアーキテクチャの提案

アプリケーション基盤の開発

1.背景

従来のインターネットアプリケーションは FTP、文字中心の Web、Telnet など比較的単純で、ネットワークに求められるものは単純なデータの送受信のみであった。従ってインターネットのネットワークアーキテクチャでは OSI7 階層モデルにおけるセッション層、プレゼンテーション層、アプリケーション層をまとめてインターネットのアプリケーション層としている(図 1、2)。しかし、近年 SCP、マルチメディア中心の双方向な Web、SSH などアプリケーションが高機能化し、更に暗号化、認証などのセキュリティ機能の要求も高まってきている。現状では前述のネットワークアーキテクチャの簡易化により、これらの機能をアプリケーション層でまかなうことになり、アプリケーションが個別に実装している。これらの機能の多くは本来ネットワークが提供すべきものである。今後更にネットワークに求められる機能は多くなり、アプリケーション開発の負担は増加すると考えられる。次世代インターネットアプリケーションの開発を円滑にするため、インターネットのネットワークアーキテクチャを再構築する時期がきていると言える。

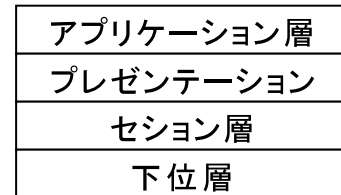


図 1

OSI 基本参照モデル

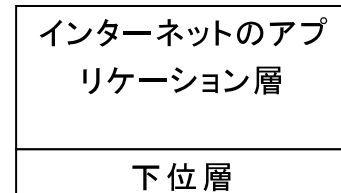


図 2

インターネット
アーキテクチャ

2.目的

当プロジェクトの目的は、ここまでつぎはぎだらけで来たインターネットの現状の打開であり、具体的には以下の 2 点である。

- i. ネットワークアプリケーションが今後必要とするネットワークに属する機能をインターネットのアプリケーション層から Intelligence and Quality Layer(IQL)として切り離すことを提案し、アプリケーションとネットワークの機能の分離を明確化すること。
- ii. IQL 上の汎用プロトコルを設計、実装しネットワークアプリケーション開発の負荷を軽減すると共に、IQL 分離の妥当性を検証するための基

盤を整えること。

3.開発内容

当初インターネットのアプリケーション層からセッション層、プレゼンテーション層を切り離し、プロトコルを定義する計画だったが、開発を進めるにつれ開発内容、目的が上記の2層で定義されている機能の範囲には収まらず、よりインターネットに相応しい切り分けが必用であると考え、インターネットのアプリケーション層の下にIQLを設け、その定義を行った。

IQL上で定義した機能は暗号化、認証、(圧縮、フォーマット変換)、下位層通信媒体の管理単位として定義したJarad(従来のセッション)の管理等インターネットアプリケーションが共通として必要とする機能で、現在インターネットのアプリケーション層に属しているものとした。

またIQLの下位層は基本的には従来のトランスポート層となるが、今後のインターネットへの拡張を考え、あらゆる媒体(レイヤ)を下位層にもてるように、IQL内にIQ Media副層(IQML)を定義し、通信媒体の抽象化を行った。これは既存のトランスポート層や、データリンク層が提供するメディア抽象化の概念を拡張したものであり、読み書きさえ可能であればあらゆる媒体をIQLの下位媒体として利用可能にするための仮想レイヤである。

IQL上に次世代インターネットアプリケーションが必要とする機能を提供する、プロトコルYJPを開発した。実装はWindows(2000以降)上のサービスとして行い、データ変換、認証、IQ Mediaをプラグイン形式で実装しユーザーが自由に追加できるようにした。アプリケーションへの接続は名前つきパイプ及び、名前つきパイプラッピングしたDLLとして提供する。

今期の開発ではプロトコル及び、APIの設計、プロトコルサービス(現時点では常駐プロセス)、API提供DLLの実装を行った。拡張機能は公開鍵暗号プラグインとしてRSAプラグイン、共通鍵暗号プラグインとしてAESプラグイン、IQ



図3

IQLを導入したインターネットアーキテクチャ

Media プラグインとして TCP プラグインを実装した。

現時点の実装では未完成な部分が多く、ネットワーク上を流れるプロトコル自体に関しては使えるというレベルにするため、公開までに更に仕様を固める必要がある。また、実装自体も一応データの送受信は出来るが、未実装の機能、バグが多く残っている。

IQL を導入したインターネットアーキテクチャを図 3 に示す。また、サービス全体の構成図を図 4 に示す。

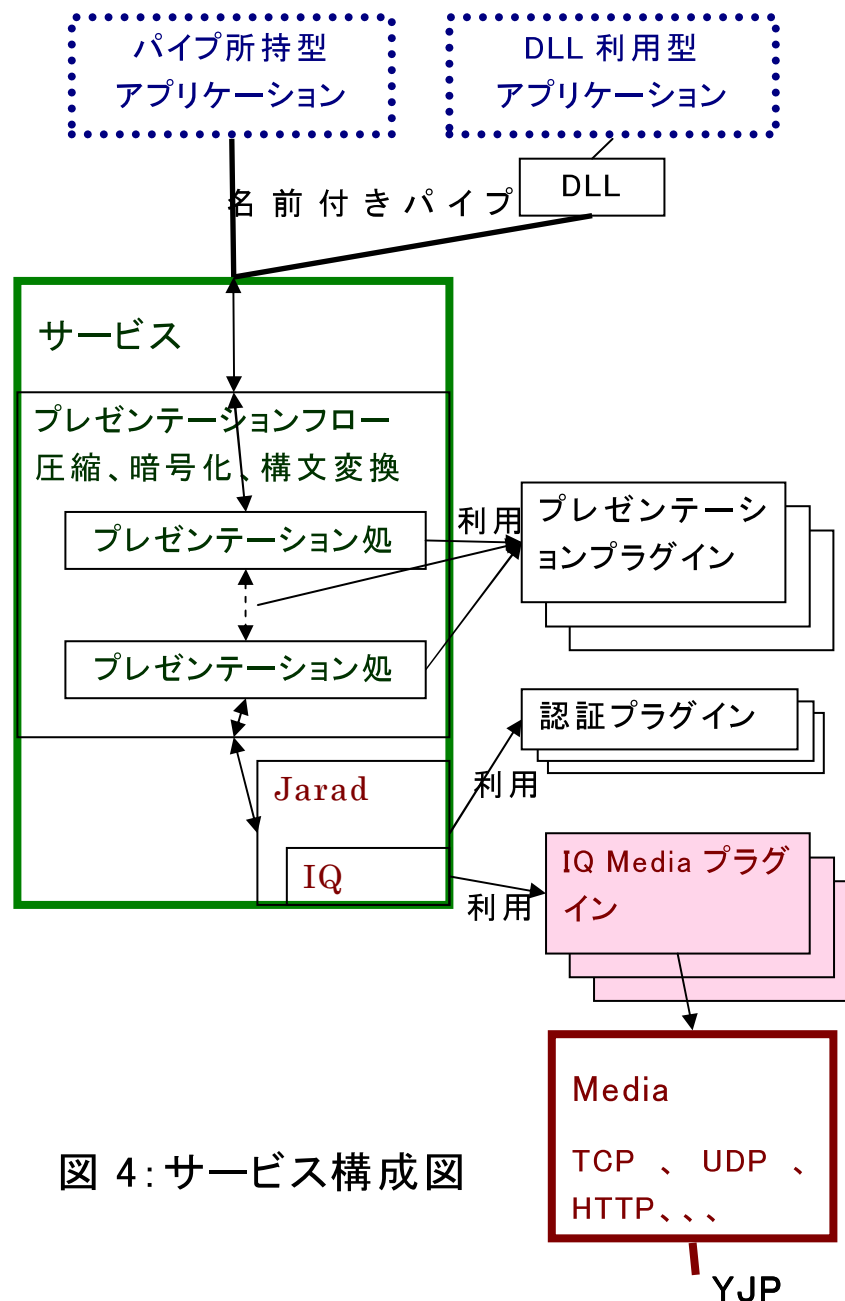


図 4: サービス構成図

4. 従来の技術(または機能)との相違

暗号化、圧縮、認証、構文変換等は全て既存のアプリケーションで実装されているものであり、ライブラリも多く存在するためこれら自体をアプリケーションにまとめて提供する価値は、アプリケーションの実装を容易にすることは確かだが、それ程大きくはない。実際、単にアプリケーションの開発負荷を減らすという試みは、.NET や Java のライブラリ等で多く存在している。しかし、これらはアプリケーション層内にネットワークと関係のない階層構造を導入することになりアプリケーション実装の手助けにはなっても、全体の構造をより複雑にしてしまってい

る。他に HTTP(及びその拡張)が暗号化や認証等の本来ネットワークが負担すべき機能を実装し実績を上げていることから、HTTP 上に様々なネットワークアプリケーションを構築するという動きが見られるが、これはネットワークアーキテクチャを無視した冗長なものである。

当プロジェクトの未踏性は、「取り敢えず」の実装で簡略化したインターネットアーキテクチャ及びそのしわ寄せで複雑かつ肥大化したアプリケーション層を適切な形に矯正する提案であり、既存の階層モデルではなく、よりインターネットに適した IQL を提案したことにある。YJP の開発もこれらの妥当性を示すためのものであり、実際に IQL を分離したアーキテクチャを利用したアプリケーションの実装が現状より「すっきり」することをネットワークアプリケーション開発者に示すことを主目的と考える。

5.期待される効果

当開発によって期待される効果は以下の通りである。

- i. 次世代インターネットに適した IQL の提案により、ネットワークとアプリケーションの機能を明確に分割し、ネットワークアプリケーションの肥大化、複雑化を抑えることが出来る。
- ii. YJP の提供により高度なネットワーク機能を活用するアプリケーションの開発が容易になる。

6.普及(または活用)の見通し

現時点では未完成な部分も多く、公開できるレベルではないため、当面の目標はプロトコルを完全にし、最低限必要なプラグイン、API を実装、マニュアル、Web サイト、開発者向けサンプルアプリを作成し公開することである。また、RFC 形式のプロトコル仕様も作成公開する。

長期的な計画として、Jarad を任意の I/O と繋ぐ機能、名前付きパイプ以外による SAP、Unix 等の別のプラットフォームへの移植、Jarad のシリアライズ、マルチキャスト、YJP を最大限に活用するための P2P による名前解決システム、アプリケーションレベルエニーキャスト(複数の通信相手の中から、ある条件にあった端末から応答を得る機能)、YJP のハードウェア化等の機能を順次実装していく。

7. 開発者名(所属)

前田 智哉(慶應義塾大学情報工学科)

(参考)公開予定 URL

<http://eme.or.tp/~iql/>