スマートフォン　非接触ICカード　クレジット

Technology Reports

オープンOS端末上のおサイフケータイにおけるクレジットサービスの開発

スマートフォンの普及が進み，そのOSがオープンソースとして公開されているが，オープンソースは有益である一方，リバースエンジニアリングなどにより脆弱性を発見され，攻撃されるリスクがある．オープンOS端末上のおサイフケータイでクレジットサービスを実現するには，従来のフィーチャーフォンとは異なるアーキテクチャが必要となる．そこで，フィーチャーフォンで実現したセキュリティレベルを保ちつつ，既存システムを改修する際のインパクトを抑えた，オープンOS端末に対応したクレジットサービスを開発した．

クレジット事業部　三浦 信幸（みうら のぶゆき）†　星野 仁（ほしの じん）
サービスプラットフォーム部　広瀬 仁一（ひろせ じんいち）　福囿 貴嗣（ふくぞの たかし）††

1. まえがき

現在，スマートフォンの普及が進んでおり，そのOSをオープンソース[*1]として公開しているものがある．オープンソースとして公開されることは，そのOSの利用・熟成や，そのOS上でのアプリケーション開発に有益である一方，リバースエンジニアリング[*2]などにより脆弱性を発見され，攻撃されるリスクがある．そのようなオープンOS端末上のおサイフケータイにて，クレジットサービスをフィーチャーフォン（ここでは従来のiモード端末のこと）と同等以上のセキュリティレベルに保つには，新しいシステムアーキテクチャが必要となる．また，フィーチャーフォン向けに構築してきた既存システムをそのような新しいアーキテクチャに適合させる場合，いかにしてシステム改修インパクトを抑え，コストの低減・開発期間の短縮を図るかが重要である．そこで，フィーチャーフォンで実現したセキュリティレベルを保ちつつ，既存システムへのインパクトを抑えた，オープンOS端末に対応したクレジットサービスを開発した．本稿では，その実現方式について解説する．

2. フィーチャーフォンとオープンOS端末でのアーキテクチャ

おサイフケータイでのクレジットサービスの実現にあたって最も重要な機能は，クレジットカードの情報をおサイフケータイ上の非接触ICチップ[*3]（FeliCa®[*4]チップ）にセキュアに書き込む機能である．書込みにあたっては，非接触ICチップサーバ（FeliCaサーバ）とFeliCaチップとの間のセキュアな通信路が用いられ，改ざん・盗聴のリスク対策が図られている．FeliCaチップ内にカード情報が書き込まれた後は，FeliCaチップのハードウェア的なセキュリティ機構によって，クレジットカード情報の改ざん防止が図られている．

フィーチャーフォンとオープンOS端末のアーキテクチャの比較を**図1**に示す．フィーチャーフォンでは端末アプリケーションが，FeliCaチップに書き込むカード情報を，カード情報を管理するカード情報等

† 現在，フロンティアサービス部
†† 現在，クレジット事業部

＊1 **オープンソース**：ソフトウェアの著作者の権利を守りながらソースコードを公開することを可能にするソフトウェア使用許諾条件の総称，または，そうして公開されたソースコードそのもの．
＊2 **リバースエンジニアリング**：ソフトウェアやハードウェアの構成や動作を解析し，製造方法や動作原理などを明らかにすること．
＊3 **非接触ICチップ**：ICカードリーダ／ライタと無線通信にて情報交換を行う半導体集積回路．

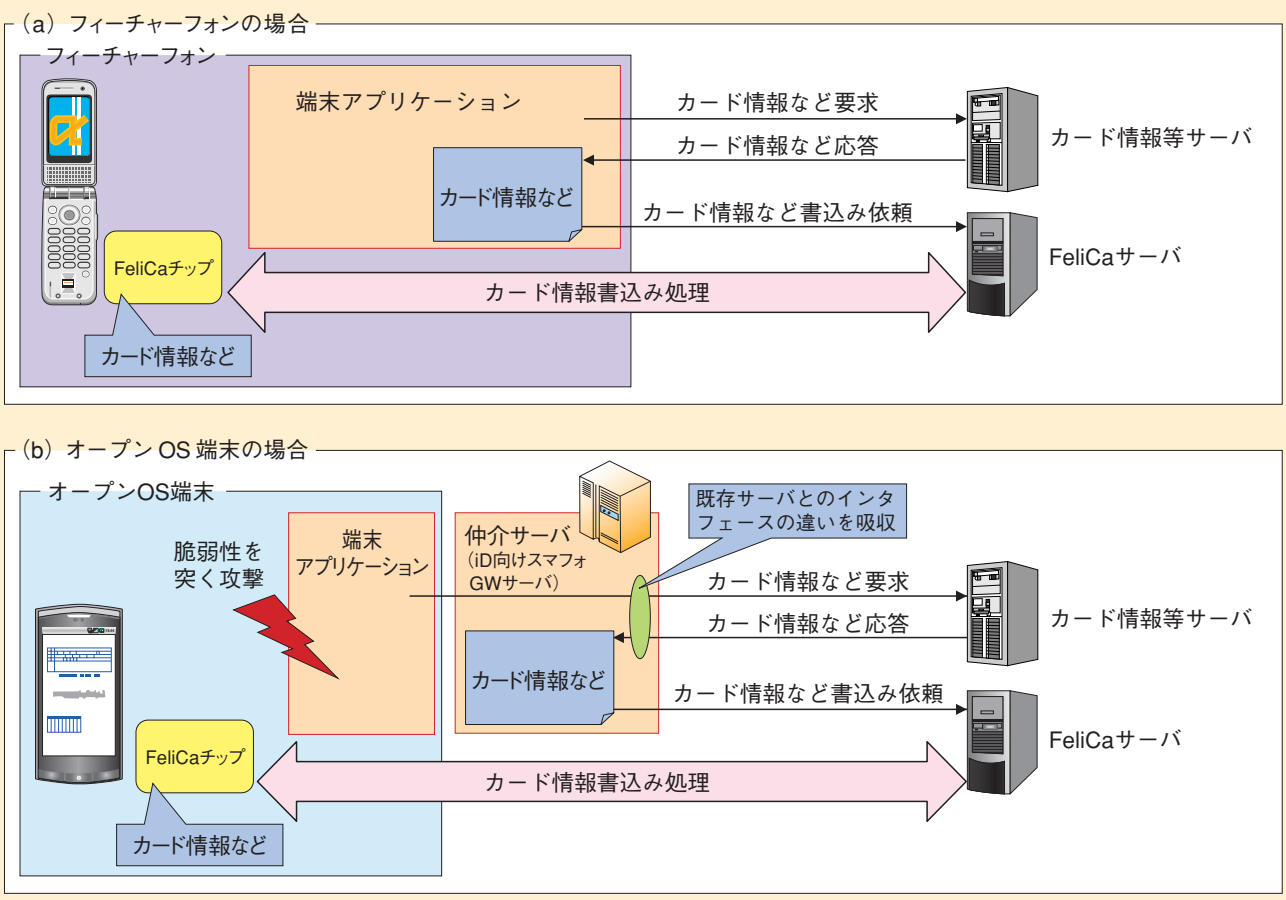


図1　フィーチャーフォンとオープンOS端末とのアーキテクチャ比較

サーバ（以下，カード情報等サーバ）からダウンロードし，いったんメモリ上に保持する．そのうえで，クレジットカード情報をFeliCaサーバに書き込む依頼を行うことで，FeliCaチップへの書込みを行っている．一方，オープンOS端末上の端末アプリケーション・メモリは脆弱性の攻撃を受ける可能性があり，オープンOS端末上にカード情報を一時蓄積すると，クレジットカード情報を偽造・改ざんされ，不正なクレジットカード情報がFeliCaチップ上に書き込まれてしまうおそれがある．このため，端末アプリケーションとカード情報等サーバやFeliCaサーバとの間に攻撃を受けにくい仲介サーバを設け，カード情報などは仲介サーバ上に一時蓄積するアーキテクチャとした．また，既存のカード情報等サーバはフィーチャーフォン向けに作られていることから，オープンOS端末上の端末アプリケーションとのインタフェースの違いを吸収する機能を仲介サーバに搭載することで，既存のサーバへのインパクトを最小限に抑えることとした．

3. 仲介サーバ・端末アプリケーションの実現

3.1 iD向けスマフォGWサーバ

iD[*5]向けスマフォGWサーバは，オープンOS端末に搭載されたFeliCaチップに対して，セキュアにクレジットカード情報を書き込むための仲介サーバである．iD向けスマフォGWサーバの機能構成を**図2**に示す．

iD向けスマフォGWサーバは，主に次の4つの機能を有する．

＊4　**FeliCa**®：ソニー㈱が開発した非接触型ICカード技術方式．同社の登録商標．

＊5　**iD**：「iD」ならびにiDのロゴは，NTTドコモの商標または登録商標．

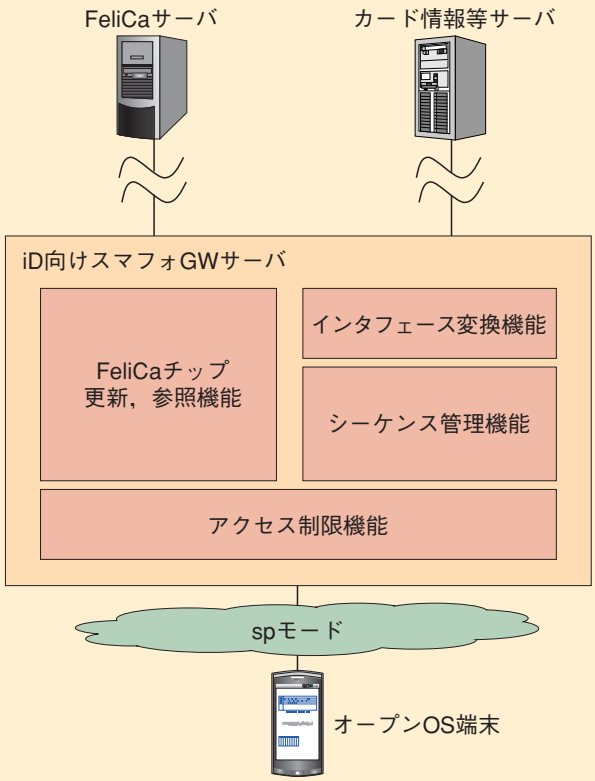


図2　iD向けスマフォGWサーバの構成

⑴FeliCaチップ更新，参照機能

セキュアにFeliCaチップに書き込む仕組みは，FeliCaサーバとして提供されている．iD向けスマフォGWサーバでは，クレジットカード情報をFeliCaサーバを用いてFeliCaチップへ直接書き込むことで，オープンOS端末のメモリへのクレジットカード情報の展開を無くし，偽造・改ざんを防止し，セキュリティを確保した．書込みと同様に，FeliCaチップに設定されているクレジットカード情報をサーバに読み出す場合についても，本仕組みを利用することで，偽造・改ざんを防止している．

⑵インタフェース変換機能

カード情報をFeliCaチップに書き込む際，iD向けスマフォGWサーバの後続システムとなるカード情報等サーバ（ドコモクレジットカードシステム（CREMO：Credit Mobile Gateway System），カード情報ダウンロードセンタ，ブランドダウンロードセンタ）向けの通信をいったん取りまとめ，端末アプリからの要求に応じて各システム間インタフェース電文を発行し，制御する．

iD向けスマフォGWサーバにて，オープンOS端末用端末アプリからのインタフェース電文をフィーチャーフォン向けインタフェース電文と同形式に変換することで，iD向けスマフォGWサーバの後続システムへの改修範囲を最小限に抑えている．これにより，コストの低減・開発期間の短縮を図った．

⑶シーケンス管理機能

オープンOS端末からの要求をセッション[*6]情報として保持し，不正な端末からの割込みが発生することを防いでいる．クレジットカード情報書込みの操作が，端末アプリケーションからの複数のインタフェース電文で構成される場合，管理情報（IPアドレス・パスワードなど）の連携情報をiD向けスマフォGWサーバにて保持し，1セッションが完了するまでもちまわる．端末アプリケーションからのインタフェース電文が規定された順番で連携されなかった場合はシーケンスエラーとし，不正なアプリケーションからの割込みが発生することを防ぐ．

⑷アクセス制限機能

iD向けスマフォGWサーバは，オープンOS端末からアクセス可能なシステムであるため，DoS（Denial of Service）攻撃[*7]などを受けるリスクがある．一般的なセキュリティ防御策は施してあるが，特定ユーザからのセキュリティ攻撃に備え，アクセス制御を行うブラックリスト機能を有する．また，サービス導入前の機能確認のため，特定のオープンOS端末からのみアクセス可能とするホワイトリストの機能も，併せて有している．

3.2　端末アプリケーション

端末アプリケーションは，FeliCaチップにエリアを確保し，複数のカードを管理するためのアプリケー

＊6　**セッション**：サーバとクライアントとの間の通信の意味のあるまとまり．ここでは，カード情報書き込みシーケンスの一連の通信をまとめて，セッションとして扱う．
＊7　**DoS攻撃**：対象のサービス停止を引き起こす悪意ある攻撃．

ションである．最大2枚のカードを管理することができ，エリアの発行，カードの追加，削除などの機能を有する．

オープンOS端末用アプリケーションの特徴としては，2章に記載のとおり仲介サーバを設け，カード情報などは仲介サーバ上に一時蓄積することでセキュリティの確保を行っている．

端末アプリケーションは、主に次の2つの機能を有する．

⑴FeliCaチップ更新・参照機能

本機能では，FeliCa搭載オープンOS端末に対し，エリアの発行，削除，カード情報の追加，削除，更新，メインカードの変更，カード情報の預入／引出など，FeliCaチップへのアクセス全般を行い，ユーザがオープンOS端末で決済を利用可能な状態にする．本機能を実現するにあたり，フィーチャーフォンでは端末にカード情報を送信し，端末アプリケーション側でFeliCaチップへ書き込む処理をしていたが，2章ならびに3.1節で記載のとおり，オープンOS端末では端末のメモリ上の情報を改ざんされる可能性がある．そのため，今回はクレジットカード情報を端末アプリケーションに送信せず，iD向けスマフォGWサーバでカード情報を終端させることで，オープンOS端末のメモリにクレジットカード情報を展開することなく，FeliCaチップへ直接クレジットカード情報を書き込む方式とした．具体的なシーケンスの比較を，**図3**および**図4**に示す．

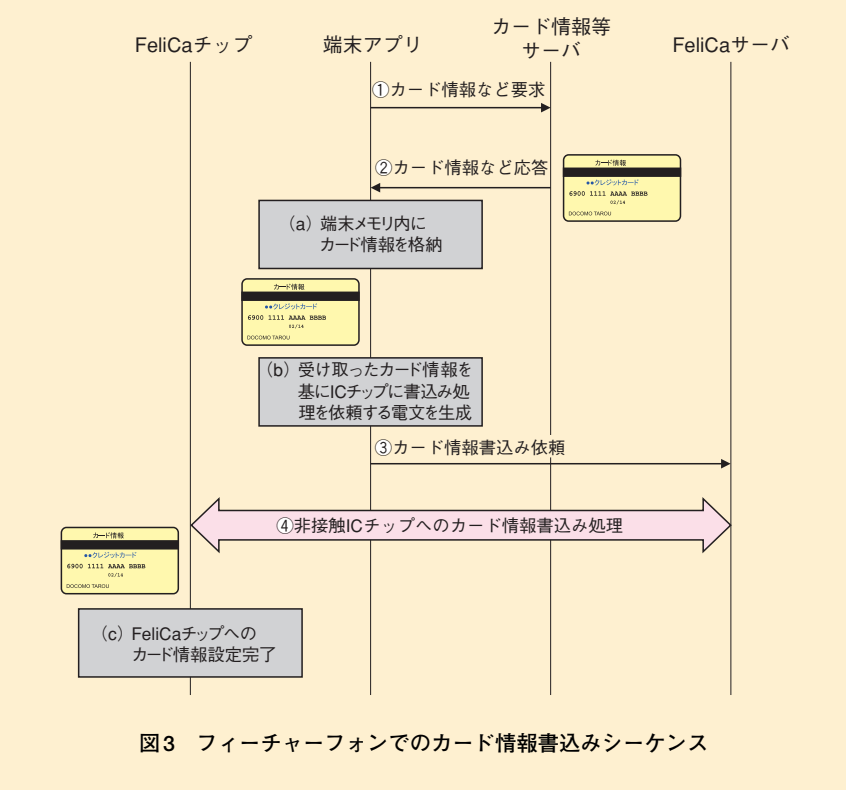


図3　フィーチャーフォンでのカード情報書込みシーケンス

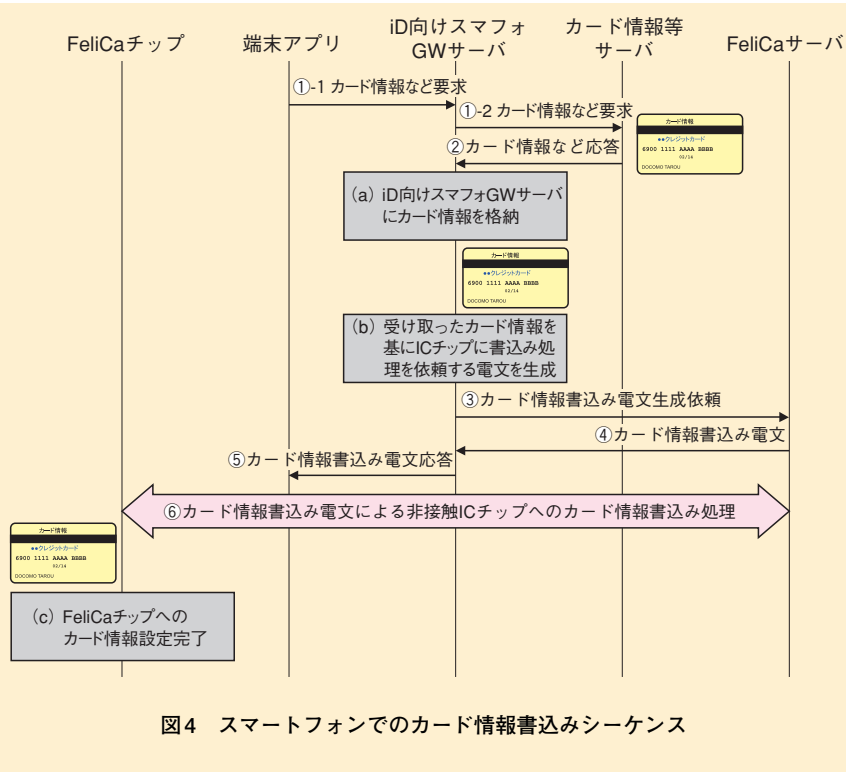


図4　スマートフォンでのカード情報書込みシーケンス

⑵カード会社ごとの固有情報表示機能

端末アプリケーションでは，最大2枚のカード情報を管理することができるが，カード会社ごとに端末アプリケーション内で表示する文言や会社のロゴなどを変更する必要がある．カード会社ごとの固有情報表示機能は，カード情報を設定する際に，カード情報等サーバから各カード会社向けの文言・画像データなどを取得することで実現している．本機能は，すでにフィーチャーフォン向けに提供してきたシステムを最大限に有効活用するために，3.1節⑵で記載のとおり，アプリケーションからのインタフェース電文をフィーチャーフォン向けインタフェース電文と同形式に変換することで，改修範囲を最小限に抑えて実現した．

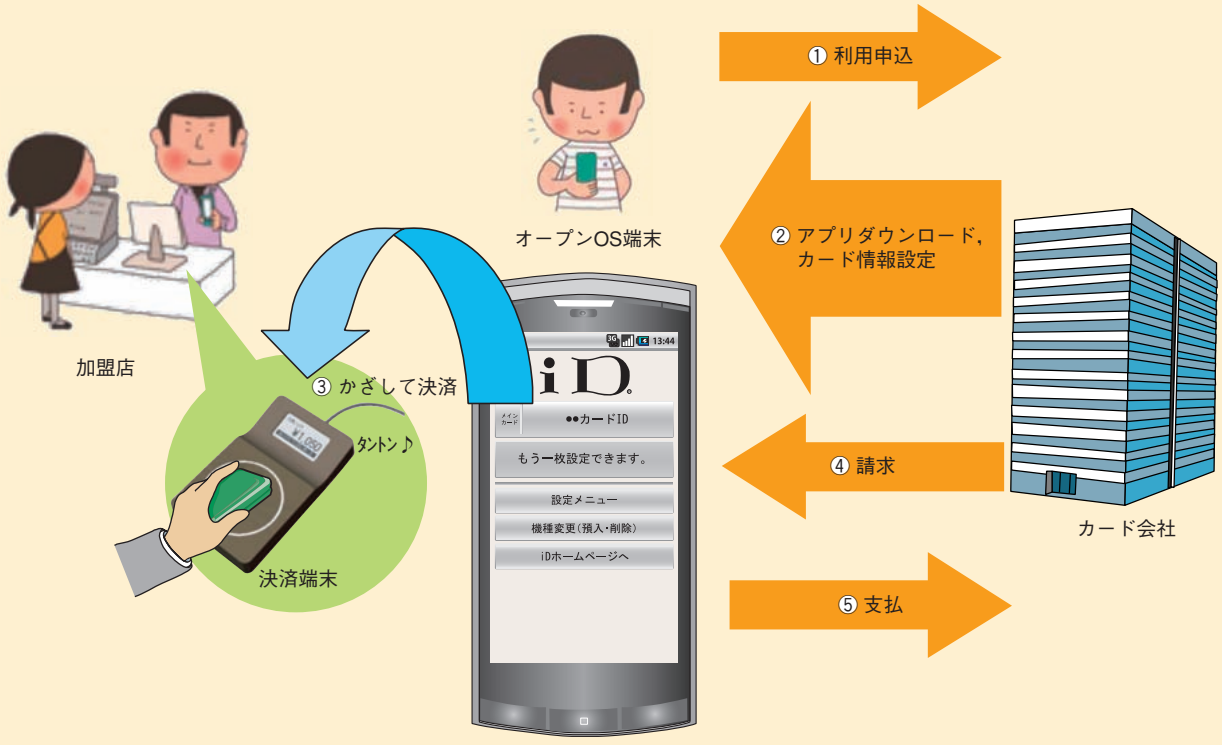
3.3 その他セキュリティ確保に関する事項

現在，端末アプリケーションからiDの設定を行うためには，spモードの3G網経由でのアクセスを必須としている．

無線LANなど他のベアラ[*8]からのアクセスを規制しているのは，オープンOS端末向けアプリケーションでは仲介サーバ（iD向けスマフォGWサーバ）を経由しているが，その仲介サーバのIPアドレスを偽装するDNS（Domain Name System）[*9]サーバが存在した場合，偽装サーバにパスワードなどを盗みとられ，その盗みとったパスワードなどから，不正なカード情報を設定される恐れがあるためであり，無線LANなど他ベアラからのアクセスを制限することとした．

4. サービスイメージ

オープンOS端末上で実現したクレジットサービスのサービスイメージを**図5**に，端末アプリの画面イメージを**図6**に示す．ユーザは，

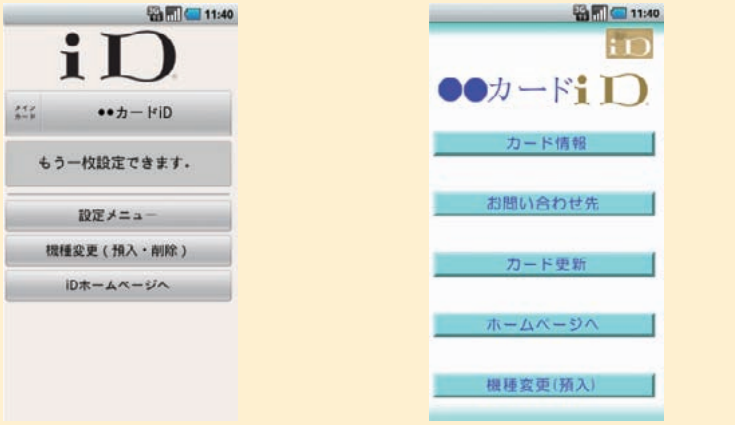


※「iD」ならびにiDのロゴは，NTTドコモの商標または登録商標．

図5　サービスイメージ

＊8　**ベアラ**：情報を伝達する通信回線．

＊9　**DNS**：IPネットワーク上のホスト名とIPアドレスの対応付けを行うシステム．



（a）端末アプリケーショントップページ　（b）カード会社ごとの固有情報表示

図6　端末アプリ画面イメージ

フィーチャーフォン・オープンOS端末を意識することなく，非接触ICクレジットサービスを利用可能となっている．

5. あとがき

本稿では，フィーチャーフォンで実現したセキュリティレベルを保ちつつ，既存システムを改修する際のインパクトを抑えた，オープンOS端末に対応したクレジットサービスの開発について解説した．今後は，オープンOS端末上のアプリケーションの自由度を生かしたサービスを検討・実現していきたいと考えている．