CAPIF　SEAL　API

3GPPにおける産業用アプリケーション連携に向けたフレームワークの標準化

ネットワーク開発部　鈴木（すずき） 悠司（ゆうじ）

近年，自動運転やドローン，スマートファクトリーなど，さまざまな産業におけるモバイルネットワークの活用が注目されている．3GPP TSG SA WG6では，多様な産業用アプリケーションが3GPPネットワークを活用するためのソリューションを検討している．特に，Release 15で導入されたCAPIFとRelease 16で導入されたSEALは，多くの産業で共通的に利用できるサービスフレームワークとして期待されている．本稿では3GPP TSG SA WG6の活動概要と，CAPIF，SEALの技術仕様を解説する．

1. まえがき

高速・大容量，低遅延，多数端末同時接続を掲げる第5世代移動通信システム（5G）の導入や，IoT（Internet of Things）技術の発展，各種産業分野のデジタル化などにより，通信に限らない多種多様な産業分野でモバイルネットワークを活用することが期待されている．3GPP（3rd Generation Partnership Project）では，SCEF（Service Capability Exposure Function）[*1]やNEF（Network Exposure Function）[*2]のAPI（Application Programming Interface）[*3]によるネットワーク機能の提供に代表されるように，3GPPドメイン外のアプリケーションとの連携も視野に入れながら技術仕様を拡張してきた．

3GPP TSG SA WG6（以下，SA6）では，従来，ミッションクリティカル[*4]な通信に関するソリューションを中心に議論してきたが，Release 15以降はこれに加え，前述のような産業連携を念頭に置き，3GPPドメイン外のアプリケーションによる3GPP

＊1　SCEF：3GPPシステムがもつ機能の一部を3GPPドメイン外に提供するための論理ノード．主に4G向けのコアネットワークで利用される．
＊2　NEF：SCEFと同様に，3GPPシステムがもつ機能の一部を3GPPドメイン外に提供するための5Gコアネットワークの機能部．
＊3　API：アプリケーションから特定のサービスを利用するためのインタフェース．本稿では，特にRESTful APIを指す．

ネットワーク活用を支援する機能の仕様策定も視野に含めて活動している．その例として，Release 15では3GPPが提供するノースバウンドAPI*5に対する統一的なフレームワークであるCAPIF（Common API Framework）*6を策定し，Release 16では各種の産業用アプリケーションが共通的に利用できる機能を切り出したSEAL（Service Enabler Architecture Layer for Verticals）*7を導入した．

本稿ではSA6の活動概要を紹介し，その中で特に産業用アプリケーション連携の基礎となるCAPIF，SEALという2種類のサービスフレームワークを解説する．

2. 3GPP SA6の活動

3GPPでは，最上位のグループであるPCG（Project Coordination Group）*8の下，無線関連技術を検討するRAN（Radio Access Network）*9，サービス機能やシステム全体のアーキテクチャを検討するSA（Service and System Aspects）*10，コアネットワーク*11や端末のインタフェースや機能を検討するCT（Core Network and Terminals）*12という3つのTSG（Technical Specification Group）*13と呼ばれるグループで，仕様策定を分担している．各TSGはそれぞれ4～6のワーキンググループに細分化され，SA6はTSG SAの中で，特にミッションクリティカル関連のアプリケーションにかかわる機能やアーキテクチャを検討するワーキンググループとして，2014年に発足した．

SA6発足当初は，パブリックセーフティ*14分野での活用を念頭に置いたミッションクリティカルサービス（プッシュ・トゥ・トーク*15通信，ビデオ通信，データ通信）を対象として仕様検討を進めていた．その後，5Gの初期仕様の策定と同じRelease 15にて，3GPPが提供するノースバウンドAPIに対する統一的なフレームワークとしてCAPIFを策定し，Release 16以降もミッションクリティカルサービスに限らない各種サービスのフレームワークや，V2X（Vehicle-to-Everything）*16・ドローン*17・スマートファクトリー*18に代表される種々の産業分野におけるアプリケーションの活用について検討を開始するなど，対象を拡大してきた．現在では「Application Enablement and Critical Communication Applications」を議論対象として，3GPPネットワークを活用するアプリケーション向けのアーキテクチャを中心に仕様検討している［1］．

3. CAPIF

3.1 CAPIF導入の目的

CAPIFは，3GPPで提供する種々のAPIに対する統一的な枠組みを提供する目的で，Release 15にて導入された．3GPPでは前述のSCEF，NEFやMBMS（Multimedia Broadcast/Multicast Service）*19向けの機能部などが，サービスAPIを提供している．一方，これらのAPIの開発・利用に際しては，提供するAPIの発行や管理，セキュリティ関連の機能など，共通して考慮すべき課題があり，CAPIFはこのような共通的な課題を解決するためのフレームワークとしての役割を担っている．

3.2 CAPIFのアーキテクチャ

CAPIFの代表的なアーキテクチャを**図1**に示す．

(1)API invoker

API invokerは，CAPIF APIおよびサービスAPIの呼出し元である．ネットワークオペレータがもつアプリケーション，ネットワークオペレータ以外の他事業者がもつアプリケーションのいずれもAPI

＊4 ミッションクリティカル：サービスを継続的に提供できることが極めて重要であり，障害などによる中断が許されない，あるいは非常に大きな損害になり得るシステムを指す．
＊5 ノースバウンドAPI：APIを提供している装置から見て，上位のアプリケーションに対して提供しているAPI．
＊6 CAPIF：ノースバウンドAPIを提供するための共通的な機能をまとめた3GPPのフレームワーク．
＊7 SEAL：3GPPネットワークを利用する複数の産業用アプリケーションで共通的に利用する機能をまとめた層．
＊8 PCG：3GPPの最高意思決定機関．3GPP活動全体の計画や進捗管理などを行う．
＊9 RAN：3GPPにおいて，コアネットワークと端末の間に位置する，無線レイヤの制御を行う基地局などで構成されるネットワークに関する仕様化を行っているグループ．
＊10 SA：3GPPにおいて，サービス要求条件，アーキテクチャ，セキュリティ，コーデック，ネットワーク管理に関する仕様化を行っているグループ．
＊11 コアネットワーク：交換機，加入者情報管理装置などで構成されるネットワーク．移動端末は無線アクセスネットワークを経由してコアネットワークとの通信を行う．

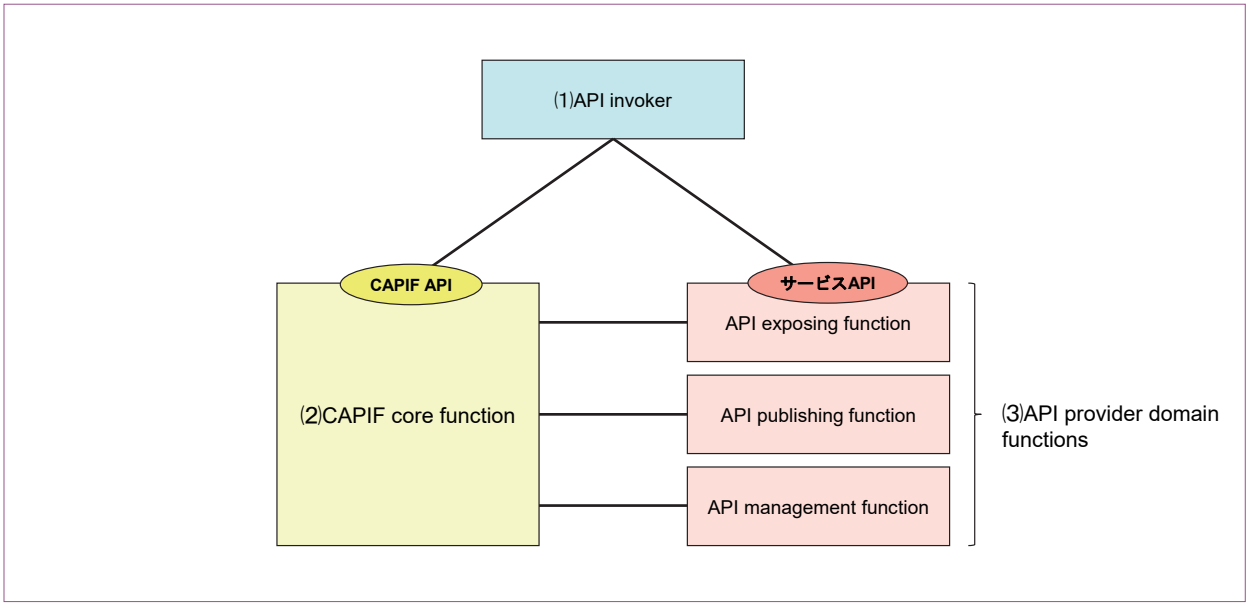

図1　CAPIFのアーキテクチャ

invokerになり得る．

(2)CAPIF core function

CAPIF core functionは，API invokerの認証・認可やAPIの登録，ポリシーの管理など，CAPIFで提供する各種機能において中心的な役割を担う．これらの機能はAPIとして提供され，API invokerをはじめとする各機能部はこのAPIを呼び出すことで機能を利用できる．CAPIF core functionは，モバイルネットワークオペレータが信頼できるドメイン内に配置される．

(3)API provider domain functions

「API exposing function」「API publishing function」「API management function」の3機能部は，総称してAPI provider domain functionsと呼ばれる．CAPIFでは，CAPIF core functionの提供者をCAPIFプロバイダ，API provider domain functionsの提供者をAPIプロバイダと定義しており，両者は別々の事業者でも同一の事業者でもよい．

API exposing functionは，API invokerからのサービスAPI呼出しを受け入れる機能部である．API publishing functionは，サービスAPIをAPI invokerが利用できるようするために，CAPIF core function宛にサービスAPI情報を発行（publish）する役目を担う．最後に，API management functionは，発行されたサービスAPIの管理を担い，サービスAPI呼出しログの監査やサービスAPIの状態の監視などの機能をもつ．

3.3　CAPIFの主な機能

ここではCAPIFの代表的な機能として，API invokerのオンボーディング，サービスAPIの発見，API invokerの認証・認可の3機能に絞って解説する．これらの機能は，API invokerがサービスAPIを利用する前段階として重要な機能である．その他の詳細な機能については文献［2］を参照されたい．

＊12 CT：3GPPにおいて，コアネットワーク内，および移動端末とコアネットワーク間のプロトコルの仕様化を行っているグループ．
＊13 TSG：3GPPにおいて，技術仕様の策定を担うグループ．
＊14 パブリックセーフティ：警察，消防，救急のような公共の安全のためのサービス．
＊15 プッシュ・トゥ・トーク：トランシーバのように，ボタンを押している間だけ発信ができる音声通信の方式．
＊16 V2X：車両と車両，車両と路上の物体（信号機など）のように，車両と周囲の環境の間で通信できるようにする技術．
＊17 ドローン：人が搭乗して操縦しない航空機のこと．UAV（Uncrewed Aerial Vehicle）とも言う．3GPPではドローン関連の機能を含むシステムをUAS（Uncrewed Aerial System）と呼ぶ．
＊18 スマートファクトリー：IoTなどの通信技術を活用した工場システム．3GPPでは特にFF（Factories of the Future）と呼ぶ．
＊19 MBMS：3GPPシステムで提供する1対多型（ブロードキャスト・マルチキャスト）の通信サービス．

⑴API invokerのオンボーディング

API invokerは，サービスAPIの呼出しを要求するにあたり，事前に自身の情報をCAPIF core functionに提供し，承認してもらわなければならない．この手順をオンボーディングと言う．オンボーディングに成功すると，API invokerは以後の認証・認可に必要な情報を受け取ることができる．

オンボーディングによりCAPIF core functionはAPI invokerを認識し，この手順で取得した情報を使って，API invokerの認証・認可ができるようになる．また，CAPIF core functionはこのオンボーディングの中で，API invokerが呼び出せるサービスAPIの情報を送ることもできる．

⑵サービスAPIの発見

API invokerが呼び出せるサービスAPIの情報については，前述のオンボーディング手順の中でCAPIF core functionから提供されるのを待つだけでなく，API invoker自身がCAPIF core functionに問い合わせることもできる．この問合せによりサービスAPI情報を取得する手順を，サービスAPIの発見（discovery）と言う．

API invokerが自身の識別情報とともに，発見したいAPIの条件をCAPIF core functionに送信すると，CAPIF core functionは保管しているAPI情報の中から条件に一致するAPIを取得する．CAPIF core functionはまた，特定のカテゴリのAPIを発見の対象から外すなど，取得したAPIの情報を自身の発見ポリシー（discovery policy）に従ってさらに選別することができる．このようにして得られたサービスAPIの一覧をAPI invokerに送信することで，API invokerは目的のサービスAPIの情報を得ることができる．

⑶API invokerの認証・認可

目的のサービスAPIの情報を取得したAPI invokerは，そのサービスAPIの呼出しにあたって認証・認可のプロセスを経る必要がある．API invokerとAPI exposing functionの間でどのような認証・認可の手法（以下，セキュリティメソッド）を採用するかを，両者がどのセキュリティメソッドをサポートするかなどの情報に基づいて，事前にAPI invokerとCAPIF core functionの間で決定する．セキュリティメソッドの種類としては，「TLS-PSK（Pre-Shared Key Ciphersuites for Transport Layer Security）＊20の利用」，「PKI（Public Key Infrastructure）＊21の利用」，「TLSとOAuth＊22トークン」の3種類が規定されている［3］．なお，このようなセキュリティ関連の詳細な仕様策定は3GPP TSG SA WG3（SA3）が担っている．

利用するセキュリティメソッドの決定後，API invokerはサービスAPIを呼び出す前段階として，あるいはサービスAPIの呼出しと同時にAPI exposing functionに認証・認可を要求する．API exposing functionは，必要に応じてCAPIF core functionと連携しながら，あらかじめ決定したセキュリティメソッドに基づいてAPI invokerの認証・認可を行う．このようなセキュリティの仕組みを統一的に提供することもCAPIFの重要な役割の1つである．

4. SEAL

4.1 SEAL導入の目的

SEALは，3GPPネットワークを利用する複数の産業用アプリケーションで共通的に利用する機能をまとめた層である．3GPPではV2X・ドローン・スマートファクトリーなど，ある特定分野のサービス・製品を提供する業界や企業の集合をバーティカルドメイン，あるいは単にバーティカルと呼ぶ．各バーティカルアプリケーションはそれぞれの要求条

＊20 TLS-PSK：事前に共有した鍵（PSK）を利用して，通信を暗号化するTLSコネクションを確立する方法．

＊21 PKI：暗号技術に用いる公開鍵の登録者を証明する仕組み．公開鍵基盤とも言う．本稿では，特にPKIを利用してTLSコネクションを確立する方法を指す．

＊22 OAuth：アクセス権限の認可を行うための標準仕様．本稿では，特にIETF RFC（Internet Engineering Task Force Request for Comments）6749で規定されたOAuth 2.0を指す．トークンと呼ばれるデータを発行してアクセス権限を制御する．

件に応じて必要な機能を実装するが，中には複数のバーティカルアプリケーション間で共通して必要となる機能もある．そのような機能をSEALとしてまとめて提供することで，バーティカルアプリケーションごとに個別に実装する必要がなくなり，効率的なシステム開発につながる．

4.2 SEALのアーキテクチャ

SEALの代表的なアーキテクチャを**図2**に示す．

SEALは，クライアント側の機能を担うSEALクライアントと，サーバ側の機能を担うSEALサーバからなる．両者は互いに通信することで位置情報管理やグループ管理などの機能を実現する．SEALサーバは3GPPネットワークシステムが提供する機能（例えば，NEFが提供するAPI）を利用することができる．なお，特定のSEALの機能に着目する場合，SEALクライアント・SEALサーバはその機能に従った名前で呼ばれることがある（例えば，位置情報管理のためのSEALサーバは特にLocation management serverと呼ばれる）．

SEALの上位にはVAL（Vertical Application Layer）が位置づけられる．このVALが，各バーティカルに特有のアプリケーション（例えば，V2Xアプリケーション）が乗る層であり，VALクライアント・VALサーバは，下位層のSEALクライアント・SEALサーバと通信することで，SEALが提供する機能を利用することができる．

4.3 SEALの主な機能

ここではSEALの代表的な機能として，位置情報管理，グループ管理，ネットワークリソース管理の3機能に絞って解説する．SA6では各バーティカル向けに個別のソリューションも検討しているが，それらの検討の中でも上記3機能の活用は特にさかん

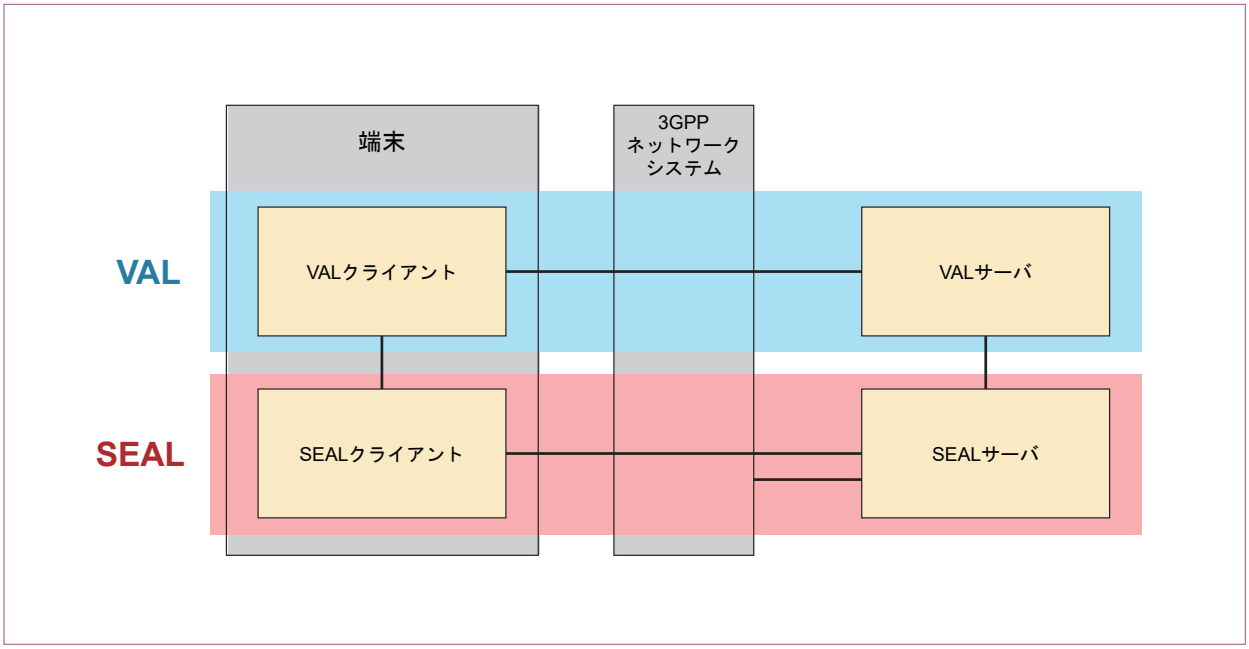

図2　SEALのアーキテクチャ

に議論されている．その他の詳細な機能については文献［4］を参照されたい．

⑴位置情報管理

位置情報管理を担うSEALクライアント・サーバはそれぞれLocation management client/serverと呼ばれる．位置情報管理機能では，VALサービス利用者の位置に関する情報を取得できる．

例えば，VALサーバが特定のVALサービス利用者の位置情報を特定したいとき，VALサーバはLocation management serverに対して位置情報報告の動作を開始するための信号として，位置情報報告トリガ（Location report trigger）を送信する．この信号を受け取ったLocation management serverは，Location management clientに位置情報を問い合わせ，受け取った位置情報をVALサーバに送信する．

VALサーバからだけでなく，ある端末から別の端末の位置情報を特定することも可能である．例えば，Location management client Aが実装されている端末の位置情報を知りたいとき，その端末とは別の端末上に実装されているLocation management client Bは，Location management serverに対して位置情報報告トリガを送信することができる．前述の例と同様に，位置情報報告トリガを受け取ったLocation management serverは，Location management client Aに位置情報を問い合わせ，受け取った位置情報をLocation management client Bに送信する．これにより，目的の端末の位置情報を取得することができる．

位置情報を取得するタイミングについても，目的に合わせて変更できる．具体的には，VALサーバまたはLocation management clientが特定のVALサービス利用者の位置情報を取得するとき，位置情報報告トリガを送信した直後に位置情報を受け取ることも，あるいは特定の条件を設定して，その条件が満たされたタイミングで位置情報を受け取る（例えば，一定時間おきに位置情報を受け取る）ことも可能である．また，Location management serverは，Location management clientから直接位置情報を受け取るだけでなく，3GPPネットワークから端末の位置情報を受け取り，その情報をVALサーバなどに送信することも可能である．

⑵グループ管理

グループ管理を担うSEALクライアント・サーバはそれぞれGroup management client/serverと呼ばれる．グループ管理機能では，複数のVALサービス利用者からなるグループの作成や，そのグループ内のメンバの管理などができる．

例えば，グループ作成権限をもつVALサービス利用者が新しくグループを作成したいとき，そのVALサービス利用者のGroup management clientはGroup management server宛にグループ作成要求（Group creation request）を送信する．このとき，同一グループ内に含めたいユーザの識別情報も一緒に送信する．この要求に基づいてGroup management serverは新規グループを作成する．グループ作成後，Group management clientからGroup management serverにグループ情報問合せ要求（Group information query request）を送信することにより，作成したグループに関する情報を取得することができる．また，Group management clientはGroup management serverに対して，グループメンバーシップ更新要求（Group membership update request）を送信することで，グループのメンバを追加・削除することもできる．

前述した位置情報管理機能と組み合わせて使うことで，位置情報ベースのグループ作成も可能である．このとき，Group management serverは，特定の

位置情報の中に存在するユーザのリストをLocation management serverに要求して取得し，そのリスト内のユーザでグループを作成する．このように，SEALの複数の機能を利用してサービスを提供することもできる．

⑶ネットワークリソース管理

ネットワークリソース管理を担うSEALクライアント・サーバは，それぞれNetwork resource management client/serverと呼ばれる．ネットワークリソース管理の具体的なユースケースとして，VALサービスの要求条件に応じたQoS（Quality of Service）[*23]の適用などができる．

目的のQoSを得たい場合，VALサーバはNetwork resource management server宛に特定の端末（もしくは複数端末からなるグループ）に対するネットワークリソース適応要求（Network resource adaptation request）を送信する．これに基づき，Network resource management serverは，目的の端末ないし端末グループにネットワークリソースを割り当てる．Network resource management serverは，PCF（Policy Control Function）[*24]などの3GPPシステムとも接続し，要求に基づいてPCC（Policy and Charging Control）プロシージャ[*25]を開始する．これにより，各VALサービスの要件に応じたQoSを適用することが可能になる．

5. あとがき

本稿では，3GPP SA6の活動概要と，そこで標準化され，産業用アプリケーションと3GPPシステムとの連携における役割が期待されるCAPIFとSEALという2種類のフレームワークについて解説した．CAPIFはRelease 15で，SEALはRelease 16で導入されて以降，今も継続的に拡張が議論されており，ドコモも機能拡張の検討に貢献している．また，Release 17以降では，エッジコンピューティング[*26]実現のためのアーキテクチャや，V2X・ドローン・スマートファクトリーといった個々の産業向けのサービスに特有な技術仕様も検討されている．現在，SA6ではRelease 18の技術検討を開始した段階であり，ドコモはさらなる産業用アプリケーションのユースケースを見据えながら，3GPP SA6での標準化活動を推進していく．

文　献

［1］ 3GPP SP-210265：“Terms of Reference (ToR) for 3GPP TSG SA WG6 (SA6),” Mar. 2021.

［2］ 3GPP TS23.222 V17.5.0：“Functional architecture and information flows to support Common API Framework for 3GPP Northbound APIs; Stage 2,” Jun. 2021.

［3］ 3GPP TS33.122 V16.3.0：“Security aspects of Common API Framework (CAPIF) for 3GPP northbound APIs,” Jul. 2020.

［4］ 3GPP TS23.434 V17.3.0：“Service Enabler Architecture Layer for Verticals (SEAL); Functional architecture and information flows,” Sep. 2021.

＊23 QoS：通信サービスの品質．帯域幅や遅延などが代表的な指標となる．

＊24 PCF：QoSなどのポリシー制御や，課金制御を担う5Gコアネットワークの機能部．

＊25 PCCプロシージャ：ポリシー制御や課金制御に関連する一連の処理．Network resource management serverからの要求は，PCCプロシージャによって3GPPシステム内部にも反映される．

＊26 エッジコンピューティング：端末に近い場所で計算処理を行うサービスの形態．通信における遅延の短縮や，ネットワーク負荷の分散などの効果が期待される．