

ドコモのパブリッククラウド活用と CCoEの果たす役割

イノベーション統括部

DOCOMO Innovations, Inc.

もりや ひろき もり たけし
 守屋 裕樹 森 健史
 なおい やすひろ
 直井 康広

ドコモでは、10年以上前からパブリッククラウドを用いた数多くのサービスを提供している。パブリッククラウドの活用においては、CCoEが中心となってより効率的かつ適切に行われるように活動を続けてきている。本稿では、それらの活動やドコモにおけるパブリッククラウド利用体制を、昨今のクラウドにおける開発トレンドと合わせて解説する。

1. まえがき

企業や組織におけるパブリッククラウド^{*1}の利用が急速に増加しており、「クラウドファースト」という言葉で代表されるように、パブリッククラウドを活用した事業展開が一般的になってきている。同時に多くの企業や組織にとって、オンプレミス^{*2}にはないパブリッククラウドの迅速性や柔軟性をうまく活用して自社のビジネスを展開、あるいは変革していく必要が出てきている。しかし、パブリッククラウドの活用においては、従来からあるオンプレミス型のITシステムの構築や運用とは違った考え方が求められることも多く、スムーズな導入や活用が

できない企業や組織も少なくない。

一般的にパブリッククラウドの利用にあたっては、導入時のサービス検証、セキュリティ対策、利用ポリシーの策定、社内における利用体制の確立、スキルの獲得、人材育成、変化の早いクラウドの情報収集やノウハウの展開といった課題に対応していくこととなる。パブリッククラウドをうまく活用するためには、従来からあるオンプレミス型のITシステムの考え方との違いを認識し、変化の早いパブリッククラウドに積極的に追従していくことが重要となる。

ドコモにおいても、10年以上前から数多くのサービスでパブリッククラウドを活用している。それを通じて、前述したような課題にも向き合い、より効

©2021 NTT DOCOMO, INC.

本誌掲載記事の無断転載を禁じます。

本誌に掲載されている社名、製品およびソフトウェア、サービスなどの名称は、各社の商標または登録商標。

*1 パブリッククラウド：インターネットを介して誰でも利用ができるクラウドコンピューティングサービス。

*2 オンプレミス：企業がシステムを構成するハードウェアを自社で保有し、自社で保守運用すること。

率的かつ適切にパブリッククラウドを活用するための活動を続けてきた。本稿では、ドコモで実施してきたそれらの活動やドコモにおけるパブリッククラウド利用体制を解説する。

2. ドコモにおけるパブリッククラウド利用

2020年12月時点での、ドコモにおけるパブリッククラウドの利用状況を解説する。

2.1 パブリッククラウドの利用規模

ドコモでは、2009年ごろに研究開発・検証目的でパブリッククラウドの利用を開始した。その後、利用範囲を拡大し、2012年から大規模商用サービスで、パブリッククラウドを採用した。利用開始時から毎年利用量は増加しており、2020年12月時点では、900

以上のAWS（Amazon Web Services）^{*3}のアカウント、250以上のGCP（Google Cloud Platform）^{*4}のプロジェクト、50以上のMicrosoft Azure^{*5}（以下、Azure）のサブスクリプションをそれぞれ運用している。

2.2 パブリッククラウドの活用範囲

ドコモにおけるパブリッククラウドの活用範囲は、多岐にわたっている。例えば、Webサービス、モバイルアプリケーションのバックエンドシステム^{*6}、データ分析基盤、機械学習、社内向けシステムなどの多くの分野でパブリッククラウドを活用している。

2.3 パブリッククラウドの利用体制

ドコモでは、パブリッククラウドを効率的に活用できるように考慮した利用体制を整えている（図1）。ドコモにおけるパブリッククラウド利用で最も特徴

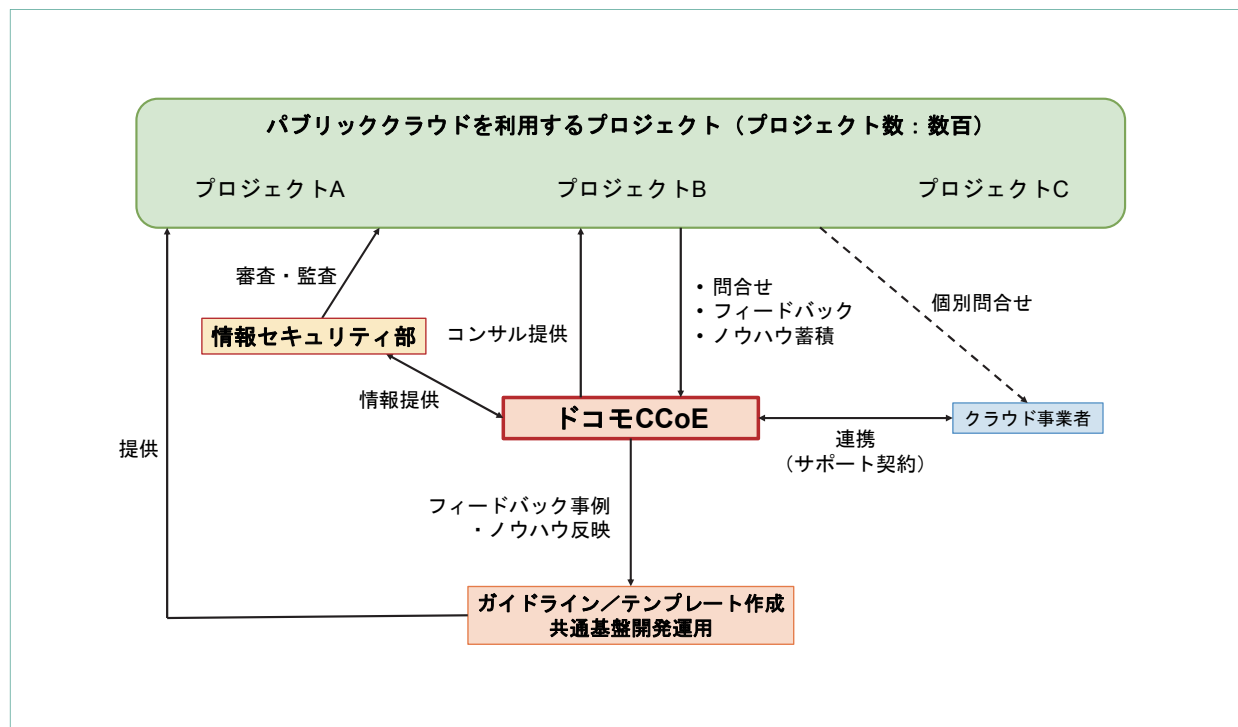


図1 ドコモのパブリッククラウド利用体制

*3 AWS：Amazon Web Services社が提供するクラウドコンピューティングサービス。

*4 GCP：Google社が提供するクラウドコンピューティングサービス。

*5 Microsoft Azure：Microsoft社が提供するクラウドコンピューティングサービス。

*6 バックエンドシステム：利用者のモバイル端末やコンピュータで動作するのではなく、サーバなどで集中的に動作させるシステム。

的な点は、明確なCCoE（Cloud Center of Excellence）^{*7}が存在することである。CCoEとは、パブリッククラウドに関する多様な専門知識をもったチームであり、ドコモではこのCCoEを中心にパブリッククラウドの活用を進めてきている。

3. ドコモCCoEの活動

ドコモのパブリッククラウド利用体制において中心的な役割を担っているCCoEの活動の詳細について解説する。

3.1 コンサルティングの提供

パブリッククラウド利用時の支援はCCoEの重要な役割である。社内プロジェクトにおいて、CCoEはパブリッククラウド上でシステムを構築する際のシステム設計支援やレビュー、セキュリティ要件を満たすための効率的な対策方法の提示などを行う。特にパブリッククラウドにおいては、最初の設計が重要で、後のコストやシステム運用業務に大きな影響を与えるため、システム設計時に支援を行うことが多い。

また、システムの運用を開始して、システムの利用が増えてくると必然的にコストも増大していく。その際にコスト最適化を行うために、コスト要因の把握や設計見直しなどの支援も実施している。

3.2 クラウドコストの取りまとめと最適化

一般的に、パブリッククラウドは柔軟な利用ができる一方で、サービス数や購入オプションの拡大に伴い、費用支払いや会計処理などが煩雑になりやすく、プロジェクトが増えた際に、稼働が増大してしまう場合がある。そこでドコモでは、CCoEが、一元的にクラウド事業者との契約を行い、一括で各プロジェクトの支払いを取りまとめて処理をすることで、各プロジェクトの負担を軽減させている。

また、一括支払いには、事務処理負担の軽減のほかにもメリットがある。パブリッククラウド事業者によっては、利用量が多くなるほど、価格が安くなるボリュームディスカウントオプションがある。支払いをまとめることで、ボリュームが確保され、社内全体で利用料を抑えることが可能になる。

3.3 最新情報の収集と展開

パブリッククラウドの進化は早く、最新の情報を常に追いかける活動は、プロジェクト業務を抱える各プロジェクトのメンバでは難しい場合がある。そこで、最新情報の取得もCCoEにて率先して実施している。例えば、パブリッククラウドに関する技術的なイベントには積極的に参加して、情報収集や発表を行っている。また取得した情報は、ノウハウとしてガイドラインへ反映したり、自ら検証を行い、社内プロジェクトメンバへ展開したりするようにしている。

3.4 クラウド業務支援ツールの作成と展開

各プロジェクトがパブリッククラウドを効率的に活用できるように、さまざまな支援ツールを作成して、社内に展開している。

クラウドでは事業展開の速度を向上させる多様な機能が提供されているが、一方で使い方を誤るとクラウドの障害に伴うサービス停止や、設定誤りによるセキュリティ事故を引き起こす可能性がある。そのため、利用者には正しくクラウドを利用するための技術知識が必要となるが、利用者の知識レベルはまちまちであり、会社としては、社員全体の技術知識の底上げが課題となる。

このためCCoEは、ドコモ視点でのクラウド利用方法の記載を特徴とするガイドラインを作成している。本ガイドラインにより、仮に知識の乏しい利用者であっても、押さえておくべき最低限の知識が短時間で習得可能となる。ガイドラインはAWS、GCP、

^{*7} CCoE：企業においてクラウドの活用を成功させるために、ベストプラクティスの確立や必要な制度、ガバナンスなどを作成し、社内に展開していく専属のチーム。

Azureに対応している。ここではAWSを対象として作成したガイドライン一覧を表1に、ガイドラインの一部抜粋例を図2に示す。

また、ガイドラインの1つであるセキュリティデザインパターン^{*8}では、クラウドを利用してシステム構築する際のセキュリティ考慮漏れを抑制できるよう、情報セキュリティ部のセキュリティチェック

項目に沿った要件（ISO/IEC27017やJISQ27002など）と、クラウド環境における要件、AWSを用いてシステム構築を行う場合の要求仕様とAWSの提供機能・サービスを並記することで、セキュリティチェック項目への準拠性を高めている。システム構築担当者はセキュリティチェック項目を満たすために一点ずつ検証を行う必要はなくなり、利用に応じ

表1 ガイドライン一覧（AWS）

No	種 類	内 容
1	クラウド開発ガイドライン	クラウドを使う場合の考え方や作法、開発フローにおける各フェーズで考慮・実施すべき指針を記載、特に設計・セキュリティなどは重点的に網羅し、間違った使い方を抑止
2	セキュリティデザインパターン	クラウドを利用し、システムを構築するにあたり、セキュリティの考慮漏れを抑制。ISO/IEC27017に沿った要件をあらかじめ用意することで、ISO管理策に対する準拠性を高めている。AWSを利用したシステムを構築するにあたり、必要となるセキュリティ要件を列記
3	セキュリティテンプレート	セキュリティデザインパターンを考慮したネットワーク構成やネットワークフィルタリング機能、基本機能を提供するインスタンス群などを生成するAWS CloudFormationテンプレートを記載、セキュリティ対策を容易に実施
4	IAMデザインパターン	AWSアカウント利用パターンに合わせて、ドコモ社内のIAMポリシー設計のベストプラクティスを記載
5	インシデント対応ガイドライン	AWSを利用する、インターネットに公開されているサービス提供システムや、社内システムなどでサイバー攻撃などのインシデントが発生した場合の対応について、実際に発生した事例を含めて記載
6	コスト最適化ガイドライン	AWSコストを管理する者向けに、コストの把握・分析方法、コスト削減・最適化の手法を記載
7	システム移行ガイドライン	オンプレミスからAWSへの移行案件をスムーズに行うために、これまでの移行事例で得た知見などを基に移行時にポイントとなる点や注意すべき点を記載
8	共通基盤化ガイドライン	複数アカウント／複数システムを運用し始めると、運用を統一化したり、運用システムを共通化することで効率化を図ると有効な場合があり、クラウドの特性を利用することで、運用の効率化をスムーズに進める方法を記載
9	コンテナガイドライン	コンテナをサービス開発／運用に取り入れようとしている人向けに、各プロジェクトで効果的、安全にコンテナ活用を実践してもらうことを目的に、こういったツールをどのように利用するのがよいか記載
10	サーバレスガイドライン	AWS上でサーバレスなシステムを開発・運用する際に、どのように導入を進めていけばよいか、こういったサービスをどのように利用するのがよいか、各プロジェクトで効果的かつ効果的にサーバレスを活用する方法を記載
11	DevOpsガイドライン	DevOpsの考え方をサービス開発／運用に取り入れようとしている者向けに、こういったツールをどのように利用するのがよいか、各プロジェクトで効果的かつ効果的にDevOpsを実践してもらうことを目的としたガイドライン

IAM : Identity and Access Management

IEC : International Electrotechnical Commission

ISO : International Organization for Standardization

^{*8} セキュリティデザインパターン：セキュリティ要件に対して、パブリッククラウドを利用した際の実現方法を記載したガイドラインの1種。

設計・製造

それでは実際に設計・製造に入っていきます。
ここからはいよいよ設計・製造を行う際の**考え方**や**ノウハウ**を解説していきます！！

ポイントはこちら

● 単一障害点の排除
あらゆるものは**いつでも故障する前提**で設計する

● コンポーネントの疎結合化
コンポーネントは**独立**させ、各コンポーネントはブラックボックスとして設計する

● スケーラブルな構成
設計は**伸縮自在性**があり、**再起動が可能**であるものにする

● オートメーション
手動作業を極力削減する

● マネージドサービスの活用
サーバではなくサービスを利用して**運用負荷を削減**する

● 全レイヤでのセキュリティ
セキュリティはAWSと責任分担モデルのため、**すべてをAWSに任せない**

● 使い捨て可能リソース
いつでも増減可能な特性を利用してアプリケーションやバッチ処理の**並列化**を検討する

● ストレージの使分け
EBSやデータベース、S3などの**ストレージを使い分ける**

● コストの最適化
クラウド特性を活かしてコストを削減

● キャッシュの利用
繰り返し利用されるデータをキャッシュして**性能向上**させる

EBS : Elastic Block Store

図2 ガイドライン例（クラウド開発ガイドラインの内容抜粋）

でセキュリティデザインパターンを参照しながらシステム構築を実施すれば、おのずとセキュリティチェック項目を満たせるようになる。セキュリティデザインパターンの一部抜粋例を図3に示す。

パブリッククラウドの機能追加やアップデートのスピードは早いので、これらの支援ツールも頻繁にアップデートをする必要がある。そのため、CCoEでは、これらのツール開発においてもアジャイル開発^{*9}を取り入れ、頻繁な機能追加やアップデートに追従していく活動も行っている。

4. ドコモにおける最新の開発トレンド

ここでは、ドコモの最新の開発現場から、サーバレス技術を適用した最新の開発事例を解説する。

4.1 サーバレス技術の登場

クラウドの世界ではこれまで別々だった開発とオ

ペレーションを分離せず、それらを統合して生産性を高めるいわゆるDevOpsの流れとともに、従来の仮想マシン^{*10}からコンテナ^{*11}の利用を前提とした方式設計が普及した。コンテナ化においては開発やリリースサイクルを加速させることに成功したものの、依然として従来の仮想マシンと同様に運用監視やセキュリティのための保守運用が必要である。コンテナ化の流れの一方で、AWSをはじめとしたパブリッククラウド事業者は、ミドルウェア^{*12}からサーバの運用管理までを含む一連のマネージドサービス^{*13}を「サーバレス」技術としてすでに提供し始めている。これはコンテナ化とは別の軸で発展しているクラウドインフラ利用技術であり、開発者や運用管理者はサーバの存在を意識することなくインフラの運用管理をすべてクラウド事業者任せ、より多くのリソースをそのビジネスロジックの開発に集中することが可能である。

*9 アジャイル開発：迅速かつ適応的にソフトウェア開発を行う軽量なアプリケーション開発手法群の総称。

*10 仮想マシン：ソフトウェアによって仮想的に構築されたサーバなどのコンピュータ。

*11 コンテナ：コンピュータ仮想化技術の一種で、1つのホストOSの上にコンテナと呼ばれる専用領域を作り、その中で必要なアプリケーションソフトを動かす方式のこと。

*12 ミドルウェア：複数のアプリケーションから共通に利用される機能を提供するソフトウェア。

ISO/IEC27017またはJISQ27002		AWSセキュリティデザインパターン	
章番号	管理策	クラウド環境における要件	AWSを用いてシステム構築を行う場合の要求仕様とAWSの提供機能・サービス
12.1.4	開発環境、試験環境および運用環境は、運用環境への認可されていないアクセスまたは変更によるリスクを低減するために、分離することが望ましい。	- クラウド環境に構築するシステムは、商用、開発、試験、バックアップ環境ごとに分離した構成とすること - 可能であれば契約を分離する - ネットワークを分離する - など	【要求仕様】 - 商用、開発、試験、バックアップなどの環境を分離する際は、AWSのアカウントを別にする。難しい場合はVPCで分離する。 - 役割（DMZ、リモート接続ネットワークセグメント、内部サーバネットワークセグメント、など）に応じたネットワークセグメントをVPC機能やサブネット機能で分離する。
13.1.3	情報サービス、利用者および情報システムは、ネットワーク上で、グループごとに分離することが望ましい。	- クラウドはインターネットにさらされた構成となるが、ファイアウォールやルーティングにより論理的にネットワークを分離し、役割に応じたネットワークセグメントを構成できること - マルチテナント環境のサービスの場合、他の利用者や環境（商用、開発、など）に影響を受けず利用を分離可能であることを確認する -物理的に分離可能 -論理的に分離可能	【AWSの提供機能・サービス】 - AWSアカウントの用途ごとの割当てにより他のテナントと環境を論理的に分け、VPC機能によりネットワーク環境を論理的に分けることができる。 - さらに物理的に環境を分ける要件がある場合は、以下のどちらかを利用する。 -ハードウェア専用インスタンス -Dedicated Hosts - サブネット機能により、VPC内に複数の仮想サブネットを作成できる。それにより役割に応じたサブネットを構成することができる。 - VPCピアリングを利用することで2つのVPCを同じネットワーク内に存在するように扱うことができる。 【備考】 - Multi-AZ構成にすることで可用性を向上できる。
14.1.2	公衆ネットワークを経由するアプリケーションサービスに含まれる情報は、不正行為、契約紛争、並びに認可されていない開示および変更から保護されることが望ましい。	機能要件	
14.1.3	アプリケーションサービスのトランザクションに含まれる情報は、次の事項を未然に防止するために、保護されることが望ましい。 -不完全な通信 -誤った通信経路設定 -認可されていないメッセージの変更 -認可されていない開示 -認可されていないメッセージの複製または再生	機能要件	

DMZ : DeMilitarized Zone
 JIS : Japanese Industrial Standards
 VPC : Virtual Private Cloud

図3 セキュリティデザインパターン例（社外向けVersionではISO27017規格をベースに記載）

4.2 ドコモでのサーバレス適用開発事例

ドコモが2020年6月にリリースしたドコモオープンイノベーションクラウドのポータルサイトは、以下のようなReact^{*14}ベースの一般的なウェブアプリケーションシステムである（図4(a)）。

ドコモオープンイノベーションクラウドの開発にあたって最初のリリースまでの期間は4カ月、そして運用・保守要員は最小限に抑えるという制約があった。そこで可能な限りサーバ管理をAWSにオフロード^{*15}するため、AWS Lambda^{*16}などを利用したサーバレスアーキテクチャを全面的に採用して開発を行った（図4(b)）。その結果、開発期間を大幅に短縮し、短期間でリリースに成功した。

本稿執筆時点で運用開始から1年、ネットワークやサーバなどインフラを起因とした障害はゼロである。可用性においてサーバレスでは、冗長性や

フォールトトレランス^{*17}があらかじめビルトインされている恩恵を受けている。運用・保守要員は2〜3名と当初の目標を達成した。今後、ユーザアクセス増加によるスケーラビリティの確保が必要な局面でもサーバレスであれば自動で対応可能である。料金も使用した分だけ支払う従量課金であるため、本プロジェクトでは大幅なコスト削減を実現した。

5. あとがき

本稿では、ドコモにおけるパブリッククラウドの活用とCCoEの果たす役割について解説した。パブリッククラウドの利用は今後も増えることが予想される中で、それらをうまく利用し、ビジネスを成功に導くことが重要である。そのためにCCoEは今後もそれぞれのプロジェクトがパブリッククラウドを

^{*13} マネージドサービス：クラウドサービスのうち、リソースのプロビジョニングや運用の大半をクラウド事業者の責任で実施しているサービス。クラウドコンピューティングサービスのうち、特にPaaSやSaaSを指す。

^{*14} React：ユーザインタフェース構築のためのJavaScriptライブラリ。

^{*15} オフロード：システムやサービス、ネットワークの処理を別の同様のサービスに振り分け本来のサービスの処理を軽減すること。

^{*16} AWS Lambda：AWSが提供するFaaSの1つ。アプリケーションコードの実行環境が提供されており、利用者は作成したソースコードを登録してアプリケーションが実行できる。

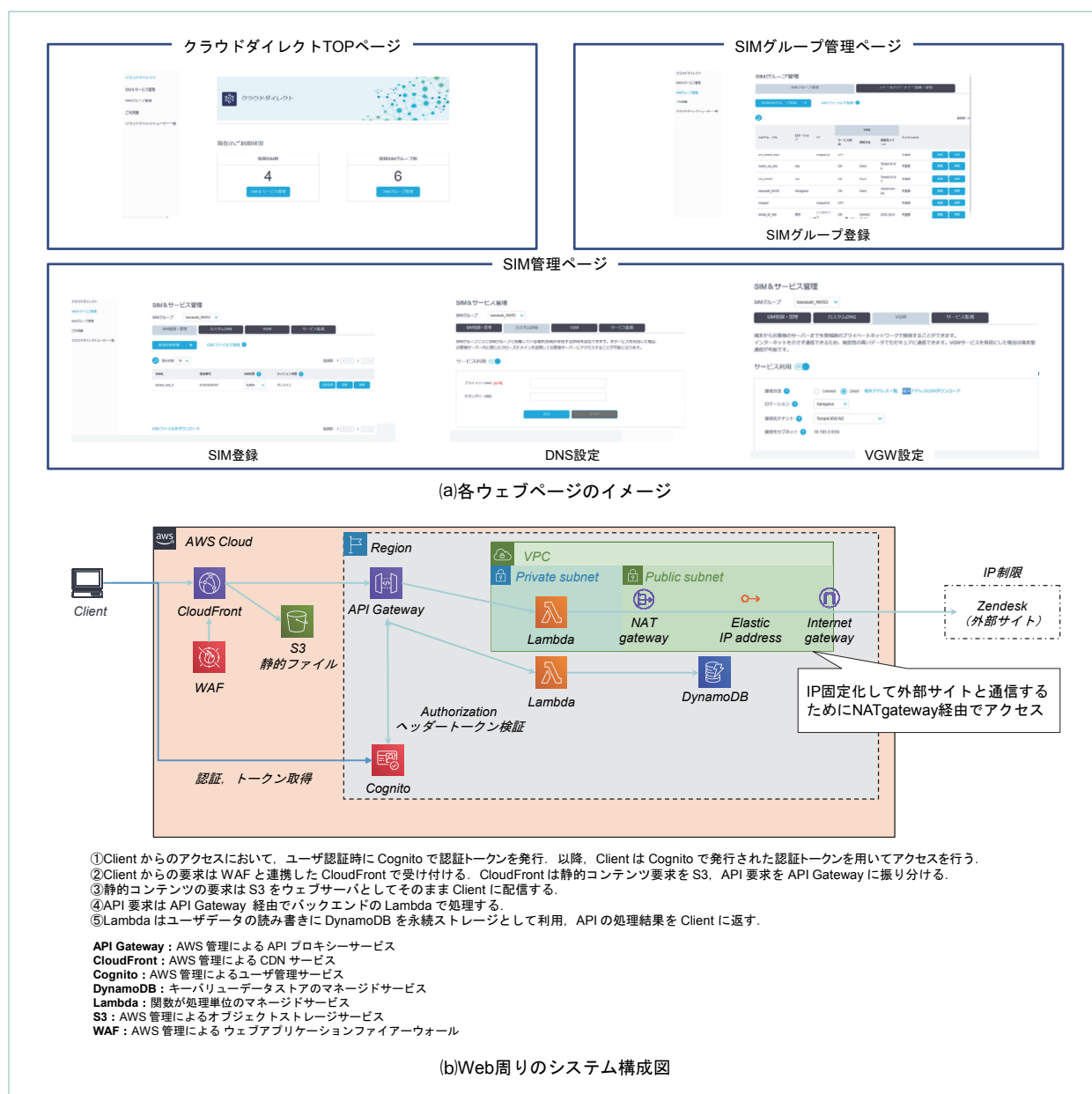


図4 ドコモオープンインペーションクラウド

最大限に活用できるように支援の範囲を広げていきたい。

また、サーバレスといった最新技術を商用サービスにいち早く導入・実践することは次世代のイノ

ベーションへの挑戦でもある。そのマインドを育てながら、今後もドコモ社内で開発の効率化を促進、成功事例を増やしていきたいと考えている。

*17 フォールトトレランス：システムに障害が発生した場合にも正常に機能し続けること。