docomo MEC™情報セキュリティポリシー

株式会社NTTドコモ

2022年7月1日(第3版)

目次

初めに

- docomo MEC™は、5G時代に求められる低遅延、高セキュリティなどMEC（Multi-access Edge Computing）の特長を持つMECサービスです。MEC基盤「Compute O」、「Compute V」、「Compute D」や当社のネットワークとMECをダイレクトにつなぐ「MECダイレクト」、その管理機能「ネットワーク・オン・デマンド」などを提供しています。
- docomo MEC™は、株式会社NTTドコモ（以下、「当社」と表記）の情報セキュリティポリシーおよびプライバシーポリシーを順守しています。本ドキュメントでは、docomo MEC™のセキュリティに対する考え方、対策と関連する機能の概要を紹介します。個別の機能の詳細はそれぞれのドキュメントをご参照ください。

docomo MEC™におけるセキュリティの考え方

セキュリティの考え方

- docomo MEC™では責任分担モデルを採用しています。詳しくは経済産業省の「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」及び「クラウドセキュリティガイドライン活用ガイドブック」をご参照ください。
- docomo MEC™では、仮想マシンインスタンスや仮想ネットワークなどのコンポーネント、またそれを作成するためのwebコンソールやAPIを、基盤IaaSサービスとして提供しています。
- 当社はdocomo MEC™において、HW運用保守（物理装置、ファシリティ）及び、基盤IaaSサービスの提供について、責任を有しています。

<table>
<tr><th>対策者</th><th colspan="2">対策対象</th><th></th></tr>
<tr><td rowspan="3">お客様</td><td rowspan="3">構築
システム</td><td>アプリ
ケーション</td><td rowspan="2">■ 構築システムのセキュリティを高めるために
システム構築者が対策する。</td><td rowspan="2">対策例
■ OSファイアウォール
■ アカウント管理
■ クライアントサイド暗号化　等</td></tr>
<tr><td>ミドルウェア</td></tr>
<tr><td>OS</td><td colspan="2">■ クラウド基盤が用意した機能（基盤サービス）を利用し、セキュリティを高める</td></tr>
<tr><td rowspan="4">ドコモ</td><td colspan="2">基盤サービス提供</td><td colspan="2">セキュリティグループ　スナップショット　Floating IP　等</td></tr>
<tr><td colspan="2">HW保守運用</td><td colspan="2" rowspan="3"> 
</td></tr>
<tr><td></td><td>物理装置</td></tr>
<tr><td></td><td>ファシリティ</td></tr>
</table>

- ユーザがwebコンソールを通じて作成したサーバーやインストールしたアプリケーション、保管したデータなどの「リソース及びコンポーネント」(以下、「ユーザリソース」と表記）は、事前に合意した利用規約の元で、ユーザが任意に変更・削除できます。ユーザーリソースは、ユーザーの責任によって管理することができます。docomo MEC™では、ユーザーリソースの内容、特性等については関知していません。なお、ユーザーリソースと外部間の通信につきましても、同様に内容、特性等について関知いたしません。ただし、ユーザリソースやdocomo MEC™に対して攻撃的通信が行われている場合あるいは、利用規約に反した使われ方が見受けられた場合においては、予告なくユーザリソースを削除する場合もあり、その限りではありません。

docomo MEC™におけるセキュリティ対策

概要

本項では、当社がdocomo MEC™のサービス提供にあたり、実施しているセキュリティ対策を述べています。

サービス構成

機密性

- docomo MEC™では、当社の情報セキュリティポリシーおよびプライバシーポリシーを順守しています。ユーザとの契約に関する情報など特に重要なデータについては、docomo MEC™を構成するシステム内に保持していません。
- docomo MEC™ではwebコンソールへの通信を暗号化することで、webコンソールへのログインやオペレーションを盗聴などの脅威から保護しています。また、ユーザリソースが格納される物理ディスクをハードウェアレベルで暗号化（サーバサイド暗号化）することで、万が一、物理ディスクが流出しても情報が漏洩することがないように対策しています。
- ユーザが構築したユーザリソースと外部との通信についてはユーザ自身で対策する必要があります。例えば、ユーザが構築したWebサーバを構築しその通信を暗号化し保護する必要がある場合は、HTTPS通信機能をユーザ自身で設定いただくこととなります。ユーザリソースに格納されたユーザのデータについても暗号化による保護が必要な場合はユーザ自身で行っていただく必要があります。

完全性

- docomo MEC™では、ユーザがWebコンソールを通じて作成したサーバのウイルスチェックや脆弱性チェックなどのセキュリティ対策を実施していません。コンピュータウイルス等の不正プログラムによる被害を防ぐためには、ユーザ側で適切な対策を行ってください。
- また、ユーザリソースのデータ保護についても、各サービスごとに提供させるドキュメントを参照して、バックアップを取得するなど適切な対策をユーザ自身で行うようにしてください。

可用性

- docomo MEC™は、ユーザリソースと（当社が基盤全体を管理するための）管理領域が仮想的に分離しています。また、ユーザリソース内部はユーザごとにネットワークも含め分離する機能を提供しています。ただし、ユーザリソース内部には他ユーザと共有するリソース（共有サーバ、共有ネットワーク装置、及び共有回線）も存在するため、他ユーザの影響を受ける可能性があります。例えば、共有回線を利用するインターネット接続では特定のユーザが著しく高いトラフィックで通信を行うことで他のユーザの通信帯域が抑制される可能性があります。そのようなことが生じないように当社ではユーザの利用申込時にシステム構成や共有リソースの使用計画などを確認するようにしております。
- 可用性の保障について、個々の提供する機能がサービスとして利用不可の場合に障害とみなします。具体的には、Webコンソールからの各種機能の操作が不可能な状態や、ネットワークやストレージ輻輳など、広範囲に基盤へ影響が出ている状態を障害と定義します。また、基盤設計上は、単一の物理ホスト故障やインスタンス故障、冗長化されたネットワーク機器を切り替える為の短時間の通信断が発生する可能性があります。このような単一故障や切り替えに伴う短時間の通信断は障害とみなしません。サービスの可用性が必要な場合には、ユーザにてインスタンスの冗長化等の可用性を向上する設計を行っていただく必要があります。
- ユーザリソースのOS、アプリケーション、データについてはユーザにより適切な監視及び、インシデント管理を行ってください。データセンター及び、当社事業所では事故・災害時に備えて責任者や役

割、対応手順等をまとめたドキュメント類を策定しています。また、大規模な事故・災害を想定した訓練も実施しています。

サービス管理

サービスの運用体制

- 当社では情報管理委員会を設置するとともに、各組織に情報管理責任者を配置し、情報セキュリティ対策をすみやかに実施できる情報セキュリティ管理体制を構築しています。
- 当社では、情報資産の保護および適切な管理を行うため社内規定を整備し、明確な方針・ルールを周知徹底するようにしております。
- 従業員に対しては、情報セキュリティリテラシーの向上を図るとともに、当社の情報資産の適切な管理を実行するための教育・訓練を継続的に実施しています。
- docomo MEC™の情報システムおよび情報資産にアクセスするための認証画面を不特定多数に公開しないよう実装するとともに、アクセス制御ポリシーにおいて、アクセス権限を付与する対象者の数を必要最低限にすること、アクセス権限を必要最小限に限定すること、権限が集中しないように分離することを規定しています。
- 情報システムに対する攻撃や不正アクセス行為等およびその予兆、故障時の調査に備えログを収集しています。収集したログは定期的に分析し情報管理責任者に報告しています。

サービスの継続的な開発、提供とライフサイクル

- 当社では、サービスのセキュリティ品質を維持するために、システムの開発着手前にサービスの仕様が社内規定を順守していることを評価するとともに、サービス提供前にセキュリティ仕様の実装評価、脆弱性診断、を行い適切なセキュリティ対策がなされていることを確認しております。さらに、情報セキュリティ対策を定期的に評価、見直すことにより情報セキュリティマネジメントの継続的改善を実施しています。
- docomo MEC™では、要求仕様の策定、開発着手、品質の評価、サービスの提供に至るまで、サービスのライフサイクルを適切に管理するためのルール、体制を整備して、ライフサイクルの各ステップにおいて、ユーザへ提供する価値、品質がユーザの期待に応えられるものであることを評価しております。ユーザ要望を起点とした継続的な開発のために、アンケート等を通じて要望を収集し、中長期のロードマップに反映していきます。立案した計画に基づき、持続的な機能開発を実施していきます。変更機能リリース前には、変更機能の動作確認はもちろん、当該機能の影響度を検証するために、検証環境上でのリグレッション試験を実施し、その結果を責任者により確認しております。機能リリース時は、必ず複数名での作業及び、事前レビュー済の手順書に従った作業を前提とした上で、作業中や作業後の監視を強化することで、品質向上に繋げております。

監視の実施

- docomo MEC™では監視は24時間/365日で行い、異常を迅速に検知・通知する監視機能の実装と体制を整備しています。
- 監視の対象は、各機器（物理サーバー、ネットワーク、ストレージなど）、システムの性能・リソース・基盤サービスインタフェース、不正アクセス行為等になります。
- 当社の監視はdocomo MEC™全体に対するものであり、ユーザ個別のユーザリソースの監視は実施していません。ユーザリソースに対する適切な監視及び、対応はユーザにて実施するものとなります。

キャパシティ管理

- docomo MEC™では、ユーザがスムーズなソリューションの創出に取り組めるように、利用申込の際に必要なリソース量、システム構成などを確認させていただいております。docomo MEC™全体のリソースについて、使用状況および余剰を定期的に把握する管理プロセスを定めており、リソースの枯渇を未然に防ぐように適宜、リソースの増強を図っていきます。

インシデント管理

- 当社では、docomo MEC™に対する監視やログや検知したイベントの定期的な分析、外部機関からの脆弱性情報の提供に基づき、インシデント及びその予兆などのイベント管理を行っています。情報セキュリティのインシデントのパターン、影響度のレベル、状況に応じた対応手順を明確にし関係者に周知しています。インシデントの発生時には対応手順に基づき情報伝達を関係者に行い、対処にあたります。ユーザリソースに影響する可能性があるインシデントの発生時にはメールなどの手段により通知を行います。
- また当社では、障害の再発防止を図るために、発生した障害情報の蓄積・原因分析を行い、技術的防止策あるいは運用による防止策を検討した上で、関係者への水平展開を行っております。

クライアント(開発)端末管理

- 当社では、機器の種類や取り扱う情報に応じて開発/運用で使用するクライアント端末を適切な場所に設置することとしております。重要な情報を取り扱う端末については専用の独立した部屋に設置し、運用手順を文書化し、許可されている者だけの入室を確実にするための対策を講じています。
- クライアント端末についてはコンピュータウイルスなどの悪意のあるソフトウェア対策、ソフトウェア脆弱性対策を実施しています。悪意のあるソフトウェアを検知した場合の対応手順を明文化し関係者に周知しています。これによって、感染拡大防止、報告、調査、駆除、再発防止を図っています。さらに、クライアント端末にはシステムソフトウェア構成管理と内蔵ストレージの暗号化を行っております。

第三者委託

- 情報システムの開発や運用等で業務委託を行う場合は、事前に委託業務範囲や委託先選定条件等を明確にし適格性を審査しています。委託先には当社と同等以上のセキュリティレベルを維持するように要請し、セキュリティ基準等を着実に順守するため、必要なセキュリティ要件を盛り込んだ委託契約を締結しています。
- 当社の社内規定に準拠した情報システムの開発がなされるか開発の着手時およびサービス提供開始前にセキュリティの仕様の実装を審査しています。委託先のセキュリティ管理状況を定期的に確認し、順守できていないセキュリティ基準が存在した場合は速やかに対応することとしています。
- また、これらのセキュリティレベルが適切に維持されていることを確認するために、業務委託先への定期的な監査などを実施します。

その他

SLA（Service Level Agreement）規定

- docomo MEC™ではサービスを維持する品質基準を設定したSLA(Service Level Agreement)規定を定めています。SLA規定ではユーザが利用中のインスタンスの稼働率を対象として基準を99.95%と定めております。基準の詳細及び基準を達成できなかった場合の取り扱いについてはサービス利用規約を参照ください。

法制度

- docomo MEC™では、契約の成立、効力、解釈及び履行については、日本国法に準拠するものとします。ユーザと当社との間でdocomo MEC™に関連して訴訟の必要性が生じた場合は、東京地方裁判所を第一審の専属的合意管轄裁判所とします。docomo MEC™の利用にかかる義務および責任、禁止事項、データの取り扱い等はサービス利用規約を参照ください。

コンプライアンス

- 当社は、経営の根幹となるべきコンプライアンス(法規や倫理の順守)の基本を、グループ全体で共有し徹底するために「NTTドコモグループ倫理方針」を定め、倫理観の醸成に積極的に取組みます。
- 当社は、お客さまの大切なパーソナルデータを活用させていただくにあたっては法令を遵守することはもちろん、「データ活用によるお客さまや社会への新たな価値の継続的な提供」とともに「お客さまにとって最適なプライバシー保護」を実現すべく、「NTTドコモ パーソナルデータ憲章 -イノベーション創出に向けた行動原則」を定め、企業活動のあらゆる場面において、お客さまのパーソナルデータを取扱う際の意思決定の基準とします。
- 当社は、内部規定の整備と監査体制の整備・充実を行い、情報セキュリティ監査を実施し、適切な情報セキュリティ対策を実施します。詳細は「NTTドコモセキュリティポリシー」を参照ください。

利用契約終了後の措置

- 解約・解除その他の事由によりdocomo MEC™の契約が終了した場合には、ユーザーは契約の終了する日までにデータ等を削除するものとします。なお、ユーザーが期日までに削除しなかった場合は、当社がデータ等を削除するものとします。

セキュリティ関連機能

本章では、ユーザがdocomo MEC™を活用する際に役立つセキュリティ関連機能・サービスを紹介します。個々の機能・サービスの仕様についてはCompute O、Compute V、Compute Dのドキュメントをご確認ください。

ファシリティ設備・装置

- docomo MEC™で使用しているデータセンタは、Compute OとCompute V、Compute Dにて、国内各地域に分散して配置しています。
- 各データセンタは、ドコモの局舎内にあり、高い耐震性、耐火性を備えています。また電源、空調などについても、局舎のものを使用しており、高い堅牢性と耐久性を備えています。
- また、サーバルームへの入室は複数の認証手段が必要であり、高い機密性が保たれています。

docomo MEC™へのアクセス・運用管理

Webコンソールへのログイン画面

docomo MEC™のWebコンソールへログインする際には、IDおよびパスワードが必要です。IDおよびパスワードをユーザは自らの責任において厳重に管理する必要があります。なお、IDおよびパスワードが盗聴されないようwebコンソールへの通信を暗号化しており、Webコンソールに対しては不正アクセスチェック等の対策を当社で実施しています。

- Compute O

    - WebコンソールはIDおよびパスワード認証に加え、IP許可制限を実施しており、申込時に申請された固定のグローバルIPアドレス以外からのWebコンソールへのアクセスを制限することでセキュリティを確保しています。
- Compute V
    - WebコンソールはIDおよびパスワード認証に加え、WebコンソールへのアクセスにSSL-VPN接続を必須とすることでセキュリティを確保しています。またWebコンソールへのログイン後のユーザリソースに関する操作については、Webコンソール内の操作ログにて確認可能です。
- Compute D
    - WebコンソールはIDおよびパスワード認証に加え、IP許可制限を実施しており、申込時に申請された固定のグローバルIPアドレス以外からのWebコンソールへのアクセスを制限することでセキュリティを確保しています。

マルチアカウント

Webコンソールの操作に対して、操作範囲に制限を設けたアカウントを作成する機能を意味しています。

- Compute O
    - MEC基盤全体を操作可能な権限を持つアカウントと割り当てられたユーザリソースのみを操作可能な権限を持つアカウントが存在します。前者を当社が管理し、後者をユーザに提供しております。なお、ユーザに提供するアカウントについて、ユーザリソース内の操作可能な範囲を細分化し制限することはできません。
    - また、ユーザアカウントの作成機能はユーザに開放しておらず、ご提出された申請書に基づき当社で作業を実施いたします。
- Compute V
    - MEC基盤全体を操作可能な権限を持つアカウントと割り当てられたユーザリソースのみを操作可能な権限を持つアカウントが存在します。前者を当社が管理し、後者をユーザに提供しております。ユーザに提供するアカウントについて、ユーザリソース内の操作可能な範囲を細分化し制限することが可能です。
    - また、ユーザアカウントの作成機能をユーザに開放していますので、任意のユーザアカウントの作成及び、適切な権限を設定することが出来ます。具体的な操作可能な範囲や権限の割り当て等の手順については、Compute Oのドキュメント「チュートリアル> ユーザ管理」を参照してください。
- Compute D
    - MEC基盤全体を操作可能な権限を持つアカウントと割り当てられたユーザリソースのみを操作可能な権限を持つアカウントが存在します。前者を当社が管理し、後者をユーザに提供しております。なお、ユーザに提供するアカウントについて、ユーザリソース内の操作可能な範囲を細分化し制限することはできません。
    - また、ユーザアカウントの作成機能はユーザに開放しておらず、ご提出された申請書に基づき当社で作業を実施いたします。

操作ログ

Webコンソールの操作ログ、及び仮想サーバに対する操作ログを意味します。

- Compute O
    - Compute OのWebコンソール上での仮想サーバや仮想ネットワークを操作したログについて、ユーザへ提供しておりません。

    - ユーザにて構築された仮想マシンに対する操作ログについては、ユーザで取得及び保管をお願いします。
- Compute V
    - Compute VのWebコンソール上での仮想サーバや仮想ネットワークを操作したログについて、ユーザへ提供しています。
    - ユーザにて構築された仮想マシンに対する操作ログについては、ユーザで取得及び保管をお願いします。
- Compute D
    - Compute DのWebコンソール上での仮想サーバや仮想ネットワークを操作したログについて、ユーザへ提供しておりません。
    - ユーザにて構築された仮想マシンに対する操作ログについては、ユーザで取得及び保管をお願いします。

アクセスログ

- docomo MEC™で提供している基盤IaaSサービスへのアクセスは、統合管理ソリューションにてログを監視、および蓄積し、一定期間ごとに分析を行っています。異常時はドコモからユーザに通知することとし、機密性の観点でから当該ログを開示することはありません。
- ユーザにて構築された仮想マシンに対するアクセスログについては、ユーザ側にて取得及び保管をお願いします。

時刻の管理

- Compute O
    - NTPサーバは提供していないため、ユーザ側にてインターネットで公開されているNTPサーバへの同期をお願いします。
- Compute V
    - IaaSサービスとして、NTPサーバを提供しております。NTPへの同期についてはCompute Vのドキュメント「チュートリアル> はじめに」をご確認ください。
- Compute D
    - NTPサーバは提供していないため、ユーザ側にてインターネットで公開されているNTPサーバへの同期をお願いします。

仮想サーバ

ログイン認証

仮想サーバへの遠隔ログイン認証の方式として、一般的にID/パスワードによる認証と、より安全性の高い公開鍵による認証（キーペア認証）が挙げられます。

- Compute O

    - 基盤IaaSサービスとして、Webコンソールでキーペアを発行する機能を提供しています。Linux仮想サーバを作成する際に、キーペアの設定及び、任意のID/PWの設定が可能です。

- Compute V

    - 基盤IaaSサービスとしては、キーペアを発行する機能を提供していません。また、作成した仮想サーバには、基盤側で予め定めたID/PWが設定されています。初期構築時、仮想サーバにPW認

証にてログイン後、PWの変更及びキーペアの設定をユーザで実施して頂くようお願いします。

- Compute D
    - 基盤IaaSサービスとして、Webコンソールでキーペアを発行する機能と、ローカル環境のコマンドライン上でキーペアを作成し、それをインポートする方法を提供しています。Linux仮想サーバを作成する際に、キーペアの設定及び、任意のID/PWの設定が可能です。

高可用性（High Availability機能）

仮想サーバの予期せぬ故障に備えて、可用性を向上させる取り組みが重要です。具体的には、仮想サーバの冗長化構成、バックアップ/復旧手段の確立などの対策が必要となります。

- Compute O
    - 基盤IaaSサービスとしては提供しておりません。可用性を高めるためにはユーザで仮想サーバの冗長構成、バックアップからの定期取得、その復旧手順を整備するなどの対策が必要となります。
- Compute V
    - 基盤IaaSサービスとしてオートヒーリング機能を提供しています。オートヒーリング機能は、物理サーバに障害が発生した際に、自動で別の物理サーバ上で仮想マシンを再起動する機能を意味します。ただし、ユーザで仮想サーバのOS再起動時に、自動的にサービスを再開する仕組みを構築するなどの対策が必要となります。また、オートヒーリング間のサービス停止が許容できず、更なる高可用性を求めるためには、冗長化構成や非アフィニティルールの設定がユーザで必要です。詳細はCompute Vのドキュメント「リファレンス> コンピュート」を参照してください。
- Compute D
    - 基盤IaaSサービスとしては提供しておりません。可用性を高めるためにはユーザで仮想サーバの冗長構成、バックアップからの定期取得、その復旧手順を整備するなどの対策が必要となります。

SSL 証明書

- ユーザで構築するシステムに対するSSL証明書の提供はしておりません。ユーザで取得をお願いいたします。

仮想サーバのバックアップ

ユーザで構築する仮想サーバやそこに格納するデータのバックアップはユーザ自身の責任でご対応をお願いします。

- Compute O
    - 仮想サーバのディスクをイメージ化して保存するスナップショット機能を提供しています。取得したスナップショットから、別サーバとして新規作成し、バックアップ時の状態を復元することが可能です。詳細なバックアップ取得方法等はCompute Oのドキュメントを参照ください。
- Compute V

    - 仮想サーバを任意のタイミングでバックアップを取得する機能です。取得したバックアップデータから、別サーバとして新規作成し、バックアップ時の状態を復元させることが可能です。詳細なバックアップ取得方法等はCompute Vのドキュメント「チュートリアル>バックアップ」を参照ください。
- Compute D
    - 仮想サーバのディスクをイメージ化して保存するスナップショット機能を提供しています。取得したスナップショットから、別サーバとして新規作成し、バックアップ時の状態を復元することが可能です。詳細なバックアップ取得方法等はCompute Dのドキュメントを参照ください。

ネットワーク

仮想ネットワーク

ユーザリソース内におけるネットワークセキュリティを高めるために、DMZ、内部通信、管理通信など用途に応じて、ネットワークセグメントを分離することが必要です。そのために、docomo MEC™では、ユーザリソース内に任意の仮想ネットワークを作成することができる機能を提供しております。

- Compute O
    - ユーザで仮想ネットワークやネットワークセグメントを作成できる機能を提供しています。当該機能を使用して、ユーザでネットワークセグメントを分離した設計・構築をお願いいたします。
- Compute V
    - ユーザリソースの初期ネットワークとして、DMZ、内部通信、管理通信など用途に応じたネットワークセグメントを準備しております。ユーザで任意の仮想ネットワークも作成することが可能です。
    - 準備済みネットワークには何点か注意事項もございます。例えば、サーバへの遠隔ログインに使うセグメントは準備済みの管理通信セグメントを使用する必要がある　などです。詳しくは、Compute Vのドキュメント「チュートリアル>ネットワークの作成」を参照してください。
- Compute D
    - ユーザで仮想ネットワークやネットワークセグメントを作成できる機能を提供しています。当該機能を使用して、ユーザでネットワークセグメントを分離した設計・構築をお願いいたします。

仮想ルータ

docomo MEC™では、仮想ネットワークのセグメント間を接続するための基盤IaaS機能として、仮想ルータを提供しております。セグメント間のルーティング設定等が可能となります。

- Compute O
    - ユーザで用途に応じた任意の仮想ルータを作成し、ルーティングの設定をすることで、ネットワークセグメントを分離してください。
    - 仮想ルータには性能制限がございます、詳しくはCompute Oのドキュメントを参照してください。性能制限を超えた使い方を求める場合は、ユーザでインスタンスルータを構築してください。
- Compute V

    - ユーザリソースの初期として、外部通信間及び内部通信間に使用する仮想ルータを準備しております。ユーザで任意の仮想ルータの作成はできません。詳細な使い方は、Compute Vのドキュメント「チュートリアル> ネットワークの作成」を参照してください。
- Compute D
    - ユーザで用途に応じた任意の仮想ルータを作成し、ルーティングの設定をすることで、ネットワークセグメントを分離してください。
    - 仮想ルータには性能制限がございます、詳しくはCompute Dのドキュメントを参照してください。性能制限を超えた使い方を求める場合は、ユーザでインスタンスルータを構築してください。

仮想サーバに対するファイアウォール

- 仮想サーバーへの通信を、あらかじめ定義したルールに従って、L3レベルでフィルタリングする機能（セキュリティグループ）です。本機能を使用した仮想サーバへのアクセス制御は、ユーザの責任にて実施してください。本機能について、Compute O、Compute V、Compute Dで、各々特性・注意事項があります。詳しくは各ドキュメントを参照してください。

MECダイレクト

- 当社のネットワークとMECをダイレクトにつなぐことで伝送遅延の低減を実現するとともに、インターネットなど他網からのアクセスを防止できます。また、番号認証による接続制限により登録回線以外からの接続は制限されます。
- MECダイレクトの管理機能としてモバイル回線の接続先のMEC拠点や閉域網をユーザ自身が柔軟に変更できる「ネットワーク・オン・デマンド」機能を提供します。

ネットワークセキュリティサービス

- MEC基盤上のシステムとそこにつながるデバイスの通信状況・セキュリティ状況を可視化し、セキュリティ脅威から保護するオプションサービスとなります。セキュリティソフトウェアを組み込んだ仮想サーバのイメージを当社が提供し、ユーザがそのイメージから仮想サーバインスタンスを起動しユーザリソースに組み込むことにより保護の範囲・対象を柔軟に設定できます。

テナント間接続

- テナント間接続は、同一拠点内のプライベート LAN 同士をL2接続することができるネットワークサービスです。

リージョン間接続

- リーション間接続は、Compute OとCompute Vのプライベート LAN同士を、当社所有の閉域網を経由し、L3接続することができるネットワークサービスです。

テンプレート

- Compute D
    - Kubernetesテンプレートにより、予めセキュリティ対策用OSSをインストールし、各種デフォルト設定を行ったサーバ環境を提供します。

    - すべてのセキュリティ対策について保証するものではなく、用途に応じて追加設定が必要です。詳しくはComtepu Dのドキュメントを参照してください。

GPU

- Compute O
    - Ubuntuを搭載した物理GPUサーバを提供します。ご利用の際は仮想ネットワークと接続するGPU接続サービスも必要です。ログイン認証などのOS以上の設定、構築はユーザ自身で行っていただく必要があります。故障に備え複数台の冗長構成の構築やバックアップの取得をユーザで実施することを推奨します。
- Compute V
    - 仮想化されたGPUサーバ、vGPUサーバを提供します。GPU接続サービスが必要です。セキュリティについては通常の仮想サーバインスタンスと同様であり、物理サーバが故障した場合は他の物理サーバで自動的に再起動するオートヒーリングが適用されます。
- Compute D
    - インスタンスに接続可能なGPUを提供します。GPU接続サービスは不要です。GPUの提供については、GPUを認識するところまでとなります。GPUドライバのライセンス管理、および導入、動作確認はユーザ自身で行っていただく必要があります。

監視

- docomo MEC™では責任分担モデルに従い、基盤サービスを当社の基準に基づき監視しております。検知された異常はメールなどでお客様に通知いたします。異常が発生した際は迅速な復旧を最優先に基盤サービスを保守しますが、一部のHW故障など復旧に際してバックアップからの仮想サーバの起動などお客様の作業が必要となる可能性もあります。
- OS以上の保守運用はお客様自身でご対応いただく必要があり、システムの監視が必要な場合は監視サーバの構築などをお客様自身で実施いただくこととなります。

基本監視

- ドコモ側コンポーネントの稼働状況・負荷状況の監視を自動で行い、異常が発生した場合には、メールにて通知します。お客様のサーバについてはお客様自身で監視サーバを構築し、実施していただく必要があります。

有人監視

- ドコモ側コンポーネントの稼働状況を 24 時間 365 日監視します。異常が発生した場合には、メール又は電話で通知し、必要に応じて1次対応を行います。

メンテナンス及び各種通知

通知について

- docomo MEC™では、ユーザー向けの情報として、メンテナンス・障害情報などのお知らせをお送りしています。

メンテナンスについて

- 保守または工事によりdocomo MEC™の利用を注する場合には、あらかじめユーザに通知します。ただし、緊急やむをえない場合は、この限りではありません。

障害について

- 故障やセキュリティインシデントなどの障害を検知した際はユーザにその発生を当社からメールで通知します。発生した障害が回復した際は回復した旨をユーザに当社からメールで通知します。
- 通知先のメールアドレスはdocomo MEC™の利用申込時に登録いただいたメールドレスとなります。通知が適切に行われるようにメールアドレスに変更が生じた際は当社法人営業にご連絡をいただきますようお願いします。

ペネトレーションテスト

- ユーザが性能試験や（侵入試験などの）脆弱性診断を希望される場合は実施の 1 か月前までに当社が定める申請書を当社に提出する必要があります。これらの試験は当社サービスの提供や他ユーザへ影響を及ぼす可能性があるため、当社の判断により実施をお断りする場合があります。なお、お断りする場合の理由は開示できません。