docomo MEC®情報セキュリティポリシー

株式会社NTTドコモ

2025年7月1日(第7版)

※docomo MECおよびMECダイレクトはNTTドコモの登録商標です。

目次

- 初めに
- 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におけるセキュリティ対策
  - 概要
  - サービス構成
    - 機密性
    - 完全性
    - 可用性
  - サービス管理
    - サービスの運用体制
    - サービスの継続的な開発、提供とライフサイクル
    - 監視の実施
    - キャパシティ管理
    - インシデント管理
    - クライアント(開発)端末管理
    - 第三者委託
  - その他
    - SLA（Service Level Agreement）規定
    - 法制度
    - コンプライアンス
    - 利用契約終了後の措置
- セキュリティ関連機能
  - ファシリティ設備・装置
  - 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
    - マルチアカウント
    - 操作ログ
    - アクセスログ
    - 時刻の管理
  - 仮想サーバー
    - ログイン認証
    - 高可用性（High Availability機能）
    - SSL 証明書
  - 仮想サーバーのバックアップ
  - ネットワーク
    - 仮想ネットワーク
    - 仮想ルーター
    - 仮想サーバーに対するファイアウォール
    - MECダイレクト
    - ネットワークセキュリティサービス
    - テナント間接続
    - リージョン間接続
  - テンプレート

    - GPU
    - 監視
        - 基本監視
        - 有人監視
    - メンテナンス及び各種通知
        - 通知について
        - メンテナンスについて
        - 障害について
    - ペネトレーションテスト
- Compute Eのセキュリティ対策について
    - セキュリティ対策について

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 D」、「Compute E」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。

- ユーザーが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、「ユーザーリソース」と表記）は、事前に合意した利用規約の元で、ユーザーが任意に変更・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、ユーザーリソースや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、予告なくユーザー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。ユーザー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、ユーザー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（サーバーサイド暗号化）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。
- ユーザーが構築したユーザーリソースと外部との通信についてはユーザー自身で対策する必要があります。例えば、ユーザーが構築したWebサーバー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通信機能をユーザー自身で設定いただくこととなります。ユーザーリソースに格納されたユーザー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ー自身で行っていただく必要があります。

完全性

- docomo MECでは、ユーザーがWebコンソールを通じて作成したサーバー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。コンピューター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、ユーザー側で適切な対策を行ってください。
- また、ユーザー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ー自身で行うようにしてください。

可用性

- docomo MECは、ユーザーリソースと（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、ユーザーリソース内部はユーザー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、ユーザーリソース内部には他ユーザーと共有するリソース（共有サーバー、共有ネットワーク装置、及び共有回線）も存在するため、他ユーザー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ー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ー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ー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、ユーザー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。
- ユーザーリソースのOS、アプリケーション、データについてはユーザー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、ユーザーへ提供する価値、品質がユーザー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。ユーザー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、ユーザー個別のユーザーリソースの監視は実施していません。ユーザーリソースに対する適切な監視及び、対応はユーザー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、ユーザー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。ユーザー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ー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規定ではユーザー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。ユーザーと当社との間で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、ユーザーが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 D、Compute Eのドキュメントをご確認ください。またCompute Eのセキュリティ関連機能に関しては、次章のCompute Eのセキュリティ対策をご覧ください。

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ーは、Compute O、Compute Dにて、国内各地域に分散して配置しています。
- 各データセンターは、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、サーバー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ー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 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ー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、後者をユーザーに提供しております。なお、ユーザーに提供するアカウントについて、ユーザー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、ユーザーアカウントの作成機能はユーザーに開放しておらず、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 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ー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、後者をユーザーに提供しております。なお、ユーザーに提供するアカウントについて、ユーザー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、ユーザーアカウントの作成機能はユーザーに開放しておらず、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、及び仮想サーバー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ーや仮想ネットワークを操作したログについて、ユーザーへ提供しておりません。
  - ユーザー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、ユーザー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ーや仮想ネットワークを操作したログについて、ユーザーへ提供しておりません。
  - ユーザー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、ユーザー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ー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。

- ユーザー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、ユーザー側にて取得及び保管をお願いします。

時刻の管理

- Compute O
  - NTPサーバーは提供していないため、ユーザー側にてインターネットで公開されているNTPサーバーへの同期をお願いします。
- Compute D
  - NTPサーバーは提供していないため、ユーザー側にてインターネットで公開されているNTPサーバーへの同期をお願いします。

仮想サーバー

ログイン認証

仮想サーバー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仮想サーバーを作成する際に、キーペアの設定及び、任意のID/PWの設定が可能です。
- Compute 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仮想サーバーを作成する際に、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）

仮想サーバー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、仮想サーバーの冗長化構成、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ーで仮想サーバーの冗長構成、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 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ーで仮想サーバーの冗長構成、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

- ユーザー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。ユーザーで取得をお願いいたします。

仮想サーバーのバックアップ

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

- Compute O
  - 仮想サーバー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、別サーバーとして新規作成し、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 D
  - 仮想サーバー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、別サーバーとして新規作成し、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

ユーザー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、ユーザー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
  - ユーザー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、ユーザー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 D
  - ユーザー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、ユーザー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。

仮想ルーター

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、仮想ルーター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
  - ユーザーで用途に応じた任意の仮想ルーターを作成し、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。
  - 仮想ルーター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、ユーザーでインスタンスルーターを構築してください。
- Compute D
  - ユーザーで用途に応じた任意の仮想ルーターを作成し、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。

    - 仮想ルーター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、ユーザーでインスタンスルーターを構築してください。

仮想サーバー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ーへのアクセス制御は、ユーザーの責任にて実施してください。本機能について、Compute O、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ー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ーのイメージを当社が提供し、ユーザーがそのイメージから仮想サーバーインスタンスを起動しユーザー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ー環境を提供します。
    - 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サーバーを提供します。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、構築はユーザー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ーで実施することを推奨します。

- 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、動作確認はユーザー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さまに通知いたします。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ーの起動などお客さま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さま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ーの構築などをお客さま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。お客さまのサーバーについてはお客さま自身で監視サーバーを構築し、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の利用を中止する場合には、あらかじめユーザーに通知します。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ー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ー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

- ユーザーが性能試験や（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ー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。

Compute Eのセキュリティ対策について

Compute Eは、NTTドコモビジネスが提供するデータ利活用プラットフォームであるSmart Data Platform（以下、SDPF）をIaaS基盤としています。この章ではCompute Eのセキュリティに関する情報を記載いたします。

セキュリティ対策について

Compute Eのサービス基盤における主なセキュリティ概要は以下の通りです。

項目	説明
仮想サーバー	仮想化ソフトウェアによって論理的に分離されています。
ストレージ	管理するソフトウェアの制御により、論理的に分離されています。 なお、他のユーザーの利用による性能への影響を懸念するお客さまには、IOPS性能確保型のブロックストレージメニューをご用意しています。
ネットワーク	SDN、VLAN 技術などを活用した仮想ネットワークによって論理的に分離されています。 クラウド環境と外部環境を接続するネットワークとして、インターネット接続のメニューをご用意しています。