WideAngle AI Advisor
サービス仕様書

2026 年 11 月 11 日

NTT ドコモビジネス株式会社
マネージド＆セキュリティサービス部

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

目次

1. はじめに ... 3
1.1. 本書の目的 ... 3
1.2. 関連文書 ... 3
1.3. 用語の定義 ... 4
1.4. 本書の注意事項 ... 5
2. サービス概要 ... 6
2.1. サービス概要 ... 6
3. サービス仕様 ... 7
3.1. 提供区分 ... 7
3.2. 提供メニュー ... 7
3.3. 提供条件 ... 8
3.4. 提供機能 ... 9
3.5. サービスレベル ... 27
3.6. 提供地域 ... 27
3.7. AI SOC(マネージド SOAR 連携)時の提供条件 ... 27
4. 工事・故障対応 ... 29
4.1. 工事 ... 29
4.2. 故障対応 ... 29
5. 料金 ... 31
5.1. サービスの価格 ... 31
6. お申し込み・ご利用 ... 32
6.1. お申し込み ... 32
6.2. 標準開通日 ... 33
6.3. 開通案内・配布同梱物 ... 33
6.4. お問い合わせ受付 ... 34
6.5. お問い合わせ受付・運用受付/通知方法 ... 34
6.6. 工事通知（メンテナンス通知） ... 35
6.7. 故障通知 ... 35
7. 重要事項・留意事項 ... 36
7.1. 重要説明事項 ... 36
7.2. 留意事項 ... 39
改訂履歴 ... 40

記載されている会社名や製品名は、各社の商標または登録商標です。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

1. はじめに

1.1. 本書の目的

本書は、WideAngle AI Advisor のサービス提供機能、利用条件、および注意事項などについて記述したものです。本書に記載の内容について、予告なく変更される場合があります。

1.2. 関連文書

本書は、AI Advisor のサービス提供機能、利用条件、および注意事項などについて記述したものです。本書に記載の内容について、予告なく変更される場合があります。

文書名
WideAngle AI Advisor_サービス仕様書
WideAngle AI Advisor_利用規約
【新規】WideAngle AI Advisor_申込書
【変更】WideAngle AI Advisor_申込書
【廃止】WideAngle AI Advisor_申込書
【簡易変更】WideAngle AI Advisor_申込書
WideAngle_AI_Advisor_ヒアリングシート（新設）
WideAngle AI Advisor_ユーザーマニュアル
WideAngle AI Advisor_管理者マニュアル

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

1.3. 用語の定義

本サービスで使用する用語は以下の通りです。

用語	定義
NTT ドコモビジネス／NTT dB	NTT ドコモビジネス株式会社の略称。
LLM	大規模言語モデル。大量のテキストデータを使って学習された、人間のような自然な文章を生成できる AI モデル。
RAG	検索拡張生成。ユーザーの質問に対して、関連性の高い情報を文書データから検索し、その情報を参照して回答を生成する技術。
Microsoft Sentinel	Microsoft が提供するクラウドネイティブの SIEM（Security Information and Event Management）および SOAR（Security Orchestration, Automation and Response）サービス。
JVNDB	独立行政法人情報処理推進機構（IPA）が提供する脆弱性データベース。
SLA	サービスレベルアグリーメント。サービスの提供者と利用者間で、サービスの品質に関する合意。
ZIA	Zscaler Internet Access の略称。Zscaler が提供するユーザーがインターネットにアクセスする際のセキュリティを確保するクラウドベースのセキュア Web ゲートウェイサービス。
Prisma Access	Palo Alto Networks が提供するクラウドネイティブなセキュリティプラットフォーム。
マネージド SOAR	Microsoft Sentinel を基盤に、NTT ドコモビジネスが提供する WideAngle の一環として、検知から対処、復旧までを運用サポートする SOAR 型サービス。
AI SOC	AI Security Operation Center。マネージド SOAR と連携し、発生したインシデントに対して自動で分析を実行する機能を提供するソリューション。
AI Agent	人間が与えた目的やルールに基づき、周囲の状況（データ、システム状態、ユーザー入力等）を認識し、推論・判断を行いながら、必要に応じて外部システムやツールと連携して自律的に処理を実行する AI システム。
MITRE ATT&CK	MITRE Adversarial Tactics, Knowledge。攻撃者が使用する手法（戦術・技術）を体系化した国際的なフレームワーク。
Watchlist	Microsoft Sentinel において、外部からインポートしたデータを「参照用リスト」として保持し、ログデータとの照合や相関分析に活用するための機能。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

Severity	発生したアラート、インシデントの重大度を High/Medium/Low/Informational の 4 段階で示したもの。本サービスでは Sentinel 上の判定結果と AI による判定結果が存在。
アーティファクト	AI Advisor が分析の過程で参照したデータ。インシデントレポートと共に表示される。
KQL	Kusto Query Language。Microsoft Sentinel で利用されているデータクエリ言語で、本サービスではログ分析に用いられている。
内部不正	不正ログインや大量ファイルのダウンロードをはじめとした内部起因のセキュリティリスク。本サービスにて設定情報を登録しつつインシデントの自動分析が可能。
外部脅威	サイバー攻撃や第三者による不正アクセスをはじめとした外部起因のセキュリティリスク。本サービスにて設定情報を登録しつつインシデントの自動分析が可能。

1.4. 本書の注意事項

本書に記載するサービス仕様の内容は、当社 Web サイトへの掲載をもってお客さまへ周知されたものとみなします。

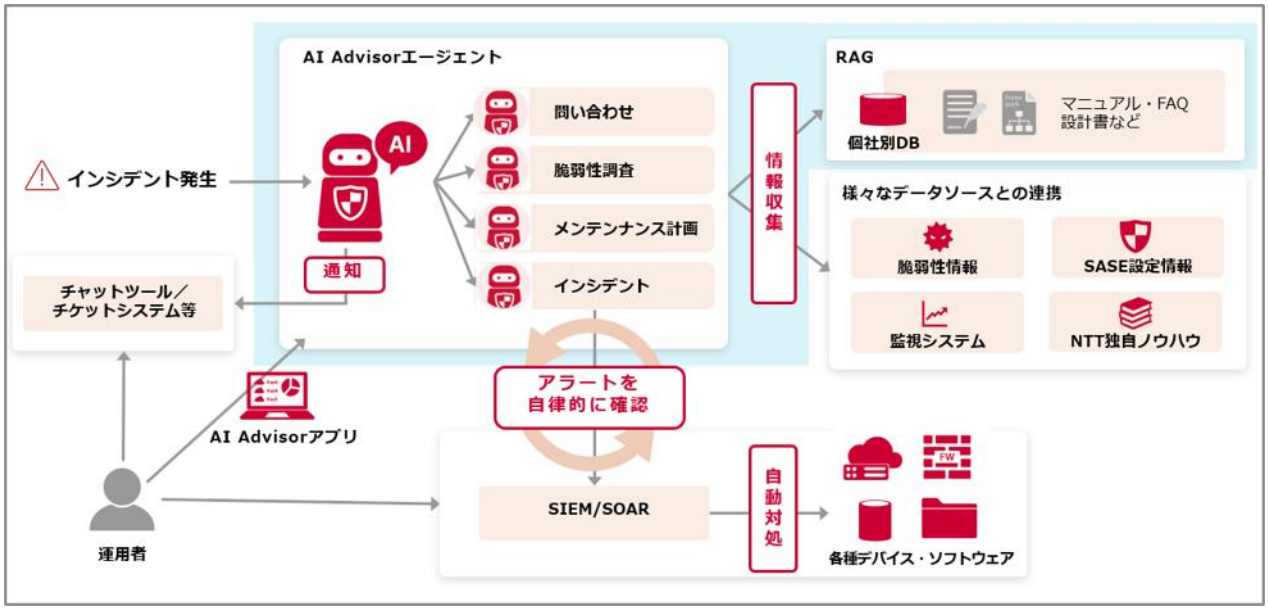
© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

2. サービス概要

2.1. サービス概要

「AI Advisor」は LLM（大規模言語モデル）を活用し、IT 運用・セキュリティ業務に必要な知識提供や対応判断を支援する AI アシスタントサービスです。
セキュリティ運用に関するさまざまな問いかけに対し、お客さま環境固有の情報と NTT 独自のノウハウを掛け合わせた実用的な回答をお届けします。運用者は AI Advisor のアプリを経由して自然言語によるセキュリティ運用に関する問い合わせを行うことが可能です。
構成情報などセキュリティ運用に欠かせないお客さま独自の固有情報を元に回答を生成することも可能です。さらに、NTT がこれまで蓄積してきた独自ノウハウや IoC などの情報も学習させることで、AI Advisor はお客さまのシステム構成を理解したうえで、より高度な回答を生成することが可能となります。また運用ツールと連携させることで、運用者の業務負担軽減に貢献します。
また、WideAngle マネージド SOAR と連携し、発生したインシデントに対して自動で分析を実行し、調査レポートを生成する機能も提供します。AI SOC がお客さまのインデント対応業務をサポートします。

（参考）サービス提供イメージ※



※提供機能の範囲としては、上図の青色で示した範囲であり、脆弱性情報のデータソースや SIEM/SOAR 等のセキュリティ製品は提供範囲外です。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

3. サービス仕様

3.1. 提供区分

本サービスのサービス提供/保守区分は、下図の通りです。

<table>
<tr><td colspan="2">接続構成</td><td>
</td><td></td><td></td><td>
</td></tr>
<tr><td colspan="2">構成品</td><td>お客さま環境</td><td>AI Advisor
(Google Cloud)</td><td>NTTドコモビジネスサポートサイト
※共用設備</td><td>サービス運用</td></tr>
<tr><td colspan="2">サービス
契約区分</td><td>お客さま</td><td colspan="3">NTTドコモビジネス</td></tr>
<tr><td colspan="2">サービス
責任区分</td><td>お客さま</td><td>インフラ：Google
アプリ：NTTドコモビジネス</td><td colspan="2">NTTドコモビジネス</td></tr>
<tr><td colspan="2">資産区分</td><td>お客さま</td><td>Google</td><td colspan="2">NTTドコモビジネス</td></tr>
<tr><td rowspan="2">工事
区分</td><td>開通SO</td><td>―</td><td>NTTドコモビジネス</td><td>―</td><td>―</td></tr>
<tr><td>設定/
作業</td><td>―</td><td colspan="3">NTTドコモビジネス</td></tr>
<tr><td>保守
区分</td><td>問合せ/故障
対応</td><td>―</td><td colspan="3">NTTドコモビジネス</td></tr>
</table>

3.2. 提供メニュー

AI Advisor は、「Standard」「Premium」「Lite」の 3 つのメニューがあります。

またそれぞれのプランにチケット追加オプションをアドオンすることができます。

各メニューの提供内容は以下のように定められています。

メニュー		チケット数	ポータル機能 (ユーザー登録数)	提供機能種別※1
基本	Premium	2,000 チケット	200 人まで	A/B
	Standard	1,000 チケット	100 人まで	A/B
	Lite	500 チケット	2 人まで	B
オプション※2	チケット追加	500 チケット	―※3	―※3

※1 第 3.4.章 提供機能参照

※2 最大で 5 まで追加可能

※3 基本メニューの契約に依存

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

3.3. 提供条件

3.3.1. サポート対応時間

- 日本時間の平日 9:00～17:30 を AI Advisor のサポート対応時間とします。
- 該当の時間帯以外も AI Advisor ポータル画面にアクセス可能ですが、サポートはありません。
- 日本時間の土日、祝日、12 月 29 日から 1 月 3 日はサポート対応時間に含まれません。

3.3.2. 利用制限

- AI Advisor の利用回数はチケット制で月ごとに上限を設定しており、設定されている上限を超えると利用制限がかかる仕様となります。設定されているチケット数の上限を超えた場合、追加チケットの契約をお願いしております。
- AI Advisor に登録できるユーザーアカウントについて上限を設けます。
- AI Advisor に参照させるファイルを格納するためのストレージについても上限を設けます。

3.3.3. 推奨環境

- 以下の端末環境での利用を推奨します。
  OS: Windows 11
  ブラウザ: Google Chrome

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

3.4. 提供機能

本章では、主な提供機能について示します。

3.4.1. 一般利用者向け機能

一般利用者向けに以下の機能を提供します。

項番	機能種別	機能	詳細	消費チケット数
1	A	質問応答機能	ユーザーからのプロンプトを受けて回答する機能	1 チケット= 100 問合せ
2	A	脅威インテリジェンス連携機能	IP／ドメイン／URL の危険性について脅威インテリジェンスを参照して回答する機能	1 チケット= 100 問合せ
3	A	RAG 機能	あらかじめフォルダに登録したファイル情報に関連する質問回答を可能とする機能	—
4	A	添付ファイルに関する文章生成機能	ユーザーのプロンプトに加えて、アップロードした添付ファイルに基づき回答する機能	1 チケット= 100 問合せ
5	A	ダッシュボード機能	Microsoft Sentinel、脆弱性データベースに接続し、情報を一覧表示する機能	—
6	A	プロンプトテンプレート機能	よく使うプロンプトをテンプレートとして保存する機能	—
7	A	設定管理機能	LLM が回答する際のトーンや形式を設定する機能	—
8	A	履歴管理機能	過去の質問応答を履歴として保存する機能	—
9	A	ユーザー認証機能	お客さま環境の認証基盤と SAML で連携したユーザー認証機能	—
10	A	インシデントレポート生成機能	Microsoft Sentinel と連携して、分析レポートを生成する機能	1 チケット= 1 回答分
11	A	Zscaler（ZIA）連携機能	ZIA の URL フィルタリングの設定情報を参照し、回答する機能	1 チケット= 100 問合せ
12	A	Prisma Access 連携機能	Prisma Access の URL フィルタリングの設定情報を参照し、回答する機能	1 チケット= 100 問合せ
13	A	脆弱性情報データベース連携機能	CVE 番号や JVN 番号をもとに脆弱性情報の詳細について回答する機能	1 チケット= 100 問合せ
14	A	ユーザー認可機能	一般利用者向け機能、管理者向け機能に対して、権限に応じたアクセス制御を行う機能	—

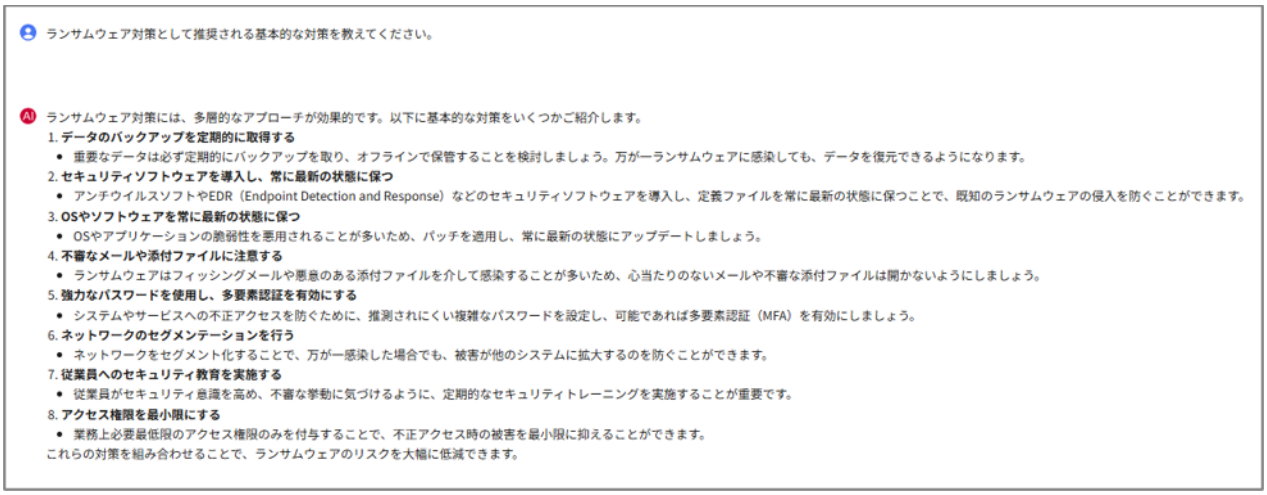
© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

※上記以外のカスタマイズ（他システムとの連携など）や RAG の精度向上コンサルなどはサービスに含まれません。

（1） 質問応答機能

チャット形式で LLM に対して、IT 運用・セキュリティ対応に関して質問する機能を提供します。
月の利用上限を超えた場合にはエラーとなります。

＜画面イメージ＞



（2） 脅威インテリジェンス連携機能

脅威インテリジェンス情報を参照し IP／ドメイン／URL の危険性を分析・評価して回答をする機能を提供します。

＜画面イメージ＞



（3） RAG 機能

事前にフォルダにマニュアルや FAQ などのファイルを格納しておくことで、ファイルに記載されている内容に基づいた回答を生成する機能を提供します。LLM 回答時に参照するフォルダを選択可能とします。利用可能なフォルダは 5 個で、ラベルは申請時に提出していただくヒアリングシートで確認します。選択したフォルダの中から関連度の高い上位 10 件のドキュメントを回答生成に使用します。関連度は星（☆）の数で表され、星が多いほど関連度が高いことを示します。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

<画面イメージ>



また、回答時に使用したファイルを確認することが可能です。

<画面イメージ>



（４）　添付ファイルに関する文章生成機能

アップロードした添付ファイルに関する文章生成機能を提供します。

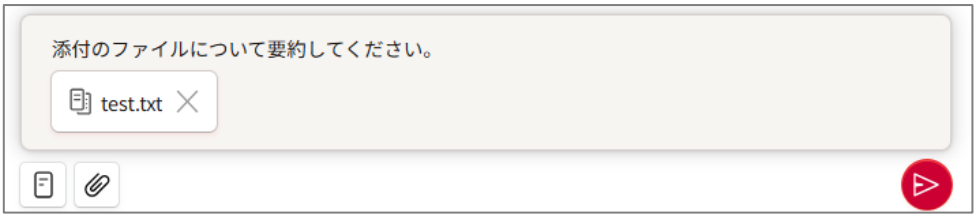
1 回のプロンプト入力につき 1 ファイル指定することが可能です。

対応しているファイル形式は以下の通りです。

形式	1 ファイルあたりのサイズ上限
ドキュメント：TXT、CSV、PDF 画像：PNG、JPEG、WebP	6MB 未満

※文字コードについては、UTF-8 をサポートしています。

<画面イメージ>



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

（５）　ダッシュボード機能

・インシデントダッシュボード

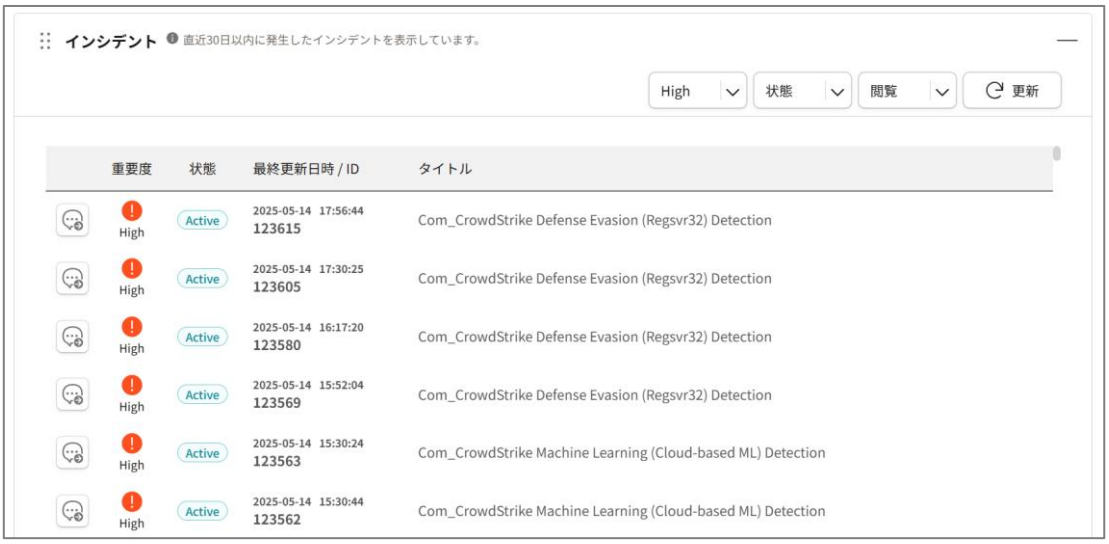
Microsoft Sentinel と連携し、インシデント一覧を表示する機能を提供します。

重要度と閲覧状況で絞り込みを可能とします。

選択したインシデントについて内容を確認するためのプロンプトを自動入力する機能を提供します。

インシデントの優先順位づけをするためのプロンプトを自動入力する機能を提供します。一度に取得できるインシデントの情報は 500 件までです。

＜画面イメージ＞



・脆弱性情報ダッシュボード

JVNDB の情報を取得し、脆弱性情報の一覧を表示する機能を提供します。

重要度と閲覧状況で絞り込みを可能とします。

選択した脆弱性情報について内容を確認するためのプロンプトを自動入力する機能を提供します。

＜画面イメージ＞



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

（6）　プロンプトテンプレート機能

LLM に質問する内容（プロンプト）をテンプレート化して設定する機能を提供します。

あらかじめプロンプトを設定しておくことで、繰り返し使用する質問文を効率的に入力できます。システムで準備されているプロンプトテンプレートを利用することも可能です。

<画面イメージ>



（7）　設定管理機能

以下の LLM の回答に関するパラメータ調整機能を提供します。

・トーン

・形式

・長さ

<画面イメージ>



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

（８）　履歴管理機能

同一セッション内での問い合わせ履歴を参照可能とする機能を提供します。

ログアウトもしくは 12 時間経過するとリセットされます。

＜画面イメージ＞



（９）　ユーザー認証機能

お客さまが用意した認証基盤（Entra ID／Okta など）と SAML により連携しユーザー認証する機能を提供します。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

（１０） インシデントレポート生成機能

Microsoft Sentinel の API を利用し、発出されたインシデントに関する分析レポートを生成する機能を提供します。分析ではインシデントの関連情報／MITRE ATT&CK 情報／脅威インテリジェンス情報をもとに、LLM による脅威度判定を行います。AI SOC によるインシデントの自動分析が完了している場合、インシデントに紐づく最新の AI SOC 分析結果をレポート形式で出力します。

・インシデント基本情報(インシデント番号、タイトル、発生日時、更新日時／ステータス、検知製品名)

※AI SOC による自動分析が完了している場合は、「AI SOC 分析時間」も出力されます。

・インシデント概要（発生インシデントの要約)

・インシデント解説（発生インシデントの解説)

・深刻度の判定結果（Sentinel によるアラート深刻度の判定結果、AI によるアラート深刻度の判定結果、AI によるアラート深刻度の判定根拠）

・MITRE ATT&CK 分類結果(戦術、技術の分類)

・エンティティ情報(種類ごとの実データとその調査結果)

・プロセス分析結果

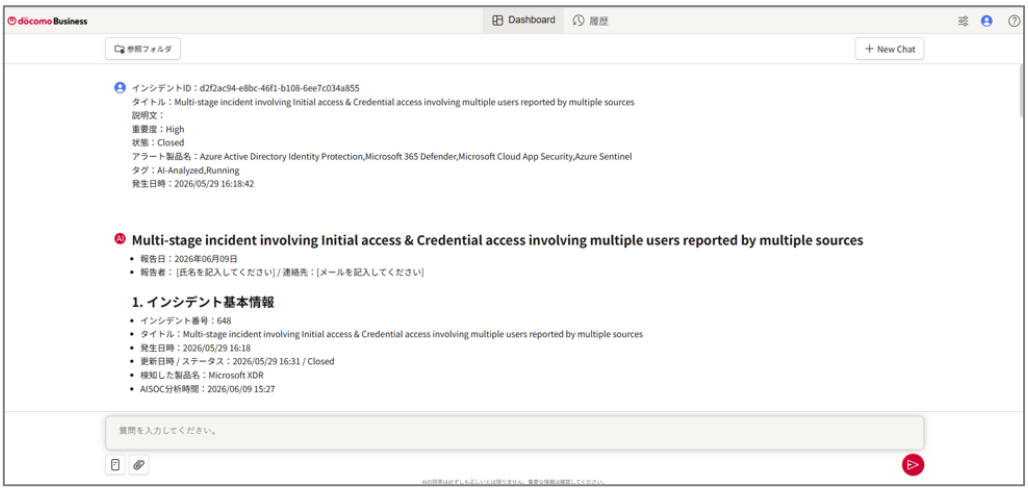
※AI SOC による自動分析が完了している場合のみ出力されます。

・推奨アクション(AI からの提案)

・備考(そのほか補足・注意事項あれば記載)

※AI SOC による自動分析が完了している場合は、出力されません。

<画面イメージ>

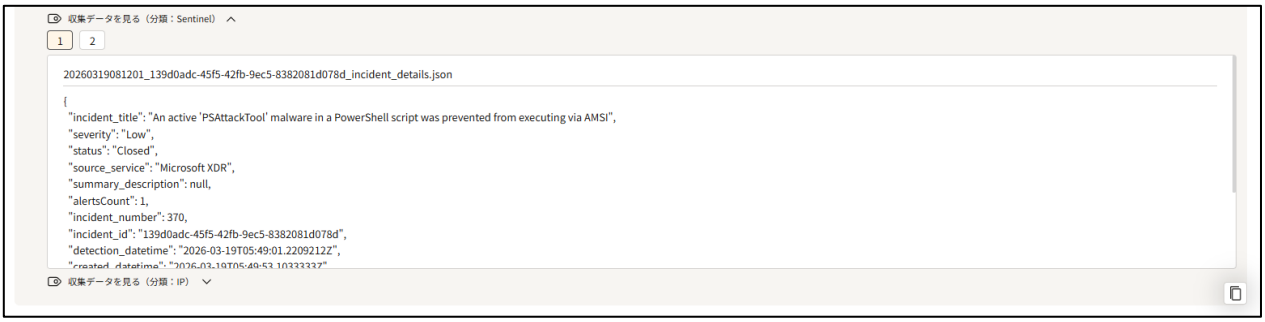


また、インシデントレポートと共に分析の過程で参照したデータ(アーティファクト)が表示され、分析結果の根拠を後から確認する事が可能です。Microsoft Sentinel の API で取得した情報および脅威インテリジェンス情報(IP／Domain／URL)、レポート生成にて実行したKQLのクエリを参照可能です。

※KQL のクエリは AI SOC による自動分析が完了している場合のみ表示されます。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

<画面イメージ>



（１１） Zscaler（ZIA）連携機能

Zscaler（ZIA）の API を利用し、URL フィルタリング設定に関する以下の情報を確認して回答をする機能を提供します。

・URL カテゴリ（URLCategories）

・URL フィルタリングポリシー（urlFilteringRules）

・URL とクラウドアプリ制御ポリシー設定（advancedUrlFilterAndCloudAppSettings）

<画面イメージ>



（１２） Prisma Access 連携機能

Prisma Access の API を利用し、URL フィルタリング設定に関する以下の情報を確認して回答をする機能を提供します。

・セキュリティルール（Security Rules）

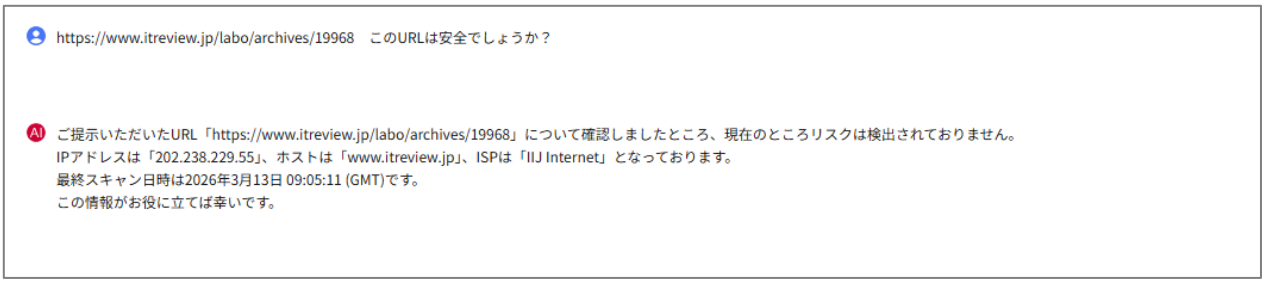
・プロファイルグループ（Profile Groups）

・URL フィルタ設定（URL Filtering）

・カスタム URL カテゴリ（Custom URL Categories）

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

<画面イメージ>



（１３） 脆弱性情報データベース連携機能

脆弱性情報に関連する API を利用し、CVE 番号および JVN 番号に紐づく脆弱性情報を取得して回答する機能を提供します。

・CVE 脆弱性詳細情報（CVEDetailInfo）

・JVN 脆弱性詳細情報（VulnDetailInfo ）

<画面イメージ>



（１４） ユーザー認可機能

ユーザーごとに設定した権限(ロール)に応じて、アクセス制御を行う機能を提供します。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

3.4.2. 管理者向け機能

管理者向けに以下の機能を提供します。

項番	機能種別	機能	詳細	消費チケット数
1	A	RAG ファイル管理機能	RAG で利用するファイルを登録、削除する機能	—
2	B	ユーザー認証機能	お客さま環境の認証基盤と SAML で連携したユーザー認証機能	—
3	B	ユーザー管理機能	ユーザーの登録・削除・更新を行う機能	—
4	B	ユーザー認可機能	一般利用者向け画面、管理者向け画面に対して、権限に応じたアクセス制御を行う機能	—
5	B	利用状況表示機能	契約中のプランや上限に対する利用チケット数など、AI Advisor の利用状況を表示する機能	—
6	B	分析用プロンプト設定機能	お客さまの環境に応じた分析を実現するため、AI SOC の分析用プロンプトを設定する機能	1 チケット＝100 回※1

※1 入力内容に対してガードレールによるチェックを実施します。ガードレールにより入力がブロックされた場合、1 回の入力としてカウントされ、100 回につき 1 チケットを消費します。

※上記以外のカスタマイズ（他システムとの連携など）や RAG の精度向上コンサルなどはサービスに含まれません。

（1） RAG ファイル管理機能

AI Advisor の RAG にファイルをアップロードするための機能を提供します。

各フォルダのファイルの一覧表示、登録、削除を可能とします。

<検索できるファイルの条件>

以下の条件に該当しないファイルは、エラーとなり検索対象になりません。

形式	1 ファイルあたりのサイズ上限
HTML、TXT、JSON、XHTML、XML などのテキストベースのファイル	10MB 未満
PPTX、DOCX、XLSX	200 MB 未満
PDF	40 MB 未満

※文字コードについては、UTF-8 をサポートしています。

※1 つのファイルに含まれる情報量が 1,000 チャンク(50 万文字程度)を超える場合、当該ファイルは検索対象にできません。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

（2） ユーザー認証機能

お客さまが用意した認証基盤（Entra ID／Okta など）と SAML により連携しユーザー認証する機能を提供します。

（3） ユーザー管理機能

ユーザーの登録・削除・更新を行う機能を提供します。ユーザーはメールアドレスで識別します。メールアドレスをカンマ区切りで入力することで、複数のユーザーを同時に手動登録することも可能です。ご希望いただいたお客さまには、ユーザーがデータベースに存在しない際、該当のメールアドレスを保存し、自動でチャット利用者の権限を付与することができる自動登録機能も提供します。

ユーザー登録時に設定できる権限（ロール）は以下の通りです。

ロール	説明
チャット利用者	一般利用者向け画面の機能のみ利用可能です。
運用担当者	一般利用者向け画面の他に管理画面向け画面にもアクセスし、RAG ファイルのアップロードや分析用プロンプトの設定をすることが可能です。（ユーザー登録はできません。）
SOC 担当者※1	分析用プロンプトの設定、ユーザーの追加・削除、ロールの付与・変更が可能です。
テナント管理者	ユーザーの追加・削除、ロールの付与を含めすべての操作が可能です。

また、各ロールの利用可能な範囲を整理すると以下の通りです。

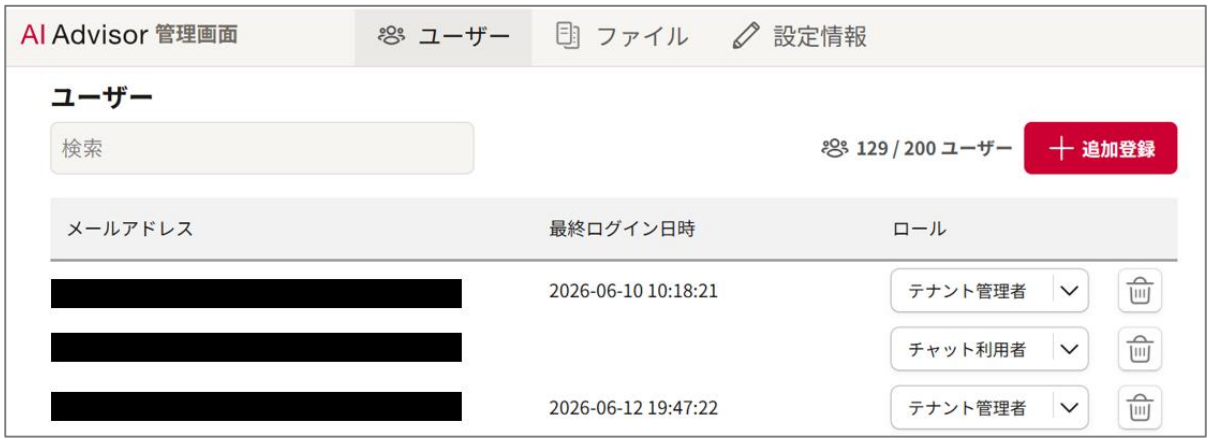
ロール/機能	一般利用者向け画面の各機能※2	RAG ファイル管理機能※2	分析用プロンプト設定機能	ユーザーの追加・削除	ロールの付与・変更
チャット利用者	○	-	-	-	-
運用担当者	○	○	○	-	-
SOC 担当者※1	-	-	○	○	○
テナント管理者	○	○	○	○	○

※1 WideAngle マネージド SOAR 未契約のお客さまは SOC 担当者ロールが非表示となっております。

※2 Lite プランのお客さまは RAG ファイル管理機能及び一般利用者向け機能が利用できません。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

<画面イメージ>



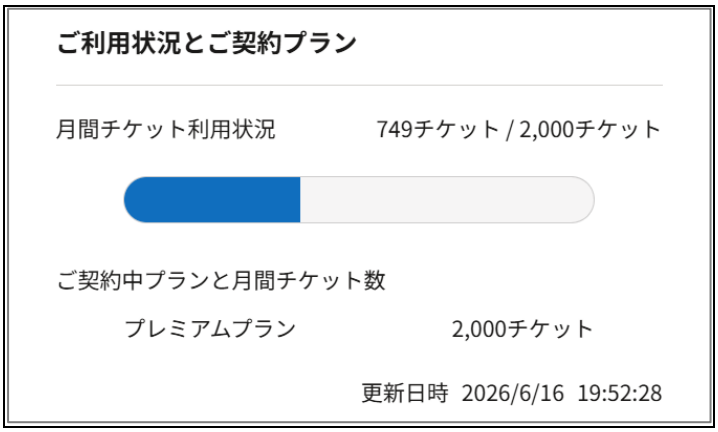
（4） ユーザー認可機能

ユーザーごとに設定した権限(ロール)に応じて、アクセス制御を行う機能を提供します。

（5） 利用状況表示機能

契約のプラン(基本プラン+追加チケット利用数)、及び上限に対するチケットの利用状況を確認することができる機能です。

<画面イメージ>



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

（6）　分析用プロンプト設定機能

AI SOC によるインシデント自動分析に活用する事前情報を登録・更新することができる機能です。分析用プロンプトに、ネットワーク情報やお客さまの拠点に関する情報、機密情報の定義等を設定することで、お客さま固有の考慮事項を踏まえた分析が可能になります。

分析用プロンプトは、ネットワーク情報や拠点情報等を設定する「外部脅威分析」用と機密情報の定義等を設定する「内部不正分析」用の２種類で構成されており、それぞれに必要な情報を登録できます。

※内部不正分析用プロンプトの設定・利用は、「Threat Detection(ログソース：Microsoft Purview)」をマネージド SOAR の契約デバイスとしてご契約いただく必要があります。

＜画面イメージ＞



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

3.4.3. 定期実行機能

以下の定期実行機能を提供します。

項番	機能種別	機能	詳細	消費チケット数
1	B	インシデント自動分析機能	Microsoft Sentinel(マネージド SOAR)と連携し、分析対象のインシデントを監視して分析する機能	1 チケット＝1 アラート分析

※上記以外のカスタマイズ（他システムとの連携など）や RAG の精度向上コンサルなどはサービスに含まれません。

（1） インシデント自動分析機機能

マネージド SOAR をご契約されている方は、インシデントの自動分析機能が利用可能となります。同機能ではマネージド SOAR で検知されたインシデントに対し、関連情報を自動収集・整理し、分析結果を生成する機能を提供します。インシデントの自動分析には「外部脅威」を対象とした分析と「内部不正」を対象とした分析があります。

自動分析は、以下の流れで実施します。

※内部不正を対象とした分析のご利用は、「Threat Detection(ログソース：Microsoft Purview)」をマネージド SOAR の契約デバイスとしてご契約いただく必要があります。

1. 解析対象の取得

マネージド SOAR が Watchlist に登録した分析対象のインシデントのリストを 10 分間隔で取得します。インシデントは時系列順に分析しますが、中でも Severity が"High”のインシデントを優先して分析します。

取得したインシデントは 1 件ずつ処理し、1 件処理完了したら最新のリストを取得し直します。

※ 同時に多数のインシデントが発生した場合、処理開始まで時間を要する可能性もございます。

2. 処理前コメント書込み

Microsoft Sentinel の API を利用し、分析開始時にインシデントに紐づくコメント欄に、分析開始した旨を記載します。

3. 個社情報読み込み

事前に受領した個社固有の環境情報を参照し、顧客毎に最適化された指示や調査内容を分析に組み込みます。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

4. インシデント情報取得

Microsoft Sentinel の API を利用しインシデントに紐づくアラート情報、関連エンティティ等の詳細情報を取得します。

5. MITRE ATT&CK 情報収集

攻撃者の戦術・技術・手順を体系化したサイバーセキュリティナレッジ「MITRE ATT&CK」の基準に基づき、当該インシデントの戦術や技術に関する分類・評価を行います。

※MITRE ATT&CK 情報収集は外部脅威を対象とした分析に限定して実施されます。

6. 脅威インテリジェンス連携

脅威インテリジェンス情報を参照し、IP／ドメイン／URL の危険性を分析・評価します。

7. ログ分析機能

ログ分析機能は主に「プロセス分析」と「エンティティ毎の相関分析」の 2 つの機能を提供します。

①プロセス分析

インシデントに紐づくプロセス ID をキーに下記の対象テーブルから Microsoft 365 Defender の API を用いてログを収集し、親子関係・行動証跡を分析します。

＜製品毎の対象テーブル＞

製品名	テーブル名	外部脅威分析	内部不正分析
MDE (Microsoft Defender for Endpoint)	DeviceEvents	○	○
	DeviceFileEvents	○	○
	DeviceProcessEvents	○	○

②エンティティ毎の相関分析

分析対象のエンティティ（Host／File／Account／IP／URL）をキーに下記の対象テーブルから Microsoft Sentinel および Microsoft 365 Defender の API を用いてログを収集し、分析を行います。参照先のテーブルやログの取得回数は AI が判別しており、約 30 件のエンティティを分析可能です。

※AI が分析対象を選択している為、これ以上の分析は不要と判断した場合は 30 件未満となる場合もございます。

製品毎の対象テーブルと利用用途は以下となります。各ログは、格納先（Analytics 層／Data Lake）に応じて参照し、分析に利用します。また、下記以外にも、Log Analytics のカスタムログテーブルに格納されたネットワークログについて、お客さま環境ごとに分析対象として設定可能です。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

＜製品毎の対象テーブル＞

製品名	テーブル名	外部脅威分析	内部不正分析
XDR （Extended Detection and Response）	SecurityIncident	○	○
	SecurityAlert	○	○
MDE （Microsoft Defender for Endpoint）	DeviceImageLoadEvents	○	○
	DeviceInfo	○	○
	DeviceLogonEvents	○	○
	DeviceNetworkEvents	○	○
	DeviceNetworkInfo	○	○
	DeviceRegistryEvents	○	○
	DeviceFileCertificateInfo	○	○
	DeviceTvmSoftwareInventory	○	-
	DeviceTvmSoftwareVulnerabilities	○	-
MDO （Microsoft Defender for Office 365）	EmailEvents	○	○
	EmailUrlInfo	○	○
	EmailAttachmentInfo	○	○
	EmailPostDeliveryEvents	○	○
	UrlClickEvents	○	○
MDI （Microsoft Defender for Identity）	IdentityLogonEvents	○	○
	IdentityQueryEvents	○	○
	IdentityDirectoryEvents	○	○
MDA （Microsoft Defender for Cloud Apps）	CloudAppEvents	-	○
EntraID （Microsoft Entra ID）	SigninLogs	○	○
	AuditLogs	○	○
	AADNonInteractiveUserSignInLogs	○	-
	AADServicePrincipalSignInLogs	○	-
	AADManagedIdentitySignInLogs	○	-
	AADProvisioningLogs	○	-
	ADFSSignInLogs	○	-
	AADUserRiskEvents	○	-
	AADRiskyUsers	○	-

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

	NetworkAccessTraffic	○	-
	AADRiskyServicePrincipals	○	-
	AADServicePrincipalRiskEvents	○	-
	MicrosoftGraphActivityLogs	○	-
	EnrichedOffice365AuditLogs	○	-
	RemoteNetworkHealthLogs	○	-
UEBA (User and Entity Behavior Analytics)	OfficeActivity	-	○
	Anomalies	-	○
	BehaviorAnalytics	-	○
	IdentityInfo	-	○
	Operation	-	○
	UserPeerAnalytics	-	○
AMA（Azure Monitor Agent）	Syslog	○	-
	CommonSecurityLog	○	-

8. インシデント統合分析

ログ分析の結果に加え、これまで収集した情報を基に分析を行います。エンティティ毎の脅威度分析、インシデント全体の脅威度推論、脅威度推論の算出根拠、推奨アクションを考察します。

9. 分析結果・KQL 実行結果のコメント書き込み機能

Microsoft Sentinel の API を利用し、各過程で調査・分析を実施した結果をインシデントコメントとして 3 万文字以内で出力します。加えて分析結果とは別のコメントとして、分析に使用した KQL の実行結果も出力します。

それぞれの出力内容は以下となります。

■分析結果

・出力内容

・インシデントの最終更新日時

・インシデントサマリ

・脅威度情報(Sentinel によるアラート深刻度の判定結果、AI によるアラート深刻度の判定結果)

・MITRE ATT&CK 分類結果(戦術、技術の分類)

・プロセス分析結果

・エンティティ分析結果(エンティティの種類、実データ、分析元のソース情報、調査結果)

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

・分析結果（結果の概要、AI によるアラート深刻度の判定根拠、推奨アクション）
・メタ情報（分析ステータス、分析開始時刻、インシデントに紐づくアラート数、SessionID ）
・ユーザー関連情報（高リスクユーザーの情報、及び対象ユーザーの時系列アクティビティ）
※ユーザー関連情報は内部不正を対象とした分析結果にのみ出力されます。

■KQL 実行結果
・分析に使用し、実行に成功した KQL クエリの一覧

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

3.5. サービスレベル

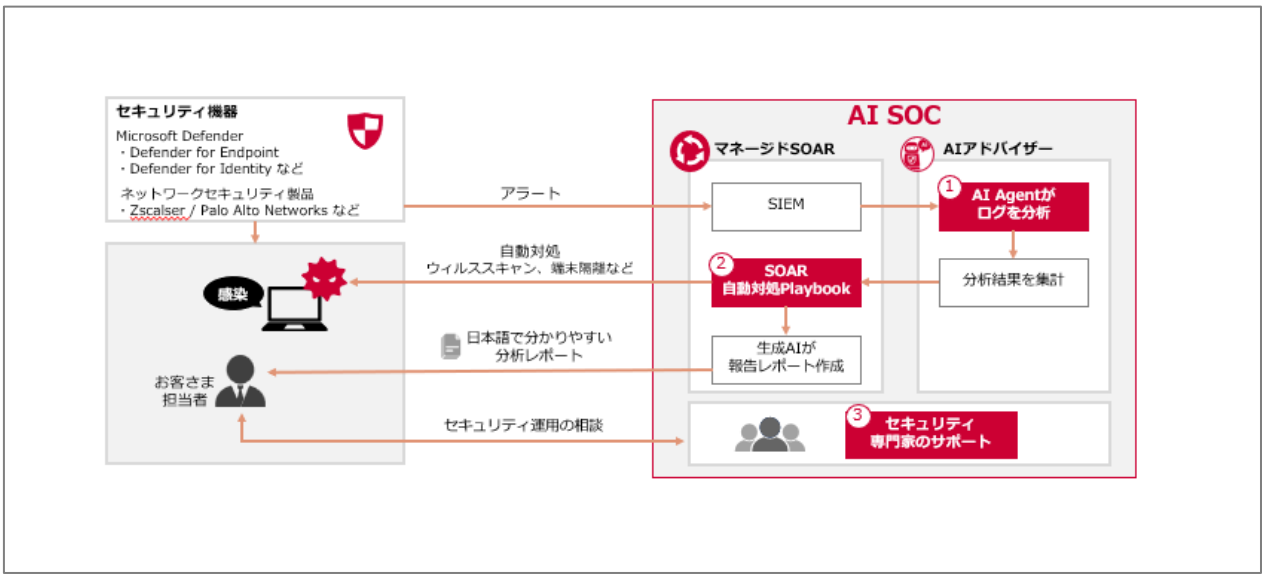
本サービスは、SLA（Service Level Agreement）の定めはありません。

3.6. 提供地域

日本国内の法人、かつ日本国内での契約を対象とします。

3.7. AI SOC(マネージド SOAR 連携)時の提供条件

＜AI SOC 時の提供構成例＞



・提供条件

インシデント自動分析機能の利用には、WideAngle マネージド SOAR の契約が必要です。

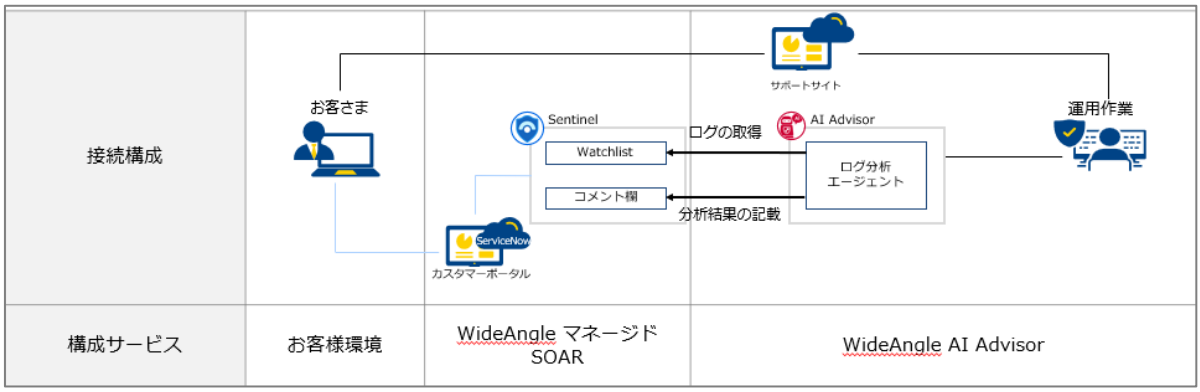
・提供区分

WideAngle マネージド SOAR 連携時(AI SOC)の提供区分については、以下の通りです。

以下の責任区分に基づき、故障対応・お問い合わせ受付のスタンスを定めるものとします。

WideAngle マネージド SOAR の詳細な提供区分については、「WideAngle マネージド SOAR_サービス仕様書」に準ずるものとします。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.



・責任分界点

AI Advisor における Microsoft Sentinel 連携機能については、以下を責任分界点とします。

①AI Advisor（Sentinel 連携機能）の責任範囲

Microsoft Sentinel 上の Watchlist を参照し、Watchlist に記載のインシデントをもとにログ分析を実施し、その結果を Microsoft Sentinel のコメント欄に記載する

②WideAngle マネージド SOAR サービスの責任範囲

Microsoft Sentinel 上のインシデントを Watchlist に記載する。

AI Advisor 分析結果に基づき自動対処（ウイルススキャン、端末処理等）の実行

・故障の切り分け

Microsoft Sentinel 側のサービス障害、または Sentinel の検知ロジックに起因する事象については、AI Advisor の故障には含まれません。ただし、AI Advisor と Microsoft Sentinel 間の連携処理において、AI Advisor 側の処理異常が確認された場合は、AI Advisor の故障として切り分けを実施します。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

4. 工事・故障対応

4.1. 工事

本サービスの工事については「6.6. 工事通知（メンテナンス通知）」を参照ください。

4.2. 故障対応

本サービスでは、Google Cloud の監視サービスを用いて、サービスの正常性監視を行います。Google Cloud の監視サービスにて異常を検知した場合や、お客さまより故障のお問い合わせをいただいた場合に、調査を行い以下の対応を行います。

- 必要に応じて NTT ドコモビジネスにて原因の調査を実施し、故障と判断された場合は、NTT ドコモビジネスお客さまサポートにてお客さまへ通知を行います。
- また、NTT ドコモビジネスにて復旧対応を実施する必要がある場合は、NTT ドコモビジネスにて復旧対応を行います。

【調査結果と通知・対応】

故障箇所	原因	通知・対応
AI Advisor サービスの故障	NTT ドコモビジネスの設定が原因と判断された場合	NTT ドコモビジネスお客さまサポートを通じてお客さまに通知し、NTT ドコモビジネスにて復旧対応を行います
	お客さま側の利用方法、設定が原因と判断された場合	NTT ドコモビジネスお客さまサポートを通じてお客さまに通知し、お客さまにて復旧対応を行っていただきます
	Google Cloud 側の故障が原因と判断された場合、または Google 社から故障情報がアナウンスされた場合	NTT ドコモビジネスお客さまサポートを通じてお客さまに通知する（Google Cloud 社が提供するクラウドサービスのため、NTT ドコモビジネスによる復旧対応は行いません）
Google Cloud 接続までのネットワーク故障	サービス提供対象外のため、NTT ドコモビジネスによる調査、復旧対応は行いません	

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

本サービス情報サイトとして、NTT ドコモビジネスお客さまサポートサイトを公開しています。

https://support.ntt.com/aiadvisor

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

5. 料金

5.1. サービスの価格

- 本サービスの料金は、**WideAngle AI Advisor 利用規約**の料金表に定めます。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

6. お申し込み・ご利用

6.1. お申し込み

6.1.1. 申込方法

- 申し込み内容によって、新設、変更、簡易変更、廃止の申込パターンがあります。
- ご契約者情報の変更（譲渡/改称/継承など）は、簡易変更申込書で対応します。
- ヒアリングシート記載内容の変更は、弊社営業担当までお問い合わせください。

申込パターン	説明	申込書	ヒアリングシート
新設	新規で契約する場合	●	●
変更	料金変更が発生する以下の契約変更の場合 ・提供プラン（問い合わせ回数上限）の契約変更 ・オプションの増減	●	—
簡易変更	料金変更が発生しない以下の契約変更の場合 ・譲渡/改称/継承等による契約者情報の変更 ・契約者住所の変更 ・契約に関する連絡先の変更	●	—
廃止	契約を解約する場合	●	—

6.1.2. 申込書

- サービスを新規で契約する際、契約内容を変更する際、解約する際の申込書式です。
- 申込パターンによって、新設、変更、簡易変更、廃止の申込書があります。

申込パターン	申込書
新設	新設申込書
変更	変更申込書
簡易変更	簡易変更申込書
廃止	廃止申込書

6.1.3. ヒアリングシート

- サービス提供に必要な詳細ヒアリング情報をお客さまに記入いただくシートです。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

6.1.4. 開通試験

サービス導入時の初期構築時に以下の開通試験を行います。

- AI Advisor URL のアクセス試験
- 管理者 URL のアクセス試験

6.2. 標準開通日

- 標準開通日は次の日程です。
- NTT ドコモビジネスが申し込みを受理し、不備が無いことを確認した時点から起算した日数となります。尚、当日 15 時を過ぎた場合は翌営業日受付の扱いとなります。

申込種別	標準開通日	備考
新設	10 営業日	左記の標準開通日は、お客さまの条件が満たされている場合の目安です。お客さま側の条件が満たされていない場合は、例外となります。
廃止	3 営業日	—
変更	5 営業日	左記の標準開通日は、お客さまの条件が満たされている場合の目安です。お客さま側の条件が満たされていない場合は、例外となります。
簡易変更	2 営業日	申込書に希望開通日はなく、また開通案内も送付しません。左記の標準開通日は目安です。

6.3. 開通案内・配布同梱物

- 新設申し込み、変更申し込みの場合に開通案内を発行します。
- 廃止申し込み、簡易変更申し込みの場合、開通案内などは発行しません。
- 送付物は、NTT ドコモビジネスの BOX サービスを利用して送付します。次の手順でファイルを受領していただきます。
  ① お客さまへ、送信元が”<wa-sac-customer@ntt.com>”からメールが届きます
  ② お客さまはメール本文の URL をクリックして、BOX の Web サイトへアクセスします
  ③ ファイルダウンロードには、申込書に記載のパスワードを入力します

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

- 各申し込みで送付するものは次のものです。

申込 / 送付物	新設 「サービス利用開始のお知らせ」	変更 「サービス利用内容変更のお知らせ」
開通案内（ご利用内容のご案内）	●	●
サービス利用に必要な情報の通知 AI Advisor ポータル URL など	●	●

6.4. お問い合わせ受付

- 監視・運用担当にて、故障インシデントに関するお問い合わせを受け付けます。

窓口業務	受付時間	手段	主な内容
お問い合わせ受付	NTT ドコモビジネスお客さまサポート受付：24 時間 365 日 対応時間：平日（年末年始除く）9:00～17:30	NTT ドコモビジネスお客さまサポート	• 故障インシデントに関するお問い合わせ（回数制限なし）

※NTT ドコモビジネスお客さまサポートの故障などによりご利用できない場合、一時的にお問い合わせをお受けできない場合がございます。

6.5. お問い合わせ受付・運用受付/通知方法

- お問い合わせ受付の対応方法は以下となります。
- お客さまとのやり取りは NTT ドコモビジネスお客さまサポートを介して行われます。

項目	対応方法
お問い合わせ	・お客さまからのお問い合わせは、NTT ドコモビジネスお客さまサポートの「お問い合わせ」より、お問い合わせ内容を入力いただき、監視・運用担当から回答をします。

<お問い合わせについて>

- アプリケーションの利用方法に関するお問い合わせは、AI Advisor に質問してください。
- プロンプトや RAG のチューニングに関するお問い合わせには回答できません。
- 英語（日本語以外）でのお問い合わせには回答できません。
- お客さま設備や、お客さま調達区分に対するお問い合わせには回答できません。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

6.6. 工事通知（メンテナンス通知）

工事（メンテナンス）の通知は、NTT ドコモビジネスお客さまサポートに掲載します。
工事（メンテナンス）の実施中は一時的に本サービスが利用できなくなる場合があります。

（1） 計画メンテナンス

- サポート対応時間以外の時間帯でメンテナンスウィンドウを設定します。
- 本メンテナンスウィンドウを利用して、NTT ドコモビジネスは、基盤設備のバージョンアップや不具合等の修正を行います。バグや脆弱性の対応については、NTT ドコモビジネスの判断基準において、月に 1 回の本メンテナンスウィンドウで、パッチ適用等の対処を行います。
- メンテナンスウィンドウにて NTT ドコモビジネスが作業を行う場合は、1 週間前までに NTT ドコモビジネスお客さまサポート上で事前にアナウンスします。

（2） 緊急メンテナンス

- アプリケーションの故障に伴い、緊急リリースが必要になった場合は、定期リリース以外の時間帯でメンテナンスが実施される可能性があります。
- 緊急を要するメンテナンスについては、可能な限り早くサポートサイト上でアナウンスします。

6.7. 故障通知

- サービス故障発生時や緊急性の高い脆弱性対応で AI Advisor ポータル閉塞を伴う作業に該当する場合には、NTT ドコモビジネスお客さまサポート上で故障通知を実施します。
- 事前に、NTT ドコモビジネスお客さまサポートの「工事・故障情報通知サービス」登録することにより、工事・故障情報を、プッシュ型でお客さまへメール配信することが可能です。
- 本サービスの故障発生時は、NTT ドコモビジネスお客さまサポート上で故障通知を実施し、NTT ドコモビジネスお客さまサポート以外の故障報告（障害レポート、月次報告など）は提出しません。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

7. 重要事項・留意事項

7.1. 重要説明事項

7.1.1. 品質について

- 本サービスは、SLA（Service Level Agreement）を規定しません。

7.1.2. アクセス回線について

- 本サービスを利用するためのインターネット回線については、お客さまにてご準備ください。回線にかかる費用（ISP 料金を含みます）は、本サービスとは別に発生し、ご利用になった通信会社から利用料金が請求されます。

7.1.3. 最低利用期間

- 最低利用期間はありません。

7.1.4. 料金

- 本サービスの料金は利用規約 別紙 料金表に記載します。
- 初期費用は利用開始月の利用料金とあわせて一括で請求します。
- 課金開始日が毎月 2 日以降となる場合、課金開始日を含む月の料金は日割り計算となります。
- 契約解除日が毎月末日の前日以前となる場合、契約解除日を含む月の料金は日割り計算します。
- 契約開始初月で解約した場合の初期費用は発生いたします。
- お客さま都合により本サービス開通日までにご利用のご案内をお受取になれなかった場合は、本サービスの料金の返還はいたしません。

7.1.5. 提供中止

- NTT ドコモビジネスは、災害・広域停電・インターネット障害・パンデミックなどの事態が発生し、本サービスを提供することが困難な場合は本サービスの一部または全部の提供を中止することがあります。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

7.1.6. 契約の成立

- 契約の成立は、お客さまからお申し込みを頂いた日をもって成立するものとさせていただきます。ただし、そのお申し込みに不備がある場合など、お承りできない事があります。また、お承りのご連絡は、ご利用開始時の開通通知をもって代えさせていただきます。

7.1.7. 契約の解除

- お客さまが本サービスの利用規約に記載のお客さまの義務の規定に違反したとき、NTT ドコモビジネスは契約を解除することがあります。

7.1.8. 免責

- NTT ドコモビジネスは、AI Advisor における生成 AI の回答がすべてのセキュリティ上の脅威や攻撃を検知・対処することについて保証を行わず、これらに関連して契約者に損害が発生したとしても責任を負いません。
- 当社は本サービスを仕様書に従い提供するものであり、契約者は、当社が本サービスについて正確性、実現性、有用性、有効性を保証するものではないことを了承し、契約者の責において本サービスを利用するものとします。
- 生成 AI が助言をするというサービスの性質上、契約者の登録する情報が正確であることを前提としています。それに依拠して、提供した情報に誤りがあり提言に基づいた実施事項が契約者に対して損害を与えた場合、当社に責任を負担させないものとします。
- 当社は、本規約の変更等により契約者が本サービスを利用するにあたり当社が提供することとなっている設備、端末等以外の設備、端末等の改造又は変更（以下、この条において「改造等」といいます）を要する場合であっても、その改造等に要する費用については負担しません。
- 当社は、本サービスが日本国外の地域の規制（法令、規則、政府ガイドライン等を含みますがこれに限りません）に適合していること、および日本国外の地域で利用可能であることについて何ら保証を行わず、契約者もしくは契約者のエンドユーザーによる日本国外の地域での本サービスの利用または契約者もしくは契約者のエンドユーザーの保存データおよび生成等データの日本国外から日本国内への移転によって発生したいかなる損害についても当社は責任を負いません。
- 当社の責めによらない原因での故障又は障害（サービスの一部を構成する第三者の電気通信設備・電気通信回線・製品・ソフトウェア・サービス等に起因する障害を含みます。）については、当社は責任を負わないものとします。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

7.1.9. サービスの廃止

- 本サービスは、お客さまからの廃止申込により契約が終了し廃止されます。

7.1.10. ログ分析における免責事項

- 本サービスは生成 AI を用いた支援サービスであり、生成 AI の特性上、回答内容は確率的な推論に基づいて生成されます。そのため、提供される回答は常に正確性・完全性・最新性を保証するものではなく、誤った情報や不完全な内容を含む場合があります。本サービスが提供する分析結果、助言、推奨事項については、最終的な判断および対応は利用者の責任において実施されるものとします。
- 取得したインシデントは 1 件ずつ処理し、1 件処理完了したら最新のリストを取得し直します。
  ※ 同時に多数のインシデントが発生した場合、処理開始まで時間を要する可能性もございます。
- 分析対象となるエンティティ数が 30 個を超える場合は生成 AI による推論精度が低下する可能性があります。このため、本サービスではエンティティ数を制御し、重要度の高い情報を優先して分析する設計としています。
- 本サービスにおける脅威インテリジェンス（TI）情報には、外部サービスおよび NTT ドコモビジネス独自の情報源が含まれます。セキュリティ上の理由から、利用している一部の TI ソースの詳細は非公開とします。また、TI の内容や利用方法は、予告なく変更される場合があります。

7.1.11. MFA(多要素認証)の設定について

- AI Advisor はお客さまが保有する認証基盤と SAML を用いて連携します。そのため、MFA(多要素認証)の有無はお客さま自身にて設定できますが、以下の点を考慮して設定してください。

  1. MFA（多要素認証）をご利用いただくことにより、アカウントのセキュリティを強化し、第三者による不正侵入からの防御をより高めることができます。
  2. MFA（多要素認証）を利用いただかない場合、アカウントのセキュリティを脆弱にするおそれがあるため、MFA（多要素認証）を利用されることを強く推奨します。
  3. また、パスワードについても一定期間内で繰り返しログイン失敗した際はアカウントロックをする設定、初期パスワードの初回使用時に変更を強制する設定を強く推奨します。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

7.2. 留意事項

7.2.1. ご利用について

- 提供する各種推奨事項の実行はお客さまの判断・責任において行われるものとします。
- 本業務の中で発生した著作物に関する著作権は NTT ドコモビジネスに帰属します。お客さまの内部使用に限って利用は可能ですが、関連会社以外の第三者に配布・公開はできません。

7.2.2. サービス全般の注意事項について

- ご利用開始時および変更時に通知する『開通案内』は、送信元が<wa-sac-customer@ntt.com>からメール通知が届きますので、このドメインからのメールが受信できるようにしてください。また、送付物をダウンロードする際のパスワードは、お申し込み時にお客さまに記載いただいたものを使用し NTT ドコモビジネスから通知は致しません。
- 同業者様からのお申し込みはお断りすることがあります。あらかじめご了承ください。
- 弊社被災により運用業務の継続に支障をきたす場合でも、お客さまの業務が停止する等のリスクは最小限のため、DR/BCP 対策をとらない運用体制となっています。
- データのバックアップについても最小限の構成となっております。システムに登録するプロンプトやファイルなどは必要に応じてお客さまの方で保管をお願いします。

7.2.3. AI セキュリティの対応について

・本サービスは入力プロンプトに対してチェックする仕組みを導入し、悪意のあるプロンプトに対して回答しないように対処しています。
・本サービスに入力されたデータや各種ログは、AI モデルの学習には利用されません。
・AI Advisor に対する 攻撃行為（擬似攻撃を含む）やペネトレーションテスト等の実施は禁止します。お客さまにてセキュリティ検証等を実施される場合であっても、AI Advisor に対する 脆弱性診断、侵入試験、負荷試験、その他これらに類する行為は実施できません。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

改訂履歴

バージョン	主な変更	日付
1.00	初版発行	2025 年 5 月 27 日
1.10	・商号変更に伴い、企業名、ロゴ、コピーライトの変更 ・3.3 (1) 3 インシデントダッシュボードの表示上限件数を 500 件に修正 ・3.3 4 プロンプトテンプレート　画面イメージの差し替え ・3.3 4 プロンプトテンプレート　プロンプト例について記載を追加	2025 年 7 月 3 日
1.20	・「1.3 用語の定義」に「Zscaler Internet Access（ZIA）」を追加 ・「3.4 提供機能」の RAG 機能の詳細を更新、添付ファイルに関する文章生成機能、Sentinel 連携機能、Zscaler（ZIA）連携機能を追加 ・「3.4 提供機能」のユーザー認証機能の詳細を SAML 認証を前提とした記載に変更 ・「3.4 提供機能」の質問応答機能の画面イメージを最新化 ・「3.4.2 管理者向け機能」のユーザー管理機能を削除 ・「3.4.2 管理者向け機能」の RAG ファイルの注意書きとしてサポートしている文字コードについて記載を追加	2025 年 10 月 1 日
1.30	・「3.4.2 管理者向け機能」の Google Cloud プレビュー版の記載を削除	2026 年 1 月 5 日
2.0	AISOC 機能に関する以下記載 1.3 用語の定義に追記 1.4 本書の注意事項について記載 3.2 提供メニューに新規メニュー追記 3.2.2 利用制限のチケットについて追記 3.4 提供機能の表を新規機能実装にあたり、全体的に修正 3.7AISOC 時の提供条件について記載 6.1 申込方法についてオプションの増減を追記 7.1.2 アクセス回線について表現を修正 7.1.10 ログ分析における免責事項について記載 7.2.3AI セキュリティの対応について記載	2026 年 5 月 20 日
2.10	・基本メニュー「Lite」におけるユーザー登録数の最新化 3.2. 提供メニュー ・一般利用者向け機能/管理者向け機能の追加 3.4. 提供機能 ・メンテナンスウィンドウタイミングの更新 6.6. 工事通知(メンテナンス通知) ・MFA(多要素認証)に関する記載を追記 7.1. 重要説明事項 ・軽微文言修正	2026 年 7 月 6 日
2.20	・「KQL」「内部不正」「外部脅威」に関する定義を追記 1.3.　用語の定義 ・提供機能区分の見直し(定期実行機能の追加) 3.4.　提供機能 ・レポート生成時に実行した KQL クエリを、アーティファクトとして参照可能である旨を追記 3.4.1　一般利用者向け機能詳細 ・分析用プロンプトの区分（外部脅威／内部不正）の追記と画面イメージの最新化 3.4.2.　管理者向け機能詳細 ・インシデント自動分析に「外部脅威」「内部不正」の 2 種類がある旨を追記 ・MITRE ATT&CK 情報収集が外部脅威分析のみで実施される旨を追記 ・プロセス分析、エンティティ相関分析で使用するテーブルを表形式で追記 ・ネットワークログ（カスタムテーブル）を分析対象として設定可能な旨を追記	2026 年 10 月 1 日

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

	・コメント出力に KQL 実行結果を追加 ・分析結果に高リスクユーザー情報、ユーザーの時系列アクティビティを追加 3.4.3. 定期実行機能詳細 ・軽微文言修正	
2.21	・第三者サービス等に起因する故障・障害に関する免責事項を追記 7.1. 重要説明事項	2026/11/11

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.