つなごう。驚きを。幸せを。

WideAngle
AI Advisor ユーザーマニュアル

2026 年 4 月 1 日

NTT ドコモビジネス株式会社

プラットフォームサービス本部　M&S 部セキュリティサービス部門

目次

1. はじめに

1.1. 本書について

本書は、AI Advisor のユーザーマニュアルです。AI Advisor およびその操作について理解を深めることを目的として作成されています。
本書の内容は予告なしに変更または更新されることがあります。
また、ご利用可能な機能につきまして、
Zscaler（ZIA）連携機能、Prisma Access 連携機能、ならびにインシデントレポート生成機能は
ご契約プランにより利用可否が異なり、当該機能をご利用いただけない場合がありますので予めご了承ください。

1.2. AI Advisor についてのお問い合わせ先

故障の疑いがある場合は、サポートサイト
（https://support.ntt.com/aiadvisor/inquiry/detail/pid22000027ht）にて受け付けます。

2. ユーザー認証機能

お客様環境の認証基盤と SAML で連携したユーザー認証機能を提供します。

2.1. 推奨環境

以下の端末環境での利用を推奨します。
OS: Windows11
ブラウザ: Google Chrome

2.2. サービスの URL

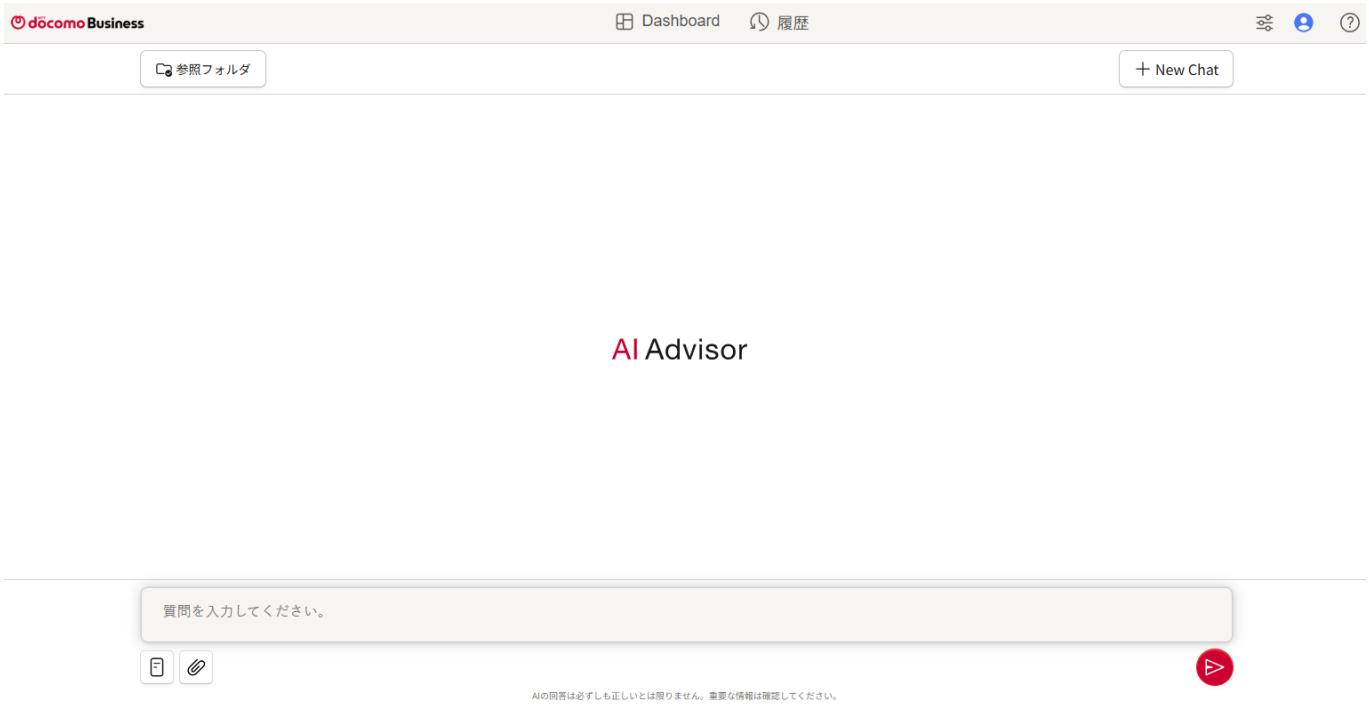
接続先の URL は開通案内時に個別に連絡いたします。

2.3. ログイン

① 接続先の URL にアクセスします。

② お客様環境の認証基盤と SAML で連携したユーザー認証を行います。

③ 以下の画面が表示されると、ログイン完了となります。



2.4. ログアウト

ユーザーアイコンをクリックし、[ログアウト]をクリックします。

3. 質疑応答機能

チャット形式で 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。

- インシデントに関する質問に関しては「6-2 インシデントレポートの作成」をご参照ください。

3.1. 質問入力および回答

- 質問を入力し、実行ボタンをクリックします。
  例：「CVE-2024-6387 の脆弱性について教えてください。」と入力

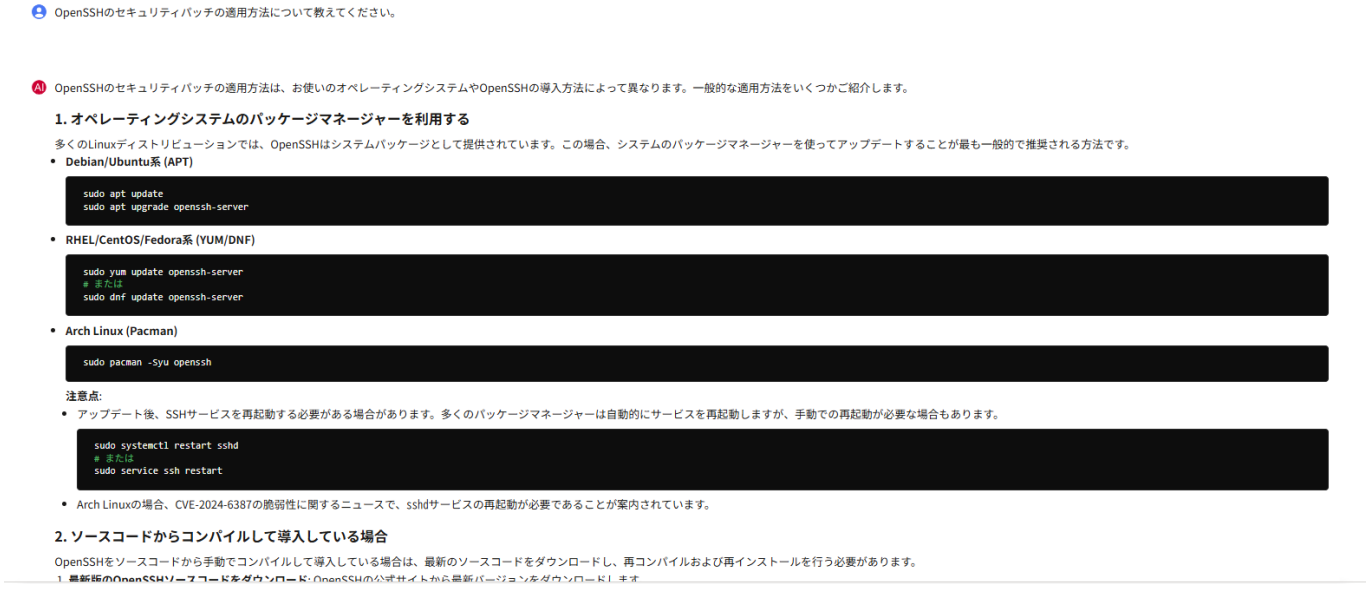
- 回答生成に必要な処理の進捗状況が表示されます。

① AI Advisor から、質問に対する回答が出力されます。

3.2. 追加質問のレコメンド

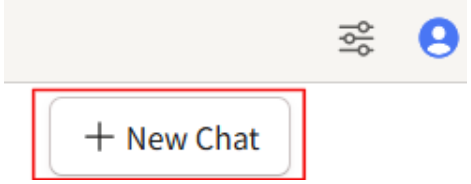
① AI Advisor の回答後に表示される追加質問のレコメンドをクリックし、実行ボタンをクリックします。
例：「私が担当するシステムが OpenSSH を利用していますか」をクリックします
※自担当のシステム情報について回答する場合は、「4.RAG 機能」の参照フォルダの指定を実施してください

② AI Advisor が追加質問に対して回答します。



3.3. 新規チャットの作成

[New Chat]をクリックすることで、新規チャットを開始します。



4. 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。
AI Advisor 回答時にフォルダを参照するかどうかは選択可能とします。

4.1. 参照フォルダの指定

[参照フォルダ]をクリックし、参照する RAG のフォルダを選択し、[閉じる]をクリックします。

4.2. 質問入力および回答

① 質問を入力し、実行ボタンをクリックします。
例：「CVE-2024-6387 の脆弱性が社内システムに影響するか教えてください。」と入力

② 選択した RAG のフォルダを参照し、AI Advisor から質問に対する回答が出力されます。[★数字]を選択することで、参照したファイルの情報を確認可能です。
※[★数字]の数字は、質問に対する適合度が高いファイルほど大きい数字になります。

CVE-2024-6387はOpenSSHのサーバー（sshd）におけるセキュリティ上のリグレッション（CVE-2006-5051）に関する脆弱性です。認証されていないリモートの攻撃者が、設定された時間内に認証に失敗することで、sshdがシグナルを安全でない方法で処理する競合状態を悪用する可能性があります。これにより、機密性、完全性、可用性に高い影響を与える可能性があります。
この脆弱性は、OpenSSHサーバーのバージョン9.8より前のバージョンに影響します。社内システムでOpenSSHを使用している場合は、影響を受ける可能性があります。
CVE-2024-6387に関する詳細情報は以下のURLからも確認できます。

- [redacted]

ご利用のOpenSSHサーバーのバージョンをご確認いただき、必要に応じてアップデートや対策をご検討ください。

該当ファイルを見る

★10 ★9 ★8 ★7 ★6 ★5 ★4 ★3 ★2 ★1

適合度 0.67 【運用情報】システム概要書_91.md.txt

システム名: **AI協奏型サイバー攻撃予測・防御プラットフォーム "Aegis Mind"**

コンセプト: AI技術を駆使し、サイバー攻撃の発生を未然に予測し、組織のネットワーク、システム、データを自動的に防御するプラットフォーム。従来のセキュリティシステムのように、過去の攻撃パターンや既知の脆弱性に依存するのではなく、AIがサイバー攻撃者の行動、技術、動機を分析し、未来の攻撃を予測し、先手を打つことで、組織を高度なサイバー脅威から保護する。

独自性:

* **多層的脅威インテリジェンス収集:** 世界中のセキュリティ情報源、ダークウェブ、ソーシャルメディア、技術フォーラムなどからの情報を収集し、AIがリアルタイムに分析し、最新の脅威動向を把握する。
* **攻撃者のプロファイリング:** AIが過去の攻撃事例、マルウェアのコード、攻撃者の通信パターンなどを分析し、攻撃者のスキル、目的、戦略を予測する。

5. 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基づき回答する機能を提供します。

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。

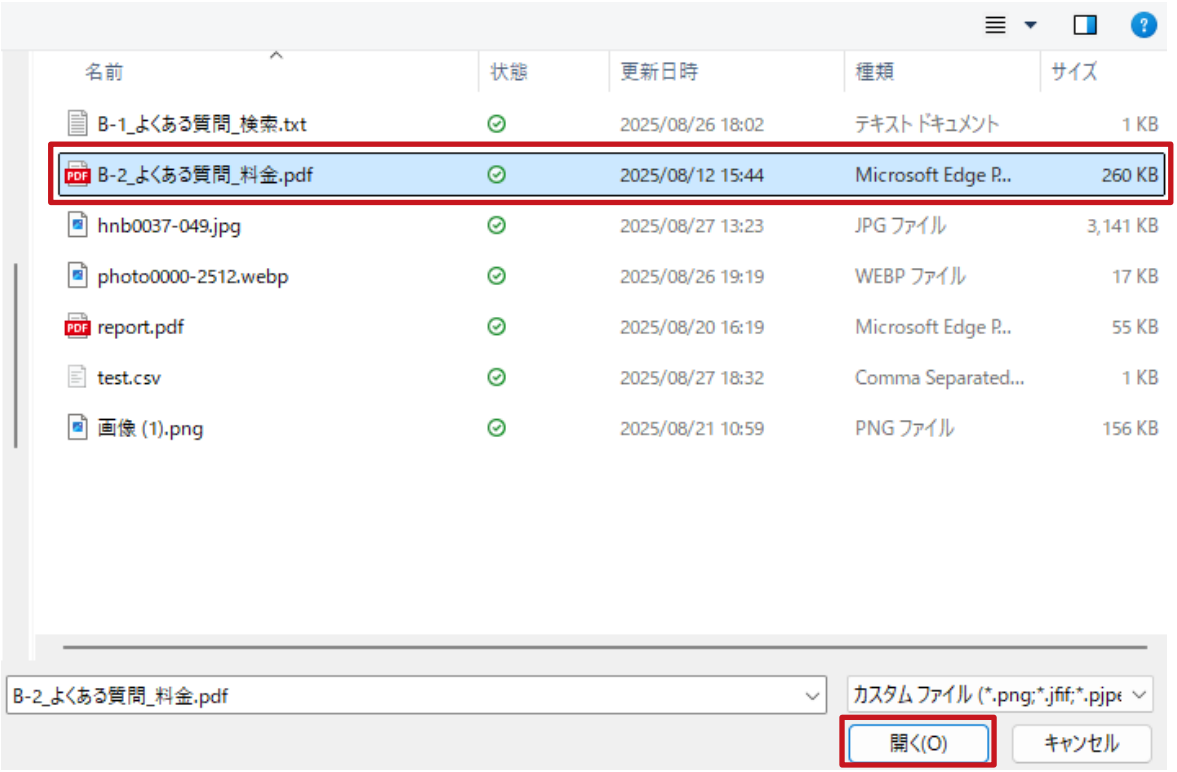
形式	1 ファイルあたりのサイズ上限
ドキュメント：TXT、CSV、PDF 画像：PNG、JPEG、WebP	6MB 未満

※文字コードについては、UTF-8 をサポートしています。

5.1. 添付ファイルの指定

① 左下の添付ファイルアイコンをクリックします。

② 添付するファイルを選択し、[開く]をクリックします。



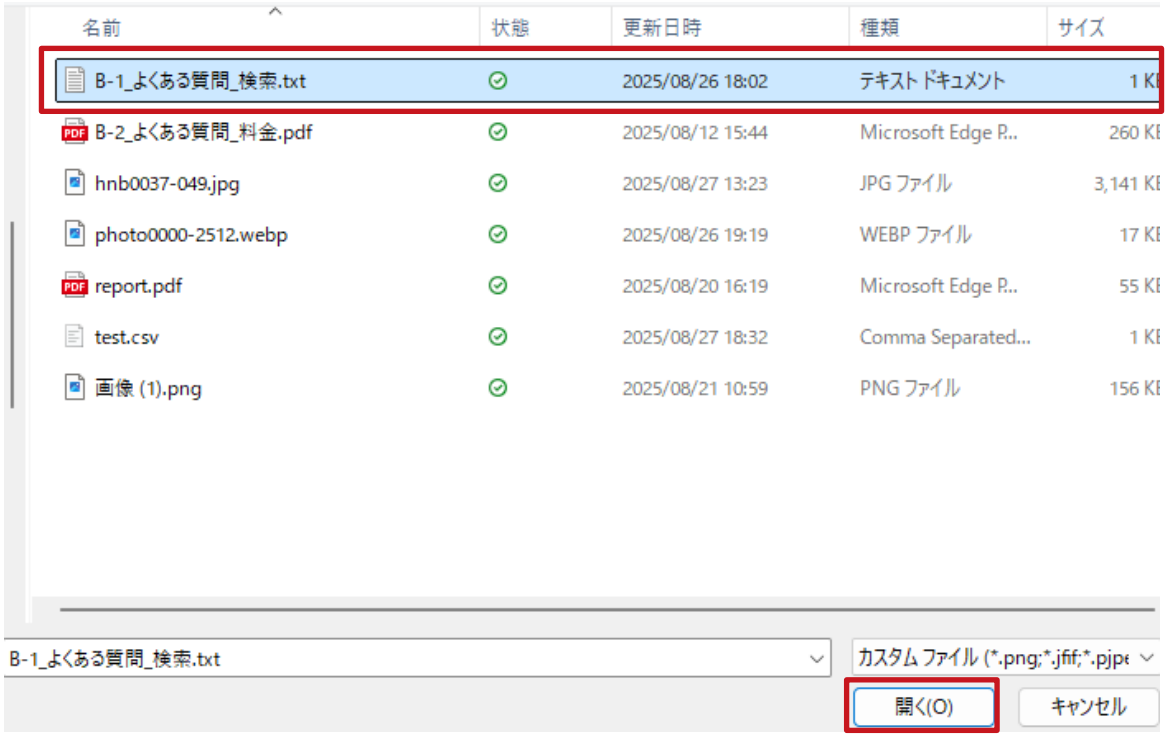
③　質問の下にアップロードされた添付ファイルが表示されます。
　　質問を入力し、実行ボタンをクリックします。

④　添付ファイルに基づき回答が出力されます。

5.2. 添付ファイルの変更

①　左下の添付ファイルアイコンをクリックします。

②　変更するファイルを選択し、[開く]をクリックします。



③　質問の下にアップロードされた添付ファイルが表示されます。

5.3. 添付ファイルの削除

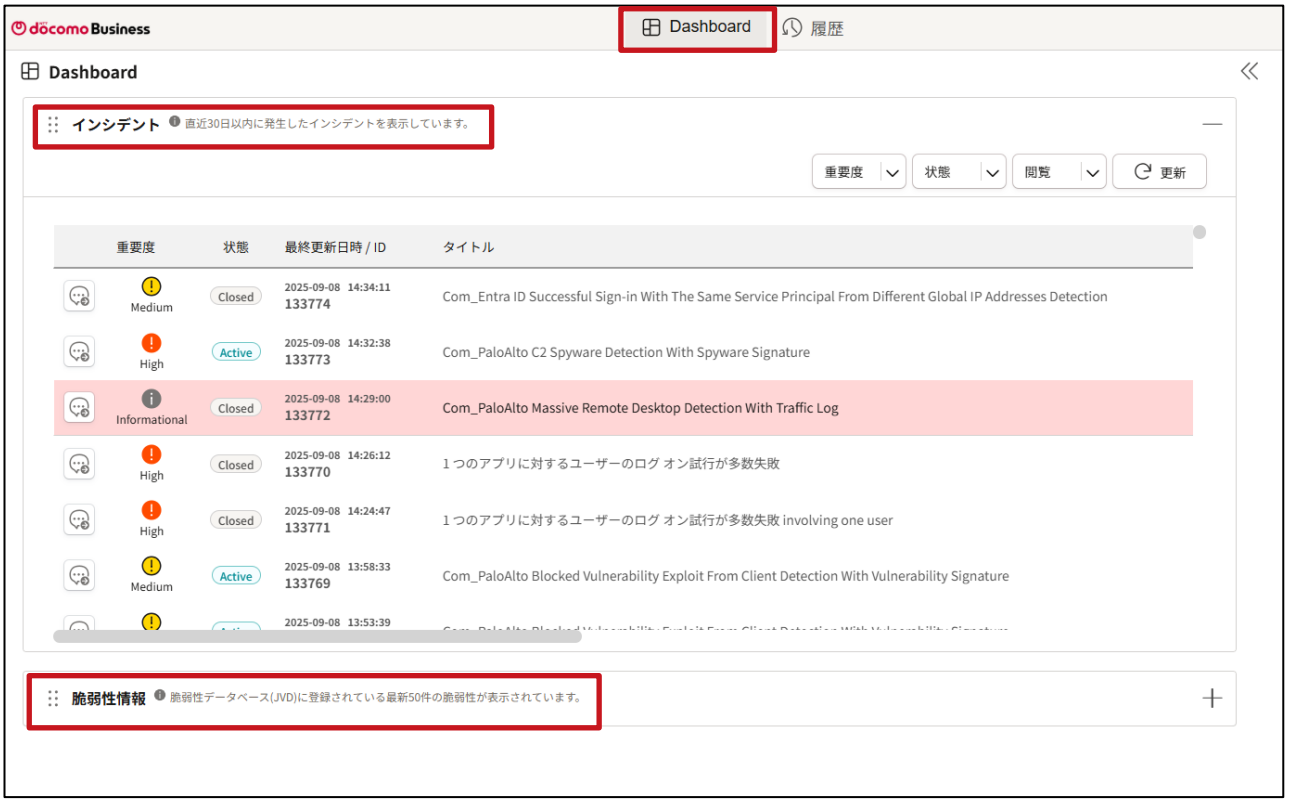
①　添付ファイルの×をクリックします。

6. ダッシュボード機能

Microsoft Sentinel と連携し、インシデント一覧を表示する「インシデントダッシュボード」と、JVNDB の情報を取得し、脆弱性情報の一覧を表示する「脆弱性情報ダッシュボード」を提供します。
※インシデント一覧は Microsoft Sentinel をご利用のお客さまが連携設定した場合のみ使用可能です。

6.1. 一覧表示

Dashboard>インシデント、または Dashboard>脆弱性情報に移動するとインシデントおよび脆弱性情報の一覧を表示します。



6.2. インシデントレポートの作成

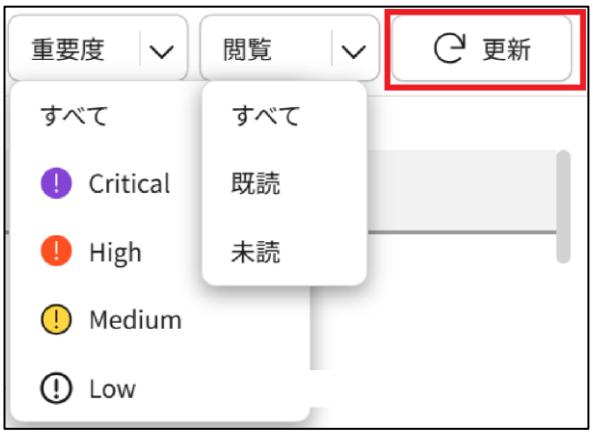
インシデントの一覧を開き、[更新]をクリックすると、最新のインシデントを一覧表示します。

[重要度]、[状態] 、[閲覧]のプルダウンをクリックし、表示される項目を選択することで一覧表示をフィルタリングします。

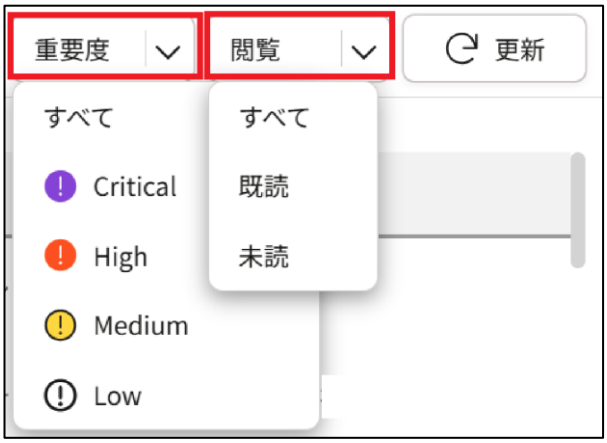
[レポート作成]をクリックすると、自動的にプロンプトが入力されます。実行ボタンをクリックし、AI Advisor に質問することで、対象のインシデントのレポートを回答します。

6.3. 脆弱性情報の確認

脆弱性情報の一覧を開き、[更新]をクリックすると、最新の脆弱性情報を一覧表示します。



[重要度]や[閲覧]のプルダウンをクリックし、表示される項目を選択することで一覧表示をフィルタリングします。



[AI Advisor に聞く]をクリックすると、自動的にプロンプトが入力されます。実行ボタンをクリックし、AI Advisor に質問することで、対象の脆弱性情報の解説、対処方法を回答します。

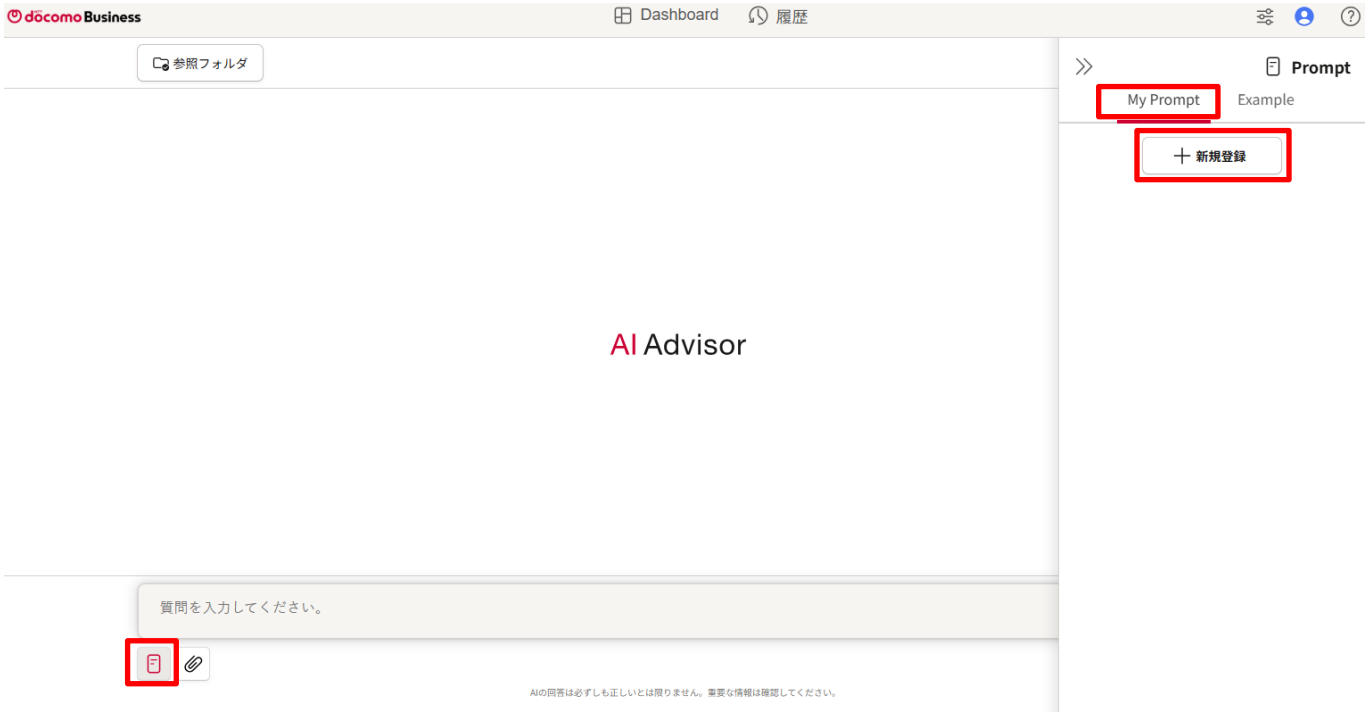
7. プロンプトテンプレート機能

AI Advisor 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。

7.1. プロンプトテンプレートの新規登録

① Prompt のアイコンをクリックし、Prompt を表示させます。

② My Prompt で[新規登録]をクリックします。



③ 名前（必須）、説明（任意）、プロンプト（必須）に入力し、[保存]をクリックします。

7.2. プロンプトテンプレートの適用

① 対象のプロンプトテンプレートの 3 点リーダーにカーソルを合わせ、[適用]をクリックします。
※プロンプトに変数を設定していない場合、手順②はスキップしてください。

② 変数に代入する文字列を入力し、[適用]をクリックします。

③　適用したプロンプトが質問入力欄に自動的に出力されます。

7.3. プロンプトテンプレートの削除

①　対象のプロンプトテンプレートの 3 点リーダーにカーソルを合わせ、[削除]をクリックします。

②　ウインドウが表示され、[削除]をクリックします。

7.4. プロンプトテンプレートの編集

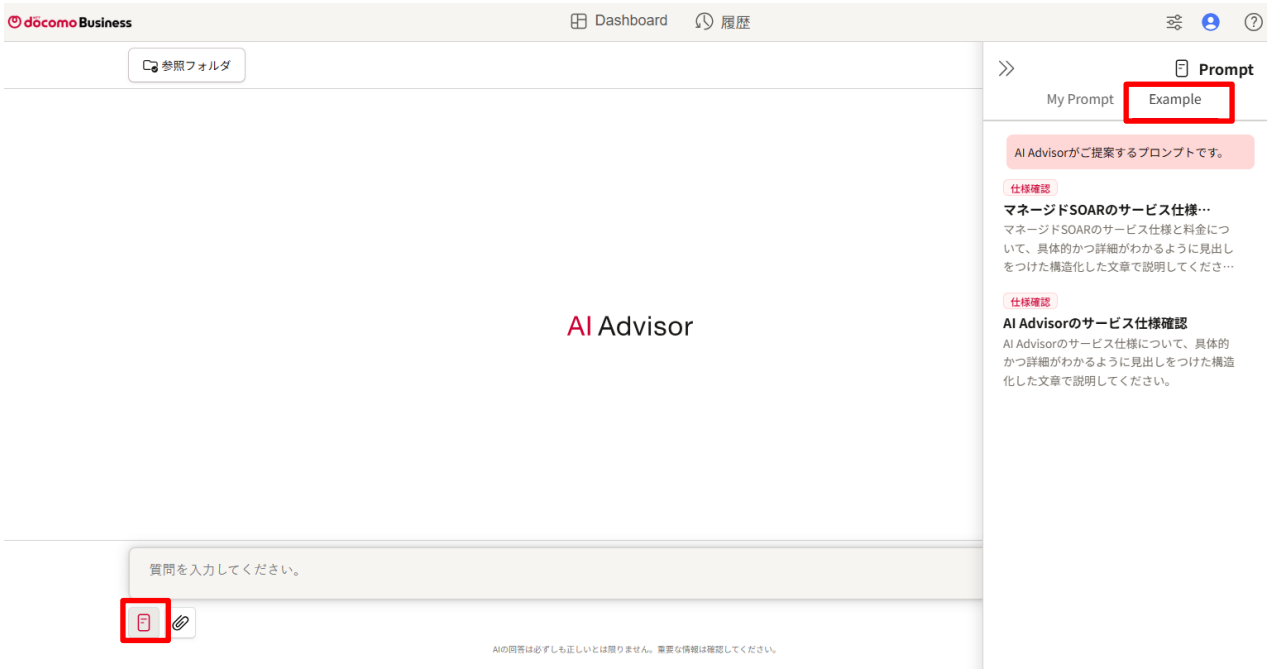
① 対象のプロンプトテンプレートの 3 点リーダーにカーソルを合わせ、[編集]をクリックします。

② プロンプトテンプレートを編集し、[保存]をクリックします。

7.5. システムに登録済のプロンプトの使用

Prompt のアイコンをクリックし、Prompt を表示させます。

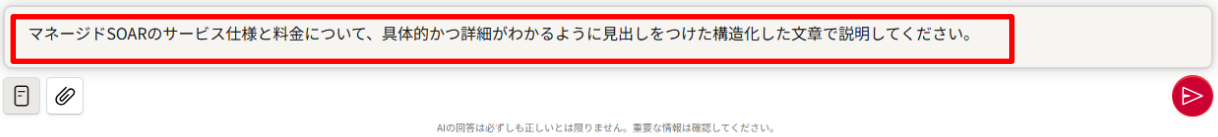
Example をクリックすると AI Advisor に予め登録されているプロンプトが使用できます。



7.6. システムに登録済のプロンプトの適用

① 対象のプロンプトテンプレートの 3 点リーダーにカーソルを合わせ、[適用]をクリックします。

② 適用したプロンプトが質問入力欄に自動的に出力されます。

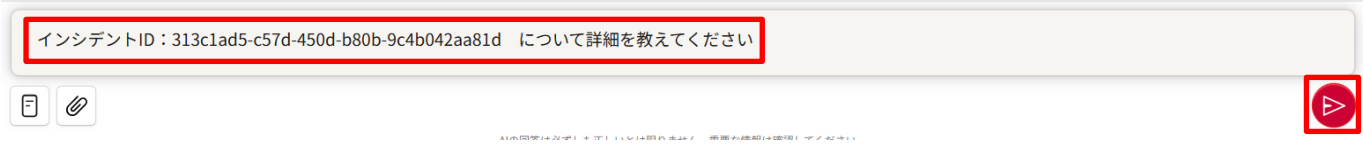


8. インシデントレポート生成機能

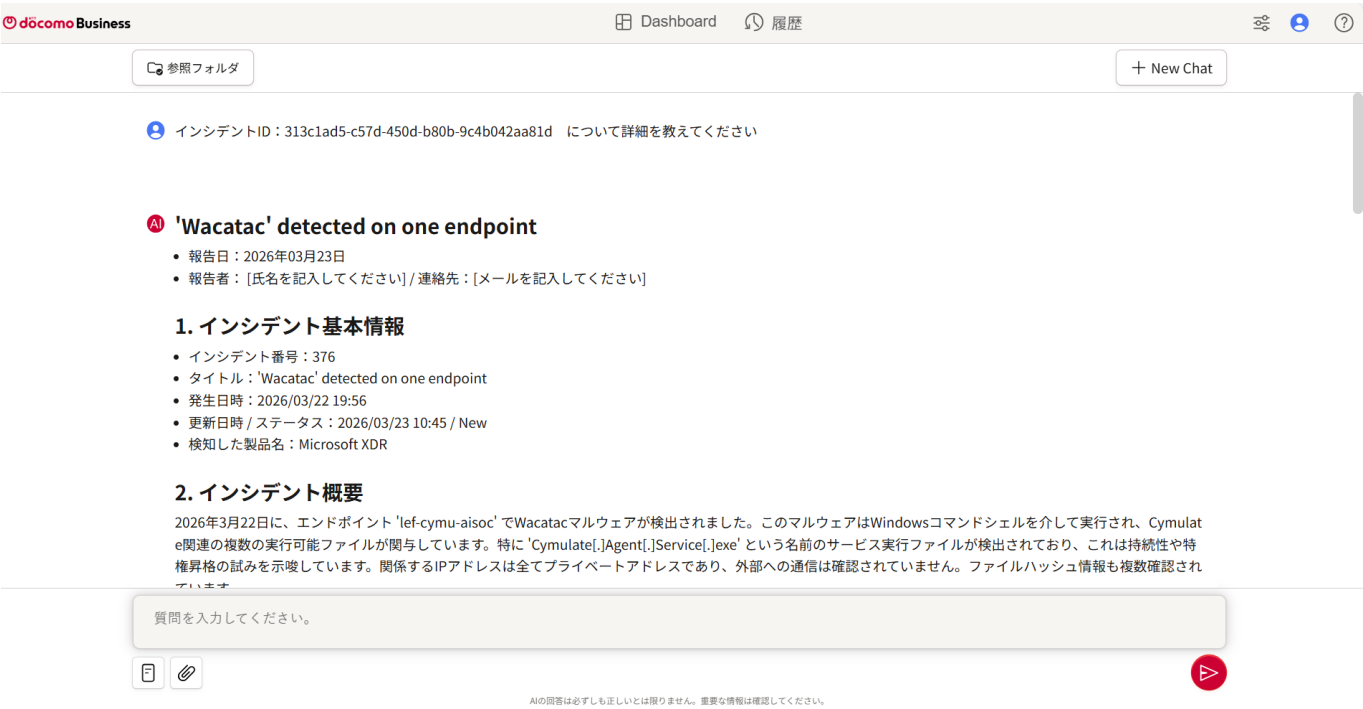
インシデントの関連情報／MITRE ATT&CK 情報／脅威インテリジェンス情報を基に、発生したインシデントに関するインシデントレポートを生成する機能を提供します。

8.1. インシデントレポート生成

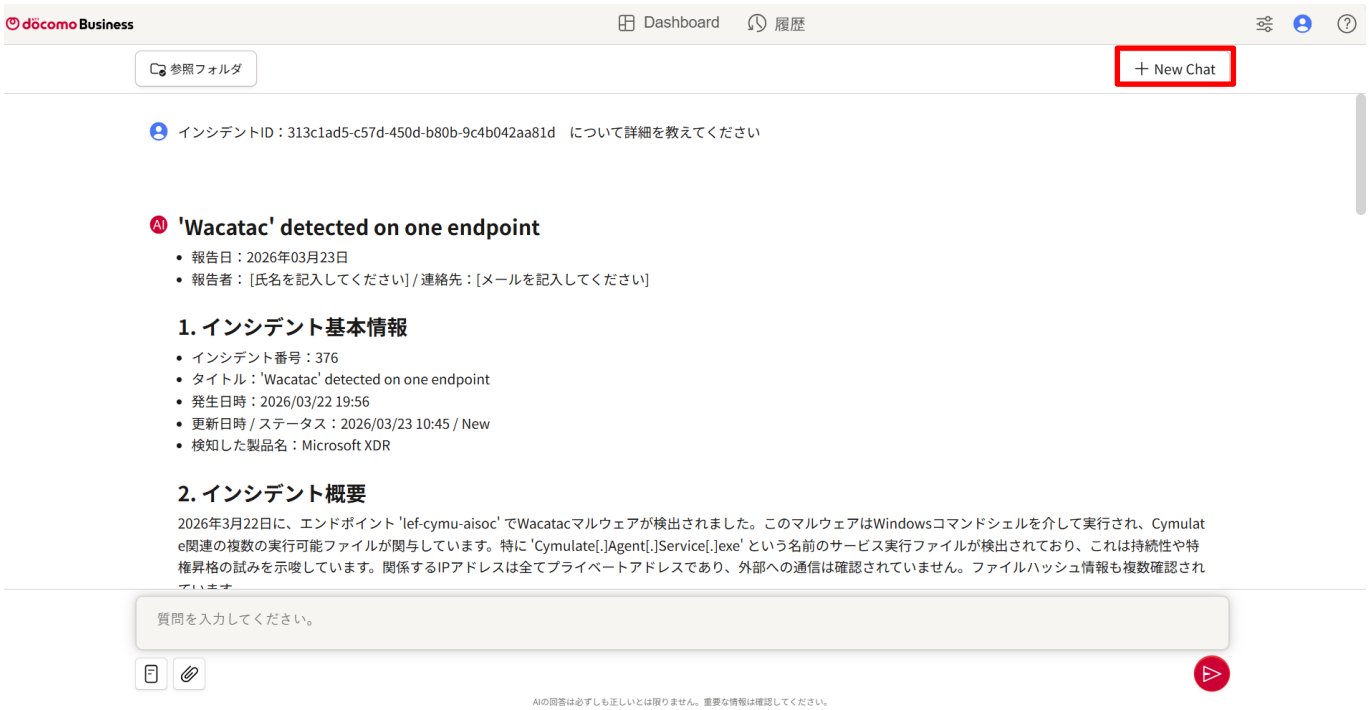
- 質問を入力し、実行ボタンをクリックします。
  例：「インシデント ID：313c1ad5-c57d-450d-b80b-9c4b042aa81d について詳細を教えてください」と入力



- 入力インシデント ID に関するインシデントレポートが生成されます。



- 別のインシデント ID に対してレポートを作成する場合は、「New Chat」を押下してください。



8.2. アーティファクトの参照

分析の過程で参照したデータ(アーティファクト)を証跡として参照できる機能を提供します。

- レポート下部に表示される「収集データを見る（分類：○○）」の参照したい情報をクリックします。
  「収集データを見る（分類：Sentinel）」
  ：Microsoft Sentinel の API で取得した情報を参照可能です。
  「収集データを見る（分類：○○(IP、Domain、URL)）」
  ：IP／Domain／URL それぞれの脅威インテリジェンス情報を参照可能です。

- 数字ボタンをクリックしてアーティファクト情報を参照可能です。

9. 脅威インテリジェンス連携機能

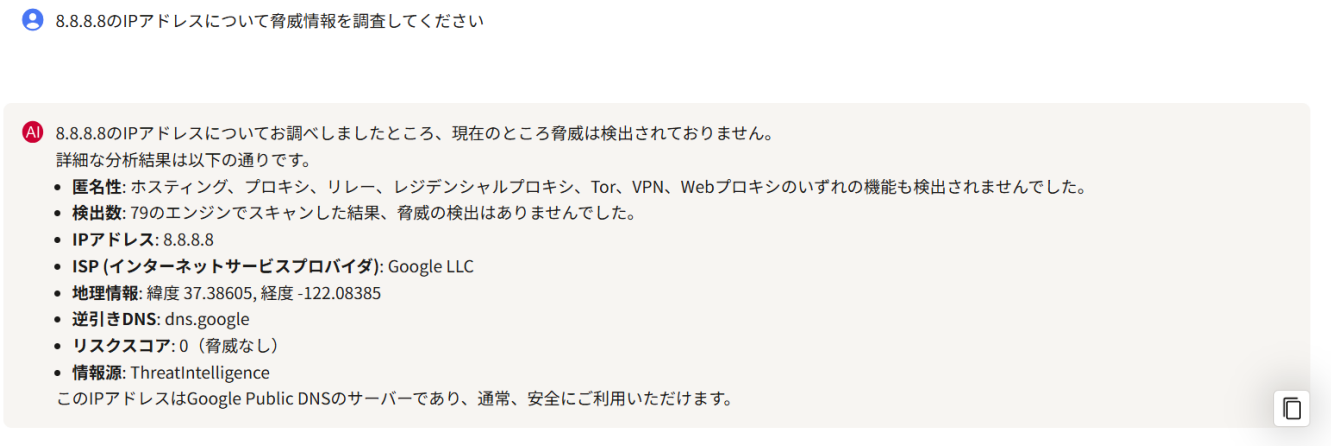
脅威インテリジェンス情報を参照し IP／ドメイン／URL の危険性を分析・評価して回答をする機能を提供します。

9.1. 脅威インテリジェンス連携

- 質問を入力し、実行ボタンをクリックします。

  例：「8.8.8.8 の IP アドレスについて脅威情報を調査してください」と入力

- 脅威インテリジェンス情報に基づき、回答が出力されます。



10. Zscaler（ZIA）連携機能

Zscaler（ZIA）の API を利用し、URL フィルタリング設定情報を参照して回答をする機能を提供します。

10.1. ZIA 連携

① 質問を入力し、実行ボタンをクリックします。

例：「「www.ntt.com」がどのポリシーが原因でブロックされているか確認してください」と入力

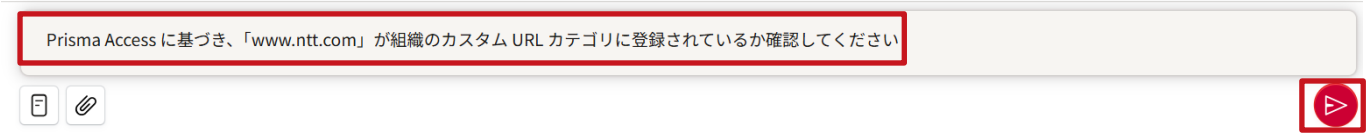
② ZIA の URL フィルタリング設定情報に基づき、回答が出力されます。

11. Prisma Access 連携機能

Prisma Access の API を利用し、URL フィルタリング設定情報を参照して回答をする機能を提供します。

11.1. Prisma Access 連携

- 質問を入力し、実行ボタンをクリックします。
  例：「Prisma Access に基づき「www.ntt.com」が組織のカスタム URL カテゴリに登録されているか確認してください」と入力



- Prisma Access の URL フィルタリング設定情報に基づき、回答が出力されます。

12. 設定管理機能

以下の AI Advisor 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

12.1. トーン調整

設定に移動し、AI Advisor の回答のトーンを調節します。

12.2. 形式調整

設定に移動し、AI Advisor の回答の形式を調節します。

12.3. 長さ調整

設定に移動し、AI Advisor の回答の長さを調節します。

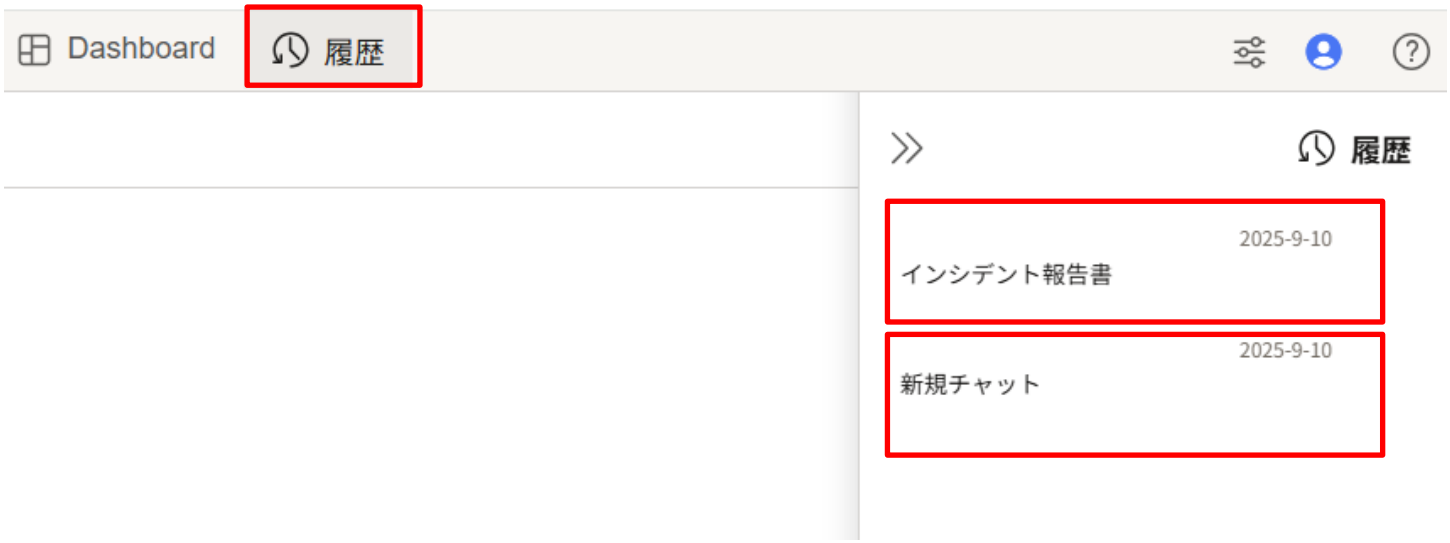
13. 履歴管理機能

同一セッション内での問合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 時間経過し、セッションが変わるとリセットされます。

13.1. 履歴の参照

[履歴]をクリックし、表示される履歴を選択することで過去のチャットを参照します。



13.2. 履歴の削除

① 対象の履歴にカーソルを合わせ、ゴミ箱ボタンをクリックします。

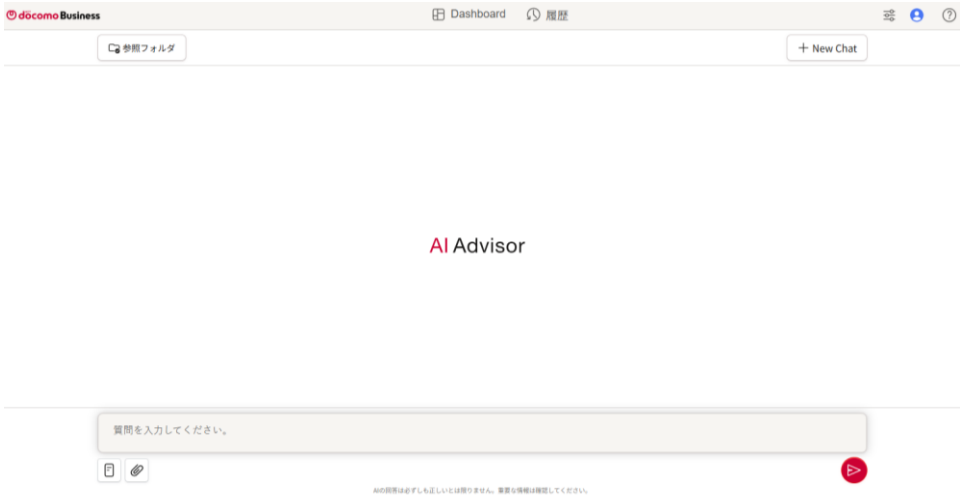
② ウインドウが表示され、[削除]をクリックします。

14. その他

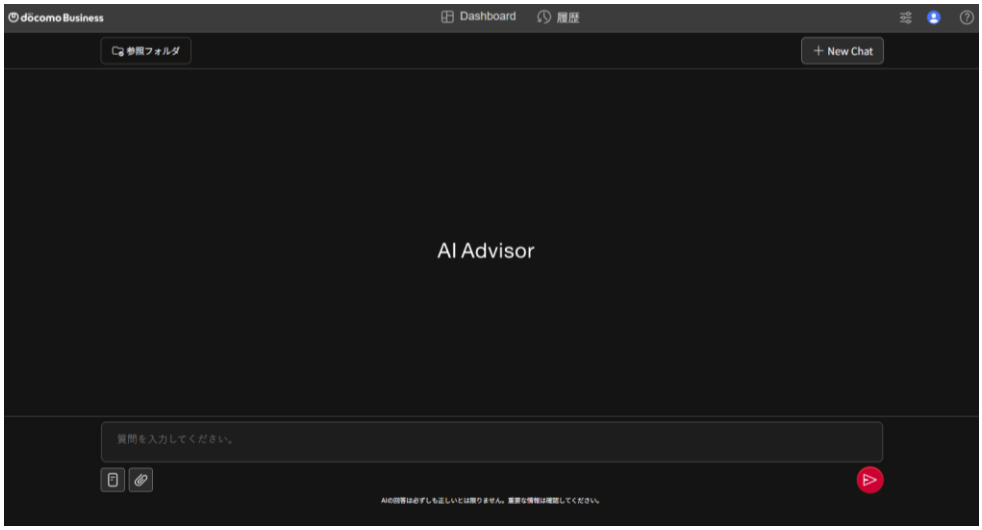
14.1. カラーモードの変更

カラーモードを選択することで、AI Advisor の外観を変更します。

■ライトモード

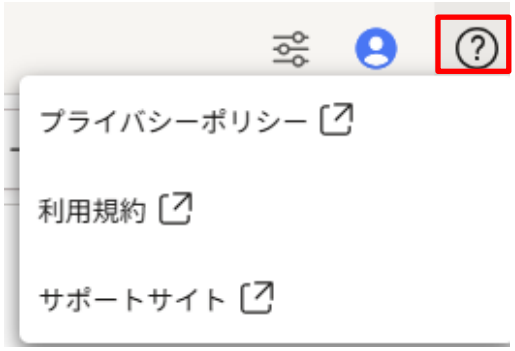


■ダークモード



14.2. サポートリンク

？を押下することで、サポートリンク集を開きます。



サポートリンクの遷移先は下記を参照しています。

・プライバシーポリシー：https://www.ntt.com/about-us/hp/privacy.html

・利用規約：https://www.ntt.com/content/dam/nttcom/hq/jp/about-us/disclosure/tariff/pdf/c419.pdf

・サポートサイト：https://support.ntt.com/aiadvisor/

改訂履歴

バージョン	主な変更	日付
1.0 版	初版発行	2025 年 5 月 27 日
1.1 版	商号変更に伴い、企業名、ロゴ、コピーライトの変更 6.5～6.6 システムに登録済のプロンプトの説明追加 9.2 サポートリンクの説明追加	2025 年 7 月 1 日
1.2 版	社名変更に伴い、ヘッダーのドコモビジネスのロゴを差し替え デザイン変更に伴い、画面イメージを最新化 2. ユーザー認証機能の内容を SAML 認証を前提とした記載に変更 5. 添付ファイルに関する文章生成機能の説明追加 8. Sentinel 連携機能を追加 9. Zscaler（ZIA）連携機能を追加	2025 年 10 月 1 日
2.0 版	1.1.一部注意文言の削除(「この資料は作成時に限られた検証環境における結果にもとづいて作成しているため、お客さま固有の環境に対して適切であるか十分に検証されていないことをあらかじめご了承ください」) 3. 質疑応答機能にインシデントの質問に関する補足追加 3.1 質問入力および回答にプログレスの表示に関する説明追加 8.インシデントレポート生成機能を追加 9.脅威インテリジェンス連携機能を追加 11.Prisma Access 連携機能を追加	2026 年 4 月 1 日