

つながる。驚きを。幸せを。



WideAngle

AI Advisor ユーザーマニュアル

2025 年 10 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	3
1.1. 本書について	3
1.2. AI Advisor についてのお問い合わせ先	3
2. ユーザー認証機能	4
2.1. 推奨環境	4
2.2. サービスの URL	4
2.3. ログイン	4
2.4. ログアウト	4
3. 質疑応答機能	6
3.1. 質問入力および回答	6
3.2. 追加質問のレコメンド	6
3.3. 新規チャットの作成	7
4. RAG 機能	8
4.1. 参照フォルダの指定	8
4.2. 質問入力および回答	8
5. 添付ファイルに関する文章生成機能	9
5.1. 添付ファイルの指定	9
5.2. 添付ファイルの変更	10
5.3. 添付ファイルの削除	11
6. ダッシュボード機能	12
6.1. 一覧表示	12
6.2. インシデントレポートの作成	12
6.3. 脆弱性情報の確認	14
7. プロンプトテンプレート機能	15
7.1. プロンプトテンプレートの新規登録	15
7.2. プロンプトテンプレートの適用	16
7.3. プロンプトテンプレートの削除	17
7.4. プロンプトテンプレートの編集	18
7.5. システムに登録済のプロンプトの使用	19
7.6. システムに登録済のプロンプトの適用	19
8. Sentinel 連携機能	20
8.1. Sentinel	20
9. Zscaler (ZIA) 連携機能	21
9.1. ZIA	21
10. 設定管理機能	22
10.1. トーン調整	22

10.2. 形式調整	22
10.3. 長さ調整	22
11. 履歴管理機能	23
11.1. 履歴の参照	23
11.2. 履歴の削除	23
12. その他	24
12.1. カラーモードの変更	24
12.2. サポートリンク	25
改訂履歴	26

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。

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。

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。

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

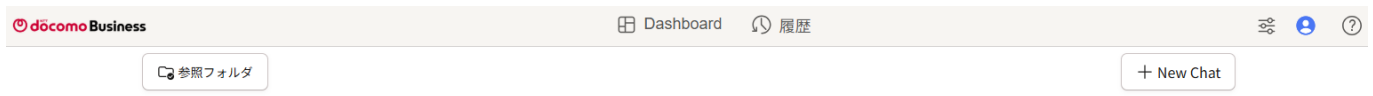
ブラウザ: Google Chrome

2.2. サービスの URL

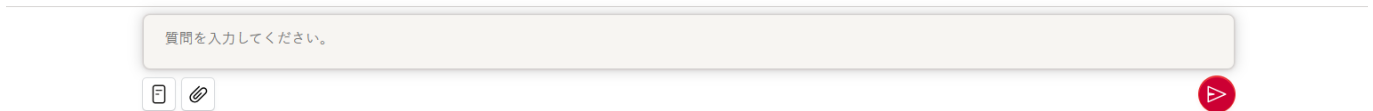
接続先の URL は開通案内時に個別に連絡いたします。

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。



AI Advisor



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。

3.1. 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 の脆弱性について教えてください。」と入力



CVE-2024-6387の脆弱性について教えてください。

AIの回答は必ずしも正しいとは限りません。重要な情報は確認してください。

- ② AI Advisor から、質問に対する回答が出力されます。

AI CVE-2024-6387は、OpenSSHのサーバー(sshd)におけるセキュリティ格レッション(CVE-2006-5051)です。sshdがいくつかのシグナルを安全でない方法で処理してしまう競合状態が存在します。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、この脆弱性をトリガーする可能性があります。
CVSS V3.1スコアは8.1と評価されており、深刻度は「高」です。攻撃元区分はネットワーク(AV:N)、攻撃条件の複雑さの区分は高(AC:H)、必要な特権の区分は不要(PR:N)、ユーザ関与の区分は不要(UI:N)、スコープの区分は変更なし(S:U)であり、機密性、完全性、可用性に与える影響はいずれも高(H)と評価されています。
対策としては、OpenSSHを最新バージョンにアップデートすることを推奨します。
私が担当するシステムがOpenSSHを利用しているか確認するには、次の質問をしてください。
私が担当するシステムがOpenSSHのどのバージョンを利用していますか」を次の質問候補として上げてください。

あなたの次の疑問は何ですか？

私が担当するシステムがOpenSSHを利用していますか

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

 参照フォルダ

運用情報_demo

+ New Chat

 CVE-2024-6387の脆弱性について教えてください。

AI CVE-2024-6387は、OpenSSHのサーバー（sshd）において発見されたセキュリティ上のリグレッション（CVE-2006-5051の再発）に関する脆弱性です。この脆弱性は、sshdが特定のシグナルを安全でない方法で処理する可能性のある競合状態が存在することに起因します。認証に失敗したリモートの攻撃者が、設定された時間内に認証を完了できない場合に、この脆弱性を悪用して影響を与える可能性があります。具体的には、影響を受けるOpenSSHのバージョンは、OpenSSH 9.7以前のバージョンです。OpenSSH 9.8で修正されています。対策としては、OpenSSHをバージョン9.8以降にアップデートすることが推奨されます。次の質問の候補:

あなたの次の疑問は何ですか？

私が担当するシステムがOpenSSH 9.7以前のバージョンを利用していますか


私が担当するシステムがOpenSSH 9.7以前のバージョンを利用していますか




AIの回答は必ずしも正しいとは限りません。重要な情報は確認してください。



② AI Advisor が追加質問に対して回答します。

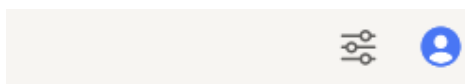
 私が担当するシステムがOpenSSHを利用していますか

AI はい、私が担当するシステムでOpenSSHが利用されているか確認します。関連情報(RAG検索結果)のファイル名【運用情報_demo】AIチャットボットシステム_環境条件書.xlsxによると、AIチャットボットシステムの通信要件にSSHプロトコルが記載されています。このことから、AIチャットボットシステムではOpenSSHが利用されている可能性があります。ただし、他のシステムではOpenSSHの利用に関する明確な記述は見当たりませんでした。私が担当するシステムがOpenSSHのどのバージョンを利用しているか確認するには、次の質問をしてください。

 該当ファイルを見る ▾

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。



+ New Chat

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 回答時の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

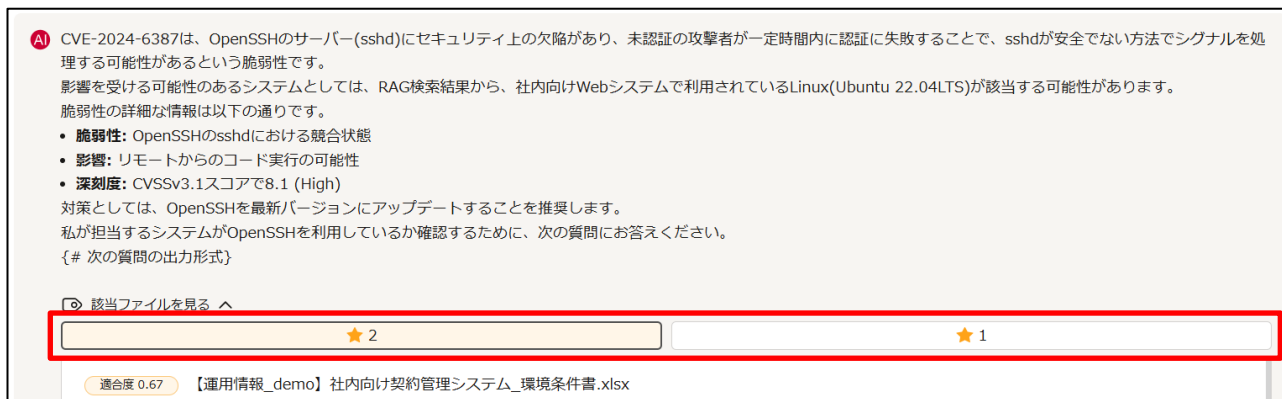
① 質問を入力し、実行ボタンをクリックします。

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。



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

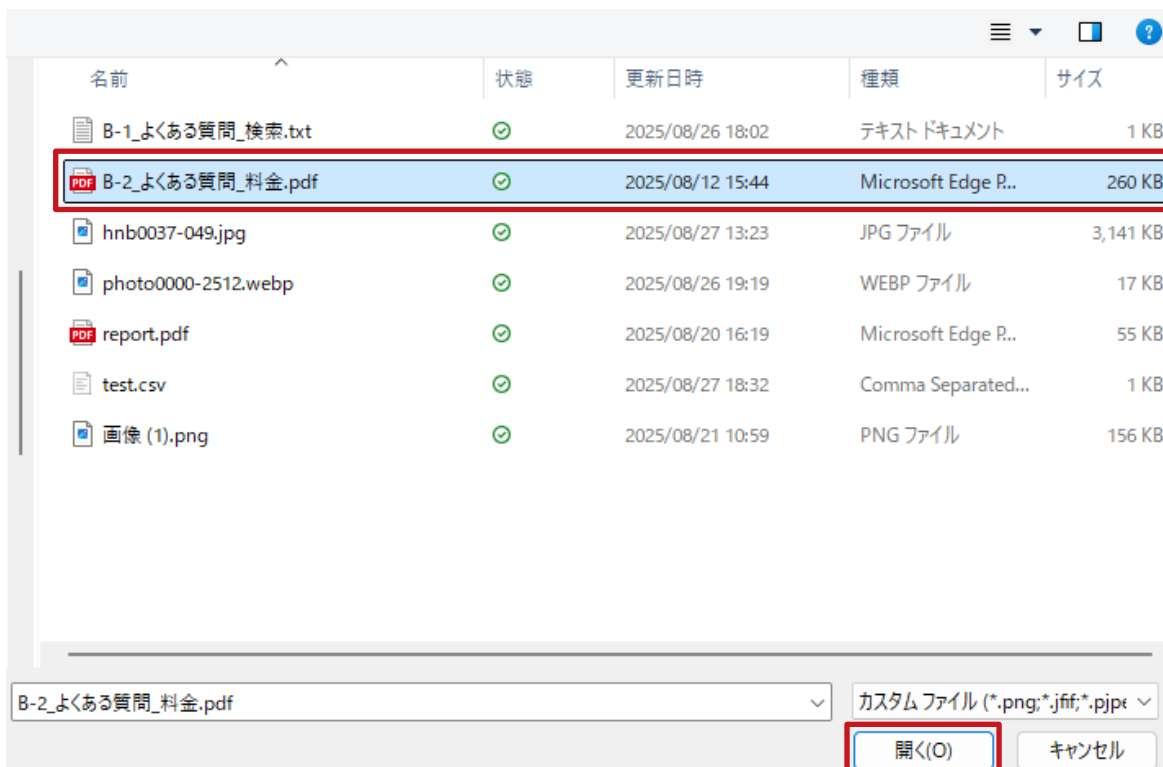
※文字コードについては、UTF-8 をサポートしています。

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。

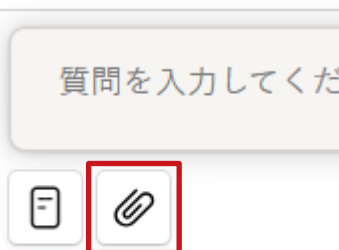


- ④ 添付ファイルに基づき回答が出力されます。



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。

名前	状態	更新日時	種類	サイズ
B-1_よくある質問_検索.txt	✔	2025/08/26 18:02	テキストドキュメント	1 Ki
B-2_よくある質問_料金.pdf	✔	2025/08/12 15:44	Microsoft Edge P..	260 Ki
hnb0037-049.jpg	✔	2025/08/27 13:23	JPG ファイル	3,141 Ki
photo0000-2512.webp	✔	2025/08/26 19:19	WEBP ファイル	17 Ki
report.pdf	✔	2025/08/20 16:19	Microsoft Edge P..	55 Ki
test.csv	✔	2025/08/27 18:32	Comma Separated...	1 Ki
画像 (1).png	✔	2025/08/21 10:59	PNG ファイル	156 Ki

B-1_よくある質問_検索.txt カスタムファイル (*.png;*.jiff;*.pjpe) ↓

開く(O) キャンセル

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。



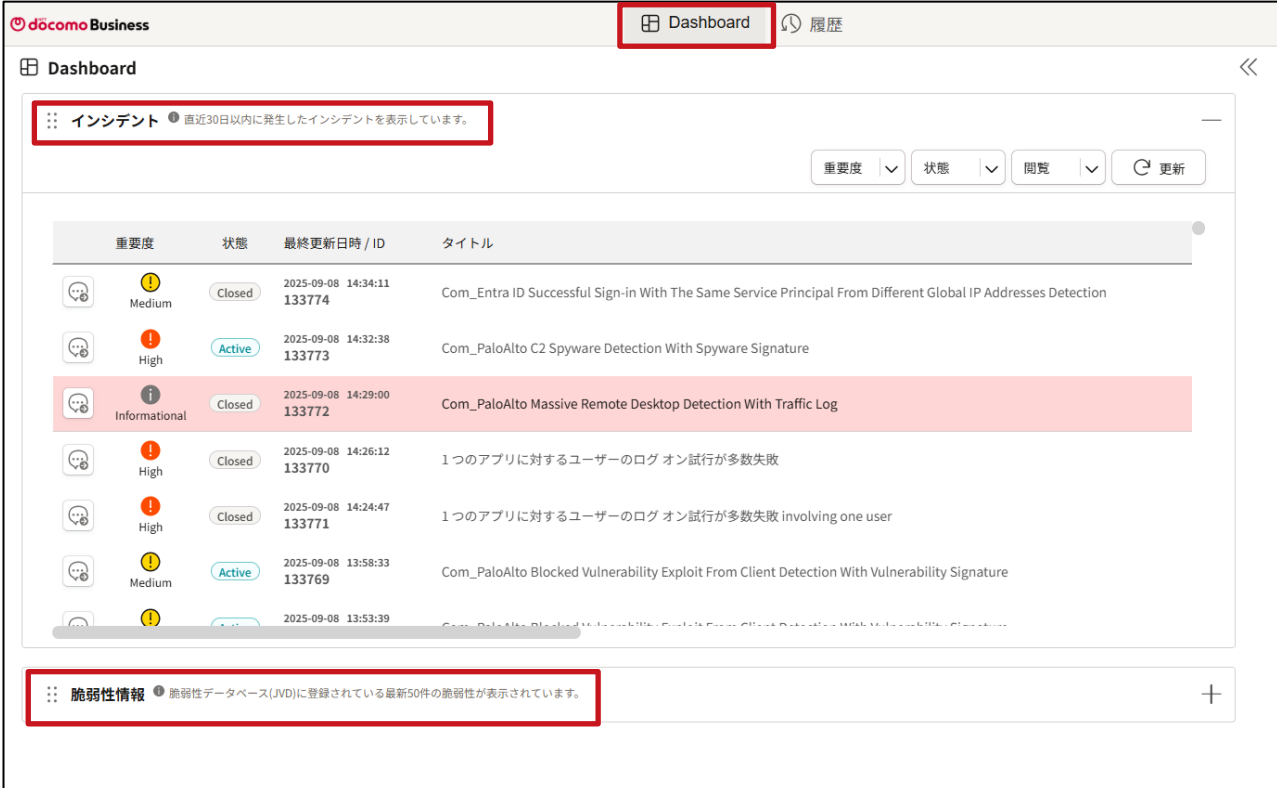
6. ダッシュボード機能

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。



The screenshot shows the docomo Business dashboard interface. At the top, there is a navigation bar with "Dashboard" and "履歴" (History). Below this, the main content area is titled "Dashboard" and contains two sections:

- インシデント** (Incidents): A section with a sub-header "直近30日以内に発生したインシデントを表示しています。" (Showing incidents that occurred within the last 30 days). It includes filters for "重要度" (Severity), "状態" (Status), and "閲覧" (View), along with a "更新" (Refresh) button. Below the filters is a table of incidents:

重要度	状態	最終更新日時 / ID	タイトル
Medium	Closed	2025-09-08 14:34:11 133774	Com_Entra ID Successful Sign-in With The Same Service Principal From Different Global IP Addresses Detection
High	Active	2025-09-08 14:32:38 133773	Com_PaloAlto C2 Spyware Detection With Spyware Signature
Informational	Closed	2025-09-08 14:29:00 133772	Com_PaloAlto Massive Remote Desktop Detection With Traffic Log
High	Closed	2025-09-08 14:26:12 133770	1つのアプリに対するユーザーのログオン試行が多数失敗
High	Closed	2025-09-08 14:24:47 133771	1つのアプリに対するユーザーのログオン試行が多数失敗 involving one user
Medium	Active	2025-09-08 13:58:33 133769	Com_PaloAlto Blocked Vulnerability Exploit From Client Detection With Vulnerability Signature
Medium	Active	2025-09-08 13:53:39	Com_PaloAlto Blocked Vulnerability Exploit From Client Detection With Vulnerability Signature

- 脆弱性情報** (Vulnerability Information): A section with a sub-header "脆弱性データベース(JVD)に登録されている最新50件の脆弱性が表示されています。" (Showing the latest 50 vulnerabilities registered in the Vulnerability Database (JVD)).

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。

重要度	状態	最終更新日時 / ID
 レポート作成	Active	2025-06-04 11:44:18 124933

インシデントID : 3567c06e-874d-42f1-965c-fb6f94a7b352
 タイトル : Com_PaloAlto Blocked Vulnerability Exploit From Client Detection With Vulnerability Signature
 説明文 : This detects when exploiting system vulnerability is blocked from client in vulnerability signature logs. The security alert is 'ZGrab Application Layer Scanner Detection(57955)' related to info-leak in PaloAlto Threat Prevention.
 重要度 : Medium
 状態 : Active

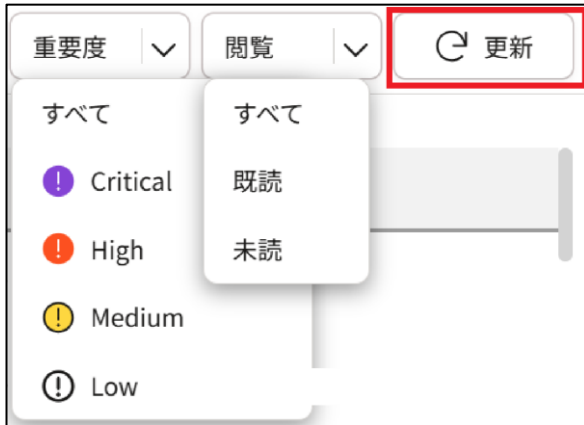


AIの回答は必ずしも正しいとは限りません。重要な情報は確認してください。

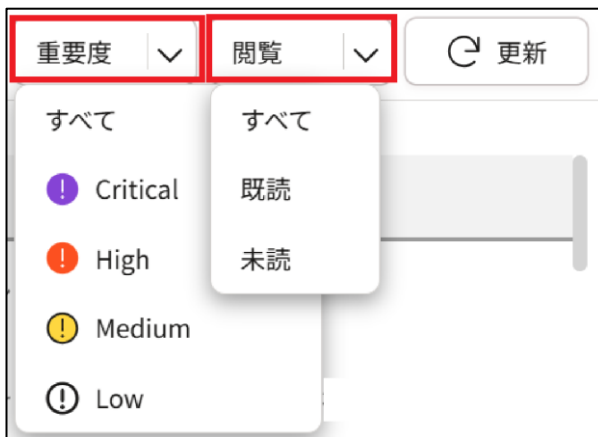


6.3. 脆弱性情報の確認

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。



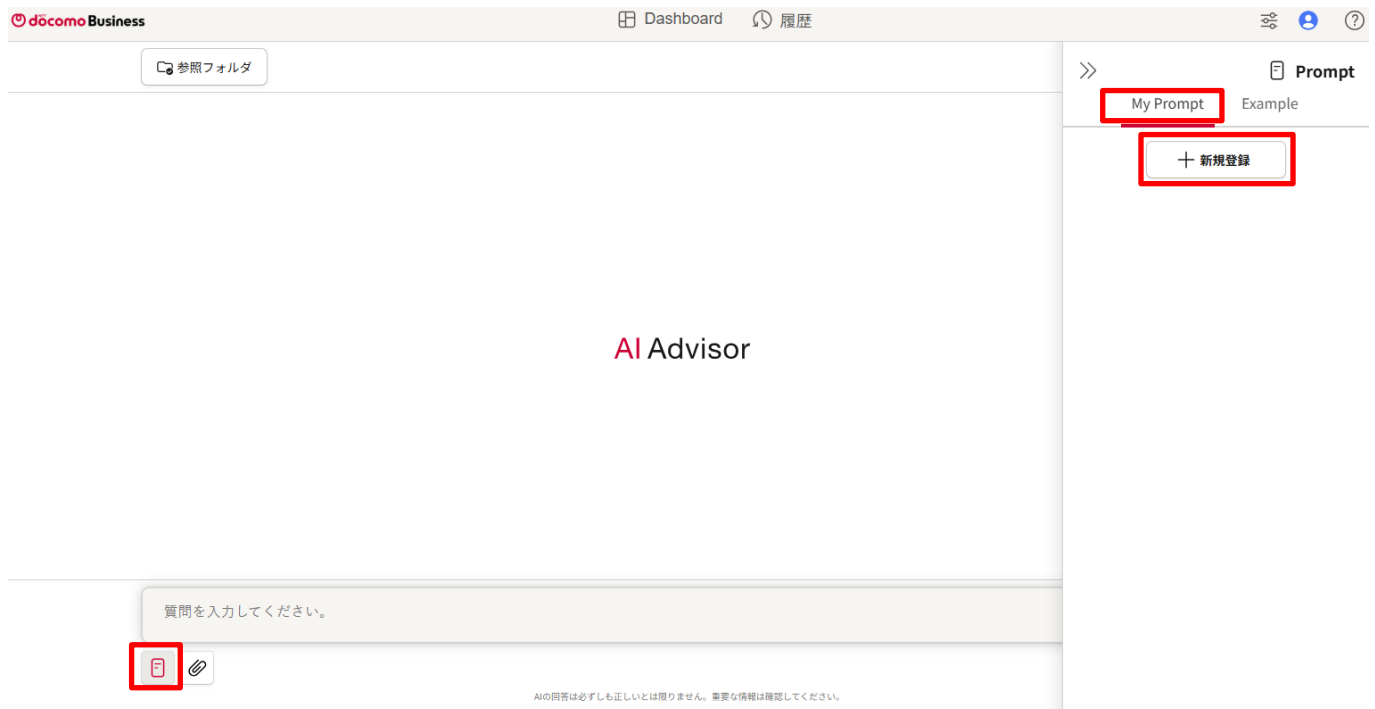
AIの回答は必ずしも正しいとは限りません。重要な情報は確認してください。

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。



My Promptの設定

名前 必須 0/20

タイトルを入力してください。

① タイトルを入力してください

説明 任意 0/200

プロンプトの説明を入力してください。

プロンプト 必須 0/2000

プロンプトの内容を入れてください。
 変数を表すには {{ }} を使ってください。
 例：{{name}} is a {{adjective}} {{noun}}

保存

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。

✕

プロンプトの適用

選択中のプロンプト

{{CVE番号}}の脆弱性について教えてください。

CVE番号 必須

CVE-2024-6387

適用

- 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。

CVE-2024-6387の脆弱性について教えてください。 |

📄 📄

▶

AIの回答は必ずしも正しいとは限りません。重要な情報は確認してください。

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。

>>

📄 Prompt

My Prompt Example

+ 新規登録

脆弱性用プロンプト ⋮

脆弱性を調べる際のプロンプト

{{CVE番号}}の脆弱性について教えてください。

🗑️ 削除

🗨️ 適用

✎ 編集

- ② ウィンドウが表示され、[削除]をクリックします。

削除しますか？

削除すると元に戻すことはできません。削除しますか？

キャンセル

削除

✕

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。



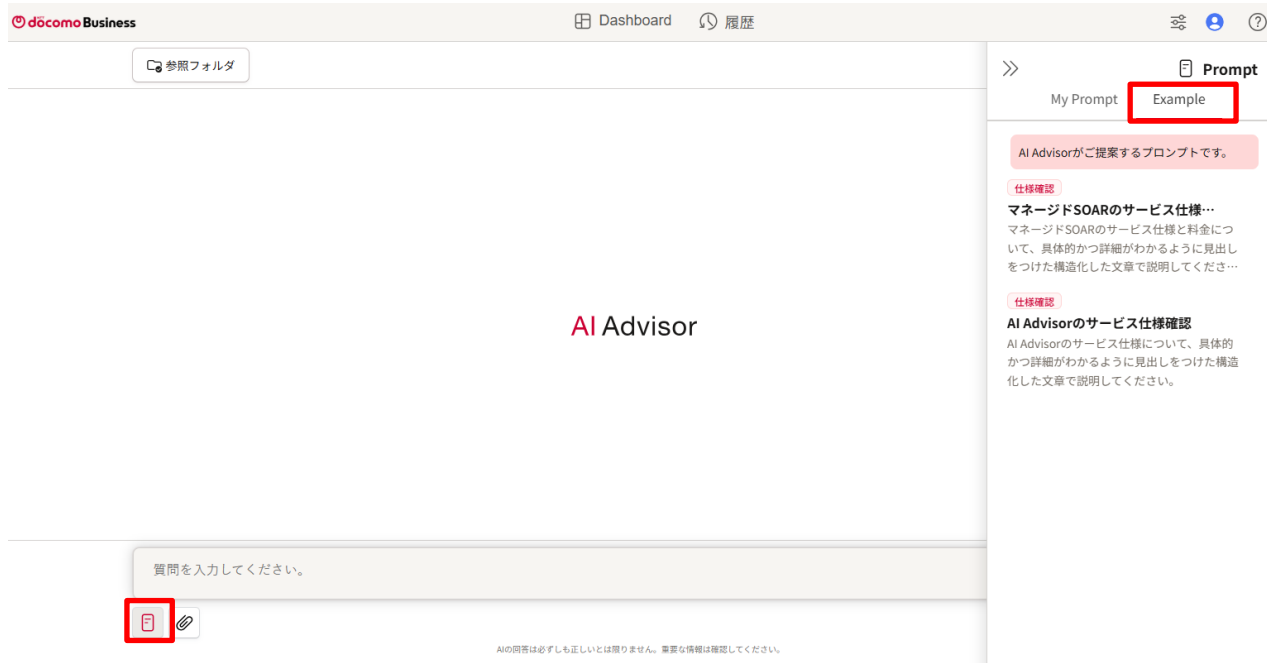
② プロンプトテンプレートを編集し、[保存]をクリックします。



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。

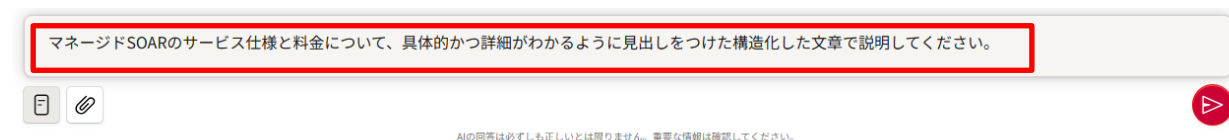


7.6. システムに登録済のプロンプトの適用

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. Sentinel 連携機能

Sentinel の API を利用し、発出されたアラートに関するエンティティ情報を確認して回答する機能を提供します。

8.1. Sentinel

① 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 : 9e8b20f8-d152-459c-995d-ca0f375082f8 について詳細を教えてください」と入力



インシデントID : 9e8b20f8-d152-459c-995d-ca0f375082f8について詳細を教えてください

AIの回答は必ずしも正しいとは限りません。重要な情報は確認してください。

② エンティティ情報に基づき、回答が出力されます。

AI インシデントID : 9e8b20f8-d152-459c-995d-ca0f375082f8 にて以下のエンティティが検出されました。

- アカウント: [REDACTED]
- IPアドレス: [REDACTED]
- DNS解決: [REDACTED]

インシデントが発生した場合は、迅速な初動対応が非常に重要です。以下の手順で対応を進めてください。

1. インシデントの確認と封じ込め:

- インシデントの内容を正確に把握し、影響範囲を特定します。
- 影響を受けているシステムやネットワークを隔離し、これ以上の被害拡大を防ぎます。
- 関連するログやデータ保全を行い、証拠を確保します。

2. 影響評価と状況共有:

- インシデントによる業務への影響度（停止、データ損失など）を評価します。
- 関係者（経営層、IT部門、法務部門など）に迅速に状況を共有します。
- 必要に応じて、顧客や取引先への情報開示の準備をします。

3. 復旧計画の策定と実行:

- 封じ込められたシステムやデータの復旧計画を策定します。
- バックアップからのリストアやシステムの再構築を行います。
- 復旧作業中は、セキュリティ対策を強化し、再発防止策を検討します。

これらのステップは、インシデント対応の初期段階で実施すべき重要な事項です。

9. 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。

9.1. ZIA

② 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

「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。

📄
📎

▶

AIの回答は必ずしも正しいとは限りません。重要な情報は確認してください。

③ 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。

📄 docomo Business
🏠 Dashboard 📜 履歴
🔍 🌐 ?

📁 参照フォルダ

+ New Chat

🔍 「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。

📌 AI 「www.ntt.com」は、URLカテゴリ「Custom-CategoryA_20230601」と「AI_Advisor_Block」に含まれています。
このURLは以下のポリシーによってブロックされています。

- Custom-CategoryA_20230601 は、URLフィルタリングルール「URL_Block_kensho-zs-05」によってブロックされる可能性があります。
- AI_Advisor_Block は、URLフィルタリングルール「AI_Advisor_Block_test」によってブロックされます。

どちらのポリシーが原因でブロックされているかは、環境設定に依存します。

あなたの次の疑問は何ですか？

URLフィルタリングルールの適用順序について教えてください。

質問を入力してください。

📄
📎

▶

AIの回答は必ずしも正しいとは限りません。重要な情報は確認してください。

10. 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

10.1. 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。



10.2. 形式調整

設定に移動し、AI Advisor の回答の形式を調節します。



10.3. 長さ調整

設定に移動し、AI Advisor の回答の長さを調節します。

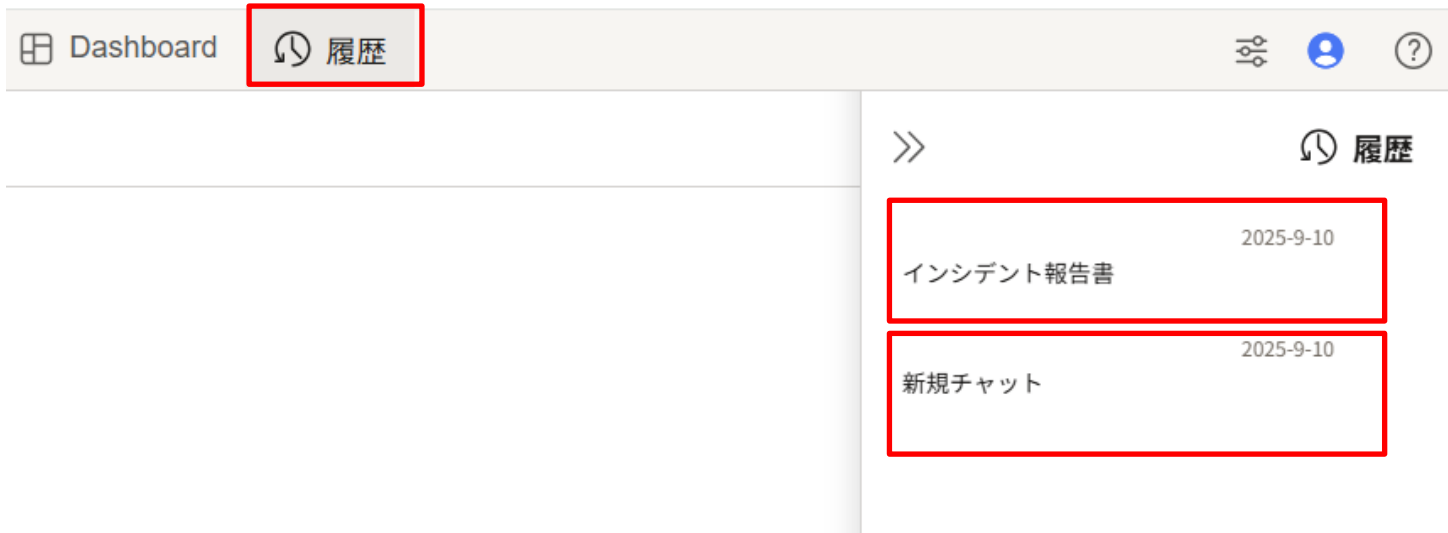


11. 履歴管理機能

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。

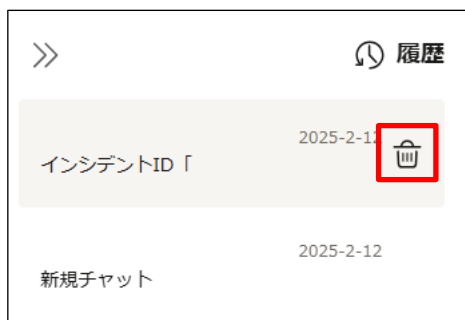
11.1. 履歴の参照

[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。



11.2. 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 ウィンドウが表示され、[削除]をクリックします。



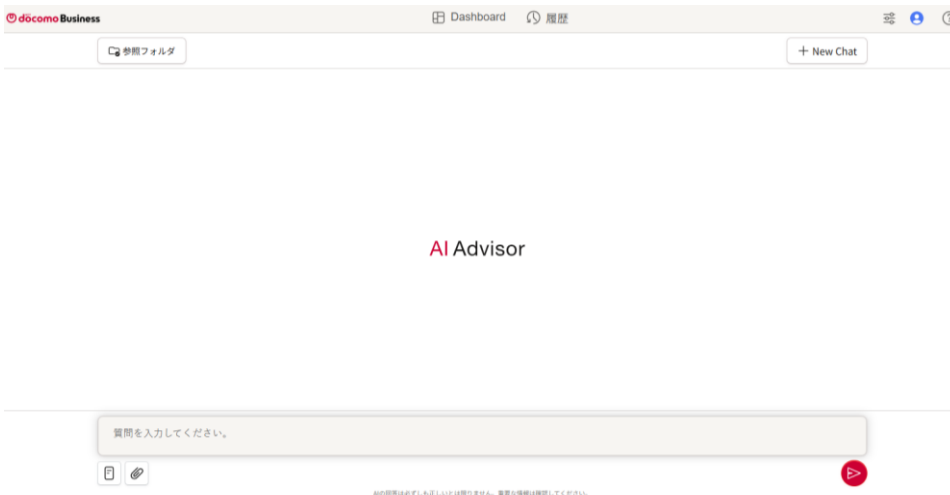
12. その他

12.1. カラーモードの変更

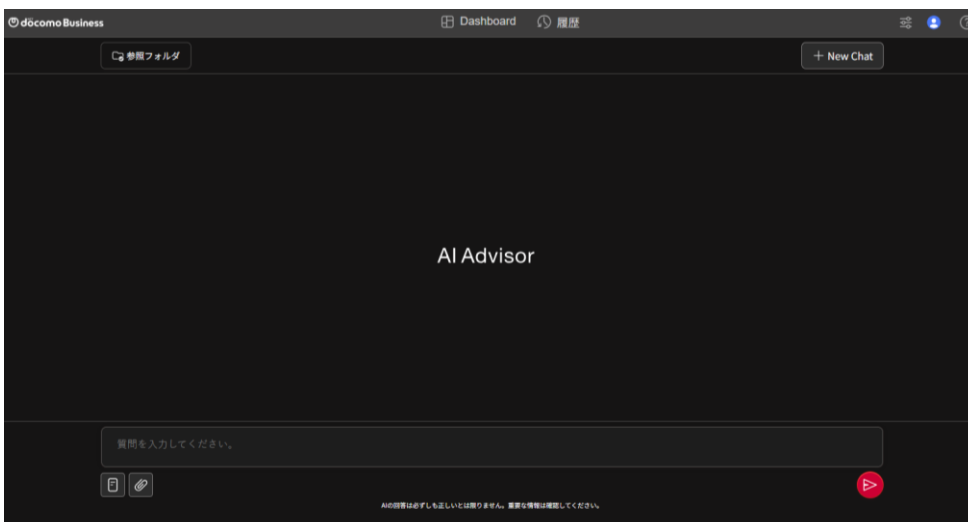
カラーモードを選択することで、AI Advisor の外観を変更します。



■ ライトモード

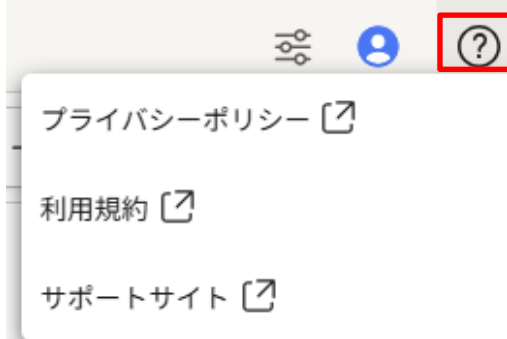


■ ダークモード



12.2. 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