

WideAngle AI Advisor ユーザーマニュアル

バージョン 2.2

2026 年 10 月 1 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

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	10
5.1. 添付ファイルの指定	10
5.2. 添付ファイルの変更	11
5.3. 添付ファイルの削除	12
6. ダッシュボード機能	13
6.1. 一覧表示	13
6.2. インシデントレポートの作成	13
6.3. 脆弱性情報の確認	15
7. プロンプトテンプレート機能	16
7.1. プロンプトテンプレートの新規登録	16
7.2. プロンプトテンプレートの適用	17
7.3. プロンプトテンプレートの削除	18
7.4. プロンプトテンプレートの編集	19
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	20
8. インシデントレポート生成機能	21
8.1. インシデントレポート生成	21
8.2. アーティファクトの参照	22
9. 脅威インテリジェンス連携機能	24
9.1. 脅威インテリジェンス連携	24
10. Zscaler (ZIA) 連携機能	25

10.1. ZIA 連携	25
11. Prisma Access 連携機能	26
11.1. Prisma Access 連携	26
12. 設定管理機能	27
12.1. トーン調整	27
12.2. 形式調整	27
12.3. 長さ調整	27
13. 履歴管理機能	28
13.1. 履歴の参照	28
13.2. 履歴の削除	28
14. その他	29
14.1. カラーモードの変更	29
14.2. サポートリンク	30
改訂履歴	31

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。

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

お客さま環境の認証基盤と 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

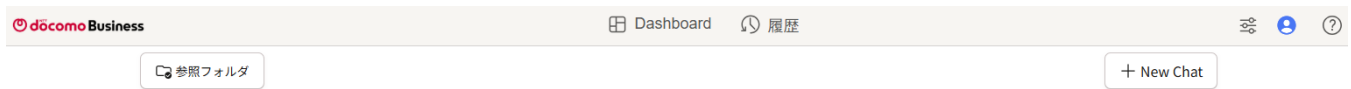
ブラウザ: Google Chrome

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 お客さま環境の認証基盤と 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

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。必要な情報は確認してください。

- ※ 認可機能により、AI Advisor にユーザー情報が登録されていない場合はアクセスできません。
アクセスできない場合は、システム管理者にご確認ください。

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

- 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






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 回答生成に必要な処理の進捗状況が表示されます。

回答を生成しています....

エージェントへ接続中：収集情報から回答を生成しています...

該当ファイルを見る

- ③ AI Advisor から、質問に対する回答が出力されます。

CVE-2024-6387の脆弱性について教えてください。

脆弱性の詳細

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悪用する可能性があります。これにより、高レベルの機密性、完全性、可用性への影響が生じる可能性があります。

影響

- 深刻度: 緊急 (CVSS:3.1スコア: 8.1)
- 攻撃経路: ネットワーク
- 攻撃の複雑さ: 高
- 必要な特権: 不要
- ユーザーとの対話: 不要
- 機密性への影響: 高
- 完全性への影響: 高
- 可用性への影響: 高

脆弱性が存在するソフトウェア

- OpenSSH サーバー (sshd)

対策

この脆弱性に対処するためには、OpenSSHを最新バージョンにアップデートし、関連するセキュリティパッチを適用することが推奨されます。最新情報については、OpenSSHの公式リリースノートやベンダーからのセキュリティアドバイザリを確認することが重要です。

この脆弱性は「CWE-362: 競合状態」として分類されています。

該当ファイルを見る

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サーバーの特定のバージョンを利用していますか？

CVE-2024-6387に関する追加情報はありますか？

OpenSSHのセキュリティパッチの適用方法について教えてください。

3.2. 追加質問の Recommend

追加質問では、直前の会話内容を踏まえた質問候補が表示され、選択して入力が可能です。

- ① AI Advisor の回答後に表示される追加質問の Recommend 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

🔍 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）におけるセキュリティの欠陥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際に発生する競合状態に起因します。

脆弱性の詳細

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悪用する可能性があります。これにより、高レベルの機密性、完全性、可用性への影響が生じる可能性があります。

影響

- 深刻度: 緊急 (CVSS:3.1スコア: 8.1)
- 攻撃経路: ネットワーク
- 攻撃の複雑さ: 高
- 必要な特権: 不要
- ユーザーとの対話: 不要
- 機密性への影響: 高
- 完全性への影響: 高
- 可用性への影響: 高

脆弱性が存在するソフトウェア

- OpenSSH サーバー (sshd)

対策

この脆弱性に対処するためには、OpenSSHを最新バージョンにアップデートし、関連するセキュリティパッチを適用することが推奨されます。最新情報については、OpenSSHの公式リリースノートやベンダーからのセキュリティアドバイザリを確認することが重要です。

この脆弱性は「CWE-362: 競合状態」として分類されています。

📄 該当ファイルを見る

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 サーバーの特定のバージョンを利用していますか？

CVE-2024-6387に関する追加情報はありますか？

OpenSSHのセキュリティパッチの適用方法について教えてください。

② AI Advisor が追加質問に対して回答します。

🔍 OpenSSHのセキュリティパッチの適用方法について教えてください。

AI OpenSSHのセキュリティパッチの適用方法は、お使いのオペレーティングシステムやOpenSSHの導入方法によって異なります。一般的な適用方法をいくつかご紹介します。

1. オペレーティングシステムのパッケージマネージャーを利用する

多くのLinuxディストリビューションでは、OpenSSHはシステムパッケージとして提供されています。この場合、システムのパッケージマネージャーを使ってアップデートすることが最も一般的で推奨される方法です。

• Debian/Ubuntu系 (APT)

```
sudo apt update
sudo apt upgrade openssh-server
```

• RHEL/CentOS/Fedora系 (YUM/DNF)

```
sudo yum update openssh-server
# または
sudo dnf update openssh-server
```

• Arch Linux (Pacman)

```
sudo pacman -Syu openssh
```

注意点:

- アップデート後、SSHサービスを再起動する必要がある場合があります。多くのパッケージマネージャーは自動的にサービスを再起動しますが、手動での再起動が必要な場合もあります。

```
sudo systemctl restart sshd
# または
sudo service ssh restart
```

- Arch Linuxの場合、CVE-2024-6387の脆弱性に関するニュースで、sshdサービスの再起動が必要であることが案内されています。

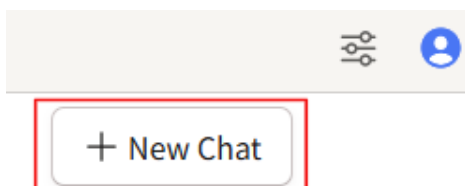
2. ソースコードからコンパイルして導入している場合

OpenSSHをソースコードから手動でコンパイルして導入している場合は、最新のソースコードをダウンロードし、再コンパイルおよび再インストールを行う必要があります。

1. 最新のOpenSSHソースコードをダウンロード: OpenSSHの公式サイトから最新バージョンをダウンロードします。

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

フォルダにマニュアルや FAQ などのファイルを事前に設定しておくことで、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

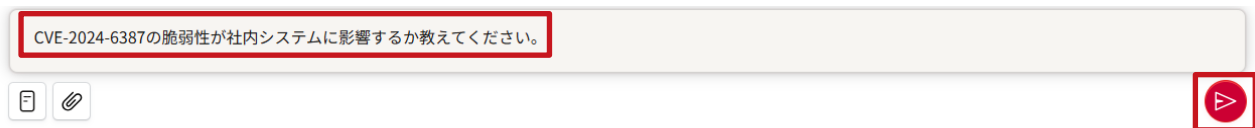
[参照フォルダ]をクリックし、参照する RAG のフォルダをクリックし、[閉じる]をクリックします。



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]をクリックすることで、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。

A 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。

• [\[Redacted URL\]](#)

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 [へ](#)

★ 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

質問入力時にローカルファイルを選択し、中身を参照・考慮しつつ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

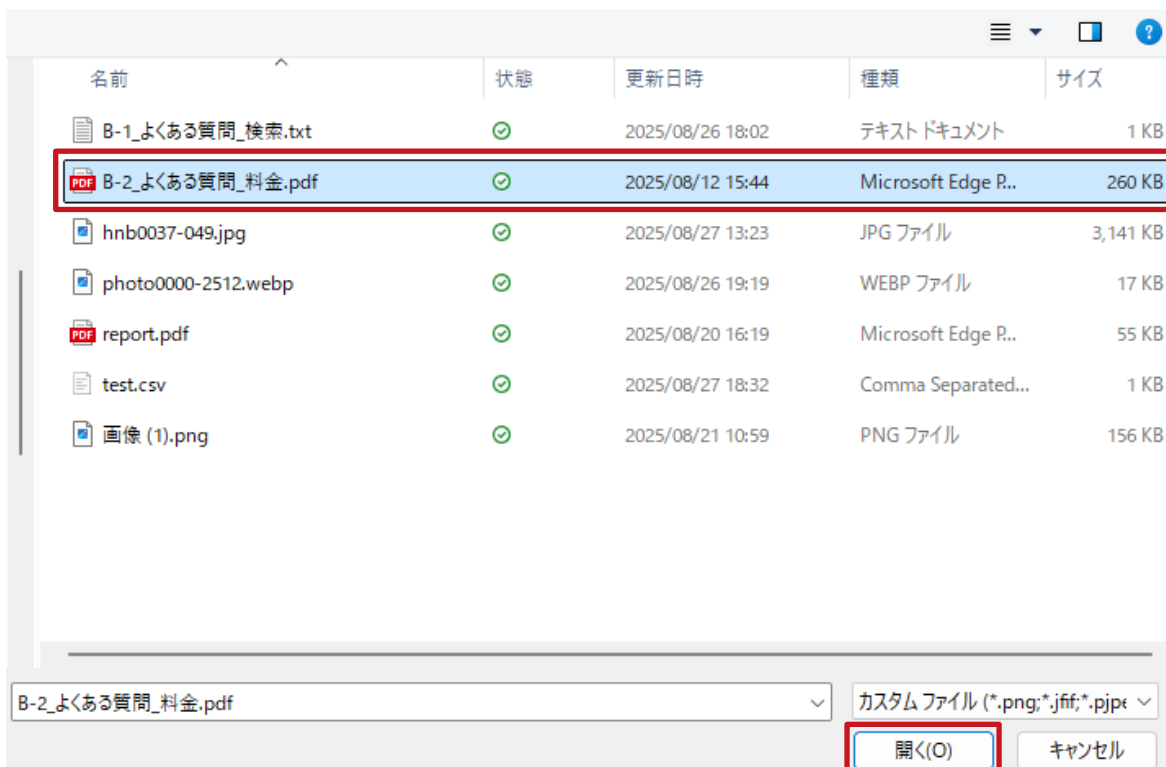
※文字コードについては、UTF-8 をサポートしています。

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。

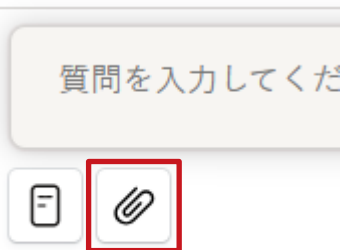


- ④ 添付ファイルに基づき回答が出力されます。



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。

質問を入力してください。

 B-1_よくある質問_検索.txt




AIの回答は必ずしも正しいとは限りません。必要な情報は確認してください。

5.3. 添付ファイルの削除

① 添付ファイルのxをクリックします。

質問を入力してください。

 B-1_よくある質問_検索.tx




AIの回答は必ずしも正しいとは限りません。必要な情報は確認してください。

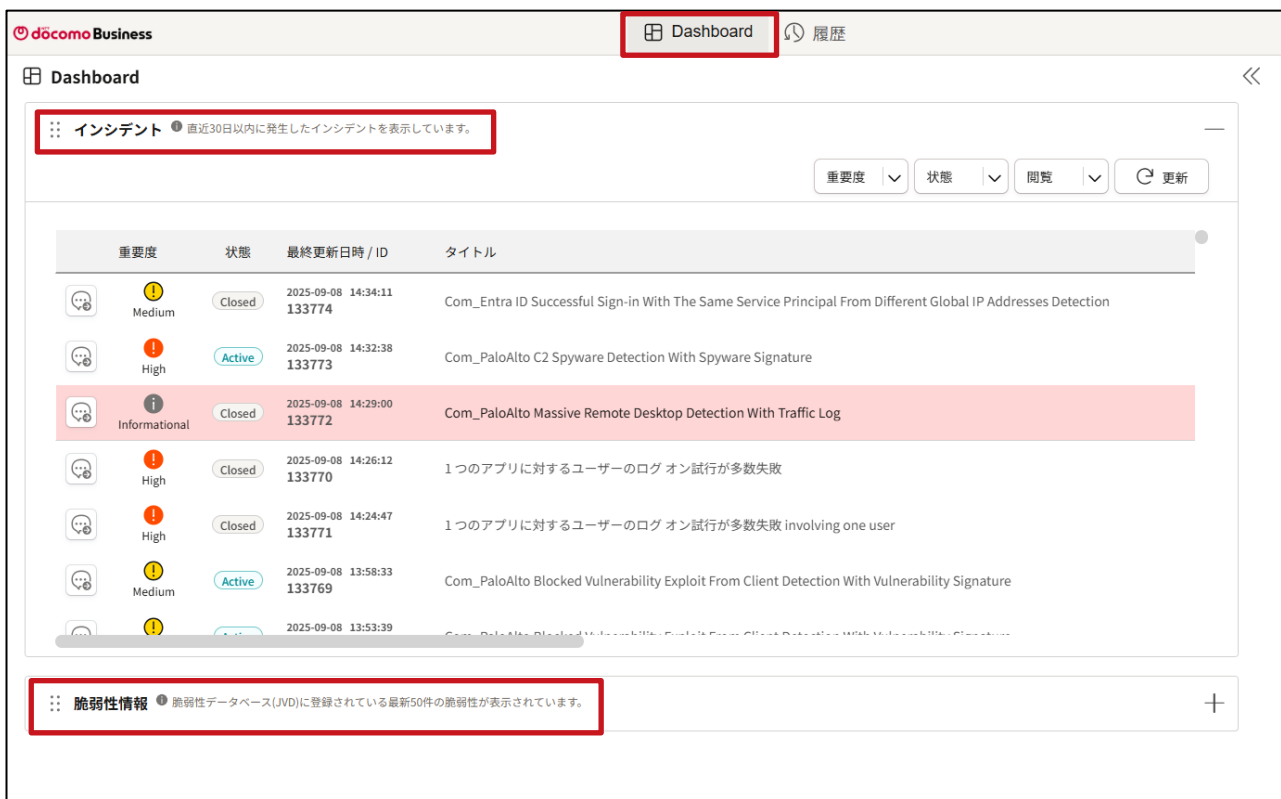
6. ダッシュボード機能

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's a navigation bar with "Dashboard" and "履歴" (History). Below this, the "Dashboard" section is active, displaying two main panels: "インシデント" (Incidents) and "脆弱性情報" (Vulnerability Information). The "インシデント" panel includes a filter for "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 features a table with columns for "重要度" (Severity), "状態" (Status), "最終更新日時 / ID" (Last Updated Time / ID), and "タイトル" (Title). The table lists several incidents, including "Com_Entra ID Successful Sign-in With The Same Service Principal From Different Global IP Addresses Detection", "Com_PaloAlto C2 Spyware Detection With Spyware Signature", and "Com_PaloAlto Massive Remote Desktop Detection With Traffic Log". The "脆弱性情報" panel shows a link to "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。" (Latest 50 vulnerabilities registered in the Vulnerability Database (JVD) are displayed).

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

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 ▼ 更新

すべて High Medium Low Informational

すべて New Active Closed

すべて 既読 未読

[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。



重要度 ▼ 状態 ▼ 閲覧 ▼ 更新

すべて High Medium Low Informational

すべて New Active Closed

すべて 既読 未読

[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。



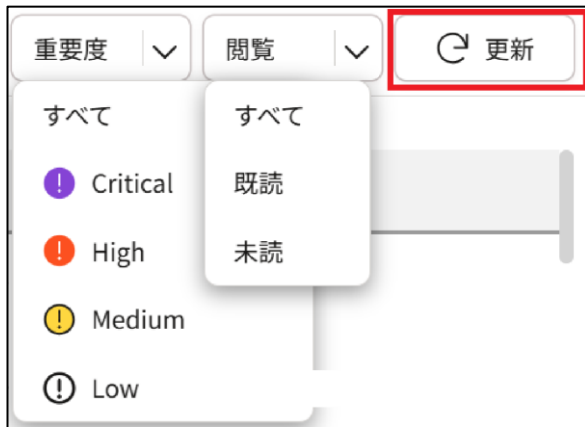
重要度	状態	最終更新日時 / ID	タイトル	
	レポート作成	New	2026-03-22 20:18:47 376	'Wacatac' detected on one endpoint

インシデントID: 313c1ad5-c57d-450d-b80b-9c4b042aa81d
 タイトル: 'Wacatac' detected on one endpoint
 説明文:
 重要度: Medium
 状態: New
 アラート製品名: Microsoft Defender Advanced Threat Protection

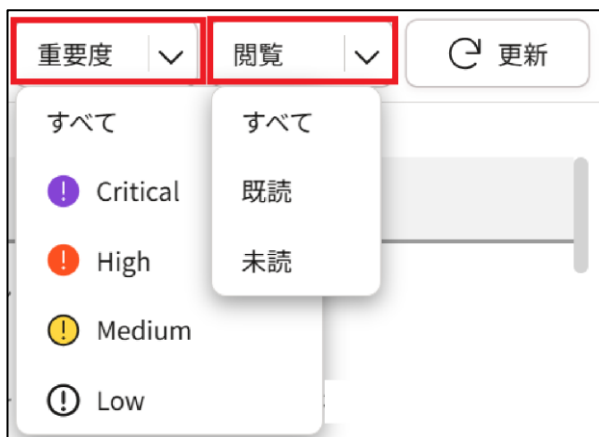
14

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。

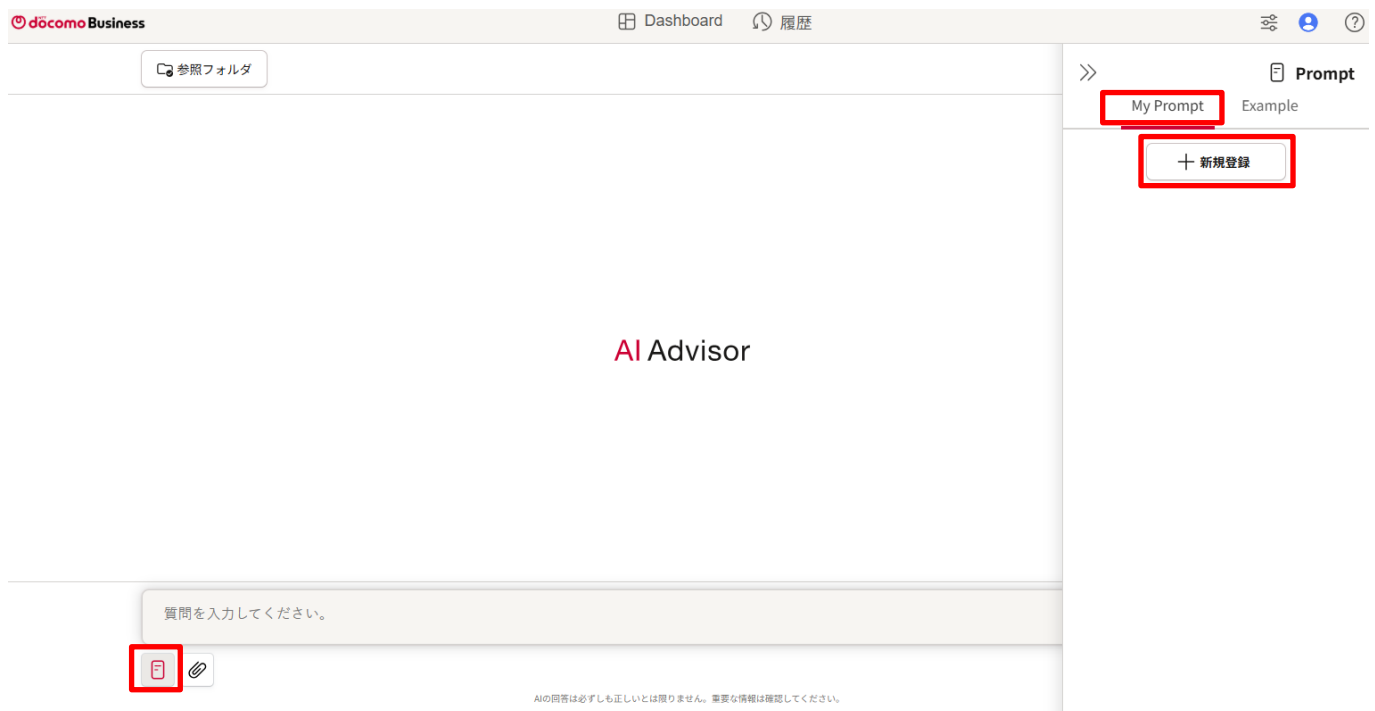
7. プロンプトテンプレート機能

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

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 **必須** 0/2000

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。

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。



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
 い。

適用
 削除
 編集

- ② ウィンドウが表示され、[削除]をクリックします。

A screenshot of a confirmation dialog box. At the top right is a close button (X). The title is '削除しますか？' (Do you want to delete?). The main text is '削除すると元に戻すことはできません。削除しますか？' (You cannot return to the original state after deletion. Do you want to delete?). There are two buttons at the bottom: 'キャンセル' (Cancel) on the left and '削除' (Delete) on the right. The '削除' button is highlighted with a red border.

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。



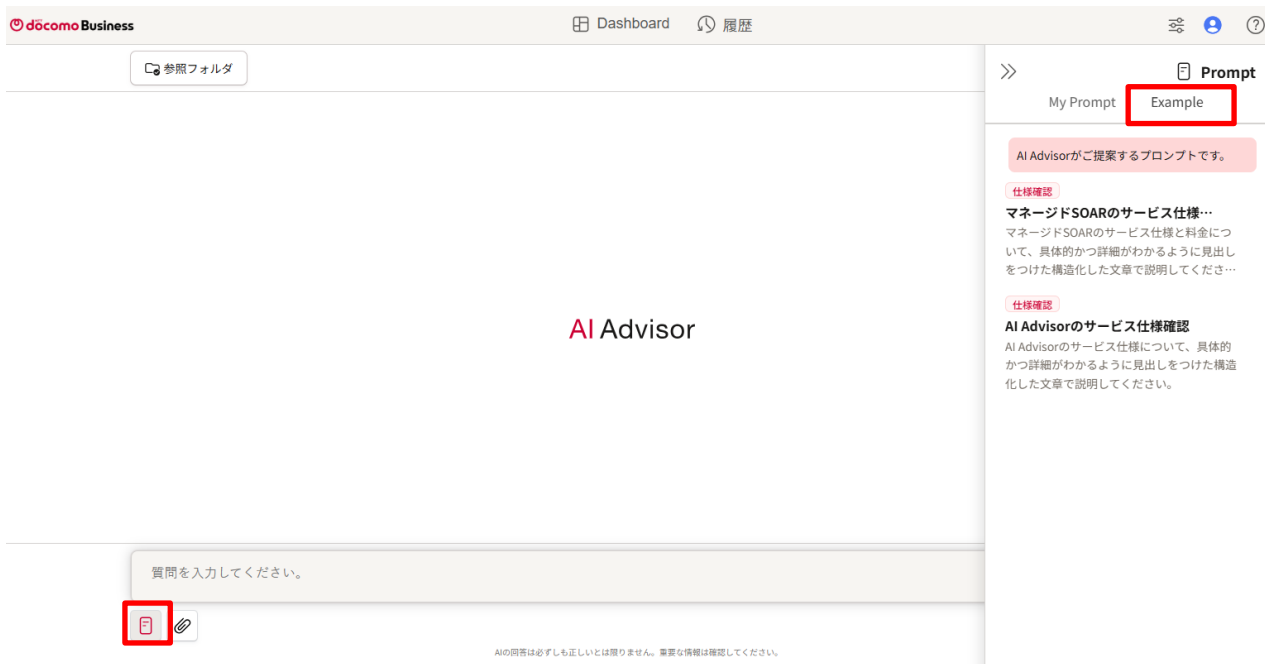
② プロンプトテンプレートを編集し、[保存]をクリックします。



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。

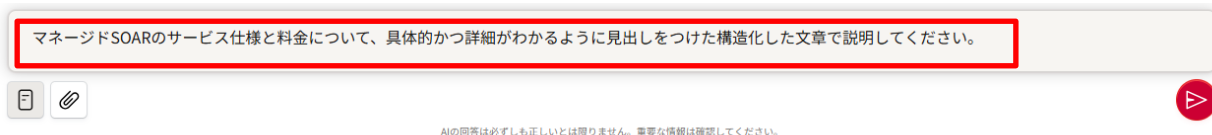


7.6. システムに登録済のプロンプトの適用

- 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。



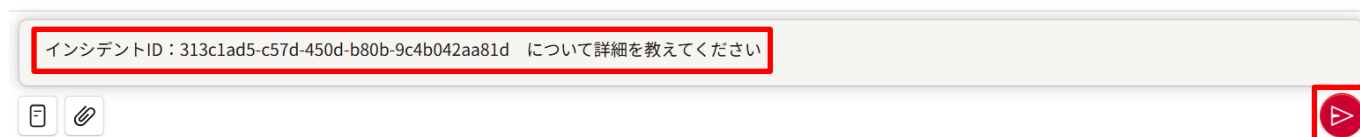
8. インシデントレポート生成機能

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

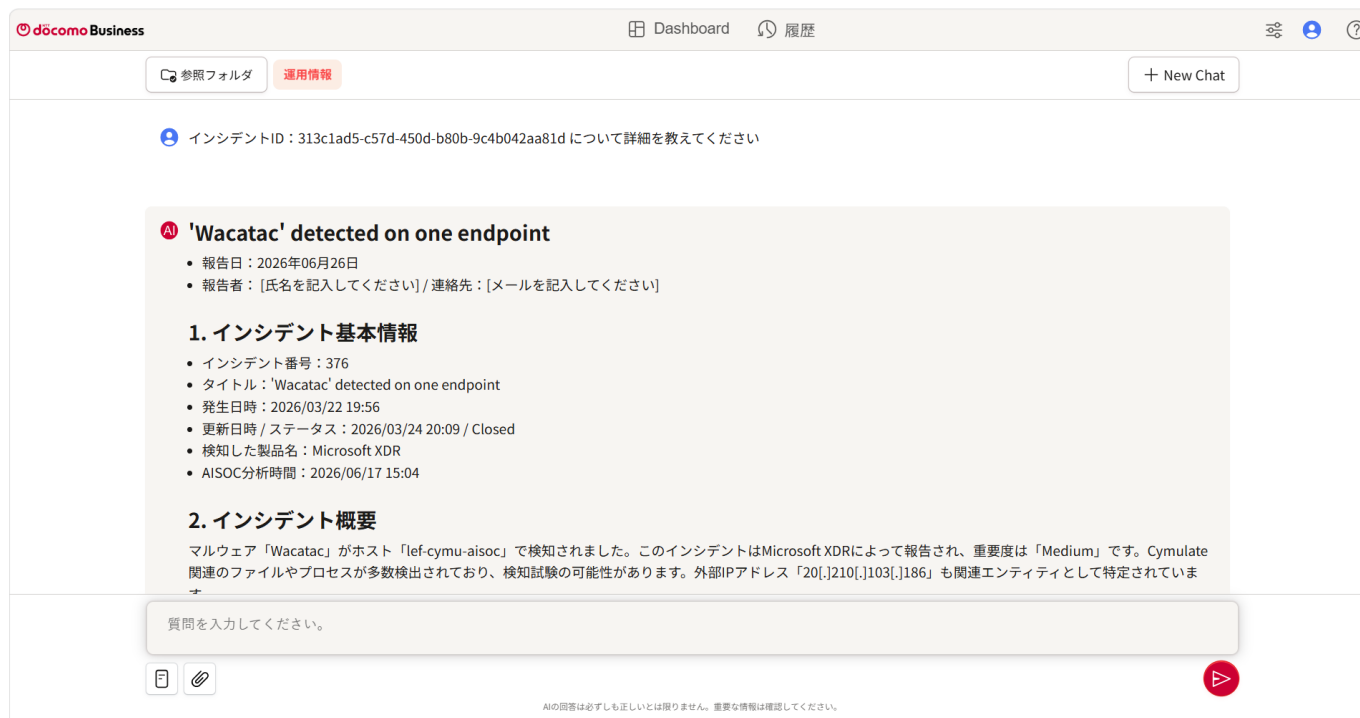
① レポート生成したいインシデント ID を含む形で質問を入力し、実行ボタンをクリックします。

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



② 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。

WideAngle マネージド SOAR をご契約の場合、対象のインシデント ID に紐づく AI SOC の分析結果が存在する場合はその結果をレポート形式で出力します。



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

AI 'Wacatac' detected on one endpoint

- 報告日：2026年06月26日
- 報告者：[氏名を記入してください] / 連絡先：[メールを記入してください]

1. インシデント基本情報

- インシデント番号：376
- タイトル：'Wacatac' detected on one endpoint
- 発生日時：2026/03/22 19:56
- 更新日時 / ステータス：2026/03/24 20:09 / Closed
- 検知した製品名：Microsoft XDR
- AISOC分析時間：2026/06/17 15:04

2. インシデント概要

マルウェア「Wacatac」がホスト「lef-cymu-aisoc」で検知されました。このインシデントはMicrosoft XDRによって報告され、重要度は「Medium」です。Cymulate 関連のファイルやプロセスが多数検出されており、検知試験の可能性あります。外部IPアドレス「20[.]210[.]103[.]186」も関連エンティティとして特定されています。

質問を入力してください。

③ 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」をクリックしてください。



Dashboard 履歴





参照フォルダ

New Chat

 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

AI 'Wacatac' detected on one endpoint

- 報告日: 2026年03月23日
- 報告者: [氏名を記入してください] / 連絡先: [メールを記入してください]

1. インシデント基本情報

- インシデント番号: 376
- タイトル: 'Wacatac' detected on one endpoint
- 発生日時: 2026/03/22 19:56
- 更新日時 / ステータス: 2026/03/23 10:45 / New
- 検知した製品名: Microsoft XDR

2. インシデント概要

2026年3月22日に、エンドポイント 'lef-cymu-aisoc' でWacatacマルウェアが検出されました。このマルウェアはWindowsコマンドシェルを介して実行され、Cymulate関連の複数の実行可能ファイルが関与しています。特に 'Cymulate[.]Agent[.]Service[.]exe' という名前のサービス実行ファイルが検出されており、これは持続性や特権昇格の試みを示唆しています。関係するIPアドレスは全てプライベートアドレスであり、外部への通信は確認されていません。ファイルハッシュ情報も複数確認されています。

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。

8.2. アーティファクトの参照

アーティファクトでは、AI SOC がどのような情報をもとに分析したかを確認できます。

分析時に参照したデータや、ログの検索・分析に使用した KQL クエリ※¹を確認することで、分析結果の根拠や分析の過程の把握が可能です。

- ④ 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。
 - 「収集データを見る（分類：KQL）」：AI SOC の分析に用いた KQL クエリを参照可能です。※²

※¹ ※² KQL クエリ（Kusto Query Language）とは、ログデータを検索・集計・分析するための処理内容を記述したものです。WideAngle マネージド SOAR をご契約で、対象のインシデント ID に紐づく AI SOC の分析結果が存在する場合のみ参照可能となります。

- 『Cymulate[.]Agent[.]Service[.]exe』に関連するWindowsサービスの起動設定と実行権限を確認し、不審な設定があれば無効化または削除する。
- エンドポイント 'lef-cymu-aisoc' 上のイベントログを詳細に分析し、マルウェアの初期侵入経路、横展開の試み、データ窃取の有無などを特定する。
- 使用された可能性のあるMITRE ATT&CKテクニック (T1059.003, T1543.003) に基づいて、他のエンドポイントにおける同様の活動をプロアクティブに検索する（ハンティング）。

8. 備考

- Cymulate関連ファイルが多数検出されており、これは正規のセキュリティテストツールであるCymulateが悪用された可能性、またはマルウェアがCymulateを装っている可能性を示唆しているため、その関連性を詳細に調査する必要があります。
- 検出されたマルウェアWacatacはトロイの木馬型であり、外部通信が確認されていない現状でも、内部でのデータ窃取や追加マルウェアの展開、コマンド&コントロール（C2）サーバーへの接続準備などの活動を進めている可能性を考慮し、システム内部での挙動を深く分析する必要があります。
- 『lefadmin』という管理者権限を持つ可能性のあるユーザーがログインしていた形跡があり、このアカウントの侵害があった場合、システムへの影響がさらに拡大する危険性があるため、アカウントの活動ログや他の管理対象システムでの活動を確認し、侵害範囲を特定することが重要です。

Generated by AI Advisor

- 🔍 収集データを見る（分類：Sentinel） ▼
- 🔍 収集データを見る（分類：IP） ▼



別インシデント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。

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。



⑤ 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。

ール（C2）サーバーへの接続準備などの活動を進めている可能性を考慮し、システム内部での挙動を深く分析する必要があります。

- 『lefadmin』という管理者権限を持つ可能性のあるユーザーがログインしていた形跡があり、このアカウントの侵害があった場合、システムへの影響がさらに拡大する危険性があるため、アカウントの活動ログや他の管理対象システムでの活動を確認し、侵害範囲を特定することが重要です。

Generated by AI Advisor

🔍 収集データを見る（分類：Sentinel） へ

1 2

```
"summary_description": null,
"alertsCount": 4,
"incident_number": 376,
"incident_id": "313c1ad5-c57d-450d-b80b-9c4b042aa81d",
"detection_datetime": "2026-03-22T10:56:52.5752845Z",
"created_datetime": "2026-03-22T10:57:34.2533333Z",
"last_modified_datetime": "2026-03-23T01:45:58.2493748Z",
"last_activity_datetime": "2026-03-22T10:58:27.6096085Z",
"tactics": [
  "Execution"
]
```

🔍 収集データを見る（分類：IP） ▼



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

⑥ 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





⑦ 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。

 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

-  8.8.8.8のIPアドレスについて調べましたところ、現在のところ脅威は検出されていません。
- 詳細な分析結果は以下の通りです。
- **匿名性:** ホスティング、プロキシ、リレー、レジデンシャルプロキシ、Tor、VPN、Webプロキシのいずれの機能も検出されませんでした。
 - **検出数:** 79のエンジンでスキャンした結果、脅威の検出はありませんでした。
 - **IPアドレス:** 8.8.8.8
 - **ISP (インターネットサービスプロバイダ):** Google LLC
 - **地理情報:** 緯度 37.38605, 経度 -122.08385
 - **逆引きDNS:** dns.google
 - **リスクスコア:** 0 (脅威なし)
 - **情報源:** ThreatIntelligence
- このIPアドレスはGoogle Public DNSのサーバーであり、通常、安全にご利用いただけます。



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






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 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。



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。

 「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。






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。

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

⑧ 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

📄 🔗

▶

⑨ 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。

📁 参照フォルダ

+ New Chat

🔗 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

AI

「www.ntt.com」は、Prisma Access の「Mobile Users」フォルダにあるカスタム URL カテゴリ「AIAdvisor-test」に登録されています。このカテゴリには、「www.ntt.com」と「example.com」の2つのURLがリストされています。

📄

あなたの次の疑問は何ですか？

📄 🔗 ▶

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。

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。



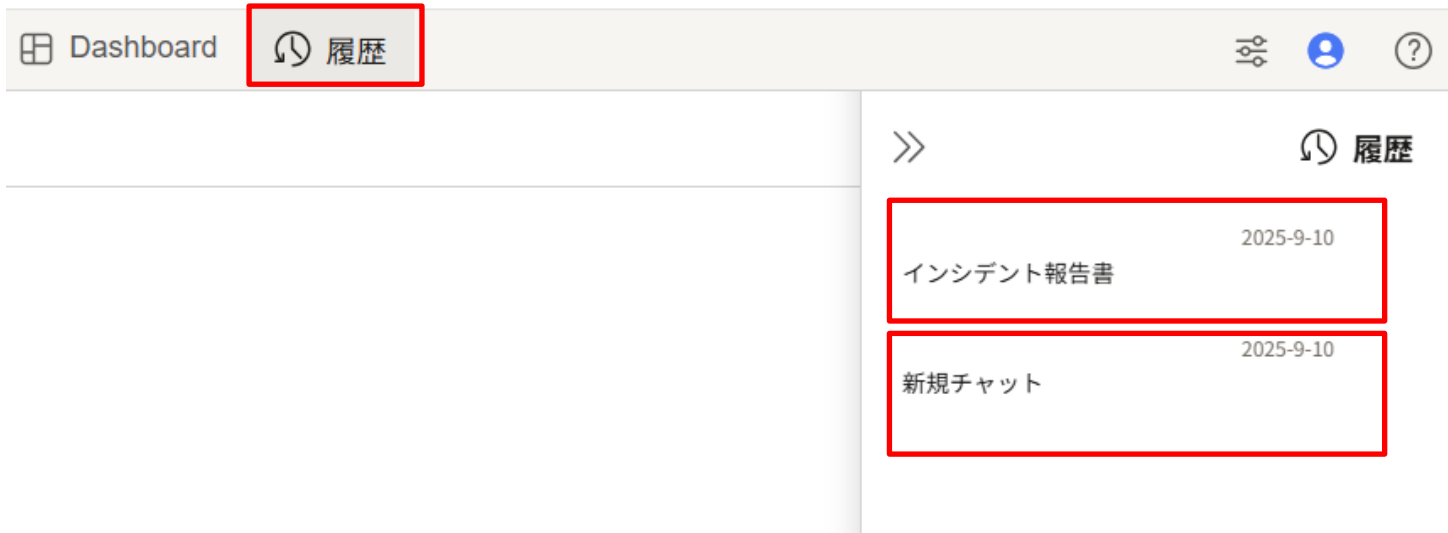
13. 履歴管理機能

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 時間経過によりセッションが自動的に切り替わることでリセットされます。

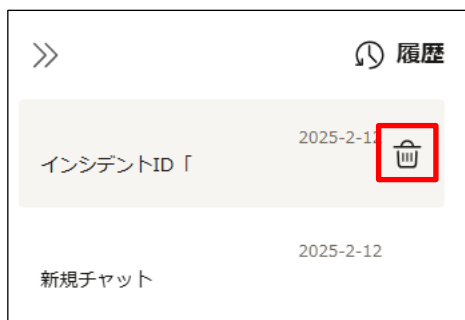
13.1. 履歴の参照

[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 ウィンドウが表示され、[削除]をクリックします。



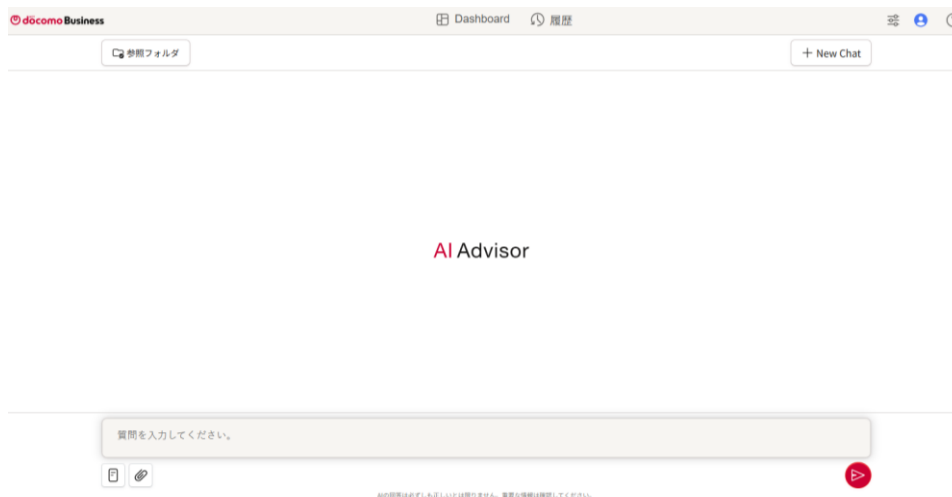
14. その他

14.1. カラーモードの変更

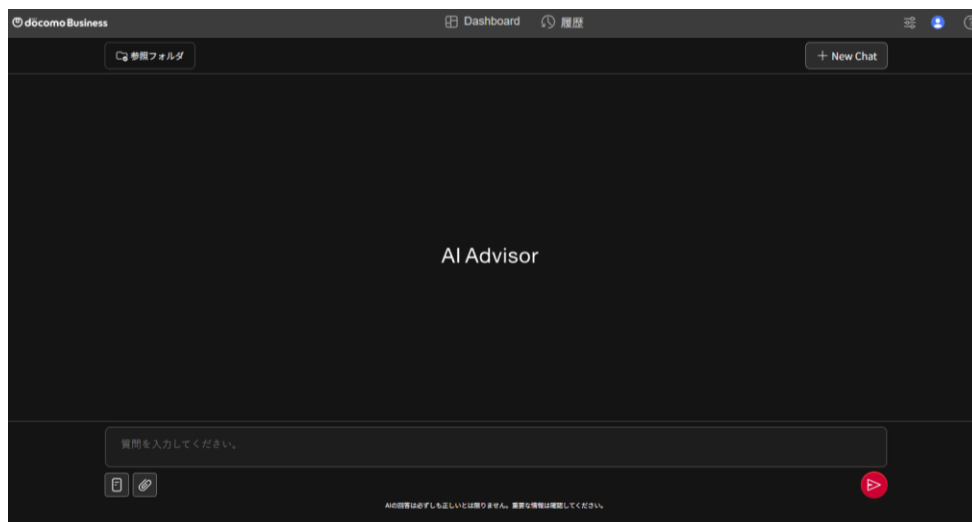
カラーモードを選択することで、AI Advisor の外観を変更します。



① ライトモード

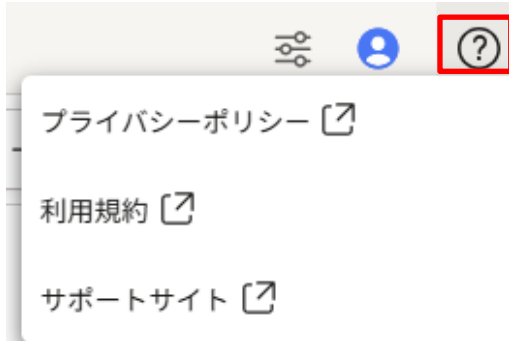


② ダークモード



14.2. サポートリンク

「？」をクリックすることで、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
2.1 版	2.3.認可機能に伴う注釈の追加 8.1.AI SOC 機能をご契約の場合のインシデントレポート生成に関する注釈の追加 その他軽微な文言等の修正・更新	2026 年 7 月 1 日
2.2 版	8.2.KQL が表示される旨の追加	2026 年 10 月 1 日