

Darktrace 社製品テクニカルサポート仕様

本仕様に、図研ネットウエイブが提供する Darktrace 社製品の技術支援サービスの内容を定めております。
尚、本仕様は予告なく変更されることがあります。

1. 受付および対応時間

平日（弊社営業日）9時～17時00分

2. サービスの内容

本サービスは、弊社より販売した Darktrace 社製品に限り下記内容を提供します。

- 2.1. 製品に機能不全が疑われる場合の障害対応
- 2.2. 障害についての回避策、ワークアラウンドの助言
- 2.3. メーカーが公開する情報の提供
- 2.4. メーカーサポート終了後の弊社ナレッジによる助言
- 2.5. 製品の操作に関する助言
※サポートされた OS、ブラウザによる操作が対象です。
※全般的なコンフィグレーションファイルの作成支援、精査を行うものではありません。
※助言を基に設定する際は、利用環境に応じて適切な値を設定してください。
- 2.6. リモート接続による確認
※リモート接続によるハードウェア診断がある場合となります。
※ハードウェア障害の確認のみ実施します。

3. サービスの運用

- 3.1. お問い合わせ言語
日本語のみ。
- 3.2. お問い合わせ対象地域
日本国内のみ。
- 3.3. お問い合わせ時の必要情報
保守サポート ID、モデル、シリアルナンバー、ご使用中のファームウェアバージョン、事象内容、発生状況。
- 3.4. お問い合わせ方法
E-Mail、電話及び弊社が指定のシステム経由で1インシデント1件としてお問い合わせください。インシデント内容と異なるお問い合わせをする場合は、新たにお問い合わせください。
- 3.5. お問い合わせご担当者
Darktrace 製品のシステム管理者又はこれに準ずる方。
- 3.6. 情報
調査を目的として入手した情報は、メーカーに提示・提出します。
- 3.7. サポートのクローズ
サポート要員からの回答後、1週間経過してもお問い合わせ担当者からの連絡がない場合。
- 3.8. 対応時間
対応受付時間内に受け付けても、当日の回答をお約束するものではありません。また、お客様からの回答時

間の指定についてご要望は承りますが、時間内の回答をお約束するものではありません。

4. サービスの責任

- 4.1. 「2.サービスの内容」での回答、「3.8.対応時間」の如何に問わず、間接的障害、付随的損害、結果的損害、データの損失等に関し、それらの可能性を知っていたか否かにかかわらず、一切の責任を負わないものとします。
- 4.2. 天災、火災、その他の不可抗力によりサポートを提供できない場合があります。

5. サービス範囲外

下記の技術支援を希望される場合は、別途有償対応となる場合がございます。別途営業までご相談下さい。

- 5.1. リアルタイム、至急、回答時間を指定されたお問い合わせへの対応
- 5.2. 運用開始前・構築中の技術支援（テスト、運用試験中等含む）
※弊社で作業を請け負った場合は担当者にお問い合わせください。
- 5.3. 弊社が定めていない操作方法
- 5.4. メーカーサポートが終了したバージョン
- 5.5. 弊社が定めていない他社製品、サービスとの連携
メーカーが公開している情報がある場合は、その情報をもって回答とします。
- 5.6. 他社製品に関する操作、設定、助言
- 5.7. 動作に関するお問い合わせ
動作に関する内容は、メーカーが公開している情報をもって回答とします。
- 5.8. ご契約のメーカーサポートサービス範囲外のお問い合わせへの対応
- 5.9. メーカー有償サービスの対応
メーカー有償サービスをご契約の場合は、メーカーに直接お問い合わせください。
- 5.10. ハードウェア不良による交換の判断
ハードウェア交換の必要の有無はメーカーが判断します。
- 5.11. 設定の確認、比較（バージョンアップ時含む）
- 5.12. 運用およびコンサルティング
・動作の方針、要望を伺って実施する調査、設定内容の作成、作成支援、変更作業
・設定のチューニングに関する作業、作業支援
・設定の正当性確認、比較、支援（アップグレード時含む）
・アップグレード作業

- ・システム設計、ネットワーク設計に関するお問い合わせ
 - ・テスト方法の検討、テストの作成方法、テストの実施及び支援
 - ・マルウェア、脆弱性、アプリケーション情報の提供
 - ・インシデントの説明及びログの解析、パケット解析
 - ・アラートの解説、解析
 - ・無効化、対策、調査、回復、ロールバック等のインシデント対応の支援、作業
 - ・攻撃手法の説明
検知テスト手法、各種攻撃に関する説明。
 - ・検体の調査、検証
 - ・検知された内容に関する正常性の判断
 - ・ログ内容からの判断
ログの内容から攻撃、誤検知を判断する作業。
 - ・検知した内容に関する正常性の判断
 - ・セキュリティインシデントの説明及びセキュリティログの解析、それらのパケット解析
 - ・機能において作成されたレポートの内容説明
 - ・インシデント、脆弱性等の対応、運用に関する打ち合わせへの出席
 - ・レポート作成
- 5.13. 動作・設定検証（障害時の状況再現を目的とした検証を除く）
- 5.14. 障害時以外での公開されていない情報に関するお問い合わせ
- 5.15. 脆弱性の説明、対策、検知確認
メーカーが公開している情報をもって回答とします。
- 5.16. プログラミング、正規表現の記述方法に関する説明
- 5.17. オンサイト及びオンラインでの技術支援（情報採取、設定変更作業、立ち会いなど）
- 5.18. リモート作業
機器へログインし、設定の確認、設定変更、ログの確認、ログの取得作業、コンフィグのバックアップおよびリストア作業。
- 5.19. 他ベンダー製品を含むシステムの障害切り分け支援
一例として以下に記載します。
- ・端末
 - ・ネットワーク機器
 - ・Firewall 製品およびUTM 製品 など
- 上記の切り分けを実施いただいた上でお問い合わせください。
- 5.20. 稼働環境に関する対応
一例として以下に記載します。
- ・パブリッククラウド、仮想基盤の設定、操作方法
 - ・パブリッククラウド、仮想基盤の設計
 - ・パブリッククラウド、仮想基盤上の機能の設定、操作方法
 - ・オペレーティングシステムの操作、設定方法
 - ・デプロイやインストール時に発生したパブリッククラウド、仮想基盤上のログの解析
 - ・デプロイに利用するサードパーティツールの操作、

設定方法

カスタマーポータル内に掲載されている情報がある場合は、その情報をもって回答とします。

- 5.21. パフォーマンス不足によって発生した事象が認められる場合の対応
- 5.22. 仕様一覧表等、多数情報の表内への記載
- 5.23. 仕様に関するお問い合わせ
仕様に関する内容は、メーカーが公開している情報をもって回答とします。
- 5.24. 運用説明、技術仕様書、マニュアル作成、報告書等の資料作成