Sophos Taegis™ MDR - 日本

本サービス仕様書は、Sophos Taegis MDR（以下、「**本サービス**」）について説明するものです。本サービス仕様書に含まれる大文字表記の用語は、下記で定義される契約書、または後述の用語集セクションで定義される意味を有します。
本サービス仕様書は、以下のいずれかに組み込まれるものとします。(i) 本サービスのサブスクリプション購入を対象とする、お客様と ソフォスとの間で署名または署名により締結された契約書、(ii) 係る署名済み契約が存在しない場合、本サービス仕様書は https://www.sophos.com/legal に掲載されている Sophos End User Terms of Use（利用規約）（総称して「契約書」）。なお、契約書の条項と本サービス仕様書の条項の間に矛盾がある場合には、本サービス仕様書の条項が優先されます。

契約書に異なるの定めがある場合であっても、お客様は以下について認識し、同意します。(i) ソフォスは、本サービスの全体的な機能性を実質的に低下または劣化させることなく、本サービスを随時変更または更新する場合があります。(ii) ソフォスは、本サービス仕様書が提供されるサービスの内容を正確に反映するために、本サービス仕様書をいつでも変更または更新する場合があり、更新されたサービス仕様書は https://www.sophos.com/legal に掲載された時点で効力を生じます。

概要

本サービスは、Sophos Taegis™ XDR（以下、「**XDR**」）内で、24 時間 365 日（以下、「**24x7**」）のセキュリティ監視と調査をお客様に提供します。本サービスには、脅威の検出と調査、脅威とプロアクティブな対応アクション、XDR 内からのソフォスセキュリティアナリストへの 24x7 アクセス、脅威ハンティング、および以下で説明する追加のサポートと機能が含まれます。

備考:

- サービスおよび関連するサポートは、特に明記されていない限り、英語で提供されるものとします。
- このサービスディスクリプションでは、「エンドポイント」は「資産」と同義で使用します。
- **複数の XDR テナント（つまり、追加のマネージド テナント）を持つお客様の場合**、以下に別段の定めがない限り、**サービスコンポーネントとサービス レベル アグリーメント**（SLA）は、お客様のすべてのテナントに適用されます。

サービスコンポーネント

セキュリティアナリストへの 24x7 アクセス

英語を話すセキュリティアナリストと日本語を話すセキュリティアナリストは、XDR のアプリケーション内チャットまたはチケットシステム、または電話を通じて 24 時間 365 日で対応できます。

注: 日本の標準勤務時間（月曜日から金曜日の 9:00 から 17:00（UTC+9）と定義）の間、日本語を話す製品サポートチームのメンバーが日本語でお客様をサポートします。

Sophos Taegis™ MDR 向け追加サービス

Taegis™ MDR のお客様は、Taegis™ MDR サブスクリプションの初回注文時またはサービス期間中いつでも、追加料金でサービスユニットを購入することができます。サービスユニットは、プロアクティブサービスまたは緊急インシデント対応(「EIR」)に使用できます。詳細については、Addendum – Secureworks Services for Taegis™ MDR、Secureworks Services for Taegis MDR Catalog Overview、および IMR and MDR Catalog in Japan をご覧ください。

脅威の検出と調査

ソフォスは、XDR 内で検出された脅威をレビューし、調査します。ソフォスがさらなる分析を必要とすると判断した脅威は、XDR 内で調査が作成されます。ソフォスは、十分な証拠が収集され、脅威に悪意があると判断された場合、またはソフォスが調査を進めるためにお客様からのさらなる情報を必要とする場合、XDR、電子メール、またはサポートされているインテグレーションを通じてお客様に通知します。

ソフォスは、すべてのお客様のサービスと Taegis エクスペリエンスを積極的に改善するために、Taegis の定期的なアップデートと変更を行っています。そのため、XDR 内では、価値の低いアラートを最小限に抑え、価値の高いアラートに時間を集中させるように設計された、カスタマイズされた抑制ルール、イベントフィルタの変更、アラートチューニングが表示される場合があります。

複数の XDR テナント（つまり、追加のマネージドテナント）をお持ちのお客様への注意: 脅威は監視され、調査はお客様の XDR テナントごとに個別に作成されます。脅威の検出と調査は、複数のテナント間でまとめて実行されることはありません。

応答

ソフォスは、お客様から書面による承認を受けた後、お客様に代わって Taegis™ XDR 内でサポートされている脅威対応アクションを実行します。これは、以下に記載するプロアクティブレスポンスの形で行われる場合があります。サポートされているアクションの最新のリストは、お客様のリクエストに応じて提供できます。サポートされている一部のアクションについて、お客様はオプションで、Taegis™ XDR 内で Taegis Actions を使用して、ソフォスがプロアクティブな対応アクション（事前承認済み封じ込めアクションとも呼ばれます）を実行することを承認することができます。プロアクティブ対応が有効になっているお客様は、こちらを参照してください。

複数の XDR テナント（つまり、追加のマネージドテナント）をお持ちのお客様向けの注意: 脅威対応アクションは、お客様の XDR テナントごとに個別に実行されます。脅威対応アクションは、複数のテナント間でまとめて実行されることはありません。

Taegis 内で悪意のある活動が観察され、ソフォスがアクティブな脅威として確認した場合、ソフォスは追加の対応措置（Unlimited Response）を実行します。お客様が許可した侵入、脆弱性、または技術テストに関連する活動は、Unlimited Response の対象外です。ソフォスが Unlimited Response が必要かどうかを判断する際には、以下のすべての基準を満たす必要があります。

- お客様の Sophos Taegis MDR サブスクリプションの範囲内のアクティブなレポート資産で発生している、お客様の環境で観察されたアクティビティは、人間の敵対者の存在を示しています（例:水平移動の成功、データ流出、資格情報アクセス、特権昇格の証拠）
- 敵対者の活動またはセキュリティインシデントが、ソフォスが作成した調査に起因している
- 脅威に関連するシステムは、悪意のあるアクティビティが発生する前の少なくとも過去 7 日間、サポートされている統合を通じて Taegis にテレメトリをアクティブに送信しています

Unlimited Response には、次のアクティビティのみが含まれます。

- Taegis 内にあるテレメトリのエンドポイント分析
- Taegis と統合されたネットワークセンサーからのネットワーク分析
- ソフォスの対応契約の結果として発見されたマルウェアの悪意のあるコード分析
- Taegis 内で利用可能なサポートされているインテグレーションから収集されたデータのログ分析
- テレメトリデータを Taegis にアクティブに送信するエンドポイントのトリアージデータ
- Taegis でサポートされている対応アクション

注: Unlimited Response の利用は、お客様の顧問弁護士との特権的な関わりやサイバー保険会社との関わりを必要とする事項には適用できません。このような問題については、インシデントレスポンスの対応を開始するために、チャットを介してセキュリティアナリストまでご連絡ください。

ソフォスは、セキュリティインシデントの状況について、実施された活動に関する情報や注目すべき発見事項など、セキュリティインシデントの状況に関する最新情報を書面でお客様に提供します。調査結果は、発見時にお客様に通知されます。Unlimited Response の活動が完了すると、ソフォスは、調査の詳細と推奨事項を含む調査レポートをお客様に送付します。このレポートは、XDR の調査内でお客様に配信され、レポートが配信された時点で、調査は終了したと見なされます。同様に、Unlimited Response プロセスにおいて、ソフォスがお客様からの連絡を求め、72 時間以内に連絡がない場合、調査は終了したものとみなされます。お客様が同じ根本原因の活動を理由に Unlimited Response を複数回リクエストした場合、お客様は、Unlimited Response の資格を継続するために、ソフォスが推奨するセキュリティ体制の変更を実施する必要があります。

脅威ハンティング

ソフォスは、サポートされているインテグレーションから XDR を通じて脅威ハンティングを実施します。ソフォスは、収集したお客様のテレメトリを検査し、脅威アクター（その戦術、技術、手順、または「**TTP**」を通じて）異常なユーザーアクティビティ、ネットワーク通信、およびアプリケーションの使用、永続化メカニズムなどの活動を検出します。さらに、ソフォスは、お客様の情報技術（以下、「**IT**」）環境全体で脅威ハンティングを毎月実施し、現在のインシデント対応の取り組みから収集した侵害と戦術の関連指標を探しています。脅威ハンティングの一部として脅威が検出されると、調査と顧客通知が XDR、電子メール、またはサポートされているインテグレーションを介して作成されます。

複数の XDR テナント（つまり、追加のマネージドテナント）をお持ちのお客様への注意: 脅威ハンティングは、お客様の XDR テナントごとに毎月個別に実施されます。

ソフォスの脅威インテリジェンス

XDR は、Sophos Threat Intelligence に基づいています。お客様のネットワークとエンドポイントのテレメトリは、ネットワーク、エンドポイント、および動作の指標と継続的に比較され、お客様の IT 環境内の脅威を特定します。

継続的な改善

ソフォスは、お客様のセキュリティ体制の継続的な改善を推奨します。Taegis MDR のお客様向けに、ソフォスは四半期ごとの脅威の傾向、プログラムの目標、XDR の注目すべきアクティビティを提供し、改善のための推奨事項を提供します。ソフォスは、独自の裁量により追加の専門家と共に本項に定めるサポートを提供することがあります。

複数の XDR テナント（つまり、追加のマネージドテナント）を有するお客様の注意事項: お客様は、特定のテナント レベルのレビューではなく、顧客レベルで統合されたレポートと推奨事項を受け取ります。ただし、アラート、調査、脅威ハンティングなど、XDR の注目すべきアクティビティは、お客様の XDR テナントごとに提供されます。

サービスフェーズ

サービスの提供には主に 2 つの段階、**オンボーディング**と**ステディステート**があります。

オンボーディング

オンボーディングと展開に先立ち、ソフォスはお客様の XDR インスタンスへのアクセスをプロビジョニングすることでお客様のサービスを有効化します。これによりお客様は、1）オンラインドキュメント、2）Taegis™ XDR エンドポイントエージェントを準備、展開するためのガイドにアクセスできるようになります。

お客様は、Taegis エンドポイントエージェントまたはその他のサードパーティ製エンドポイントエージェント、および Taegis™ XDR コレクターをお客様の環境に導入する責任を負います。XDR コレクターのダウンロード方法は、オンラインドキュメントに記載されています。ソフォスは、必要に応じ質問について電話会議を通じてリモートでお客様をサポートします。

お客様がライセンスボリュームの少なくとも 40%を展開（例 エンドポイントに XDR と互換性のあるエンドポイントエージェントを展開）し、お客様が Taegis™ MDR オンボーディング概要のパート 1 およびパート 4 内のトレーニングビデオを完了したことを確認した場合、オンボーディングが完了し、以下に定めるセキュリティ調査のサービスレベルに達したものとみなします。但し、ソフォスは、Taegis MDR サービスの効果を最大化するため、お客様がライセンスボリュームすべてのエンドポイントに Taegis エンドポイントエージェント（またはその他の互換性あるエンドポイントエージェント）を展開することを強く推奨します。完全に展開が完了するまで、お客様は、お客様の環境に対する Taegis MDR サービスの能力が低下するというリスクを理解し、同意し、受け入れるものとします。これらの制限の詳細については、『MDR オンボーディングガイド』を参照してください。

複数の XDR テナント（つまり、追加のマネージドテナント）をお持ちのお客様への注意: ソフォスは、お客様の XDR テナントの各インスタンスへのアクセスをプロビジョニングします。お客様は、お客様の各 XDR テナントにエンドポイント エージェントとデータ コレクターを展開する責任があります。各テナントのステディステートに到達するには、そのテナントに割り当てられたライセンスボリュームの少なくとも 40%

を展開し、**各テナントの**顧客担当者が Taegis™ MDR オンボーディング概要のパート 1 と 4 内のトレーニング ビデオの完了を確認する必要があります。オンボーディング中、ソフォスはお客様と協力して、各テナントのライセンスボリュームの初期割り当てを決定し、文書化します。ステディステートに達した後、お客様は、各 XDR テナントに対して（ライセンス量に応じた）エンドポイント エージェントの総量をお客様の裁量で再配分することが出来ます。ソフォスは、複数テナントのオンボーディングに必要な複雑さとプロジェクト管理をサポートする「Enablement Plus」を強くお勧めします。

ステディステート

お客様の環境のステディステートの監視は、お客様がライセンス ボリュームの少なくとも 40% を展開し（つまり、XDR と互換性のあるエンドポイント エージェントをエンドポイント）、**かつ**お客様は、Taegis™ MDR オンボーディング概要のパート 1 とパート 4 内のトレーニングビデオの完了を確認した時点で開始されます。

フェーズ	アクティビティ

オンボーディング	***タイミング: XDR のアクティブ化からステディステートになるまで***
	• 以下を含むお客様に関する詳細情報について確認します。
	  ○ IT 環境
	  ○ エンドポイントエージェントの展開
	  ○ XDR との統合
	  ○ 主な連絡先と他の XDR ユーザー
	  ○ お客様資産の物理的な場所
	  ○ お客様の重要な資産 （エンドポイント） と価値の高いターゲット
	• お客様は、Taegis™ MDR オンボーディング概要のパート 1 と 4 のトレーニングビデオを完了します。

最初のベースライン会議	***タイミング: ステディステートの監視が開始されてから約 4 週間後*** • 共有プログラムの目標を定義して、継続的な改善のための計画を確立する • お客様の IT 環境、セキュリティコントロール、その他の関連する状況を理解するために、お客様のプロファイルを確認する • XDR の検出メカニズムがお客様にどのように適用できるかについてのガイダンスを提供する • 顧客向けに作成された注目すべきアラート、調査、脅威ハンティングを確認する

フェーズ	アクティビティ
四半期ごとの更新	***タイミング: ベースライン会議が実施された後、四半期ごと*** • プログラムの目標と計画を確認する • 脅威の状況に関する最新のトピックを確認する • 調査とアラートの傾向を確認する • セキュリティ体制のガイダンスを提供する

お客様の義務

お客様は、以下に列挙する義務を履行する必要があり、後章に記載する「サービスレベルアグリーメント」（以下、「**SLA**」）の遵守を含め、本契約に基づくソフォスの義務履行可否は、お客様のこれら義務の遵守に依ることを認識し、これに同意するものとします。本サービスに関するお客様の義務不履行により、サービス機能の制限および低下、本サービスの管理対象コンポーネントおよび／または SLA の停止、または本サービスの監視のみコンポーネントへの移行が生じる場合があります。

複数の XDR テナント（つまり、追加のマネージドテナント）をお持ちのお客様への注意: 以下に列挙する「お客様の義務」は、お客様の **XDR テナントごと**に必須であり、適用されます。

お客様は、次のことを実施します。

- お客様の IT 環境において、本サービスのライセンスが付与される各エンドポイントに XDR と互換性のあるエンドポイントエージェントがインストールされていることを確認する
- 各エンドポイントに互換性のある互換性のあるエンドポイントエージェントを導入する（上記の通り、ライセンスボリュームの少なくとも 40%が導入されれば、ステディステートへの移行を開始できる）
- サードパーティ製のエンドポイントエージェントのライセンスおよび/またはサポートを正規の供給元から取得する
- 本サービスを実行するための十分なネットワーク帯域幅とアクセスの可用性を確保する
- サービスが最適に稼働していることを担保するため、統合の正常性と関連するお客様資産の健全性を監視する
- XDR との統合で必要となる適切なアクセスをソフォスに提供する
- ソフォスの統合機能でサポートされているバージョンでセキュリティコントロールが動作していることを確認する

- XDR との統合のための認証情報と権限を管理する
- お客様の認可された連絡先リスト（権限や関連情報を含む）が最新の状態であることを確認する
- ソフォスがお客様に対する脅威について調査を行う際に、情報と支援（ファイル、ログ、IT 環境のコンテキストなど）を迅速に提供する
- XDR 内でレポートをスケジュールし、アドホックレポートを実施する
- カスタムルールの作成と管理（カスタムアラートの検出と分析など）は、お客様ごとで異なり、ソフォスではサポートされないため、内部サポートを確保する

サービスレベルアグリーメント（SLA）

ソフォスが調査を実行し、脅威が悪意のあるものであるかどうかを判断する能力は、互換性のあるエンドポイントエージェントがお客様の IT 環境のライセンス対象のエンドポイントにインストールされていることに依存します。以下のサービスレベルは、本サービスの一部としてライセンスを取得し、ソフォスインフラストラクチャとアクティブに通信しているエンドポイントに適用されます。

注: ソフォスが SLA を提供する調査の種類はセキュリティ調査のみであり、他の種類の調査には SLA は提供されません。

サービスレベル	定義	測定	目標	クレジット
セキュリティ調査	ソフォスは、XDR の脅威を監視します。悪意のある行為が検出された場合、ソフォスは調査を実施し、分析を提供し、お客様に通知します。 ソフォスは、XDR、電子メール、またはサポートされているインテグレーションの使用を含む電子的な方法でお客様に通知します。 進行中の調査または監視の一部として特定された後続の関連アクティビティは、既存の調査に追加されます。	ソフォスによって測定された、調査作成タイムスタンプから顧客通知タイムスタンプまでの時間	60 分未満	タイムスタンプの差が 60 分から 240 分の場合、月額サービス料の 1/100 タイムスタンプの差が 240 分を超える場合、月額サービス料の 1/30 1 暦日につき最大 1 クレジットが付与されます（米国東部標準時に基づく）。

サービスレベル	定義	信用
Unlimited Response	IR ホットライン、XDR のアプリケーション内チャット、または XDR 内のチケットシステムを通じて提出された Unlimited Response の緊急リクエストは、4 時間以内にソフォスチームによって承認されます。	SLA が満たされていない各暦日（米国東部標準時に基づく）の月額サービス料金の 1/100

保証の除外

本サービスはリスクの軽減を目的としていますが、リスクを完全に排除することは不可能であり、したがって、ソフォスは、お客様のネットワークに侵入、侵害、またはその他の不正な活動が発生しないことを保証するものではありません。

追加情報

本サービスの請求は、XDR の請求と同時に開始され、XDR のログイン資格情報が電子メールでお客様に送信されたときに発生します。最新の詳細については、アカウントマネージャーにお問い合わせいただくか、ご購入時のお客様の契約書に記載されている正式な規約をご参照ください。

互換性のあるブラウザ、統合、検出器、ダッシュボード、及びトレーニングについては、Taegis XDR 内のドキュメントを参照してください。リリースノートなどその他の情報も入手できます。

用語集

用語	説明
追加のマネージドテナント	お客様に複数の XDR テナントを提供する Taegis MDR のアドオンです。
アラート	XDR 内の検出器によって検出、優先順位付けが行われた疑わしいまたは悪意のある振る舞いです。
エンドポイントエージェント	エンドポイントにインストールされ、脅威の分析および検出のために、エンドポイントのアクティビティおよびオペレーティングシステムの詳細に関する情報を収集し、XDR に送信するために使用されるアプリケーションです。 XDR と互換性のあるエンドポイントエージェントのリスト： https://docs.taegis.secureworks.com/at_a_glance/#endpoints

用語	説明
統合	アプリケーションプログラミングインターフェース（以下、「**API**」）コール、または接続された技術に対して合意されたサービスを実施するためのその他のソフトウェアスクリプトです。
調査	XDR 内の中心的な場所で、顧客の IT 環境の資産を標的とする脅威に関する証拠、分析、推奨事項を収集するために使用されます。調査は、セキュリティやインシデントレスポンスなどのタイプに分類されます。
セキュリティアナリスト	ソフォスのセキュリティ専門家であり、お客様にとって「重大」および「高」と判断されたアラートを分析し、調査を作成してエスカレーションします。 ***注:*** セキュリティアナリストは、ソフォスの他の文書では、Taegis MDR アナリストまたは MDR アナリストと呼ばれることもあります。
セキュリティインシデント	XDR が生成した出来事で、お客様の環境で侵害または侵害の疑いが発生したものです。
セキュリティ調査	XDR の「重大」または「高」のアラートまたはその他イベントに対して、セキュリティアナリストが脅威の有効性を判断するための予備的な調査手順を完了した後に実施される調査のタイプです。
サービスレベルアグリーメント（SLA）	定義されたサービス提供基準を満たすための拘束力のある合意です。
サービス期間	本サービスがお客様に提供される、契約書で特定された期間です。
脅威	XDR によって特定された活動で、お客様の IT 環境の資産に害を及ぼす可能性のあるものです。
脅威ハンティング	既存のセキュリティメカニズムを回避する現在または過去の脅威を積極的かつ反復的に発見し、その情報を将来の対策開発やサイバーレジリエンスの向上に役立てます。