Sophos Taegis™ Elite Threat Hunting - 日本

本サービス仕様書は、Sophos Taegis Elite Threat Hunting（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

本サービスの利用には、Sophos Taegis™ MDR、Taegis MDR Plus、または Taegis MDR Enhanced（以下、「**MDR**」）のサブスクリプションが必要となります。

- **MDR の新規のお客様:** MDR と同時に Elite Threat Hunting をご購入頂いたお客様の場合、オンボーディングに先立ち、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。
- **MDR の既存のお客様:** 既存の MDR サブスクリプションに Elite Threat Hunting を追加するお客様の場合、 ソフォスは Elite Threat Hunting の契約書の発効日にお客様のサービスを有効にします。

本サービスは、お客様にスレットハンター、定期的な脅威ハンティングに関するミーティング、継続的な人間主導の脅威ハンティング、及びカスタマイズされた脅威ハンティングを提供します。

備考:

- サービス及び関連するサポートは、日本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）を有するお客様の場合**、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

エリート脅威ハンティング

ソフォスは、人間主導による脅威ハンティングを実施し、関連する調査結果は XDR の調査内でお客様に提供されます。お客様に割り当てられた脅威ハンターが主導するソフォス独自の方法論、専門知識、脅威分析、及び脅威インテリジェンスは、戦術、技術、手順（以下、「**TTP**」）を通じて未知の脅威及び未発見の脅威アクターを特定するとともに、可視性の欠陥、設定ミス、または発見されたデータソースの欠落を特定するために使用されます。さらに、スレットハンターは、収集されたお客様のテレメトリを検査して、異常なユーザー アクティビティ、ネットワーク通信、アプリケーションの使用と永続化メカニズムなどのアクティビティを検出します。

ソフォス Threat Hunting チームは、Threat Hunting に特化したサポートを月曜から金曜の 9:00 – 17:00 JST(UTC+9）に一般提供しています。ただし、すべてのサポート問い合わせについては、お客様はソフォス Security Operations Center（以下、「**SOC**」）に連絡する必要があり、SOC は必要に応じて Threat Hunting チームと連携します。お客様が上記の期間内にない時間にソフォス SOC にサポートを求め、お客様の問題を解決するために脅威ハンティング固有の情報が必要な場合、脅威ハンティングチームは上記の時間内にできるだけ早く関与します。

エリート脅威ハンティングには、次のものが含まれます。

- 脅威ハンティングを効果的に実施する目的で、お客様と協力してお客様の環境を完全に理解する脅威ハンターの割り当て
- XDR でお客様のテレメトリ全体を継続的に人間主導の脅威ハンティングし、お客様のセキュリティ体制を危険にさらす検出されない脅威とセキュリティ上リスクのある露出を探します

- お客様と合意した時間に、スレットハンターと毎月最大 2 回のタッチポイントミーティングを行い、以前に共有された脅威ハンティングの調査結果について話し合い、お客様のリスクと目的に合わせて要求されたカスタマイズされた脅威ハンティング（以下で説明）について話し合い、合意します。
- お客様の要求に応じて、毎月最大 4 回までカスタマイズされた脅威ハンティングを実施します（最大 1 週間に 1 回、要求されたハンティングを開始するまでに最低 3 営業日の処理時間）。お客様のソフォスによる調査依頼のうち、実行不可能と判断された場合は、月間限度額にカウントされます。これらの脅威ハンティングには、以下が含まれますが、これらに限定されません。
    - アーティファクト主導の脅威ハンティング
    - クラウドとネットワークの脅威ハンティング
    - 仮説主導型の脅威ハンティング
    - 脅威インテリジェンス主導の脅威ハンティング
- 脅威ハンティング中に発見されたすべての活動のうち、重大と見なされ、確認されたセキュリティインシデントまたは脅威（設定ミス、可視性の欠陥など）を表す可能性のあるすべての活動について、Taegis の調査を通じて分析及びお客様へのエスカレーションを行う。

備考:

- **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: 上記の Elite Threat Hunting アクティビティ**から作成された調査は、対応するお客様の XDR テナントに表示されます。毎月提供されるカスタマイズされた脅威ハンティングの最大数は、テナントの数に関係なく 4 回です。スレットハンターとのタッチポイントミーティングの最大数は、テナントの数に関係なく 2 回です。

  明確にするために、顧客に 4 つの個別のテナントがある場合、個々のテナントに対して同じカスタマイズされた脅威ハンティングを実行すると、1 つではなく 4 つのカスタマイズされた脅威ハンティングとしてカウントされます。

- エリート脅威ハンティングは、関連する MDR の指定されたオンボーディング アクティビティが完了し、お客様がステディステートに入るまで開始できません。（関連するサービスの説明を参照してください。 https://www.sophos.com/en-us/legal/）。さらに、ソフォスは、本サービスの効果を最大化

するために、お客様がサポート対象のエンドポイントエージェントをすべてのエンドポイント（お客様のライセンス数量まで）に完全に展開することを強くお勧めします。すべてのエンドポイントに完全に展開されるまで、お客様は、本サービスがお客様の環境に対して機能が低下するリスクを理解し、同意し、受け入れるものとします。

- Elite Threat Hunting のお客様が CrowdStrike エンドポイントの使用を希望される場合は、標準の Falcon Data Replicator（FDR）を CrowdStrike または CrowdStrike 認定リセラーから直接購入する必要があります。

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

MDR のステディステートが達成されると（https://www.sophos.com/en-us/legal/).の該当する MDR サービスの説明に記載されている定義に従い）、お客様と スレットハンターとの初回ミーティングが調整されます。この初回ミーティングでは、スレットハンターがハンティング方法と初期戦略を説明し、お客様はスレットハンターにお客様の環境とハンティングの優先順位を伝えます。

ステディステート

スレットハンターとの最初のミーティングの後、お客様の MDR サービスもステディステートにあると想定し、ステディステートのサービスが開始されます。注意事項として、MXDR ではお客様がライセンス数量の少なくとも 40%のエンドポイントエージェントを展開し（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にデプロイした場合）、MDR Onboarding Overview のパート 1 と 4 のトレーニング ビデオの完了を確認した場合に、ステディステートと見なされます。

フェーズ	アクティビティ
オンボーディング	***タイミング:MDR がステディステートになったら*** • エリート脅威ハンティングの紹介電話会議を進行して、お客様と以下の内容について話し合います。 　○ 概要と成果物

フェーズ	アクティビティ
	○ 役割、責任、範囲 ○ 隔週(月 2 回まで）の運用電話会議
隔週の会議	***タイミング:ステディステートサービス開始から約2 週間後*** • 顧客向けに作成された注目すべきアラート、調査、脅威ハントを確認する • お客様の環境と体制の変更について話し合う • 脅威の状況の進展とハンティング戦略について話し合う
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*** • 最近のハンティング・イニシアチブと調査結果の要約は、エグゼクティブ・レポーティングに含めるためにカスタマーCSM に送信されます

お客様の義務

お客様は、以下に列挙される義務を履行する必要があり、ソフォスが本契約に基づく義務を履行できるかどうかは、お客様がこれらの義務を遵守するかどうかに依存することを認識し、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の不遵守は、制限およびサービス能力の低下につながる可能性があります。

複数の XDR テナント（つまり、追加のマネージドテナント）を有するお客様の場合: 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。

お客様は以下のことを実施します。

- スレットハンターに対応して、隔週のミーティングを調整する
- 上記のタイミングに従って、カスタマイズされた脅威ハンティングリクエストに対応する（最大で週に 1 回、リクエストされたハンティングを開始するまでの期間は、最低 3 営業日）
- スレットハンターから提供された推奨事項と調査結果を受け入れる

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、お客様のネットワークへの侵入、侵害、またはその他の不正な活動が発生しないことをソフォスが保証するものではありません。

追加情報

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、XDR 内のドキュメント(https://docs.ctpx.secureworks.com/)を参照してください。リリースノートなどのその他の情報も入手できます。

用語集

用語	説明
アーティファクト主導の脅威ハンティング	このプロアクティブなアプローチは、潜在的な脅威を発見するために、メールボックスルールや永続的メカニズムなど、特定のアーティファクトに焦点を当てることから始まります。これは、既知の悪意のある活動を見つけるために既存のデータを分析することに重点を置いた事後対応型の方法です。
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.ctpx.secureworks.com/at_a_glance/#endpoints.

用語	説明
仮説主導型の脅威ハンティング	このプロアクティブな方法には、環境と攻撃者の行動に関する知識に基づいて、潜在的な脅威に関する仮説を立てることが含まれます。ハンターは、これらの仮説を検証し、隠れた脅威を明らかにするために、特定の調査を設計します。
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。
プロアクティブなリスクの特定	攻撃者に悪用される前に、組織の IT 環境内の潜在的なセキュリティリスク、設定ミス、不十分なセキュリティ管理策をプロアクティブに探索するプロセスです。
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。

用語	説明
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。
カスタマイズされた脅威ハント	顧客によってリクエストされた脅威ハントで、脅威ハントの実行可能性と実行は、スレットハンターによって決定されます。
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。
脅威ハンター	脅威ハンティングを専門とするソフォスの専任セキュリティ専門家です。
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。
脅威インテリジェンス主導の脅威ハンティング	IOC（Indicator of Compromise: 侵害の指標）を使用してネットワーク内を探索する、リアクティブな脅威ハンティングのタイプです。