Sophos Managed Detection and Response

サービス仕様書（Sophos MDR および Sophos MDR Plus）

> **注: これは機械的に生成された翻訳で、お客様の便宜のためにのみ提供されています。この機械的に生成された翻訳は、人間による翻訳の質に匹敵するものではなく、エラーが含まれている可能性があります。この翻訳は「現状のまま」提供され、翻訳の正確性、完全性、または信頼性については保証されません。 本書の英語版と翻訳版の間に矛盾がある場合は、英語版が優先されます。**

このサービス仕様書では、Sophos Managed Detection and Response（ **「Sophos MDR」** ）および Sophos Managed Detection and Response Plus（ 「**Sophos MDR Plus**」） （それぞれ「**本サービス**」）について説明します。

本サービス仕様書は、該当する場合、以下のいずれかの一部であり、これに組み込まれます。(i) お客様またはマネージド サービス プロバイダー (「**MSP**」) が ソフォス と締結した、本サービスのサブスクリプションの購入に関する手動またはデジタル署名済みの契約。(ii) マネージド サービス プロバイダーが ソフォス と締結した、サービスの一部であるオファリングの購入に関する手動またはデジタル署名済みの契約。(iii) 上記の署名済みの契約が存在しない場合は、本サービス仕様書は https://www.sophos.com/legal に掲載されている ソフォス エンド ユーザー利用規約 (総称して**「本契約」**) の条項に準拠します。本契約の条項と本サービス仕様書の条項との間に矛盾がある場合は、本サービス仕様書の条項が優先されます。

本契約のいかなる規定にもかかわらず、お客様/MSP は、以下の事項を認識し、同意するものとします。(i)ソフォスは、サービスの全体的な範囲またはレベルを実質的に低下させない限り、サービスを随時変更または更新することができます。(ii) ソフォスは、サービスの変更を反映するために、このサービス仕様書を随時変更または更新することができます。ただし、このような更新は、サービスに関するソフォスの義務を実質的に低下させるものではありません。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有効になります。

I.定義

本サービス仕様書で使用されている大文字で始まる用語で、本契約で別途定義されていないものは、以下の意味を持ちます。

「エージェントレスサードパーティエンドポイント」とは、サポートされているサードパーティのエンドポイントセキュリティ製品を実行し、Sophos XDR または XDR Sensor を必要とせずにテレメトリを Sophos Central に継続的に送信するように構成されたデバイスまたはサーバーシステムを意味します（つまり、API ベースの取り込み、ログまたはイベントのストリーミング/エクスポート、コネクタ、またはその他のサポートされている送信方法）。

「ケース」とは、Sophos Central 内の記録であり、関連する検出、分析、通信、対応措置、ステータス更新、解決の詳細などを含め、調査、問い合わせ、または要求を文書化および追跡するものです。ケースは自動的に生成される場合もあれば、Sophos Central 経由でお客様または MSP からのリクエストに基づいて生成される場合もあります。

「対象エンドポイント」とは、お客様/MSP によって本サービスの対象として指定され、サービス提供の条件として、ソフォスのドキュメントに従って適切に構成され、運用されており、必要なテレメトリを継続的に送信して Sophos Central を通じてソフォスから見える状態を維持している、監視対象エンドポイントまたはエージェントレスサードパーティエンドポイントを意味します。

「検出」とは、ソフォス、またはソフォスが提供する検出メカニズム（ソフォスが作成したルール、シグネチャ、モデル、分析、脅威インテリジェンス、相関ロジックを含む）によって、対象エンドポイントまたは統合システムによって生成されたデータが悪意のある活動または疑わしい活動の兆候であると判断することを意味します。明確にするために、検出には、Sophos Central 内またはサードパーティツール内を問わず、お客様/MSP（またはお客様/MSP に代わってパートナーまたは受益者）が作成した検出コンテンツによって生成されたデータは含まれません。

「ヘルス」とは、Sophos Central 内で確認できる、セキュリティ制御の有効性やソフォスによる本サービス提供能力に影響を与える、対象エンドポイントおよび統合システムの構成と設定の状態を意味します。

「インシデント」とは、ソフォスが確認した、お客様/MSP 資産の機密性、完全性、または可用性を脅かすシステムへの侵害または不正アクセスを意味し、対話型攻撃者の行動、データの暗号化または破壊、認証情報の悪用、またはデータの漏洩などの悪意のある活動が存在するため、インシデント対応が必要となります。

「インシデント対応」とは、第 III 章第 2 条に記載されているように、インシデントの調査、封じ込め、軽減、および無力化のためにソフォスがリモートで実行する技術的なプロセスを意味します。

「インシデント対応アドバイザー」または「アドバイザー」とは、第 III 章第 2.1.2 条(a)に詳述されているように、インシデント発生時にお客様/MSP の主要な連絡窓口として割り当てられたソフォスの担当者を意味します。

「統合システム」とは、ソフォスがサポートする統合機能および統合メカニズムを使用して、テレメトリ、アラート、またはセキュリティイベントを Sophos Central に送信するように構成された、ソフォスがサポートするシステムまたはソフォス以外のシステム（たとえば、ID、クラウド、電子メール、ファイアウォール、ネットワーク、またはその他のセキュリティ関連システム）を意味します。統合システムには、対象となるエンドポイントは含まれません。

「調査」とは、ソフォスがケース内の活動が悪意のあるものであり、脅威対応が必要かどうかを判断するために用いる正式なプロセスおよび方法を意味します。

「調査対象ケース」とは、検出または脅威ハンティングの結果から発生したケースであり、ソフォスの合理的な判断において、その活動が悪意のあるものかどうかを判断するための分析を必要とするセキュリティ上の関連性があると判断されるケースを意味します。調査ケースは、ソフォスによる人的レビューと自動化プロセスの組み合わせによって実施され、ソフォスによって手動で作成される場合もあります。

「監視対象エンドポイント」とは、本サービス提供をサポートするために Sophos XDR または XDR Sensor がインストールされ、稼働しているすべてのシステムを意味します。サポート対象のオペレーティングシステムおよびプラットフォームは、ソフォスのドキュメントに記載されており、ソフォスは随時これらのドキュメントを更新する場合があります。

「優先調査」とは、潜在的な影響、緊急性、攻撃者の行動、影響を受ける資産など、入手可能な証拠を総合的に評価した結果、ソフォスが重大度の高い、または重大な調査案件として分類したケースを意味します。ソフォスが調査案件を優先調査として分類した場合、その分類は本サービス仕様書のすべての目的において最終的なものとなります。

「修復ガイダンス」とは、お客様/MSP が、ヘルス状態への対処、脅威対応のサポート、またはインシデントの軽減もしくは解決のために、対象エンドポイント、統合システム、またはお客様/MSP のセキュリティツールに対して講じる必要のある措置に関して、ソフォスが提供するガイダンスを意味します。

「対応措置」とは、Sophos Central 内で実行される措置、および監視対象エンドポイントまたは統合システムに対して実行される措置を含め、悪意のある活動または疑わしい活動を調査、封じ込め、妨害、または無力化するために、ソフォス が手動または ソフォス の自動システムを通じて実行する措置を意味します。対応措置には、お客様への通知、リモート照会、ホストの隔離、プロセスの終了、悪意のあるアーティファクトの削除または隔離、インジケータのブロック、ユーザーの無効化、セッションの取り消し、Sophos Central 内の構成、ポリシー、またはその他の設定の変更、サポート対象製品へのインジケータの更新または挿入、および該当する統合によってサポートされるその他の措置が含まれますが、これらに限定されません。エージェントレスサードパーティエンドポイントの場合、応答アクションとは、ホストの隔離とホストの隔離解除のみを意味します。サポートされている Sophos 製品および統合機能で利用可能な対応アクションについては、Sophos MDR 対応アクションのドキュメントに記載されており、随時更新されます。

「サービスソフトウェア」とは、本サービスの状況に応じて、Sophos XDR および/または XDR Sensor を意味します。

「Sophos XDR」とは、Sophos Endpoint Protection with XDR のことです。

「脅威ハンティング」とは、Sophos Central 内で利用可能なデータを、手動と自動化された活動を組み合わせて、積極的に反復的に検索し、既存の制御を回避した可能性のある悪意のある活動の兆候や指標を特定するプロセスを意味します。

「脅威対応」とは、ソフォスが、該当する場合はお客様/MSP との協力のもと、悪意のある活動または疑わしい活動を封じ込め、妨害し、軽減し、または無力化するために使用する方法、プロセス、通信、および対応措置を意味します。脅威対応には、ソフォスが実施する対応措置と、お客様/MSP に提供される修復ガイダンスが含まれる場合があります。

「脅威対応モード」とは、Sophos Central でお客様/MSP が選択した認証モデルを意味し、第 1.2 条でさらに詳しく説明するように、脅威対応中にソフォスが対応アクションを実行するかどうかと方法を決定します。

「XDR センサー」とは、Sophos XDR センサーのことです。

II.サービスレベル

お客様/MSP が購入できる本サービスには、2 つのレベルがあります。

1. **Sophos MDR** :第 3.1 条に記載されている活動および特典のみが含まれます。
2. **Sophos MDR Plus** ：MDR Plus プランには、第 3.1 条および第 3.2 条に記載されている活動と特典が含まれます。第 2.1 条に基づくインシデント対応は、Sophos XDR を実行している監視対象エンドポイントでのみ実施されます。サービスレベル契約（第 2.2 条）および侵害保護保証（第 2.3 条）は、これらの項に規定されているとおりに適用されますが、第 IV 章および第 V 章に記載されている要件および除外事項が適用されます。

III.サービス範囲

本サービスは、お客様/MSP が購入したティアに応じて、以下に説明する活動で構成されます。

1.Sophos MDR および Sophos MDR Plus に適用される活動 1.1 オンボーディング

本サービス提供の前提条件として、お客様/MSP はオンボーディング時に以下の活動を実施する必要があります。

a.お客様/MSP は、(i)連絡先情報を提供し、(ii)コミュニケーションの好み（例えば、電子メール、電話、および/または Sophos Central）を決定し、(iii)Sophos Central 内で脅威対応モードを選択します。MSP は、提供される本サービスに関する連絡窓口として機能しなければならない。受益者 MSP の。

b.MSP は、(i) ソフォスが本サービスを実行するために必要な受益者からの同意または情報の取得、(ii) 受益者が本サービス仕様書に基づいてお客様に求められるすべての行動をとることの確保、および(iii) 受益者に対し本サービスのリスクと潜在的な影響について助言することについて、単独で責任を負います。

c.お客様/MSP またはパートナーは、ソフォスのドキュメントに従って、対象となるエンドポイントおよび統合システムが該当するテレメトリを Sophos Central に送信するように環境を構成します。

これには、(i)監視対象エンドポイントへの該当するサービスソフトウェアのインストールと構成、および(ii)テレメトリを Sophos Central に送信するように該当するエージェントレスサードパーティ製エンドポイントを構成することが含まれる場合があります。

1.2 脅威対応モード

上記第 1.1 条に従い、お客様/MSP は Sophos Central で希望する脅威対応モードを選択します。 利用可能な脅威対応モードは以下のとおりです。

i. **承認**：ソフォスが脅威対応を実行するための事前承認を与え、対応措置が実行された後に通知を受け取るようにします。
ii. **協働**：ソフォスは調査を実施しますが、お客様/MSP の書面による同意なしには対応措置は講じません。ただし、リモート照会や証拠収集などの特定の対応措置は、お客様の同意や関与なしに実施される場合があります。
    - 協働後、承認：***「協働」***の下にオプションがあります。選択された場合、 ソフォスがお客様の指定したすべての連絡先に合理的な方法で連絡を試みた後も、お客様/MSP から確認応答を受け取らなかった場合、ソフォスが承認モードで動作することを許可します。
iii. **通知のみ**:ソフォスは調査を実施し、修復に関するガイダンスを提供します。お客様/MSP は、通知のみの対応が封じ込めおよび妨害対策を大幅に遅らせ、お客様/MSP のシステム、事業運営、およびデータに対するリスクを高める可能性があることを認識し、これに同意するものとします。

1.3 ヘルスチェックソフォスは、第 1.1 条に記載されているオンボーディングプロセスの完了後 30 日以内に、ヘルスの初期評価を実施します。これには、セキュリティ制御の有効性や本サービスの提供に影響を与える可能性のある状況を特定するために、Sophos XDR の構成と設定をレビューすることが含まれる場合があります。 。ソフォスは、初回評価時または本サービス契約期間中のいつでも、健康状態を特定し、必要に応じてお客様/MSP に通知し、改善策に関するガイダンスを提供する場合があります。是正措置に関するガイダンスを適時に実施しない場合、サービス品質の低下、またはソフォスによる調査の実施および対応措置の実施能力の制限につながる可能性があります。

1.4 トリアージ、調査、および脅威への対応。

a.トリアージと優先順位付け。ソフォスは検出結果を分析し、さらなる分析のためにアクティビティを特定、集約、優先順位付けします。トリアージによって、ソフォスによるレビュー用の機械生成ケースが作成される場合があります。

b.調査。ソフォスは、活動が悪意のあるものか不審なものかを確認し、適切な対応を決定するために調査を実施します。調査では、テレメトリ、脅威インテリジェンス、自動化、および人間による分析が活用される。ソフォスは、調査結果を利用して、想定される活動や無害な活動を除外し、お客様/MSP の環境における疑わしい活動の可視性を向上させる場合があります。フィルタリングの決定は、ソフォスがその時点で入手可能な情報に基づいて合理的な判断で行い、ソフォスは過去にフィルタリングされたアクティビティを遡って再調査する義務を負いません。調査ケースは、ソフォスが当該活動が悪意のあるものではないと判断した場合、脅威対応を正当化しない場合、またはお

客様/MSP が選択した脅威対応モードでソフォスが行動することを許可されていない場合、対応措置なしで解決されることがあります。

c.重大度の分類。ソフォスは、優先順位付けと対応の判断に役立てるため、調査対象事例を重大度別に分類します。重大度の分類は、ソフォスが入手可能なすべての証拠に基づいて誠意をもって決定するものであり、単一の要因が決定的な要素となることはありません。ソフォスの重大度の分類は、第 2.2 条に基づくサービスレベル契約の測定を含め、本サービスの説明の目的において適用されます。重大または高重大度に分類される調査事例は、第 I 章で定義されている優先調査です。

ソフォスは、追加情報が入手可能になった場合、調査案件を再分類することがあります。調査案件が重大度「高」または「重大」に再分類された場合、再分類の時点で優先調査案件となります。

以下の指標はあくまで例示です。重大度は、上述のように入手可能な証拠全体に基づいて決定され、個々の指標だけで重大度分類が決定されることはありません。

重大度	**例示指標**	**ソフォスの対応アプローチ**
重大	ランサムウェアのアクティブな展開、キーボード操作による攻撃者の活動、横方向の移動、データ漏洩、サプライチェーンの侵害、または外部機器の悪用が確認された場合。	ソフォスは、お客様/MSP が指定した担当者に対し、電話による連絡を開始します。該当する脅威対応モードでソフォスが行動することが許可されている場合、ソフォスは適切な対応措置を講じ、電話で講じた措置を確認します。承認が必要な場合、ソフォスは推奨される対応措置について承認を求めます。
高	C2 ビーコン機能を備えたマルウェア、アカウント侵害、侵害後のツール、またはペイロード配信を伴うエクスプロイトが確認されました。	ソフォスは、権限を与えられた場合、適切な対応措置を講じます。ソフォスは、脅威が封じ込められたと判断した場合、ケース更新を通じて通知を行います。脅威が封じ込められない場合、またはさらなる対応やお客様/MSP の関与または承認が必要な場合、ソフォスはお客様/MSP の指定担当者に電話で連絡を取ります。
中	潜在的に不要なプログラム、裏付けとなる兆候のない孤立した疑わしい活動、防止された汎用マルウェア、または明確な悪意のある文脈のない管理者関連の活動。	ソフォスは当該活動を調査し、必要に応じて、また承認されている場合は、適切な対応措置を講じます。ソフォスは、ケースの更新情報または電子メールを通じて連絡を取り、ケースが「高」または「重大」に再分類されない限り、電話による連絡は行いません。

d.脅威への対応。　脅威対応が必要な場合、ソフォスはお客様/MSP が選択した脅威対応モードに従って脅威対応を実行します。脅威対応には、(i) ソフォスが対象エンドポイント、Sophos Central、

または統合システムに対して実行する対応措置が含まれる場合があります。 Sophos 製品の機能またはサポートされている統合を通じて技術的にサポートされている場合、および（ii）お客様/MSP が対象エンドポイント、統合システム、またはお客様/MSP のセキュリティツールに対して実行する必要のあるアクションに関する修復ガイダンスがお客様/MSP に提供されます。。お客様/MSP は、レスポンスアクションを実行するために必要な該当する製品機能および統合の設定と有効化について、単独で責任を負います。ソフォスは、独自の裁量により、本サービスでサポートされる Sophos 製品および対応アクションを随時追加、変更、または削除する場合があります。

e.通知と報告。ソフォスは、第 IV 章第 7 条（サービス通知）に従って、お客様/MSP にケースを通知し、重大な健康問題や設定ミスに関する通知も行う場合があります。ソフォスは、検出、ケース、および対応措置に関するレポートとステータス更新を、ソフォスが本サービスに適切と判断する形式、内容、および頻度で、Sophos Central を通じて提供します。Sophos Central で利用可能な標準レポートを超えるカスタムレポートは対象外であり、別途プロフェッショナルサービス契約として提供される場合があります。

1.5 利用可能性。第 1.4 条に記載されているすべての監視、調査、および措置は、年中無休 24 時間体制で実施されます。お客様/MSP も直接通話するソフォスへのアクセス権を持ち、疑わしいインシデントを年中無休 24 時間体制でレビューできるようにします。

1.6 サービスレベル目標。以下のサービスレベル目標は、調査案件（脅威ハンティング活動によるものではなく）に関するタイミングガイドラインをお客様/MSP に提供するために使用されます。これらの目標は、対象となるエンドポイントおよび統合システムに関する調査にのみ適用されます。これらの目標はサービスレベル契約ではなく、統合の種類、データの可用性、およびお客様/MSP が選択した脅威対応モードによって異なる場合があります。

ケース作成の目標時間	検出結果が Sophos Central に取り込まれてから 2 分
初期対応の目標時間	ケース作成から、以下のいずれか 1 つ以上の開始まで 30 分以内：（i）お客様/MSP への連絡、（ii）調査証拠の収集、または（iii）対応措置の開始（該当する場合、およびサポートがある場合）。

1.7 脅威ハンティング。ソフォスは、脅威インテリジェンスと調査で確認された関連する侵害指標に基づき、既存の制御を回避した可能性のある脅威を探索するために、手動と自動化された方法を組み合わせた脅威ハンティングを実施します。脅威ハンティングは、Sophos Central で利用可能なデータ（対象となるエンドポイントおよびサポートされている統合システム向け）に限定され、攻撃者の行動や戦術の特定に重点を置いています。脅威ハンティングによって悪意のある活動の兆候が発見された場合、調査ケースが作成されます。明確にするために、既存の検出結果に対応して動作する自動分析、相関ルール、またはアラートによってトリガーされるワークフローは、事後的な調査に該当し、脅威ハンティングには該当しません。

1.8 リモートアクセスと管理者アクセス。本サービス提供をサポートするため、ソフォスはソフォスが所有または選択したリモートアクセスツールを使用して、対象エンドポイントにアクセスしたり変更を加えたりする場合があります。また、お客様/MSP の Sophos Central 環境への管理者アクセスを使用して、構成を表示または変更する場合があります。

お客様または MSP が脅威対応*「承認」モード*を選択した場合、このようなアクセスには各アクションごとに追加の承認は必要ありません。お客様または MSP が脅威対応の*「協働」モード*を選択した場合、ソフォスは変更を実行する前に承認を求めます。ソフォスによる対象エンドポイントおよび Sophos Central へのすべてのアクセスは記録され、ログに記録されます。

お客様/MSP は、ソフォスがお客様/MSP/受益者の環境に変更を加えたり、構成を修正したりすることを承認すると、お客様/MSP/受益者のシステムおよびインフラストラクチャの中断または劣化につながる可能性があることを認識し、これに同意するものとします。 さらに、お客様/MSP は、このような変更に対する承認を与えない場合、新たな悪意のある活動が発生したり、既存の悪意のある活動が悪化したりする可能性があることを認識するものとします。 お客様/MSP が変更または修正を行うための承認要求を拒否した場合、ソフォスは、そのような新たなまたは悪化した悪意のある活動から生じる、またはそれに関連するいかなる損害についても、お客様/MSPに対して責任を負いません。

1.9 言語サポート。ソフォスは、標準サービスおよび/または製品機能の一部として、オプションの言語サポート、またはサードパーティプロバイダーを通じた翻訳サポート（ **「言語サポート」** ）を提供する場合があります。お客様/MSP は、ソフォスが第三者による翻訳の正確性、完全性、信頼性について責任を負わないこと、およびソフォスが言語サポートに起因する問題について責任を負わないことを認識し、これに同意するものとします。

2. MDR Plus サービスティアのみに適用される追加の適用範囲と特典

2.1 インシデント対応。

インシデント対応はリモートで行われ、Sophos XDR を実行している監視対象エンドポイントに影響を与えるインシデントにのみ適用されます。お客様/MSP は、ソフォスからの修復ガイダンスに基づき、その他のすべてのシステムにおける封じ込め、駆除、および復旧について引き続き責任を負います。第 2.1 条に基づく調査活動および是正ガイダンスは、利用可能なテレメトリおよびサービス機能によってサポートされている統合システムおよびその他のお客様/MSP システムにも適用される場合があります。ただし、該当する統合システムが、インシデント発生前にソフォスのドキュメントに従って Sophos Central にテレメトリを送信するように構成されていることが条件となります。

インシデント対応には、以下に説明する活動と支援が含まれます。

2.1.1 インシデント対応の開始。

ソフォスは、独自の裁量により、観測または報告された活動が確定インシデントに該当することを確認した後、インシデント対応を開始します。潜在的なインシデントは、検出、統合システム、お客様/MSP レポート、脅威インテリジェンス、脅威ハンティング、またはソフォスの内部分析を通じ

て特定される可能性があり、そのような活動は、インシデント対応を開始する前に、トリアージと重大度分類の対象となります。明確にするために、お客様/MSP からの疑わしい活動に関する報告は調査のきっかけとなる可能性はありますが、それ自体がインシデント対応の引き金となるわけではありません。

インシデント対応の開始を促す可能性のある状況には、以下のようなものが含まれますが、これらに限定されません。

- 監視対象エンドポイントにおける攻撃者による対話型アクティビティ
- 特権またはアクセスを可能にする認証情報の侵害が確認されました
- 不正アクセスまたはデータ漏洩データ
- 監視対象エンドポイントの暗号化、破壊、または重大な妨害

活動の重大度は、ソフォスが入手可能な証拠を総合的に評価して決定するものであり、単一の指標や条件だけで判断されるものではありません。ソフォスは、活動の重大度に関する専門的な評価に基づき、あらゆる活動に対するインシデント対応を開始するか否かを単独で決定する権利を有します。

2.1.2 インシデント対応の範囲

インシデント対応において、以下の活動が対象となります。

a.インシデント対応アドバイザー。インシデント対応が開始されると、ソフォスはインシデント期間中、インシデント対応アドバイザーを割り当てます。

i. **割り当て:** ソフォスは、インシデント発生中、アドバイザーの継続性を維持するために合理的な努力を払いますが、アドバイザーの対応時間や運用上の要件に基づいてアドバイザーを再割り当てする場合があります。
ii. **対応時間:** アドバイザーは通常の営業時間内であれば対応可能です。上記時間外は、ソフォスの担当者がサポートいたします。 ソフォスは、アドバイザーの個別の対応状況に関わらず、すべてのアクティブなインシデントに対して 24 時間 365 日体制で対応します。
iii. **対応範囲:** アドバイザーは、調整とコミュニケーションのサポートのみを提供し、インシデントのライフサイクル全体を管理したり、利害関係者の調整、アクションの優先順位付け、部門横断的な連携など、お客様/MSP の対応活動の運用上の制御を引き受けることはありません。

b.トリアージと調査

i. 事案の重大度、範囲、影響、および優先順位を特定するために、トリアージと調査を実施し、封じ込めを支援します。
ii. 検出結果、テレメトリ、および関連データソースを分析し、悪意のある活動の性質と範囲、使用された手法、および関連する要因を特定します。
iii. 可能な場合は、インシデントのタイムラインを作成します。

c.封じ込めと脅威への対応

i. ソフォスが合理的に判断した、サポートされている対応アクションを実行し、悪意のある活動を封じ込め、軽減し、妨害し、または無力化します。
ii. お客様または MSP の関与が必要なアクション、あるいはソフォスでは実行できないアクションについて、修復ガイダンスを提供します。
iii. さらなる悪意のある活動のリスクを軽減し、再発を防止するための推奨事項を提示します。

d.コミュニケーションとコラボレーション

i. Sophos Central を通じて、ケースに関する連絡、ステータス更新、および追跡情報を提供します。
ii. お客様/MSP からの要請に基づき、発生中のインシデント期間中に、リソースの可用性に応じて会議をスケジュールします。

e.インシデント解決

i. ソフォスは、悪意のある活動が封じ込められた、軽減された、または無力化された、あるいはそれ以上のインシデント対応活動が不要であるとの評価に基づいて、インシデントがクローズされたと判断します。案件が終了すると、インシデント対応アドバイザーの任務は終了し、本サービス提供は第 1 条で説明されている標準的なサービス活動（24 時間 365 日の監視、調査、脅威対応など）に戻ります。

f.インシデント発生後のサポート

i. 既存の優先調査の中で、活動の性質と範囲、使用された手法、関連する要因、および再発防止のための推奨事項を記述したインシデント概要を提出します。
ii. インシデント解決後、Sophos Central の設定、ポリシー、保護状況を確認する健全性評価を実施し、再発防止のための修復ガイダンスを提供します。

2.1.3 第三者への引き渡し。

お客様/MSP が第三者のデジタルフォレンジックおよびインシデント対応会社を利用することを選択した場合、またはインシデント対応に関してソフォス、お客様/MSP、および当該第三者の間で三者間契約が締結されている場合（それぞれ**「第三者対応事業者」**）、お客様/MSP は、影響を受けるインシデントに対するインシデント対応活動をソフォスが第三者対応事業者に移行するよう、書面（電子メールを含む）で要求することができます。ソフォスは、円滑な移行を促進するために合理的に協力し、移行時点までにソフォスが収集した関連する調査結果、状況の更新、および成果物を

提供します。これらの調査結果および証拠はすべて、ソフォスのテレメトリに基づいて入手可能な範囲で提供されるものであり、完全なフォレンジック記録を構成するものではありません。お客様/MSP は、移行を円滑に進めるために合理的な協力を行う必要があり、これには第三者対応事業者の要件の適時な伝達、必要なアクセスや情報共有の調整などが含まれます。ソフォスは、お客様/MSP の要請に応じて移行に関する協議に参加する場合がありますが、第三者対応事業者とのエンゲージメントの調整、スケジュール調整、管理については責任を負いません。

移行後、ソフォスは影響を受けるインシデントに対するインシデント対応活動を終了し、担当のインシデント対応アドバイザーをリリースします。第 1 条に基づく標準サービスの提供は、引き続き影響を受けずに継続されます。

お客様/MSP からの書面による要請に基づき、ソフォスは関連するソフォステレメトリデータおよび調査結果を第三者対応事業者と共有する場合があります。

当該インシデントに対するインシデント対応活動の再開は、ソフォスの裁量に委ねられます。

2.1.4 除外事項。

第 2.1.2 条で明示的に言及されていない活動は、インシデント対応の範囲外であり、これには以下が含まれますが、これらに限定されません。

- 正式な法的保管記録文書または法廷で認められる証拠の作成
- 復号サービス
- ダークウェブ監視
- システムの復元または復旧
- ディスクレベルのフォレンジックイメージングまたは分析
- 電子情報開示または訴訟支援
- ランサムウェア交渉
- オンサイトサービス
- 規制、コンプライアンス、または違反通知に関するガイダンス

インシデント対応は、インシデント発生時に第 2.1 条に規定された要件を満たしていなかったお客様/MSP の資産には適用されません。インシデント対応は、侵入テスト、レッドチーム演習、敵対者シミュレーション演習、または同様のテスト活動には適用されません。

2.2 サービスレベル契約（「**SLA**」）。本条に定める SLA は、MDR Plus サブスクリプションを購入したお客様、または MSP の場合は個々の MSP 受益者にのみ適用されます。明確にするために、SLA はお客様ごと、または受益者ごとに適用され、MSP アカウント全体には適用されません。

a.定義。本サービスレベル契約には、以下の定義済み用語が適用されます。
「優先調査」とは、第 I 章に定める意味を有します。
「対応時間」とは、ソフォスが優先調査を特定してから、以下のいずれか早い時点までの経過時間を意味します。(i) ソフォスが合意された通信チャネルを通じて該当するお客様/MSP に通知するた

めの連絡を開始した時点、または(ii) お客様/MSP が脅威対応モードの承認を選択した場合にソフォスが対応アクションを開始した時点。

b.本サービスへの取り組み。対応時間は、以下の開始日から毎月測定される優先調査の 90% に対して 60 分以内となります。(i) 新規お客様または受益者 (MSP 経由) のサービス購入日から 60 日後、または (ii) 既存のお客様または受益者 (MSP 経由) のサービスサブスクリプション更新日の初日。ソフォスが、過去 12 ヶ月間のいずれかの期間において、前述の月間応答時間に関する約束を 3 ヶ月以上満たせなかった場合、ソフォスは SLA を履行しなかったものとみなされます。

c.サービスクレジット。 上記のとおり、ソフォス が対象となるお客様または受益者に対する SLA を履行できなかった場合、該当するお客様または MSP (影響を受ける受益者の代理として) は、以下のいずれか少ない方の金額に相当するサービス クレジットを受け取る資格があります。(i) 前回の請求期間中に本サービスに対して支払われた料金の 5%、または (ii) 5,000 ドル (5,000 USD) (**「サービスクレジット」**)。サービスクレジットは、次回の本サービス利用期間の料金に充当されます。MSP（マネージドサービスプロバイダー）の場合、サービスクレジットは、影響を受ける受益者に関連付けられた MSP アカウントにのみ発行されます。ソフォスは、受益者に対して直接支払いまたはクレジットを発行する義務を負わず、受益者のアカウントに対するあらゆる下流調整については、MSP が単独で責任を負います。該当するサブスクリプションが前払い期間終了後に失効した場合、獲得したサービスクレジットはすべて失効します。

d.サービス料金の返金請求手続きお客様/MSP は、サービスクレジットを受け取る資格を得た日から 30 暦日以内に、書面でサービスクレジットを申請し、件名に「MDR サービスクレジット」と記載して SLACreditClaims@sophos.com にその申請書を提出する必要があります。申請には、関連するログまたはレポートデータからの証拠を添付する必要があります。お客様/MSP は、暦年ごとに 3 回までサービスクレジットを請求できます。すべてのサービスクレジット申請は、ソフォスによる検証の対象となります。

e.除外事項。ソフォスは、第 IV 章および第 V 章に規定された条件により、SLA の全部または一部を満たす責任を負わないものとします。

2.3 侵害防止保証。この保証は、 www.sophos.com/ legal に記載されている条件に従って提供されます。

IV.お客様/MSP の責任

いずれのサービスレベルにおいても、お客様/MSP は、本サービス仕様書の第 III 章第 1.1 条およびその他の箇所でお客様/MSP に求められる措置に加えて、本サービスの提供を円滑化および可能にするために以下の措置を講じる必要があることを認識し、これに同意するものとします。また、お客様/MSP がこれらの措置を講じなかったことに起因する、本サービス提供の劣化、不完全、または失敗について、ソフォスは一切の責任を負わないものとします。ソフォスは、お客様/MSP が必要な措置を講じるまで、本サービスの提供を一時停止する権利を留保します。ソフォスからの書面による通知（ソフォスからお客様/MSP 指定の担当者への電子メール通知を含む）後、必要な措置を完了しなかった場合、お客様/MSP は本契約の重大な違反とみなされます。

1. **オンボーディング**：お客様/MSP は、必要なオンボーディング活動を完了します。
2. **インストールおよび統合要件**：お客様/MSP/受益者は以下を満たす必要があります。
   a. 有効な Sophos Central アカウントを所有していること。
   b. 監視対象エンドポイントに該当するサービスソフトウェアをデプロイおよび構成する。
   c. エージェントレスサードパーティエンドポイントを設定する。
   d. 必要な統合システムを構成して、該当するテレメトリを互換性のある形式で Sophos Central に送信するようにします。
   e. 該当する場合は健康診断の要件を遵守する（第 III 条第 1.3 項に記載）。
   f. Sophos ソフトウェアのサポート対象バージョン、およびサポート対象のサードパーティツールと統合機能のみを実行する。
3. **必要最低限の配備数：**お客様/MSP は、サービスソフトウェアがライセンス容量の少なくとも 80%に展開されなければならないことを認識し、これに同意するものとします。これは、ソフォスが本サービス提供のためにお客様/MSP の環境を十分に把握するために必要な措置です。

4. **既知の脅威の修復**：お客様/MSP は、ソフォスまたはお客様/MSP/受益者が使用するその他の第三者技術によって報告された侵害をタイムリーに修復するために、合理的な努力を払う必要があります。ソフォスは、お客様または MSP が適切な時期に是正措置を講じなかったことに起因するいかなる問題についても責任を負いません。さらに、ソフォスは、ソフォスが既に推奨される是正措置に関するガイダンスを提供済みの検出結果について、お客様/MSP に通知したり、新しいケースを生成したりする義務を負いません。
5. **時刻と日付の設定**：お客様/MSP は、対象となるすべてのエンドポイントが正確な時刻と日付設定を維持していることを確認する必要があります。
6. **お客様/MSP 担当者**：お客様/MSP は、少なくとも 1 人の主要担当者と 1 人の代替担当者を指定し、Sophos Central 内で最新の状態に維持する必要があります。各担当者は、(i)脅威対応中の対応アクションを承認し、(ii)構成またはポリシーの変更を承認し、(iii)優先度の高い調査およびインシデント中のエスカレーションポイントとして機能するための技術的およびビジネス上の知識と権限を有している必要があります。受益者にとって、MSP は受益者に代わって正式な連絡窓口として行動しなければならないものとします。
7. **サービス通知。**ソフォス は、本サービス関連の通信および通知を次のように提供します。(i) ケースおよび調査の詳細は Sophos Central を通じて提供されます。(ii) ケースおよび調査に関する通知は、お客様/MSP の指定連絡先に電子メールで送信され、受信者に追加の詳細について Sophos Central を参照するように指示する場合があります。(iii) 電話による連絡は、第 III 章第 1.4 条 (c) に記載されているとおりに開始されます。お客様/MSP は、正確かつ最新の連絡先情報を維持し、指定された連絡先が本サービスに関する連絡を受信できる状態にあることを保証する責任を負います。ソフォスは、不正確または古い連絡先情報、あるいはお客様/MSP が指定した連絡先が利用できないことに起因する通信の遅延または不履行につい

て一切責任を負いません。ソフォスからの通知または連絡は、上記のいずれかの経路を通じて配信された時点で有効となります。

8. **迅速な対応**：お客様/MSP は、ソフォスからの連絡や要求に対し、速やかに対応しなければなりません。優先調査の場合、お客様/MSP は、ソフォスからの連絡に対して 60 分以内に商業的に合理的な努力を尽くして応答することに同意し、遅延によってリスクと影響が増大する可能性があることを認識するものとします。

9. **サービス範囲外の行為**：本サービス仕様書に明示的に記載されていないすべての活動は、本サービスの範囲外となります。お客様/MSP は、以下の事項について単独で責任を負います。(i) 本サービスの範囲外のあらゆる行為（例：オンサイト対応に関するソフォスの提案、すべての訴訟および電子情報開示サポート、法執行機関との連携）を行うこと、および(ii) お客様/MSP の具体的な指示に基づいて、本サービス仕様書に記載されていないソフォスのあらゆる行為。お客様/MSP は、本サービス契約開始日以前に発生または存在したセキュリティインシデント、脅威、または侵害について、ソフォスが責任を負わないことを認識し、これに同意するものとします。さらに、お客様/MSP は、ソフォスによって解決できない統合システム内のインシデントおよび/または確認された脅威を無力化する責任を負います。

10. **ソフォス以外のシステム**：お客様/MSP は、以下の事項を認識し、同意するものとします。(i) ソフォスは、ベンダーまたは第三者によってソフォス以外のシステムに加えられた変更が統合またはソフォスの本サービス提供能力に影響を与える場合、その変更について責任を負いません。(ii) ソフォスは、サポート対象の統合を追加、削除、および変更する場合があります。お客様/MSP は、統合が正しく機能していることを確認し、テレメトリが流れていない場合や統合の設定が誤っている場合は、ソフォスに通知する必要があります。

11. **パートナーによる行動**：お客様は許可することができますｗパートナーズお客様に代わって本サービスの範囲内で特定の行動をとる場合、お客様は当該パートナーのすべての行動または不作為について責任を負う。ソフォスは、パートナーの行為または不作為について一切責任を負いません。

12. **MSP の追加責任**：MSP は、MSP が本サービスを提供する受益者が、本サービス仕様書に記載されている、または本サービスに内在するすべてのリスクを受け入れることに同意していることを確認する責任を単独で負います。MSP は、受益者からソフォスに対して提起されたいかなる請求についても、当該請求が、MSP が本サービス仕様書または本サービスに関する契約に基づく義務を完全に履行しなかったことに起因する場合、ソフォスを補償し、免責するものとします。

13. **セキュリティテストと侵入テスト**：お客様/MSP が脆弱性テスト、侵入テスト、またはその他のセキュリティテスト活動を実施する場合、お客様/MSP は、ソフォスが MDR 侵入テストポリシーで公開しているソフォスの脆弱性テストおよび侵入テストポリシーを遵守する必要があります。

V。追加条項

1. **サービス除外事項：** お客様/MSP は、ソフォス が以下の場合には責任を負わず、本サービス仕様書または本契約 (適用される SLA を含む) の違反とはみなされないことに同意し、これを承認します。(i) 業界全体またはインフラストラクチャ全体のランサムウェア、サイバー戦争、またはその他のサイバー攻撃の結果として、ソフォス がインシデントにタイムリーに対処するためのリソースを提供できないために、本契約に基づく義務の履行が遅延または不履行になった場合。(ii) 戦争、ストライキ、暴動、犯罪、天災、またはリソース不足など、予見できない状況または ソフォス の合理的な制御を超える原因による場合。(iii) 法令、政令、規則、または命令の制定など、法的禁止による場合。(iv) 契約の条件に従って ソフォス が本サービスを一時停止している期間中。(v) お客様/MSP が契約に違反している場合 (お客様に未払いの請求書がある場合を含むがこれに限定されない)。(vi) 予定されているメンテナンス期間中。
2. **サービス機能：**お客様/MSP は、ソフォスが本サービスの一部として商業的に合理的な技術とプロセスを実装しているものの、ソフォスは本サービスがすべての脅威やインシデントを検出、防止、封じ込め、無力化、または軽減することを保証するものではないことを同意し、認識するものとします。お客様/MSP は、ソフォスがそのような保証または保証書を提供したと誰に対しても表明しないことに同意します。