SOPHOS

緊急インシデント対応 – サービス仕様書

本サービス仕様書は、ソフォスの緊急インシデント対応サービスを説明しており、次のサービス（個別または総称して **「サービス」**と呼びます）を含みます。

- **エンゲージメント管理**
- **インシデント対応**
- **デジタルフォレンジック**
- **ビジネスメール詐欺**
- **コンプロマイズ評価**
- **脅威ハンティング**
- **脅威インテリジェンスおよびリサーチ**
- **身代金交渉**
- **エンゲージメントレポート**
- **サービスソフトウェア展開**

本サービス仕様書におけるすべての太字の用語は、下記の規約（以下で定義）または以下の定義セクションで与えられた意味を持ちます。

本サービス仕様書は、適用される場合、次のものの一部として、組み込まれています。

(i) お客様またはマネージドサービスプロバイダー（**“MSP”**）がソフォスとの間でサービスの購入をカバーする手動またはデジタル署名された規約

(ii) MSPがソフォスとの間でサービスの一部であるオファリングの購入をカバーする手動またはデジタル署名された規約

(iii) そのような署名された規約が存在しない場合、本サービス仕様書は、https://www.sophos.com/legal に掲載されているソフォスエンドユーザー利用規約の条件に従います（総称して **“規約”**と呼ばれます）。規約の条件と本サービス仕様書の条件に矛盾がある場合、本サービス仕様書の条件が優先されます。

規約に反するいかなることにもかかわらず、お客様/MSPは次のことを認め、同意します。

（i）ソフォスは、お客様/MSPに通知することなく、サービスの全体的な機能を実質的に低下させることなく、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、提供されるサービス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ことができ、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る太字の用語で、規約で別途定義されていないものは、以下に示す意味を持ちます。

「アクティブ脅威」は、資産またはデータの感染、侵害、または無許可のアクセスを指します。

「封じ込め」または「封じ込め策」は、無力化前に、インシデント対応中に脅威の拡散と影響を制限するために取られる措置を意味します。これには、ネットワークセグメンテーション、影響を受けたエンドポイントの隔離、アカウントの一時停止、脅威アクターの操作を中断し、さらなる侵害や損害を防ぐための他の防御策が含まれる場合があります。

SOPHOS

「インシデント」とは、お客様/MSP の資産に対して差し迫った懸念または脅威をもたらすシステムの疑わしい侵害または無許可のアクセスを指し、インタラクティブな攻撃者、データの暗号化または破壊、または情報の流出を含むがこれに限定されません。

「インシデントコマンダー」は、ステークホルダーの調整、行動の優先順位付け、部門間の整合性とコミュニケーションを含む、全体的なサービスエンゲージメント・ライフサイクルを管理する責任を持つソフォスの担当者です。インシデントコマンダーは、お客様/MSPとセキュリティサービスチームとの間の主要な連絡役を務め、タイムリーで整合性のある範囲内のサービス提供を確保します。
「インシデントリード」は、サービスエンゲージメントの実行を管理する責任を持つ主要なソフォスの担当者です。インシデントリードは、フォレンジック分析、証拠収集、タイムラインの再構築、技術的な所見の開発を監督し、ソフォスの担当者の努力を調整して、調査の厳密さとサービスエンゲージメントの目的および範囲との整合性を確保します。

「インシデント対応」は、セキュリティサービスチームによって実行される技術的プロセスであり、調査、緩和、封じ込めおよび脅威の無力化を行います。

「調査」は、セキュリティサービスチームが悪意のある活動かどうかを確認し、脅威対応が必要かどうかを判断するために使用する正式なプロセスおよび方法です。

「無力化」または**「無力化措置」**は、利用可能な証拠に基づき、セキュリティサービスチームが合理的に判断して、インシデントがサービス対象エンドポイント上に存在しなくなったことを確認した時点で達成される「脅威の無力化」の状態を意味します。脅威無力化プロセスには、以下を目的として実施される調査および対応措置が含まれます。
(i) 攻撃者によるアクセスの削除
(ii)　侵害された資産またはデータへのさらなる損害の防止

“対応アクション”は、調査および脅威ハンティングを実施するために、サービス対象エンドポイントに対して行う操作をいい、これにはリモートクエリ、ホストの隔離、プロセスの終了、IP アドレスのブロック、アカウントの無効化、サンプルファイルの収集、悪意のあるアーティファクトの削除を含みますが、これに限定されません。

“サービス対象エンドポイント”は、サービス提供の範囲内にある物理的または仮想的なエンドポイントデバイスまたはサーバーシステムです。

“セキュリティサービスチーム”は、調査、脅威ハンティング、対応アクション、インシデント対応、展開など（これらに限定されません）を実施するソフォスチームを指します。

″調査対象システム″とは、インシデントの範囲および影響を理解するために関連する、あらゆるデジタルシステム、デバイス、インフラサービス、またはその他のデータを指します。

“脅威ハンティング”は、悪意のある活動の信号や指標を特定するために、手動および半自動の活動を組み合わせて、データを能動的かつ反復的に検索するプロセスです。

“脅威対応”とは、悪意のある活動を封じ込めまたは妨害するために、セキュリティサービスチームおよびお客様/MSP が適宜実施する手法、プロセス、コミュニケーションならびに対応アクションを指します。

SOPHOS

注意:

- ソフォス Intercept X Advanced with XDR は、以下「ソフォス XDR」といい、ソフォス XDR Sensor は、以下「XDR センサー」といいます。
- 本サービス仕様書内でサービスソフトウェアという用語が使用される場合、文脈に応じてソフォス XDR、ソフォス NDR および/または XDR センサーを意味するものとみなされます。

II. サービスの説明

ソフォスは、本サービス仕様書に従い、お客様のサービススケジュールに定められたサービスを提供します。お客様/MSP が下記第 III 条に基づくオンサイトサービスを要請しない限り、すべてのサービスはリモートで提供されます。
サービス提供は、お客様/MSP とのキックオフコールをもって開始されます。

a) お客様/MSP/受益者のインフラに関する情報を取得する
b) サービス対応における初期目標、作業範囲および優先事項について合意する
c) お客様/MSP 側の主要な関係者およびサービス提供におけるそれぞれの役割を特定する
d) お客様/MSP とのコミュニケーションの頻度および希望する連絡方法を確立する

MSP は、MSP の受益者に提供されるあらゆるサービスの連絡窓口として対応しなければならない。

1 エンゲージメント管理

1.1 本サービスの対応項目

エンゲージメント管理には、以下のいずれかが含まれます。

- インシデントリードの割り当て、およびお客様/MSP の要請に応じたサービス提供の調整を監督するインシデントコマンダーの割り当て
- お客様/MSP の優先事項および利用可能なリソースに沿った、本サービス活動の計画およびスケジュール調整
- 進捗状況、リスク、課題（阻害要因）および主要なマイルストーンに関する定期的なステータス報告
- 本サービスの対象範囲（スコープ）、調査結果、実施した対応措置およびサービス結果に関する文書を維持・管理（必要に応じて、共有アーティファクトのトラッキング文書の更新を含む）
- フォレンジック調査、対応、交渉、およびお客様の利害関係者を含む技術系・非技術系の各ワークストリーム間の調整を行い、適切な連携および整合性を確保
- エンゲージメント期間中におけるエスカレーション管理および本サービスに関する問い合わせ対応の中央窓口として機能すること

1.2 本サービスの対象外事項

上記に明示的に定められていない活動および以下の活動は、本サービスの対象範囲外となります。

- 法務機能、規制対応機能、または経営機能の正式な代行者として行動すること

SOPHOS

1.3 お客様/MSP の義務

お客様/MSP は、本サービスの提供を円滑にし、かつ可能にするために、以下の措置を講じなければならないものとします。お客様/MSP が必要な措置を講じなかったことに起因して、本サービスの提供品質の低下、不完全なサービス提供、またはサービス提供の失敗が生じた場合、ソフォスは一切の責任を負わないものとします。

- 対応アクションを含む本サービスの提供に関してソフォスを支援するため、最大 3 名のお客様/MSP 担当者を指名すること
- 予定されたステータスおよび調整の電話会議に参加すること
- 文書、推奨事項、および割り当てられたタスクについて、適時に確認し、対応すること
- 部門横断的な調整を支援するため、関連する事業部門および技術部門の関係者が参加できるようにすること

2 インシデントレスポンス

2.1 本サービスの対応項目

インシデントレスポンスには、以下のいずれかが含まれます。

- インシデントに関する技術的分析を実施し、調査対象システム、攻撃経路（Attack Vectors）、永続化メカニズム、および脅威アクターの行動の特定
- 調査結果に基づき、封じ込めおよび脅威の無力化の戦略の策定、および推奨
- 現在の環境における有効性の検証のため、サービスソフトウェアの構成設定およびテレメトリのレビュー
- 必要に応じた、調査結果を検証するための攻撃的検証活動（Offensive Operations）の実施（これには、ペネトレーションテスト、脆弱性スキャン、および Active Directory 評価が含まれるが、これらに限定されない）
- アクティブな脅威または進行中の悪意ある活動が検出された場合、お客様/MSP の要請に基づき、当該アクティブな脅威を封じ込めまたは無力化するための適切な対応措置を講じる（これには、システムの隔離、侵害指標（Indicators）のブロック、および悪意のあるプロセスの終了が含まれるが、これらに限定されない）
- インシデントの性質に基づき、システム強化、復旧・是正措置、および再発防止に関する技術的な推奨事項の提供
- インシデントレスポンス活動、対応結果および調査結果に関する書面または口頭による報告

2.2 本サービスの対象外事項

上記に明示的に定められていない活動および以下の活動は、本サービスの対象範囲外となります。

- 調整業務、プロジェクトの進捗管理、エスカレーション対応等のエンゲージメント管理業務（これらはエンゲージメント管理サービスにおいて提供されるものとします）。

2.3 お客様/MSP の義務

お客様/MSP は、本サービスの提供を円滑にし、かつ可能にするために、以下の措置を講じなければならないものとします。お客様/MSP が必要な措置を講じなかったことに起因して、本サービスの提供品質の低下、不

完全なサービス提供、またはサービス提供の失敗が生じた場合、ソフォスは一切の責任を負わないものとします。

- サービス対象エンドポイントにサービスソフトウェアを展開し、調査対象システムへのアクセスを提供
- 対応アクションを含む本サービスの提供に関してソフォスを支援するため、最大 3 名のお客様/MSP 担当者を指名すること
- Sophos がお客様/MSP に対して指定したすべての対応事項について、遅滞なく実施すること
- 双方で合意したすべての会議通話に参加すること

3 デジタルフォレンジックス

3.1 本サービスの対応項目

デジタルフォレンジックスには、以下のいずれかが含まれます。

- 必要に応じて、サービス対象エンドポイントおよび/または調査対象システムから、インシデントに関連するデジタル証拠を収集すること
- 調査の一環として、収集した証拠をフォレンジックツールおよびフォレンジック手法を用いて分析し、侵害の指標（Indicators of Compromise：IOC）を特定するとともに、攻撃者の活動を追跡すること
- 現在または過去の脅威に関する適用可能なテレメトリデータを確認すること
- 調査およびフォレンジック分析の過程で特定された疑わしいマルウェアについて、静的解析および/または動的解析を実施すること
- 証拠分析によって特定された主要な事象の時系列および、調査中に特定された IOC の一覧を含む書面または口頭による報告を提供すること

3.2 本サービスの対象外事項

上記に明示的に定められていない活動および以下の活動は、本サービスの対象範囲外となります。

- 法的な証拠保全手続に必要な正式なチェーン・オブ・カストディ（Chain of Custody）文書、または法廷で証拠能力を有する証拠資料を作成すること
- 別途書面による明示的な合意がある場合を除き、高度なマルウェア解析（逆アセンブル、リバースエンジニアリングまたはエクスプロイト開発分析を含む）を実施すること
- 収集したフォレンジックデータの長期的な保管、管理またはアーカイブサービスを提供すること

3.3 お客様/MSP の義務

お客様/MSP は、本サービスの提供を円滑にし、かつ可能にするために、以下の措置を講じなければならないものとします。お客様/MSP が必要な措置を講じなかったことに起因して、本サービスの提供品質の低下、不完全なサービス提供、またはサービス提供の失敗が生じた場合、ソフォスは一切の責任を負わないものとします。

- ソフォスに対し、調査対象システムに係る管理者権限、ログデータおよびフォレンジックデータへのアクセスを提供すること
- 必要に応じて、サービス対象エンドポイントへサービスソフトウェアを導入すること

- 対象システムからのデジタル証拠収集を含む本サービスの提供に関してソフォスを支援するため、最大 3 名のお客様/MSP 担当者を指定すること
- 双方が合意したすべての電話会議に参加すること
- ソフォスが指定したすべての対応事項について、遅滞なく実施すること

4 侵害評価

4.1 本サービスの対応項目

侵害評価には、以下のいずれかが含まれます。

- お客様/MSP と連携し、潜在的な脅威に関する情報を収集するとともに、お客様/MSP が本サービスの対象とすることを希望するサービス対象エンドポイントを特定すること
- サービスソフトウェアがインストールされているサービスエンドポイント、またはお客様/MSP が Sophos に提供した関連データに基づき、侵害の兆候（Indicators of Compromise：IOC）の有無を調査すること
- アクティブな脅威が特定された場合、お客様/MSP に通知し、調査結果を提供するとともに、さらなる調査および封じ込めのための推奨策を提示すること
- 本サービスの対象範囲内において侵害の証拠が確認されなかった場合、分析対象データセットに IOC が存在しなかったこと、および使用した調査手法を記載した書面による通知をお客様/MSP に提供すること
- 実施した脅威ハンティングの活動内容、結果、および推奨事項をまとめた書面によるサマリーを提供すること

4.2 本サービスの対象外事項

上記に明示的に定められていない活動および以下の活動は、本サービスの対象範囲外となります。

- 脅威の発見に基づいて修正を実施、およびシステムをパッチ適用すること

4.3 お客様/MSP の義務

お客様/MSP は、本サービスの提供を円滑にし、かつ可能にするために、以下の措置を講じなければならないものとします。お客様/MSP が必要な措置を講じなかったことに起因して、本サービスの提供品質の低下、不完全なサービス提供、またはサービス提供の失敗が生じた場合、ソフォスは一切の責任を負わないものとします。

- サービス対象エンドポイントにサービスソフトウェアを導入すること
- サービス提供を支援する担当者として、最大 3 名までのお客様/MSP 指定担当者を任命すること
- ソフォスから要請されたデータを遅延なく提供すること
- 合意したすべての電話会議またはオンライン会議に参加すること

5 脅威インテリジェンスとリサーチ

5.1 本サービスの対応項目

脅威インテリジェンスとリサーチには、以下のいずれかが含まれます。

- お客様/MSP から提出された IOC データについて、脅威の背景情報、関連性、潜在的な帰属先、ならびに既知の脅威アクターまたは攻撃キャンペーンに関連する戦術、技術および手順（TTPs）を含む、高レベルの分析的エンリッチメントを提供すること
- お客様/MSPから提供されたハッシュ値、URL、IPアドレス等のデータについて、オープンソースおよびダークウェブ上での調査を実施し、主要な調査結果をお客様/MSP へ報告すること
- 侵害事案との関連が疑われるお客様/MSP のデータについて、オープンソース・インテリジェンス（OSINT）調査を実施すること
- 必要に応じて、悪意のあるファイルまたはアーティファクトのリバースエンジニアリングを実施し、その挙動特性および IOC を抽出するとともに、脅威アクターの特定（アトリビューション）およびコンテキスト分析を支援すること
- 調査結果および推奨事項について、書面または口頭によるサマリーを提供すること

5.2 本サービスの対象外事項

上記に明示的に定められていない活動および以下の活動は、本サービスの対象範囲外となります。

- 現在進行中のインシデントに関連する封じ込め、無力化、または復旧活動。
- **確定的な結論および脅威の帰属の保証**

  お客様/MSP は、ソフォスが提供するすべての調査結果および分析が、評価時点で入手可能な情報および脅威インテリジェンスに基づくものであることを認識し、これに同意するものとします。また、かかる調査結果および分析は最終的または決定的なものではなく、「現状のまま」で提供されるものであり、ソフォスはそれらに関していかなる表明、保証、または確約も行わないものとします。

5.3 お客様/MSP の義務

お客様/MSP は、本サービスの提供を円滑にし、かつ可能にするために、以下の措置を講じなければならないものとします。お客様/MSP が必要な措置を講じなかったことに起因して、本サービスの提供品質の低下、不完全なサービス提供、またはサービス提供の失敗が生じた場合、ソフォスは一切の責任を負わないものとします。

- 脅威インテリジェンスとリサーチ活動の実施に必要となる、関連性があり正確なデータまたは成果物（アーティファクト）をすべて提供すること。
- サービス提供を支援する担当者として、最大 3 名までのお客様/MSP 指定担当者を任命すること
- ソフォスに共有する機密情報または専有情報については、本サービスの範囲内で利用するために必要な権限が適切に付与されていることを確認し、適用されるすべての法令および秘密保持契約を遵守したうえで提供すること
- 合意されたすべての会議（電話会議を含む）に参加すること

6 脅威ハント

6.1 本サービスの対応項目

脅威ハントサービスには、以下のいずれかが含まれます。

- サービス対象エンドポイント上の IOC の調査を行うか、お客様/MSP からソフォスに提供された関連データに基づく調査を実施するため、サービス対象エンドポイント上で本サービスソフトウェアを最大 30 日間利用すること
- 証拠分析によって特定された主要なイベントのタイムライン、調査中に特定された IOC の一覧、および使用した調査手法を含む書面または口頭によるサマリーを提供すること
- 調査結果に基づく概要レベルの推奨事項を提供すること
- 本サービスの対象範囲内において侵害の痕跡が確認されなかった場合は、分析対象データセットに IOC が存在しなかったこと、および実施した分析手法を記載した書面による通知をお客様/MSP に提供すること

6.2 本サービスの対象外事項

上記に明示的に定められていない活動および以下の活動は、本サービスの対象範囲外となります。

- 脅威の発見に基づいて修正を実施したり、システムをパッチ適用したりすること

6.3 お客様/MSP の義務

お客様/MSP は、本サービスの提供を円滑にし、かつ可能にするために、以下の措置を講じなければならないものとします。お客様/MSP が必要な措置を講じなかったことに起因して、本サービスの提供品質の低下、不完全なサービス提供、またはサービス提供の失敗が生じた場合、ソフォスは一切の責任を負わないものとします。

- サービス対象エンドポイントにサービスソフトウェアを展開すること
- サービス提供を支援する担当者として、最大 3 名までのお客様/MSP 指定担当者を任命すること
- ソフォスから要請されたデータを遅延なく提供すること
- 合意したすべての電話会議またはオンライン会議に参加すること

7 身代金交渉

7.1 本サービスの対応項目

ランサムウェア交渉支援には、以下のいずれかが含まれます。

- ランサムウェア事件に関連する情報（身代金要求メモ、脅威アクターとの通信、影響を受けたシステムを含む）を収集するために、セキュリティサービスチームとお客様/MSP との間で電話会議を実施する
- 既知の TTP および過去の活動に基づいて、脅威アクターの行動とプロファイルを評価する
- 推奨するコミュニケーションのトーン、交渉の進め方（ペース）、および応答内容を含む、潜在的な交渉戦略に関する助言を提供する
- お客様/MSP と協力して交渉の目的を定義する
- 身代金要求に関する協議を円滑に進めるため、脅威アクターとの交渉を実施する（すべての交渉活動は、お客様/MSP のフィードバックおよび指示に厳格に従って実施される）
- 交渉プロセス全体を通じて お客様/MSP に定期的な状況報告を行い、脅威アクターとの通信内容の要約および推奨される次の対応策を提供する
- 必要に応じて、身代金の支払い手続きを専門とする第三者サービスプロバイダーを紹介または推奨する。お客様/MSP は以下を認識し、これに同意するものとする

SOPHOS

(i) 当該第三者サービスプロバイダーの利用はお客様/MSP の単独の裁量によるものであり、お客様/MSP 自らのデューデリジェンス、法務レビュー、および制裁規制やマネーロンダリング防止規制を含む適用法令への適合確認を条件とすること

(ii) Sophos は当該第三者サービスプロバイダーのサービスを管理、保証、推奨するものではなく、またそのサービスに関していかなる責任も負わないこと

- 交渉活動の概要、観察された脅威アクターの行動、および交渉結果をまとめた書面による報告書を提供する

7.2 本サービスの対象外事項

上記に明示的に定められていない活動および以下の活動は、本サービスの対象範囲外となります。

- 制裁規制、輸出管理規制、マネーロンダリング防止（AML）要件を含む、法的または規制上の助言を提供すること
- お客様/MSP の代わりに身代金の支払いを促進、立て替え、または実施すること
- 暗号化されたデータの復号および／または復旧を支援すること
- 身代金支払い後のデータ復元や、継続的な連絡・交渉への応答を含め、脅威アクターの行動または履行について保証すること

7.3 お客様/MSP の義務

お客様/MSP は、本サービスの提供を円滑にし、かつ可能にするために、以下の措置を講じなければならないものとします。お客様/MSP が必要な措置を講じなかったことに起因して、本サービスの提供品質の低下、不完全なサービス提供、またはサービス提供の失敗が生じた場合、ソフォスは一切の責任を負わないものとします。

- ランサムウェア交渉戦略および身代金支払いに関する意思決定権限を有し、かつ本サービスの提供を支援するためのお客様/MSP 担当者を最大 3 名まで指名すること
- 利用可能なすべての脅威アクターとの通信記録および身代金要求文書（ランサムノート）へのアクセスを、完全かつ適時に提供すること
- サービス提供中におけるソフォスからの問い合わせや推奨事項に対し、速やかに対応すること
- 合意されたすべてのカンファレンスコールに参加すること

リスクの承認および補償（Risk Acknowledgment and Indemnification）

- お客様/MSP は、犯罪的な脅威アクターとの通信または交渉には、本質的なリスクが伴うことを認識し、これを承諾するものとします。これには、履行不能、恐喝行為の継続、データの破壊、評判の毀損、ならびに法的・規制上のリスクへの曝露が含まれますが、これらに限定されません。
- また、お客様/MSP は、ソフォスが当該脅威アクターの行動または結果を管理できる立場にはなく、データの復元や悪意のある活動の停止を含め、交渉プロセスから生じるいかなる結果についても保証しないことを理解し、これに同意するものとします。
- さらに お客様/MSP は、身代金支払いまたは交渉戦略に関連してお客様/MSP が行った判断または行為に起因または関連して発生する一切の請求、責任、損失、損害、費用または支出（合理的な弁護士費用を含む）について、ソフォス、その関連会社、およびそれらの取締役、役員、従業員ならびに代理人を補償し、防御し、一切の責任を負わせないものとします。これには、適用される法令、規制、制裁措置への違反または不遵守に起因するものが含まれますが、これに限定されません。

SOPHOS

8 エンゲージメントレポート

8.1 本サービスの対応項目

エンゲージメントレポートサポートには、以下のいずれかが含まれます。

- 経営層および非技術系ステークホルダー向けに作成したインシデントのエグゼクティブサマリー
- インシデント期間中における脅威アクターの主要な活動および行動を時系列で可視化したグラフィカルなタイムライン
- 調査で確認された脅威アクターの TTP に関する詳細な分析結果、ならびに MITRE ATT&CK フレームワークへのマッピングおよび関連する推奨緩和策
- 調査により特定された IOC の包括的な一覧
- 調査結果に基づく概要レベルのセキュリティ推奨事項および改善提言

8.2 本サービスの対象外事項

上記に明示的に定められていない活動および以下の活動は、本サービスの対象範囲外となります。

- 法的助言、法的見解、または法的推奨事項の提供
- コンプライアンスに関する助言または規制上の評価の提供
- **脅威アクターの帰属（アトリビューション）に関する確定的な判断または保証**

  お客様/MSP は、Sophos が提供するすべての調査結果および分析が、評価時点で入手可能な情報および脅威インテリジェンスに基づくものであり、確定的なものではないことを認識し、これに同意するものとします。これらの結果および分析は「現状のまま」で提供されるものであり、ソフォスはその内容についていかなる表明、保証または結果の保証も行いません。

8.3 お客様/MSP の義務

お客様/MSP は、本サービスの提供を円滑にし、かつ可能にするために、以下の措置を講じなければならないものとします。お客様/MSP が必要な措置を講じなかったことに起因して、本サービスの提供品質の低下、不完全なサービス提供、またはサービス提供の失敗が生じた場合、ソフォスは一切の責任を負わないものとします。

- エンゲージメントレポートを安全に提供できる有効な電子メールアドレス、またはセキュアなファイル共有プラットフォームへのアクセスを提供すること
- エンゲージメントレポートの受領および関連する質問や確認事項への対応を含め、本サービスの提供を支援する お客様/MSP 担当者を最大 3 名まで指名すること
- エンゲージメントレポートのレビューおよび関連する協議に参加する適切なステークホルダーを特定し、エンゲージメントレポートの口頭説明が要求された場合には、その参加を確保すること
- レポート受領後 5 営業日以内に、適時にフィードバックを提供し、またはフォローアップの質問を行うこと。当初の時間制サービス契約の範囲内で説明や修正対応を行うため、この期間内に対応を行うものとする。当該期間経過後に行われる追加対応の要請については、追加のサービス時間の購入が必要となる。
- 合意されたすべてのカンファレンスコールに参加すること

SOPHOS

9 ビジネスメール詐欺

9.1 本サービスの対応項目

ビジネスメール詐欺（BEC）に関するサービスには、以下のいずれかまたは複数が含まれます。

- セキュリティサービスチームとお客様/MSP との間で電話会議を行い、メール環境および不正なメールアカウントアクセスの疑い（「ビジネスメール詐欺（Business Email Compromise、BEC）」）に関する情報を収集する
- BEC の影響範囲および被害状況を調査し、サービス提供中を通じて主要な調査結果をお客様/MSP に報告する
- BEC が確認された場合、原因、侵害経路（攻撃ベクトル）、永続化メカニズム、および脅威アクターが使用した手法ならびに主要な調査結果を共有すること
- BEC の調査結果の書面または口頭による要約を提供すること

9.2 本サービスの対象外事項

上記に明示的に定められていない活動および以下の活動は、本サービスの対象範囲外となります。

- お客様/MSP のメール環境を設定または構築すること

9.3 お客様/MSP の義務

お客様/MSP は、本サービスの提供を円滑にし、かつ可能にするために、以下の措置を講じなければならないものとします。お客様/MSP が必要な措置を講じなかったことに起因して、本サービスの提供品質の低下、不完全なサービス提供、またはサービス提供の失敗が生じた場合、ソフォスは一切の責任を負わないものとします。

- 本サービスの提供に必要な範囲で、メール環境への必要かつ適切なアクセス権限をソフォスに提供すること
- 本サービスの提供を支援するお客様/MSP 担当者を最大 3 名まで指名すること
- 合意されたすべての電話会議に参加すること

10 サービスソフトウェアの展開

10.1 本サービスの対応項目

サービスソフトウェア展開サービスには、以下のいずれかまたは複数が含まれます。

- お客様/MSP に対して、専任のセキュリティサービスチームを割り当てる
- お客様/MSP と電話会議を実施し、本サービスの対象としてお客様/MSP が指定するサービス対象エンドポイントを特定する
- お客様/MSP が指定したサービス対象エンドポイントにサービスソフトウェアをインストールおよび展開する
- キックオフコールにおいて確立された連絡手段を通じて、ソフォスの導入エンジニアへの 24 時間 365 日のアクセスを通じて、お客様/MSP にサポートおよびガイダンスを提供する

- サービス対象エンドポイントにおけるサービスソフトウェアのインストール状況に関する書面によるサマリーを提供する

10.2 本サービスの対象外事項

上記に明示的に定められていない活動および以下の活動は、本サービスの対象範囲外となります。

- 非ソフォス製品およびサービスの構成および/またはトラブルシューティング
- お客様/MSP デバイスの OS アップグレード、パッチ適用、および復元
- お客様/MSP デバイスのブート問題のトラブルシューティング

10.3 お客様/MSP の義務

お客様/MSP は、本サービスの提供を円滑にし、かつ可能にするために、以下の措置を講じなければならないものとします。お客様/MSP が必要な措置を講じなかったことに起因して、本サービスの提供品質の低下、不完全なサービス提供、またはサービス提供の失敗が生じた場合、ソフォスは一切の責任を負わないものとします。

- サービスソフトウェアを展開するためのサービス対象エンドポイントを特定し、優先順位を設定すること
- サービス提供を支援するために、最大 3 名のお客様/MSP 担当者をソフォスに割り当てること
- 管理アクセスと技術的専門知識を持つお客様/MSP の担当者を確保し、サービス対象エンドポイントへのサービスソフトウェアのインストール作業についてソフォスへ適時支援すること
- 合意されたすべての電話会議に参加すること

III. オンサイトサービス規約

お客様/MSP が上記サービスのいずれかについてオンサイトサポートを希望し、ソフォスがその要請を受諾した場合、両者はまず計画協議を実施し、オンサイトエンゲージメントの目的、範囲、必要なスキルセット、および実施期間を定義するものとします。　この協議結果に基づき、ソフォスは派遣する適切なソフォスサービスチームの要員を選定し、想定される費用および移動時間の見積書を書面で提示して、お客様/MSP による確認および承認を受けます。お客様/MSP が当該見積書を書面で承認するまで、ソフォスは移動を開始せず、また移動に関連する費用も発生させないものとします。お客様/MSP は、別途書面により両者で合意しない限り、ソフォスの担当者が現地の営業時間内（1 日あたり最大 8 時間を超えない範囲）で業務を実施することに同意するものとします。

- **コストカテゴリ**

  お客様/MSP は、以下の 3 つのコストカテゴリに対して責任を負います：

  1. **実際の費用：**これには、オンサイトエンゲージメントに関連して発生する合理的かつ必要な実費がすべて含まれます。具体的には、以下のような費用が該当します。
     - 往復航空運賃（フライトが 4 時間未満の場合はエコノミークラス、4 時間以上 8 時間以下の場合はプレミアムエコノミークラス、8 時間を超える場合はビジネスクラス）
     - 往復鉄道運賃（所要時間が 6 時間未満の場合は普通車、6 時間を超える場合はグリーン車または同等のビジネスクラス）

- 燃料費（運転する場合）
- 宿泊費
- 食費および雑費
- 地上交通費（タクシー、ライドシェアサービス、レンタカー等）
- ビザ取得費用または入国に必要な書類関連費用、および適用される税金または各種手数料

2. **移動時間:**上記の実際の費用に加えて、ソフォスはお客様/MSP の拠点への往復移動にかかる時間を請求するものとします。移動時間は、担当要員の自宅からお客様/MSP の拠点（または該当する場合は現地ホテル）までの**ドア・ツー・ドア**の移動時間として算定されます。移動時間は、お客様/MSP の該当するサービスの標準時間単価の **50%**に相当する時間単価で請求されます。移動時間に対する請求額は、該当サービスに適用される お客さま/MSP の標準時間単価の 50%に相当する時間単価で計算されます。
3. **待機時間:**お客様/MSP が、オンサイトエンゲージメントの開始に必要なアクセス権、情報、または準備状況を適時に提供できなかったことにより、ソフォスの担当者が現地で待機した時間、または対応開始を待機していた時間については、すべて請求対象となります。当該時間は、対象サービスに適用される**標準時間単価**に基づいて請求され、オンサイト対応に従事する担当者 1 名あたり **1 日最大 8 時間まで**請求されるものとします。

- **規約のキャンセルまたは延期**
  お客様/MSP が、予定された開始日より前、または移動手配が確定もしくは開始された後に、オンサイトサポートを中止または延期した場合、お客様/MSP は、すでにソフォスが負担した返金不可または回収不能な移動関連費用の全額をソフォスに支払うものとします。

お客様/MSP のオンサイトエンゲージメントに対する義務:

お客様/MSP は、本サービスの提供を円滑に実施できるよう、以下の対応を行うものとします。お客様/MSP がこれらの義務を履行しなかったことに起因して、本サービスの品質低下、不完全な提供、または提供不能が生じた場合、ソフォスは一切の責任を負わないものとします。

- オンサイトエンゲージメントに先立ち、必要な施設入館許可、物理的な入室権限、およびセキュリティクリアランスを事前に手配すること（これには、必要に応じて営業時間外のアクセス権限の手配も含まれる）
- 合意された作業範囲に含まれる関連システム、環境、インフラストラクチャコンポーネント、および関係者へのアクセスを適時に提供すること
- 本エンゲージメントを支援するためにソフォスが求める情報、文書、または意思決定に関する依頼に対し、適時に対応すること
- ソフォスが本エンゲージメント期間中に使用するツール、ソフトウェア、またはアクセス手段について、必要な承認または許可を取得し、ソフォスに提供すること
- 適切な作業スペースを確保するとともに、電源、ネットワーク接続、および必要なシステムまたはツールへの物理的またはリモートアクセスを利用可能な状態にすること

- 合意したすべての定期報告会議およびブリーフィングに参加し、また、予定されたすべての進捗報告会議、技術説明会、およびエンゲージメント完了後のレビュー会議において、指定された利害関係者が出席し、積極的に参加することを確保すること。
- オンサイトエンゲージメント期間中に安全な作業環境を確保するため、適用される安全衛生規則およびセキュリティ関連の手順や規程を遵守すること。

IV. お客様/MSP の責任

お客様/MSP は、上記第 II 条に定める対応事項に加え、本サービスの提供を円滑かつ適切に実施できるよう、以下の対応を速やかに実施することを認識し、これに同意するものとします。 お客様/MSP が当該対応を実施しなかったことに起因して、本サービスの品質低下、不完全な提供、または提供不能が生じた場合、ソフォスは一切の責任を負わないものとします。また、お客様/MSP が必要な対応を完了するまで、ソフォスは本サービスの提供を一時停止する権利を留保します。さらに、ソフォスからの書面による通知（お客様/MSP 指定の連絡先へのセキュリティサービスチームからのメール通知を含む）を受領した後も、お客様/MSP が必要な対応を完了しない場合、当該不履行は本契約に対する 重大な契約違反を構成するものとします。

1. インストール/アクセス要件

お客様/MSP/受益者は、以下を実施しなければなりません。

a) 有効でアクティブなソフォス Central アカウントを持っていること（該当する場合）
b) サービス対象エンドポイントの最低システム要件を満たすために必要な対応を実施すること（これには、システムパッチの適用やオペレーティングシステムのサポートされているバージョンへのアップグレードを含むがこれらに限定されない）
c) サービスソフトウェアをすべてのサービス対象エンドポイントに導入し、適切に設定すること
d) ソフォスがサービスを実行できるように、調査対象システムへの必要なアクセスと必要な管理資格情報（認証情報）や管理者権限を提供すること

2. 既知の侵害の修復

お客様/MSP/受益者がサイバーセキュリティ上の脅威の検知および防御のために利用する第三者製テクノロジー、またはソフォスに報告されたアクティブな脅威に関して、お客様/MSP は合理的な努力をもって適時に是正措置をしなければなりません。お客様/MSP が適時に是正措置を実施しなかったことに起因して発生した問題について、ソフォスは一切の責任を負わず、またいかなる法的責任も負わないものとします。さらに、ソフォスがすでに推奨是正手順を提供している場合、セキュリティサービスチームは、当該事項について お客様/MSP に追加の通知を行う義務を負わず、また対応アクションやその他の緩和措置を実施する義務も負わないものとします。

3. 日時設定

お客様/MSP は、すべてのサービス対象エンドポイントにおいて、日時設定が正確であることを確保しなければなりません。ソフォスは、不正確な日時設定（調査対象システムを含む）に起因してお客様/MSP が被った、または発生したエラー、問題、もしくは残存リスクについて責任を負わないものとします。

4. 補足データ

サービス提供期間中、セキュリティサービスチームは追加の補足データの提供を求める場合があります。お客様/MSP は、ソフォスが当該補足データへ常時アクセスできるよう確保しなければなりません。
補足データには、以下が含まれますが、これらに限定されません。
a) エンドポイント、サーバー、またはネットワークのログ
b) システム構成図
c) お客様/MSP／受益者の事業環境および技術環境に関する資料、文書、その他の関連リソース
なお、ソフォスのシステム上に保管された補足データの削除については、お客様/MSP からの書面による要請を受領した後に手続きが開始されるものとします。

5. お客様/MSP の担当者

お客様/MSP は、サービス提供中にソフォスと連携するために、適切なスキルを持つ担当者を少なくとも 1 名指名しなければなりません。お客様/MSP の担当者は、サービスに関する意思決定を行うために必要な技術的知識、業務上の知識、および権限を有していなければなりません。

6. タイムリーな応答

お客様/MSP は、ソフォスから連絡を受領した場合、速やかに書面にて受領を確認し、ソフォスからの依頼や要求に対して適時に対応しなければなりません。

7. サービスの範囲外の対応

本サービス仕様書で明示的に定められていないすべての活動は、サービスの範囲外です。お客様/MSP は、以下について単独で責任を負うものとします。
(i) 本サービスの範囲外となるあらゆる対応を実施すること（これには、以下が含まれますが、これらに限定されません）

- ソフォスが提案するオンサイト対応に関する措置の実施
- すべての訴訟対応および e-Discovery 支援
- ディスカバリー要求（証拠開示請求）または召喚状への対応
- 法執行機関との連携・対応
- その他、本サービス記述書に明示的に含まれていない活動

(ii) お客様/MSP の個別の指示に基づき、ソフォスが実施したものであって、本サービス仕様書に定められていない活動に関する一切の責任
すなわち、本サービス仕様書に規定されていない業務については、お客様/MSP がその実施および結果について全面的な責任を負うものとし、ソフォスは責任を負わないものとします。

8. パートナーによる対応

お客様は、本サービスの範囲内において、パートナーに対しお客様の代理として一定の行為を実施することを認めることができます。その場合、お客様は当該パートナーの行為および不作為について全面的な責任を負うものとし、ソフォスはパートナーの行為または不作為に関して一切の責任を負わないものとします。

9. MSP の追加責任

MSP は、以下について単独で責任を負うものとします。
(i) ソフォスが本サービスを提供するために必要となる、受益者からの同意または情報を取得すること

(ii) 受益者が、本サービス仕様書においてお客様に求められるすべての義務および対応事項の履行を確実にすること
(iii) 受益者が、本サービスの提供に伴うリスクを十分に理解していること
(iv) MSP が本サービスを提供する各受益者が、当該リスクのすべてを受容することに同意していること
さらに、受益者がソフォスに対して請求、訴訟その他の申立てを行い、その全部または一部が、MSP による本サービス仕様書、ソフォスエンドユーザー利用規約、または本サービスに関する契約上の義務の不履行に起因する場合、MSP はソフォスを防御し、補償し、かつ一切の損害、責任、費用および請求から免責するものとします。

V. 追加条項

1. サービス適用除外

お客様/MSP は、以下のいずれかの事由に起因する場合、ソフォスが本サービス仕様書または本契約（適用される SLA を含みます）に基づく責任を負わず、また本サービス仕様書もしくは本契約の違反とみなされないことを認識し、これに同意するものとします。
(i) 業界全体またはインフラ全体に影響を及ぼすランサムウェア攻撃、サイバー戦争行為、その他の大規模なサイバー攻撃により、セキュリティサービスチームが本サービスのいずれかの側面に対して必要なリソースを適時に提供できず、その結果としてソフォスの義務の履行に遅延または不履行が生じた場合
(ii) ソフォスの合理的な支配の及ばない予期しない事由または状況に起因する場合（これには、戦争、ストライキ、暴動、犯罪行為、天災地変、またはリソース不足が含まれますが、これらに限定されません）
(iii) 法律上の禁止に起因する場合（これには、新たな法律、法令、規則、命令その他の法的措置の制定または発効が含まれますが、これらに限定されません）
(iv) ソフォスが本契約の条件に従って本サービスを一時停止している期間
(v) お客様/MSP が本契約に違反している場合（未払いの請求書が存在する場合を含みますが、これに限定されません）
(vi) 計画されたメンテナンス期間または緊急メンテナンス期間

2. サービスの機能および能力に関する面積

お客様/MSP は、ソフォスが本サービスの提供にあたり商業上合理的な技術および運用プロセスを採用していることを認識するものの、本サービスまたは本サービスに基づくソフォスの提案、推奨事項もしくは対応計画が、すべての脅威、脆弱性、マルウェアその他の悪意ある活動の特定、検知、封じ込め、排除または復旧を実現することについて、ソフォスがいかなる保証も行わないことを了承するものとします。さらに、お客様/MSP は、ソフォスがそのような保証または担保を提供している旨を第三者に表明しないものとします。

SOPHOS

附属書 B

サービススケジュール

（別途提供）

SOPHOS

附属書 C

オンサイトサービス規約見積もり

サンプル

こんにちは［名前］

オンサイトエンゲージメントのための推定旅行および経費コストの詳細な内訳を以下に示します。

これらの見積もりは、[Y]日間現地にいる[X]人のコンサルタントに基づいています。

旅行/経費タイプ	推定コスト USD*
フライト	$
ホテル	$
食事	$
タクシー/バス/鉄道	$
移動時間	$

* 上記費用は見積額であり、変更される場合があります。オンサイトサービスエンゲージメントの詳細については、サービス仕様書（別紙 A）をご確認ください。

オンサイトサービスエンゲージメントの実施を希望され、かつ本サービス提供に関連する上記見積費用に同意される場合は、本メールに返信いただき、本条件を承諾する旨をご連絡ください。

ただし、当該対応は、お客様とソフォスの間で Statement of Work（SOW）が正式に締結されることを前提とします。