SOPHOS

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。 本契約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。

デジタルフォレンジックおよびインシデント対応 - サービス仕様書

このサービス仕様書は、デジタルフォレンジックおよび緊急インシデント対応サービス（「**本サービス**」）について規定しています。サービス仕様書におけるすべての大文字の用語は、本契約（以下に定義）または下記の定義条項に定められた意味を有するものとします。

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、本サービスの購入に関する署名またはデジタル署名済みの契約。(ii) MSP がソフォスと締結した、サービスの一部である提供物の購入に関する署名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の条項に準拠します（総称して「**本契約**」 ）。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。

本契約に別段の定めがある場合でも、お客様/MSP は以下のことを認識し、同意します。(i) ソフォスは、お客様/MSP に通知することなく、サービスの全体的お客様な機能を実質的に低下させたり劣化させたりすることなく、随時サービスを変更または更新することができること。および (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、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効力を生じること。

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。

「**アクティブな脅威**」とは、資産またはデータへの感染、侵害、または不正アクセスを指します。

「**封じ込め**」とは、無害化の前に脅威の拡散と影響を制限するためにインシデント対応中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、および攻撃者の活動を妨害し、さらなる侵害や損害を防ぐことを目的としたその他の防御策が含まれる場合があります。

SOPHOS

「**DFIR エンゲージメント**」とは、ソフォス が本サービスの下で提供する以下のいずれかのエンゲージメントの種類を意味します。エンゲージメントマネジメント、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、侵害評価サービス仕様書、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、ランサムウェア交渉、エンゲージメントレポート、またはサービスソフトウェアの導入であり、それぞれサービス仕様書の第 II 章に詳述されています。

「**DFIR サービス時間**」とは、サービス仕様書に記載されている一つ以上の DFIR エンゲージメントに適用される可能性のあるサービスのライセンス証書、SOW、またはその他の発注文書に基づき、お客様/MSP が利用可能な時間を意味します。

「**インシデント**」とは、対話型の攻撃者による活動、データの暗号化、破壊、または流出を含むがこれらに限定されない、お客様/MSP の資産に対する差し迫った懸念または脅威をもたらすシステムへの侵害または不正アクセスが疑われる事象をいいます。

「**インシデントコマンダー**」とは、関係者との調整、対応アクションの優先順位付け、部門横断的な整合性の確保およびコミュニケーションを含む、全体的な本サービスのエンゲージメントに関する全体的なライフサイクルを管理するソフォスの担当者をいいます。インシデントコマンダーは、適時かつ整合性が取れた契約範囲内の本サービスの提供を確実にするため、お客様/MSP とセキュリティサービスチーム間の主要な連絡窓口として機能します。

「**インシデントリード**」 は、本サービスのエンゲージメントの実行を管理する責任を負う主要なソフォス担当者です。インシデントリードは、フォレンジック分析、証拠収集、タイムライン再構築、技術的所見の開発を監督し、ソフォスの担当者の取り組みを調整して、調査の厳密性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**」とは、セキュリティサービスチームが調査、軽減、封じ込めおよび脅威無害化を実行するために行う技術的なプロセスをいいます。

「**調査**」とは、セキュリティサービスチームが、特定の活動が悪意のあるものであり、脅威対応を必要であるかを確認するために実施する正式な手順と手法をいいます。

「**無害化**」とは、セキュリティサービスチームが利用可能な証拠に基づき、インシデントが本サービスの対象エンドポイント上に存在しないと合理的に判断した時点における「***脅威無害化***」の結果をいいます。脅威無害化プロセスには、攻撃者のアクセスを削除し、侵害された資産やデータへのさらなる損害を防ぐために、調査と対応アクションを実施することが含まれます。

「**対応アクション**」 とは、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などを含むがこれらに限定されない、調査と脅威ハンティングを行うためのサービス対象エンドポイントに対して実施する操作のことをいいます。

「**サービス対象エンドポイント**」とは、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、あるいはサーバーシステムを指します。

「**セキュリティサービスチーム**」とは、調査の実施、脅威ハンティング、対応アクション、インシデント対応および導入を含むがこれらに限定されないサービスを提供するソフォスのチームをいいます。

「**調査対象システム**」とは、インシデントの範囲と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、インフラストラクチャサービス、またはその他のデータを指します。

「**脅威ハンティング**」とは、手動と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調査し、悪意のある活動の兆候や指標を特定するプロセスをいいます。

II.サービスの説明

本サービスにより、お客様/MSP はサービス仕様書に記載されている一つ以上の DFIR エンゲージメントのために DFIR サービス時間を利用できます。お客様/MSP に利用可能な DFIR サービス時間の数は、該当するサービスのライセンス証書に記載されます。本サービスは、お客様/MSP が第 III 章でオンサイトサービスエンゲージメントを要求しない限り、リモートで提供されます。本サービスの提供は、以下の目的でお客様/MSP とのキックオフコールから開始されます。

a) お客様/MSP/受益者のインフラストラクチャに関する情報を取得すること。
b) サービスエンゲージメントの当初の目的、範囲、優先順位を合意すること。
c) お客様/MSP からの主要な関係者と、それぞれの本サービスの提供における役割を特定すること。
d) お客様/MSP とのコミュニケーションの頻度と連絡方法に関する取り決めを行うこと。

MSP は、MSP の受益者に対して本サービスが提供される場合の連絡先として機能しなければなりません。

1　エンゲージメント管理

1.1　範囲内の成果物

エンゲージメントマネジメントの成果物は、該当する場合、以下の活動を含む場合があります。

- サービス提供の調整を監督するインシデントリードを任命し、お客様/MSP から要請があった場合は、インシデントコマンダーを任命すること。
- お客様/MSP の優先順位と利用可能なリソースを踏まえ、本サービスの提供に係る活動の計画とスケジュールの調整を行うこと。
- 進捗状況、リスク、阻害要因、主要なマイルストーンについて、定期的な状況報告を行うこと。
- 本サービスの範囲、調査結果、実施した対応アクション、および本サービスの成果に関する文書を維持管理し、必要に応じて共有の追跡アーティファクトを更新すること。
- フォレンジック、インシデント対応、交渉、お客様の関係者に係る技術的および非技術的な各作業領域を横断的に調整し、それらの活動の整合性を確保すること。
- エンゲージメント期間中のエスカレーション管理およびサービス関連の中心的な連絡窓口として機能すること。

1.2 範囲外の成果物

以下を含め、上記に明記されていない活動は、本サービスの範囲外とします。

- 法務上、規制上、または経営上の正式な役割または責任を代行すること。

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化し、可能にするために、以下の措置を講じるものとします。また、お客様/MSP が必要な対応を講じなかったことに起因する本サービスの品質が低下し、不完全となり、提供できなかった場合、ソフォスは一切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を支援するために、最大 3 名のお客様/MSP 担当者を指名すること。
- 予定された状況報告会および調整会議に出席し、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適時に確認を行い、回答すること。
- 部門横断的な調整をサポートするために、関連する事業部門および技術部門の関係者の参加を確保すること。

2 インシデント対応

2.1 範囲内の成果物

インシデント対応の成果物には、該当する場合、以下の活動が含まれる場合があります。

- インシデントの技術的な解析を実施し、調査対象システム、侵入経路、永続化メカニズム、および脅威アクターを特定すること。
- 調査結果に基づき、封じ込めおよび脅威無無害化戦略を決定し推奨すること。
- サービスソフトウェアの設定とテレメトリを確認し、現在の環境における有効性を検証すること。
- 必要に応じて、侵入テスト、脆弱性スキャン、Active Directory 評価などを含むがこれらに限定されない、調査結果を検証するための攻撃的な運用を実施すること。
- アクティブな脅威または進行中の悪意のある活動が検出された場合に、お客様/MSP の要望に応じて、システムの隔離、侵害の痕跡のブロック、悪意のあるプロセスの終了を含むがこれらに限定されない、当該アクティブな脅威の封じ込め、または無害化を目的として適切な対応アクションを講じること。
- インシデントの性質に基づいて、セキュリティ強化、是正措置、および将来の防止のための技術的な推奨事項を提供すること。
- インシデント対応の活動内容、対応結果、および調査結果の要約を書面または口頭で提供すること。

2.2 範囲外の成果物

上記に明記されていない活動は、本サービスの範囲外です。

- 調整、プロジェクトの進捗管理、エスカレーション対応などのエンゲージメントマネジメントタスク（エンゲージメントマネジメントサービスの対象となるもの）。

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化し、可能にするために、以下の措置を講じるものとします。また、お客様/MSP が必要な対応を講じなかったことに起因する本サービスの品質が低下し、不完全となり、提供できなかった場合、ソフォスは一切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本サービスソフトウェアを導入し、調査対象システムへのアクセスを提供すること。
- 対応アクションを含む本サービスの提供を支援するために、最大 3 名のお客様/MSP 担当者を指名すること。
- ソフォスが特定されたすべての対応事項を、お客様/MSP が適時に完了すること。
- 合意されたすべての電話会議に出席すること。

SOPHOS

3 デジタルフォレンジック

3.1 範囲内の成果物

デジタルフォレンジックのエンゲージメントにおける成果物には、該当する場合、以下の活動が含まれる場合があります。

- 該当する場合、サービス対象エンドポイントおよび/または対象の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、収集された証拠をフォレンジックツールと技術を使用して分析し、侵害の痕跡（IOC）を特定し、脅威アクター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を確認すること。
- 調査およびフォレンジック分析中に特定された疑わしいマルウェアについて、静的分析および/または動的分析を実施すること。
- 証拠分析により判明した主要な事象のタイムラインと、調査により特定された侵害の痕跡のリストを含む要約を、書面または口頭で提供すること。

3.2 範囲外の成果物

以下を含め、上記に明記されていない活動は、本サービスの範囲外とします。

- 正式な証拠保全記録または裁判上の証拠能力を有する資料を作成すること。
- 書面で明示的に合意された場合を除き、高度なマルウェアの逆アセンブル、リバースエンジニアリング、またはエクスプロイト開発に関する分析を実施すること。
- 収集されたフォレンジックデータの長期的な保存、管理、またはアーカイブを提供すること。

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化し、可能にするために、以下の措置を講じるものとします。また、お客様/MSP が必要な対応を講じなかったことに起因する本サービスの品質が低下し、不完全となり、提供できなかった場合、ソフォスは一切責任を負わないものとします。

- ソフォスに、管理者権限、調査対象システムに関するログおよびフォレンジックデータを提供すること。
- 該当する場合、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。
- 調査対象システムからのデジタル証拠の収集を含むソフォスによる本サービスの提供を支援するために、最大 3 名のお客様/MSP 担当者を指名すること。
- 合意されたすべての電話会議に出席すること。

- ソフォスが特定されたすべての対応事項を、お客様/MSP が適時に完了すること。

4 侵害評価

4.1 範囲内の成果物

侵害評価のエンゲージメントの成果物には、該当する場合、以下の活動が含まれる場合があります。

- お客様/MSP と協力して、潜在的な脅威に関する情報を収集し、お客様/MSP が本サービスの適用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、またはお客様/MSP からソフォスに提供された関連データに基づいたサービス対象エンドポイントに対して、侵害の痕跡（「**IOCs**」）の調査を実施すること。
- アクティブな脅威が特定された場合、お客様/MSP に通知し、調査結果を提供し、さらなる調査と封じ込めのための措置を推奨すること。
- 本サービス範囲内で侵害の証跡が見つからない場合は、分析されたデータセット内に侵害の痕跡が存在しないこと、および使用した方法を文書化した書面による通知をお客様/MSP に提供すること。
- 脅威ハンティング活動、成果、および推奨事項の書面による要約を提出すること。

4.2 範囲外の成果物

以下を含め、上記に明記されていない活動は、本サービスの範囲外とします。

- 脅威の発見事項に基づき、システムの修正やパッチ適用を行うこと。

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化し、可能にするために、以下の措置を講じるものとします。また、お客様/MSP が必要な対応を講じなかったことに起因する本サービスの品質が低下し、不完全となり、提供できなかった場合、ソフォスは一切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。
- ソフォスによる本サービスの提供を支援するために、最大 3 名のお客様/MSP 担当者を指名すること。
- 必要なデータを適時にソフォスに提供すること。
- 合意されたすべての電話会議に出席すること。

SOPHOS

5 脅威インテリジェンスおよび調査

5.1 範囲内の成果物

脅威インテリジェンスおよび調査のエンゲージメントの成果物には、該当する場合、以下の活動が含まれる場合があります。

- 提出された侵害の痕跡のデータに対する高レベルな分析的強化を提供すること。これには、脅威の文脈、関連性、潜在的な帰属先、および既知の脅威アクターやキャンペーンに関連付けられた識別可能な戦術、技術、手順（TTPs）を含みます。
- お客様/MSP から提出されたハッシュ、URL、IP などのデータについて、オープンソースおよびダークウェブ検索を実施し、主要な調査結果をお客様/MSP に伝達すること。
- 侵害との関連している潜在的な可能性があるお客様/MSP データをオープンソースで調査すること。
- 悪意のあるファイルや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、該当する場合は、振る舞い特性、IOC（侵害の痕跡）を抽出し、脅威アトリビューションと文脈分析をサポートすること。
- 発見事項および推奨事項の書面による要約を提出すること。

5.2 範囲外の成果物

以下を含め、上記に明記されていない活動は、本サービスの範囲外とします。

- アクティブなインシデントに関連する封じ込め、無害化、または修復対応。
- **確定的な結論の提供と脅威アトリビュートの特定を保証すること**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、評価時点での利用可能な情報および脅威インテリジェンスに基づいていることを認識して、同意するものとします。かかる調査結果は確定的なものではなく、「現状有姿」で、いかなる表明、保証または約束を伴わずに提供されることを承諾します。

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化し、可能にするために、以下の措置を講じるものとします。また、お客様/MSP が必要な対応を講じなかったことに起因する本サービスの品質が低下し、不完全となり、提供できなかった場合、ソフォスは一切責任を負わないものとします。

- 脅威インテリジェンスおよびリサーチ活動を可能にするために、関連する正確なデータまたはアーティファクトをすべて提供してください。
- エンゲージメント全体を通じた調整とコミュニケーションの円滑化を含むソフォスによる本サービスの提供を支援するために、最大 3 名のお客様/MSP 担当者を指名すること。

- ソフォスと共有される機密情報または専有情報は、サービス範囲内での使用が適切に承認されており、適用されるすべての法律および機密保持契約を遵守して提供されることを確保すること。
- 合意されたすべての電話会議に出席すること。

6 脅威ハンティング

6.1 範囲内の成果物

脅威ハンティングのエンゲージメントの成果物には、該当する場合、以下の活動が含まれる場合があります。

- サービス対象エンドポイント上のサービスソフトウェアを最大 30 日間使用し、またはお客様/MSP からソフォスに提供された関連データに基づいて、サービス対象エンドポイント上の侵害の痕跡の調査を実施すること。
- 証拠分析により判明した主要な事象のタイムラインと、調査により特定された侵害の痕跡のリストを含む要約を、使用した手法とあわせて、書面または口頭で提供すること。
- 調査結果に基づいた高レベルの推奨事項を提供すること。
- 本サービス範囲内で侵害の証跡が見つからない場合は、分析されたデータセット内に侵害の痕跡が存在しないこと、および使用した方法を文書化した書面による通知をお客様/MSP に提供すること。

6.2 範囲外の成果物

以下を含め、上記に明記されていない活動は、本サービスの範囲外とします。

- 脅威の発見事項に基づき、システムの修正やパッチ適用を行うこと。

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化し、可能にするために、以下の措置を講じるものとします。また、お客様/MSP が必要な対応を講じなかったことに起因する本サービスの品質が低下し、不完全となり、提供できなかった場合、ソフォスは一切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。
- ソフォスによる本サービスの提供を支援するために、最大 3 名のお客様/MSP 担当者を指名すること。
- 必要なデータを適時にソフォスに提供すること。
- 合意されたすべての電話会議に出席すること。

SOPHOS

7 ランサムウェア交渉

7.1 範囲内の成果物

ランサムウェア交渉エンゲージメントの成果物には、該当する場合、以下の活動が含まれる場合があります。

- ランサムウェアインシデントに関連する情報（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など）を収集するため、セキュリティサービスチームおよびお客様/MSP との電話会議を実施すること。
- 既知の TTP と過去の活動に基づき、脅威アクターの行動とプロファイルを評価すること。
- 推奨されるコミュニケーションのトーン、進め方、対応方針を含め、潜在的な交渉戦略について助言すること。
- お客様/MSP と協力して交渉目標を定義すること。
- 脅威アクターと関わり、身代金要求に関する議論を促進すること。すべての交渉活動は、お客様/MSP からのフィードバックおよび指示に厳密に従って実施されます。
- 交渉プロセスを通して、脅威アクターとのコミュニケーションの要約および提案される次の対応策を含む、定期的な最新情報をお客様/MSP に提供すること。
- 適切な場合は、身代金の支払いの仲介を専門とする第三者のサービスプロバイダーを推奨すること。*お客様/MSP は、以下のことを認識し、同意します。(i) 当該第三者の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 による必要なデューデリジェンス、法的審査、およびすべての適用される法令、制裁およびアンチマネーロンダリング規制の遵守を条件とすること。(ii) ソフォスは、かかる第三者が提供するサービスについて、管理、承認、または責任の負担を行うものではないこと。*
- 交渉関連活動、観測された脅威アクターの挙動、および結果の要約を書面により提供すること。

7.2 範囲外の成果物

以下を含め、上記に明記されていない活動は、本サービスの範囲外とします。

- 制裁、輸出管理、マネーロンダリング要件に関する法的または規制上の助言の提供。
- お客様/MSP に代わって、仲介、名義貸し、または身代金支払いを行うこと。
- 暗号化されたデータの復号化および/または復元を支援すること。
- 身代金支払い後のデータ復元や継続的な連絡および交渉対応を含む、脅威アクターの行為または履行を保証すること。

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化し、可能にするために、以下の措置を講じるものとします。また、お客様/MSP が必要な対応を講じなかったことに起因する本サービスの品質が低下し、不完全となり、提供できなかった場合、ソフォスは一切責任を負わないものとします。

- ランサムウェア交渉戦略と支払いに関する決定を下し、ソフォスによる本サービスの提供を支援するために、最大 3 名のお客様/MSP 担当者を指名すること。
- 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への適時かつ完全なアクセスを提供すること。
- サービス提供中、ソフォスからの問い合わせや推奨事項に迅速に回答すること。
- 合意されたすべての電話会議に出席すること。

  リスクの認識と補償:*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従事することに伴う固有のリスクを認識し、これを承諾するものとします。これには、不履行、継続的な恐喝、データ破壊、評判の毀損、または法的および規制上のリスクが含まれますが、これらに限定されません。お客様/MSP はさらに、ソフォスが脅威アクターの行為や結果を制御するものではなく、データ復旧や悪意のある活動の停止を含む交渉プロセスからいかなる結果も保証しないことを理解するものとします。お客様/MSP は、身代金の支払いまたは交渉戦略に関連する、適用される法律、規制、または制裁への不遵守を含む、お客様/MSP の決定または行動から生じるあらゆる請求、責任、損失、損害、費用、または経費（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、およびそれぞれの取締役、役員、従業員、代理人を補償し、防御し、免責することに同意します。*

8 エンゲージメントレポート

8.1 範囲内の成果物

エンゲージメントレポートの成果物には、該当する場合、以下の活動が含まれる場合があります。

- 経営層や非技術的な関係者向けに簡潔にまとめた、高レベルなインシデントの要約の提供。
- インシデント期間中における脅威アクターの主要な動きと活動を時系列で示した図表形式のタイムラインを提供すること。
- 調査中に特定された脅威アクターの TTPs の強化された要約と、構造化された MITRE ATT&CK フレームワークへのマッピングし、確認された TTPs に合わせた適用可能な緩和策をあわせて提供すること。
- 調査中に特定された侵害の痕跡の包括的な表。
- 調査結果に基づく高レベルの助言的推奨事項

SOPHOS

8.2 範囲外の成果物

以下を含め、上記に明記されていない活動は、本サービスの範囲外とします。

- 法的助言、推奨事項、または法的意見の提供
- 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
- **確定的な結論の提供と脅威アトリビュートの特定を保証すること。**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、評価時点での利用可能な情報および脅威インテリジェンスに基づいていることを認識して、同意するものとします。かかる調査結果は確定的なものではなく、「現状有姿」で、いかなる表明、保証または約束を伴わずに提供されることを承諾します。

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化し、可能にするために、以下の措置を講じるものとします。また、お客様/MSP が必要な対応を講じなかったことに起因する本サービスの品質が低下し、不完全となり、提供できなかった場合、ソフォスは一切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出できる有効な電子メールアドレス、または安全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や、それに伴うフォローアップの質問や明確化を含む、本サービスの提供を円滑化するために、最大 3 名のお客様/MSP 担当者を指名すること。
- 関連する関係者を特定し、報告書のレビューおよび、エンゲージメントレポートの口頭でのプレゼンテーションが求められた場合に、関連する議論へ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提出し、当初の時間単位サービス契約の範囲内で明確化や修正に対応できるようにすること。当該期間以降に行われた依頼については、追加のサービス時間の購入が必要となります。
- 合意されたすべての電話会議に出席すること。

9 ビジネスメール詐欺

9.1 範囲内の成果物

ビジネスメール詐欺に関するエンゲージメントの成果物には、該当する場合、以下の活動が含まれる場合があります。

- セキュリティサービスチームおよびお客様/MSP の電話会議を実施し、メール環境と、メールアカウントの不正アクセス（「ビジネスメール詐欺」または「BEC」）の疑いに関する情報を収集すること。
- BEC の範囲を調査し、本サービス提の供を通じて、お客様/MSP に主要な調査結果を報告すること。

- BEC が確認された場合、原因、侵入経路、永続化メカニズム、および脅威アクターによって使用された技術を特定するための解析を実施し、本サービスの提供を通じて、お客様/MSP に主要な調査結果を伝達すること。
- BEC の調査結果の要約を文書または口頭で提供すること。

9.2 範囲外の成果物

以下を含め、上記に明記されていない活動は、本サービスの範囲外とします。

- お客様/MSP のメール環境のセットアップまたは設定。

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化し、可能にするために、以下の措置を講じるものとします。また、お客様/MSP が必要な対応を講じなかったことに起因する本サービスの品質が低下し、不完全となり、提供できなかった場合、ソフォスは一切責任を負わないものとします。

- 本サービスの提供を支援するために、ソフォスにメール環境への必要なすべてのアクセスを提供すること。
- ソフォスによる本サービスの提供を支援するために、最大 3 名のお客様/MSP 担当者を指名すること。
- 合意されたすべての電話会議に出席すること。

10 サービスソフトウェアの導入

10.1 範囲内の成果物

サービスソフトウェア導入エンゲージメントの成果物には、該当する場合、以下の活動が含まれる場合があります。

- お客様/MSP にセキュリティサービスチームを割り当てること。
- お客様/MSP と電話会議を行い、お客様/MSP が本サービス を適用したいサービス対象エンドポイントを特定すること。
- お客様/MSP が定義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導入すること。
- お客様/MSP に対し、キックオフコールで確立された連絡手段を通じて、サービス提供に関するサポートとガイダンスのために、ソフォスの導入エンジニアへの 24 時間年中無休のアクセスを提供すること。

- 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ついて書面の要約を提供すること。

10.2 範囲外の成果物

以下を含め、上記に明記されていない活動は、本サービスの範囲外とします。

- ソフォス製品およびサービス以外の製品やサービスの構成および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 デバイスの起動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化し、可能にするために、以下の措置を講じるものとします。また、お客様/MSP が必要な対応を講じなかったことに起因する本サービスの品質が低下し、不完全となり、提供できなかった場合、ソフォスは一切責任を負わないものとします。

- ソフォスの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、優先順位付けすること。
- ソフォスによる本サービスの提供を支援するために、最大 3 名のお客様/MSP 担当者を指名すること。。
- 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する際にソフォスを適時に支援するために、管理者権限と技術的専門知識を持つカスタマー/MSP の担当者を確保すること。
- 合意されたすべての電話会議に出席すること。

III.オンサイトサービスエンゲージメント

お客様/MSP が上記に記載されている DFIR エンゲージメントについてオンサイトサポートを要請し、ソフォスが当該要請を受け入れた場合、両当事者は、当該オンサイトサポートの目的、作業範囲、必要な専門スキル及び実施期間を確定するため、事前に協議を行うものとします。当該協議に基づき、ソフォスは派遣する適切なソフォスサービスチームの担当者を選定し、お客様/MSP の確認と承認のため、想定される費用および移動時間の見積書を書面で提供します。お客様/MSP が書面で見積書を承認するまで、出張は開始されず、出張関連費用は発生しないものとします。お客様/MSP は、別途書面により合意したバイア意を除き、ソフォスの担当者が現地の営業時間内（1 日あたり 8 時間を超えないものとする）に業務を実施することに同意します。

- **費用区分**

  お客様/MSP は、以下の 3 つの費用区分について費用を負担するものとします。

1. **実費:**これには、現地でのエンゲージメントに関連して発生するすべての合理的な必要費用が含まれます。往復航空運賃（フライト時間が 4 時間未満の場合はエコノミークラス、4 時間から 8 時間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（所用時間が 6 時間未満の場合はエコノミークラス、6 時間を超える場合はビジネスクラス）、燃料費（自動車を利用する場合）、宿泊費、食事およびその他の付随費用、地上交通費（例：タクシー、ライドシェア、レンタカー）、ビザまたは入国関連書類、および適用される税金や手数料が含まれます。
2. **移動時間:**上記の実際の費用に加え、ソフォスは、お客様/MSP の拠点への往復にかかった移動時間（担当者の自宅からお客様/MSP の場所（または該当する場合の現地のホテル）までの基点から終点までの所要時間）について請求します。移動時間は、該当する本サービスのお客様/MSP の標準時間単価の **50 パーセント（50%）**に相当する時間単価で請求されます。
3. **待機時間:**ソフォスの担当者がオンサイトまたは待機している間に、お客様/MSP がタイムリーなアクセス、情報、またはエンゲージメント開始の準備を提供できなかった場合、オンサイトサービスエンゲージメントに従事する各担当者につき 1 日 8 時間を上限として、その時間は本サービスに適用される標準時間単価で請求されるものとします。

- **エンゲージメントのキャンセルまたは延期**
  お客様/MSP が、予定開始日より前にオンサイトエンゲージメントをキャンセルまたは延期した場合、あるいは移動手配が確定または開始された後にキャンセルまたは延期した場合、お客様/MSP は、上記に規定される移動時間の費用を含む、すでに負担した返金不能または回収不能な移動費用の全額をソフォスに支払うものとします。

オンサイトエンゲージメントにおけるお客様/MSP の義務:

お客様/MSP は、本サービスの提供を円滑化し、可能にするために、以下の措置を講じるものとします。また、お客様/MSP が必要な対応を講じなかったことに起因する本サービスの品質が低下し、不完全となり、提供できなかった場合、ソフォスは一切責任を負わないものとします。

- オンサイトでのエンゲージメントに先立ち、必要なすべての施設への立ち入り許可、物理的な入館承認、およびセキュリティクリアランス（必要な場合は時間外アクセスを含む）を事前に手配すること。
- エンゲージメントにおいて合意された範囲で特定されたすべての関連システム、環境、インフラストラクチャ構成要素、および担当者へのアクセスを適時に提供すること。
- エンゲージメントを支援するために必要となるすべての情報、文書、または意思決定に関するソフォスからの要請に、適時に対応すること。

- エンゲージメント中にソフォスが使用するツール、ソフトウェア、またはアクセス手段について必要となる承認または許可を取得し、提供すること。
- 適切な作業場所を指定し、電源、ネットワーク接続、必要なシステムやツールへの物理的または仮想的なアクセスを確保すること。
- 合意済のすべての予定された更新およびブリーフィング会議に出席し、すべての予定されている状況更新、技術ブリーフィング、およびエンゲージメント後のレビューにおいて、指定された関係者の出席と参加を確保すること。
- オンサイトでの活動中、安全な作業環境を確保するために、適用される健康、安全、セキュリティに関する要件を遵守すること。

IV.お客様/MSP の責任

お客様/MSP は、上記第 II 章に記載されている措置に加え、サービス提供を促進し可能にするために、以下の措置を速やかに講じることに同意します。また、お客様/MSP が必要な対応を講じなかったことに起因する本サービスの品質が低下し、不完全となり、提供できなかった場合、ソフォスは一切責任を負わないものとします。ソフォスは、お客様/MSP が必要な対応を実施するまで、本サービスの提供を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（セキュリティサービスチームからお客様/MSP 指定連絡先への電子メールによる通知を含む）を受領した後も、必要な措置を完了しない場合、当該不履行は、お客様/MSP による本契約の重大な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、a）該当する場合、有効でアクティブな Sophos Fusion アカウントを保有していること、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の措置を講じること（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展開および設定すること、および d）ソフォスが本サービスを実行するために必要な調査対象システムへのアクセスおよび必要な管理認証情報/権限を提供することを行わなければならないものとします。
2. **既知の侵害の修復。**お客様/MSP は、ソフォスまたはお客様/MSP/受益者がサイバーセキュリティ上の検知と保護のために利用するその他の第三者技術によって報告されたアクティブな脅威について、適時に修復するために合理的な努力をするものとします。ソフォスは、お客様/MSP が適時に修復措置を講じなかったことによって引き起こされたいかなる問題についても責任を追わないものとします。さらに、セキュリティサービスチームは、ソフォスがすでに推奨する修復手順を提供したものについて、お客様/MSP に通知し、対応アクションや緩和措置を取る義務を負わないものとします。.

3. **時刻と日付の設定。**お客様/MSP は、すべてのサービス対象エンドポイントに正確な時刻と日付の設定がされていることを確認するものとします。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 が経験または被るエラー、問題、残存リスクについて責任を負わないものとします。

4. **サポートデータ。**本サービスの提供期間中、セキュリティサービスチームは追加のサポートデータを要求する可能性があり、お客様/MSP はソフォスが常にそのようなサポートデータにアクセスできるようにするものとします。そのような裏付けとなるデータには、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ログ、b) アーキテクチャ図、および c) お客様/MSP/受益者の事業環境および技術環境に関連する資料とリソース。ソフォスシステムからのサポートデータの削除は、お客様/MSP からの書面による要請があった場合に開始されます。

5. **お客様/MSP 担当者。**お客様/MSP は、サービスの提供中にソフォスと協力する、適切なスキルを持った担当者を少なくとも 1 名指名するものとします。お客様/MSP の担当者は、本サービスに関する決定を下すために必要な技術的および事業上の知識と権限を持っていなければならないものとします。.

6. **タイムリーな対応。**お客様/MSP は、ソフォスからの連絡があった場合、速やかに書面で受領を確認し、ソフォスからの要請に適時に対応しなければならないものとします。

7. **サービス範囲外の行為。**サービス仕様書に明示的に記載されていない活動は、すべて本サービスの範囲外とします。お客様/MSP は、（i）本サービス範囲外のいかなる行為（例：オンサイト対応に関するソフォスの提案、開示請求や召喚状への対応を含むすべての訴訟および e-Discovery 支援、法執行機関との協力など）、（ii）お客様/MSP の個別の指示に基づいてソフォスが実施した本サービス範囲外の行為について、単独で責任および義務を負うものとします。

8. **パートナーによる行為。**お客様は、お客様に代わって本サービスの範囲内で特定の対応をパートナーに実施させることができます。その場合、お客様は当該パートナーの一切の作為または不作為について責任を負います。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。

9. **MSP の追加責任。**MSP は、以下の事項について単独で責任を負います。(i) ソフォスが本サービスを提供するために、受益者から必要とされる同意または情報を取得すること、(ii) 受益者がサービス仕様書において、お客様に求められるすべての措置を講じることを保証すること、(iii) 受益者が本サービスの実施に伴うリスクを理解していることを保証すること、および(iv) MSP が本サービスを提供するすべての受益者が、かか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。MSP は、サービス仕様書、本サービスに関するソフォスの利用規約、または本契約に基づく MSP の義務を十分に履行しなかったことに起因する、受益者からソフォスに対して提起された請求について、ソフォスを補償し、損害を与えないものとします。

SOPHOS

V. 追加条項

1. **サービス除外事項。**お客様/MSP は、以下の場合には、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 を含む）の違反とはみなされず、また、いかなる責任も負わないことを認識し、これに同意します。(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、セキュリティサービスチームがサービスのいかなる側面に対しても適時に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) 法律、政令、規則、または命令の制定など、法的禁止による場合、(iv) 本契約の条件に従い、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 が本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）、または (vi) 計画メンテナンスまたは緊急のメンテナンスの期間中。

2. **サービス機能。**お客様/MSP は、ソフォスがサービスの一環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ことを認識し、これに同意するものとします。ただし、ソフォスは、本サービスの結果としてソフォスが行うサービス、またはソフォスの推奨事項および計画が、すべての脅威、脆弱性、マルウェア、またはその他の悪意のある脅威の特定、検出、封じ込め、根絶、または回復をもたらすことを保証しません。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。

SOPHOS

別紙 B

本サービスのライセンス証書

（別途提供されるものとします。）

SOPHOS

別紙 C

オンサイトサービスエンゲージメントの見積もり

****サンプル****

こんにちは[Name]

オンサイトでのエンゲージメントにかかる想定される出張費用および経費の詳細な内訳を以下に示します。

これらの見積もりは、[X]名のコンサルタントが[Y]日間のオンサイト勤務をすることを基にしています。

出張/費用の種類	**見積費用 USD***
フライト	$
ホテル	$
食事	$
タクシー/バス/鉄道	$
移動時間	$

上記の費用は概算であり、変更される可能性があります。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）をご覧ください。

オンサイトサービスエンゲージメントを進め、本サービスの提供に関連する上記の概算費用に同意される場合は、本メールにご返信いただき、適用される条件への同意をお願いいたします。上記は、貴社とソフォスとの間で署名された SOW の受領を条件とします。