cisco SECURE

オファー説明書：Cisco Umbrella

このオファー説明書（以下「**本オファー説明書**」）は、Cisco Umbrella（以下「クラウドサービス」）について説明するものです。お客様のサブスクリプションには、本オファー説明書とシスコ エンド ユーザー ライセンス契約（www.cisco.com/go/eula に掲載されています）またはお客様およびシスコ間の同様の規約（以下「**本契約**」）が適用されます。本オファー説明書にて大文字の英字で始まり、本オファー説明書で別途定義されていない用語は、本契約内で定められた意味を持つものとします。

目次

1. 説明

Cisco Umbrella は、複数のセキュリティサービスを単一のクラウドベースのプラットフォームに統合することでインターネットへのアクセスを保護し、ネットワーク、ブランチオフィス、ローミングユーザーによるクラウドアプリケーションの使用を管理するクラウド セキュリティ プラットフォームです。Cisco Umbrella は、パッケージおよび展開モデルに応じて、セキュアな Web ゲートウェイ、クラウド提供型のファイアウォール（以下「CDFW」）、DNS レイヤのセキュリティ、クラウド上のマルウェア対策、回線内のデータ喪失防止（DLP）、その他クラウド アクセス セキュリティ ブローカ（CASB）機能およびリモートブラウザ分離などの機能を統合し、ユーザーのアクセス先を問わず効果的に保護します。ユーザーがオンラインの接続先に接続する前の段階でインターネットへのセキュアなインターフェイスとして機能し、詳細なインスペクションと制御機能で効果的に脅威をブロックしてコンプライアンスに対応します。世界最大の脅威インテリジェンス チームの 1 つである Cisco Talos によってサポートされており、Cisco Umbrella Investigate を通じて脅威インテリジェンスにインタラクティブにアクセスできるため、インシデント対応と脅威調査に役立ちます。

Cisco Umbrella Investigate では、悪意のあるドメイン、IP、ネットワーク、およびファイルハッシュに関するシスコの特定の脅威インテリジェンスにアクセスできます。シスコは、日々発生する数十億もの DNS 要求に基づく多様なデータセットを活用し、インターネット上の異なるネットワーク間の接続をリアルタイムに確認しながら、統計モデルとヒューマンインテリジェンスを適用して攻撃者のインフラストラクチャを特定しています。Cisco Umbrella Investigate のデータには、Web ベースのコンソールまたは API を介してアクセスできます。技術仕様、設定要件、特徴および機能に関する詳細な情報については、Cisco Umbrella のドキュメンテーション [英語] を参照してください。また、Cisco Umbrella の各種パッケージに関する情報については、パッケージ比較表 [英語] を参照してください。

お客様の Cisco Umbrella のサブスクリプションには、シスコの統合型セキュリティ プラットフォームである Cisco SecureX へのアクセス権が含まれています。Cisco SecureX には脅威インテリジェンスの集約、さまざまなシスコ製セキュリティ製品とサードパーティ製セキュリティ製品における可視性の統合、ワークフローの自動化などの機能があります。SecureX の詳細については、SecureX オファー説明書（https://www.cisco.com/c/en/us/about/legal/cloud-and-software/cloud-terms.html）を参照してください。

2. 補足条項

2.1. 制限

お客様が、シスコとの契約に基づき、エンドカスタマーの代理としてシスコ クラウドサービスを利用することが許可されているシスコのサービスプロバイダーである場合、お客様は、そのようなエンドカスタマーの利益となる目的でのみクラウドサービスを使用できます。

2.2. 免責事項

ファイル、ネットワーク、エンドポイントに侵入および攻撃する新たな技術が開発され続けているため、シスコはクラウドサービスが絶対的なセキュリティを保証することの表明または保証はいたしません。シスコは、クラウドサービスがお客様のすべてのファイル、ネットワーク、およびエンドポイントを、すべてのマルウェア、ウイルス、および第三者による悪意のある攻撃から保護することを表明および保証しません。シスコは、クラウドサービスが統合するあらゆるサードパーティ製のシステムおよびサービス、ならびに継続中の統合サポートについても、表明および保証を一切しません。注文に含まれる、一般的に利用可能な製品ではない、アクセス可能な統合については、「現状有姿」で提供されるものとします。

2.3. 対象ユーザー

価格設定がユーザーベースであるパッケージの場合、公開されている Cisco Umbrella データシートに別段の記載がない限り、対象ユーザーごとに 1 つのユーザーライセンスを購入する必要があります。「対象ユーザー」とは、インターネットに接続している各従業員、再委託先、および Cisco Umbrella の展開対象である（すなわち、保護される）許可を得たその他の個人のことをいいます。下記のセクション 2.4 および 2.6 に記載されているように、追加のユーザーライセンスが必要になる場合があります。

2.4. Umbrella SIG – 平均帯域幅

Cisco Umbrella Security Internet Gateway（以下「SIG」）Essentials、Cisco Umbrella SIG Advantage、および Cisco Umbrella SIG for Education（総称して、以下「Umbrella SIG」）は、95 パーセンタイル計算に基づき、1 ユーザーにつき最大で毎秒 50 キロビット（以下「kbps」）の平均帯域幅の対象になります。これは、95% の時間、帯域幅使用量がこの値以下であることを意味します。95 パーセンタイルモデルを使用すると、短い時間において使用量のピークが制限を超えることを認めることになります。この計算は下記のとおりです。

シスコは、お客様の 1 ユーザーあたりの平均帯域幅を特定するために、30 日間を 1 つの周期として、お客様による Umbrella SIG の使用量を継続的に測定します。お客様の 1 ユーザーあたりの平均帯域幅が 50 kbps を超えているとシスコが判断した場合、シスコは、お客様の平均帯域幅を 50 kbps まで下げるために必要な追加のライセンスを購入するようお客様に要求する権利を留保します。平均帯域幅の式は次のとおりです。

平均帯域幅 = 95 パーセンタイル帯域幅/対象ユーザー数

95 パーセンタイル帯域幅は次のとおり計算します。

- お客様のトラフィックの送信先である Cisco Umbrella の各データセンターにおいて、30 日間にわたりお客様のトラフィックサンプルを観察します。
- 各データセンターにおけるトラフィックサンプルの上位 5% を破棄し、次に高いトラフィックサンプルの値を採用します（この「次に高いトラフィックサンプルの値」を「ピーク値」といいます）。
- 各データセンターのピーク値を合算します。

この計算のためのトラフィックサンプルには、該当するパッケージの Umbrella DNS、セキュアな Web ゲートウェイ（プロキシ）、クラウド提供型ファイアウォール（以下「CDFW」）のトラフィックが含まれます。

たとえば、あるデータセンターのピーク値が 1,000,000 kbps であり、2 つ目のデータセンターのピーク値が 10,000 kbps である場合、95 パーセンタイル帯域幅は 1,000,000 + 10,000 = 1,010,000 kbps になります。1 ユーザーあたりの平均帯域幅は、1,010,000 kbps をお客様のサブスクリプションに基づいてライセンスされた対象ユーザーの数で除した値になります。サブスクリプションの対象となるユーザー数が 25,000 の場合、監視期間のユーザーごとの平均帯域幅は、1,010,000 / 25,000 = 40.4 kbps です。

2.5. Umbrella SIG およびUmbrella CDFW の禁止事項

Umbrella SIG および Umbrella CDFW の使用に関連して、お客様は（i）外部拠点に対して、サービス拒否（DoS）攻撃または第三者のサービス提供条件への違反として外部拠点が合理的にみなす可能性がある、またはその他シスコがブラックリストに登録される合理的な可能性がある定期的かつ頻繁なクエリの自動送信（たとえば、お客様の管理下にない第三者の組織をポートスキャンすることや、Cisco Umbrella を使用して第三者に対し攻撃的なセキュリティ技術を使用することによるものが含まれます）を確立すること、（ii）クラウドサービスを使用し、適用法令に反して、Web サイトまたはブロックされているサービスにアクセスすること、および（iii）違法行為に関連してお客様の身元を意図的に隠すため、またはその他法的手続きを回避するためにクラウドサービスを使用することができません。また、お客様は第三者による（i）から（iii）の行為を許可してはなりません。お客様のネットワーク上で行われているとされる違法行為に関連するお客様による Umbrella SIG または Umbrella CDFS の使用に関してシスコが第三者から情報提供依頼、催告書またはこれらに類似するその他の問い合わせを受けたときに、シスコは、法的手続きの遵守または国のセキュリティ要件の充足のために必要な場合、またはシスコ、シスコのビジネスパートナー、お客様、他者の権利、財産または安全を保護するために必要な場合、または適用法が別途義務付けている場合に、お客様の氏名または名称を当該第三者に開示することがあります。

2.6. Umbrella DNS Security - DNS クエリ月間平均件数

Cisco Umbrella DNS Security Essentials および Cisco Umbrella DNS Security Advantage（総称して、以下「DNS Security」）には DNS クエリ月間平均件数（以下で定義します）の上限があります。その上限は、1 対象ユーザーあたり 1 日につき 3,000 件になります。シスコは、お客様の DNS クエリ月間平均件数を特定するために、1か月単位でお客様による DNS Security の使用状況を継続的に監視します。シスコは、お客様の DNS クエリ月間平均件数が、1 対象ユーザーあたり 1 日につき 3,000 件を超えていると判断した場合、お客様に追加ライセンスを購入するよう要求する権利を留保します。

DNS クエリ月間平均件数 =（該当月の DNS クエリ件数/該当月の日数）/ライセンスが付与された対象ユーザー数

たとえば、お客様が 1,000 対象ユーザー分のライセンスを購入し、対象ユーザーが過去 30 日間に合計 3,000,000 件の DNS クエリを送信した場合、DNS クエリ月間平均件数は次のようになります。

(3,000,000/30)/1,000 = 100

2.7. Cisco Umbrella Investigate for MSSP

SKU が UMB-INV-CONSOLE-SP もしくは UMB-INV-INT-API-SP またはその両方である Cisco Umbrella Investigate for MSSP（総称して、以下「Investigate for MSSP」）をお客様が購入した場合、矛盾する規定が本契約にあったとしても、お客様は、第三者である顧客に接続サービス、管理サービス、および運用サービス、またはこれらの一部を提供する過程においてのみ、当該顧客の利益のために、Investigate for MSSP を調査実施ツールおよびレポート作成ツールとして使用することができます。

お客様が Investigate for MSSP を共同ブランディングする場合、ガイドライン（http://www.cisco.com/c/dam/en/us/products/collateral/security/umbrella/umbrella-sps-co-branding-guidelines.pdf [英語]）および本契約に記載の知的財産および商標に関するその他のガイドラインがお客様に適用されます。明確にするために付言すると、お客様が Investigate for MSSP を使用して得た調査データまたは調査結果を第三者である顧客に提供する場合、お客様は前述のガイドラインに従って、その情報源として常にシスコの名称を記載する必要があります。

2.8. シスコが管理する S3 Log Storage

特定の Cisco Umbrella パッケージでは、DNS、プロキシ、およびイベントログ用の、シスコが管理する S3 ストレージまたは企業が管理するストレージ（すなわち、お客様自身のストレージ）を選択することができます。シスコが管理する S3 Log Storage の保存期間は、7 日間、14 日間、または 30 日間のいずれかを選択できます。30 日間を超える保存期間を必要とする場合、お客様が管理するストレージを選択するか、保存期間が満了する前に、シスコが管理するストレージからお客様が管理するストレージにデータをエクスポートする必要があります。シスコが管理する S3 バケットへのロギングが有効になっている場合、各ログファイルが 1 回だけダウンロードされるように、そのバケットにあるファイルのダウンロードおよび同期を設定する必要があります。シスコは、ログファイルが 1 回ではなく複数回ダウンロードされた場合、S3 バケットにあるログのダウンロードを（キーのローテーションまたはその他の方法によって）一時停止する権利を留保します。https://docs.umbrella.com/deployment-umbrella/docs/cisco-managed-s3-bucket で入手可能な、シスコが管理する S3 バケットに関するドキュメンテーションをご確認ください。

3. サービスレベル契約

3.1. Umbrella DNS Security

Umbrella DNS Security に関する本サービスレベル契約において、「本サービス」とは、シスコの再帰 DNS サービスのことをいい、Web ベースのユーザーインターフェイス、構成システム、ならびにその他のデータアクセス手法およびデータ操作手法は含まれません。シスコは、商取引上の合理的な努力を尽くして、Cisco Umbrella サービスの可用性を各暦月の 99.999% として維持するものとします。可用性は、該当する暦月の合計稼働時間（分単位とし、以下で定義します）を、その月の総分数から計画的なメンテナンスおよび第三者の行為（以下で定義します）に起因する Cisco Umbrella サービスの停止時間（分単位とし、以下で定義します）を引いた値で除し、これに 100 を乗じて算出します。計算式は、次のとおりです。

可用性 = （X÷ Y）×100 X：暦月中の合計稼働時間数（分単位）

Y：（当該暦月の合計時間（分単位））-（計画的なメンテナンスまたは第三者の行為による停止時間（分単位）の合計）

この計算において、（i）「停止」とは、お客様のインターネット接続が正常であるにもかかわらず Umbrella DNS サービスが完全に到達不能である状況のことをいい、（ii）「稼働時間」とは、計画的なメンテナンスおよび第三者の行為による停止を除く、停止が発生していない時間（分単位）のことをいい、（iii）「第三者の行為」とは、シスコによる合理的な制御が及ばないすべての行為のことをいいます。第三者の行為には、他社が管理しているインターネットネットワークやトラフィック交換点の稼働状況、ストライキ、労働者不足、暴動、反乱、火災、洪水、嵐、爆発、天災、戦争、テロ、行政措置、労働状況、地震、資材不足が含まれますが、これらに限定されません。停止の発生有無に関して争いが生じた場合、シスコは、シスコのシステムログ、監視レポート、および構成記録に基づき、誠実に判断します。お客様の記録とシスコの記録との関係については、シスコの記録を優先します。シスコは、第三者の行為に起因する停止に対する責任を負わないものとします。

3.2. Umbrella SIG

Umbrella SIG の本サービスレベル契約において、「本サービス」とは、Umbrella Secure Internet Gateway（以下「SIG」）Essentials、Umbrella SIG Advantage、および Umbrella SIG for Education クラウドサービスのことをいい、Web ベースのユーザーインターフェイス、ダッシュボード、レポート、およびお客様の Umbrella 管理者が利用できるその他のサービスは含まれません。シスコは、商取引上の合理的な努力を尽くして、各暦月における本サービスの可用性が 99.99 % となるようにし、これを維持します。

可用性は、該当する暦月の合計稼働時間（分単位とし、以下で定義します）を、その月の総分数から計画的なメンテナンスおよび第三者の行為（以下で定義します）に起因する停止時間（分単位とし、以下で定義します）を引いた値で除し、これに 100 を乗じて算出します。計算式は、次のとおりです。

可用性 =（X ÷ Y）X 100

X：暦月中の合計稼働時間（分単位）

Y：（当該暦月の合計時間（分単位））-（計画的なメンテナンスもしくは第三者の行為またはその両方による停止時間（分単位））

「稼働時間」とは、Umbrella の冗長化されたグローバル インフラストラクチャをお客様が活用できるように本サービスが適切に設定されている場合に、お客様が発信したエンド ユーザー インターネット トラフィックを本サービスが受信できる状態であることをいいます。お客様が IPSec トンネルを使用している場合、適切な設定とは、フェールオーバー動作を備えたプライマリトンネルおよびセカンダリトンネルが本サービスに設定されていることを意味します。

「停止」とは、上記のとおり本サービスが適切に設定されているときに、お客様が発信したエンド ユーザー インターネット トラフィックを本サービスが受信できない状況のことをいい、計画的なメンテナンスおよび第三者の行為に起因する停止は含まれません。

「第三者の行為」とは、シスコの合理的な制御が及ばない行為のことをいいます。これには、お客様のネットワークがインターネットトラフィックをシスコに転送できないこと、他社 （ISP など）が管理しているインターネットネットワークまたは他社が管理しているトラフィック交換点の稼働状況、特定の地域でシスコがインターネットトラフィックを処理することを禁止または制限している現地の規制または慣行、不可抗力事由（ストライキ、労働者不足、暴動、反乱、火災、洪水、嵐、爆発、戦争、テロ、行政措置、労働状況、地震、資材不足など）、および本サービスの使用ボリュームまたは使用容量を満たす十分なライセンスをお客様が購入しておらず、これを購入していればサービスレベル目標が満たされていた状況が含まれますが、これらに限定されません。

停止の発生有無に関して争いが生じた場合、シスコは、シスコのシステムログ、監視レポート、および構成記録に基づき、誠実に判断します。顧客の記録とシスコの記録との関係については、シスコの記録を優先します。シスコは、第三者の行為に起因する停止に対する責任を負わないものとします。

4. データ保護

Cisco Umbrella および Cisco SecureX のプライバシーデータシート（こちらに掲載されています）[英語] では、クラウドサービスを提供する過程でシスコが収集および処理する個人データを説明しています。さらに、一部の Umbrella パッケージでは、Cisco Secure Malware Analytics のファイルレピュテーション機能およびファイル分析機能（旧称：AMP エコシステムおよび脅威グリッド）を活用しています。Cisco Trust Portal で入手可能な該当するプライバシーデータシート [英語] をご確認ください。 シスコがあらゆるカテゴリのデータを処理、使用、および保護する方法の詳細については、Cisco's Security and Trust Center のページを参照してください。

5. サポートとメンテナンス

5.1. Umbrella SIG および Umbrella DNS Security のテクニカルサポート

Umbrella SIG および Umbrella DNS Security パッケージにはオンラインサポートおよび電話によるサポートが含まれています。お客様がシスコパートナーから直接サポートを受ける場合を除き、シスコは、これらのパッケージについて、下表に定めるとおり対応します。その際、サービスの問題を解決するために、お客様に情報提供を依頼する場合があります。お客様は、依頼された情報をシスコに提供することに合意し、情報の提供が遅れた場合には問題解決および対応までの時間が遅くなる可能性があることを了解するものとします。

電話サポートでは、Cisco Technical Assistance Center（TAC）が 24 時間 365 日サポートを提供します。お客様は使用方法や問題のトラブルシューティングについて電話で問い合わせできるほか、オンラインツールで Web ケースを送信できます。

シスコ製品に関する有用な技術および一般情報を提供する、Cisco.com へのアクセス、ならびに、シスコのオンライン ナレッジ ベースとフォーラムへのアクセスもできます。なお、シスコによるアクセス制限が随時適用される場合があります。

次の表は、シスコの応答目標をケースの重大度別にまとめたものです。お客様は、前述のパッケージ向けの Enhanced サポートまたは Premium サポートを選択することができます。シスコは、割り当てられたケースの重大度を、以下に示す重大度の定義に合わせて調整する場合があります。

ソフトウェア サポート サービス	Technical Support のカバレッジ	重大度 1 または 2 のケースにおける応答時間目標	重大度 3 または 4 のケースにおける応答時間目標
Enhanced	電話、Web により 24 時間 365 日	30 分以内に応答	2 時間以内に応答
Premium	電話、Web により 24 時間 365 日	15 分以内に応答	1 時間以内に応答

本項には次の定義が適用されます。

応答時間：ケース管理システムでケースが送信されてからサポートエンジニアが連絡するまでの時間を意味します。

重大度 1：Umbrella SIG または Umbrella DNS Security（該当する方）が使用できないか停止している、またはケース送信者の事業運営に致命的または重大な影響が及ぶ状況であることを意味します。ケース送信者とシスコは、この状況を解決するためにフルタイムのリソースを投入します。

重大度 2：Umbrella SIG または Umbrella DNS Security（該当する方）の性能が低下しているか、許容できないソフトウェアの性能によってケース送信者の事業運営の重要な部分に悪影響が及ぶ状況であることを意味します。ケース送信者およびシスコは、事態を解決するために、標準営業時間中にフルタイムでリソースを投入します。

重大度 3：Umbrella SIG または Umbrella DNS Security（該当する方）に障害が発生しているが、ほとんどの事業運営が機能し続けている状況であることを意味します。ケース送信者およびシスコは、事態を解決するために、標準営業時間中にリソースを投入するように努めます。

重大度 4：機能または稼働状況に関する軽微かつ断続的な問題が生じているか、Umbrella SIG または Umbrella DNS Security（該当する方）に関する情報が必要である状況のことを意味します。ケース送信者の業務にはほとんどまたはまったく影響を及ぼしません。ケース送信者とシスコは、要求に応じてサポートまたは情報を提供するために、標準営業時間中にリソースを提供するように努めます。

営業日：クラウドサービスが実施される関連地域内において、1 週間のうちで一般的に営業活動があるものと受け入れられている日を意味します。ただし、現地の休日やシスコが定めた休日は除きます。

現地時間：ヨーロッパ、中東、およびアフリカで提供されているサポートの場合は中央ヨーロッパ時間を、オーストラリアで提供されているサポートの場合はオーストラリアの東部標準時を、日本で提供されているサポートの場合は日本標準時を、それ以外のすべての場所で提供されているサポートの場合は太平洋標準時を意味します。

5.2. Cisco Umbrella DNS Security および Cisco Umbrella SIG 以外のパッケージ向けの Cisco Umbrella テクニカルサポート

Umbrella SIG および Umbrella DNS Security のパッケージである場合を除き、お客様がシスコパートナーから直接サポートを受けていない限り、シスコは、該当する下記のテクニカルサポートレベル、ならびに優先順位および目標応答時間に従って、Cisco Umbrella 向けのテクニカルサポートを提供します。Umbrella SIG および Umbrella DNS Security 以外の Cisco Umbrella のパッケージである場合、組み込み済みの Cisco Umbrella 向けサポートオプションは、以下で説明する Basic レベルになります。

シスコは、割り当てられたケースの重大度または優先順位を、以下の定義に合わせて調整する場合があります。

テクニカルサポートレベル	説明
Basic	電子メールによる連絡のみ オンラインツール（ナレッジベース、フォーラム、ドキュメンテーション、ケースポータル、通知など）へのアクセス
Gold	電子メールによる連絡 オンラインツール（ナレッジベース、フォーラム、ドキュメンテーション、ケースポータル、通知など）へのアクセス P1 要求に対する365 日 24 時間の電話サポート P2 ~ P3 要求に対する 24 時間平日のみの電話サポート（日曜午後 4 時（米太平洋標準時刻）~ 金曜午後 5 時（米太平洋標準時刻））
Platinum	専任のテクニカル・アカウント・マネージャ（TAM） 電子メールによる連絡 オンラインツール（ナレッジベース、フォーラム、ドキュメンテーション、ケースポータル、通知など）へのアクセス P1 要求に対する365 日 24 時間の電話サポート P2 ~ P3 要求に対する 24 時間平日のみの電話サポート（日曜午後 4 時（米太平洋標準時刻）~ 金曜午後 5 時（米太平洋標準時刻））

サポートの優先度	目標対応時間	説明
P1： 停止（可用性 SLA で定義）	電話による要求から 30 分以内 電子メールによる要求から 2 時間以内	シスコは 24 時間 365 日解決に取り組み、問題の解決または合理的な回避策の開発にあたります。
P2： 技術的な問題	1 営業日	お客様のインターネット接続が正しく機能しているときに、クラウドサービスを利用することができても応答が遅い場合には、問題が発生しています。問題には、クラウド サービスの利用にやや影響する、お客様のアカウントに関する技術的な質問や設定の問題が含まれます。シスコは、営業時間中継続して解決に取り組み、問題を解決するか計画を策定して、お客様とシスコの双方が合意するまで対応します。
P3： 情報要求	2 営業日	情報要求には、アカウントに関する質問、パスワードのリセット、機能に関する質問が含まれます。シスコの担当者が応答時に、またはその後の可能な限り早い時点で、解決に取り組むよう割り当てられます。

シスコ製品に関する有用な技術および一般情報を提供する、Cisco.com へのアクセス、ならびに、シスコのオンライン ナレッジ ベースとフォーラムへのアクセスもできます。なお、シスコによるアクセス制限が随時適用される場合があります。