オファー説明書：Cisco Secure Cloud Insights

このオファー説明書（以下「本オファー説明書」）では、Cisco Secure Cloud Insights（以下「クラウドサービス」）について説明しています。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。本オファー説明書もしくは注文書またはその両方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の意味は、本契約に定めるとおりとします。

1. 説明

1.1. Cisco Secure Cloud Insights

Cisco Secure Cloud Insights は、JupiterOne® と連動して市場に投入されたクラウドネイティブのプラットフォームです。これにより、企業が保持する変化の激しいサイバーアセットのすべてについて、詳細な分析情報を得ることができます。また、Cisco Secure Cloud Insights は、マルチクラウド展開（パブリッククラウドおよびプライベートクラウドの両方）に加え、オンプレミス型のインフラストラクチャが混在するハイブリッド環境を監視します。Cisco Secure Cloud Insights は API 主導型であり、エージェントレス統合によって、組織のデジタル環境におけるエンティティ間の設定および相互作用をマッピングするために必要なデータを取り込みます。このような接続された豊富なデータセットは、事前に作成された 550 を超えるクエリを使用して調査し、理解しやすい視覚的なグラフで表示することができます。また、JupiterOne 独自のクエリ言語である J1QL で、ユーザー独自のクエリを簡単に作成することも可能です。作成したクエリは、セキュリティアラートに変換したり、既存のコンプライアンス ベンチマーク（SOC 2 など）を強化するために利用したり、カスタム標準を作成するためにグループ化したりすることもできます。

Cisco Secure Cloud Insights の機能は、クラウドセキュリティ動態管理（CSPM）に関する組織のニーズに対応します。Secure Cloud Insights を使用すると、セキュリティとコンプライアンスのギャップを特定し、ワークフローを自動化し、組織のセキュリティ体制の継続的な監視を維持することにより、増え続ける攻撃から生じる損失を抑えることができます。関係性と相互作用を把握することにより、調査も迅速になり、脅威の封じ込めと対処も容易になります。さらに、アウトバウンド統合によって、アラートを、チケットシステム、電子メールエイリアス、メッセージング アプリケーション、パブリケーション/キューイングサービスにルーティングできます。アラートは、シスコが提供する他のサービス（Cisco Secure Cloud Analytics や Cisco SecureX など）を含む他のサービスとカスタム API を介して共有することもできます。Secure Clouds Insights には CSPM ツールなどがあります。

1.2. Cisco SecureX

お客様の Secure Cloud Insights 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（Cisco SecureX Incident Manager Response または Cisco Threat Response を通じた）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 [英語] をご確認ください。

2. 補足条項

免責事項

ファイル、ネットワーク、およびエンドポイントに侵入し、これらを攻撃する新たな手法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確保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。

3. データ保護

シスコの Cisco Secure Cloud Insights 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。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、シスコの Security and Trust Center のページを参照してください。

4. サポートとメンテナンス

クラウドサービスにはオンラインサポートが含まれています。シスコは、下記の表に記載されているとおりの対応でサポートを実施します。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。

オンラインサポートでは、オンラインツール、電子メール、Web によるケースの送信を通じてのみサポートとトラブルシューティングを利用できます。電話によるサポートは提供されていません。ケースの重大度またはエスカレーション ガイドラインは適用されません。シスコは、送信されたケースに対し、遅くとも翌営業日の標準営業時間内に応答します。

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。

お客様がクラウドサービスとともに本ソフトウェアにアクセスできる場合、シスコは、（i）報告を受けた問題に対する回避策またはパッチ、および（ii）使用許諾済みのバージョンの本ソフトウェアに対するメジャーリリース、マイナーリリース、およびメンテナンスリリースを提供します。いずれも Cisco Software Central で入手可能です。お客様は、報告された本ソフトウェアの問題を修正するために、本ソフトウェアの最新リリースにアップデートすることが必要になる場合があります。

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。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
電話による Basic サポート	電話、Web により 24 時間 365 日	1 時間以内に応答	翌営業日内に応答
Basic サポート（オンラインによるサポートのみ）	Web	翌営業日の標準営業時間内にすべてのケースに応答	

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：クラウドサービスが使用できない、ダウンしている、またはケース送信者の業務に対して深刻なまたは著しい影響を与えてい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：クラウドサービスのパフォーマンスが低下するか、許容できないソフトウェアパフォーマンスによってケース送信者の業務の重要な部分に悪影響が及んでいることを意味します。ケース送信者およびシスコは、この状況を解決するために、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：クラウドサービスに障害が発生しているが、ほとんどの業務が正常に機能している状態を意味します。ケース送信者およびシスコは、この状況を解決するために、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：機能またはパフォーマンスに関する軽微かつ断続的な問題が発生したか、クラウドサービスに関する情報が必要な状態を意味します。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、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。

標準営業時間：TAC コールを処理するそれぞれの Cisco TAC 所在地における現地時間で、営業日の午前 8 時から午後 5 時を意味します。

壊滅的なイベント、外部のサービス拒否（DoS）もしくはその他セキュリティ違反、または運用上のインシデントが原因である場合を含め、予期しないまたは計画外のダウンタイムの期間中、クラウドサービスへのアクセスおよびその使用が一時停止することがあります。