cisco SECURE

オファー説明書：Cisco Security Analytics and Logging

このオファー説明書（以下**「本オファー説明書」**）では、Cisco Security Analytics and Logging SaaS（以下「**SAL SaaS**」または「**クラウドサービス**」）および Cisco Security Analytics and Logging オンプレミス（以下「**SAL OP**」または「**本ソフトウェア**」）**について説明しています。**お客様の本ソフトウェア使用権もしくはクラウドサービス使用権またはその両方には、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。

1. 説明

1.1. Cisco Security Analytics and Logging

Cisco Security Analytics and Logging（以下「SAL」）は、IT 運用を合理化するための Central Log Management（CLM）を提供します。また、SAL には強化された可視性と高度な脅威検出のためにログを分析する機能が追加されています。SAL は Cisco ファイアウォールログ（FTD および ASA）とともに発売され、ネットワークフローログやその他のログ取得先が段階的に含まれるようになりました。さまざまな種類のログが同一のオファー構造によってカバーされています。かかるオファー構造は、ネスト式のライセンス付与モデル（すなわち、下位のライセンスが上位のライセンスの機能にネストされます）を採用しています。ライセンスは次のとおりです。

(a) **Essentials**（旧称：Logging and Troubleshooting（LT））：拡張性の高い一元的なロギングサービス。長期保持オプションを選択できるほか、検索、ファイル管理、ダウンロードなどの高度なビューア制御により詳細な集計が可能です。

(b) **Advantage**（旧称：Log Analytics（LA））：振る舞いモデリング技術を使用して、高度な脅威の有無を確認するためにログを分析するオプション機能。これらの脅威検出アルゴリズムは既存の Cisco Stealthwatch 分析機能を活用しますが、トリガーされるアラートは SAL のログ用にカスタマイズして新たに用意したものです。

(c) **Premier**（旧称：Total Network Analytics（TA））：Cisco Stealthwatch のネイティブなログとログ分析結果を集約し、エンドツーエンドの分析を実現します。

SAL SaaS ライセンスには、ファイアウォールのログを表示する Cisco Defense Orchestrator（CDO）の使用権が含まれています。さらに、Advantage（Log Analytics）と Premier（Total Network Analytics）のライセンスには、高度な脅威検出を実行するための Stealthwatch Cloud（SWC）の使用権が含まれています。SAL SaaS では、CDO および SWC のサブスクリプションを必要としていません。また、SAL でログを取得するファイアウォールデバイスを CDO で管理することは必須ではありません。

同様に、SAL OP ライセンスでは Stealthwatch Enterprise（SWE）の仮想アプライアンスおよび物理アプライアンスを使用しますが、SAL OP のために SWE のフローレートライセンスを別途取得する必要はありません。ただし、SWE については、引き続きフローレートライセンスが必要です。

1.2. Cisco SecureX

お客様の SAL 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 Threat Response としても知られている Cisco SecureX 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。SAL データは SWC もしくは SWE またはその両方におけるアラートのトリガーであるため、かかるアラートは、Stealthwatch の SecureX とのネイティブな統合を使用して SecureX において可視化されます。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. 超過料金

Security Analytics and Logging のライセンスの料金は、1 日あたりのギガバイト（GB） 単位のログの量に基づいて設定されます。SAL SaaS のオファーである場合にのみ、シスコは毎月の超過分を後払いで請求する場合があります。各暦月の末日に、シスコはその月のファイアウォールのイベントログの実際の平均的な 1 日あたりの量を計算し、超過分をお客様に自動的に請求します。たとえば、お客様が 1 日あたり 10 GB のサブスクリプションを購入した場合、お客様が取得できるファイアウォールのイベントログの量は 1 暦月（30 日間）につき 300 GB になります。かかる暦月の末日時点でお客様が 330 GB を使用していた場合、1 日あたりの平均使用量は 330/30 = 11 であり、シスコはその月の超過使用分（1 日あたり 1 GB）の料金をお客様に請求する権利を有するものとします。

2.2. 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および本ソフトウェア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、クラウドサービスおよび本ソフトウェアが、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、クラウドサービスおよび本ソフトウェアの統合先であ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、いかなる表明および保証もしません。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

SAL、CDO、SWE、SWC および 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、Cisco’s 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

Security Analytics and Logging（SaaS）のサブスクリプションには、Basic サポート（オンラインによるサポートのみ）が含まれています。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。

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
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	

Security Analytics and Logging（オンプレミス）のサブスクリプションには、電話サポートとオンラインサポートが付帯する、組み込み済みの Basic SWSS サポートが含まれています。

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
Basic SWSS	Cisco Technical Assistance Center への 24 時間 365 日のアクセス（オンラインおよび電話）	1 時間以内に応答	翌営業日内に応答

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：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。