データ シート
Cisco Public

Digital China Cloud が運用する Cisco Secure Access China

ハイブリッドワーク環境の保護

2025 年 3 月

目次

中国本土は、多くの多国籍企業にとって重要な市場です。多国籍企業にとって、中国におけるプレゼンスの確立は、ビジネスや事業運営における大きなチャンスをもたらすからです。こうしたチャンスは中国国内での事業運営における、またグローバル組織の他の地域との、コラボレーションやハイブリッドワーク環境を取り入れることで生まれます。この複雑な環境で成功するには、オンラインセキュリティを確保し、現地の規制を確実に遵守するソリューションやイノベーションが求められます。

中国向けセキュリティサービスエッジ

セキュリティサービスエッジ（SSE）は、あらゆる組織のハイブリッドワーク戦略の実現に向けた鍵となる要素です。多層防御を提供する SSE はクラウド内の複数のセキュリティ機能を組み合わせ、パブリック SaaS アプリケーション、データセンターやプライベートクラウドのプライベートアプリケーション、インターネット全体などのさまざまなリソースに中国国内のさまざまな場所からアクセスして作業するユーザーを保護します。オフィス、自宅、外出先など、どこで仕事をしていても、エンドユーザーには安全で透過的な体験が保証されます。

お客様のセキュリティ態勢を強化するため、中国における SSE ソリューションには、ポリシーの適用に加えて、優れたユーザー体験、IT の複雑さの軽減、そしてセキュリティの有効性の向上が求められます。それと同時に、組織は規制要件にも対応する必要があります。そのため、組織が従業員の保護と成長目標の達成を両立できるような、規制に準拠したソリューションが不可欠です。

Digital China Cloud が運用する Cisco Secure Access China

Digital China Cloud（DCC）が運用する Cisco Secure Access China は、クラウド提供型セキュリティ SSE ソリューションです。中国本土においてデバイスや接続先を問わず、シームレスかつ透過的でセキュアなアクセスを提供します。コンプライアンスを重視した設計で、グローバルな事業運営と中国のダイナミックな市場との橋渡しを通じて組織を支援します。Cisco Secure Access China は Cisco Secure Access グローバルと同様のメリットをもたらし、SSE に欠かせないコアコンポーネントに加えて、VPN-as-a-Service（VPNaaS）、統合型インライン DLP、侵入防御システム（IPS）、Talos を活用した脅威検出などの拡張機能も備えています。またこれらをシンプルなライセンスと管理プラットフォームで利用できます。このため、中国国内におけるユーザーを保護し、必要なあらゆるリソースやアプリケーションにシームレスにアクセスできるようになります。図 1 を参照してください。

Cisco Secure Access China は、他のシスコやサードパーティベンダーの製品との相互運用を容易にする共通の管理制御、データ構造、およびポリシー管理の機能を備えています。たとえば、Secure Access China では、さまざまな SAML アイデンティティ プロバイダー（IdP）や Active Directory を使用できます。中国の規制された環境で許可されている SD-WAN を含む、シスコの他のサービスとも統合します。

Secure Access China は、セキュリティを強化してリスクを減らし、中国におけるコンプライアンスを確保しつつ IT 運用を簡素化し、ユーザーにスムーズなアクセスを提供して生産性を高めます。

図 1.
Cisco Secure Access China の機能

ユーザーが使いやすい

Secure Access China は、中国国内の、ローミング中の、または出張で中国を訪れるユーザーの体験を効率化します。ユーザーは迅速な認証を通じて目的のアプリケーションにアクセスできるため、生産性が向上し、迂回されがちなセキュリティ手順を確実に実施することでリスクや中断を最小限に抑えられます。また、中国国内においても使い慣れた Cisco Secure Client を使って、接続や認証を行い、目的のアプリケーションに直接移動できます。

中国のセキュア Web ゲートウェイ（SWG）により、従業員はオフィス内でも外出先でも一貫して、安全にインターネットにアクセスできます。すべての Web トラフィックをモニターして脅威から保護し、パフォーマンスを犠牲にすることなくセキュリティを維持できます。Secure Access グローバルと Secure Access China の両方のリージョンに展開して設定した場合、国際ローミングユーザーが中国を訪れると、自動的に Secure Access China を使用して、中国の規制に準拠したユーザーおよびグループのポリシーを適用できます。同様に、中国のユーザーが海外でローミングする場合には、グローバルインスタンスに接続できます。

IT をより簡単に

Cisco Secure Access グローバルの展開により、セキュリティの運用と導入が簡素化され、自動化されます。IT チームは、この機能を活用してポリシー管理を一元化できます。中国のデータ主権とデータローカライゼーションへの厳密なコンプライアンスを確保すべく、Secure Access China は、最優先事項としてこの要件に対応し、大きな損失につながる規制リスク、罰金、そして評判に対して生じうる悪影響の軽減を目指します。Secure Access China の管理では、使い慣れたダッシュボードを使用できるため、トレーニングや管理ツールの使用が簡素化されます。データレポート、アラート、ログは、デフォルトで中国国内で保存されます。その他にも管理者には、お客様が管理する独自のストレージを保存または設定する選択肢もあります。

すべてのユーザーにより安全な環境を

Cisco Secure Access China は、グローバルな多層防御アーキテクチャアプローチに従い、高度なサイバー脅威に対処します。この堅牢なアプローチにより、エンドユーザーは感染したファイル、悪意のある Web サイト、不正な攻撃、そしてフィッシングやランサムウェアなどの一般的な脅威から確実に保護されます。攻撃対象領域が大幅に減少するため、IT チームやセキュリティチームは最小権限による制御を効果的に適用し、組織全体のセキュリティ態勢を強化できます。

Security Access China によって、IT チームは国内のネットワークアクティビティの可視性を高め、放置すれば組織のセキュリティを侵害する可能性のある許可されていないアプリケーションの使用を特定し、ブロックして、データ漏洩を防ぎます。さらなるメリットをもたらし、セキュリティをより一層強化するのが、中国でのネットワーク セグメンテーションと、厳格なアクセス制御や侵入防御などの利用可能な機能を組み合わせた活用です。これにより、内部リソースを効果的に保護し、悪意のある攻撃者がその存在を検出すらできないようにします。このプロアクティブな防御メカニズムは、機密データを保護するだけでなく、事業継続性を維持し、中国独自の規制環境下で業務を管理するための安全で効率的な環境を促進します。

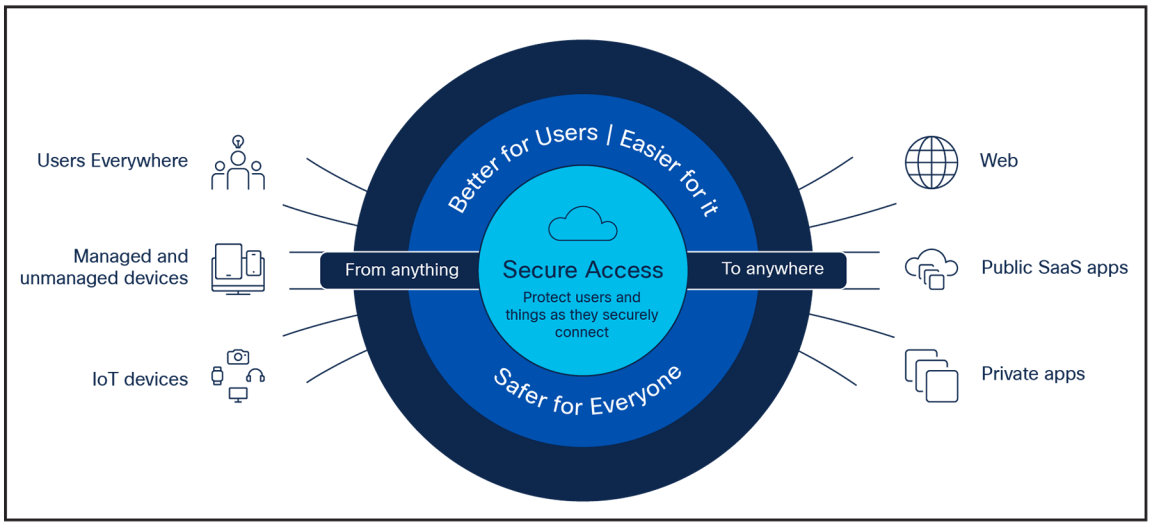

図 2.
デバイスや接続先を問わないセキュアな接続

機能とメリット

表 1. 機能と利点

機能	メリット
VPN-as-a-Service (VPNaaS)	幅広い互換性を備えた仮想プライベートネットワーク（VPN）は、既存のインフラストラクチャや運用を大幅に変更することなく多様な環境に対応できる、実績ある展開の選択肢です。Secure Access China はクラウド提供型 VPN を提供し、Web 以外のインターネットトラフィックへのセキュアアクセスを含む、幅広いリソース、プライベートサーバーへのセキュアアクセスをユーザーに提供します。 • IT の簡素化（ローカル IP プール、複数の VPN プロファイル）。 • SAML、RADIUS、証明書などの複数の認証方式を使用したアイデンティティベースのアクセス制御。 • エンドポイントポスチャ評価により、アクセス制御のきめ細かさが向上します。 • ヘッドエンドまたはトンネルタイプを選択する必要がなく、接続が簡素化されます。 • 機能の例：スプリットトンネリングとトンネルのすべてのサポート、ピアツーピア通信、信頼ネットワーク検出。

機能	メリット
セキュア Web ゲートウェイ（SWG）	すべての Web トラフィック（http/https）をログに記録して検査し、透過性、制御、および保護を強化します。IPsec トンネル、PAC ファイル、プロキシチェーンを使用してトラフィックを転送し、完全な可視性、URL およびアプリケーションレベルの制御、高度な脅威からの保護を実現します。 • ポリシーやコンプライアンス規制に違反する接続先をブロックするための、カテゴリまたは特定の URL によるコンテンツフィルタリング。 • ダウンロードしたファイルをスキャンして、マルウェアやその他の脅威を検出します。 • ファイルタイプごとのブロッキング（例：.exe ファイルのダウンロードのブロック）。 • TLS の全体または一部を復号することで、隠蔽された攻撃や感染から保護します。 • 一部のアプリで特定のユーザーアクティビティをブロックするためのきめ細かなアプリ制御（例：Dropbox へのファイルアップロード、Gmail へのファイル添付、Facebook での投稿/共有）。 • 完全な URL アドレス、ネットワーク アイデンティティ、許可またはブロックされたアクション、外部 IP アドレスが含まれた詳細なレポート。 • カスタマイズ可能な制御とトラフィックパスオプションを備えたインターネットベースの SaaS アプリケーションの保護。
クラウド アクセス セキュリティ ブローカ（CASB）	• 使用中の選択したクラウドアプリケーションを検出、レポート、ブロックします。クラウドの利用を管理し、攻撃的、非生産的、高リスク、または不適切なクラウドアプリケーションの使用をブロックしてリスクを軽減します。 • OAuth ベースの承認から Microsoft 365 や Google のテナントまで、リスクの高いプラグインや拡張機能の承認の検出、ブロック、および取り消しを行います。 • ベンダーカテゴリ、アプリケーション名、検出された各アプリケーションのアクティビティ量に関するレポート。 • Web レピュテーションスコア、財務状態、関連するコンプライアンス認定といったアプリの詳細やリスク情報。 • グループ/個人がアクセスできる SaaS アプリケーションのインスタンスを制御するためのテナント制限。
データ漏洩防止（DLP）	インラインまたはリアルタイムのデータ損失防止（DLP）。データをインラインで分析し、組織外部に流出する機密データを可視化および制御します。より効率的な管理と規制順守のための統合されたポリシーとレポート機能。 • 個人を特定できる情報（PII）に対して 77 か国にまたがる 1,200 を超える組み込みのグローバル識別子を設けて、保護医療情報（PHI）、GDPR、HIPAA、PCI などに準拠。 • オンプレミスの DLP ソリューションとの統合により、イベント管理と修復ワークフローを一元化します。 • カスタムフレーズ（プロジェクト名など）を追加できるユーザー定義のディクショナリ。 機密データの使用状況の検出と報告、および不正使用の特定に役立つドリルダウンレポート。
高度なマルウェア防御	既知のレピュテーションが低いファイルを防止、検出、ブロックします。悪意のあるファイルをエンドポイントに到達する前に検出して修復することにより、セキュリティ保護を強化します。 • セキュリティ管理者の有効性と効率を高めます。 既知のマルウェアエクスプロイトをはじめ、ウイルス、ワーム、トロイの木馬、アドウェアなどの脅威をブロックします。
サービスとしてのファイアウォール（FWaaS） **および** **侵入防御システム（IPS）**	すべてのポートとプロトコルにおいて、インターネット上またはお客様のプライベート インフラストラクチャ上で、ユーザーと接続先/アプリケーション間のトラフィックを完全に可視化し、包括的なセキュリティ制御を可能にします。ローミング中の、または分散拠点のキャンパスネットワークからインターネットやプライベート アプリケーションにアクセスするリモートユーザーが含まれます。 • インターネット、プライベートネットワーク、プライベート アプリケーションにアクセスするユーザー/グループ、ネットワーク、またはデバイスを保護するための L3/4 アクセス制御ルール。 • Snort 3.0 をサポートするカスタマイズ可能な IPS プロファイル。インターネットとプライベートアクセスの両方について、ルールに一致するトラフィックパターンに対してルールごとに IPS 検査を行います。

機能	メリット
	• 特定されるアプリケーションの継続的な増加に基づく、レイヤ 7 アプリケーション、アプリケーションプロトコル、およびポート/プロトコルの可視性と制御。 • 検査の前に、インターネットまたはプライベートアクセスのトラフィックを復号します。 • ユーザーとプライベート アプリケーション間のトラフィックに対する双方向のファイル検査とファイルタイプの制御。 スケーラブルなクラウド コンピューティング リソースにより、アプライアンスのキャパシティに関する問題を解消します。
Talos 脅威インテリジェンス	世界最大の民間の脅威インテリジェンスチームの 1 つである Cisco Talos は、脅威データと分析の膨大なデータベースを有し、サイバー脅威を特定してインシデント対応率を向上させます。
管理およびレポートコンソール	Secure Access China は、インターネット、パブリック SaaS アプリケーション、およびプライベート アプリケーションへのアクセス全般において、インテントベースのルールを使用してセキュリティポリシーの作成と管理を統合します。広範なロギングや、企業のセキュリティ オペレーション センター（SOC）へのログのエクスポート機能を提供します。 • あらゆるユーザーのあらゆるアプリに対するポリシーを一元的に定義。セキュリティポリシーの構築プロセスを簡素化し、中国における組織全体でポリシー定義の一貫性を促進します。 • 統合されたソース（ユーザー、デバイス）と統合されたリソース（アプリケーション、接続先）により、アタッチポイントやアクセスするアプリケーションに関係なく、セキュリティポリシーがユーザーに対応するようになります。 • 進行中のポリシー管理アクティビティを削減します。 • 集約されたレポート作成機能により、可視化と検出までの時間が改善されます。 SOC/セキュリティアナリストの調査プロセス全体を簡素化します。
デバイス サポート	• Cisco Secure Client は Secure Access China に含まれており、追加料金はかかりません。 • インターネットトラフィック、VPNaaS 経由のプライベートトラフィック用の Windows および MacOS 上の Secure Client。 • SWG 保護を備えたローミングユーザー向け Cisco Security。
Catalyst SD-WAN との統合：インターネットまたは SaaS アプリケーションにアクセスするブランチユーザー	Catalyst SD-WAN と Secure Access の統合と自動化により、ブランチユーザーから Web および SaaS アプリケーションへのステアリングを Cisco Secure Access で保護することが可能になります。 • Secure Access のマルチレイヤ セキュリティ ソリューションによる脅威からの保護の強化。 • ブランチの SD-WAN ロケーションと Secure Access 間のトンネルを自動化し、IT の展開を簡素化します。 • ユーザーがローミング場所とオンプレミスの場所の間を移動するときのエクスペリエンスの一貫性が向上します。 • Secure Access の一元化されたポリシー管理、拡張と縮小の容易さ、およびキャパシティの制約からの解放により、IT やセキュリティの運用を簡素化します。

パッケージオプション

Cisco Secure Access China には、Secure Access Essentials と Secure Access Advantage の 2 つの主要な階層があります。どちらの階層も、セキュア インターネット アクセス（SIA）とセキュア プライベート アクセス（SPA）の 2 つのユースケースで使用できます。これらは単一のサブスクリプションの一部として購入され、単一の統合されたダッシュボードとサービスとして提供されます。お客様は、階層でユースケースを一方のみ購入するか両方購入するかを選択できます。次の表に、概要の比較を示します。

表 2. ライセンスパッケージ

カテゴリ	機能	Essentials	Advantage
Secure Access	Secure Internet Access（SIA） ▪ ローミングモジュール（Web） ▪ SD-WAN DIA ▪ Cisco Secure Client VPN ▪ PAC、プロキシチェーン	✓	✓
	Secure Private Access（SPA） ▪ セキュアリモートアクセス（RAVPN） ▪ 国内のブランチ間、RAVPN とブランチ間	✓	✓
基本的なセキュリティ	Web アプリケーションおよびプライベート アプリケーションのレイヤ 3 およびレイヤ 4 制御向け Firewall-as-a-Service	✓	✓
	セキュア Web ゲートウェイ（プロキシ Web トラフィック、URL フィルタリング、コンテンツフィルタリング、高度なアプリ制御）	✓	✓
	CASB クラウドアプリケーションの検出、リスクスコアリング、テナント制御	✓	✓
高度なセキュリティ	レイヤ 7 クラウドファイアウォール		✓
	侵入防御システム（IPS）による保護		✓
	Web アプリケーションのデータ損失防止（DLP）、リアルタイム（インラインのみ）		✓
サポート	階層化されたパートナーおよびシスコサポートが E メールや電話で提供する 24 時間 365 日のソリューションサポートを含む	24 時間 365 日	24 時間 365 日

Cisco Secure Access China ソリューション サポート サービス

Cisco Secure Access China の初回のサポートは、このサービスの運用事業者である DCC が現地において提供します。Cisco TAC サポートチームとのパートナーシップにより、Secure Access China には、ソリューションサポート用に個別の SKU が含まれています。

- DCC チケットポータルや電話サポートによるテクニカルサポート（24 時間 365 日対応）
- シビラティ（重大度）1 および 2 のケースに対する応答時間は 30 分以内
- 中国語のサポート
- 技術的なオンボーディングと導入の支援

その他の情報

詳細については、Cisco Secure Access China をご覧ください。

米国本社
カリフォルニア州サンノゼ

アジア太平洋本社
シンガポール

ヨーロッパ本社
アムステルダム（オランダ）

シスコは世界各国に約 400 のオフィスを開設しています。オフィスの住所、電話番号、FAX 番号は当社の Web サイト（**www.cisco.com/jp/go/offices**）をご覧ください。

Printed in USA

Cxx-xxxxxx-00　03/25