Ivanti Connect Secure: Secure Access VPN for the Everywhere Workplace

概要

今、現代的な働き方はリモートワークであり、最新の職場はオフィスや従来のデータセンターを超えてクラウドへと広がっています。ユーザーが必要とするアプリケーションの数や複雑さが増し、ユーザーが接続に使用するデバイスの種類も増える一方、悪意あるアクターの脅威が絶え間なく迫っているため、Everywhere Workplaceの保護は非常に困難な課題となっています。

Ivanti Connect Secureは、リモートユーザーやモバイルユーザーがいつでもどこでも、あらゆるウェブ対応デバイスから企業のリソースにアクセスできる、シームレスでコスト効率の高いSSL VPNソリューションを提供します。パワフルで使いやすいIvanti Connect Secureは、あらゆる規模の組織、あらゆる主要産業で最も広く導入されているSSL VPNです。

製品説明

企業やサービスプロバイダーは、場所やデバイスに依存しないネットワーク接続を安全に提供し、許可されたユーザーのリソースへのアクセスを制御するという難しい課題を抱えています。侵害と脅威は依然として制御不能な状況になりつつあり、在宅勤務への変革が拡大につれて、オフィス外から接続する従業員やユーザーの数が増え続けています。

Ivanti Secure Access Client

Ivanti Connect SecureにはIvanti Secure Access Clientが含まれています。Ivanti Secure Access Clientは、モバイルおよびPCデバイス向けの動的なマルチサービスネットワーククライアントです。Ivanti Secure Access Clientsは導入が簡単で、ユーザーはどのデバイスからでも、どこからでも、クリックするだけですぐに接続できるようになります。

Ivanti Secure Access Clientは、アプリごとのVPN、オンデマンドVPN接続、常時接続モード、ロックダウンモードをサポートしています。Ivanti Secure Access Clientはまた、フルトンネルとFQDNまたはIP/ネットワークベースのスプリットトンネル接続にも対応しています。

Ivanti Secure Access Clientは、データセンターでもクラウドでも、ユーザーのネットワーク接続を保護します。ユーザーフレンドリーなパッケージの Ivanti Secure Access Clientは、ユーザーのエンドポイントで適切なネットワークとセキュリティサービスを動的に有効にします。Ivantiによって、正常な接続が保たれ、モバイルデバイスが約束する生産性を実現できます。

Ivanti Secure Access Clientは、リモートアクセス（SSL VPN）とローカルアクセス（NAC）をシームレスに切り替えて、ユーザーのデバイス上で動的なアクセス制御を行います。また、Ivanti Clientは、モバイルおよびデスクトップのコンピュータデバイスに対する包括的なエンドポイントのセキュリティポスチャ評価、および必要に応じて隔離と修復を可能にします。

Ivanti Security Appliance

Ivanti Secure Access Clientは、リモートアクセス（SSL VPN）とローカルアクセス（NAC）をシームレスに切り替えて、ユーザーのデバイス上で動的なアクセス制御を行います。また、Ivanti Clientは、モバイルおよびデスクトップのコンピュータデバイスに対する包括的なエンドポイントのセキュリティポスチャ評価、および必要に応じて隔離と修復を可能にします。

アーキテクチャと主要コンポーネント

Ivanti Security Appliance (ISA) は、Ivantiが提供する新世代のアプライアンス製品です。ISAシリーズのアプライアンスはスピードとセキュリティに特化した製品で、SMBからエンタープライズまで、あらゆる組織のニーズに合わせて拡張することができます。ISAシリーズのアプライアンスは、固定構成のラックマウント型ハードウェアとして使用できるほか、仮想アプライアンスとしてデータセンターまたはクラウドに展開することも可能です。ハードウェア、ソフトウェア、カーネルの最適化により大幅にパフォーマンスを向上させた ISAアプライアンスは、ラボテストにおいて同等のPSAシリーズのアプライアンスに比べ、大幅なスループットの改善が確認されました。

Ivanti Connect Secureは、Ivanti Security Appliance（ISA）およびIvanti PSAシリーズのアプライアンスで、以下の通りハードウェアとして、または仮想アプライアンスとして利用することができます。

Ivanti Security Appliance (ISA)シリーズ

- ISA 6000 アプライアンス：固定構成、1Uラックマウントアプライアンス、最大2,500のSSL VPN同時接続ユーザーをサポート
- ISA 8000 アプライアンス：固定構成、1Uラックマウントアプライアンス、最大25,000のSSL VPN同時接続ユーザーをサポート
- 仮想アプライアンス（ISA-Vシリーズ）：VMware ESXi、Microsoft Azure、Amazon Web Services、Google Cloudプラットフォーム
- 仮想アプライアンス（ISA-Vシリーズ）ラインナップ：
  - ISA4000-V: 最大250ユーザーをサポート
  - ISA6000-V: 最大2500ユーザーをサポート
  - ISA8000-V: 最大25,000ユーザーをサポート

Ivanti PSA シリーズ

- PSA3000 アプライアンス：固定構成、1Uラックマウントアプライアンス、最大200のSSL VPN同時接続ユーザーをサポート
- PSA5000 アプライアンス：固定構成、1Uラックマウントアプライアンス、最大2,500のSSL VPN同時接続ユーザーをサポート
- PSA7000 アプライアンス：固定構成、2Uアプライアンス、最大25,000のSSL VPN同時接続ユーザーをサポート
- Virtual 仮想アプライアンス（PSA-Vシリーズ：VMware ESXi、KVM、Microsoft Hyper-V、Microsoft Azure、Amazon Web Service、Open StackFablic、Alibaba Cloud
- 仮想アプライアンス（PSA-Vシリーズ）ラインナップ：
  - PSA3000-V: 最大200ユーザーをサポート
  - PSA5000-V: 最大2,500ユーザーをサポート
  - PSA7000-V: 最大10,000ユーザーをサポート

特徴・メリット

特徴	説明
レイヤ3 SSL VPN	■ きめ細かなアクセスコントロールを備えたデュアルトランスポート（SSL + 暗号ペイロード）によるフルレイヤ3 VPN接続 ■ コンプライアンスに対応した“Always-on VPN with Lockdown Mode” と “VPN Only Access” モード（VPN接続はユーザーの位置情報に基づいて自動的に接続/切断されます） ■ ユーザーログイン後にユーザーベース認証にステップアップできるマシンベースVPN
アプリケーションVPN	■ 特定のアプリケーションから特定の宛先へのトラフィックをトンネリングするクライアント/サーバプロキシアプリケーション ■ 「オンデマンドVPN」と「アプリ単位VPN」によるシームレスでセキュアなユーザーエクスペリエンス
SAML経由のレイヤ7 ウェブシングルサインオン（SSO）	■ エンドユーザーはレイヤ3トンネルを経由してネットワークに認証されると同時に、SAML SSOのサポートにより、ブラウザ経由のウェブアプリケーションアクセスにSSOが可能
条件付きアクセス	■ ネットワークとデータを保護するために、一連の自動化されたポリシーによってデバイスとユーザーを検証し、認証します。それぞれのアクセス試行は動的に評価され、有効なポリシーに基づいてリアルタイムで制御されます。アプリケーションアクセスのきめ細かな制御とゼロトラストの実施を実現
アドバンストユーザーポータル	■ HTML5対応ブラウザから、公開アプリケーションやユーザーが追加したアプリケーションおよびリンクへのセキュアなクライアントレスアクセス ■ ユーザーの役割に応じて動的に生成 ■ Advanced HTML5によるRDP/Telnet/VNC/SSHアクセス ■ Web rewriter/Web Proxy機能内蔵 ■ マルチポータル対応（例：従業員用SSOポータル、受託業者用2FAポータルなど）
洗練されたユーザー体験	■ リモートアクセスからローカルLANアクセスへのスムーズなローミング（Ivanti Policy Secure） ■ 遠隔地や社内からの迅速で安全なアクセスを実現するシングルサインオン（SSO）（Ivanti Cloud SecureおよびIvanti Policy Secureとの統合）
ステートフルエンドポイントのインテグリティと評価	■ 簡単なポリシー定義により、認証前のデバイス評価および修復 ■ Windows（デスクトップおよびモバイル）、MacOS、Apple iOS、Android
柔軟な起動オプション（スタンドアロンクライアント、ブラウザベースの起動）	■ ウェブブラウザまたはデスクトップから直接SSL VPNを簡単に接続可能 ■ 自動接続機能により、マシンの起動時やログオン時にVPN自動接続が可能 ■ VPNオンデマンド機能により、企業内の認証済みアプリケーションへアクセスが必要な場合に、OSの機能を活用してバックグラウンドでシームレスにVPN接続を実施
クラウドセキュリティソリューションに対応	■ クラウドとデータセンターへのアクセスを融合し、次世代ワーカーのためのシームレスなユーザーエクスペリエンスを実現 ■ ハイブリッドDCアクセスに関するコンプライアンスルールの追加機能
事前設定オプション（Windows、Macのみ）	■ 管理者は、エンドユーザーが選択できるゲートウェイをリスト化し、ゲートウェイの展開の事前設定が可能

特徴・メリット

認証オプション	■ 複数のユーザー属性を用いた動的な多要素認証による適応型認証 ■ 管理者はIvantiを導入することで、Windows Hello for Businessによる生体認証のサポート、ハードウェアトークン、スマートカード、ソフトトークン、スマートカード、ソフトトークン、Google Authenticator、ワンタイムパスワード、証明書認証など、さまざまな認証メカニズムを使用してリモートユーザー認証が可能 ■ 管理者は、ユーザー認証をIDプロバイダーと連携するために、どのインターフェース（内部/外部/管理）からAAAトラフィックを送信するか選択可能 ■ OAuth/OpenID Connectのサポートにより、Connect Secure（Relying Partyとして動作）に接続しながら、Google、OKTA、Azure ADなどの標準的なOpenIDプロバイダーと統合可能
VMware HorizonとCitrix XenApp/ XenDesktop VPN	■ VMwareとCitrixの最新バージョンをサポート
きめ細かいSSL暗号設定	■ あらかじめ設定された暗号方式の中から特定の暗号方式を選択することで、安全性の高いコンプライアンスを実現
REST API	■ アプライアンスへのプログラム的アクセスのための包括的なRESTベースのAPI

豊富なアクセス権限管理機能

特徴	説明	メリット
カスタム表記による動的なロールマッピング	■ ネットワーク、デバイス、セッションの属性の組み合わせにより、アクセス可否の決定が可能 ■ セッション単位で属性をダイナミックに組み合わせて、ロールマッピングの決定が可能 ■ MDMとの連携により、デバイスの属性を取得し、アクセス許可の前に適切なポリシー判断を適用	■ 管理者はユニークなセッションごとに目的別にプロビジョニングが可能
NAC（Ivanti Policy Secure）によるSSL VPNフェデレーション	■ ログイン時にSSL VPNのユーザーセッションをNACセッションにシームレスにプロビジョニング ■ セッションデータはSSL VPNとNAC用のIvanti Applianceで共有されるため、こうしたタイプの環境内であれば、ユーザーは1回認証を受けるだけでアクセスが可能 ■ NACプロファイラで発見したデバイスの属性によって、ポリシーやアクセス決定を制御することも可能	■ リモート、ローカルを問わず、ユーザーは1回のログインで、アクセス制御ポリシーで保護された企業リソースにシームレスにアクセスが可能 ■ エンドユーザーの使い勝手が簡素化
RSA Authentication Managerのサポート	■ RSA Authentications Manager 8.1では、リスクベース認証の利用が可能	■ メールアカウントによるもう一つの認証レイヤーオプションを提供
標準規格に基づく内蔵型タイムベースワンタイムパスワード(TOTP)	■ スマートフォンによる多要素認証が可能	■ ユビキタスなスマートフォンを活用し、モバイルアプリでワンタイムパスコードを生成する、費用対効果の高いセルフサービス型の二要素認証メカニズムを展開できます。RFC6238に基づく実装です。
ユーザーごとの複数セッション	■ リモートユーザーは、複数のリモートアクセスセッションの実行が可能	■ リモートユーザーは、ノートパソコンとスマートフォンから同時にVPNアクセスする場合など、複数の認証セッションを同時に開くことが可能
ユーザー履歴の同期	■ 異なるIvantiアプライアンス間で、ユーザーのブックマークなどのユーザー履歴の同期に対応	■ 地域間の移動が多く、異なるIvantiアプライアンス上のIvantiConnectSecureに接続しなければならないユーザーに対して、一貫したエクスペリエンスを提供
モバイルフレンドリーなSSL VPNログインページ	■ Apple iPhone/iPad、Google Android、Nokia Symbianなどのモバイル端末向けにカスタマイズされた定義済みHTMLページを提供	■ モバイルデバイスのユーザーに、シンプルかつ強化されたユーザーエクスペリエンスと、デバイスの種類に応じてカスタマイズされたウェブページを提供
強力な認証とアイデンティティおよびアクセス管理（IAM）プラットフォームとの統合	■ SecurID、Security Assertion Markup Languageのサポート機能 ■ （SAML）標準ベースのSAML v2.0サポート 、および公開鍵基盤（PKI）/デジタル証書 ■ OAuth/OpenID Connect対応	■ 企業の既存の認証方式を活用し、管理の簡素化を支援

管理の容易さ

特徴	説明	メリット
モバイルデバイス管理（MDM）の統合	■ 統合されたレポートとダッシュボードで管理を簡素化 ■ MDMの属性を活用し、よりインテリジェントで一元化されたポリシー作成が可能 ■ IvantiクライアントをiOSおよびAndroidデバイスにMDMベースで透過的に “ノータッチ “での展開が可能	■ MDMへの投資を拡大し、エンドポイントを包括的に可視化させ、追加のモバイルユースケースをサポート
セキュアブラウザ	■ VPNクライアントをインストール/管理/起動することなく、企業内のウェブアプリケーションに安全にアクセスできるモバイルブラウザ	■ ITチームは、モバイルデバイスにVPNを展開し、管理する必要がなくなります。エンドユーザーはVPNの起動に煩わされる必要がありません。いつも通りブラウザーを起動しリソースにアクセスできる、シームレスなエンドユーザーエクスペリエンスを実現します。
ブリッジ認証局（BCA）対応	■ クライアント証明書認証による連携済みPKIのデプロイに対応。ブリッジ認証局は、異なるトラストアンカー（ルート認証局）から発行されたクライアント証明書を相互認証するためのPKI拡張（RFC5280 に規定）です。 ■ 管理者UIでポリシー拡張を設定し、証明書の検証時に適用することも可能	■ 高度なPKIを導入しているお客様が組織やユーザー間でデータやアプリケーションを共有する前に、Ivanti Appliance基準に準拠した厳格な証明書の検証を行えるようになります。
マルチホストネーム対応	■ 1つのアプライアンスから異なる仮想エクストラネットWebサイトをホストする機能	■ サーバーの増設費用を節約 ■ 区分化されたエントリーURLによるユーザーエクスペリエンスの提供 ■ 間接管理費の削減
直感的なダッシュボードデザイン	■ データセンターとクラウドへのエンタープライズアクセスを1つのコンソールで表示、制御できます。	■ 動的な情報とレポートへの素早いアクセス ■ ドラッグ&ドロップ機能でカスタマイズ可能なレイアウト
カスタマイズ可能なユーザーインターフェース	■ フルカスタマイズによるサインオンページの作成	■ 其々のロールに対して個別のデザインを提供し、ユーザーエクスペリエンスの合理化を図ります。
アプリケーションランチャー（AL）	■ 非JAVA系ブラウザへの対応を強化	■ JavaやActive Xをサポートしない最新世代のブラウザ（Apple、Microsoft、Google、Firefoxなど）に対応
Neurons for Secure Access (nSA)	■ Ivanti Connect Secure Deploymentsの集中管理、分析、レポート作成プラットフォーム（オプション） ■ コンフィグ管理、ワンクリックでのアップグレード、一元化されたログ、トラブルシューティング	■ 設定とゲートウェイのライフスタイルを一元管理することで、時間とコストを削減 ■ 強化された行動分析により、問題になる前にリスクのあるユーザーを特定 ■ 複数ノードまたはグローバルに展開されているノードの管理を簡素化

Flexible Single Sign-On (SSO) Capabilities

特徴	説明	メリット
SAMLシングルサインオンによるクラウドやウェブアプリケーションへのアクセス	■ SAML 2.0 ベースの SSO は、Salesforce.com や Google Apps など、現在最も普及している SaaS (Software as a Service) アプリケーションを含むさまざまなウェブアプリケーションに対応 ■ Ivanti Connect Secure Layer 3 VPN トンネルを経由した接続でも SSO 機能を利用できるのは、業界唯一 ■ Ivanti Connect Secure は、SAML アイデンティティプロバイダ（IdP）および SAML サービスプロバイダ（SP）としての展開をサポート	■ ユーザーのウェブおよびクラウドアプリケーションにシングルサインオンし、ユーザーの接続体験を簡素化
Kerberos制約付き委任	■ Kerberos制約付き委任 プロトコルをサポート ■ ユーザーがバックエンドサーバーにプロキシできない認証情報でIvanti Connect Secureにログインすると、ゲートウェイはユーザーに代わってActive Directoryインフラストラクチャからkerberosチケットの取得が可能 ■ このチケットは、セッション中、Ivanti Connect Secureにキャッシュされます。 ■ ユーザーがKerberosで保護されたアプリケーションにアクセスすると、アプライアンスはキャッシュされたKerberos認証情報を使用して、パスワードの入力を要求することなくアプリケーションにログインさせることができます。	■ 固定パスワードの管理が不要になり、管理の手間とコストをの削減を実現
Kerberos SSOとNT LAN Manager (NTLMv2)に対応	■ Ivanti Connect Secureは、ユーザーの認証情報を使用して、KerberosまたはNTLMv2を介して自動的に認証します。	■ ユーザーは異なるアプリケーションにアクセスするたびごとに認証情報を入力する必要がなくなり、ユーザーエクスペリエンスを簡素化することができます。
パスワード管理の統合	■ ディレクトリストア（LDAP、ADなど）のパスワードポリシーと広範囲に統合可能な標準インターフェイス	■ ユーザー認証に既存のサーバーを活用 ■ ユーザーは、Ivanti Connect Secureインターフェースから直接パスワードを管理できます。
ウェブベースSSO基本認証とNTLM	■ 異なるアクセス管理システムで保護されている他のアプリケーションやリソースに、ログイン情報を再入力することなくアクセスできるようにします。	■ ウェブベースやMicrosoftのアプリケーションに複数の認証情報を入力・管理する手間を省くことができます。
ウェブベース、SSOフォームベース、ヘッダー変数ベース、SAMLベース	■ ユーザー名、認証情報、その他お客様が定義した属性を、他の製品の認証フォームやヘッダー変数として引き渡します。	■ ユーザーの生産性を向上させ、カスタマイズされたエクスペリエンスを提供します。
OAuth/OpenID Connect	■ OAuth/OpenID Connect対応で、Connect Secureに接続しながら（Relying Partyとして動作します）、Google、OKTA、Azure ADなどの標準的なOpenIDプロバイダーと統合できます	■ 既存のOAuth環境と統合し、ユーザーIDのフェデレーションを容易にします。

Provision by Purpose

Feature	Description	Benefit
クライアントの保護	■ 単一の統合型リモートアクセスクライアントで、LANアクセスコントロール、ダイナミックVPN機能をリモートユーザーに提供することも可能です。	■ Ivanti Clientでは、VPNやLANアクセスコントロールなど、異なる機能ごとに複数のクライアントを導入・管理する必要がありません。エンドユーザーは、クリックするだけで接続できます。
クライアントレス コアウェブアクセス	■ Outlook Web Access、SharePointなど、現在最も一般的なウェブアプリケーションを含む、さまざまな種類のウェブベースアプリケーションへのアクセスを保護します。 ■ Ivanti Connect Secureでは、EricomなどのWebSocketトランスレータを通して、サードパーティ製のRDP経由によるHTML5へのRemote Desktop Protocol (RDP) アクセスが可能です。	■ さまざまなエンドユーザーのデバイスから最も簡単にアプリケーションやリソースにアクセスできる形態で、極めてきめ細かいセキュリティコントロールのオプションを提供します。 ■ ウェブブラウザのみによる完全なクライアントレス方式
モバイルデバイス向けIPsec/IKEv2対応	■ リモートユーザーは、インターネット鍵交換（IKEv2）VPN接続をサポートするモバイルデバイスから接続できます。 ■ 管理者は、IPsec/IKEv2経由のアクセスに対して、厳密な証明書またはユーザー名/パスワード認証を有効にすることができます。	■ IKEv2をサポートしているが、クライアントがまだ利用できない新しいデバイスのための完全なL3 VPNサポート
仮想デスクトップインフラストラクチャ（VDI）対応	■ VMware View Managerとの相互運用を可能にし、管理者はIvanti Connect Secureで仮想デスクトップを展開できます。	■ VMwareサーバーにホストされた仮想デスクトップへのシームレスなアクセスをリモートユーザーに提供します。 ■ VMware Viewクライアントの動的な配信（動的なクライアントフォールバックオプションを含む）を提供し、ユーザーが仮想デスクトップに接続できるようにします。
ゼロタッチプロビジョニング	■ OpenStackの一元化されたオーケストレーションを使ってPCSを導入します。 ■ 手動でのデータ入力を必要とせず、ローカルDHCPサーバーから初期設定を取得します。 ■ REST APIによる設定と管理。	■ ActiveSyncを介して、社員、受託業者、パートナーなど多くのユーザーが 携帯電話から企業のリソースにアクセスできるようにします。
ActiveSync Proxy	■ クライアントソフトウェアをインストールする必要なく、モバイルデバイス（iOS や Android デバイスなど）からプロキシ経由で Exchange サーバーへのセキュアなアクセス（強力な暗号化 + 証明書認証）を可能します。最大 5,000 の同時セッションが可能です。	■ 企業やサービスプロバイダーは、場所やデバイスに依存しないネットワーク接続を安全に提供し、許可されたユーザーのリソースへのアクセスを制御するという難しい課題を抱えています。侵害と脅威は依然として制御不能な状況になりつつあり、在宅勤務への変革が拡大につれて、オフィス外から接続する従業員やユーザーの数が増え続けています。
Secure Application Manager (SAM)	■ 軽量なアプリケーションのダウンロードで、クライアント/サーバーアプリケーションへのアクセスを可能にします。	■ ウェブブラウザのみでクライアント/サーバーアプリケーションにアクセスできます。また、プリインストールされたクライアントを必要とせず、ターミナルサーバーアプリケーションへのネイティブなアクセスも提供します。

Ivantiについて

Ivantiは「Everywhere Workplace（場所にとらわれない働き方）」を実現します。場所にとらわれない働き方により、従業員は多種多様なデバイスでさまざまなネットワークからITアプリケーションやデータにアクセスし、高い生産性を保つことができます。Ivanti Neurons自動化プラットフォームは、業界をリードする統合エンドポイント管理、ゼロトラストセキュリティと、エンタープライズサービス管理のソリューションをつなぎ、デバイスの自己修復および自己保護、またエンドユーザーのセルフサービスを可能にする統合ITプラットフォームを提供します。Fortune 100の96社を含む40,000社以上の顧客が、クラウドからエッジまでIT資産の管理、検出、保護、サービスのためにIvantiを選択し、従業員があらゆる場所にいても作業できる優れたユーザー体験を提供しています。詳細については、www.ivanti.co.jp をご参照ください。

ivanti

ivanti.co.jp
+81 (0)3-6432-4180
contact@ivanti.co.jp