データシート

Zscaler Internet Access

すべてのユーザー、アプリ、場所のための AI 活用型の保護

Zscaler Internet Access™ は、業界で最も包括的なゼロトラスト プラットフォームを使用して、インターネットと SaaS への安全で高速なアクセスを定義します。

クラウドファースト、モバイルファーストの環境に十分対応できない従来のネットワーク セキュリティ

従来のハブ&スポーク アーキテクチャーは、ユーザーが主に本社や支店で作業し、アプリケーションが企業のデータ センターにのみ存在し、かつ攻撃対象領域が組織の承認を得た範囲に限定されていた場合においては効果的でした。しかし現在、脅威の環境は劇的な変化を遂げ、ランサムウェアや暗号化された脅威、そしてサプライ チェーン攻撃などの高度な脅威が従来のネットワーク防御を突破できるようになっています。このような状況の今だからこそ、リスクと複雑性を総合的に削減しながら、ビジネス イニシアチブを柔軟に推進するクラウド ネイティブなセキュリティ ソリューションの導入が求められているのです。

Zscaler Internet Access

クラウドファースト、モバイルファーストを推進する現代の企業を保護するには、ゼロトラストの原則に基づいて構築された根本的に異なるアプローチが必要です。Zscaler Zero Trust Exchange™ の一部である Zscaler Internet Access は、世界で最も導入されているセキュリティ サービス エッジ (SSE) プラットフォームである、セキュア Web ゲートウェイのリーダーとして培った 10 年以上の経験を基に構築されています。

主なメリット：

- **AI によるサイバー脅威とデータ流出の防止：**AI を活用したサイバー脅威対策とデータ保護サービスが高度な脅威から組織を保護します。このサービスは、世界最大 のセキュリティ クラウドが提供する1 日あたり 300 兆の 脅威シグナルから得られるリアルタイムのアップデート によって強化されています。
- **卓越したユーザー エクスペリエンスの実現：**インターネットとSaaS の世界トップクラスの高速エクスペリエンス (従来のセキュリティ アーキテクチャーに比べ最大40%高速) が、生産性を高め、ビジネスの敏捷性を向上させます。
- **セキュリティ アーキテクチャーの近代化：**コストが高く、複雑で低速なアプライアンスの 90% を Zscaler のクラウドネイティブなゼロトラスト プラットフォームに置き換えることで、139%のROIを達成できます。

世界最大のセキュリティ クラウドから配信されるスケーラブルな SaaS プラットフォームが、従来のネットワーク セキュリティ ソリューションを排除すると同時に、包括的なゼロトラスト アプローチで高度な攻撃を阻止し、データ流出を防ぎます。主な特長として、次の 4 つが挙げられます。

現代のハイブリッドな働き方を支えるトップクラスの一貫したセキュリティ：セキュリティをクラウドに移行することで、すべてのユーザー、アプリ、デバイス、場所が、アイデンティティーとコンテキストに基づいて常に脅威から保護されるようになります。また、ユーザーがどこにいてもセキュリティ ポリシーが適用されます。

物理的なインフラを必要としない高速アクセス：クラウドに直接接続するアーキテクチャーにより、高速でシームレスなユーザー エクスペリエンスが実現します。また、バックホールの排除、パフォーマンスやユーザー エクスペリエンスの向上、ネットワーク管理の簡素化が可能になります。物理的なインフラは一切必要ありません。

世界最大のセキュリティ クラウドが提供する AI 活用型の保護：SSL 復号されたものも含め、すべてのインターネットおよび SaaS トラフィックにインライン検査を実施します。毎日 300 兆のシグナルを受信する脅威インテリジェンスに基づき、AI を活用した一連のクラウド セキュリティ サービスでランサムウェア、フィッシング、ゼロデイ マルウェアやその他の高度な攻撃を阻止します。

管理の簡素化：AI を取り入れたクラウド ネイティブなセキュリティ ソリューションのため、管理が必要なハードウェアは一切ありません。また、効率的なワークフローやビジネスを中心としたポリシーにより、担当部門は戦略的目標に集中する時間を確保できるようになります。

AI 活用型の統合セキュリティとデータ保護サービス

Zscaler Internet Access には、サイバー攻撃やデータ流出を阻止する AI 活用型の包括的なセキュリティとデータ保護サービスが含まれています。100% クラウド型の SaaS ソリューションであるため、ハードウェアを追加したり、導入までに時間をかけたりすることなく、最新機能を追加できます。Zscaler Internet Access の一部として利用できるモジュールは、次のとおりです。

- **クラウド セキュア Web ゲートウェイ (SWG):** AI を活用したリアルタイムの分析と URL フィルタリングで、ランサムウェア、マルウェアなどの高度な攻撃を排除し、安全で高速な Web エクスペリエンスを提供します。2020 年 Gartner MQ for SWG でリーダーと評価されたベンダーは、Zscaler のみです。
- **クラウド アクセス セキュリティ ブローカー (CASB):** 統合された CASB でクラウド アプリを保護すると同時に、SaaS や IaaS 環境全体でデータを保護し、脅威を阻止しながらコンプライアンスに準拠します。
- **クラウド情報漏洩防止 (DLP):** 完全なインライン検査や完全データ一致 (EDM)、光学式文字認識 (OCR)、機械学習などの高度な手法を使用して、転送中のデータを保護します。

- **Zscaler Firewall とクラウド IPS:** 業界をリードする保護をすべてのポートとプロトコルに拡張し、エッジや拠点のファイアウォールをクラウド ネイティブ プラットフォームに置き換えます。
- **Zscaler Sandbox:** AI 活用型の検疫により、未確認や回避型のマルウェアを Web およびファイル転送プロトコル全体にわたって阻止し、すべてのユーザーに一貫したグローバルな保護をリアルタイムで適用します。
- **AI 活用型のクラウド ブラウザー分離：**ユーザー、Web、SaaS の間に仮想のエア ギャップを作成することで、Web ベースの攻撃を無効化し、データ流出を防ぎます。
- **デジタル エクスペリエンス モニタリング：**アプリケーション、クラウド パス、エンドポイント パフォーマンスのメトリクスを一元的に表示させることで分析とトラブルシューティングを効率化し、IT 運用のオーバーヘッドの削減とチケット解決の高速化を可能にします。
- **拠点向けゼロトラスト接続：**ユーザー、サーバー、IOT/OT デバイスに拠点またはデータ センターのルーティング不可能な接続を使用することで、リスクや複雑性を軽減します。
- **DNS セキュリティ：**場所に左右されることなく、すべてのポートおよびプロトコルで、あらゆるユーザー、デバイス、アプリケーションの DNS セキュリティとパフォーマンスを最適化します。

ユーザーとワークロードのための Zscaler Internet Access

Zscaler Internet Access は、あらゆるインターネットや SaaS の宛先にアクセスするクラウド ワークロードのリスクを排除します。ワークロードがインターネットにアクセスする際に、VPN、ファイアウォール (仮想ファイアウォールを含む)、WAN テクノロジーなどの従来のネットワーク中心のツールを経由する必要がなくなるため、個別のセキュリティ ツールを追加することなく侵害やラテラル ムーブメントを防止できます。ZIA の包括的なセキュリティとデータ保護機能をワークロードに適用することで、ユーザーとワークロードのゼロトラスト セキュリティを単一の統合プラットフォームで実現できるようになります。

また、ZIA を Zscaler Private Access と組み合わせることで、プライベート アプリやワークロードの場所 (パブリック クラウドまたはプライベート データ センター) に左右されることなく、すべてに対して保護を拡張できます。

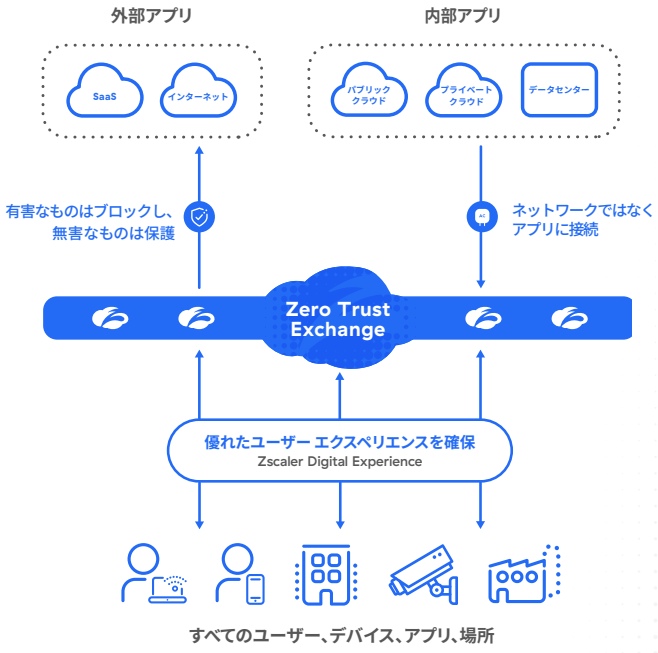

図 1: Zero Trust Exchange

ユース ケース

サイバー脅威対策とランサムウェア対策

従来のネットワーク セキュリティから Zscaler の革新的なゼロトラスト アーキテクチャーに移行することで、侵害の防止、攻撃対象領域の排除、ラテラル ムーブメントの阻止、データの保護が可能になります。

詳細はこちら →

ハイブリッド ワークの保護

従業員、パートナー、顧客、サプライヤーが、あらゆる場所やデバイスから Web アプリケーションやクラウド サービスに安全にアクセスでき、優れたデジタル エクスペリエンスを得られる環境を確保します。

詳細はこちら →

データ保護

偶発的な外部公開、データの盗難、二重脅迫型ランサムウェアなどを阻止し、ユーザーや SaaS アプリ、パブリック クラウド インフラからのデータ流出を防止します。

詳細はこちら →

インフラの近代化

エッジや拠点のファイアウォールを必要としない高速で安全なクラウドへの直接接続により、コストのかかる複雑なネットワークを排除します。

詳細はこちら →

Zscaler Zero Trust Exchange のエコシステム

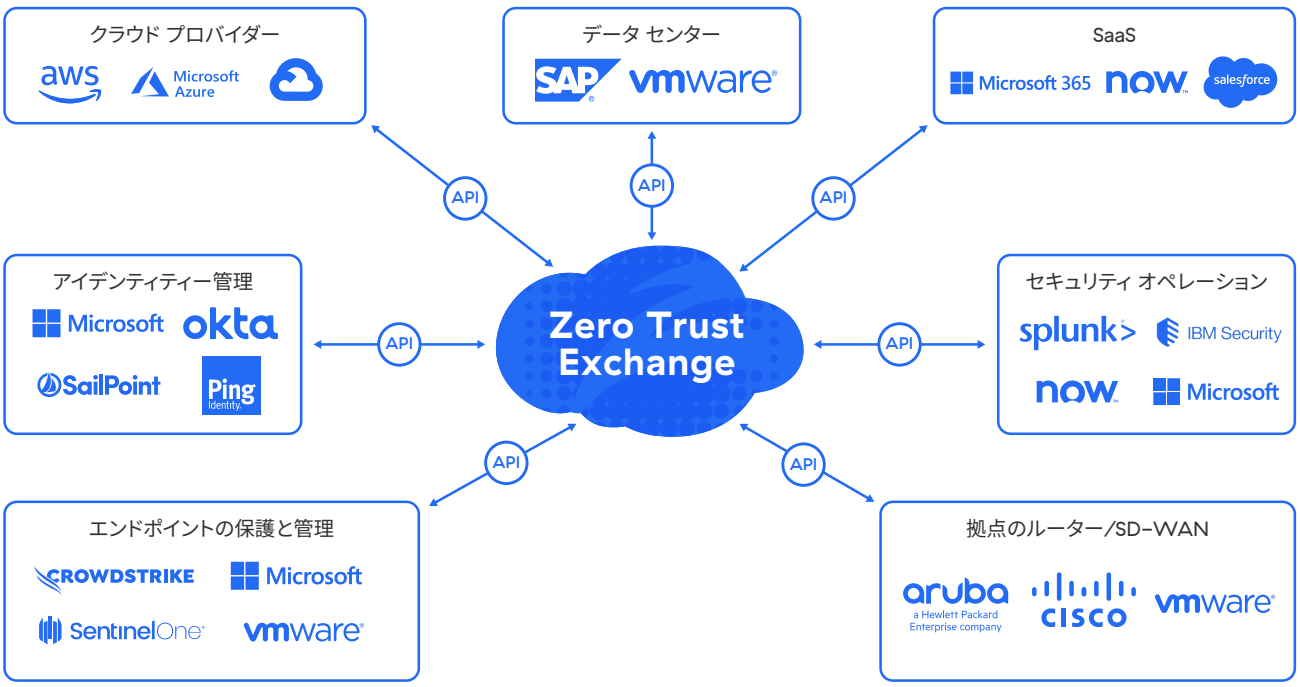

図 2: Zscaler Internet Access のパートナー エコシステム

表 1: ZSCALER INTERNET ACCESS の特長と機能	
特長	**詳細**
機能	
URL フィルタリング	指定された Web カテゴリーや接続先へのユーザー アクセスを許可、ブロック、警告、または分離することで、Web ベースの脅威を阻止し、組織のポリシーに対するコンプライアンスを確保します。
SSL インスペクション	無制限の TLS/SSL トラフィック検査を行い、暗号化されたトラフィックに潜む脅威とデータ流出を特定します。また、プライバシーや規制の要件に基づいて、検査する Web カテゴリーやアプリを指定することもできます。
DNS セキュリティ	不審なコマンド&コントロール接続を特定し、Zscaler の脅威検知エンジンにルーティングして、コンテンツ全体を完全に検査します。
ファイル制御	アプリ、ユーザー、ユーザー グループに基づいて、アプリケーションへのファイルのダウンロード / アップロードをブロックまたは許可します。
帯域幅制御	帯域幅のポリシーを適用することで、ビジネスクリティカルなアプリケーションが業務に関係のないトラフィックより優先されるようにします。
高度な脅威対策	マルウェア、ランサムウェア、サプライ チェーン攻撃、フィッシングなどの高度なサイバー攻撃を独自の高度な脅威対策で阻止します。また、組織のリスク許容度に基づいて、ポリシーを詳細に設定することもできます。
データのインライン保護 (転送中データが対象)	フォワード プロキシと SSL 検査機能により、危険な Web の接続先やクラウドアプリへの機密情報の流れをリアルタイムで制御し、データに対する内部および外部からの脅威を阻止します。加えて、アプリが承認されているか管理されていないかどうかを問わず、ネットワークデバイスのログを必要とせずに高度なインライン保護を提供します。
帯域外データの保護 (保存データが対象)	API 統合を使用して、SaaS アプリやクラウド プラットフォーム、そしてそれらのコンテンツをスキャンし、保存されている機密データを識別してリスクの高い共有や外部共有などを取り消すことで自動修復を行います。
侵入防止	ボットネット、高度な脅威、ゼロデイ脅威から完全に保護しながら、ユーザー、アプリ、脅威に関するコンテキスト情報を取得します。クラウド IPS および Web IPS は、ファイアウォール、サンドボックス、DLP、CASB 間でシームレスに機能します。
動的なリスクベースのアクセスとセキュリティ ポリシー	セキュリティとアクセスのポリシーをユーザー、デバイス、アプリケーション、コンテンツのリスクに自動的に適応させます。
Traffic Capture	シームレスなパケット キャプチャー：Zscaler のポリシー エンジン内の特定の基準によって、トラフィックを簡単に復号してキャプチャーし、アプライアンスを追加することなく、効率的なセキュリティ フォレンジックを支援します。
マルウェア分析	高度な AI/ML で悪意のあるインラインのペイロードに潜む未知の脅威を検出、防止、隔離することで、脅威の感染源からの攻撃を阻止します。
DNS フィルタリング	既知および悪意のある接続先に対する DNS リクエストを制御、ブロックします。
Web 分離	アクティブ コンテンツを無害なピクセル データとしてエンド ユーザーのブラウザーにストリーミングすることで、Web ベースの脅威を無効化します。
関連付けされた脅威に関するインサイト	コンテキスト化および関連付けされたアラートには脅威スコアや影響を受ける資産、重大度などに関する情報が含まれており、調査と対応にかかる時間を短縮できます。
アプリケーションの分離	機密データの流出を防ぐために、コピー / 貼り付け、アップロード / ダウンロード、印刷などのユーザー操作をきめ細かく制御することで、管理対象外のデバイスが SaaS、クラウド、プライベート アプリに安全かつエージェントレスにアクセスできるようにします。
デジタル エクスペリエンス モニタリング	アプリケーション、クラウド パス、エンドポイント パフォーマンスのメトリクスを一元的に表示させることで、分析とトラブルシューティングを効率化します。
拠点向けゼロトラスト接続	Zero Trust Exchange を通じて拠点の接続を近代化することで、攻撃対象領域を排除し、ラテラル ムーブメントを防止します。
ワークロードとインターネット間の通信の保護	ワークロードとインターネット間の通信における侵害を防止し、ラテラル ムーブメントを阻止します。すべての通信に対して SSL インスペクション、IPS、URL フィルタリング、データ保護が行われます。
IoT デバイスの可視化	自動検出、継続的なモニタリング、業界をリードする自動ラベル付け機能を備えた AI/ML 分類により、ビジネス全体の IoT デバイス、サーバー、管理対象外ユーザーのデバイスをすべて把握します。

特長	詳細
プラットフォームの特長	
柔軟な接続オプション	• **Zscaler Client Connector (ZCC):** Windows、macOS、iOS、iPadOS、Android、Linux をサポートする軽量エージェントを介して、Zero Trust Exchange にトラフィックを転送します。 • **GRE または IPsec トンネル：**ZCC がインストールされていないデバイスを対象に、GRE および / または IPsec トンネルを使用して Zero Trust Exchange にトラフィックを送信します。 • **ブラウザー分離：**統合されたクラウド ブラウザー分離により、BYOD または管理対象外のデバイスをシームレスに接続します。 • **プロキシ チェーン：**Zscaler は、特定のプロキシ サーバーから別のプロキシ サーバーへのトラフィック転送をサポートしますが、本番環境では推奨しません。 • **PAC ファイル：**ZCC がインストールされていないデバイスを対象に、PAC ファイルを使用して Zero Trust Exchange にトラフィックを送信します。
クラウド型の展開	ZIA は、SaaS サービスとして提供される 100% クラウドネイティブなプラットフォームです。組織固有のユース ケースにも対応できるよう、Private Service Edge や仮想サービス エッジも使用できます。
データ プライバシーとデータ保持	データをログに記録する際、コンテンツがディスクに書き込まれることはなく、記録が行われる場所を決定するための制御をきめ細かく行います。ロールベースのアクセス制御 (RBAC) を使用して、読み取り専用アクセス権の付与、ユーザー名の匿名化 / 難読化、部門や役割に応じたアクセス権の付与を主要なコンプライアンス規制に従って行います。 データは製品に応じて、6 か月 (またはそれ以下) のローリング期間にわたって保持されます。 追加ストレージを購入することで、必要な期間にわたってデータを保持することもできます。
主要なコンプライアンス認証	次の認証を取得しています。 • FedRAMP • ISO 27001 • SOC 2 Type II • SOC 3 • NIST 800-63C コンプライアンス認証の一覧はこちらを参照してください。
きめ細かな API サポート	Zscaler は多くのアイデンティティー、ネットワーキング、セキュリティ ベンダーとの間で REST API 統合を維持しています。例えば、Zscaler と組織で採用しているクラウドベースまたはオンプレミスの SIEM (Splunk など) との間でログを共有することもできます。 詳細はこちら
ダイレクト ピアリング	主要なインターネットおよび SaaS プロバイダーやパブリック クラウドの接続先とのダイレクト ピアリングにより、可能な限り最速のトラフィック パスを確保します。
サービス レベル アグリーメント (SLA)	
可用性	99.999% (失われたトランザクションによる測定値)
プロキシのレイテンシー	100 ミリ秒以下 (脅威スキャンおよび DLP スキャンが有効な場合を含む)
ウイルスの特定	既知のウイルスやマルウェアすべて
サポートするプラットフォームとシステム	
Client Connector	サポート対象は次のとおりです。 • iOS 9 以降 • Android 5 以降 • Windows 7 以降 • macOSX 10.10 以降 • CentOS 8 • Ubuntu 20.04 詳細はこちら
Branch Connector	サポート対象は次のとおりです。 • VMware vCenter または vSphere Hypervisor • Centos • Redhat

Zscaler Internet Access のエディション

	ZIA Essentials エディション	ZIA Business エディション	ZIA Transformation エディション	ZIA Unlimited エディション
プラットフォーム サービス	コンテンツ フィルタリング インライン AV、TLS/SSL インスペクション、Nanolog ストリーミング	(+) SSL プライベート証明書	(+) クラウド NSS、NSS ログの復旧、データセンターへの拡張アクセス、IPSec トンネル、コンテキスト アラート、ZIA 仮想 Private Service Edge (8)	(+) ソース IP アンカリング、テスト環境、優先順位の分類、ZIA 仮想 Private Service Edge (32)、サーバーと IoT の保護 (1GB/10 ユーザー)
高度な脅威対策 (AI 活用型のフィッシングと C2 検出など)	✓	✓	✓	✓
AI 活用型の検疫を備えたクラウド型サンドボックス	アドオン	アドオン	✓	✓
AI を活用したリスクベースの分離	アドオン	アドオン	Standard (100MB/ユーザー/月)	Advanced Plus (150OMB/ユーザー/月)
関連付けされた脅威に関するインサイト	—	✓	✓	✓
動的なリスクベースのポリシー	—	—	✓	✓
統合デセプション	—	—	Standard (最低 1000の ZIAライセンスが必要)	Standard (最低 1000の ZIAライセンスが必要)
DNS 解決とフィルタリング	最大 64 ルール	最大 64 ルール	✓	✓
DNS トンネル検出	—	—	✓	✓
帯域幅コントロール	—	✓	✓	✓
クラウド ファイアウォール	ネットワーク、アプリケーション サービス、ロケーション、FQDN (最大 10 ルール)	ネットワーク、アプリケーション サービス、ロケーション、FQDN (最大 10 ルール)	(+) さまざまな場所で働くユーザー、ロケーション、アプリケーションのディープ パケット インスペクション	(+) さまざまな場所で働くユーザー、ロケーション、アプリケーションのディープ パケット インスペクション
認証されていないトラフィックの保護	0.5GB/ユーザー/月	1GB/ユーザー/月	1.5GB/ユーザー/月	2GB/ユーザー/月
クラウド アプリ制御とテナント制限	✓	✓	✓	✓
SaaS アプリの分離	アドオン	アドオン	Standard (100MB/ユーザー/月)	Advanced Plus (150OMB/ユーザー/月)
情報漏洩防止、CASB、Inline Web Essentials、SaaS API (1 アプリ)	—	Data Protection Standard (DLPおよびCASB Essentials)	(+) SaaS API レトロ スキャン	✓
SaaS API、App Total、管理対象外のデバイス、分類、インシデント管理	アドオン	アドオン	アドオン	✓
デジタル エクスペリエンス モニタリング	—	Standard	Standard	Standard
Premium Support Plus	アドオン	アドオン	アドオン	✓

ライセンス モデル

Zscaler Internet Access のすべてのエディションは、ユーザーごとの料金です。エディション内の一部の製品については、ユーザー数以外で価格が異なる場合があります。料金設定の詳細は、Zscaler の担当者までお問い合わせください。

包括的な Zero Trust Exchange の一部

Zero Trust Exchange は高速で安全な接続を可能にし、インターネットを企業ネットワークとして利用することで、場所を問わない働き方を実現します。また、ゼロトラストの原則である最小特権アクセスに基づき、コンテキストベースのアイデンティティーとポリシー施行を用いて包括的なセキュリティを提供します。

> 「企業がランサムウェア攻撃を受けた場合、身代金の支払い以外にも、環境内の膨大なシステムが使用できないという深刻な事態に陥ります。このような事件がニュースになると、心配した経営層から確認の連絡が入りますが、AutoNation の体制は万全だと胸を張って言えます」
>
> **Ken Athanasiou 氏**、VIP 兼 CISO、AutoNation

zscaler™ | Experience your world, secured.™

Zscaler について

Zscaler (NASDAQ: ZS) は、より効率的で、俊敏性や回復性に優れたセキュアなデジタル トランスフォーメーションを加速しています。Zscaler Zero Trust Exchange は、ユーザー、デバイス、アプリケーションをどこからでも安全に接続させることで、数多くのお客様をサイバー攻撃や情報漏洩から保護しています。世界 150 拠点以上のデータ センターに分散された SSE ベースの Zero Trust Exchange は、世界最大のインライン型クラウド セキュリティ プラットフォームです。詳細は、**zscaler.jp** をご覧いただくか、Twitter で **@zscaler** をフォローしてください。

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.jp