データ シート

Zscaler Zero Trust Device Segmentation

脅威のラテラル ムーブメント対策を簡素化し、拠点や工場のネットワークを保護

デバイス セグメンテーションは、Zscaler Zero Trust Networking の中核となる機能です。この機能によって、脅威のラテラル ムーブメントが企業ネットワークで発生する原因が解消されるため、IT 部門はリスクの軽減、コンプライアンスの確保、ビジネスの稼働時間の向上などをすべて実現できます。

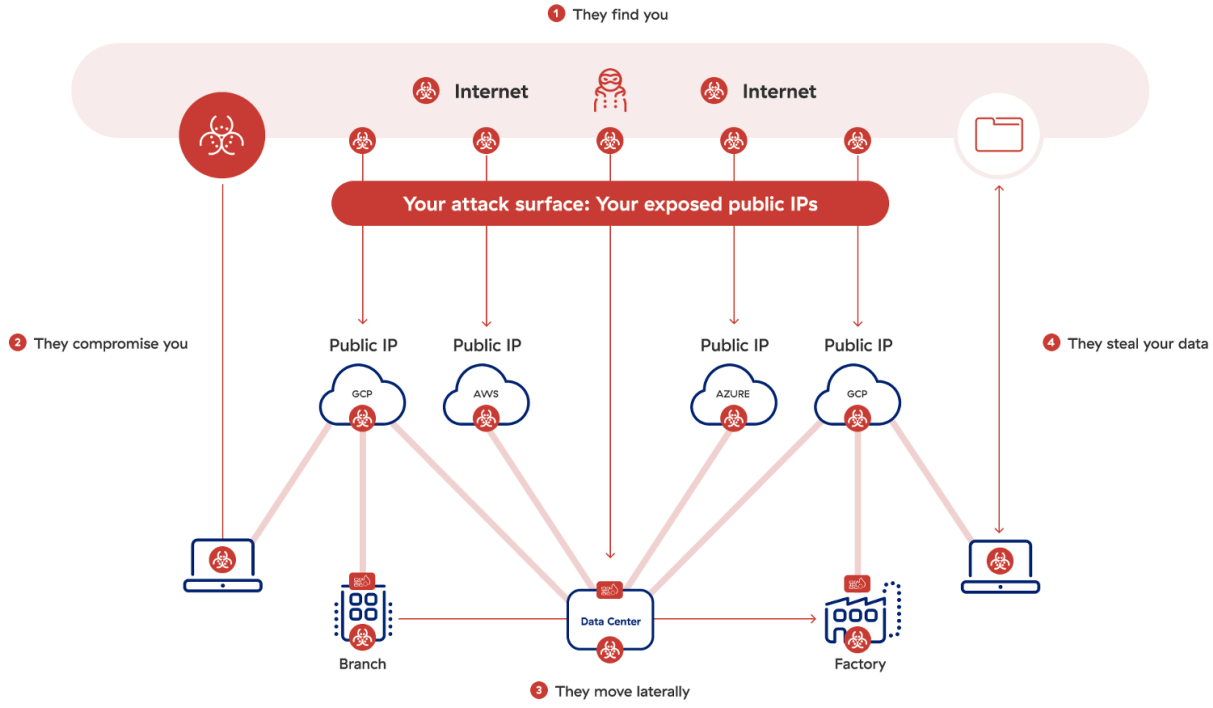
高度化する脅威とコンプライアンスの課題

国家支援型の脅威アクターによる、米国の重要インフラへのサイバー攻撃に関する注意喚起や警告が急増しています。2024 年 2 月 7 日、連邦捜査局 (FBI)、サイバーセキュリティ インフラストラクチャー セキュリティ庁 (CISA)、国家安全保障局 (NSA) は政府機関に向けて合同で警告を発し、交通システムや石油天然ガス パイプライン、水処理プラント、電力網などの重要インフラを混乱させようとしている脅威アクターについて言及しました。この警告は、空港、航空機運航会社、鉄道のセキュリティを確保するために TSA が講じた同様の措置や、最近の DOE サイバーセキュリティ ベースライン、および CIP-015-1 のほぼ最終的な NERC 更新を補完するものです。

OT/IoT テクノロジーは、スピードとトランザクションの効率性を第一に考えるように設計されており、セキュリティへの対応は後回しになっているのが実状です。OT/IoT は現在、サイバー犯罪者の格好の攻撃対象となっており、Zscaler ThreatLabz の調査でも、これらを対象とした攻撃が前年比で 400% 増加していることがわかっています。中でもランサムウェア攻撃は最も頻繁に発生しており、侵害全体の 61% が OT に接続された組織を標的にしています。

Zscaler Zero Trust Networking

ユーザー、デバイス、ワークロードが通信するための、よりシンプルで安全、かつ費用対効果の高い手段



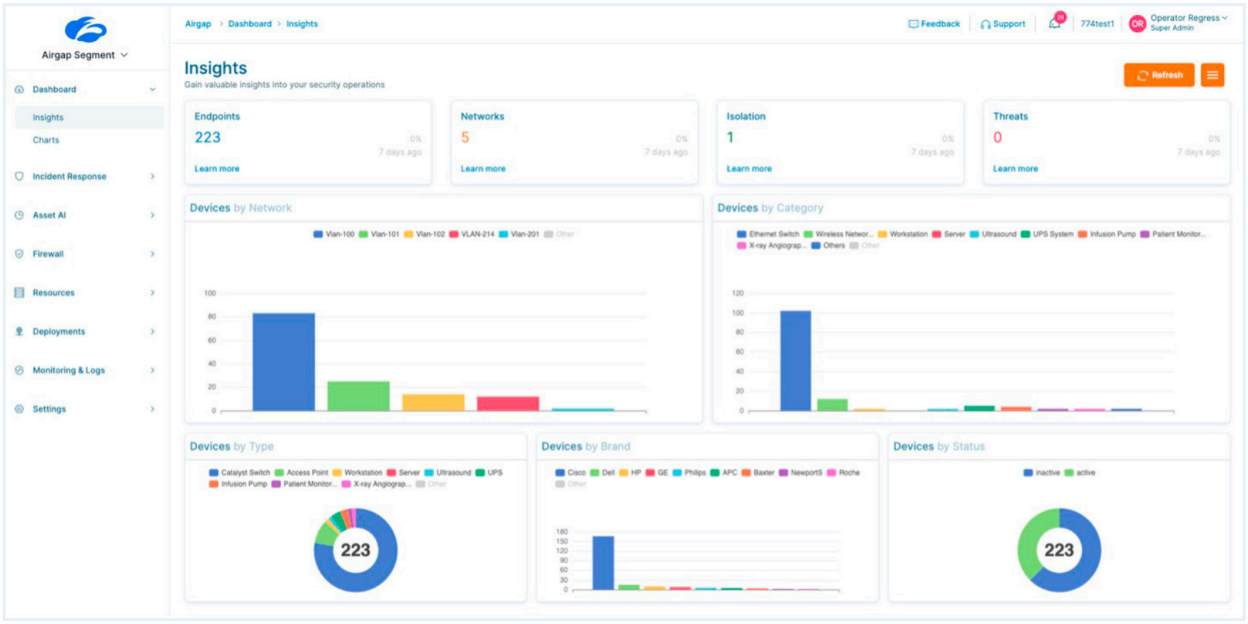
ランサムウェア攻撃の仕組み

EPA、CISA、FBI はシステム オペレーターに対し、サイバーセキュリティを強化するための指針としてゼロトラストを採用するよう求めた大統領令に従い、取り組みを実施することを強く推奨しています。以下の項目はこの推奨事項の中でも特に重要な要素です。Zscaler Zero Trust Device Segmentation を採用することで、これらの領域にすぐに対処できます。

- インターネットへの露出の削減
- 脆弱性への露出の削減
- ネットワーク セグメンテーション
- ログの収集
- 許可されていないユーザーによる接続の禁止
- 悪用されるリスクがあるインターネット上のサービスの廃止
- OT/IoT からインターネットへの接続の制限
- 関連する脅威の検出
- OT/IT 資産のインベントリーの作成

デバイス セグメンテーションのための より安全なアーキテクチャー

ネットワーキングの基本とされてきたセグメンテーションは、アクセス制御リスト (ACL) やファイアウォールなどのツールを使用して、南北 (クライアントとサーバー間) トラフィックを管理してきました。しかし、OT セグメンテーションでは、デバイスとワークロード間を水平方向に流れる、より脆弱な東西トラフィックに焦点が移ります。共有 VLAN は旧式のスイッチング アーキテクチャーを採用しており、デバイス同士が相互に認識して通信できるため、マルウェアが拡散しやすい脆弱な環境が生まれます。残念ながら、クラウド ワークロード向けに開発されたエージェントベースのソリューションでは、OT で一般的な旧式のヘッドレス マシンをセグメント化できません。また、従来の ACL ベースのアプローチは依然として非常に複雑です。



Zscaler Zero Trust Device Segmentation のダッシュボード

Zscaler は、ユーザー、デバイス、ワークロードが通信するための、よりシンプルで安全、かつ費用対効果の高い方法として、Zscaler Zero Trust Networking を導入しました。デバイス セグメンテーションは、現代のネットワークをきめ細かく可視化し、制御するための基礎的なステップとして、このアプローチの重要な要素となっています。

Zscaler は、旧式のヘッドレス システムを含むすべての IP エンドポイントを「1 つのネットワーク セグメント」に分離します。そして、すべての脅威のラテラル ムーブメントを阻止するエージェントレス ソリューションで、VLAN 内のセグメンテーションの課題を解消します。これにより、複雑な ACL や既存のインフラの変更が不要になり、最もきめ細かく効果的なセグメンテーションが可能になります。

ユース ケース

エージェントレスのデバイス セグメンテーションの代表的なユース ケースとして、以下が挙げられます。

LAN 内部のセグメンテーション

ゼロトラストを LAN に拡張するには、東西トラフィックをセグメント化します。これにより、内部の攻撃対象領域が縮小し、重要な OT/IoT ネットワークにおける脅威のラテラル ムーブメントが排除されます。NAC やファイアウォールベースのセグメンテーションは一切必要ありません。

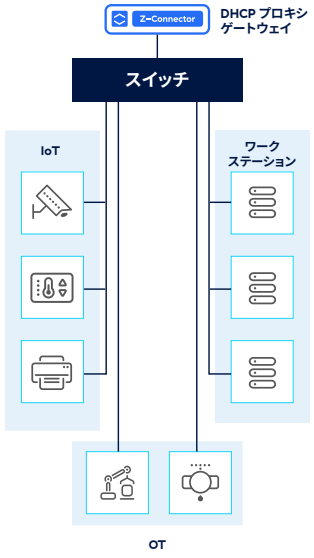
ネットワークにゼロトラスト セグメンテーションを実施するシンプルな方法は以下のとおりです。

- すべてのデバイスを 1 つのセグメントに自動プロビジョニングする (/32 を使用)
- 不正なデバイスが MAC を装ってネットワークに侵入するのを防ぐために、デバイス、ユーザー、アプリのトラフィック パターンを分析して自動的にグループ化する
- ユーザーとデバイスのアイデンティティーとコンテキストに基づいて、東西トラフィックのポリシーを動的に施行する

IT/OT セグメンテーション

Zscaler Zero Trust Device Segmentation は、ランサムウェアの機能を止めるキル スイッチとして機能し、業務を中断することなく、重要でないデバイス通信を無効化して脅威のラテラル ムーブメントを阻止します。このソリューションは、IoT デバイスや OT システム、エージェントをインストールできないデバイス上のランサムウェアなどの高度な脅威を無力化します。

- 任意のデバイス上の既知の MAC アドレスを自動的にグループ化し、ポリシーを施行する (例：管理者以外のカメラへの RDP アクセスを拒否)
- 不明な MAC アドレスを自動的に分離し、デバイスが侵害された場合の影響範囲を制限する
- 資産管理システムと統合し、安全なアクセス制御ポリシーを確保する



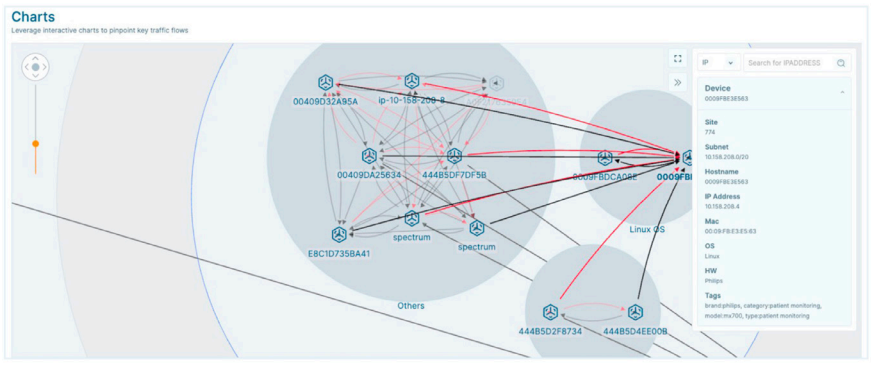
各デバイスを 1 つのセグメントに分離する、
自動化された IoT/OT セグメンテーション

デバイスの自動検出と分類

OT/IoT トラフィックの大部分はローカル ネットワーク内にとどまるため、東西トラフィックを継続的に可視化することが重要です。ネットワーク管理者は、デバイスの自動検出と分類により、複雑なインベントリー管理なしで、IoT/OT システムのパフォーマンス、稼働時間、セキュリティをより適切に管理できます。

以下を行うことで、ネットワークとデバイスを効果的に可視化できます。

- エンドポイント エージェントなしで、OT/IoT デバイスを検出して分類し、インベントリーを作成する
- トラフィック パターンとデバイスの振る舞いをベースライン化し、許可されたアクセスと許可されていないアクセスを特定する
- パフォーマンス管理と脅威マッピングに活用できる、ネットワークに関する正確な情報を取得する

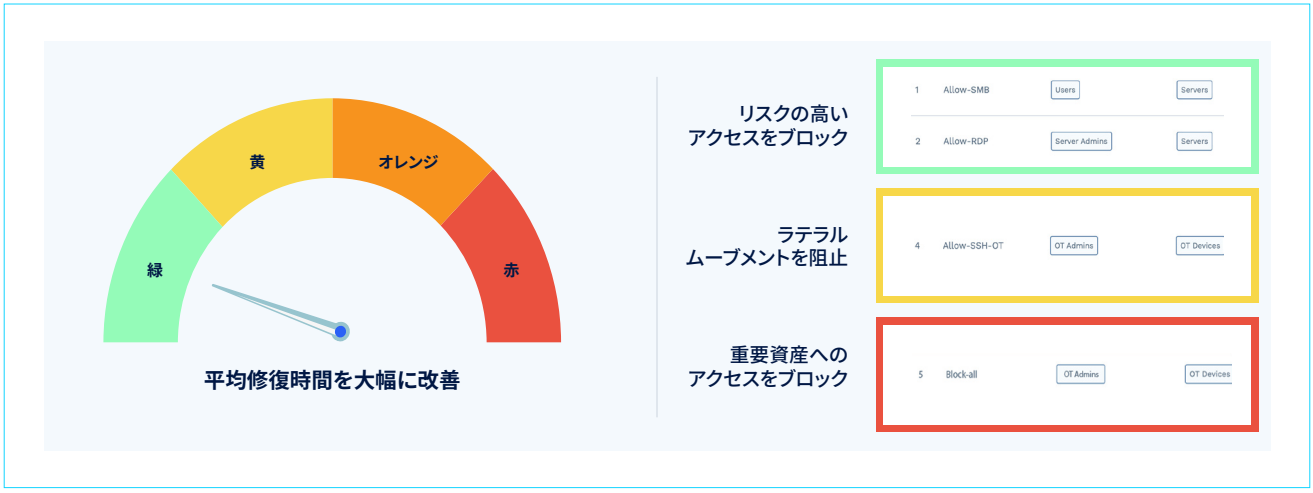


デバイス検出のダッシュボード

インシデント対応の自動化

新しい Zscaler Ransomware Kill Switch では、ワンクリックで攻撃対象領域を削減できます。Zscaler Zero Trust Device Segmentation ソリューションに統合されたこの機能は、既知の脆弱なプロトコルやポートを段階的に制限し、病院全体や工場のフロアなど重要なネットワークへのアクセスを瞬時に無効化します。すべてに重大度が事前に設定されているため、ビジネスのダウンタイムを最小限に抑えられます。

Ransomware Kill Switch は、多層型のポリシー施行ポイントとして機能し、進行中の侵害に対して段階的なインシデント対応を行うため、既存のセキュリティ ツールへの投資の増強につながります。Ransomware Kill Switch の各層には、「仮想ヒューズ」またはデフコン レベルに類似した機能があります。この機能により、事前定義されたエスカレーション パスに従ってエンドポイントとの間の不要なネットワーク通信がすべてブロックされるため、水平移動の阻止と攻撃対象領域の削減が可能になります。



このソリューションは、業務を中断することなく、重要でないデバイス通信を無効化して脅威のラテラル ムーブメントを阻止します。また、IoT デバイスや OT システム、エージェントをインストールできないデバイス上のランサムウェアなどの高度な脅威も無力化します。

Zscaler は、API を介して Ransomware Kill Switch を完全に制御します。IT 組織は、これらのプログラム可能なインターフェイスを使用して、セキュリティ情報とイベント管理 (SIEM)、セキュリティ オーケストレーションの自動化と対応 (SOAR)、EDR/XDR ソリューションなどの既存のセキュリティ オーケストレーション ツールを有効にできます。こうすることで、インシデント対応の自動化、侵害されたエンドポイントの瞬時の隔離、感染の影響範囲の封じ込めが可能になります。

これにより、既存のネットワークとセキュリティのインフラへの投資を保護しながら、セキュリティ態勢をすぐに改善できます。

メリット

きめ細かな封じ込めで水平方向への拡散を制限

事前設定された自動インシデント対応で侵害に適切に対処

組織の IT ネットワークとコア ネットワーク間など、重要な境界層で厳格な封じ込めを実行

疑わしいポートとプロトコルを効果的にシャットダウンし、ビジネスの稼働時間を最大化

LAN における脅威のラテラル ムーブメントを排除

攻撃対象領域を縮小するために、すべてを独自の「1 つのネットワーク」に分離し、攻撃対象領域や脅威のラテラル ムーブメントのリスクを排除します。侵害されたデバイスでさえ、隣のデバイスに感染することはできません。

従来のセグメンテーション ツールに関連する運用の複雑さとコストを削減

NAC や東西ファイアウォールのような旧式で IP 中心のネットワーキング テクノロジーや、ACL または手動の VLAN セグメンテーションなどの複雑な構造なしに、すべての IP エンドポイントをセグメント化できます。

東西トラフィックの可視性を強化

デバイスの自動検出と分類により、東西トラフィックが完全に可視化されます。ネットワーク管理者は、エージェントをインストールできないデバイスも含め、あらゆるデバイスのパフォーマンス、稼働時間、セキュリティをより適切に管理できます。

ネットワークを中断させることなく導入

エージェントレスの技術により、業務を中断することなく迅速に導入できます。ネットワーク アーキテクチャーの変更やデバイスの IP アドレスの再指定は必要ありません。

コンプライアンスを迅速に確保

連邦政府のサイバー基準では、あらゆる業界でゼロトラストの基盤としてセグメンテーションを提唱するようになっています。Zscaler のエージェントレス アプローチにより、迅速かつ瞬時に導入でき、コンプライアンス態勢が向上します。

機能

Airgap の分離

- エージェントレスのデバイス分離
- ワンクリックでのデバイス隔離
- Airgap の分離による違反検出
- MAC アドレスベースのフィルタリング

ゼロトラスト セグメンテーション

- ネットワークベースのセグメンテーション

デバイスベースのセグメンテーション

- 自律的なグループ化とポリシー
- VLAN 内と VLAN 間のポリシー制御
- 動的なタグベースのポリシー
- デバイスとユーザーのアイデンティティーベースのポリシー
- 時間ベースのポリシー
- ゾーンベースのポリシー
- 階層的なポリシー フレームワーク

資産の検出とプロファイリング

- エンドポイントとネットワークの検出
- デバイス フィンガープリンティング
- プロファイルベースのデバイスの分類
- ICS/ 医療のプロトコルのデコード

高可用性

- VRRP を使用した 2 ノード クラスター
- セッション同期を使用した VRRP
- 構成と状態の同期
- リンクの集約
- インターフェイスの稼働状況モニタリング
- ソフトウェアのヒットレス アップグレード
- 稼働中のハードウェアのリプレース

ルーティングとネットワークのサービス

- 動的なルーティング ーBGP、OSPF
- マルチキャスト ルーティング ーIGMP、PIM
- DHCP サーバー、リレー / プロキシ
- VLAN トランキング
- ネットワーク アドレスの変換
- ポリシーベースのルーティング
- 等コスト マルチ パス (ECMP)
- サイト間 VPN

インシデント対応

- Ransomware Kill Switch

可視性とロギング

- ポリシー相関を含むトラフィック マップ
- 統合された柔軟なデータ レイク
- セグメント内とセグメント間のすべての通信に対するセッション開始ログ
- SIEM/ ログ コレクターへのログのエクスポート

柔軟な導入モデル

- Airgap のゼロタッチ ゲートウェイ プロビジョニング
- サイトのテンプレートとプロファイル
- スタンドアロン、高可用性クラスター、またはマルチクラスター展開
- 物理マシンまたは仮想マシンベースの Airgap ゲートウェイ

モニタリングとトラブルシューティング

- リモート デバッグ コンソール
- Airgap ゲートウェイのローカル CLI
- SNMP サポート

クラウドベースの一元管理

- シングル サインオン (SSO) と MFA
- ログイン イベントと構成変更の監査証跡
- ロールベースのアクセス制御
- マルチテナント クラウド配信プラットフォーム
- API ベースのアクセス

サードパーティーとの統合

- Microsoft Active Directory
- SIEM 統合
- EDR ベンダー ーCrowdStrike、SentinelOne
- 資産管理 ーArmis
- SSEーZscaler ZIA

Zscaler のゲートウェイ アプライアンスのサイジング

Zscaler が提供するハードウェアまたは仮想のゲートウェイ アプライアンスのサイジングは、以下の表のとおりです。

ハードウェアの仕様 (物理ゲートウェイの導入)

	XS	S1	S2	M	L	XL
利用可能時期	2024年6月	2024年6月	利用可能	利用可能	利用可能	25年度第1四半期
ハードウェア モデル	ZT400	ZT600	Dell VEP4600	Dell VEP4600	Dell VEP4600	未定
CPU	4C Atom	8C Atom	4C Xeon	8C Xeon	16C Xeon	16C Xeon
メモリー	16GB	16GB	16GB	32GB	64GB	64GB
ストレージ	64GB	64GB	128GB	256GB	960GB	256GB
ポート	4x 1GbE	4x 1GbE	6x 1GbE 2x 1GbE (SFP)	4x 1GbE 2x 10 GbE	4x 1GbE 6x 10 GbE	4x 25GbE
フォーム ファクター	デスクトップ	デスクトップ	1U	1U	1U	1U
その他の機能	ファンレス		RPS	RPS	RPS	RPS
スループット (64KB HTTP)	4 Gbps	8 Gbps	10 Gbps	20 Gbps	40 Gbps	80 Gbps
セッション	25万	50万	50万	100万	200万	200万
エンドポイント数	200	500	1,000	2,000	4,000	未定

仮想アプライアンスのサイジング

	XS	S1	S2	M
利用可能時期	利用可能	利用可能	利用可能	利用可能
CPU	2 vCPU	4 vCPU	8 vCPU	16 vCPU
メモリー	8GB	16GB	32GB	64GB
ストレージ	256GB	256GB	256GB	256GB
ポート	4x vNIC	4x vNIC	4x vNIC	4x vNIC
スループット(64KB HTTP)	5 Gbps	10 Gbps	20 Gbps	40 Gbps
セッション	25万	50万	100万	200万
エンドポイント数	200	500	2,000	4,000

Zscaler の技術専門家によるデモ

当社の技術専門家とのデモを依頼して、重要インフラを保護する Zscaler ソリューションの詳細をご確認ください。

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 SASE 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