統合ゼロトラストの実践：

さまざまな領域に対応する高度な脅威対策を Zscaler と CrowdStrike で実現

パートナーシップの概要

はじめに

サイバー脅威環境はかつてないスピードで進化しており、攻撃者を検知できる時間はわずか 48 分[1]、場合によっては 51 秒[2] にまで短縮されています。これに加えて、マルウェアを使用しない攻撃が 79%[3] 増加しており、攻撃者は認証情報の窃取や信頼の悪用などの高度な手法を駆使して、マルウェアに特化した従来の防御策を突破しています。

さらに状況を複雑にしているのが、AI の急速な導入に伴う新たな脆弱性です。組織は 3.6 ペタバイト以上もの AI 関連の機密データを移動しており、これが事業運営の妨害や知的財産の窃取を狙う攻撃者にとって格好の標的となっています。十分に可視化されていない攻撃対象領域や静的で事後対応型のポリシーでは、こうした新たなリスクに積極的に対応できません。

これらの課題は、断片化されたセキュリティ アーキテクチャーによってさらに深刻化しています。サイロ化したツールや統合されていないプラットフォームは運用の非効率化やコストの増加を招くだけでなく、攻撃者に狙われやすい脆弱性も生み出します。これらの問題を解決するには、優れたプラットフォームを統合できるソリューションを採用する必要があります。

[1、2、3] CrowdStrike 2025 年版グローバル脅威レポート

Zscaler と CrowdStrike: 複雑なサイバーセキュリティ課題への挑戦

現代の動的な脅威に対応するには、高度に統合されたセキュリティ ソリューションのエコシステムが不可欠です。Zscaler と CrowdStrike はこの協働型アプローチを通じて、それぞれの強みを補完し合い、エンタープライズ セキュリティの新たな可能性を切り開いています。どちらもクラウドネイティブ プラットフォーム上に構築されており、従来型のモデルを改修したものではなく、現代のセキュリティ ニーズに合わせて設計されています。

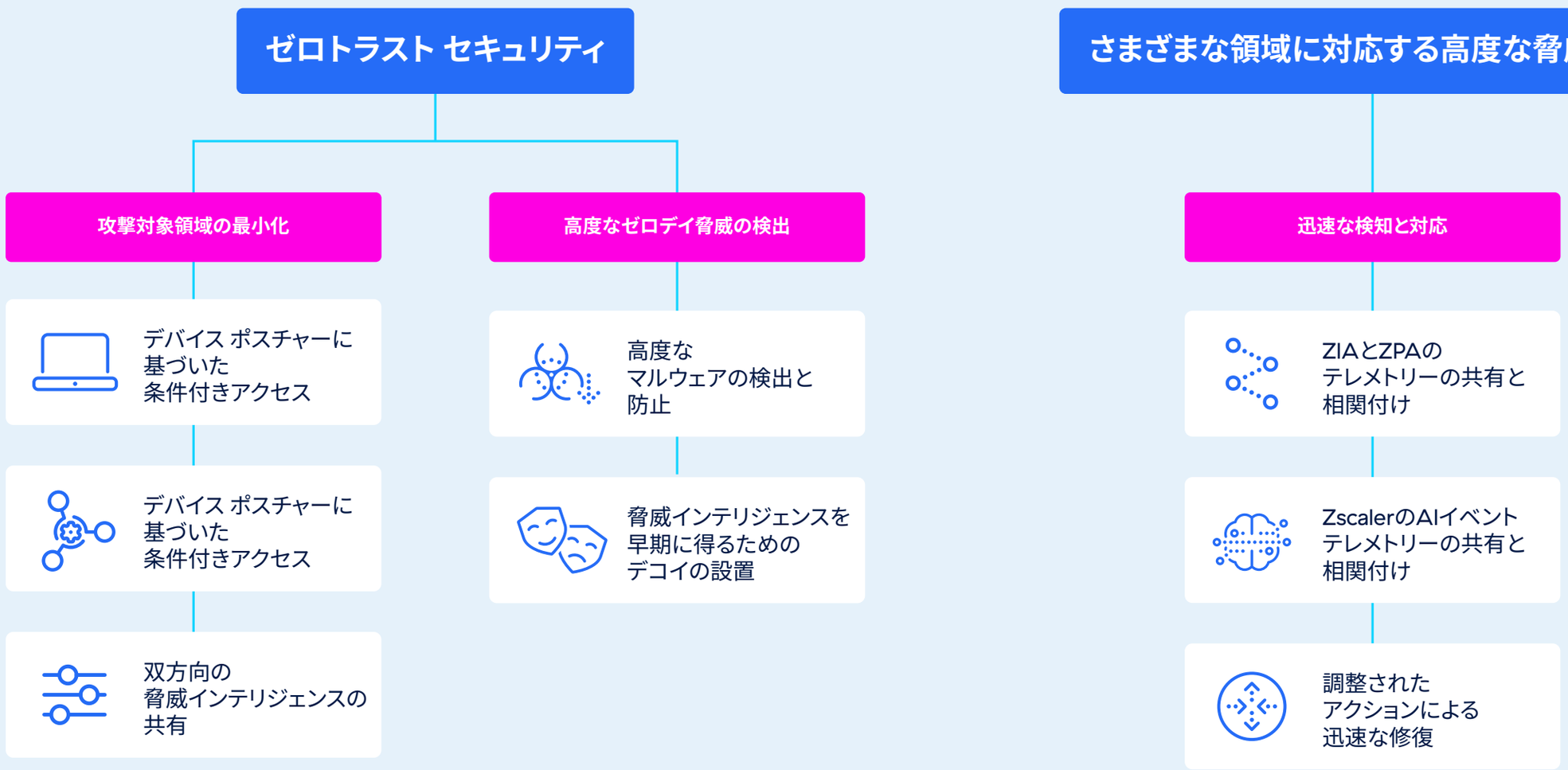
両社はゼロトラストを共通理念とし、インライン セキュリティ、安全なアクセス、エンドポイント保護、高度な脅威の検知と対応における業界基準を確立しています。このパートナーシップは、お客様の主要なニーズであるセキュリティの強化、コスト削減、管理の効率化に応えるとともに、今日の動的な脅威の課題への迅速かつ効果的な対応を可能にします。

Zscaler と CrowdStrike は、両社のクラウドネイティブ プラットフォームを連携させ、組織が従来のサイバー リスク管理から予防的なサイバー レジリエンス体制へと移行できるよう支援します。両社間のさまざまな統合を通じてインテリジェントなアクセス制御、適応型ポリシー、脅威インテリジェンスの共有を実現し、エンドポイント、ネットワーク、アプリケーションの脅威を効果的に最小化します。

統合の詳細

Zscaler と CrowdStrike は、ゼロトラスト原則とさまざまな領域に対応する脅威対策を融合したシームレスなセキュリティ フレームワークを構築し、現在の高度な脅威環境に対応するための多層型防御を提供します。このフレームワークによって、攻撃対象領域の最小化、新たな脅威の検出、対応の効率化が可能となり、組織全体で堅牢かつ実用的な保護が実現します。

ZscalerとCrowdStrikeが提供する多層型防御の統合フレームワーク



ゼロトラスト セキュリティ

Zscaler と CrowdStrike は、共有されたインテリジェンスを活用し、すべてのインタラクションにゼロトラスト原則を施行することで、アクセスを保護するとともに脆弱性を軽減します。

- **攻撃対象領域の最小化：**Zscaler と CrowdStrike は、安全で信頼できるデバイスのみが組織のアプリケーションとデータにアクセスできるようにすることで、攻撃対象領域を削減します。Zscaler は、CrowdStrike から提供される各デバイスに関するリアルタイムのリスク評価とアクティブなセキュリティ アラートに基づき、アクセスを自動的に調整します。また、CrowdStrike の最新の脅威インテリジェンスを活用し、Zscaler は有害な Web サイトや脅威を予防的にブロックします。これらの統合により、変化するリスクに常に適応するよりスマートなゼロトラストベースの保護を実現し、攻撃者が侵入したり、業務を中断させたりするリスクを大幅に削減します。

- **高度なゼロデイ脅威の検出：**Zscaler と CrowdStrike は、ゼロデイ脅威から組織を保護します。Zscaler は、高度なサンドボックス テクノロジーと CrowdStrike からの最新のデバイス情報を活用し、未知のマルウェアが拡散する前に迅速に検出、隔離します。また、Zscaler は攻撃者を早期にあぶり出すためのデコイを設置し、信頼できる早期警告とインテリジェンスを CrowdStrike に提供します。この統合された機能によって、組織は新たな脅威の一歩先を行き、被害が発生する前に対応できるようになります。

さまざまな領域に対応する高度な脅威対策

Zscaler と CrowdStrike は、組織のネットワークやエンドポイントで脅威を迅速に検出し、相関付けを行い、修復します。

- **迅速な検知と対応：**Zscaler Internet Access (ZIA) と Zscaler Private Access (ZPA) は、CrowdStrike Falcon Insight XDR と脅威テレメトリーを共有し、相関付けることで、ネットワーク トラフィック、エンドポイント、ワークロード全体で統合された脅威検出を可能にし、可視性を向上させます。また、Zscaler は AI を活用したイベント テレメトリーを CrowdStrike と共有し、脅威の相関付けの精度を高め、AI を悪用した脅威や異常をより迅速に特定します。この連携によって自動対応ワークフローが強化され、脅威の封じ込めや迅速な修復、トリアージ時間の短縮が可能となるほか、統一された正確なアクションで運用への影響を最小限に抑えることができます。

ZscalerとCrowdStrikeは、両社のクラウドネイティブ プラットフォームを連携させ、組織が従来のサイバー リスク管理から予防的なサイバー レジリエンス体制へと移行できるよう支援します。ゼロトラスト原則とさまざまな領域に対応する脅威対策を融合したシームレスな多層型防御を通じて、最新の高度な脅威に対応します。

この多層型防御アプローチは、最高水準のゼロトラスト フレームワークとさまざまな領域にわたる可視化、検知、対応を統合することで、組織がサイバーリスクに積極的に対処できる体制を構築し、最適なレジリエンスを確保できるようにします。Zscaler と CrowdStrike の統合は、以下の新しいユース ケースをサポートします。

- **セキュリティ態勢に基づいたアプリケーションへの条件付きアクセス制御**
  Zscaler は、CrowdStrike Falcon の Zero Trust Assessment (ZTA) スコアを統合することで、セキュリティに準拠した信頼できるデバイスにのみアクセスを許可します。脅威検出シグナルを活用して、準拠していないエンドポイントをブロックし、機密性の高いアプリケーションを保護します。ブラウザー分離は新たなセキュリティ レイヤーを追加し、制限付きのグループを保護しながら、ユーザーの生産性を維持します。

- **防御態勢を強化する脅威インテリジェンスの共有**
  CrowdStrike は、侵害の痕跡 (IoC) に関する貴重な脅威インテリジェンスを Zscaler と共有し、Zscaler がカスタム ブロック リストを強化できるようにします。これにより、ネットワーク上の悪意のあるドメインや URL をブロックし、予防的な脅威対策を行います。

- **リスク評価と意思決定のためのリアルタイムのコンテキストを備えた適応型アクセス**
  Zscaler は CrowdStrike からの Zero Trust Assessment (ZTA) デバイス スコアとデバイスのセキュリティ インシデント シグナルを活用し、適応型アクセス制御を施行します。適応型ポリシーはリアルタイムのリスク変化に応じて動的に調整されるため、コンテキストを踏まえた精度の高い意思決定とポリシー施行が可能になります。

- **高度なマルウェアの検出と防止**
  Zscaler の高度なクラウド サンドボックスは、ゼロデイ マルウェアを検出し、CrowdStrike Falcon を通じて隔離ワークフローを即座に開始します。これにより、セキュリティ部門は感染したエンドポイントを迅速に隔離し、適切な判断を下し、脅威の拡散を未然に防ぐことができます。

- **脅威インテリジェンスを早期に得るためのデコイの設置**
  Zscaler Deception は、デコイを展開して重要なシステムから離れた場所に攻撃者を誘導することで、攻撃サイクルの早い段階で侵害を検知します。信頼性の高いアラートは CrowdStrike Falcon と共有されるため、脅威対応ワークフローの改善、侵害されたファイルの除去、より迅速で効果的な防御体制の構築が可能になります。

- **ZIA と ZPA のテレメトリーの共有と相関付け**
  Zscaler は、ZIA と ZPA からのネットワーク テレメトリーを CrowdStrike の次世代 SIEM と共有し、さまざまな領域にわたって脅威の可視性と検出を強化します。脅威が検出されると、クロスプラットフォームのワークフローがユーザー アクセスを制限し、重要なアプリケーションを隔離します。そして、脅威を迅速に封じ込めながら、不正なアクティビティーを防止します。

- **AI イベント テレメトリーの共有と相関付け**
  Zscaler は AI イベント ログを CrowdStrike の次世代 SIEM と共有し、重要な AI ベースのセキュリティ インサイトを相関付けます。ノイズを排除することで、可視性を向上させ、検出速度を高め、不正な AI の使用を阻止し、アプリケーションとエンドポイント全体で堅牢な防御を確保します。

- **調整されたポリシー対応を可能にする脅威インテリジェンス共有の自動化とオーケストレーション**
  Zscaler と CrowdStrike は、自動化と同期されたワークフローを通じて、脅威インテリジェンスの共有を効率化し、調整された対応アクションを促進します。SecOps 部門は FALCON Fusion に組み込まれた SOAR ワークフローを活用して、ZIA の高度なサンドボックス、CrowdStrike の次世代 SIEM、ZIA のポリシー施行エンジン間でクローズドループの修復プロセスを構築できます。

統合のメリット

- **統合ゼロトラストの実践：**Zscaler と CrowdStrike は、動的なアクセス制御を施行して攻撃対象領域の露出を削減することで、ゼロトラスト セキュリティを強化します。正規のユーザーには重要なシステムへの安全なアクセスを提供しながら、攻撃の可能性がある活動を制限します。脅威インテリジェンスの共有により、セキュリティ部門は運用効率が向上し、ネットワーク レイヤー全体の可視性を改善できます。

- **予防型のゼロデイ防御：**危険な動作や未知の脆弱性に関する早期のインサイトを活用し、ゼロデイ脅威を迅速に特定して軽減します。Zscaler と CrowdStrike を組み合わせることで、防御を強化し、新たな攻撃から機密データやワークロードを保護できます。

- **迅速な脅威検出と AI 防御：**ネットワークやエンドポイントのテレメトリーに加えて、AI を活用したイベント ログを一元化することで、脅威の検知、調査、そして対応のスピードが向上します。この統合された仕組みにより、脅威の迅速な相関付けとセキュリティ ワークフローの効率化が可能となるため、攻撃者がシステム内に留まる時間を短縮し、リスクを最小限に抑制できます。

- **脅威の封じ込めの自動化：**Zscaler と CrowdStrike のプラットフォームで統合された対応ワークフローにより、セキュリティ部門は正当なビジネス活動を中断することなく、脅威を迅速に封じ込め、修復できます。自動化されたオーケストレーションにより、運用への影響を抑えながらインシデント対応を効率化し、時間とリソースを節約します。

進化する脅威への防御を強化する Zscaler と CrowdStrike の統合

AI を悪用した攻撃や新たな脆弱性が増加するなか、サイロ化したセキュリティ ツールや旧式のアプローチでは防御が難しくなっています。今、組織に求められるのは、高度な脅威に対応するために構築されたスピード、インテリジェンス、多層型防御を備えた適応型の統合サイバーセキュリティ エコシステムです。

Zscaler と CrowdStrike は、戦略的パートナーシップを通じて統合的なアプローチを提供します。Zscaler のクラウドネイティブなネットワークとゼロトラスト機能を、CrowdStrike の業界をリードするエンドポイントでの検知と対応技術と組み合わせることで、AI を悪用した脅威やマルウェアを使用しない攻撃など、新たな脅威に対する組織のレジリエンスを向上させます。

お客様の主要なニーズに応えるこのパートナーシップは、攻撃者の一歩先を行き、セキュリティ対策を合理化し、堅牢な防御をリアルタイムで維持する統合ソリューションを提供することで、複雑さを軽減し、コスト効率を高めます。Zscaler と CrowdStrike の連携は、サイバーセキュリティの革新的な未来を象徴するものです。適応性を備えた強力な統合型アプローチは、現代の複雑化する脅威環境への対応と防御を可能にします。

参考資料

統合ソリューションの詳細：**www.zscaler.com/jp/partners/crowdstrike**
Zscaler と CrowdStrike の展開ガイド (英語)

CrowdStrike について：
CrowdStrike は、現代の企業を動かす人、プロセス、テクノロジーを保護し、円滑な機能を可能にする、世界で最も先進的なクラウドネイティブ プラットフォームを提供し、セキュリティを再定義してきました。CrowdStrike は、エンドポイント、クラウド ワークロード、アイデンティティー、データなど、最も重要なリスク領域を保護し、お客様が攻撃者の一歩先を行き、侵害を阻止できるようにします。CrowdStrike Falcon® プラットフォームは、CrowdStrike Security Cloud を搭載し、リアルタイムの攻撃指標、進化する攻撃者の手口に関する脅威インテリジェンス、組織全体からの充実したテレメトリーを活用して、超高精度の検知、自動化された保護と修復、精鋭による脅威ハンティング、優先付けられた脆弱性のオブザーバビリティーなどをすべて単一の軽量エージェントを通じて提供します。CrowdStrike のソリューションで、お客様は優れた保護、パフォーマンス向上、複雑さの低減、即時の価値実現を達成できます。詳細は、crowdstrike.com でご確認ください。

CROWDSTRIKE

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™ プラットフォームは、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.com/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.com/jp**

zscaler™

Zero Trust Everywhere