CLOUDFLARE

ビジネスインパクト

Zero Trustがリスク低減と技術効率改善をどのように実現するか

少ないオーバーヘッドでより多くを保護

Zero Trustベストプラクティスが財務とセキュリティにもたらす効果を定量化

サイバーリスクを低減

95% Zero Trust原則をビルトインしたSASEアーキテクチャによって、攻撃対象領域が縮小[1]

72% Zero Trust導入の最大の理由は「データセキュリティ強化」と答えたITリーダーの割合[2]

61% 「IDとリスクポスチャに基づく強力な認証」をメリットとして挙げたIT/セキュリティ専門家の割合[3]

↓23% Zero Trustをデプロイすることにより、デプロイしない場合に比べ、企業のデータ漏洩の平均コストを削減[4]

技術効率を改善

$700万 5組織へのZero Trust導入で削減されたレガシーセキュリティ費用（平均）[5]

$20 フルタイム当量 重複するセキュリティサービスをクラウドベースのZero Trustプラットフォームに換えることで節約（月額）[5]

↓80% 新しいインフラストラクチャのプロビジョンと保護の手間を削減[5]

39% 組織で使っているセキュリティ技術が古く、Zero Trustで最新化可能[6]

複雑なサイバーセキュリティの問題点[7]

#1 データ漏洩やサイバー攻撃の成功による財務的損失

#2 市場機会があってもすばやい革新は無理

#3 運用上の耐障害性が欠如

要因

- IDとコンテキストに基づく制御を全リクエストに適用し、過剰な信頼を抑制
- 全ユーザー、全アプリケーション、全デバイスの可視性を高め、すばやく修正
- 脅威のラテラルムーブメントを抑制

要因

- レガシーポイントソリューションを単一クラウドプラットフォームに統合することによって簡素化
- オンプレミス装置にトラフィックをバックホールしない、シンプルなセキュリティワークフロー
- ハイブリッドワークフォース全体に一貫したポリシーを適用

Zero Trustはあなたの組織の戦略思考の転換です

従来のITセキュリティ：境界が信頼を決定		Zero Trust：境界なし、常に検証
境界を保護、ネットワーク内は安全（「城と堀」）	保護	リスクを想定、影響を軽減（暗号化、検査、マイクロセグメント）
境界でのログインのみをログ記録	可視性	場所を問わず全ログイン、全リクエストをログ記録
デフォルトは許可、ネットワークロケーションに基づく静的アクセス	制御	デフォルトは拒否、IDとコンテキストに基づく最小特権アクセス

Zero Trustでサイバーリスク低減を始めましょう

ご相談のお申し込みはこちら

相談はまだいいという方は：

- Zero Trustがチームの生産性をいかに改善するかを知ってください：**概説を読む**
- 同業他社がハイブリッドワークにどう取り組んでいるかを知ってください：**概説を読む**
- Zero Trustを実現するためのベンダー非依存型ロードマップをご覧ください：**ホワイトペーパーを読む**

1. Cloudflareのお客様の体験に基づく
2. 「Capterra's 2022 Zero Trust Survey」、2022年8月（リンク）
3. 「Global Study on Zero Trust Security for the Cloud」、Ponemon Institute LLC、2022年7月（リンク）
4. 「The Cost of a Data Breach Report」、IBM、2022年（リンク）
5. 「The Total Economic Impact ™ of Zero Trust Solutions from Microsoft」、Forrester Research、2021年12月（リンク）
6. 「Security Outcomes Study」、Cisco、2021年12月（リンク）
7. 「2022 Global Digital Trust Insights」、PWC、2022年9月（リンク）