Cisco Security Summit

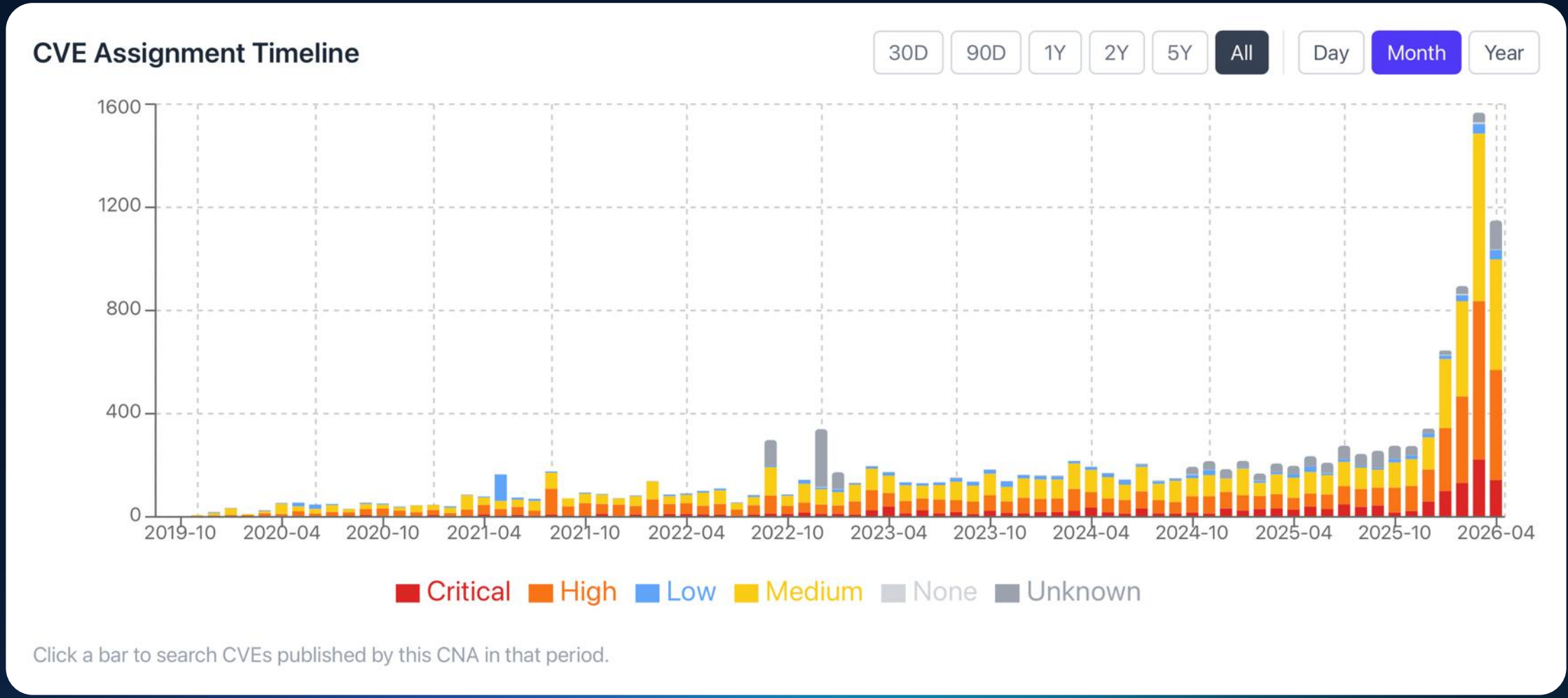
AI 時代のサイバー防御戦略ナビゲーション

Matt Fussa
Trust & Compliance 担当 VP

2026 年 7 月 10 日

新たな AI 脅威環境

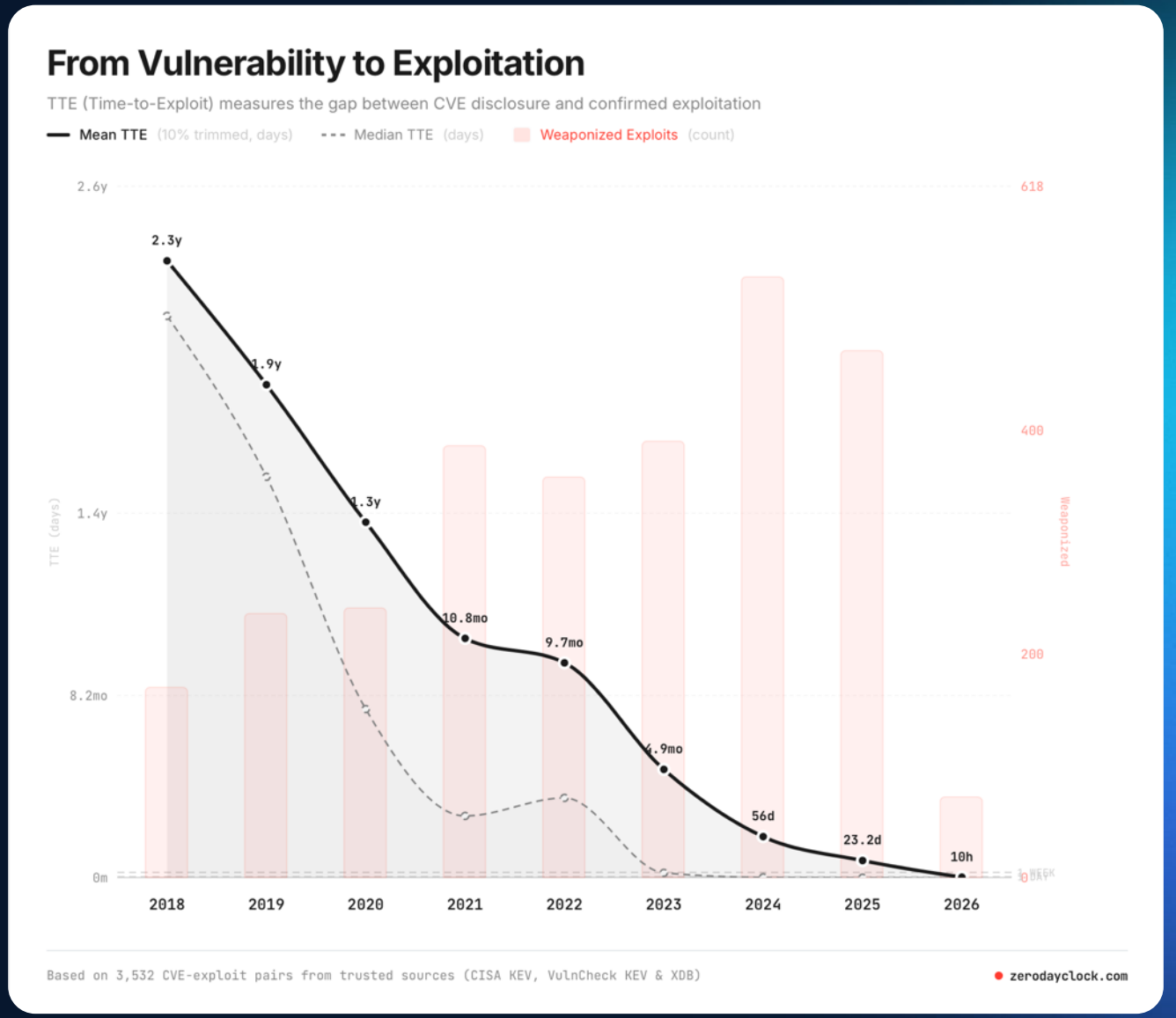
脆弱性報告数が急増



出典: https://vulntools.net/cnas/GitHub_M

兵器化までの猶予期間が消滅

業界全体のあらゆるベンダーに影響



出典：https://zerodayclock.com/

攻撃者は AI スピードで脆弱性を検出

48%

老朽化または
陳腐化した状態にある
ネットワークアセットの割合
（世界規模）

40%

攻撃の標的となった
脆弱性上位 100 件のうち、
サポート終了システムに
影響が波及したものの割合

32%

攻撃の標的となった
脆弱性のうち、10 年以上前に
検出されていたものの割合

23%

攻撃の標的となった
システム・機器のうち、
ネットワーク
インフラストラクチャ
デバイスが占める割合

出典：Talos の『一年の総括』、（シスコの重要レポート最新版）

シスコの適応策

シスコによる課題へのアプローチ

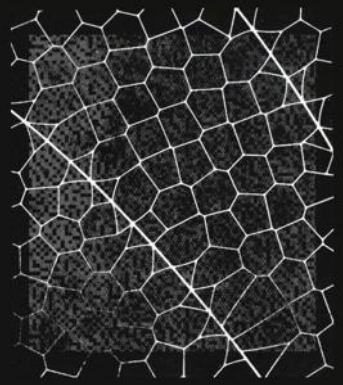
- 業界でのコラボレーションとリーダーシップ
- 既存のコードの修復
- 開発プロセスの統合
- イノベーション実現による脅威への対処
- レジリエントなインフラストラクチャ

AI 主導のセキュリティ
業界でのコラボレーションとリーダーシップ

ANTHROP\C

Project Glasswing

AI 時代に
不可欠なソフトウェアの保護



OpenAI

2026 年 4 月 14 日　セキュリティ　安全性

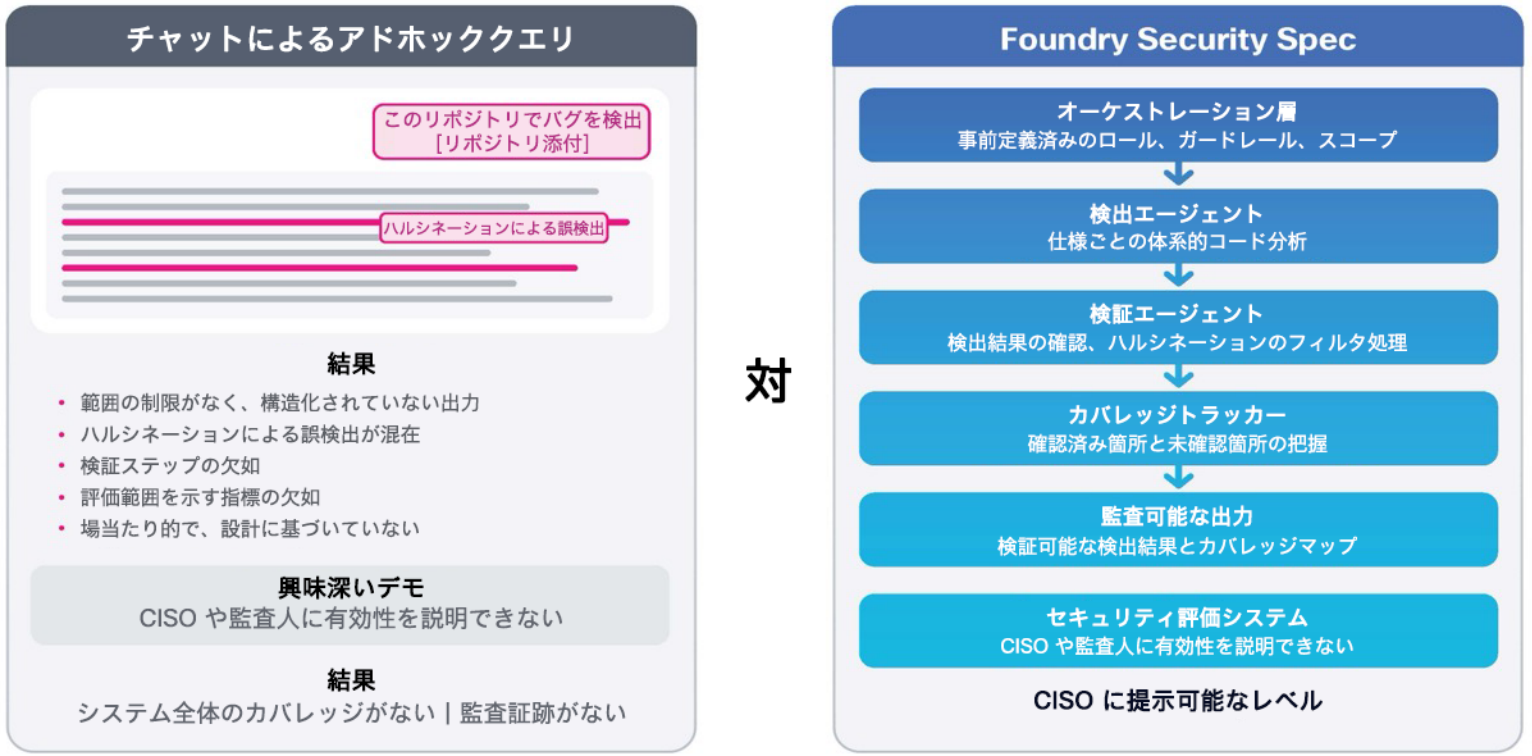
次世代のサイバー防御に向けた信頼できるアクセス

当社は、あらゆる人を守るサイバー防御担当者を支援すべく、信頼できるアクセス、保護対策、エコシステムのサポートを絶えず進化させていきます。

Foundry Security Spec

ノイズだらけのアラートを脱却し、実証可能な脅威の特定へ

github.com/CiscoDevNet/foundry-security-spec



これを基盤として構築し、

環境に合わせて適応させ、

コミュニティへ貢献

Project CODEGUARD

https://project-codeguard.org

4

セキュリティの自動化

結果：安全なコード開発

3

PR のレビュー

CodeGuard のルールをプルリクエストのレビュープロセスに組み込み、コード品質とセキュリティを強化

2

コードスキャン

包括的なコードスキャンを実施して、潜在的な問題を早期に検出

1

ルールの適用

コード作成時に CodeGuard のルールを適用し、セキュリティ上の問題を防止

シスコが実現する
レジリエントな
インフラストラクチャ

すぐに得られる
基本のセキュリティ態勢

デフォルト搭載の充実した防御機能

セキュリティリスクとなる
レガシー機能の排除

優れた検出と対応を実現する高度な機能

cisco

統合開示モデル

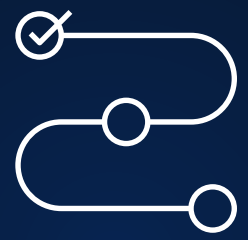
「1 件の脆弱性につき 1 つの CVE」モデルからの脱却

重大な脆弱性に
優先的に対処

1

実用的インテリジェンスにより
重大な問題にパッチを
迅速に適用

2



軽微な修正は標準の
リリースサイクルに集約

3

cisco

今後の対応

レガシーシステムのリスクに今すぐ対処すべき理由

1. レガシーシステムは現代の脅威が生まれる前に設計されたものであり、最新の攻撃に対する保護機能を搭載していない。
2. EOL を迎えるということは、現代のセキュリティ標準に適合しない古い手法（パッチ適用など）で管理しなければならないことを意味する。
3. 新機能や今後登場するイノベーション（レジリエントなインフラストラクチャ、ライブ保護など）は、レガシーハードウェアをサポートしていない。

お客様への「確実な」推奨事項

基本対策の徹底	フィッシング耐性のある MFA、ゼロトラストアーキテクチャ、一貫したパッチ管理、厳格な最小権限アクセスを最優先する
構造的リスクの排除	EOL システムを排除し、メモリ安全性とエクスプロイト対策を備えた最新プラットフォームへと刷新する
マシンスピードでの自動化	検出、トリアージ、封じ込めの自動化に投資する
アクティブ防御の組み込み	ワークロードとトラフィックパスそのものに保護機能を組み込み、リアルタイムでの防御を実現
防御のための AI 活用	脅威ハンティング、適合性テスト、デジタルツイン、検証に AI を活用。これにより展開サイクルを短縮

優先順位の高いアクション

1. 可視性の確保
2. 更新とアップグレード
3. レガシーリスクの排除
4. 既知の脅威の優先順位付け
5. 防御の刷新
6. 自動パッチ適用インフラへの投資

外部リソース

ホワイト ペーパー

防御態勢の強化：AI活用型攻撃の時代における防御のためのガイダンス

ウェブサイト

防御体制の強化

ビデオ　（英語のみ）

Glasswing: Mythos demands a new model for infrastructure

シスコブログ

AI を活用したサイバー防衛の時代へ

わずか 8 週間で 8 年分のセキュリティ研究を実現：AI が切り拓くサイバーセキュリティの変革

基盤の強化：AI によって加速する脆弱性発見に対する、予測可能でお客様重視の対応


CISCO