リアルタイムで中断なくデータセンター ネットワーキングのセキュリティリスクを軽減

重要なデータセンター インフラストラクチャにおける脆弱性のコスト

AI バックエンドと推論システムを支えるデータセンターは、現代のビジネスに不可欠です。ただし、その重要な役割によってリスクも高まります。パッチが適用されていない CVE やゼロデイ攻撃は、経済的損失、企業イメージの低下、サービスの中断を招く可能性があります。

現在の脅威環境において、この「パッチ適用のギャップ」は重大な脆弱性です。攻撃者が CVE をエクスプロイトするのに数時間しかかからない一方、防御システムが実稼働環境全体でパッチをテストして展開するのには数週間、場合によっては数か月かかることも珍しくありません。

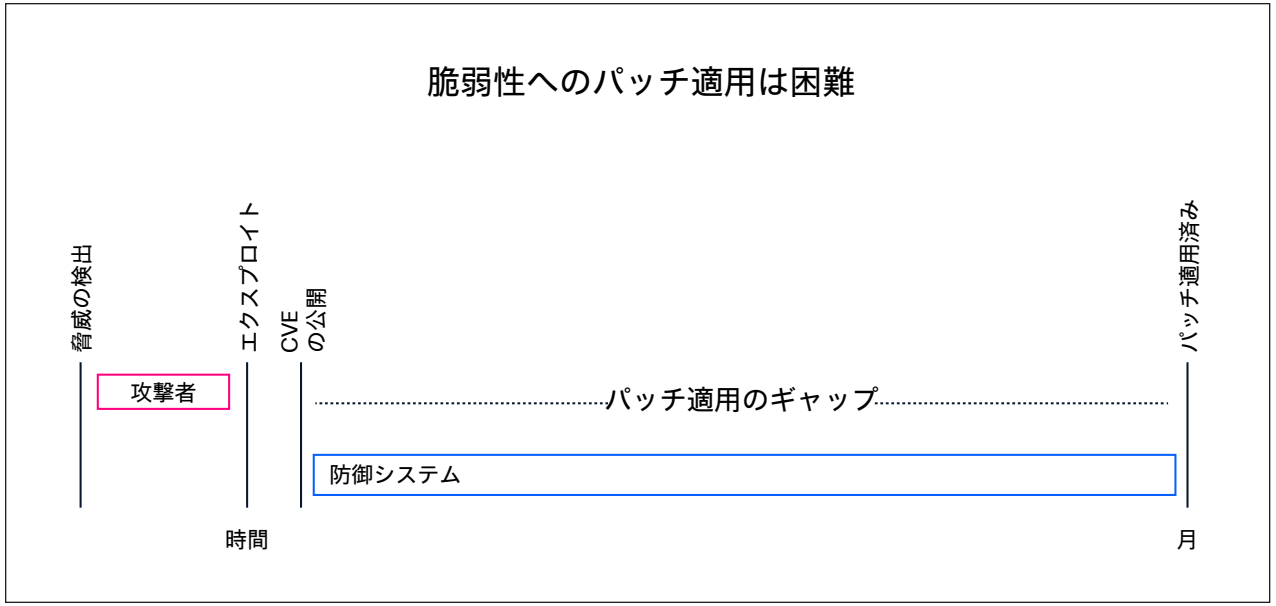

図 1.　脆弱性へのパッチ適用は困難

Cisco® Live Protect は、Cisco Nexus® スイッチに脆弱性シールドを即座に提供することで状況を一変させます。これにより、ネットワークを停止させることなく攻撃を阻止できます。データセンター インフラストラクチャを維持するには、一貫したセキュリティと信頼性の高い稼働時間が必要です。従来の CVE へのパッチ適用は、多くの場合、中断やダウンタイムを発生させます。N9000 シリーズ スイッチ向け Cisco Live Protect は、脆弱性を即座に軽減するリアルタイムのシールドを提供し、緊急メンテナンスや緊急のアップグレードを必要とせずに、継続的な保護と安定性を確保します。

Cisco Live Protect を選ぶ理由

従来のパッチ適用では、メンテナンスウィンドウと再起動が必要であり、ダウンタイムが発生する可能性があります。Cisco Live Protect は、セキュリティに対する革新的なアプローチを提供します。

- **ゼロダウンタイム：**スイッチを再起動することなく、実稼働システムにセキュリティポリシーを適用できます。
- **即時保護：**通常の PSIRT アップグレードがスケジュールされるはるか前でも、脅威が検出され次第、脆弱性を保護します。
- **継続的な再検証：**eBPF を活用したセキュリティ オブザーバビリティにより、セキュリティ態勢を維持します。
- **運用効率：**PSIRT バンドルの完全なアップグレードが適用されると、セキュリティ SMU（シールド）は削除されます。

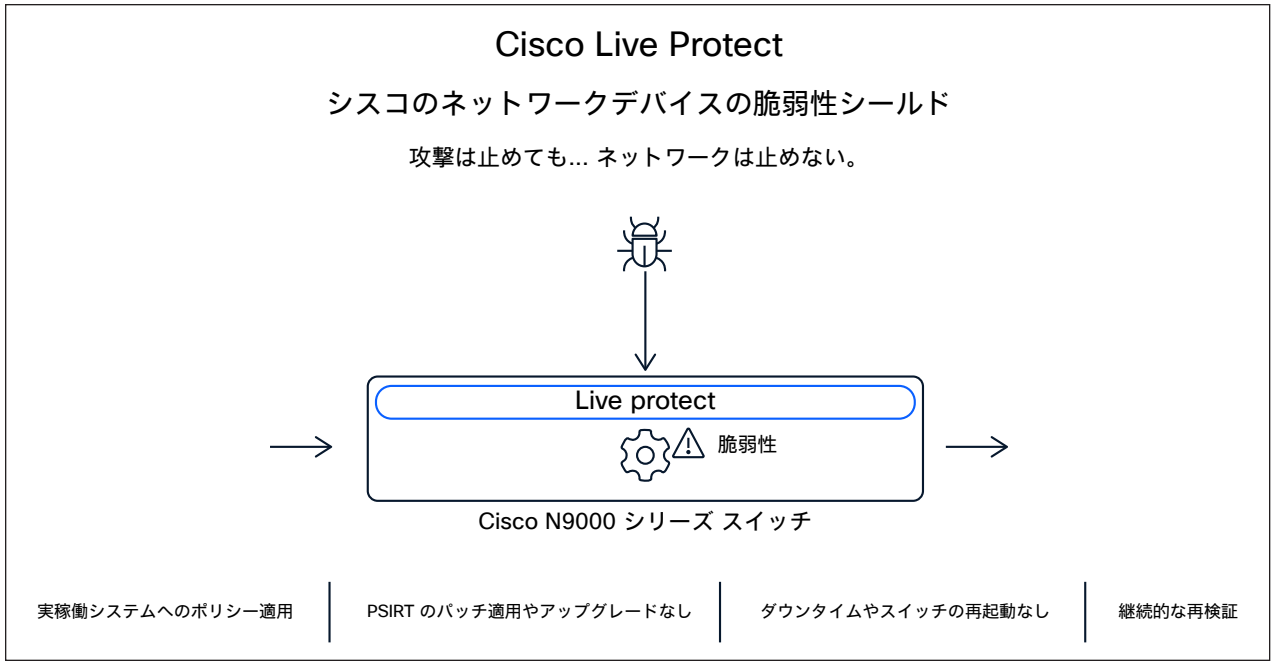

図 2.　Live Protect

eBPF が実現するイノベーション

シスコは、10.6(1)F リリース以降、Cisco NX-OS に直接組み込まれたエンタープライズグレードの Tetragon エージェントを市場に初めて投入しています。Live Protect は eBPF（extended Berkeley Packet Filter）を活用し、以下についてカーネルレベルの詳細な可視性と適用を実現します。

- 特権昇格の防止
- コントロールプレーン保護
- API と CLI のセキュリティ
- ファイル I/O モニタリング

サポートされるプラットフォーム

Live Protect は、**Essentials 以上のライセンス**をお持ちの Nexus のお客様が利用できます。

プラットフォームサポート（Cisco NX-OS 10.6(2)F）：

- Cisco N9300 および N9200 固定型プラットフォーム（24GB 以上の RAM）
- Cisco N9300 スマートスイッチ
- Cisco N9400 シリーズ スイッチ

仕組み

Cisco Live Protect は、高度な eBPF テクノロジーを使用して、データセンターのネットワークデバイスのリアルタイムセキュリティを実現します。構成は回数変更可能で、Cisco NX-OS CLI または API を介した個々のデバイスの管理、または CI/CD パイプラインを介したデータセンターファブリック全体の完全な自動化が可能です。Nexus Dashboard は一元化されたオーケストレーションを提供し、CVE の影響を受けるデバイスを即座に可視化し、セキュリティシールドのデプロイメントを自動化し、その有効性を継続的に監視します。

コンポーネント

- **Cisco Live Protect:** eBPF テクノロジーを使用してネットワークデバイスにカーネルレベルの保護を提供します。
- **Tetragon エージェント:** CVE 補完コントロールを展開可能な eBPF ポリシーにコンパイルします。
- **Nexus Dashboard:** すべての Cisco Nexus スイッチにわたるオーケストレーション、可視性、モニタリングのための一元化されたコンソール
- **統合ツール:** API、CLI、CI/CD パイプラインのサポートにより、シームレスな自動化と管理を実現

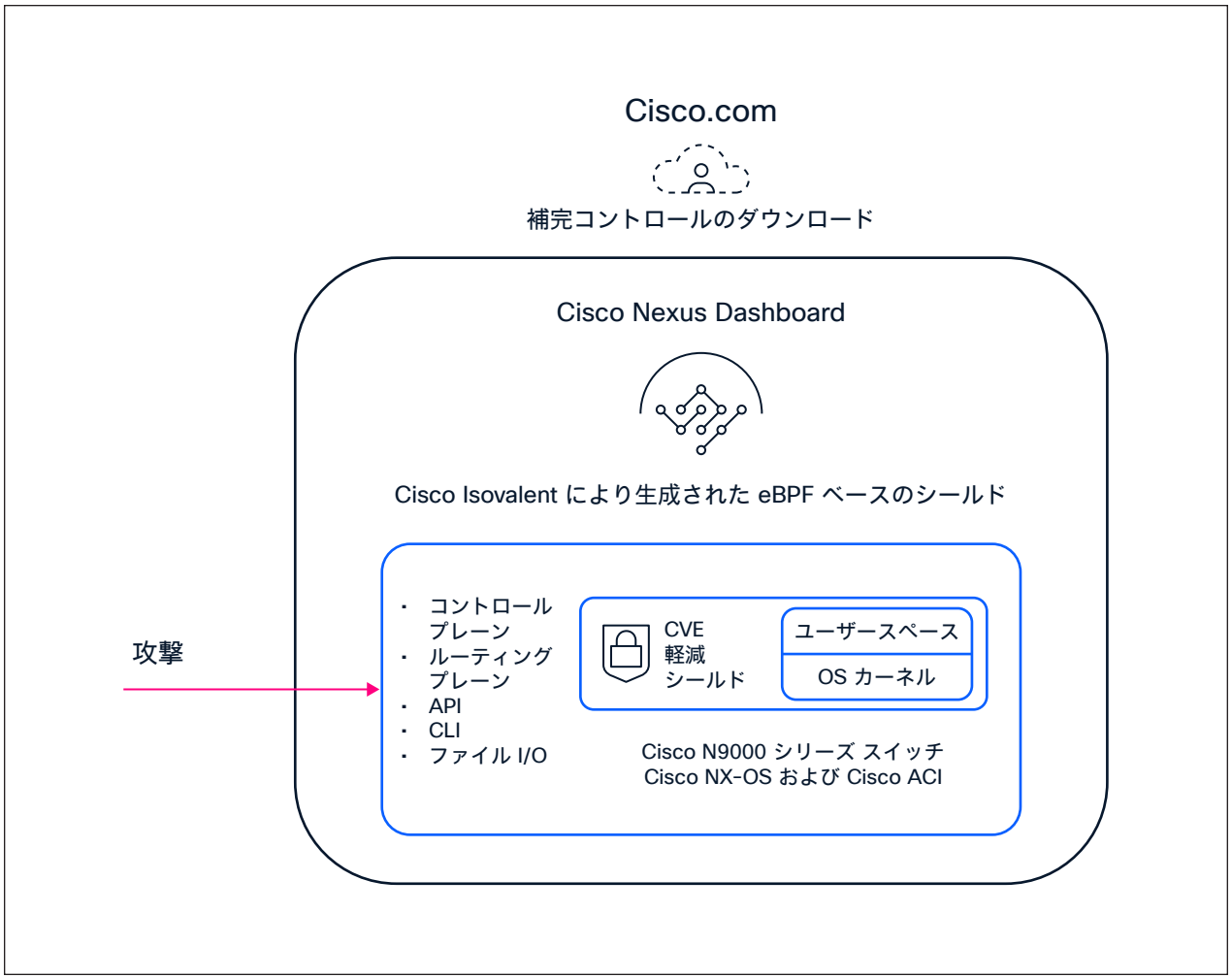

図 3.　Cisco N9000 シリーズ スイッチ向けの Live Protect と CVE 軽減策

Live Protect は、Cisco NX-OS および Cisco ACI® 環境でアップグレードを効率化し、脆弱性を継続的に軽減することで、インフラストラクチャのコアからシステム全体にわたって、中断のないセキュリティとパフォーマンスを維持します。

詳細を見る

Cisco Live Protect でデータセンターを保護し、リアルタイムの自動化されたセキュリティとゼロダウンタイムを実現します。

詳細については、Cisco Live Protect のブログをご覧になるか、今すぐシスコの担当者にお問い合わせください。

技術情報

Cisco Live Protect の Web ページ

Cisco Live Protect の実際の動作をビデオで確認

Cisco NX-OS リリースノート。

ユースケース

業界	Cisco Nexus と Live Protect の主なユースケース
金融サービス	• リアルタイムの CVE 軽減策 • ゼロデイ攻撃からの保護 • 重要なアプリケーションのダウンタイム最小化 • コンプライアンスと監査への対応の強化
医療	• 機密性の高い患者データの保護 • リアルタイムの CVE 軽減策 • 医療システムの継続的な可用性 • コンプライアンス (HIPAA など)
小売と e- コマース	• 決済と顧客データの保護 • ピーク時のダウンタイムの最小化 • CVE とゼロデイ攻撃からのリアルタイム保護 • PCI DSS への準拠
政府 / 公共部門	• 一元化されたセキュリティ オーケストレーション • ゼロデイ脅威対応 • 法規制の遵守 • 機密情報の保護と、公共サービスの稼働時間の確保
通信およびサービスプロバイダー	• 高度な脅威 (DDoS など) に対する防御 • 中断のないネットワークパフォーマンスの維持 • セキュリティ運用の自動化 • ポリシー管理の一元化
エネルギー / 公益事業	• 重要な制御システムの保護 • CVE とゼロデイ攻撃のリアルタイム軽減 • 法規制の遵守 • レジリエンスと稼働時間の維持
教育および研究	• 知的財産と機密データの保護 • デジタルリソースへの継続的なアクセス • 脅威へのリアルタイム対応 • セキュリティ運用の自動化
製造	• OT および IT 環境の保護 • 脆弱性のリアルタイム軽減 • 知的財産の保護 • ビジネスの継続性の保証

C22-5771857-00 02/26